MOBILE SECURITY

Undang-undang Republik Indonesia Nomor 28 tahun 2014 tentang Hak Cipta
Lingkup Hak Cipta
Pasal 1
Hak Cipta adalah hak eksklusif pencipta yang timbul secara otomatis berdasarkan prinsip deklaratif setelah suatu ciptaan diwujudkan dalam bentuk nyata tanpa mengurangi pembatasan sesuai dengan ketentuan peraturan perundang-undangan.
Ketentuan Pidana Pasal 113
(1) Setiap Orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf i untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp 100.000.000 (seratus juta rupiah).
(2) Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp 500.000.000,00 (lima ratus juta rupiah).
(3) Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf a, huruf b, huruf e, dan/atau huruf g untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).
(4) Setiap Orang yang memenuhi unsur sebagaimana dimaksud pada ayat (3) yang dilakukan dalam bentuk pembajakan, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau pidana denda paling banyak Rp 4.000.000.000,00 (empat miliar rupiah).

MOBILE SECURITY

Riko Herwanto, S.Kom., MTI

DarmaJaya Press

Perpustakaan Nasional RI:
Katalog Dalam Terbitan (KDT)

MOBILE SECURITY

Penulis:
Riko Herwanto, S.Kom., MTI

Rancang Sampul & Penata Isi
Aura Creative

ISBN:

Cetakan Mei 2022
xii + 152 hlm. ; 15.5 x 23 cm

Penerbit
Darmajaya (DJ) Press

Alamat :
Kampus IIB DARMAJAYA
Jl. Zainal Abidin Pagar Alam No 93,
Bandar Lampung 35142, INDONESIA

KATA PENGANTAR

Assalamu'alaikum warahmatullahi wabarakatuh.
Bismillahirrahmanirrahim.

Alhamdulillah, segala puji selalu Kami panjatkan kepada Allah SWT atas ridho-Nya sehingga penulis mampu menyelesaikan buku berjudul 'Mobile Security' dengan lancar tanpa kendala berarti.

Buku ini ditulis sebagai media panduan mudah dan menyenangkan untuk melakukan proses perkuliahan. Keberhasilan buku ini tentu tidak akan terwujud tanpa adanya dukungan dan bantuan dari berbagai pihak.

Mempelajari kelemahan dan ancaman yang berhubungan dengan perangkat komputasi mobile memiliki penekanan spesifik pada teknik pencegahan termasuk konfigurasi keamanan sebagaimana juga kemanan perangkat lunak. Terdiri dari topik mobile computing, kelemahan komunikasi wireless, teknik pencegahan pada kelemahan komunikasi wireless infrastruktur, kelemahan platform mobile, kelamahan aplikasi mobile, teknik pencegahan kelamahan aplikasi mobile, kelemahan perangkat mobile, teknik pencegahan kelamahan perangkat mobile dan persyaratan kebijakan keamanan perangkat mobile perusahaan.

Ucapan terima kasih penulis sampaikan kepada keluarga yang selalu mendukung dan memberikan do'a terbaik dalam setiap perjalanan yang penulis lakukan. Ucapan terima kasih juga penulis sampai kepada Civitas Academica Institut Informatika dan Bisnis Darmajaya, beribu ucapan terima kasih pada semua pihak yang turut mendukung penulis yang tidak bisa penulis sebutkan satu per satu.

Buku ini tidak luput dari kekurangan dan kesalahan. Jika pembaca menemukan kesalahan apapun, penulis mohon maaf setulusnya. Selalu ada kesempatan untuk memperbaiki setiap kesalahan, karena itu, dukungan berupa kritik & saran akan selalu penulis terima dengan tangan terbuka.

Bandar Lampung, 29 November 2020

Penulis

DAFTAR ISI

KATA PENGANTAR ..... **v**
DAFTAR GAMBAR ..... **vii**
BAB I. CONFIDENTIALITY, INTEGRITY, AVAILABILITY, THREAT AND ETHICS **1**
1.1. Pendahuluan 1
1.2. Apa itu Mobile Security? 2
1.3. Risiko dan Serangan Seluler 3
1.4. Confidentiality / Privacy 5
1.5. Integrity 5
1.6. Availability 5
1.7. Threat 7
1.8. Ethics 12
1.9. Think Like A Hacker 21
1.10. Kesimpulan 22

BAB II. ANDROID PROGRAMMING **24**
2.1. Pendahuluan 24
2.2. Environment Setup dengan Android SDK 25
2.3. Menjalankan aplikasi pada perangkat Android nyata 29
2.4. Pengenalan pada Pemrograman Berorientasi Objek 36
2.5. Kesimpulan 39

BAB III. ANDROID CORE COMPONENTS **41**
3.1. Pendahuluan 41
3.2. Activity & Intent 42

3.3. Services 44
3.4. Broadcast Receiver 45
3.5. Content Provider 46
3.6. Kesimpulan 47

BAB IV. LOST DEVICE 49
4.1. Pendahuluan 49
4.2. Locate - Lock 51
4.3. Wipe 51
4.4. Kesimpulan 53

BAB V. MOBILE AUTHENTICATION 54
5.1. Pendahuluan 54
5.2. Single Sign-On. 55
5.3. Two Factor Authentication. 57
5.4. Permission 61
5.5. Kesimpulan 64

BAB VI. KRIPTOGRAFI 67
6.1. Pendahuluan 67
6.2. Enkripsi (Encrypt) 69
6.3. Dekripsi (Decrypt) 70
6.4. Hashing 71
6.5. Key Management 76
6.6. Digital Signature 77
6.7. Kesimpulan 80

BAB VII. MOBILE PRIVACY 83
7.1. Pendahuluan 83
7.2. Data Privacy 84
7.3. Location Privacy 87
7.4. Kesimpulan 88

BAB VIII. MOBILE MALWARE 90
7.1. Pendahuluan 90
7.2. Taksonomi 91
7.3. Jenis Malware Seluler 92
7.4. Kesimpulan 96

BAB IX. MOBILE SPYWARE 98
9.1. Pendahuluan 98
9.2. Apa Itu Spyware? 99
9.3. Cara Kerja Spyware 99
9.4. Bagaimana Bisa Terinfeksi Spyware 100
9.5. Jenis Spyware 102
9.6. Siapa Target Spyware 104
9.7. Bagaimana Cara Menghilangkan Spyware 104
9.8. Bagaimana Melindungi Diri Dari Spyware 105
9.9. Kesimpulan 106

BAB X. SECURE MOBILE APP DEVELOPMENT 107
10.1. Pendahuluan 107
10.2. Apa itu Keamanan Aplikasi Seluler 108
10.3. Apa itu Pengujian Keamanan Aplikasi Seluler 109
10.4. Kesimpulan 110

BAB XI. MOBILE SMS SECURITY 111
11.1. Pendahuluan 111
11.2. Celah Keamanan SMS 112
11.3. Kesimpulan 114

BAB XII. MOBILE PHISHING 116
12.1. Pendahuluan 116
12.2. Taktik Umum Mobile Phishing 117
12.3. Kesimpulan 119

BAB XIII. MOBILE NETWORK EXPLOITS 121
13.1. Pendahuluan 121
13.2. Serangan berdasarkan jaringan GSM 121
13.3. Serangan berdasarkan Wi-Fi 123
13.4. Serangan berbasis Bluetooth 124
13.5. Kesimpulan 125
DAFTAR PUSTAKA 127
GLOSARIUM 132
INDEKS 142

DAFTAR GAMBAR

Gambar.1.1.	Penggunaan Perangkat Mobile dari Tahun ke Tahun	3
Gambar 1.2.	Prinsip Keamananan Data	4
Gambar 1.3	Mobile Threat	11
Gambar 2.1.	Start –Up Android Studio	26
Gambar 2.2.	Instalasi SDK	27
Gambar 2.3.	Pengaturan Perangkat	30
Gambar 2.4.	USB Debuging	31
Gambar 2.5.	USB Debugging-2	31
Gambar 2.6.	Running Device Path	34
Gambar 2.7.	Mementukan IP Address	35
Gambar 3.1.	Bagian utama dari aplikasi android	42
Gambar 3.2.	Activity pada Aplikasi Android	43
Gambar 3.3.	Jenis Intent Pada Aplikasi Android	44
Gambar 3.4.	Jenis Servis pada Aplikasi Android	45
Gambar 3.5.	Jenis Broadcast pada Aplikasi Android	45
Gambar 5.1	Cara Kerja Single-Sign-On	57
Gambar 5.2.	Cara Kerja Two Factor Authenticator	60
Gambar 6.1	Proses Kriptografi	68
Gambar 6.2.	Proses Enkripsi	70
Gambar 6.3.	Proses Enkripsi - Dekripsi	71
Gambar 6.4.	Proses Hashing	74
Gambar 6.5.	Struktur Hash	74
Gambar 6.6.	Fungsi Hash	75
Gambar 6.7.	Cara Kerja Key Management	76
Gambar 6.8.	Proses Digital Signature	77

Gambar 7.1. Proses Tersebarnya Data 85
Gambar 7.2. Proses Terjadinya Location Privacy Reveal 87
Gambar 8.1. Overview Malware 91
Gambar 8.2. Cara Kerja Ransomware 93
Gambar 8.3. Proses Cryptomining Malware 94
Gambar 9.1 Siklus Kerja Spyware 99
Gambar 9.2 Teknik Mobile Spyware 106
Gambar 12.1 Teknik Mobile Phishing 118
Gambar 12.2 Siklus Mobile Phishing 119
Gambar 13.1 Spoofing Titik Akses 123
Gambar 13.2. Contoh Serangan menggunakan Bluetooth 125

BAB I.

CONFIDENTIALITY, INTEGRITY, AVAILABILITY, THREAT AND ETHICS

1.1. Pendahuluan

Belakangan ini kemajuan teknologi yang ada di dunia semakin pesat. Ini ditandai dengan semakin mudahnya kita dalam mengakses sebuah informasi. Namun, ada kalanya para developer melupakan sebuah parameter dasar yang sangat vital dalam sebuah sistem informasi. Parameter ini biasa disebut dengan C.I.A atau Confidentiality, Integrity dan Availability

Bahan kajian pembelajaran pada bab 1 adalah penjelasan secara komprehensif tentang definisi **Confidentiality. Integrity, Availability.Ancaman dan Etihcs..**

Sub Capaian pembelajaran mata kuliah dalam dalam pertemuan ini adalah mahasiswa diharapkan dapat **Mengetahui dan mampu menjelaskan dan mempraktekkan mengenai konsep "CIA".**

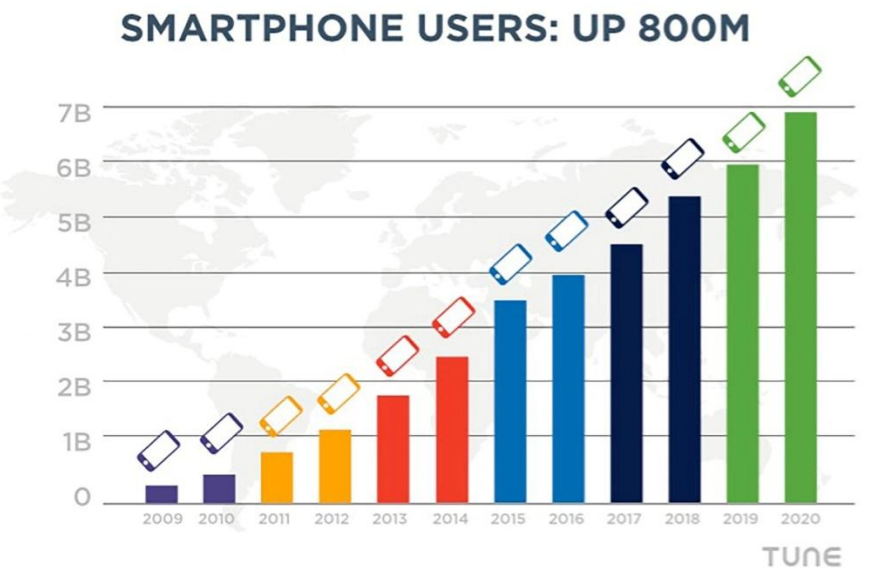
Indikator pencapaian dalam pertemuan ini adalah mahasiswa dapat mendeskripsikan **mampu menjelaskan dan mempraktekkan mengenai konsep "CIA".**

Penyampaian materi adalah dengan **ceramah, diskusi, dan praktek**

1.2. Apa itu Mobile Security?

- Mobile Security adalah perlindungan ponsel pintar, tablet, laptop, dan perangkat komputasi portabel lainnya, dan jaringan tempat mereka terhubung, dari ancaman dan kerentanan yang terkait dengan komputasi nirkabel.
- Mobile Security juga dikenal sebagai Wireless Security.
- Mengamankan perangkat seluler menjadi semakin penting dalam beberapa tahun terakhir seiring dengan banyaknya perangkat yang masuk operasi dan penggunaannya telah berkembang secara dramatis.

Gambar 1.1. menjelaskan bahwa samapai saat ini ter jadi peningkatan pengguna seluler, ada 800 juta pelanggan seluler baru dengan smartphone pada tahun ini, secara global. Pada tahun 2015 sekitar 47% dari planet ini memiliki smartphone, Pada 2016, jumlah itu akan melampaui angka 50%, mendekati hampir 4 miliar. Dengan kata lain, tumbuh lebih cepat dari populasi dunia yang saat ini 600 juta lebih pada tahun 2016. Jika ditambahkan semuanya dengan pengguna smartphone yang ada, dan akan ada 6,5 miliar pengguna seluler pada tahun 2020. Itulah sebabnya selain ratusan juta pengguna ponsel cerdas, 86% waktu seluler dihabiskan di aplikasi di negara maju, pertumbuhan cepat m-commerce dalam beberapa kuartal terakhir, dan peran besar m-commerce di dunia mobile-first India (ditambah pada tingkat yang lebih rendah, Cina)



Gambar. 1.1. Penggunaan Perangkat Mobile dari Tahun ke Tahun
sumber: https://martech.zone/mobile-economy-2016/, Why 2016 Will be a Global Tipping Point for the Mobile Economy

1.3. Risiko dan Serangan Seluler

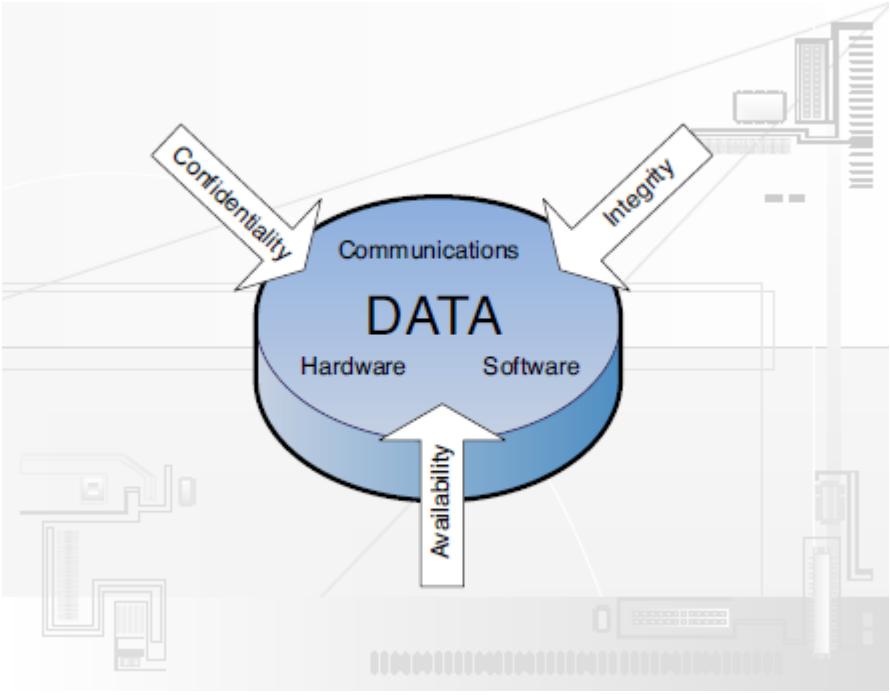
Aplikasi seluler diterapkan dalam banyak bahasa yang sama dengan versi desktop dan Web (mis., Objective-C dan Swift untuk iOS, Java untuk Android), dan karena itu rentan terhadap banyak hal yang samakerentanan dan serangan yang terkait dengan bahasa tersebut termasuk infeksi dan kompromi dengan jahat

perangkat lunak termasuk spyware, program Trojan Horse, worm, dan virus komputer. Phishing dan sosial lainnya taktik rekayasa memangsa kelemahan pengguna. Serangan lain menargetkan aplikasi seluler itu sendiri, yaitu server yang digunakan aplikasi seluler, API internal yang tidak terlindungi, rute alternatif melalui dan sekitarnya pemeriksaan keamanan, dan membuka port server.

Secara umum, keamanan komputer (computer security) melingkupi empat aspek, privacy, integrity, aunthentication, dan availability.

Hal pertama yang **kita harus tau adalah bahwa tidak ada yang benar-benar aman**. Selalu ada jalan atau melalui tindakan pencegahan keamanan yang kita membangun.

Orang IT selalu berusaha untuk mematuhi tiga prinsip inti Security yaitu : confidentiality, integrity, and availability. Secara kolektif, ketiganya adalah dikenal sebagai triad CIA seperti yang diilustrasikan pada Gambar 1.2. di bawah ini. Dimana ketiga konsep ini dapat mengamankan perangakat keras, perangkat lunak dan komunikasi.



Gambar 1.2. Prinsip Keamananan Data
Sumber : http://dedyindrasetiawan.blogspot.com/2018/09/keamanan-sistem-informasi.html

1.4. Confidentiality / Privacy

Inti utama aspek pivacy atau confidentiality adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Privacy lebih ke arah data-data yang sifatnya privat, sedangkan confidentiality biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu (misalnya sebagai bagian dari pedaftaran sebuah sevice) dan hanya diperbolehkan untuk keperluan tertentu tersebut.

1.5. Integrity

Aspek ini menentukan bahwa informasi tidak boleh diubah tanpa seizin pemilik informasi. Informasi yang diterima harus sesuai dan sama persis seperti saat infomasi dikirimkan. Jika terdapat perbedaan antara infomasi atau data yang dikirimkan dengan yang diterima maka aspek integrity tidak tercapai. Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa izin merupakan masalah yang harus dihadapi.

Berhubungan dengan akses untuk mengubah data dan informasi, data dan informasi yang berbeda dalam suatu sistem komputer hanya dapat diubah oleh orang berhak. Aspek ini menekankan bahwa informasi tidak boleh diubah tapa seizin pemilik infomasi. Adanya cirus, trojan horse, atau pemakai lain yang mengubah informasi tanpa izin merupakan contoh masalah yang harus dihadapi.

1.6. Availability

Aspek ini berhubungan dengan ketersediaan data dan informasi Data dan informasi yang berada dalam suatu sistem komputer tersedia dan dapat dimanfaatkan oleh orang yang berhak. Aspek availability atau keterseidaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Coba bayangkan jika kita sebagai user yang absah ingin mengakses mail atau layanan lainnya namun pada saat kita membutuhkannya layanan tersebut tidak dapat memenuhinya karena beberapa alasan, misalnya server yang down oleh serangan DoS, terkena Hack, atau terjadi Web Deface.

Ketiga prinsip harus diterapkan setiap kali berurusan dengan keamanan hardware, software, atau komunikasi. akronim lain untuk itu adalah AAA of computer security: authentication, authorization, and accounting.

■ **Authentication**: Ketika identitas seseorang di buat dengan bukti yang tersedia dan dikonfirmasi oleh sistem. Biasanya, ini memerlukan identitas digital dari beberapa macam,username / password, atau skema otentikasi lainnya. Aspek ini berhubungan dengan metode atau cara untuk menyatakan bahwa informasi betul-betul asli, orang yang mengases atau memberikan informasi adalah betul-betul orang yang dimaksud, atau sever yang kita hubungi adalah betul-betul server yang asli. Biasanya metode yang sangat kita kenal untuk terkoneksi dengan server dan mendapatkan layanan adalah dengan metode password dimana terdapat suatu karakter yang diberikan oleh pengguna ke server dan server mengenalinya sesuai dengan policy yang ada. Saat ini dengan perkembangan TI terdapat beberapa metode authentication yang lebih canggih dan aman seperti menggunakan retina mata, pengenalan suara, dan telapak tangan pengguna.

■ **Authorization**: Bila pengguna diberikan akses ke data tertentu Otorisasi terjadi setelah otentikasi dan dapat ditentukan dalam beberapa cara, termasuk perizinan, daftar kontrol akses, waktu hari pembatasan, dan login lain dan pembatasan fisik.

■ **Accounting**: pelacakan data, penggunaan komputer, dan sumber daya jaringan. Seringkali itu berarti logging, audit, dan pemantauan data dan sumber daya. Accounting menjadi lebih penting dalam jaringan yang aman. Konsep AAA ini juga harus diterapkan untuk setiap rencana keamanan Anda.

1.7. Threat

Cyber Threat & Mobile Threat

"CIA" memiliki kemampuan untuk memastikan keamanan informasi. Melanggar "CIA" dapat menyebabkan ancaman dunia maya. Untuk keamanan seluler, itu akan menimbulkan ancaman seluler. Sekarang, mari kita lihat beberapa ancaman dunia maya dan ancaman seluler yang ada.

Dalam sepuluh tahun terakhir, ada banyak perubahan di lingkungan kerja kita. Salah satu perubahan terbesar adalah bahwa informasi kerja penting kami tidak lagi hanya dapat diragi di kantor kami, tetapi sekarang dapat ditransmisikan ke laptop dan ponsel pintar karyawan. Sepuluh tahun yang lalu, hanya sedikit karyawan yang dapat bekerja di rumah atau di jalan, tetapi seiring dengan peningkatan teknologi seluler, semua keadaan ini menjadi kenyataan. Meskipun peningkatan seperti itu membuat hidup dan pekerjaan kita lebih mudah, informasi yang kita hasilkan dan kita hadapi menghadapi ancaman yang semakin banyak. Ancaman seluler dapat dikategorikan menjadi dua segmen utama: Aktivitas berbahaya oleh penyerang **(*Malicious Activity by Attacker*)** dan Kerentanan **(*Vulnearability*).**

- **MALICIOUS ACTIVITY by ATTACKER:**

  Dalam kasus ini, penyerang menggunakan trik berbeda untuk membujuk korban agar menginstal Aplikasi Trojan. Pengguna yang tidak bersalah mengira mereka menginstal game atau utilitas, tetapi sebaliknya mereka mendapatkan spyware tersembunyi, UI phishing, atau panggilan premium yang tidak sah. Beberapa vektor serangan termasuk dalam kategori ini adalah:

  1. **Activity Monitoring and Data Retrieval.**

     Spywares terkenal untuk jenis aktivitas ini. Data yang dihasilkan di perangkat dapat disadap secara real time misalnya mengarahkan email ke alamat pihak ketiga yang tersembunyi, membiarkan penyerang mendengar tentang panggilan telepon atau membuka rekaman mikrofon. Data

yang disimpan seperti daftar kontak atau pesan email yang disimpan juga dapat diambil.

2. **Unauthorized dialing, SMS, and Payments**
   Penjahat yang berusaha untuk memonetisasi kelemahan dalam sifat manusia dan model distribusi aplikasi seluler dapat beralih ke panggilan telepon bertarif premium dan pesan SMS bertarif premium. Dengan memasukkan fungsionalitas panggilan premium ke dalam aplikasi Trojan, penyerang dapat menghabiskan tagihan telepon korban dan meminta operator seluler untuk mengumpulkan dan mendistribusikan uang kepada mereka. Perangkat seluler juga dapat digunakan untuk membeli barang, nyata dan virtual, dan biayanya ditagihkan ke tagihan seluler pelanggan.
   Penggunaan lain dari pesan teks SMS yang tidak sah adalah sebagai vektor penyebaran worm. Setelah perangkat terinfeksi worm, ia dapat mengirim pesan teks SMS ke semua kontak di buku alamat dengan tautan untuk mengelabui penerima agar mengunduh dan menginstal worm tersebut.

3. **Unauthorized Network Connectivity (Exfiltration or Command & Control)**
   Spyware atau aplikasi berbahaya lainnya biasanya memerlukan eksfiltrasi agar dapat bermanfaat bagi penyerang. Karena perangkat seluler dirancang untuk komunikasi, ada banyak vektor potensial yang dapat digunakan aplikasi jahat untuk mengirim data ke penyerang. Program jahat yang berfungsi penuh sering kali memungkinkan penyerang untuk mengarahkan perintah ke spyware, misalnya, untuk menyalakan mikrofon atau mengambil file data pada waktu tertentu.

4. **UI Impersonation**
   Serangan phishing pada PC bekerja dengan mengelabui pengguna agar mengeklik tautan di browser mereka yang membawa mereka ke situs web palsu yang meniru UI bank

atau layanan online mereka. UI meminta pengguna untuk memasukkan kredensial mereka. Penyerang mengumpulkan kredensial dan menggunakannya untuk menyamar sebagai korban. Di perangkat seluler, ada peluang baru bagi penyerang untuk melakukan peniruan UI. Ini dapat berupa aplikasi tampilan web yang menyajikan UI seluler asli sebagai proxy ke aplikasi web asli. Dengan serangan ini, pengguna mengira mereka mengunduh aplikasi yang sah, seperti aplikasi perbankan, tetapi sebaliknya mereka mendapatkan penipu yang memberikan informasi ke situs web asli bank. Saat pengguna mengautentikasi dirinya sendiri, mereka akhirnya mengirimkan kredensial mereka ke penyerang.

Vektor lain untuk peniruan identitas adalah aplikasi berbahaya yang memunculkan UI yang meniru UI asli ponsel atau UI dari aplikasi yang sah. Korban diminta untuk mengautentikasi dan akhirnya mengirimkan kredensial mereka ke penyerang.

5. **System Modification (Rootkit, APN Proxy Config)**
   Aplikasi hasad akan sering mencoba mengubah konfigurasi sistem untuk menyembunyikan keberadaannya. Ini sering disebut perilaku rootkit. Perubahan konfigurasi juga memungkinkan serangan tertentu. Contohnya adalah memodifikasi konfigurasi proxy perangkat atau APN (Access Point Name).

6. **Logic or Time bomb**
   Logika atau bom waktu adalah teknik pintu belakang klasik yang memicu aktivitas berbahaya berdasarkan peristiwa, penggunaan perangkat, atau waktu tertentu .

- **VULNERABILITY:**
  Kategori kerentanan adalah kesalahan dalam desain atau implementasi yang mengekspos data perangkat seluler ke intersepsi oleh penyerang. Kerentanan juga dapat mengekspos perangkat seluler atau aplikasi cloud yang digunakan dari

perangkat tersebut ke akses yang tidak sah. Beberapa vektor serangan yang termasuk dalam kategori ini adalah:

1. **Sensitive Data Leakage (Inadvertent or Side Channel)**
   Kebocoran data sensitif dapat berupa saluran samping atau tidak disengaja. Penggunaan informasi perangkat dan metode otentikasi aplikasi yang sah dapat diterapkan dengan buruk sehingga mengekspos data sensitif ke pihak ketiga.

2. **Unsafe Sensitive Data Storage**
   Aplikasi seluler sering kali menyimpan data sensitif seperti perbankan dan nomor PIN sistem pembayaran, nomor kartu kredit, atau kata sandi layanan online. Data sensitif harus selalu disimpan dengan enkripsi sehingga penyerang tidak bisa begitu saja mengambil data ini dari sistem file. Perlu dicatat bahwa menyimpan data sensitif tanpa enkripsi pada media yang dapat dilepas seperti kartu micro SD sangat berisiko.

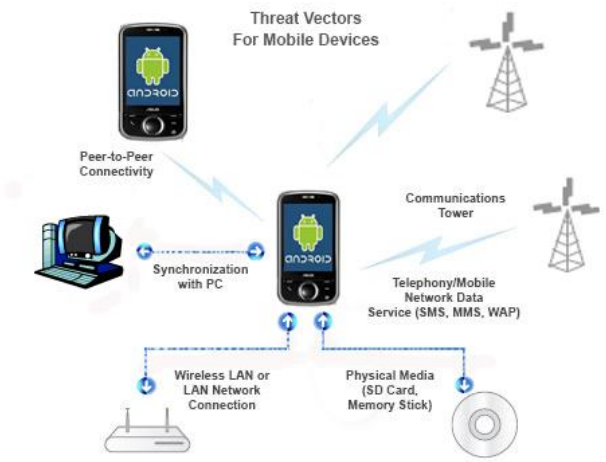
3. **Unsafe Sensitive Data Transmission**
   Penting bahwa data sensitif dienkripsi dalam transmisi agar tidak disadap oleh penyerang. Perangkat seluler sangat rentan karena mereka menggunakan komunikasi nirkabel secara eksklusif dan sering kali perangkat seluler memiliki akses ke WiFi publik, yang diketahui tidak aman. SSL adalah salah satu cara terbaik untuk mengamankan data sensitif saat transit. Jika aplikasi mengimplementasikan SSL, ia masih bisa menjadi korban serangan downgrade jika memungkinkan menurunkan HTTPS ke HTTP. Cara lain SSL dapat dikompromikan adalah jika aplikasi tidak gagal pada sertifikat yang tidak valid. Ini akan memungkinkan serangan man-in-the-middle.

4. **Hardcoded Password/Keys**
   Penggunaan kata sandi atau kunci hardcode terkadang dipandang sebagai pintasan oleh pengembang untuk membuat aplikasi lebih mudah diimplementasikan, didukung, atau di-debug. Setelah kata sandi yang di-hardcode ini ditemukan

melalui rekayasa balik, ini menjadikan keamanan sistem yang diautentikasi karena kata sandi aplikasi diketahui oleh peretas. Gambar.1.3 adalah bagan yang menunjukkan ancaman seluler.

Gambar 1.3. menjelaskan celah yang memungkinkan untuk terjadinya serangan atas perangkat seluler. Ancaman keamanan seluler adalah serangan yang dimaksudkan untuk membahayakan atau mencuri data dari perangkat seluler seperti ponsel cerdas dan tablet. Ancaman ini sering kali berbentuk malware atau spyware, yang memberikan akses tidak sah kepada pelaku jahat ke perangkat; dalam banyak kasus, pengguna bahkan tidak menyadari bahwa serangan telah terjadi.

Dengan akses, penyerang dapat melakukan berbagai tindakan jahat, mulai dari mencuri dan menjual data hingga mengakses kontak hingga mengirim pesan dan melakukan panggilan. Mereka juga dapat menggunakan perangkat untuk mencuri kredensial login dan identitas palsu pengguna. Serangan ini berdampak pada pengguna individu dan organisasi, karena satu pelanggaran dapat menyebabkan kebocoran data skala besar.



Gambar. 1.3. Mobile Threat
Sumber: https://sites.google.com/site/mobilesecuritylabware/home/fundamental-concepts-security-ethics

1.8. Ethics

Ancaman seluler yang dibahas di atas datang ke kehidupan nyata kita karena peretasan tidak etis dari peretas jahat. Di bagian terakhir ini, kita akan melihat etika peretasan. Alasan mengapa penting untuk mengetahui etika peretasan ini adalah karena etika ini adalah panduan yang baik bagi kita untuk membedakan antara peretasan etis dan peretasan tidak etis.

- **Hacker Ethic** merupakan ungkapan umum yang menggambarkan nilai-nilai moral dan filosofi yang menjadi standar dalam komunitas hacker. Budaya hacker awal dan filosofi yang dihasilkan berasal dari Massachusetts Institute of Technology (MIT) pada 1950-an dan 1960-an.
- Pedoman etika peretas memudahkan untuk melihat bagaimana komputer telah berkembang menjadi perangkat pribadi yang kita kenal dan andalkan saat ini. Poin kunci dalam etika ini adalah akses, informasi gratis, dan peningkatan kualitas hidup [6]. Etika adalah tentang bagaimana kita harus hidup. Tujuan Etika dalam Keamanan Informasi tidak hanya penting secara filosofis, tetapi juga dapat berarti kelangsungan hidup suatu bisnis atau industri.[1]

- **Ethical Challenges in Information Security**
  - Representasi yang keliru dari sertifikasi, keterampilan
  - Penyalahgunaan hak istimewa
  - Pemantauan yang tidak tepat
  - Menahan informasi
  - Membocorkan informasi secara tidak tepat
  - Masalah berlebihan
  - Konflik kepentingan
  - Masalah manajemen / karyawan / klien

[1] Michael T. Simpson , Kent Backman, James Corley. "Hands-On Ethical Hacking and Network Defense", Delmar Cengage Learning; 2 edition (March 17, 2010)

- **The Original Hacker Ethics:** Etika Hacker asli adalah semacam kode etik informal dadakan yang dikembangkan oleh hacker asli MIT dan Stanford (SAIL) pada tahun 50-an dan 60-an. "Hacker" ini adalah generasi pertama programmer, menggunakan akses terminal time-sharing ke mainframe 'bodoh', dan mereka sering menghadapi berbagai macam gangguan birokrasi yang mencegah mereka untuk mengeksplorasi sepenuhnya bagaimana sistem teknologi (komputer, tetapi juga kereta model, universitas terowongan uap, sistem telepon universitas, dll.) berfungsi. Etika mencerminkan penolakan mereka terhadap rintangan-rintangan ini, dan ideologi mereka tentang kekuatan teknologi yang membebaskan. Enam prinsip Etika Peretas tercantum di bawah ini, dengan beberapa contoh teks yang menunjukkan di mana ia muncul dalam dokumen-dokumen ini.
    1. **Akses ke komputer harus tidak terbatas dan total:** Ditegaskan sebagai keharusan kategoris untuk menghilangkan hambatan apa pun antara orang-orang dan penggunaan dan pemahaman teknologi apa pun, tidak peduli seberapa besar, kompleks, berbahaya, labirin, kepemilikan, atau kuat.
    2. **Semua informasi harus bebas:** Bebas mungkin berarti tanpa *batasan* (kebebasan bergerak = tanpa sensor), tanpa *kontrol* (kebebasan perubahan / evolusi = tanpa kepemilikan atau kepengarangan, tanpa kekayaan intelektual), atau tanpa *nilai moneter* (tanpa biaya.) Beberapa peretas bahkan menganggap ini sebagai informasi yang hidup, bebas untuk bertindak atas agensinya sendiri, seperti yang dilakukan virus, algoritme genetika, bot, dan program perangkat lunak lainnya. Sebagian besar peretas tampaknya mendukung prinsip ini dalam arti berbeda dari kata "gratis" pada waktu yang berbeda. Bagaimanapun, ketika ditanya tentang isi dari Etika Hacker, kebanyakan orang menegaskan ini sebagai prinsip utama.

3. **Ketidakpercayaan otoritas - promosikan desentralisasi:** Promosikan desentralisasi. Unsur etika ini menunjukkan sifat anarkistis, individualistis, dan libertariannya yang kuat. Peretas selalu menunjukkan ketidakpercayaan terhadap institusi besar, termasuk tetapi tidak terbatas pada Negara, perusahaan, dan birokrasi administrasi komputer ('imamat' IBM). Alat-alat seperti PC dikatakan memindahkan kekuasaan dari organisasi besar (yang menggunakan mainframe) dan meletakkannya di tangan pengguna 'orang kecil'. Tidak ada etos ini yang lebih kuat daripada di antara para cypherpunks dan ekstropian anti-statist.
4. **Peretas harus dinilai dari peretasan mereka, bukan kriteria seperti derajat, usia, ras, jenis kelamin, atau posisi:** Tidak ada etos ini yang lebih jelas daripada yang dianut oleh sebagian besar peretas tentang kekuatan penyamarataan Internet, di mana anonimitas memungkinkan agar semua 'variabel' tentang seseorang tetap tidak diketahui, dan di mana ide-ide mereka harus dinilai berdasarkan manfaatnya sendiri karena faktor kontekstual semacam itu tidak tersedia.
5. **Anda dapat membuat seni dan keindahan di komputer:** Peretasan disamakan dengan seni dan kreativitas. Lebih jauh lagi, elemen etos ini mengangkatnya ke tingkat filosofi (sebagai lawan dari pragmatisme sederhana), yang (setidaknya di beberapa bagian) adalah tentang pencarian manusia akan kebaikan, kebenaran, dan keindahan.
6. **Komputer dapat mengubah hidup Anda menjadi lebih baik:** Dalam beberapa hal, pernyataan terakhir ini benar-benar merupakan konsekuensi wajar dari pernyataan sebelumnya. Karena sebagian besar umat manusia menginginkan hal-hal yang baik, benar, dan / atau indah, fakta bahwa komputer dapat membuat hal-hal seperti itu tampaknya berarti bahwa secara aksiomatis komputer

dapat mengubah kehidupan masyarakat menjadi lebih baik. Namun, ini hanyalah pernyataan deklaratif, yang seperti yang sebelumnya mencerminkan kecintaan yang mendalam terhadap teknologi. Itu tidak menyatakan secara eksplisit bahwa komputer harus selalu mengubah kehidupan orang-orang menjadi lebih baik, atau prinsip yang akan mengikuti dari itu, yaitu bahwa tidak etis menggunakannya untuk memperburuk kehidupan masyarakat.

Who is the Computer Underground ? : CU disebut sebagai "peretas tahun 90-an" atau "peretas baru," sebagai lawan dari peretas lama, yang merupakan peretas (istilah lama) dari tahun 60-an yang berlangganan Etika Peretas asli.

1. **Hackers** (Cracker, penyusup sistem) - Ini adalah orang yang mencoba menembus sistem keamanan pada komputer jarak jauh. Ini adalah pengertian baru dari istilah tersebut, sedangkan pengertian lama dari istilah tersebut hanya merujuk pada orang yang mampu menciptakan peretasan, atau penggunaan teknologi yang elegan, tidak biasa, dan tidak terduga. Majalah tipikal (baik cetak maupun online) yang dibaca oleh peretas termasuk *2600* dan *Iron Feather Journal.*
2. **Phreaks** (Phone Phreakers, Blue Boxers) - Ini adalah orang-orang yang mencoba menggunakan teknologi untuk menjelajahi dan / atau mengontrol sistem telepon. Awalnya, ini melibatkan penggunaan "kotak biru" atau generator nada, tetapi ketika perusahaan telepon mulai menggunakan sakelar digital alih-alih elektro-mekanis, phreak menjadi lebih seperti peretas. Majalah tipikal yang dibaca oleh Phreaks termasuk *Phrack* , *Line Noize* , dan *New Fone Express.*
3. **Virus Writers** (juga, pencipta Trojan, worm, logic bomb) - Ini adalah orang-orang yang menulis kode yang mencoba untuk a) mereproduksi dirinya sendiri di sistem lain tanpa otorisasi dan b) sering memiliki efek samping, apakah itu untuk menampilkan pesan, main-main, atau buang hard drive. Agen dan laba-laba pada dasarnya adalah virii yang 'baik hati', menimbulkan

pertanyaan tentang seberapa tersembunyi aktivitas ini sebenarnya. Majalah umum yang dibaca oleh penulis Virus termasuk *40HEX*.

4. **Pirates** - Pembajakan adalah masalah non-teknis. Awalnya, ini melibatkan pelanggaran perlindungan salinan pada perangkat lunak, dan aktivitas ini disebut "meretas". Saat ini, hanya sedikit vendor perangkat lunak yang menggunakan perlindungan salinan, tetapi masih ada berbagai tindakan kecil yang digunakan untuk mencegah duplikasi perangkat lunak yang tidak sah. Bajak laut mengabdikan diri untuk menggagalkan hal-hal ini dan berbagi perangkat lunak komersial secara bebas..
5. **Cypherpunks** (cryptoanarchists) - Cypherpunks secara bebas mendistribusikan alat dan metode untuk menggunakan enkripsi yang kuat, yang pada dasarnya tidak dapat dipecahkan kecuali oleh superkomputer besar. Karena NSA dan FBI tidak dapat memecahkan enkripsi yang kuat (yang merupakan dasar dari PGP atau Pretty Good Privacy), program yang menggunakannya diklasifikasikan sebagai amunisi, dan distribusi algoritme yang menggunakannya merupakan tindak pidana. Beberapa cryptoanarchists menganjurkan enkripsi yang kuat sebagai alat untuk sepenuhnya menghindari Negara, dengan mencegah akses apapun ke informasi keuangan atau pribadi. Mereka biasanya membaca milis Cypherpunks.
6. **Anarchist** - berkomitmen untuk mendistribusikan informasi ilegal (atau setidaknya mencurigakan secara moral), termasuk namun tidak terbatas pada data tentang pembuatan bom, lockpicking, pornografi, pembuatan obat-obatan, radio bajakan, dan pembajakan TV kabel dan satelit. Dalam istilah komputer bawah tanah ini, kaum anarkis cenderung tidak mendukung penggulingan pemerintah daripada penolakan sederhana untuk mematuhi pembatasan dalam mendistribusikan informasi. Mereka cenderung membaca *Cult of the Dead Cow* (CDC) dan *Activist Times Incorporated* (ATI).
7. **Cyberpunk** - biasanya beberapa kombinasi di atas, ditambah minat pada modifikasi diri teknologi, fiksi ilmiah dari genre *Neuromancer* , dan minat pada peretasan perangkat

keras dan "teknologi jalanan." Sebuah subkultur anak muda dalam dirinya sendiri, dengan beberapa tumpang tindih dengan subkultur "primitif modern" dan "penjelajah".

New Hacker Ethics: Ada etika hacker baru yang dianut oleh para hacker tahun 90-an. Ada fragmen kontinuitas dari etika hacker lama, seperti yang bisa dilihat. Etika baru tampaknya telah berkembang seperti yang lama, secara informal dan melalui proses penguatan timbal balik.

1. "**Di atas segalanya, jangan membahayakan**" Jangan merusak komputer atau data jika memungkinkan. Mirip seperti elemen kunci dari Sumpah Hipokrates.
2. **Lindungi Privasi** Orang memiliki hak privasi, yang berarti kontrol atas informasi pribadi (atau bahkan keluarga) mereka sendiri. Hak privasi secara khusus hilang dari Konstitusi AS, tetapi mereka telah dibawa ke garis depan argumen hukum modern karena kekuatan pengawasan teknologi yang berkembang. Masih belum ada hak yang dikodifikasi atas privasi warga AS, meskipun Mahkamah Agung telah memutuskan bahwa hal itu terkandung secara implisit dalam putusannya yang melegalkan distribusi alat kontrasepsi dan hak untuk aborsi trimester pertama.
3. "**Jangan sia-siakan, mau tidak.**" Sumber daya komputer tidak boleh diam dan sia-sia. Secara etika salah untuk membuat orang keluar dari sistem ketika mereka dapat menggunakannya selama waktu menganggur. Inilah yang oleh sebagian orang disebut sebagai "etika pengendara kegembiraan". Jika Anda meminjam mobil seseorang, dan mengembalikannya tanpa kerusakan, tangki penuh bensin, dan bahkan mungkin beberapa saran untuk meningkatkan kinerja, bukankah Anda membantu mereka? Terutama jika mereka tidak pernah tahu Anda meminjamnya untuk beberapa perjalanan darat? Bukankah membuang-buang tenaga mesin yang berharga itu untuk meninggalkan mobil di tempat parkir sementara orang lain bisa menggunakannya untuk perjalanan belanjaan? (Apakah meminjam mobil dan membuat satu set kunci untuk diri Anda

sendiri merupakan pelanggaran etika sehingga Anda dapat meminjamnya kapan pun Anda mau? Bagaimanapun, inilah yang dilakukan sebagian besar peretas ketika mereka memberikan hak istimewa sysadmin kepada diri mereka sendiri.

4. **Exceed Limitations** Hacking adalah tentang melampaui batasan masalah secara terus-menerus. Beberapa peretas lama menegaskan prinsip ini, sebagai tambahan informal ketujuh dari Etika asli. Memberi tahu peretas bahwa sesuatu tidak bisa dilakukan, adalah keharusan moral baginya untuk mencoba. "Ekstropi" percaya ada kekuatan universal dari ekspansi dan pertumbuhan, kebalikan dari entropi, yang mereka sebut "ekstropi." Peretasan dipandang sebagai ekstropian karena selalu berusaha melampaui batas saat ini. Teknologi dipandang sebagai kekuatan pertumbuhan yang selalu eksponensial. Keterbatasan harus diatasi. Bagi beberapa peretas, batasan ini mungkin hukum yang tidak adil atau kode moral yang ketinggalan zaman.
5. **Orang-orang yang sangat membutuhkan komunikasi** memiliki hak untuk berkomunikasi dan bergaul dengan sesamanya secara bebas. United Nations International Telecommunications Union (ITU) telah menyatakan dalam banyak konferensi bahwa ini harus menjadi hak asasi manusia yang fundamental, yang tidak boleh dicampuri oleh negara mana pun. Kebebasan luas yang diberikan kepada penggemar radio amatir secara internasional mencerminkan keyakinan ini. Secara global, ini tetap menjadi masalah moral yang signifikan, karena kebanyakan negara berkembang tidak memiliki infrastruktur untuk memberikan hak ini. Berbagai laporan PBB telah menunjukkan bahwa terlepas dari retorika tersebut, banyak negara Dunia Ketiga tidak memiliki akses ke jalan raya informasi "global" karena mereka tidak memiliki "landasan". Infrastruktur telekomunikasi mereka kurang.
6. **Tidak Meninggalkan Jejak** Jangan tinggalkan jejak atau jejak kehadiran Anda; jangan menarik perhatian pada diri sendiri atau eksploitasi Anda. Tetap diam, agar semua orang bisa menikmati apa yang Anda miliki. Ini adalah prinsip etika, di mana peretas

mengikutinya tidak hanya untuk kepentingannya sendiri, tetapi juga untuk melindungi peretas lain agar tidak tertangkap atau kehilangan akses. Prinsip seperti itu dapat ditemukan di antara berbagai organisasi kriminal atau bawah tanah. Tentu saja, ada kontradiksi antara menegaskan kebutuhan akan kerahasiaan (serta privasi), dan kebutuhan akan informasi yang tidak dibatasi.

7. **Bagikan!** Nilai informasi meningkat dengan membagikannya kepada sebanyak mungkin orang; jangan menimbun, jangan bersembunyi. Hanya karena ingin gratis, bukan berarti harus diberikan kepada sebanyak mungkin orang. Prinsip ini dapat dilihat sebagai penjabaran dari prinsip etika asli. Etika Pirates adalah bahwa pembajakan meningkatkan minat pada perangkat lunak, dengan memberi orang kesempatan untuk mencobanya dan bereksperimen dengannya sebelum membayarnya. Jadi berbagi perangkat lunak dengan teman Anda adalah hal yang baik.
8. **Pertahanan Diri** terhadap Masa Depan Cyberpunk Peretasan dan virus diperlukan untuk melindungi orang-orang dari kemungkinan masa depan distopia 1984 / cyberpunk, atau bahkan saat ini dari kekuatan pemerintah dan perusahaan yang terus tumbuh. Merupakan keharusan moral untuk menggunakan peretasan yang setara dengan 'jujitsu,' memungkinkan individu untuk mengatasi kekuatan yang lebih besar, lebih impersonal, lebih kuat yang dapat mengendalikan hidup mereka. Jika pemerintah dan perusahaan tahu bahwa mereka dapat diretas, maka mereka tidak akan melangkahi kekuasaan mereka untuk mempengaruhi warga negara.
9. **Peretasan Membantu Keamanan** Ini bisa disebut sebagai "etika tim Tiger": menemukan celah keamanan berguna dan sopan, lalu memberi tahu orang-orang cara memperbaikinya. Peretasan adalah kekuatan yang positif, karena ini menunjukkan kepada orang-orang bagaimana memperbaiki keamanan yang lemah, atau dalam beberapa kasus untuk mengenali dan menerima bahwa keamanan total tidak dapat dicapai, tanpa pengorbanan yang drastis.

10. **Percaya, tapi Uji!** Anda harus terus-menerus menguji integritas sistem dan mencari cara untuk memperbaikinya. Jangan serahkan perawatan dan skema mereka kepada orang lain; memahami sepenuhnya sistem yang Anda gunakan atau yang memengaruhi Anda. Jika Anda dapat mengeksploitasi sistem tertentu (seperti jaringan telepon) dengan cara yang tidak pernah dimaksudkan atau diantisipasi oleh pembuatnya, itu semua menjadi lebih baik. Ini dapat membantu mereka menciptakan sistem yang lebih baik. Salah satu sistem yang mungkin memerlukan revisi, pengujian, dan penyesuaian yang konstan, tampaknya, adalah demokrasi konstitusional.

Jadi, singkatnya, etika peretas baru menunjukkan bahwa adalah tugas etis peretas baru (atau CU), untuk: 1) melindungi data dan perangkat keras 2) menghormati dan melindungi privasi 3) memanfaatkan apa yang disia-siakan oleh orang lain 4) melebihi batasan yang tidak perlu 5) mempromosikan hak masyarakat untuk berkomunikasi 6) tidak meninggalkan jejak 7) berbagi data dan perangkat lunak 8) waspada terhadap tirani dunia maya dan 9) menguji keamanan dan integritas sistem sistem komputer.

- **Ethical Hacking vs. UnEthical Hacking:** Aktivitas peretasan dapat dibagi menjadi peretasan etis dan peretasan tidak etis. Kita sudah banyak membahas tentang etika peretasan di atas tetapi bagaimana kita bisa membedakan jenis peretasan yang etis dan jenis peretasan yang tidak etis? Di bagian ini, kami akan memberikan penjelasan singkat tentang peretasan etis dan peretasan tidak etis.
    1. **Ethical Hacking:** Ethical hacking selalu dilakukan oleh ethical hacker (atau yang disebut "white hat"). Ethical hacker adalah sekelompok ahli keamanan komputer yang "mengkhususkan diri dalam pengujian penetrasi dan metodologi pengujian lainnya untuk memastikan keamanan sistem informasi organisasi ". Peretas etis ini "memiliki kemampuan untuk merusak sistem Anda, tetapi mereka memilih untuk melakukannya membuat pilihan untuk membantu mengungkap kegagalan keamanan di

sistem Anda dan kemudian membantu Anda menemukan cara untuk melindungi perusahaan Anda dari peretas lain"]. Untuk peretas etis, mereka hanya akan meretas dan menguji sistem jika mereka diizinkan oleh pemiliknya sistem untuk menemukan kelemahan keamanan atau untuk mendeteksi penyebab setelah serangan. Intinya di sini adalah bahwa peretas etis selalu melakukan pekerjaan peretasan di bawah izin pemilik sistem. Mereka hanya akan meretas sedalam pemilik spesifikasi sistem. Untuk peretasan etis, akan sangat membantu jika mengetahui lubang keamanan sistem, potensi kerentanan sistem, dan fakta apakah suatu sistem sedang diserang.

2. **UnEthical Hacking** tidak etis adalah aktivitas peretasan berbahaya yang dilakukan oleh peretas jahat. Peretas jahat juga merupakan sekelompok pakar keamanan komputer tetapi tujuan umum peretasan mereka adalah untuk mencuri informasi rahasia dari suatu sistem, merusak sistem atau meninggalkan pintu belakang ke sistem yang disusupi untuk akses di masa mendatang. Untuk peretasan jahat, peretas tidak berwenang untuk mengakses informasi yang mereka ambil dari sistem. Peretasan yang berbahaya dapat menyebabkan kerugian ekonomi yang tidak terduga bagi perusahaan karena strategi bisnis dan informasi produk dicuri. Jadi, inilah poin lainnya, peretas jahat melakukan peretasan jahat tanpa izin dan otorisasi dari pemilik sistem.

1.9. Think Like A Hacker

Untuk berpikir seperti seorang hacker, Anda harus memahami hacker. Seorang hacker yang baik memahami pikiran seorang administrator keamanan,membuat komputer dan jaringan keamanan proposisi sulit. Tapi sebaliknya seorang keamanan cerdas menyadari hacker dan metode mereka.

Tidak semua hacker berbahaya. Ada beberapa jenis hacker:

■ **White hats** : Orang-orang ini nonmalicious; misalnya, orang IT yang upaya untuk "hack" ke dalam sistem komputer sebelum ditayangkan untuk menguji sistem. Umumnya, orang yang mencoba hack memiliki perjanjian kontraktual dengan pemilik sumber daya yang akan hacked.

■ **Black hats:** Ini adalah orang jahat yang mencoba untuk masuk ke computer dan jaringan komputer tanpa otorisasi. Black hats adalah orang-orang yang mencoba pencurian identitas, pembajakan, penipuan kartu kredit, dan sebagainya.

■ **Gray hats:** Mereka adalah individu yang tidak memiliki afiliasi dengan perusahaan tetapi risiko melanggar hukum dengan mencoba untuk hack sistem dan kemudian memberitahu administrator dari sistem yang mereka berhasil melakukannya-hanya untuk membiarkan mereka tahu. beberapa Gray hats menawarkan untuk memperbaiki kerentanan keamanan untuk dihargai, tetapi jenis ini juga dikenal sebagai green hats atau mercenaries.

■ **Blue hats:** ini adalah individu yang diminta untuk mencoba untuk kembali ke Sistem oleh sebuah organisasi, tetapi organisasi tidak mempekerjakan mereka. Itu organisasi bergantung pada fakta bahwa orang hanya menikmati hacking ke sistem. Biasanya, jenis skenario terjadi ketika pengujian sistem.

■**Elite:** Elite hacker adalah orang-orang yang pertama kali mengetahui tentang kerentanan. Hanya1 dari diperkirakan 10.000 hacker memakai Elite hat-

1.10. Kesimpulan

Berdasarkan uraian di atas, maka rencana keamanan akan berisi tentang penentuan kombinasi kontrol keamanan informasi yang digunakan, serta prioritas dalam melakukan implementasinya. Isi konten dasar pada dokumen rencana keamanan informasi (information security plan), antara lain:

1. Ancaman dan kelemahan, merupakan proses untuk mereview hasil tahapan penilaian risiko, dengan mengambil informasi mengenai sesuatu yang dapat menganggu kegiatan organisasi.
2. Tujuan dan sasaran, merupakan proses menentukan target dan lingkup keamanan informasi yang ingin dicapai, sehingga dapat fokus pada aspek keamanan yang akan diselesaikan. Sasaran keamanan informasi menggambarkan spesifik hasil, kejadian atau manfaat yang ingin di capai sesuai dengan tujuan keamanan yang ditetapkan.
3. Aturan dan tanggungjawab, merupakan proses menyusun aturan dan penanggungjawab, yang mengatur kegiatan sebagai upaya untuk menurunkan risiko keamanan informasi yang bersumber dari ancaman dan kelemahan.
4. Strategi dan kontrol keamanan, merupakan proses untuk memberikan prioritas aksi yang akan dilakukan untuk mencapai tujuan dan sasaran keamanan informasi yang telah ditetapkan.

Prioritas aksi tersebut sebagai pengaman untuk menjaga kerahasiaan, keutuhan dan ketersediaan informasi, dengan penentuan control keamanan yang sesuai dengan tujuan dan sasaran yang diinginkan.

Tugas dan Diskusi:

Beri Contoh Confidentiality, Integrity dan Availability ?

Referensi:

Michael T. Simpson , Kent Backman, James Corley. "Hands-On Ethical Hacking and Network Defense", Delmar Cengage Learning; 2 edition (March 17, 2010)

BAB II.

ANDROID PROGRAMMING

2.1. Pendahuluan

Android adalah sistem operasi dan platform pemrograman yang dikembangkan oleh Google untuk ponsel cerdas dan perangkat seluler lainnya (seperti tablet).[1] Android bisa berjalan di beberapa macam perangkat dari banyak produsen yang berbeda. Android menyertakan kit development perangkat lunak untuk penulisan kode asli dan perakitan modul perangkat lunak untuk membuat aplikasi bagi pengguna Android. Android juga menyediakan pasar untuk mendistribusikan aplikasi. Secara keseluruhan, Android menyatakan ekosistem untuk aplikasi seluler[2].

Bahan kajian pembelajaran pada bab adalah penjelasan secara komprehensif tentang definisi **Android Programming: dimana didalamnya terdapat Environment setup dengan Android SDK, Menjalankan aplikasi pada perangkat Android nyata, Pengenalan pada pemrograman berorientasi objek...**

Sub Capaian pembelajaran mata kuliah dalam dalam pertemuan ini adalah mahasiswa diharapkan dapat **Mengetahui dan memahami tentang pengembangan pemrograman Android.**

[1] Murphy, Mark (June 26, 2009). Beginning Android (1st ed.). Apress. ISBN 978-1-4302-2419-8.
[2] Haseman, Chris (July 21, 2008). Android Essentials (1st ed.). Apress. ISBN 978-1-4302-1064-1.

Indikator pencapaian dalam pertemuan ini adalah mahasiswa dapat mendeskripsikan, **mampu menjelaskan dan mempraktekkan mengenai konsep pengembangan pemrograman Android.**

Penyampaian materi adalah dengan **ceramah, diskusi, dan praktek**

2.2. Environment Setup dengan Android SDK

Untuk menjalankan dan menguji aplikasi React Native Anda di perangkat android, Anda perlu mengatur Lingkungan Android. Menyiapkan lingkungan pengembangan Anda bisa agak membosankan jika Anda baru mengenal pengembangan Android. Jika Anda sudah terbiasa dengan pengembangan Android, ada beberapa hal yang mungkin perlu Anda konfiguras[1]i. Dalam kedua kasus tersebut, harap pastikan untuk mengikuti beberapa langkah berikutnya dengan cermat. Berikut adalah 3 Langkah untuk Menyiapkan Lingkungan Pengembangan Android & Android Studio.

1. Pasang Android Studio

Unduh dan instal Android Studio . Pilih pengaturan "Kustom" ketika diminta untuk memilih jenis instalasi. Pastikan kotak di samping semua yang berikut ini dicentang:

- SDK Android
- Platform Android SDK
- Performa (Intel ® HAXM)
- Perangkat Virtual Android

Kemudian, klik "Berikutnya" untuk menginstal semua komponen ini.

Setelah penyiapan selesai dan Anda disajikan dengan layar Selamat Datang, lanjutkan ke langkah berikutnya.

2. Pasang Android SDK

Android Studio menginstal Android SDK terbaru secara default. Membangun aplikasi React Native dengan kode asli,

[1] Ableson, Frank; Sen, Robi; King, Chris (January 2011). Android in Action, Second Edition (2nd ed.). Manning. ISBN 978-1-935182-72-6.

bagaimanapun, membutuhkan Android 9 (Pie) SDK secara khusus. Android SDK tambahan dapat diinstal melalui SDK Manager di Android Studio.

SDK Manager dapat diakses dari layar "Selamat datang di Android Studio". Klik "Configure", lalu pilih "SDK Manager".

Gambar 2.1. Start –Up Android Studio

Gambar 2.1. menjelaskan tampilan awal saat kita memulai sebuah proyek applikasi berbasiskan Android dengan

SDK Manager juga dapat ditemukan dalam dialog "Preferensi" Android Studio, di bawah **Appearance & Behavior → System Settings → Android SDK** .

Pilih tab "Platform SDK" dari dalam SDK Manager, lalu centang kotak di samping "Tampilkan Detail Paket" di sudut kanan bawah. Cari dan luaskan Android 9 (Pie) entri, lalu pastikan semua item berikut dicentang:

- Platform Android SDK 28
- Gambar Sistem Intel x86 Atom_64 atau Google API Gambar Sistem Atom Intel x86

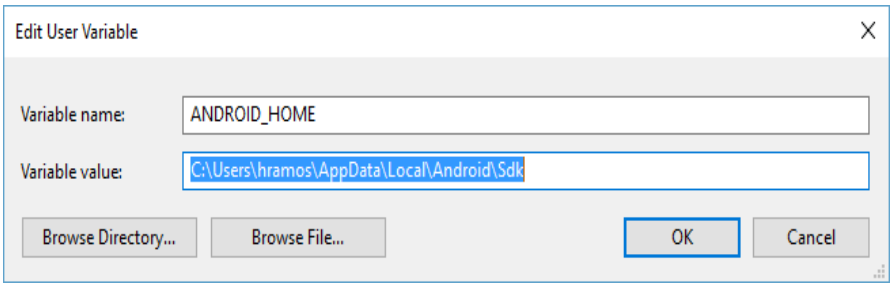
Selanjutnya, pilih tab "Alat SDK" dan centang kotak di samping "Tampilkan Detail Paket" di sini juga. Cari dan luaskan entri "Android SDK Build-Tools", lalu pastikan 28.0.3 sudah dipilih.
Terakhir, klik "Terapkan" untuk mengunduh dan memasang Android SDK dan alat pembuatan terkait.

3. Konfigurasikan variabel lingkungan ANDROID_HOME

Alat React Native memerlukan beberapa variabel lingkungan untuk disiapkan untuk membangun aplikasi dengan kode asli.

3.1. Untuk Pengguna Windows

Buka panel Sistem di bawah **Sistem dan Keamanan** di Panel Kontrol Windows, lalu klik **Ubah pengaturan** . Buka tab **Advanced** dan klik **Variabel Lingkungan**. Klik **Baru** untuk membuat ANDROID_HOME variabel pengguna baru yang mengarah ke jalur ke SDK Android Anda:



Gambar 2.2. Instalasi SDK

Gambar 2.2 merupakan Kit pengembangan perangkat lunak (SDK) adalah sekumpulan alat yang dapat digunakan oleh pembuat aplikasi untuk mengembangkan aplikasi yang dikustomisasi untuk ditambahkan, atau dihubungkan dengan, program lain. Dengan SDK, programmer dapat mengembangkan aplikasi untuk platform tertentu.

SDK diinstal, secara default, di lokasi berikut:

c:\Users\YOUR_USERNAME\AppData\Local\Android\Sdk

Anda dapat menemukan lokasi sebenarnya dari SDK dalam dialog "Preferences" Android Studio, di bawah **Appearance & Behavior → System Settings → Android SDK**. Buka jendela Command Prompt baru untuk memastikan variabel lingkungan baru dimuat sebelum melanjutkan ke langkah berikutnya.

Tambahkan alat platform ke Path

Buka panel Sistem di bawah **Sistem dan Keamanan** di Panel Kontrol Windows, lalu klik **Ubah pengaturan...** Buka tab **Advanced** dan klik **Variabel Lingkungan...** Pilih variabel **Path**, lalu klik **Edit**. Klik **Baru** dan tambahkan jalur ke alat platform ke daftar.

Lokasi default untuk folder ini adalah:

c:\Users\YOUR_USERNAME\AppData\Local\Android\Sdk\platform-tools

3.2. *Untuk Pengguna Linux*

Dengan asumsi Anda memiliki SDK yang diekstrak di ~/Android/Sdk

Tambahkan baris berikut ke file konfigurasi $HOME/.bash_profile(Jika Anda tidak dapat menemukan maka coba $HOME/.bashrc):

```
export ANDROID_HOME=$HOME/Android/Sdk
export PATH=$PATH:$ANDROID_HOME/tools
export PATH=$PATH:$ANDROID_HOME/tools/bin
export PATH=$PATH:$ANDROID_HOME/platform-tools
```

Untuk menguji apakah Anda telah mengaturnya dengan benar, jalankan perintah di bawah ini pada jendela terminal

1. Run
   echo $ANDROID_HOME
   // akan mencetak jalur ke SDK / home / Android / Sdk Anda

2. Run
   which android
   // akan mencetak / home / <user> / Android / Sdk / tools / android

3. Run
   android
   // Jika ini membuka **Android SDK Manager** , Anda siap melakukannya.

Beginilah cara Anda menginstal Android Studio dan menyiapkan Android Development Environment. Selanjutnya, Anda memerlukan perangkat Android untuk menjalankan aplikasi Android React Native Anda. Ini bisa berupa perangkat Android fisik atau lebih umum, Anda dapat menggunakan Perangkat Virtual Android yang memungkinkan Anda mengemulasi perangkat Android di komputer Anda[1].

2.3. Menjalankan aplikasi pada perangkat Android nyata

Kebanyakan ponsel dan tablet Android dapat dihubungkan ke sebuah komputer menggunakan sebuah kabel USB. Namun secara default, koneksi USB antara perangkat adodn sebuah komputer dibatasi hanya untuk transfer file.

Oleh karena itu, jika anda ingin menggunakan perangkatmu untuk pengembangan aplikasi Android, anda harus membuat sedikit perubahan konfigurasi baik pada perangkat dan komputermu. Di dalam tip singkat ini, saya akan menunjukkanmu bagaimana membuat perubahan itu.

[1] Rumbaugh, James; Michael Blaha; William Premerlani; Frederick Eddy; William Lorensen (1991). Object-Oriented Modeling and Design. Prentice Hall. ISBN 978-0-13-629841-0.

Prasyarat

Untuk bisa mengikuti tutorial ini, anda memerlukan:

Android SDK versi terbaru

Sebuah perangkat Android yang menjalankan Android 4.2 atau lebih tinggi

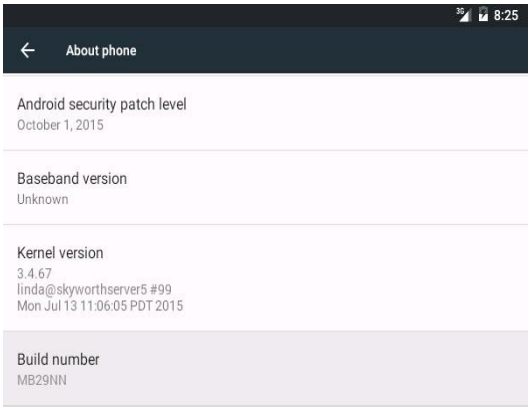
1. Mengkonfigurasi Perangkat Androidmu

Karena kebanyakan pengguna Android bukanlah pengembang aplikasi, pada perangkat yang menjalankan Android 4.2 atau lebih tinggi, semua pengaturan yang ditujukan bagi pengembang aplikasi tersembunyi secara default. Untuk menampilkan pengaturan ini, buka aplikasi Settings pada perangkatmu dan arahkan ke layar About phone. Berikutnya, scroll ke bawah hingga pada Build number dan klik itu tujuh kali.

Gambar 2.3. menjelaskan hasil pengaturan perangkat yang akan berhubungan dengan aplikasi.

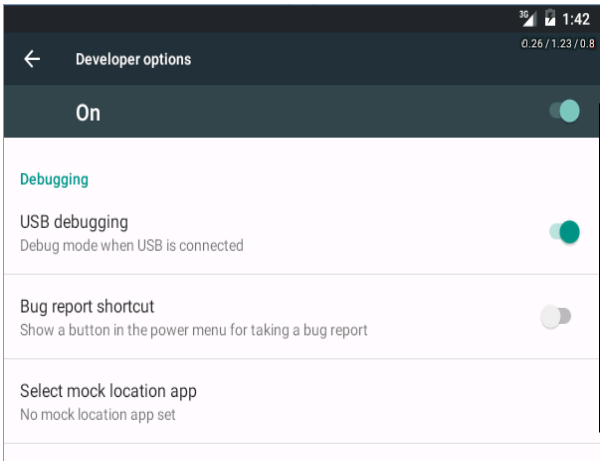
Ketika anda melakukan ini, anda harusnya dapat melihat menu Developer options. Buka itu dan pastikan pilihan USB debugging dicentang seperti pada Gambar 2.4.

USB Debugging adalah suatu tindakan yang dimanfaatkan untuk menelusuri dan mencari adanya kemungkinan cacat (bug) pada pengoperasian sistem android. Proses pencarian tersebut dapat dilakukan melalui media kabel USB. Pada awal kemunculannya, USB Debugging hanya dapat dioperasikan oleh pihak developer saja.



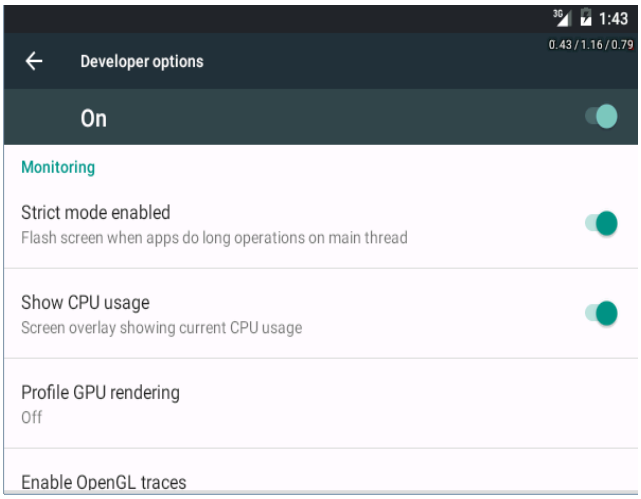
Gambar 2.3. Pengaturan Perangkat

Ketika anda melakukan ini, anda harusnya dapat melihat menu Developer options. Buka itu dan pastikan pilihan USB debugging dicentang.



Gambar 2.4. USB Debuging

Sebagai tambahan, saya menyarankan anda mencentang juga pada pilihan Strict mode enabled dan Show CPU usage. Dengan mengaktifkan option ini, lebih mudah bagimu untuk mengetahui apakah anda telah menyimpang dari pelaksanaan coding yang direkomendasikan.



Gambar 2.5. USB Debugging-2

Gambar 2.5. digunakan agar perangkatmu dapat digunakan untuk pengembangan aplikasi. Gunakan kabel USB untuk menghubungkannya ke komputer.

2. Mengkonfigurasi Komputer

Perubahan konfigurasi yang perlu anda buat pada komputer tergantung pada sistem operasi yang dijalankannya. Pada tip singkat ini, kita fokus pada OS X, Windows, dan Ubuntu.

OS X

Pada OS X, anda tidak harus membuat perubahan sama sekali.

Windows

Pada Windows 7 atau lebih tinggi, anda harus mendownload dan menginstal sebuah driver USB Original Equipment Manufacturer USB untuk perangkat Android. Biasanya, driver ini dapat ditemukan pada website pembuat perangkat. Jika anda menggunakan ponsel atau tablet Google Nexus, anda harus menginstal Google USB Driver.

Ubuntu

Pada kebanyakan jenis Ubuntu, konfigurasinya sedikit lebih banyak terlibat. Pertama-tama, anda harus menentukan vendor ID USB perangkatmu. Untuk melakukannya, anda dapat menggunakan perintah `lsusb`.

```
1 lsusb --verbose
```

Anda sekarang siap untuk melihat detail terkait USB pada semua perangkat yang terhubung pada komputermu melalui USB. Di dalam bagian Device description, cari nama perusahaan yang membuat perangkatmu dan buat catatan nilai pada bagian idVendor. Nilai itu hendaklah angka heksadesimal 4 digit.

Berikutnya, sebagai superuser, buat sebuah file baru dan beri nama itu /etc/udev/rules.d/51-android.rules.

```
1    sudo vi /etc/udev/rules.d/51-android.rules
```

Tambahkan aturan udev pada file ini:

```
1    SUBSYSTEM=="usb", ATTR{idVendor}=="YOUR_VENDOR_ID",
     MODE="0666", GROUP="plugdev"
```

Terakhir, gunakan perintah `chmod` untuk mengijinkan semua pengguna sistem membaca 51-android.rules.

```
1    sudo chmod a+r /etc/udev/rules.d/51-android.rules
```

3. Membangun Koneksi Local

Sekarang setelah kedua perangkat Android dan komputer telah dikonfigurasi, anda dapat memulai server Android Debug Bridge server, atau disingkat ADB, untuk secara otomatis membangun koneksi antara mereka.

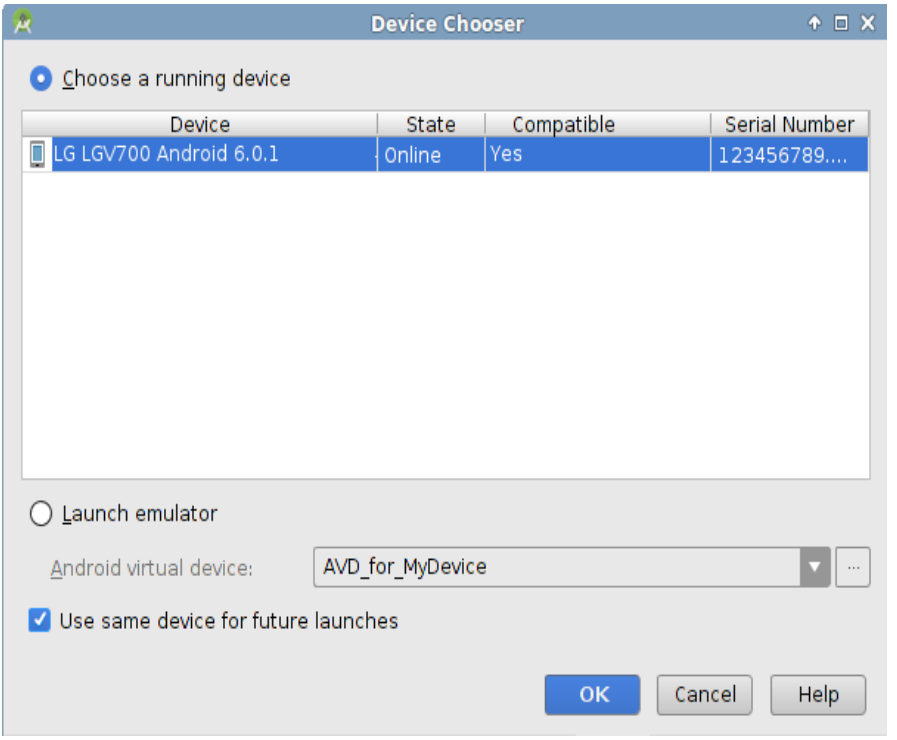
Arahkan ke direktori platform-tools pada Android SDK gunakan perintah `adb start-server` untuk memulai ADB.

```
1    adb start-server
```

Segera setelah server siap, anda melihat sebuah dialog muncul pada layer perangkatmu meminta untuk mengkonfirmasi apakah anda ingin membolehkan USB Debugging. Dialog juga berisi RSA fingerprint pada komputermu. Tekan OK untuk membentuk koneksi USB.

Mulai saat ini, anda dapat menggunakan perangkatmu alih-alih emulator saat mengembangkan aplikasi. Jika anda menggunakan Android Studio, atau menekan tombol Run di dalam toolbar, anda dapat melihat perangkatmu dalam daftar perangkat yang berjalan.

Dijelaskan pada Gambar 2.6. jenis perangkat yang akan terinstalasi dan menjalankan aplikasi.



Gambar 2.6. Running Device Path

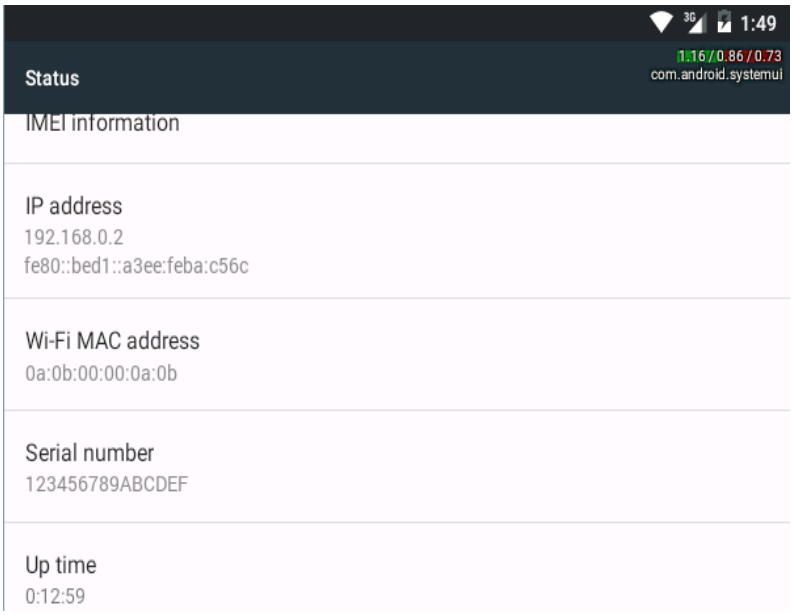
4. Membangun Sebuah Koneksi Melalui Wi-Fi

Banyak pengembang Android memiliki banyak ponsel dan tablet Android untuk melihat bagaimana tampilan dan perilaku pada ukuran layar dan versi Android yang berbeda. Menjaga semua perangkat tersebut terhubung ke komputer dengan kabel USB dapat tampak aneh. Oleh karena itu, ADB juga mengijinkan pengembang untuk menghubungkan perangkat mereka melalui Wi-Fi.

Agar perangkat dapat dikonfigurasi untuk debugging melalui koneksi Wi-Fi, hubungkan itu ke komputer dengan kabel USB. Sebagai tambahan, pastikan baik komputer dan perangkat terhubung pada jaringan Wi-Fi yang sama. Anda sekarang harus membuka sebuah port pada perangkat dimana itu dapat mengenali koneksi TCP/IP dengan menggunakan perintah `adb tcpip`. Sebagai contoh, berikut bagaimana anda membuka port 5565:

```
1    adb tcpip 5565
```

Gambar 2.7. adalah penjelasan bahwa perlu menentukan alamat IP perangkat. Untuk melakukannya, buka aplikasi Settings pada perangkat, arahkan ke layar About phone, dan klik Status. Anda dapat melihat IP address, baik dalam format IPv4 dan IPv6, di bawah heading IP address.



Gambar 2.7. Mementukan IP Address

Sekarang setelah anda mengetahui baik IP address dan port number, anda dapat mencopot perangkatmu dari komputer, dan menghubungkan itu melalui Wi-Fi dengan menggunakan perintah `adb connect`. Sebagai contoh, jika IP address perangkatmu adalah 192.168.0.2, berikut bagaimana anda dapat menghubungkannya:

```
1    adb connect 192.168.0.2:5565
```

Dari point ini, anda dapat menggunakan perangkat untuk pengembangan aplikasi Android sama seperti yang dihubungkan melalui USB.

Kesimpulan

Di dalam tip singkat ini, anda mempelajari bagaimana mengkonfigurasi baik perangkat Android dan komputer untuk USB debugging. Anda juga mempelajari bagaimana mengatur sebuah koneksi ADB melalui Wi-Fi.

Itu sangat penting bahwa anda melihat bagaimana aplikasimu bertindak pada sebanyak mungkin perangkat fisik, khususnya jika anda merencanakan untuk mempublikasikan aplikasimu pada Google Play. Mengapa begitu? Perangkat Android cenderung memiliki batasan yang, jika dibiarkan dapat menyebabkan aplikasi berperilaku aneh, atau bahkan crash.

Jika anda tidak memiliki semua perangkat Android yang ingin anda dukung, anda mungkin dapat mempertimbangkan menggunakan Cloud Test Lab milik Google, yang mengijinkanmu untuk secara mudah menjalankan dan menguji aplikasimu pada hampir semua perangkat Android populer.

2.4. Pengenalan pada Pemrograman Berorientasi Objek

Secara garis besar inilah poin-poin yang akan dibahas :
Apa Itu Pemrograman Berorientasi Objek?
Keunggulan Pemrograman Berorientasi Objek
Kelemahan Pemrograman Berorientasi Objek
Bahasa Pemrograman Yang Bisa Digunakan
Pemisalan Objek dalam Pemrograman Beriorientasi Objek
Karakteristik Pemrograman Beriorientasi Objek
Istilah-Istilah Dalam Pemrograman Berorientasi Objek

Apa Itu Pemrograman Berorientasi Objek?

Menurut dosenit.com pemrograman berorientasi objek merupakan metode yang berorientasi terhadap objek. Dimana semua data maupuan fungsi di definisikan ke dalam beberapa kelas atau objek yang tujuannya yaitu saling bekerjasama untuk memecahkan suatu masalah[1].

[1] Abadi, Martin; Luca Cardelli (1998). A Theory of Objects. Springer Verlag. ISBN 978-0-387-94775-4.

Metode ini biasa dikenal dengan istilah OOP (*Objek Oriented Programming*). Metode ini bisa memberikan fleksibiltas yang lebih banyak, pengubahan program yang mudah, dan sangat cocok digunakan untuk pemrograman yang berskala besar[1].

5 Keunggulan Pemrograman Berorientasi Objek

Ada beberapa keunggulan yang bisa kita dapatkan saat menggunakan metode OOP ini. Diantaranya :

1. *Improved Software Development Productivity* : Sistem program dapat dimodifikasi tanpa melibatkan banyak modul dimana hanya objek saja yang terlibat. Selain itu sistem program dapat dikembangkan sampai skala paling kompleks.
2. *Improved Software Maintainability* : Bagian dari software dapat dengan mudah di maintenance jika ada perubahan meskipun dalam skala yang cukup besar.
3. *Faster Development* : Metode ini didukung oleh banyak library objek, sehingga mempercepat penyelesaian program dan juga projek berikutnya.
4. *Lower Cost of Development* : Faster development tentu akan mengurangi biaya pengembangan pembuatan program
5. *Higher Quality Software* : Faster developmentpun akan memberikan lebih banyak waktu dan sumberdaya untuk proses verifikasi software.

4 Kelemahan Pemrograman Berorientasi Objek

Tentu saja setiap metode punya keunggulan dan kelemahan. Adapun kelemahan dari OOP yaitu :

1. Untuk beberapa programmer butuh waktu untuk terbiasa dengan OOP
2. Ukuran program yang dibuat dengan metode ini cukup besar
3. Runtime program lebih lambat
4. Tidak semua masalah program bisa diselesaikan dengan OOP

[1] Meyer, Bertrand (1997). Object-Oriented Software Construction. Prentice Hall. ISBN 978-0-13-629155-8.

9 Contoh Bahasa pemrograman yang mendukung OOP

Beberapa bahasa pemrograman yang bisa kita gunakan dengan metode pemrograman berorientasi objek yaitu :

- PHP
- Java
- Python
- Ruby
- C++
- Delphi
- C#
- Net
- Perl
- dan lainnya

Pemisalan Objek dalam Pemrograman Beriorientasi Objek

Objek-objek dalam dunia nyata memiliki 2 karakteristik yaitu status dan perilaku. Contoh : Sepeda mempunya status (Jumlah pedal, gir, dan ban). Sedangkan perilakunya (Mengerem, Mempercepat, dan Ubah gir).

Nah dalam pemrograman OOP ada dua karakteristik yaitu Variabel dan Method. Variable diumpamakan sebagai status sedangkan Method sebagai perilaku.

Karakteristik Pemrograman Beriorientasi Objek

- **Enkapsulasi (Pembungkusan)** : Merupakan pelindung program dan data yang sedang diolah. Enkapsulasi mendefinisikan perilaku dan melindungi program dan data agar tidak diakses secara sembarangan oleh orang lain.
- **Inheritansi :** Yaitu objek-objek yang ada disekitar kita adalah objek-objek yang saling terhubung secara hirarki. Contohnya : Lingkaran dan bujur sangkar adalah turunan dari bentuk 2D dan bentuk 2D adalah turunan dari gambar. Lingkaran dan bujur sangkar mewarisi (inherit) sifat-sifat dari bentuk 2D, juga merawisi sifat-sifat dari objek gambar. Lingkaran dan bujur sangkar dapat dikatan sebagai subsclass dari bentuk 2D.

Sedangkan bentuk 3D adalah superclass dari bola dan piramida, dst.

Istilah-Istilah Dalam Pemrograman Berorientasi Objek

- ***Class*** **:** yaitu cetakan dari object. Sebuah class berisi kode-kode yang menjelaskan bagaimana sebuah object akan berperilaku dan berinteraksi satu sama lain. Class dalam pemrograman diartikan seperti sebuah cetakan atau template.
- ***Property*** **:** merupakan variable yang dideklarasikan di dalam sebuah class, tetapi tidak berada di dalam fungsi atau method dari suatu class.
- ***Method*** **:** yaitu fungsi yang ada di dalam class. Method dapat diakses dengan tiga jenis user atau modifier. Dalam pemrograman objek method dapat menyimpan state dalam variabel dan mengimplementasikan behaviournya menggunakan method.
- ***Object*** **:** dalam dunia pemrograman objek diartikan sebagai bagian dari sebuah program. Dimana di dalamnya dihubungkan beberapa variable dan method yang salin berkaitan satu sama lain
- ***Overloading*** : yaitu pemisalan dalam sebuah class. Contoh : class mobil terdapat method info, dan class truk juga terdapat method yang sama. Inilah yang disebut dengan overloading. Jika sebuah mobil memanggil method info maka yang dikerjakan adalah method info yang berada di dalam class mobil. Tapi jika sebuah truk memanggil method info maka ada dua pilihan, yaitu : method info di class mobil dan method info di dalam class truk. Dan yang dikerjakan adalah method info di class truk.
- dan lain sebagainya

2.5. Kesimpulan

Itulah bahasan ringkas mengenai pemrograman berorientasi objek. Untuk lebih lengkapnya kamu bisa mencari referensi buku-buku atau ebook tentang OOP JAVA, PHP, dan bahasa pemrograman lainnya.

Tugas dan Diskusi:

Dalam tugas ini, Anda akan mengimplementasikan aplikasi "Hello World" untuk memverifikasi bahwa Android Studio sudah dipasang dengan benar dan mempelajari dasar-dasar pengembangan dengan Android Studio.

Tuliskan langkah-langka pengerjaannya

Referensi:

Abadi, Martin; Luca Cardelli (1998). A Theory of Objects. Springer Verlag. ISBN 978-0-387-94775-4.

Abelson, Harold; Gerald Jay Sussman (1997). Structure and Interpretation of Computer Programs. MIT Press. ISBN 978-0-262-01153-2

Gamma, Erich; Richard Helm; Ralph Johnson; John Vlissides (1995). Design Patterns: Elements of Reusable Object Oriented Software. Addison-Wesley. Bibcode:1995dper.book.....G. ISBN 978-0-201-63361-0.

Meyer, Bertrand (1997). Object-Oriented Software Construction. Prentice Hall. ISBN 978-0-13-629155-8.

Pecinovsky, Rudolf (2013). OOP – Learn Object Oriented Thinking & Programming. Bruckner Publishing. ISBN 978-80-904661-8-0.

Rumbaugh, James; Michael Blaha; William Premerlani; Frederick Eddy; William Lorensen (1991). Object-Oriented Modeling and Design. Prentice Hall. ISBN 978-0-13-629841-0.

Schach, Stephen (2006). Object-Oriented and Classical Software Engineering, Seventh Edition. McGraw-Hill. ISBN 978-0-07-319126-3.

Ableson, Frank; Sen, Robi; King, Chris (January 2011). Android in Action, Second Edition (2nd ed.). Manning. ISBN 978-1-935182-72-6.

Murphy, Mark (June 26, 2009). Beginning Android (1st ed.). Apress. ISBN 978-1-4302-2419-8.

Haseman, Chris (July 21, 2008). Android Essentials (1st ed.). Apress. ISBN 978-1-4302-1064-1.

BAB III.

ANDROID CORE COMPONENTS

3.1. Pendahuluan

Komponen aplikasi adalah blok bangunan penting dari aplikasi Android. Komponen ini digabungkan secara longgar oleh file manifes aplikasi AndroidManifest.xml yang menjelaskan setiap komponen aplikasi dan cara mereka berinteraksi. Berikut empat komponen utama yang dapat digunakan dalam aplikasi Android

Bahan kajian pembelajaran pada bab adalah penjelasan secara komprehensif tentang definisi **Android Android core components: 1. Activity & Intent.2. Services.3. Broadcast Receiver.4. Content Provider**.

Sub Capaian pembelajaran mata kuliah dalam dalam pertemuan ini adalah mahasiswa diharapkan dapat **Mengetahui dan memahami tentang komponen inti Android**.

Indikator pencapaian dalam pertemuan ini adalah mahasiswa dapat mendeskripsikan, **mampu menjelaskan dan mempraktekkan mengenai komponen inti Android.**

Penyampaian materi adalah dengan **ceramah, diskusi, dan praktek**

Gambar 3.1. Bagian utama dari aplikasi android
Sumber : https://www.wideskills.com/android/overview-android/principal-ingredients-android

Dari Gambar 3.1. mari kita lihat pengenalan singkat tentang komponen-komponen ini. Kami akan membahasnya secara rinci di bab berikutnya.

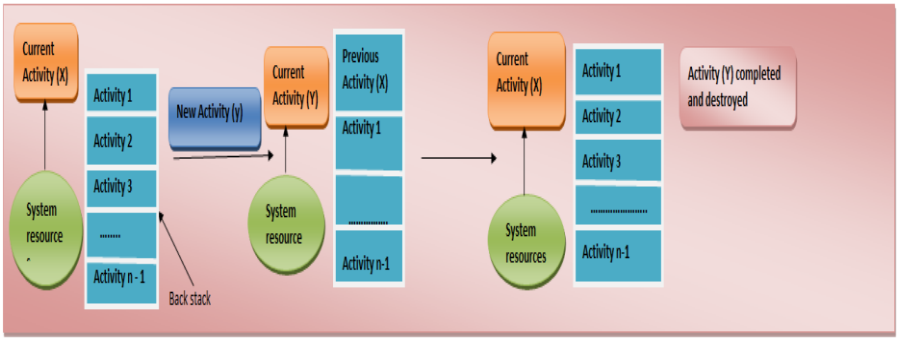
3.2. Activity & Intent

Salah satu **Activity** yang menjadi batu loncatan pertama adalah membangun aplikasi pengguna Android. Ini memberikan ruang bagi pengguna untuk melakukan apa saja. Misalnya, membuka kontak, memanggil pemanggil, dll. Semuanya dilakukan dengan berinteraksi dengan jendela dan jendela itu disediakan oleh aktivitas. Sebuah jendela disediakan untuk setiap aktivitas di mana antarmuka pengguna dilakukan. Umumnya setiap aplikasi Android memiliki lebih dari satu aktivitas. Ada satu aktivitas "utama". Semua aktivitas lainnya adalah aktivitas anak-anak. Ada tumpukan yang disebut **back-stack**. Kapan pun, ada jendela baru dimulai, aktivitas sebelumnya didorong ke back-stack dan dihentikan hingga aktivitas baru selesai. Segera setelah tombol belakang perangkat Anda ditekan, aktivitas baru dikeluarkan dari tumpukan dan dimusnahkan. Sekarang aktivitas sebelumnya dilanjutkan[1].

Misalnya, saat Anda mengirim SMS, Anda membuka messenger dan mengirim pesan. Anggaplah ini sebagai aktivitas

[1] Ableson, Frank; Sen, Robi; King, Chris (January 2011). Android in Action, Second Edition (2nd ed.). Manning. ISBN 978-1-935182-72-6.

Anda saat ini. Ketika Anda menekan tombol kembali, itu harus melanjutkan aktivitas sebelumnya dengan benar !! Aktivitas sebelumnya adalah layar beranda Anda sendiri. Mari kita pahami secara diagram.



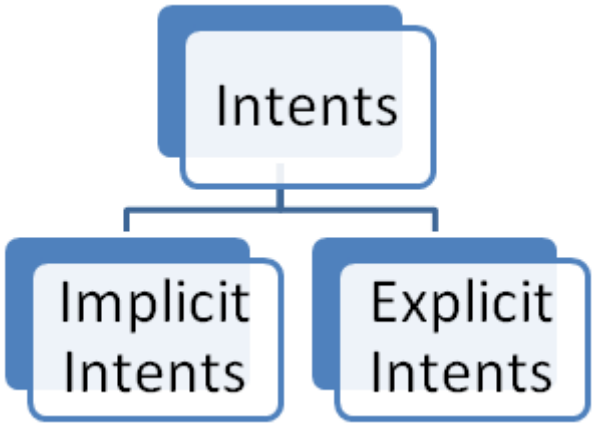
Gambar 3.2. Activity pada Aplikasi Android

Gambar 3.2. menjelaskan jika Anda seorang pemula atau tidak memiliki latar belakang komputer, Anda mungkin berpikir apa sih tumpukan, push dan pop ini. Tumpukan adalah struktur data di mana komputer mengatur datanya dalam memori. Menambahkan item ke ini disebut operasi dorong. Menghapus item disebut pop. Tumpukan memiliki struktur seperti rak buku tempat Anda menyusun buku, tetapi tidak seperti rak buku, hanya satu item yang dapat disisipkan dan dihapus dari tumpukan.

Intent adalah media komunikasi. Yaitu, komponen aplikasi saling mengirim pesan seperti yang Anda lakukan dengan teman Anda. Ini adalah objek perpesanan. Ini dapat digunakan untuk meminta tindakan dari komponen aplikasi lain. Android Intent bisa digunakan untuk membuat instance aktivitas baru atau mendapatkan hasil dari aktivitas lain. Sebuah layanan bisa dimulai dengan meneruskan maksud untuk melakukan satu operasi. Broadcast dijelaskan pada Gambar 3.3 dapat dikirim ke aplikasi lain dengan meneruskan maksud. Maksud terdiri dari dua jenis:

- **Implicit Intent**: Ini digunakan untuk mendeklarasikan tindakan umum yang akan dilakukan sehingga bagian dari aplikasi lain bisa menanganinya.

- **Explicit Intent**: Ini biasanya digunakan untuk memulai elemen baru dari aplikasi Anda sendiri. Elemen-elemen ini dimulai dengan namanya yaitu nama kelas yang memenuhi syarat. Misalnya, jika Anda ingin menelepon sahabat Anda, Anda akan melakukannya dengan nama dan jika dia tidak bersama Anda maka Anda pasti tahu alamat tempat tinggalnya. Sekarang ini adalah alamat tempat tinggal yang kami sebut sebagai nama yang memenuhi syarat.



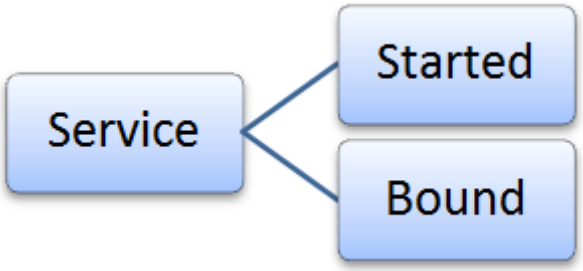
Gambar 3.3. Jenis Intent Pada Aplikasi Android

3.3. Services

Komponen penting lainnya dari aplikasi android adalah layanan. Itu tidak menyediakan antarmuka pengguna. Itu melakukan operasi yang berjalan lama di latar belakang. Sevices tidak berhenti bahkan jika komponen yang memulainya dihentikan atau dialihkan ke aplikasi lain. Sebuah Sevices dapat dihubungkan ke suatu komponen yang bahkan dapat melakukan komunikasi antar proses (IPC). Misalnya, ketika Anda menerima pembaruan email Anda di kotak masuk itu adalah Sevices. Anda mendapatkan pemberitahuan email baru meskipun Anda tidak menggunakan aplikasi email atau

melakukan hal lain. Luar biasa bukan. Sebuah Sevices dapat mengambil dua bentuk[1]:

- **Started**: Setelah Sevices dimulai, Sevices dapat berjalan tanpa batas dan biasanya melakukan operasi tunggal. Tidak ada hasil yang dikembalikan ke pengguna. Misalnya mengupload file. Setelah tugas selesai, itu harus berhenti sendiri.
- **Bound**: Dalam hal ini, komponen terikat ke Sevices sehingga tugas tertentu dapat diselesaikan. Jenis Sevices ini menyediakan antarmuka seperti klien-server. Permintaan dapat dikirim, menerima permintaan, dan mengembalikan hasil kepada pengguna. Komunikasi antar proses dicapai melalui Sevices ini. Komponen aplikasi dapat mengikat ke Sevices. Beberapa komponen dapat diikat ke jenis Sevices ini. Setelah penghancuran komponen, layanan dihentikan.



Gambar 3.4. Jenis Servis pada Aplikasi Android

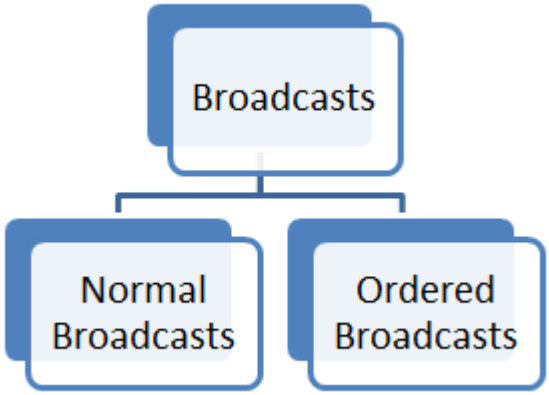
3.4. Broadcast Receiver

Broadcast adalah pesan yang disebarkan saat terjadi peristiwa apa pun. Mereka diterima oleh aplikasi. Maksud Android dapat digunakan untuk mengirimkan siaran ke aplikasi lain. Misalnya, saat perangkat Anda boot atau dinyalakan, sistem menghasilkan siaran ke semua aplikasi. Harus ada prosedur atau harus ada sesuatu yang dapat menerima siaran tersebut. Reseptor ini disebut penerima siaran. Untuk ini, Anda perlu mendaftarkan penerima dalam aktivitas

[1] Conder, Shane; Darcey, Lauren (July 24, 2012). Android Wireless Application Development Volume II: Advanced Topics (3rd ed.). Addison-Wesley Professional. ISBN 978-0-321-81384-8

yang akan kita tangani saat memprogram untuk hal yang sama[1]. Gambar 3.5. ada dua jenis siaran :

- **Normal Broadcast**: Ini bersifat asynchronous. Banyak penerima dapat diaktifkan pada saat yang sama yang tidak memiliki pesanan yang ditentukan. Tapi mereka sangat efisien.
- **Ordered Broadcast**: Mereka bersifat sinkron. Siaran yang diterima oleh satu penerima meneruskannya ke penerima lain. Siaran dikirim ke penerima secara one-to-one dan berurutan. Penerima mana pun akan meneruskan hasil ke penerima lain atau dapat menghancurkan siaran sepenuhnya.



Gambar 3.5. Jenis Broadcast pada Aplikasi Android

3.5. Content Provider

Komponen Android ini menghadirkan fungsionalitas berorientasi objek ke sistem. Content Provider merangkum data. Content Provider seperti namanya menyediakan konten dari satu proses ke proses lainnya sehingga bertindak sebagai antarmuka. Ini menyediakan gateway untuk mengakses data dari kumpulan terstruktur. Untuk mengakses data di penyedia konten, objek harus dibuat dan objek ini bertindak sebagai klien sedangkan Content Provider bertindak sebagai server. Objek inilah yang akan menerima permintaan mengambil hasil dan mengembalikan hasilnya. Android

[1] Conder, Shane; Darcey, Lauren (July 24, 2012). Android Wireless Application Development Volume II: Advanced Topics (3rd ed.). Addison-Wesley Professional. ISBN 978-0-321-81384-8

memiliki Content Provider yang mengelola video, audio, dll. Content Provider ini bersifat internal untuk aplikasi android. Misalnya, pencarian kustom di perangkat memerlukan penyedia konten.

3.6. Kesimpulan

Aspek unik dari desain sistem Android adalah aplikasi mana pun bisa memulai komponen aplikasi lain. Misalnya, jika Anda menginginkan pengguna mengambil foto dengan kamera perangkat, bisa saja aplikasi lain yang melakukannya dan aplikasi Anda bisa menggunakannya, sebagai ganti mengembangkan aktivitas sendiri untuk mengambil foto. Bila selesai, foto akan dikembalikan ke aplikasi sehingga Anda bisa menggunakannya. Bagi pengguna, kamera seakan menjadi bagian dari aplikasi Anda[1].

Saat sistem memulai komponen, sistem akan memulai proses untuk aplikasi itu dan membuat instance class yang diperlukan untuk komponen. Karenanya, tidak seperti aplikasi di sebagian besar sistem lain, aplikasi Android tidak memiliki titik masuk tunggal tidak ada main[2].

Karena sistem menjalankan setiap aplikasi dalam proses terpisah dengan izin file yang membatasi akses ke aplikasi lain, aplikasi Anda tidak bisa langsung mengaktifkan komponen dari aplikasi lain.

Tugas dan Diskusi:

1. Apa perbedaan antara maksud implisit dan eksplisit?
2. Kapan sebaiknya Anda memakai Fragmen, bukannya Aktivitas?
3. Saat Anda tengah mengganti satu Fragmen dengan yang lainnya – bagaimana Anda memastikan bahwa pengguna bisanya bisa kembali ke Fragmen sebelumnya dengan memencet tombol Kembali?
4. Bagaimana Anda akan membuat aplikasi multi thread Android tanpa memakai kelas Thread?

---

[1] Meier, Reto (March 2010). Professional Android 2 Application Development (1st ed.). Wrox Press. ISBN 978-0-470-56552-0.

[2] Haseman, Chris (July 21, 2008). Android Essentials (1st ed.). Apress. ISBN 978-1-4302-1064-1

5. Apakah ThreadPool? Apakah ia lebih efektif dari memakai beberapa Thread yang berbeda?
6. Apa hubungan antara siklus hidup AsyncTask dan siklus hidup Aktivitas? Apa masalah yang bisa muncul dan bagaimana menghindari masalah tersebut?

Referensi:

Ableson, Frank; Sen, Robi; King, Chris (January 2011). Android in Action, Second Edition (2nd ed.). Manning. ISBN 978-1-935182-72-6.

Conder, Shane; Darcey, Lauren (July 24, 2012). Android Wireless Application Development Volume II: Advanced Topics (3rd ed.). Addison-Wesley Professional. ISBN 978-0-321-81384-8.

Murphy, Mark (June 26, 2009). Beginning Android (1st ed.). Apress. ISBN 978-1-4302-2419-8.

Meier, Reto (March 2010). Professional Android 2 Application Development (1st ed.). Wrox Press. ISBN 978-0-470-56552-0.

Haseman, Chris (July 21, 2008). Android Essentials (1st ed.). Apress. ISBN 978-1-4302-1064-1.

BAB IV.

LOST DEVICE

4.1. Pendahuluan

Nomophobia adalah ketakutan ekstrim tanpa Perangkat Mobile (Ponsel) Anda. Ini tidak menyenangkan, apalagi dengan gejala fisik seperti detak jantung cepat dan dada sesak. Tentu saja, banyak orang tanpa nomofobia masih merasa mual karena kehilangan ponsel.

Bahan kajian pembelajaran pada bab adalah penjelasan secara komprehensif tentang definisi **Lost device: 1. Locate. 2. Lock. 3. Wipe..**

Sub Capaian pembelajaran mata kuliah dalam dalam pertemuan ini adalah mahasiswa diharapkan dapat **Mengetahui dan memahami ancaman atas kehilangan perangkat mobile.**

Indikator pencapaian dalam pertemuan ini adalah mahasiswa dapat mendeskripsikan, **mampu menjelaskan dan mempraktekkan mengenai pencegahan dan penaggulangan atas kehilangan perangkat mobile**.

Penyampaian materi adalah dengan **ceramah, diskusi, dan praktek**
.

Ponsel menghubungkan kita dengan teman, keluarga, rekan kerja, dan dunia pada umumnya. Perangkat seluler ini adalah perpanjangan dari diri kami sendiri, dan kami sangat merasakan ketidakhadirannya. Mereka juga mengandung banyak data pribadi. Bagaimana jika data itu jatuh ke tangan yang salah? Itu saja alasan untuk merasa cemas.

Kabar baiknya: Ada harapan. Ponsel yang hilang tidak selalu berarti hasil negatif seperti pencurian identitas. Itu terutama benar jika Anda telah mengambil langkah proaktif untuk melindungi ponsel Anda dan data di dalamnya.

1. **Melindungi:** Ambil langkah-langkah keamanan proaktif. Buat kode sandi yang kuat untuk ponsel Anda, tambahkan PIN ke kartu SIM Anda dan lakukan pencadangan data secara teratur. Berlatihlah untuk mencari lokasi ponsel Anda dari jarak jauh saat ponsel Anda aman dimiliki. Uji coba mempersiapkan Anda untuk menemukan ponsel dengan cepat jika Anda kehilangannya suatu hari nanti.

2. **Menemukan:** Ambil langkah-langkah segera untuk menemukan perangkat Anda setelah Anda menuai hilang. Tandai sebagai hilang, dan jika perlu, hapus data di dalamnya.

3. **Ubah dan Kontak:** Lindungi data pribadi Anda secara real time. Jika Anda tidak dapat menemukan perangkat Anda dan berisi, katakanlah, nomor kartu kredit, batalkan kartu-kartu ini. Ubah kata sandi email Anda dan hapus telepon sebagai perangkat terpercaya untuk otentikasi multi-faktor.

4. **Mengikuti:** Pantau terus laporan kredit, laporan bank, dan pke Anda. Meskipun ponsel Anda hilang hanya dalam 15 menit, itu sudah cukup bagi seseorang untuk memberikan informasi penting darinya.

4.2. Locate - Lock

Haruskah Saya Segera Mengunci Perangkat Saya dan Menghapus Datanya?

Ya untuk mengunci. Lakukan secepat mungkin dan tambahkan pesan di sepanjang baris, “Telepon Hilang. Silakan hubungi saya di [nomor]. ”

Penghapusan data lebih rumit. Misalnya, data dapat hilang selamanya kecuali Anda telah mencadangkannya baru-baru ini. Penghapusan bergantung pada faktor-faktor seperti ini:

- Seberapa dekat Anda dengan menemukan perangkat yang hilang atau memilikinya kembali
- Seberapa dekat Anda dengan menemukan perangkat yang hilang atau memilikinya kembali
- Seberapa sensitif data pribadi tersebut
- Tingkat perlindungan data yang telah Anda gunakan dengan ponsel Anda
- Seberapa banyak Anda bisa kehilangan secara permanen dengan penghapusan

Untuk memperluas poin terakhir, apakah Anda mencadangkan data Anda? Kapan pencadangan terakhir, dan seberapa teliti? Selain itu, penghapusan data berarti lokasi yang jauh tidak akan berfungsi lagi.

Memutuskan apakah akan menghapus perangkat Anda mengharuskan Anda untuk menyeimbangkan toleransi risiko Anda dengan realitas situasi yang dihadapi[1].

4.3. Wipe

Hapus Data dari Jarak Jauh

Anda mungkin perlu menghapus data di perangkat Anda dari jarak jauh. Ini dapat berlaku dalam kasus data ekstra-sensitif atau jika perangkat sedang bergerak, tidak dapat ditemukan atau terlalu jauh (di antara situasi lain). Berhati-hatilah jika Anda melakukan

[1] Welch, Chris. "Google's app for lost Android phones is now called Find My Device". theverge.com. The Verge. Retrieved August 17, 2019.

penghapusan data karena Anda mungkin tidak dapat lagi menemukan perangkat tersebut.

- Perlakukan penghapusan jarak jauh sebagai upaya terakhir kecuali jika datanya cukup sensitif dan / atau ponsel sudah lama hilang dan dibuka kuncinya.
- Perangkat Anda harus online. Jika offline, penghapusan dimulai saat online lagi.
- Jika Anda menemukan perangkat tersebut, gunakan cadangan iCloud atau iTunes terbaru Anda untuk memulihkan data.
- **Kunci Aktivasi** mencegah orang lain menggunakan perangkat Anda yang terhapus dari jarak jauh.
- Pesan khusus Anda terus ditampilkan setelah penghapusan data.
- Penghapusan data adalah ide yang bagus ketika Anda berencana untuk memberikan atau menjual perangkat Anda.

Pikirkan dua kali untuk **menghapus perangkat dari iCloud** setelah Anda melakukan penghapusan data. Itu menghapus Kunci Aktivasi dan pesan khusus. Dalam kasus seperti itu, seseorang dapat dengan mudah menyalakan perangkat Anda dan menggunakannya.

Hubungi operator nirkabel Anda untuk melaporkan perangkat Anda hilang (atau dicuri). Operator dapat menonaktifkan akun Anda sehingga tidak ada yang diizinkan untuk menggunakannya untuk panggilan, teks, dan data[1].

[1] "How to Find/Report a Lost/Stolen/Snatched Mobile Phone". Retrieved November 15, 2020.

4.4. Kesimpulan

Keamanan perangkat mencakup serangkaian opsi atau fitur keamanan efektif yang tersedia untuk perangkat seluler. Opsi atau fitur keamanan perangkat mencakup enkripsi perangkat lengkap, penguncian, penghapusan jarak jauh, GPS, kunci layar, segmentasi penyimpanan, GPS, kontrol inventaris, manajemen perangkat seluler, dan pengerasan.

Tugas dan Diskusi:

1. Dua metode manakah yang akan Anda gabungkan untuk melindungi data perangkat yang hilang tanpa menghapusnya dari perangkat?
2. Apa yang dimaksud dengan "**Remote Wipe**"

Referensi:

Welch, Chris. "Google's app for lost Android phones is now called Find My Device". theverge.com. The Verge. Retrieved August 17, 2019.

"How to Find/Report a Lost/Stolen/Snatched Mobile Phone". Retrieved November 15, 2020.

BAB V.

MOBILE AUTHENTICATION

5.1. Pendahuluan

Otentikasi (dari bahasa Yunani : **αὐθεντικός authentikos , "nyata, asli"**, dari **αὐθέντης authentes , "penulis"**) adalah tindakan membuktikan sebuah pernyataan , seperti identitas dari pengguna sistem komputer. Berbeda dengan identifikasi , tindakan menunjukkan identitas seseorang atau sesuatu, otentikasi adalah proses memverifikasi identitas itu.

Bahan kajian pembelajaran pada bab adalah penjelasan secara komprehensif tentang definisi **Single sign-on, Two factor authentication, Permission**

Sub Capaian pembelajaran mata kuliah dalam dalam pertemuan ini adalah mahasiswa diharapkan dapat **Mengetahui dan memahami tentang unauthorized akses sumberdaya mobile.**

Indikator pencapaian dalam pertemuan ini adalah mahasiswa dapat mendeskripsikan, **Mahasiswa mampu menjelaskan dan mempraktekkan mengenai otorisasi akses sumberdaya mobile**.

Penyampaian materi adalah dengan **ceramah, diskusi, dan praktek**

5.2. Single Sign-On.

Single Sign-On (**SSO**) adalah skema otentikasi yang memungkinkan pengguna untuk masuk dengan satu ID dan kata sandi ke salah satu dari beberapa sistem perangkat lunak yang terkait, namun independen[1].

Single Sign-On yang benar memungkinkan pengguna untuk masuk sekali dan mengakses layanan tanpa memasukkan kembali faktor otentikasi[2].

Tidak perlu bingung dengan sistem masuk yang sama (Directory Server Authentication), yang sering kali dilakukan dengan menggunakan Lightweight Directory Access Protocol (LDAP) dan database LDAP yang disimpan di server (direktori). [1] [2]

Versi sederhana Single Sign-Ondapat dicapai melalui jaringan IP menggunakan cookie tetapi hanya jika situs berbagi domain induk DNS yang sama. [3]

Untuk kejelasan, perbedaan harus dibuat antara Directory Server Authentication (same-sign on) dan single sign-on: Directory Server Authentication mengacu pada sistem yang memerlukan otentikasi untuk setiap aplikasi tetapi menggunakan kredensial yang sama dari server direktori, sedangkan Single Sign-Onmengacu pada sistem di mana satu otentikasi memberikan akses ke beberapa aplikasi dengan meneruskan token otentikasi secara mulus ke aplikasi yang dikonfigurasi[3].

Sebaliknya, **single sign-off** atau **single log-out** (**SLO**) adalah properti di mana satu tindakan keluar akan menghentikan akses ke beberapa sistem perangkat lunak[4].

Karena aplikasi dan sumber daya yang berbeda mendukung mekanisme autentikasi yang berbeda , Single Sign-On harus secara internal menyimpan kredensial yang digunakan untuk

---

[1] "SSO and LDAP Authentication". Authenticationworld.com. Archived from the originalon 2014-05-23. Retrieved 2014-05-23.
[2] "OpenID versus Single-Sign-On Server". alleged.org.uk. 2007-08-13. Retrieved 2014-05-23
[3] Jump up to:a b "Single Sign On Authentication". Authenticationworld.com. Archived from the original on 2014-03-15. Retrieved 2013-05-28.
[4] "OpenID Connect Single Sign-On (SSO)"

autentikasi awal dan menerjemahkannya ke kredensial yang diperlukan untuk mekanisme yang berbeda.

Skema otentikasi bersama lainnya, seperti OpenID dan OpenID Connect , menawarkan layanan lain yang mungkin mengharuskan pengguna untuk membuat pilihan saat masuk ke sumber daya, tetapi dapat dikonfigurasi untuk Single Sign-On jika layanan lain tersebut (seperti persetujuan pengguna) dinonaktifkan. [4] Semakin banyak login sosial federasi, seperti Facebook Connect , yang mengharuskan pengguna untuk memasukkan pilihan persetujuan saat pendaftaran pertama dengan sumber daya baru, dan karenanya tidak selalu masuk dalam arti yang paling ketat.

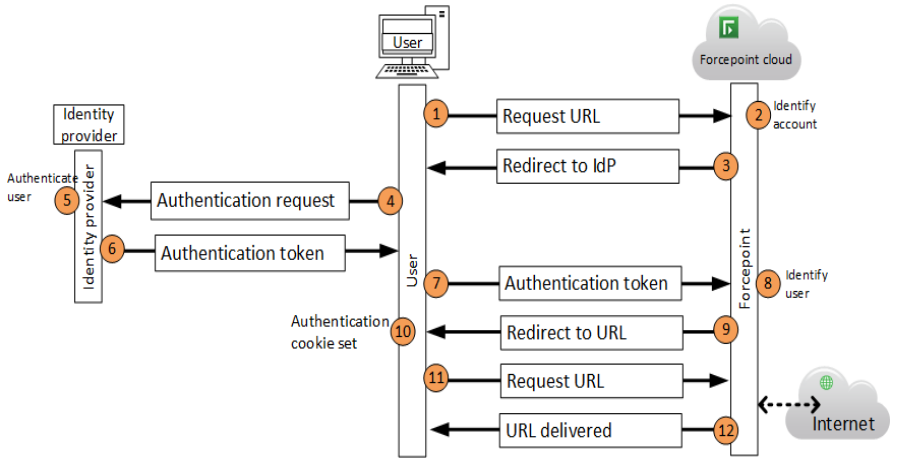
Manfaat menggunakan Single Sign-On meliputi:

- Mengurangi risiko akses ke situs pihak ketiga (kata sandi pengguna tidak disimpan atau dikelola secara eksternal)
- Kurangi kelelahan kata sandi dari berbagai kombinasi nama pengguna dan kata sandi
- Kurangi waktu yang dihabiskan untuk memasukkan kembali kata sandi untuk identitas yang sama
- Mengurangi biaya TI karena lebih rendahnya jumlah panggilan meja bantuan TI tentang sandi [5]

SSO berbagi server otentikasi terpusat yang digunakan semua aplikasi dan sistem lain untuk tujuan otentikasi dan menggabungkan ini dengan teknik untuk memastikan bahwa pengguna tidak harus secara aktif memasukkan kredensial mereka lebih dari sekali.

SSO adalah pengaturan manajemen identitas federasi (FIM), dan penggunaan sistem semacam itu terkadang disebut *federasi identitas* . OAuth , singkatan dari Open Authorization dan diucapkan "oh-auth," adalah kerangka kerja yang memungkinkan informasi akun pengguna akhir digunakan oleh layanan pihak ketiga, seperti Facebook, tanpa membeberkan kata sandi pengguna.

Gambar 5.1. ini memberikan visualisasi tentang cara kerja SSO



Gambar 5.1 Cara Kerja Single-Sign-On
Sumber: https://www.websense.com/content/support/library/web/hosted/sso_guide/how_sso_works.aspx

OAuth bertindak sebagai perantara atas nama pengguna akhir dengan menyediakan layanan dengan token akses yang memberi otorisasi informasi akun tertentu untuk dibagikan. Saat pengguna mencoba mengakses aplikasi dari penyedia layanan, penyedia layanan akan mengirimkan permintaan ke penyedia identitas untuk otentikasi. Penyedia layanan kemudian akan memverifikasi otentikasi dan memasukkan pengguna.

5.3. Two Factor Authentication.

Two Factor Authentication (2FA), kadang-kadang disebut sebagai verifikasi dua langkah atau Two Factor Authentication , adalah proses keamanan di mana pengguna menyediakan dua faktor otentikasi berbeda untuk memverifikasi diri mereka sendiri. Proses ini dilakukan untuk melindungi kredensial pengguna dan sumber daya yang dapat diakses pengguna dengan lebih baik. Two Factor Authentication memberikan tingkat keamanan yang lebih tinggi

daripada metode otentikasi yang bergantung pada otentikasi faktor tunggal (SFA), di mana pengguna hanya memberikan satu faktor - biasanya, kata sandi atau kode sandi. Metode Two Factor Authentication bergantung pada pengguna yang memberikan kata sandi, serta faktor kedua, biasanya berupa token keamanan atau biometrik faktor, seperti sidik jari atau pemindaian wajah[1].

Two Factor Authentication menambahkan lapisan keamanan tambahan ke proses otentikasi dengan mempersulit penyerang untuk mendapatkan akses ke perangkat seseorang atau akun online karena mengetahui kata sandi korban saja tidak cukup untuk melewati pemeriksaan otentikasi. Two Factor Authentication telah lama digunakan untuk mengontrol akses ke sistem dan data sensitif, dan penyedia layanan online semakin banyak menggunakan 2FA untuk melindungi kredensial penggunanya agar tidak digunakan oleh peretas yang telah mencuri database kata sandi atau menggunakan kampanye phishing untuk mendapatkan kata sandi pengguna .

Apa faktor otentikasi?

Ada beberapa cara berbeda di mana seseorang dapat diautentikasi menggunakan lebih dari satu metode otentikasi. Saat ini, sebagian besar metode otentikasi bergantung pada faktor pengetahuan, seperti kata sandi tradisional, sementara metode Two Factor Authentication menambahkan faktor kepemilikan atau faktor bawaan.

Faktor otentikasi, yang tercantum dalam perkiraan urutan adopsi untuk komputasi, meliputi berikut ini:

a. Sebuah faktor pengetahuan adalah sesuatu pengguna tahu, seperti password, PIN (nomor identifikasi pribadi) atau beberapa jenis lain dari rahasia bersama .
b. Sebuah faktor kepemilikan adalah sesuatu pengguna memiliki, seperti kartu ID, token keamanan, ponsel, perangkat mobile

[1]Rui Wang; Shuo Chen & XiaoFeng Wang. "Signing Me onto Your Accounts through Facebook and Google: a Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services"

atau aplikasi smartphone, untuk menyetujui permintaan otentikasi.

c. Sebuah faktor hal menjadi sifatnya , lebih sering disebut faktor biometrik , adalah sesuatu yang melekat dalam diri fisik pengguna. Ini mungkin atribut pribadi yang dipetakan dari karakteristik fisik, seperti sidik jari yang diautentikasi melalui pembaca sidik jari. Faktor pewarisan lain yang umum digunakan termasuk pengenalan wajah dan suara. Mereka juga mencakup biometrik perilaku , seperti dinamika penekanan tombol , gaya berjalan atau pola bicara.
d. Sebuah faktor lokasi , biasanya dilambangkan dengan lokasi dari mana upaya otentikasi sedang dibuat, dapat ditegakkan dengan membatasi upaya otentikasi ke perangkat tertentu di lokasi tertentu atau, lebih umum, dengan melacak sumber geografis upaya otentikasi berdasarkan sumber Alamat Internet Protocol (IP) atau beberapa informasi geolokasi lainnya, seperti data Global Positioning System (GPS), yang diperoleh dari ponsel pengguna atau perangkat lain.
e. Sebuah faktor waktu otentikasi Membatasi pengguna untuk waktu tertentu jendela di mana penebangan pada diperkenankan dan membatasi akses ke sistem di luar jendela itu.
f.

Perlu dicatat bahwa sebagian besar metode Two Factor Authentication bergantung pada tiga faktor otentikasi pertama, meskipun sistem yang membutuhkan keamanan lebih besar dapat menggunakannya untuk menerapkan Multi Factor Authentication (MFA), yang dapat mengandalkan dua atau lebih kredensial independen untuk lebih aman. autentikasi.

Bagaimana cara kerja otentikasi dua faktor?

Gambar 5.2. Cara Kerja Two Factor Authenticator
Sumber: https://www.merchantfraudjournal.com/two-factor-authentication-work/

Berikut penjelasn Gambar 5.2. yaitu cara kerja otentikasi dua faktor:

1. Pengguna diminta untuk masuk oleh aplikasi atau situs web.
2. Pengguna memasukkan apa yang mereka ketahui - biasanya, nama pengguna dan kata sandi. Kemudian, server situs menemukan kecocokan dan mengenali pengguna.
3. Untuk proses yang tidak memerlukan kata sandi, situs web menghasilkan kunci keamanan unik untuk pengguna. Alat otentikasi memproses kunci, dan server situs memvalidasinya.
4. Situs tersebut kemudian meminta pengguna untuk memulai langkah login kedua. Meskipun langkah ini dapat mengambil berbagai bentuk, pengguna harus membuktikan bahwa mereka hanya memiliki sesuatu yang mereka miliki, seperti token keamanan, kartu ID, ponsel cerdas, atau perangkat seluler lainnya. Ini adalah faktor penguasaan.
5. Kemudian, pengguna memasukkan kode satu kali yang dibuat selama langkah keempat.
6. Setelah memberikan kedua faktor tersebut, pengguna diautentikasi dan diberikan akses ke aplikasi atau situs web.

Elemen otentikasi dua faktor

Otentikasi dua faktor adalah bentuk MFA. Secara teknis, ini digunakan kapan saja dua faktor otentikasi diperlukan untuk mendapatkan akses ke sistem atau layanan. Namun, menggunakan

dua faktor dari kategori yang sama bukan merupakan 2FA; misalnya, memerlukan kata sandi dan rahasia bersama masih dianggap SFA karena keduanya termasuk dalam jenis faktor otentikasi yang sama: pengetahuan. otentikasi dua factor.

Sejauh layanan SFA berjalan, ID pengguna dan kata sandi bukanlah yang paling aman. Satu masalah dengan otentikasi berbasis kata sandi adalah diperlukan pengetahuan dan ketekunan untuk membuat dan mengingat kata sandi yang kuat. Kata sandi membutuhkan perlindungan dari banyak ancaman di dalam, seperti catatan tempel yang disimpan secara sembarangan dengan kredensial masuk, hard drive lama, dan eksploitasi manipulasi psikologis. Kata sandi juga menjadi mangsa ancaman eksternal, seperti peretas yang menggunakan serangan brute force, kamus, atau tabel pelangi .

Dengan waktu dan sumber daya yang cukup, penyerang biasanya dapat melanggar sistem keamanan berbasis kata sandi dan mencuri data perusahaan, termasuk informasi pribadi pengguna. Kata sandi tetap menjadi bentuk SFA yang paling umum karena biayanya yang rendah, kemudahan penerapan dan keakrabannya. Berbagai pertanyaan tantangan-respons dapat memberikan lebih banyak keamanan, bergantung pada bagaimana penerapannya, dan metode verifikasi biometrik yang berdiri sendiri juga dapat memberikan metode SFA yang lebih aman.

5.4. Permission

Adalah cara untuk mengontrol dan mengatur akses ke fungsi tingkat sistem dan perangkat tertentu oleh perangkat lunak . Biasanya, jenis izin mencakup fungsi yang mungkin memiliki implikasi privasi , seperti kemampuan untuk mengakses fitur perangkat keras perangkat (termasuk kamera dan mikrofon), dan data pribadi (seperti penyimpanan perangkat, daftar kontak , dan lokasi geografis pengguna saat ini.). Izin biasanya dideklarasikan dalam manifes aplikasi , dan izin tertentu harus diberikan secara khusus pada waktu proses oleh pengguna – yang dapat mencabut izin kapan saja.

Perangkat seluler

Pada sistem operasi seluler untuk ponsel cerdas dan tablet , jenis izin yang umum mengatur: [1] [2]

1. Akses ke penyimpanan dan informasi pribadi, seperti kontak , janji temu kalender, dll.
2. Pelacakan lokasi .
3. Akses ke kamera internal dan / atau mikrofon perangkat .
4. Akses ke sensor biometrik , termasuk pembaca sidik jari dan sensor kesehatan lainnya ..
5. akses internet .
6. Akses ke antarmuka komunikasi (termasuk pengenal perangkat keras dan kekuatan sinyal jika berlaku, dan permintaan untuk mengaktifkannya), seperti Bluetooth , Wi-Fi , Komunikasi jarak dekat (NFC), dan lainnya.
7. Melakukan dan menerima panggilan telepon .
8. Mengirim dan membaca pesan teks
9. Kemampuan untuk melakukan pembelian dalam aplikasi .
10. Kemampuan untuk "menghamparkan" dirinya sendiri dalam aplikasi lain.
11. Menginstal, menghapus, dan mengelola aplikasi.
12. Token otentikasi (yaitu yang OAuth) dari layanan web yang disimpan di penyimpanan sistem untuk berbagi antar aplikasi.

Sebelum Android 6.0 "Marshmallow" , izin diberikan secara otomatis ke aplikasi pada waktu proses, dan diberikan setelah pemasangan di Google Play Store . Sejak Marshmallow, izin tertentu sekarang memerlukan aplikasi untuk meminta izin pada waktu proses oleh pengguna. Izin ini juga dapat dicabut kapan saja melalui menu pengaturan Android. [3] Penggunaan izin di Android terkadang disalahgunakan oleh pengembang aplikasi untuk mengumpulkan informasi pribadi dan mengirimkan iklan; khususnya, aplikasi untuk menggunakan flash kamera ponsel sebagai senter(yang sebagian besar menjadi mubazir karena integrasi fungsionalitas semacam itu pada tingkat sistem pada versi Android yang lebih baru) diketahui membutuhkan sejumlah besar

izin yang tidak perlu di luar apa yang sebenarnya diperlukan untuk fungsionalitas yang dinyatakan. [4]

iOS memberlakukan persyaratan serupa untuk izin yang akan diberikan pada waktu proses, dengan kontrol tertentu ditawarkan untuk mengaktifkan Bluetooth, Wi-Fi, dan pelacakan lokasi. [5] [6]

WebPermissions

WebPermissions adalah sistem izin untuk browser web . [7] Ketika aplikasi web membutuhkan beberapa data di balik izin, ia harus memintanya terlebih dahulu. Saat melakukannya, pengguna melihat jendela yang memintanya untuk membuat pilihan. Pilihannya diingat, tapi bisa dihapus belakangan ini.
Saat ini sumber daya berikut dikendalikan:

1. geolokasi
2. pemberitahuan desktop
3. pekerja layanan
4. sensor
5. perangkat penangkap audio, seperti kartu suara , dan nama model serta karakteristiknya
6. perangkat perekam video,] seperti kamera , dan pengenal serta karakteristiknya

Model kontrol akses berbasis izin memberikan hak akses untuk objek data tertentu ke aplikasi. Ini adalah turunan dari model kontrol akses diskresioner. Izin akses biasanya diberikan dalam konteks pengguna tertentu di perangkat tertentu. Izin diberikan secara permanen dengan beberapa batasan otomatis.

Dalam beberapa kasus, izin diterapkan dalam pendekatan 'semua atau tidak sama sekali': pengguna harus memberikan semua izin yang diminta ke suatu aplikasi, atau tidak dapat menggunakan aplikasi tersebut. Izin tetap tidak transparan bagi pengguna saat izin digunakan oleh program atau aplikasi untuk mengakses data yang dilindungi oleh mekanisme kontrol akses izin. Meskipun pengguna dapat mencabut izin, aplikasi dapat memeras pengguna dengan menolak untuk beroperasi, misalnya dengan hanya mogok .

Mekanisme perizinan telah banyak dikritik oleh peneliti karena beberapa alasan, antara lain;

1. Ekstraksi dan pengawasan data pribadi yang tidak transparan, termasuk penciptaan rasa aman yang palsu;
2. Kelelahan pengguna akhir dari izin akses pengelolaan mikro yang mengarah pada penerimaan pengawasan dan intransparensi yang fatalistik; [
3. Ekstraksi data besar-besaran dan pengawasan pribadi dilakukan setelah izin diberikan.

Ada beberapa solusi, seperti XPrivacy, yang alih-alih memberikan akses ke data yang diminta alih-alih memberikan pengecualian dan membuat aplikasi crash dan mengembalikan disinformasi untuk membuat aplikasi beroperasi seolah-olah izin diberikan. Mockdroid adalah contoh lain dari pendekatan ini. Analisis statis juga dapat digunakan untuk menganalisis izin yang diminta. Metode transparansi lebih lanjut mencakup pembuatan profil perilaku longitudinal dan analisis privasi beberapa sumber dari akses data aplikasi.

5.5. Kesimpulan

- Mobile Authentication adalah verifikasi identitas pengguna melalui penggunaan perangkat seluler dan satu atau beberapa metode autentikasi untuk akses aman.
- Mobile Authentication dapat digunakan untuk mengotorisasi perangkat seluler itu sendiri atau sebagai bagian dari skema otentikasi multifaktor untuk masuk ke lokasi dan sumber daya yang aman.
- Entri kata sandi tidak tepat pada ponsel, terutama jika memasukkan huruf kapital, angka dan simbol.
- Beberapa metode alternatif otentikasi seluler meliputi:
- Kata sandi non-teks, di mana simbol atau gambar dapat dipilih dari bidang yang dibuat secara acak.
- Sertifikat digital menggunakan infrastruktur kunci publik.
- Kartu pintar dengan data otentikasi tersimpan.

- Otentikasi out of band, di mana pengguna melakukan panggilan untuk mendapatkan otentikasi.
- Kata sandi satu kali (OTP) melalui aplikasi telepon atau pesan SMS.
- Beberapa organisasi memiliki kebutuhan keamanan ekstra selain ID dan kata sandi untuk masuk, tetapi perangkat dan metode tambahan dapat membuat prosedur terlalu rumit bagi karyawan. Namun, keberadaan smartphone di mana-mana dapat membantu meringankan beban di sini. Sebagian besar ponsel cerdas memiliki perangkat GPS, memungkinkan konfirmasi kepastian yang wajar dari lokasi login, kamera untuk potensi pengenalan wajah dan pemindaian iris, mikrofon untuk pengenalan suara; beberapa juga memiliki layar sentuh yang dapat digunakan untuk pemindaian jari.
- Perangkat seluler yang menggunakan lebih dari satu kemampuan ini adalah token multifaktor yang berfungsi. Contohnya adalah penggunaan aplikasi token perangkat lunak ponsel cerdas yang memanfaatkan lokasi GPS dan memindai sidik jari, semua di dalam perangkat yang mungkin akan dibawa oleh pengguna. Bagi administrator, manfaat utama dari implementasi perangkat lunak adalah tidak ada perangkat fisik tambahan untuk dikelola.

Tugas dan Diskusi:

1. Apa arti istilah otentikasi (*Authentication*)?
2. Apa itu otentikasi multi-faktor?
3. Jelaskan salah satu metode otentikasi multi-faktor dan diskusikan pro dan kontra penggunaan otentikasi multi-faktor.

Referensi

1. *JumpCloud. 2019-05-14. Retrieved 2020-10-27.*
2. *"SSO and LDAP Authentication". Authenticationworld.com. Archived from the originalon 2014-05-23. Retrieved 2014-05-23.*
3. *"OpenID versus Single-Sign-On Server". alleged.org.uk. 2007-08-13. Retrieved 2014-05-23.*

4. "OpenID Connect Single Sign-On (SSO)".
5. "Benefits of SSO". University of Guelph. Retrieved 2014-05-23.
6. Jump up to: a b "Single Sign On Authentication". Authenticationworld.com. Archived from the original on 2014-03-15. Retrieved 2013-05-28.
7. "Sun GlassFish Enterprise Server v2.1.1 High Availability Administration Guide". Oracle.com. Retrieved 2013-05-28.
8. Laurenson, Lydia (3 May 2014). "The Censorship Effect". TechCrunch. Archived from the original on August 7, 2020. Retrieved 27 February 2015.
9. Chester, Ken (12 August 2013). "Censorship, external authentication, and other social media lessons from China's Great Firewall". Tech in Asia. Archived from the original on March 26, 2014. Retrieved 9 March 2016.
10. Rui Wang; Shuo Chen & XiaoFeng Wang. "Signing Me onto Your Accounts through Facebook and Google: a Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services".
11. "OpenID: Vulnerability report, Data confusion" - OpenID Foundation, March 14, 2012
12. "Facebook, Google Users Threatened by New Security Flaw". Tom's Guide. 2 May 2014. Retrieved 11 November 2014.
13. "Covert Redirect Vulnerability Related to OAuth 2.0 and OpenID". Tetraph. 1 May 2014. Retrieved 10 November 2014.
14. "Math student detects OAuth, OpenID security vulnerability". Tech Xplore. 3 May 2014. Retrieved 10 November 2014.
15. "Facebook, Google Users Threatened by New Security Flaw". Yahoo. 2 May 2014. Retrieved 10 November 2014.
16. "Covert Redirect Flaw in OAuth is Not the Next Heartbleed". Symantec. 3 May 2014. Retrieved 10 November 2014.
17. MIT IST. "OpenID Connect Authorization".
18. Goode, Lauren (2019-06-15). "App Makers Are Mixed on 'Sign In With Apple'". Wired. ISSN 1059-1028. Retrieved 2019-06-15.
19. "MicroStrategy's office of the future includes mobile identity and cybersecurity". Washington Post. 2014-04-14. Retrieved 2014-03-30.

BAB VI.

KRIPTOGRAFI

6.1. Pendahuluan

Kriptografi , atau kriptologi (dari bahasa Yunani Kuno **: κρυπτός** , diromanisasi : **kryptós** "**hidden, secret**"; dan **γράφειν** graphein , "**to write**", atau **-λογία** -logia , "**study**", masing-masing), adalah praktik dan pembelajaran teknik untuk komunikasi yang aman di hadapan pihak ketiga yang disebut musuh . Secara umum, kriptografi adalah tentang membangun dan menganalisis protokol yang mencegah pihak ketiga atau publik untuk membaca pesan pribadi; berbagai aspek dalamkeamanan informasi seperti kerahasiaan data , integritas data , otentikasi , dan non-repudiation adalah pusat kriptografi modern. Kriptografi modern berada di persimpangan disiplin ilmu matematika , ilmu komputer , teknik elektro , ilmu komunikasi , dan fisika . Aplikasi kriptografi meliputi perdagangan elektronik , kartu pembayaran berbasis chip , mata uang digital , sandi komputer , dan komunikasi militer[1]

Bahan kajian pembelajaran pada bab adalah penjelasan secara komprehensif tentang definisi **Kriptografi: . Enkripsi,. Dekripsi. Hashing. Key management., Digital signature.**

[1] Becket, B (1988). Introduction to Cryptology. Blackwell Scientific Publications. ISBN 0-632-01836-4. OCLC 16832704. Excellent coverage of many classical ciphers and cryptography concepts and of the "modern" DES and RSA systems

Sub Capaian pembelajaran mata kuliah dalam dalam pertemuan ini adalah mahasiswa diharapkan dapat **Mengetahui dan memahami tentang kriptografi.**

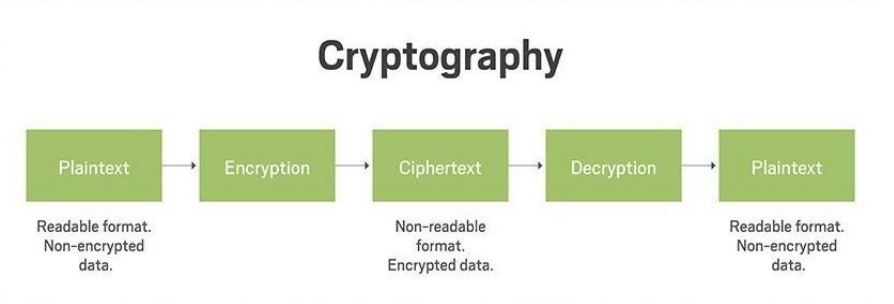
Indikator pencapaian dalam pertemuan ini adalah mahasiswa dapat mendeskripsikan, **Mahasiswa mampu menjelaskan dan mempraktekkan mengenai enkripsi dan dekripsi. teknik hashing dan digital signature.**

Penyampaian materi adalah dengan **ceramah, diskusi, dan praktek**

Kriptografi adalah ilmu yang mempelajari bagaimana membuat suatu pesan yang dikirim pengirim dapat disampaikan kepada penerima dengan aman .

Berdasarkan sejarahnya kriptografi terpisah menjadi dikotomi kode dan chipher, dengan penggunaan kode memiliki terminologi sendiri, hal ini juga berlaku pada chipher dengan istilah "**encoding, codetext, decoding**" dan lain-lain. Sebuah kode memiliki cara tersendiri untuk dapat dikembalikan ke bentuk semula. Sedangkan kode sudah tidak lagi digunakan pada kriptografi modern, dan saat ini chiper lebih dominan digunakan daripada kode untuk melakukan enkripsi data.

Pada Gambar 6.1. dijelaskan proses dari kriptografi, dimana Kriptografi adalah proses enkripsi dan dekripsi data.



Gambar 6.1 Proses Kriptografi
Sumber: https://www.techtarget.com/searchsecurity/definition/cryptography

Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, intergritas data, serta autentikasi data [1]

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

1. Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
2. Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
3. Autentikasi, adalah berhubungan dengan identifikasi/ pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
4. Non-repudiasi, atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/ terciptanya suatu informasi oleh yang mengirimkan/membuat.

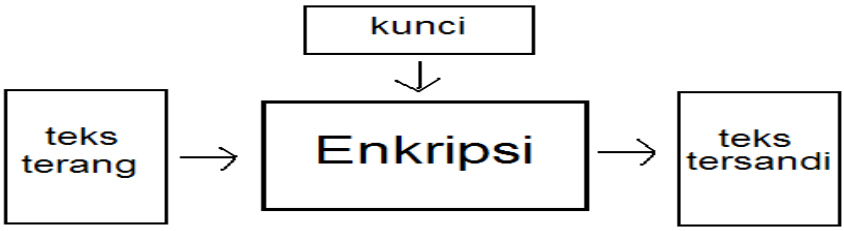
6.2. Enkripsi (Encrypt)

Di bidang kriptografi, enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Karena enkripsi telah digunakan untuk mengamankan komunikasi di berbagai negara, hanya organisasi-organisasi tertentu dan individu yang memiliki kepentingan yang sangat mendesak akan kerahasiaan yang

[1] Ibrahim A. Al-Kadi, "The Origins of Cryptology: the Arab Contributions," Cryptologia, vol. 16, no. 2 (April 1992), pp. 97–126

menggunakan enkripsi. Pada pertengahan tahun 1970-an, enkripsi kuat dimanfaatkan untuk pengamanan oleh sekretariat agen pemerintah Amerika Serikat pada domain publik. Saat ini, enkripsi telah digunakan pada sistem secara luas, seperti Internet, perdagangan elektronik, jaringan telepon bergerak, dan ATM bank[1].

Enkripsi dapat digunakan untuk tujuan keamanan. Namun, teknik lain masih diperlukan untuk membuat komunikasi yang aman, terutama untuk memastikan integritas dan autentikasi sebuah pesan, misal kode autentikasi pesan (MAC) atau tanda tangan digital. Penggunaan yang lain adalah untuk melindungi dari analisis jaringan komputer.



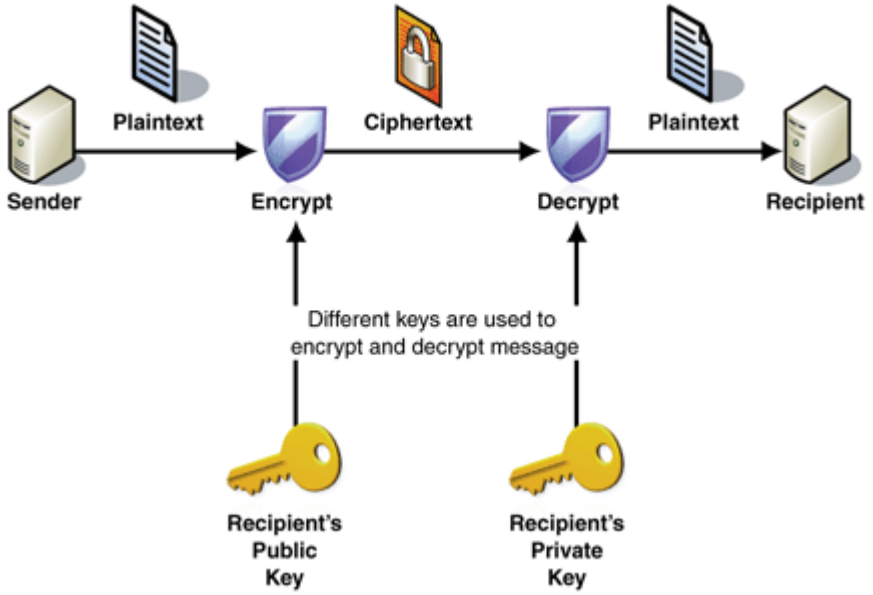
Gambar 6.2. Proses Enkripsi

Secara singkat, proses enkripsi adalah proses mengubah teks terang menjadi teks tersandi.

6.3. Dekripsi (Decrypt)

Dekripsi (Decrypt) adalah cara merubah kembali data yang tadinya telah di enkripsi menjadi sebuah kode tertentu kemudian dikembalikan ke bentuk semula, contohnya seperti kode-kode yang berbentuk hash dan binary. Proses dijelaskan pada Gambar 6.3. Pesan dikirim melalui encrypter, tidak ada yang bisa membaca teks tanpa perangkat lunak terenkripsi dan kunci yang telah digunakan. Jika ada pengguna yang bermaksud mengirim pijatan terbuka ke banyak orang (keluarga, teman, kolega, dll.) dan jika itu juga dibaca oleh banyak orang di ujung lain (server surat publik, ICQ, dll.)

[1] Stallings, William (March 2013). Cryptography and Network Security: Principles and Practice (edisi ke-6th). Prentice Hall. ISBN 978-0133354690.



Gambar 6.3. Proses Enkripsi – Dekripsi
Sumber: https://www.researchgate.net/figure/Different-keys-are-used-to-encrypt-and-decrypt-message_fig2_304290938

6.4. Hashing

Hasing adalah Transformasi aritmatik sebuah string dari karakter menjadi nilai yang merepresentasikan string aslinya.

"***Hashing mengubah sepotong data (kecil atau besar), menjadi potongan data yang relatif singkat seperti string atau integer.***"

Jika kriptografi adalah sebuah tubuh, algoritma hashing-nya akan menjadi intinya. Jika kriptografi adalah sebuah mobil, algoritma hashingnya akan menjadi mesinnya. Jika kriptografi adalah sebuah film, algoritme hashingnya akan menjadi bintangnya. Jika kriptografi adalah tata surya, algoritme hashingnya adalah matahari. Oke, itu mungkin terlalu jauh, tetapi Anda mengerti maksudnya, bukan? Sebelum kita membahas tentang apa itu algoritma hashing, mengapa ada, dan bagaimana cara kerjanya, penting untuk

memahami di mana letak mur dan bautnya. Mari kita mulai dengan **hashing** .

Tugas utama Hashing adalah untuk memastikan integritas (keutuhan). Maksudnya seperti apa ya? Contohnya, kita ada sebuah file. Dengan di-Hashing kita akan memdapatkan nilai tertentu sebagai bagian integritas file tersebut. Apabila file itu dirubah, maka nilainya tidak akan sama lagi dengan Hashing pertama. Jadi kita bisa tahu ini bukan file yang sama, ini yang kita sebuat integritas dari sebuah file. Kita bisa lihat cara ini digunakan oleh Git.

Apa Itu Hashing?

Mari kita coba membayangkan situasi hipotetis di sini. Misalkan Anda ingin mengirim pesan / file kepada seseorang dan sangat penting untuk mencapai penerima yang dituju dalam format yang sama persis. Bagaimana Anda melakukannya? Salah satu opsinya adalah mengirimnya beberapa kali dan memverifikasi bahwa itu tidak dirusak. Tapi bagaimana jika pesannya terlalu panjang? Bagaimana jika file berukuran gigabyte? Akan sangat tidak masuk akal, tidak praktis, dan, terus terang, membosankan untuk memverifikasi setiap huruf, bukan? Nah, di situlah hashing berperan.

Menggunakan algoritma hash yang dipilih, data dikompresi ke ukuran tetap. Mari kita pahami ini dengan sebuah contoh. Jika kita mengambil kalimat, "Keledai hidup lama" dan menerapkan algoritma hash **joaat** padanya, kita akan mendapatkan **6e04f289** . Nilai ini dikenal sebagai **hash** .

Hash sangat mudah digunakan saat Anda ingin mengidentifikasi atau membandingkan file atau database. Daripada membandingkan data dalam bentuk aslinya, lebih mudah bagi komputer untuk membandingkan nilai hash. Baik itu menyimpan kata sandi, dalam grafik komputer, atau dalam sertifikat SSL, hashing melakukan semuanya.

Pada dasarnya, hashing didefinisikan oleh dua karakteristik berbeda - **tidak dapat diubah** dan **keunikan** . Ketidakterbalikan menunjukkan fakta bahwa setelah Anda melakukan hash, tidak ada jalan kembali. Tidak seperti enkripsi dan pengkodean, Anda tidak

dapat dengan mudah menghapus hash pesan / data. Unik, karena tidak ada dua nilai hash yang sama untuk dua bagian data yang berbeda. Jika dua hash ditemukan sama untuk dua bagian data yang berbeda, itu disebut 'tabrakan hash' dan algoritme itu menjadi tidak berguna.

(Catatan: Kami telah menggunakan algoritma hashing **joaat di** sini karena pendek dan mudah dimengerti. Algoritma modern jauh lebih kompleks dan panjang.)

Fungsi Hashing: Inti dari Algoritma Hashing

"Di belakang setiap pria sukses, ada wanita hebat." - Groucho Marx

“Di balik setiap algoritme hash yang sukses, ada fungsi hash yang hebat.” - Kami baru saja mengarangnya.

Mari kita kesampingkan lelucon itu sejenak dan berkonsentrasi pada inti masalahnya. Fungsi hash adalah fungsi matematika yang mengubah nilai input menjadi nilai numerik terkompresi - nilai hash atau hash. Pada dasarnya, ini adalah unit pemrosesan yang mengambil data dengan panjang acak dan memberi Anda output dengan panjang tetap - nilai hash.

Proses Hashing pada Gambar 6.4 dimana hash adalah fungsi apa pun yang dapat digunakan untuk memetakan data dengan ukuran arbitrer ke nilai ukuran tetap. Nilai yang dikembalikan oleh fungsi hash disebut nilai hash, kode hash, intisari, atau sekadar hash. Nilai biasanya digunakan untuk mengindeks tabel ukuran tetap yang disebut tabel hash.

Hashing dan enkripsi berbeda tetapi juga memiliki beberapa kesamaan. Keduanya ideal dalam menangani data, pesan, dan informasi dalam sistem komputasi. Keduanya mengubah atau mengubah data menjadi format yang berbeda. Sementara enkripsi dapat dibalik, hashing tidak

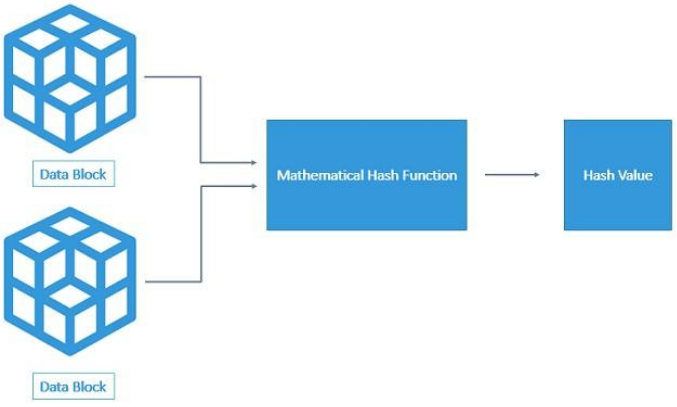
Gambar 6.4. Proses Hashing
Sumber: https://medium.com/nybles/hashing-algorithms

Panjang keluaran atau hash tergantung pada algoritma hashing. Secara umum, algoritme atau fungsi hashing paling populer memiliki panjang hash mulai dari 160 hingga 512 bit.

Sekarang, mari beralih ke bagian yang Anda tunggu-tunggu.

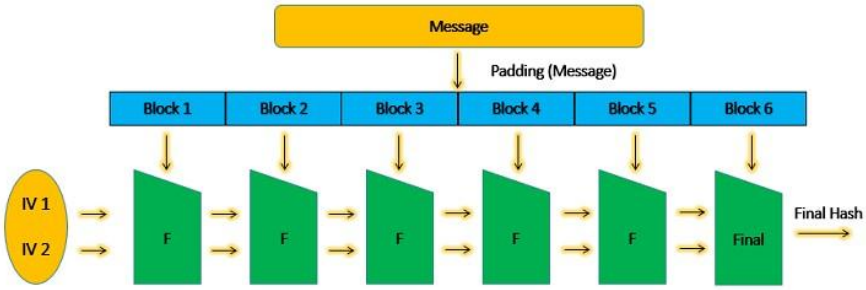
Apa Itu Algoritma Hashing? Bagaimana cara kerjanya?

Seperti yang telah kita diskusikan, fungsi hash terletak di jantung algoritme hashing. Namun, untuk mendapatkan nilai hash dari panjang yang telah ditentukan sebelumnya, Anda harus terlebih dahulu membagi data masukan menjadi blok berukuran tetap. Ini karena fungsi hash menerima data dengan panjang tetap. Blok ini disebut 'blok data'. Ini ditunjukkan pada gambar 6.5 di bawah.



Gambar 6.5. Struktur Hash
Sumber : https://cheapsslsecurity.com/blog/decoded-examples-of-how-hashing-algorithms-work/

Ukuran blok data berbeda dari satu algoritma ke algoritma lainnya. Namun untuk algoritme tertentu, tetap sama. Misalnya, SHA-1 menerima pesan / data dalam blok 512-bit saja. Jadi, jika pesan persis dengan panjang 512-bit, fungsi hash hanya berjalan sekali (80 putaran untuk SHA-1). Demikian pula, jika pesannya 1024-bit, itu dibagi menjadi dua blok 512-bit dan fungsi hash dijalankan dua kali. Namun, 99 persen dari waktu tersebut, pesan tidak akan berada dalam kelipatan 512-bit. Untuk kasus seperti itu (hampir semua kasus), teknik yang disebut **padding** digunakan. Dengan menggunakan teknik padding, seluruh pesan dibagi menjadi blok data berukuran tetap. Fungsi hash diulang sebanyak jumlah blok data. Beginilah caranya:



Gambar 6.6. Fungsi Hash
Sumber: https://blog.shiftasia.com/differences-between-encode-encrypt-hash/

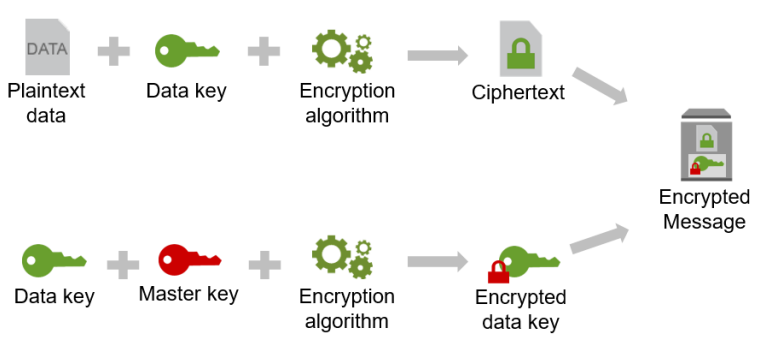
Seperti yang ditunjukkan Gambar 6.6 di atas, blok diproses satu per satu. Output dari blok data pertama diumpankan sebagai input bersama dengan blok data kedua. Akibatnya, keluaran kedua diumpankan bersama dengan blok ketiga dan seterusnya. Jadi, kami membuat hasil akhir nilai gabungan dari semua blok. Jika Anda mengubah satu bit di mana pun dalam pesan, seluruh nilai hash berubah. Ini disebut 'efek longsoran salju'.

Algoritma Hashing Populer

Algoritma Message Digest (MD)
Secure Hash Algorithm (SHA)
RACE Integrity Primitives Evaluation Message Digest (RIPEMD)
(Whirpool) Pusaran air
RSA

6.5. Key Management

Manajemen kunci mengacu pada manajemen kunci kriptografi dalam sistem kriptografi. Ini termasuk berurusan dengan pembuatan, pertukaran, penyimpanan, penggunaan, penghancuran crypto (penghancuran) dan penggantian kunci. Ini termasuk desain protokol kriptografi, server kunci , prosedur pengguna, dan protokol terkait lainnya, hal ini dijelaskan pada Gambar 6.7. Manajemen kunci menyangkut kunci di tingkat pengguna, baik di antara pengguna atau sistem. Ini berbeda dengan penjadwalan kunci, yang biasanya mengacu pada penanganan internal kunci dalam pengoperasian sandi.



Gambar 6.7. Cara Kerja Key Management
Sumber: https://info.townsendsecurity.com/definitive-guide-to-encryption-key-management-fundamentals

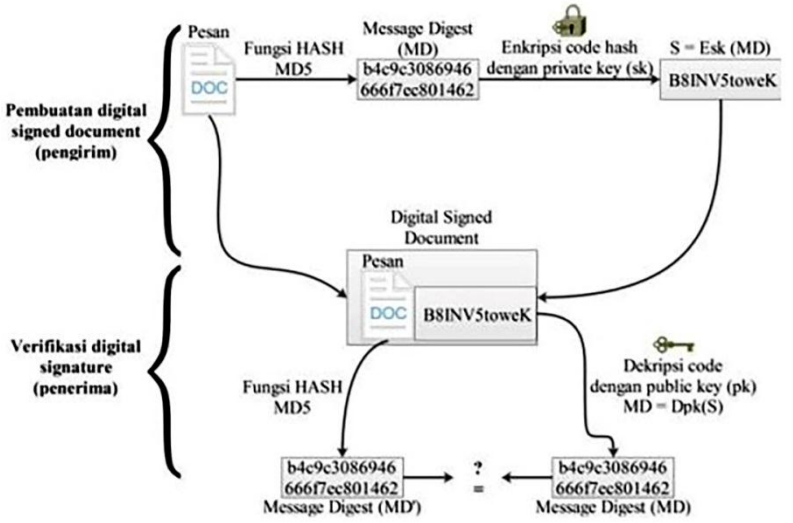
Manajemen kunci yang sukses sangat penting untuk keamanan sistem kriptografi. Ini adalah sisi kriptografi yang lebih menantang dalam arti yang melibatkan aspek rekayasa sosial seperti kebijakan sistem, pelatihan pengguna, interaksi organisasi dan departemen,

dan koordinasi antara semua elemen ini, berbeda dengan praktik matematika murni yang dapat diotomatiskan.

6.6. Digital Signature

Digital Signature adalah skema matematis yang digunakan untuk membuktikan keaslian pesan atau dokumen digital. Skema ini menjadi jaminan bahwa data dan informasi benar-benar berasal dari sumber yang benar. Tanda tangan digital terdiri dari deret fungsi hash yang dihasilkan dari proses algoritme fungsi hash tertentu yang kemudian disandikan (dienkripsi) dengan algoritme kriftografi kunci asimetris. Untuk memperifikasinya digunakan kunci publik dari algoritme tesebut.

Tanda tangan digital merupakan salah satu dari banyak cara untuk menjaga keamanan data digital. Tanda tangan digital dibuat dengan cara membubuhkan "sign" berupa kode-kode yang diletakkan pada ahir dokumen. Kode-kode ini dihasilkan dari proses enkripsi pesan dengan algoritma kriptografi. Dengan keberadaan tanda tangan digital ini, seorang penerima pesan dapat diyakinkan bahwa dokumen yang diterimanya benar dan asli berasal dari pengirim pesan sebenarnya dan tidak ada modifikasi dalam dokumen tersebut oleh pihak yang tidak berwenang atau penyusup.



Gambar 6.8. Proses Digital Signature

Proses Kerja

Adapun proses pemberian pada Gambar 6.8 tanda tangan digital adalah sebagai berikut :

1. Pengirim pesan mula-mula menghitung Message Digest (MD) dari pesan. MD diperoleh dengan mentransformasikan pesan M dengan fungsi hash satu arah.
2. MD dienkripsi dengan algoritma kriptografi kunci privat misalnya algoritma RSA. Hasil enkripsi inilah yang disebut dengan tanda tangan digital (S).
3. Tanda tangan digital (S) diletakkan pada pesan M.
4. Kemudian pesan M dikirim melalui saluran komunikasi, pesan M telah ditandatangai dengan S

Ketika pesan M telah sampai kepada penerima, adapun proses verifikasi untuk membuktikan keaslian pesan adalah sebagai berikut:

1. Tanda tangan digital (S) didekripsikan dengan kunci publik yang telah diberikan kepada penerima. Proses ini akan menghasilkan MD (Message Digest).
2. Penerima mengubah M menjadi MD' dengan fungsi hash satu arah yang sama dengan fungsi hash yang digunakan oleh pengirim.
3. Jika MD'=MD, maka tanda tangan digital yang diterima autentik dan berasal dari pengirim yang benar

Aspek Keamanan

Tanda tangan digital memberikan layanan keamanan bagi penggunanya baik data yang dikirim dalam jaringan maupun pada data yang tersimpan di dalam perangkat. Adapun aspek keamanan pada tanda tangan digital adalah sebagai berikut :

1. Otentikasi: Merupakan aspek dimana penerima informasi dapat memastikan keaslian pesan, yakni dengan kata lain data dan informasi benar-benar berasal dari sumber yang benar. Contohnya saat login menggunakan nama pengguna dan kata sandi tertentu, sistem akan melakukan otentikasi dengan cara sistem berusaha memastikan bahwa nama pengguna dan kata sandi.

2. Integritas: Merupakan aspek dimana keaslian pesan terjaga walaupun dikirim melalui jaringan yang rentan terhadap serangan, namun dapat dipastikan bahwa data atau informasi yang dikirim tidak diubah oleh orang yang tidak berhak.
3. Non-repudiation: Merupakan aspek yang berhubungan dengan keaslian pengirim pesan, dapat dipastikan bahwa pengirim adalah orang yang sebenarnya diharapkan mengirimkan data.[5]

Penggunaan

Penggunaan tanda tangan digital telah banyak dilakukan di era modern ini. Adapun beberapa contoh penggunaan tanda tangan digital yaitu, tanda tangan digital digunakan untuk pengamanan pada pengiriman surel dengan cara mengenkripsi dan kemudian membubuhkan tanda tangan digital pada surel yang dikirim. Hal ini bertujuan agar surel yang dikirim tidak dapat dimodifikasi oleh pihak yang tidak berkepentingan, serta penerima dapat meyakini keaslian surel karena jika surel telah dimodifikasi, maka tanda tangan digital tidak akan cocok. Selain itu, tanda tangan digital juga dimanfaatkan dalam pengamanan transaksi online serta mengidentifikasi peserta yang terlibat dalam transaksi. Hal ini penting agar pelaku transaksi terjamin keamanan datanya. Tanda tangan digital juga dapat digunakan untuk menandatangani dan memastikan keaslian dokumen seperti format dokumen Word, Excel, dan PDF. Lebih lanjut lagi, tanda tangan digital digunakan dalam perusahaan dengan sertifikat yang dapat disahkan secara hukum.[6]

Algoritme

Beberapa algoritme yang dapat digunakan untuk membangun tanda tangan digital adalah:RSA

1. DSA (Digital SIgnature Alghoritm)
2. SHA. Baik SHA1, SHA2, atau SHA3.
3. ElGamal
4. RSA kombinasi SHA
5. Schnorr signature
6. Algoritme Pointcheval–Stern signature
7. Rabin signature

6.7. Kesimpulan

Kriptografi adalah bidang yang sangat menarik karena banyaknya pekerjaan yang, oleh kebutuhan, dilakukan secara rahasia. Ironisnya, kerahasiaan bukanlah kunci kebaikan algoritma kriptografi. Terlepas dari teori matematika di balik algoritme, algoritme terbaik adalah algoritme yang terkenal dan terdokumentasi dengan baik karena juga teruji dan dipelajari dengan baik! Faktanya, waktu adalah satu-satunya ujian sejati dari kriptografi yang baik; skema kriptografi apa pun yang tetap digunakan tahun demi tahun kemungkinan besar bagus. Kekuatan kriptografi terletak pada pilihan (dan manajemen) kunci; kunci yang lebih panjang akan menahan serangan lebih baik daripada kunci yang lebih pendek.

Tugas dan Diskusi:

1. Apa tujuan enkripsi?
2. Apa saja kemajuan terbaru dalam teknologi enkripsi? Lakukan beberapa penelitian independen tentang enkripsi menggunakan sumber daya akademis atau praktisi, lalu tulis makalah dua hingga tiga halaman yang menjelaskan setidaknya dua kemajuan baru dalam teknologi enkripsi.

Referensi

Becket, B (1988). Introduction to Cryptology. Blackwell Scientific Publications. ISBN 0-632-01836-4. OCLC 16832704. Excellent coverage of many classical ciphers and cryptography concepts and of the "modern" DES and RSA systems.

Cryptography and Mathematics by Bernhard Esslinger, 200 pages, part of the free open-source package CrypTool, PDF download di www.cryptool.org Galat: URL arsip tidak dikenal (diarsipkan tanggal 20110722183013). CrypTool is the most widespread e-learning program about cryptography and cryptanalysis, open source.

In Code: A Mathematical Journey by Sarah Flannery (with David Flannery). Popular account of Sarah's award-winning project on public-key cryptography, co-written with her father.

James Gannon, Stealing Secrets, Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century, Washington, D.C., Brassey's, 2001, ISBN 1-57488-367-4.

Oded Goldreich, Foundations of Cryptography, in two volumes, Cambridge University Press, 2001 and 2004.

Alvin's Secret Code by Clifford B. Hicks (children's novel that introduces some basic cryptography and cryptanalysis).

Ibrahim A. Al-Kadi, "The Origins of Cryptology: the Arab Contributions," Cryptologia, vol. 16, no. 2 (April 1992), pp. 97–126.

Christof Paar, Jan Pelzl, Understanding Cryptography, A Textbook for Students and Practitioners. Springer, 2009. (Slides, online cryptography lectures and other information are available on the companion web site.) Very accessible introduction to practical cryptography for non-mathematicians.

Johann-Christoph Woltag, 'Coded Communications (Encryption)' in Rüdiger Wolfrum (ed) Max Planck Encyclopedia of Public International Law (Oxford University Press 2009). *"Max Planck Encyclopedia of Public International Law"., giving an overview of international law issues regarding cryptography.

Jonathan Arbib & John Dwyer, Discrete Mathematics for Cryptography, 1st Edition ISBN 978-1-907934-01-8.

Stallings, William (March 2013). Cryptography and Network Security: Principles and Practice (edisi ke-6th). Prentice Hall. ISBN 978-0133354690.

Kessler, Gary (17 November 2006). "An Overview of Cryptography". Princeton University.

"History of Cryptography". Binance Academy (dalam bahasa Inggris). Diakses tanggal 2 April 2020.

Fouché Gaines, Helen (1939). Cryptanalysis: A Study of Ciphers and Their SolutionPerlu mendaftar (gratis). New York: Dover Publications Inc. ISBN 978-0-4862-0097-2.

Kahn, David (1967). The Codebreakers - The Story of Secret Writing. ISBN 0-6848-3130-9.

Preneel, Bart, ed. (2000). Advances in Cryptology – EUROCRYPT 2000. Lecture Notes in Computer Science. ISBN 978-3-5406-7517-4.

Sinkov, Abraham (1966). Elementary Cryptanalysis: A Mathematical Approach. Mathematical Association of America. ISBN 0-8838-5622-0.

Yehuda, Lindell; Jonathan, Katz (2014). Introduction to modern cryptography. Hall/CRC. ISBN 978-1-4665-7026-9.

BAB VII.

MOBILE PRIVACY

7.1. Pendahuluan

Privasi informasi adalah hubungan antara pengumpulan dan penyebaran data , teknologi , ekspektasi publik terhadap privasi , dan masalah hukum dan politik yang mengelilinginya. Ini juga dikenal sebagai privasi data atau perlindungan data .

Privasi data itu menantang karena mencoba menggunakan data sambil melindungi preferensi privasi individu dan informasi yang dapat diidentifikasi secara pribadi. Bidang keamanan komputer , keamanan data , dan keamanan informasi semuanya merancang dan menggunakan perangkat lunak , perangkat keras , dan sumber daya manusia untuk mengatasi masalah ini..

Bahan kajian pembelajaran pada bab adalah penjelasan secara komprehensif tentang definisi **Data Privacy dan Location Privacy**.

Sub Capaian pembelajaran mata kuliah dalam dalam pertemuan ini adalah **mahasiswa diharapkan dapat Mengetahui dan memahami tentang privasi data dan lokasi**.

Indikator pencapaian dalam pertemuan ini adalah mahasiswa dapat **mendeskripsikan, mampu menjelaskan dan mempraktekkan mengenai privasi data dan lokasi.**

Penyampaian materi adalah dengan **ceramah, diskusi, dan praktek**

7.2. Data Privacy

Privasi data selalu penting. Itu sebabnya orang mengunci lemari arsip dan menyewa brankas di bank mereka. Namun karena semakin banyak data kami yang menjadi digital, dan kami membagikan lebih banyak informasi secara online, privasi data menjadi semakin penting.

Sebuah perusahaan mungkin memiliki informasi pribadi jutaan pelanggan – data yang perlu dirahasiakan sehingga identitas pelanggan tetap seaman dan terlindungi mungkin, dan reputasi perusahaan tetap tidak ternoda. (Bisakah Anda mengatakan "pelanggaran data"?) Tetapi privasi data bukan hanya urusan bisnis.

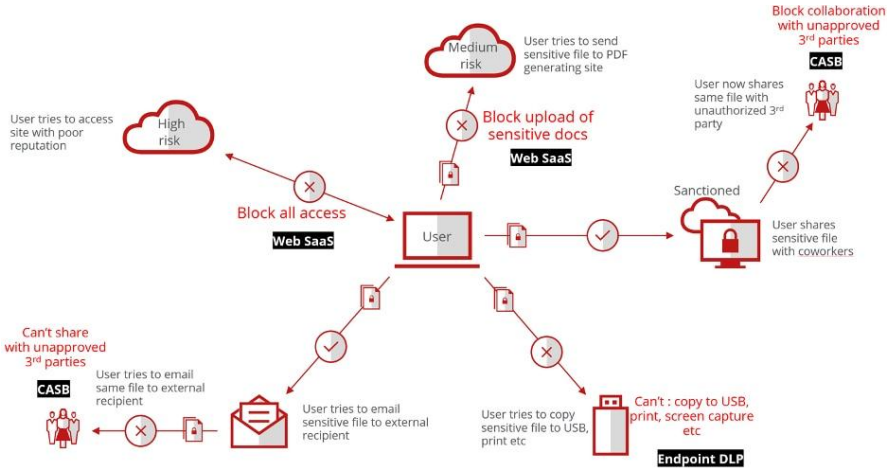
Anda, sebagai individu, memiliki banyak hal yang dipertaruhkan dalam hal privasi data. Semakin banyak Anda mengetahuinya, semakin baik Anda dalam membantu melindungi diri Anda dari sejumlah besar risiko.

Apa itu privasi data?

Privasi data berkaitan dengan bagaimana suatu informasi – atau data – harus ditangani berdasarkan kepentingan relatifnya. Misalnya, Anda mungkin tidak keberatan membagikan nama Anda dengan orang asing dalam proses memperkenalkan diri, tetapi ada informasi lain yang tidak akan Anda bagikan, setidaknya sampai Anda lebih mengenal orang itu. Namun, buka rekening bank baru, dan Anda mungkin akan diminta untuk membagikan sejumlah besar informasi pribadi, jauh di luar nama Anda.

Gambar 7.1. menjelaskan proses tersebarnya informasi di era digital, biasanya menerapkan konsep privasi data ke informasi pribadi penting, juga dikenal sebagai informasi identitas pribadi (PII) dan informasi kesehatan pribadi (PHI). Ini dapat mencakup nomor Jaminan Sosial, catatan kesehatan dan medis, data keuangan, termasuk rekening bank dan nomor kartu kredit, dan bahkan informasi dasar namun tetap sensitif, seperti nama lengkap, alamat, dan tanggal lahir. Daftar informasi pribadi bisa sangat luas, Untuk bisnis, privasi data melampaui PII karyawan dan pelanggannya. Ini juga mencakup informasi yang membantu perusahaan beroperasi, apakah itu data penelitian dan pengembangan eksklusif atau

informasi keuangan yang menunjukkan bagaimana perusahaan membelanjakan dan menginvestasikan uangnya.



Gambar 7.1. Proses Tersebarnya Data

Mengapa privasi data penting?

Ketika data yang seharusnya dirahasiakan sampai ke tangan yang salah, hal buruk bisa terjadi. Pembobolan data di lembaga pemerintah dapat, misalnya, menempatkan informasi sangat rahasia di tangan negara musuh. Pelanggaran di perusahaan dapat membuat data kepemilikan berada di tangan pesaing. Pembobolan di sekolah dapat membuat PII siswa berada di tangan penjahat yang dapat melakukan pencurian identitas. Pelanggaran di rumah sakit atau kantor dokter dapat menempatkan PHI di tangan mereka yang mungkin menyalahgunakannya.

5 tips sederhana untuk membantu melindungi data pribadi Anda

Karena privasi data adalah masalah umum, banyak organisasi pemerintah dan perusahaan menghabiskan jutaan dolar setiap tahun untuk membantu melindungi data mereka – yang dapat mencakup PII Anda – dari keterpaparan. Konsumen rata-rata mungkin tidak memiliki uang sebanyak itu untuk dibelanjakan. Tetapi ada langkah-langkah murah yang dapat Anda lakukan untuk membantu melindungi data Anda. Berikut beberapa saran:

1. Di rumah, gunakan slot surat atau pengunci kotak surat, sehingga pencuri tidak dapat mencuri surat Anda.
2. Sebelum membuang, dokumen rusak, termasuk tanda terima dan laporan bank dan kartu kredit, yang berisi informasi pribadi.
3. Pastikan untuk mengamankan jaringan Wi-Fi rumah Anda dan perangkat lain sehingga penjahat tidak bisa "menguping" aktivitas online Anda.
4. Jangan memberikan nomor Jaminan Sosial Anda secara otomatis hanya karena seseorang memintanya. Tentukan apakah mereka benar-benar membutuhkannya dan, jika demikian, tanyakan bagaimana mereka akan membantu melindunginya.
5. Gunakan kata sandi yang kuat dan unik untuk semua akun online Anda.

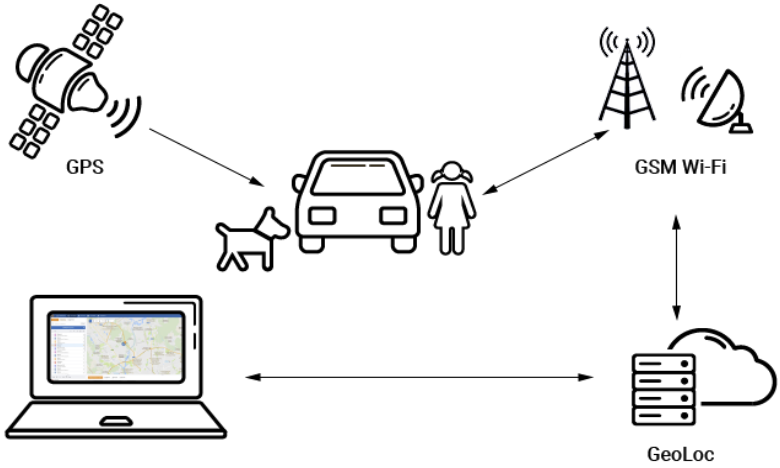
Satu rekomendasi terakhir untuk membantu Anda menjaga kerahasiaan data Anda: Nilai pengaturan privasi di akun media sosial Anda secara teratur. Jika tidak, Anda mungkin membagikan lebih dari sekadar nama Anda dengan orang yang belum pernah Anda temui – dan penjahat yang cerdas dapat menggunakan informasi itu untuk mencuri identitas Anda dan banyak lagi.

1. Data Privacy mendefinisikan siapa / pihak mana yang sah untuk mengakses data tersebut. Artinya, Data Privacy berbicara perihal hak dan kewajiban pemangku kepentingan dari data pribadi (data owner, data controller, data processor). Sedangkan, Data Protection memiliki fokus pada mekanisme perlindungan terhadap data atau melindungi data dari akses yang tidak sah, yang artinya Data Protection berbicara perihal cara kita melindungi data pribadi.
2. Data Privacy lebih ke urusan hukum/legal dan proses, sedangkan Data Protection lebih ke mengontrol keamanan data atau technical control. Dalam konteks ini, Data Privacy bisa dalam bentuk proses tata kelola dan kepatuhan terhadap aspek kontraktual dan regulasi yang berlaku, dan untuk technical control bisa dalam bentuk implementasi teknologi (misalnya

implementasi solusi encryption, data loss/leakage prevention, tokenization, anonymization, dan lain-lain).

3. Data Privacy adalah kontrol dari pemilik data atas data mana yang dapat dibagikan ke siapa/pihak mana, sedangkan Data Protection adalah kontrol yang dipegang organisasi/perusahaan atas perlindungan data pribadi.
4. Data Privacy berfokus pada data dari risiko penjualan atau penyebaran data yang tidak sah, sedangkan Data Protection berfokus pada bagaimana melindungi data dari risiko peretasan.

7.3. Location Privacy



Gambar 7.2. Proses Terjadinya Location Privacy Reveal

Karena kemampuan pelacakan lokasi perangkat seluler semakin maju (layanan berbasis lokasi), masalah yang terkait dengan privasi pengguna muncul. Data lokasi adalah salah satu data paling sensitif yang saat ini dikumpulkan seperti dijelaskan pada Gambar 7.2. Daftar informasi profesional dan pribadi yang berpotensi sensitif yang dapat disimpulkan tentang seseorang yang hanya mengetahui jejak mobilitasnya diterbitkan baru-baru ini oleh Electronic Frontier Foundation. Ini termasuk pergerakan tenaga

penjualan pesaing, kehadiran di gereja tertentu atau kehadiran individu di motel, atau di klinik aborsi. Sebuah studi MIT baru-baru ini oleh de Montjoye et al. menunjukkan bahwa empat titik ruang-temporal, perkiraan tempat dan waktu, cukup untuk mengidentifikasi 95% dari 1,5 juta orang secara unik dalam database mobilitas. Studi lebih lanjut menunjukkan bahwa kendala ini berlaku bahkan ketika resolusi set data rendah. Oleh karena itu, bahkan kumpulan data yang kasar atau kabur memberikan sedikit anonimitas.

7.4. Kesimpulan

Ancaman terhadap privasi dapat, tentu saja, berasal dari luar kerangka kerja atau kebijakan resmi, dan hanya berasal dari upaya peretas dan penjahat dunia maya untuk mencuri data, memantau target mereka, atau mencuri identitas. Dalam semua kasus, ada tindakan yang dapat Anda lakukan untuk menjaga privasi Anda.

- Baca tulisan kecilnya. Ini berlaku untuk formulir persetujuan untuk kebijakan BYOD atau MDM, ketentuan pendaftaran untuk layanan web dan akun, dan Persyaratan & Ketentuan yang terkait dengan perangkat lunak seluler Anda. Pindahkan dokumen-dokumen ini ke layar yang lebih besar jika memungkinkan, karena ini akan membuatnya tidak terlalu menyakitkan untuk dibaca.
- Periksa izin aplikasi itu . Permintaan akses yang tidak wajar ke lokasi Anda, kontak, kamera, media penyimpanan atau data pribadi (yaitu, jelas tidak terkait dengan fungsi aplikasi yang dinyatakan) harus mendiskualifikasi perangkat lunak tersebut dari pengunduhan atau penginstalan.
- Ambil tindakan fisik untuk melindungi perangkat Anda. Kata sandi , layar kunci, dan kemampuan menghapus jarak jauh (jika hilang atau dicuri) ikut bermain di sini.
- Nonaktifkan login dan check-in otomatis. Ini akan mencakup fitur "IsiOtomatis" untuk formulir online, dan izin lokasi geografis otomatis di situs tertentu.
- Gunakan informasi yang ada di luar sana. Pendukung hak konsumen, grup privasi , dan sumber daya online perwakilan

lokal Anda dapat memberikan informasi berharga tentang hak Anda, dan langkah-langkah yang ditetapkan untuk menegakkannya.

Tugas dan Diskusi:

1. Apa saja yang merupakan ancaman terhadap Keamanan Data dan Informasi
2. Jelaskan Jenis-jenis ancaman terhadap Keamanan Data dan Informasi

Referensi:

Varshavsky, Alex; Chen, Mikey; Froehlich, Jon; Haehnel, Dirk; Hightower, Jeffrey; Lamarca, Anthony; Potter, Fred; Sohn, Timothy; Tang, Karen; Smith, Ian. "Are GSM phones THE solution for localization?" In 7th IEEE Workshop on Mobile Computing Systems and Applications (HotMobile). IEEE Computer Society: 20–28.

.

BAB VIII.

MOBILE MALWARE

7.1. Pendahuluan

Mobile Malware, dalah perangkat lunak berbahaya yang dirancang khusus untuk menargetkan perangkat seluler, seperti ponsel cerdas dan tablet, dengan tujuan memperoleh akses ke data pribadi.[1]

Bahan kajian pembelajaran pada bab adalah penjelasan secara komprehensif tentang definisi **Mobile Malware.**

Sub Capaian pembelajaran mata kuliah dalam dalam pertemuan ini adalah mahasiswa diharapkan dapat **Mengetahui dan memahami tentang Mobile Malware**.

Indikator pencapaian dalam pertemuan ini adalah mahasiswa dapat mendeskripsikan, **mampu menjelaskan dan mempraktekkan mengenai penanganan dan pencegahan Mobile Malware..**

Penyampaian materi adalah dengan **ceramah, diskusi, dan praktek**

Meskipun malware seluler saat ini tidak menyebar seperti malware yang menyerang workstation tradisional, ini merupakan ancaman yang berkembang karena banyak perusahaan sekarang mengizinkan karyawan untuk mengakses jaringan perusahaan menggunakan perangkat pribadi mereka (*Bring Your Own Device*), berpotensi membawa ancaman yang tidak diketahui ke lingkungan.

[1] Mobile malware attacks and defense. Dunham, Ken. Burlington, MA: Syngress/Elsevier. 2009. ISBN 9780080949192. OCLC 318353699

Gambar 8.1. Jenis Malware

7.2. Taksonomi

Banyak jenis program jahat yang umum diketahui memengaruhi perangkat seluler:

- **Expander :** Ekspander menargetkan pengukur seluler untuk tagihan telepon tambahan dan keuntungan
- **Worm :** Tujuan utama dari jenis malware yang berdiri sendiri ini adalah untuk mereproduksi dirinya sendiri tanpa henti dan menyebar ke perangkat lain. Cacing juga mungkin mengandung petunjuk yang berbahaya dan menyesatkan. Worm seluler dapat ditularkan melalui pesan teks SMS atau MMS dan biasanya tidak memerlukan interaksi pengguna untuk eksekusi.
- **Trojan :** Tidak seperti worm, Trojan horse selalu membutuhkan interaksi pengguna untuk diaktifkan. Jenis virus ini biasanya dimasukkan ke dalam file atau aplikasi yangtampaknya menarik dan tidak berbahayayang diunduh ke perangkat dan dijalankan oleh pengguna. Setelah diaktifkan, malware dapat menyebabkan kerusakan serius dengan menginfeksi dan menonaktifkan aplikasi lainatau telepon itu sendiri, membuatnya lumpuh setelah jangka waktu tertentu atau sejumlah operasi. Data usurpation (spyware) disinkronkan dengan kalender, akun email, catatan, dan sumber informasi lainnya sebelum dikirim ke server jauh .

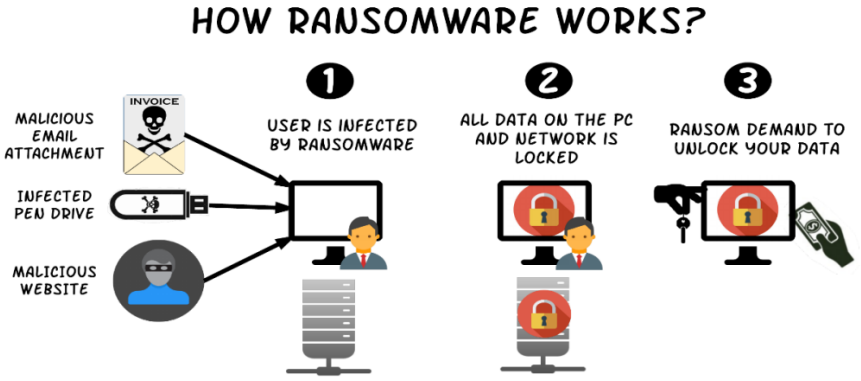
- **Spyware :** Malware ini merupakan ancaman bagi perangkat seluler dengan mengumpulkan, menggunakan, dan menyebarkan informasi pribadi atau sensitif pengguna tanpa persetujuan atau sepengetahuan pengguna. Ini sebagian besar diklasifikasikan ke dalam empat kategori: monitor sistem, trojan, adware, dan cookie pelacakan .
- **Backdoor :** Metode rahasia untuk melewati batasan keamanan untuk mendapatkan akses tidak sah ke sistem komputer. Dengan kata sederhana, pintu belakang adalah bagian kode yang memungkinkan orang lain masuk dan keluar dari sistem tanpa terdeteksi. [12]
- **Penetes :** Malware yang dirancang untuk menginstal program lain di perangkat, tanpa sepengetahuan pengguna. Ini dapat mencakup program berbahaya lain atau aplikasi jinak yang ingin disebarkan oleh penyerang (sering kali untuk keuntungan finansial dalamkampanye malvertising).

7.3. Jenis Malware Seluler

Penjahat dunia maya menggunakan berbagai taktik untuk menginfeksi perangkat seluler. Jika Anda berfokus pada peningkatan perlindungan perangkat lunak perusak seluler, penting untuk memahami berbagai jenis ancaman perangkat lunak perusak seluler. Berikut beberapa jenis yang paling umum:

- **Remote Access Tools (RATs)** menawarkan akses ekstensif ke data dari perangkat korban yang terinfeksi dan sering digunakan untuk pengumpulan intelijen. RAT biasanya dapat mengakses informasi seperti aplikasi yang diinstal, riwayat panggilan, buku alamat, riwayat penelusuran web, dan data sms. RAT juga dapat digunakan untuk mengirim pesan SMS, mengaktifkan kamera perangkat, dan mencatat data GPS
- **Bank trojans** sering kali disamarkan sebagai aplikasi yang sah dan berupaya membahayakan pengguna yang menjalankan bisnis perbankan - termasuk transfer uang dan pembayaran tagihan - dari perangkat seluler mereka. Jenis trojan ini bertujuan untuk mencuri login finansial dan detail kata sandi.

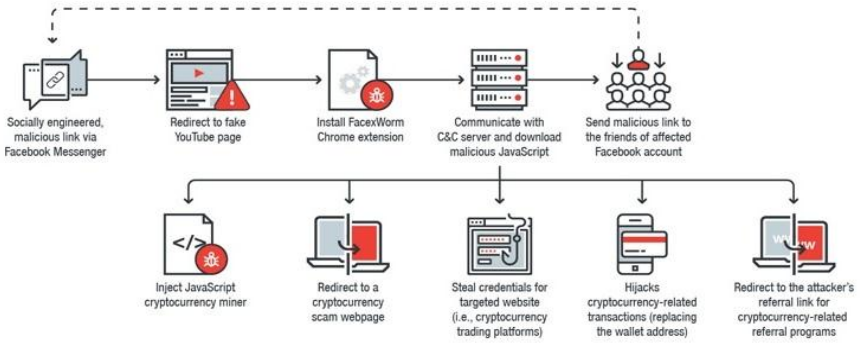
- **Ransomware** adalah jenis malware yang digunakan untuk mengunci pengguna dari perangkat mereka dan meminta pembayaran "tebusan" - biasanya dalam Bitcoin yang tidak dapat dilacak. Setelah korban membayar tebusan, kode akses disediakan untuk memungkinkan mereka membuka kunci perangkat seluler mereka.



Gambar 8.2. Cara Kerja Ransomware
Sumber: https://medium.com/@rahulsharma0856/ransomware-how-it-works-a-growing-cyber-attack-d976aee62944

Cryptomining Malware memungkinkan penyerang untuk secara diam-diam melakukan perhitungan pada perangkat korban - memungkinkan mereka untuk menghasilkan cryptocurrency. Cryptomining sering dilakukan melalui kode Trojan yang disembunyikan di aplikasi yang tampak sah[1].

[1] Suarez-Tangil, Guillermo; Juan E. Tapiador; Pedro Peris-Lopez; Arturo Ribagorda (2014). "Evolution, Detection and Analysis of Malware in Smart Devices" (PDF). IEEE Communications Surveys & Tutorials. 16 (2): 961–987. doi:10.1109/SURV.2013.101613.00077. Archived from the original (PDF) on 2017-10-31. Retrieved 2013-11-11



Gambar 8.3. Proses Cryptomining Malware
Sumber: https://www.techspot.com/news/72445-cryptocurrency-mining-malware-spread-through-facebook-messenger.html

Advertising Click Fraud dalah jenis malware yang memungkinkan penyerang membajak perangkat untuk menghasilkan pendapatan melalui klik iklan palsu.

CARA MELINDUNGI PERANGKAT

1. instal aplikasi hanya dari sumber tepercaya
    a. Sebelum mengunduh aplikasi, teliti aplikasi dan penerbitnya. Periksa ulasan dan peringkat pengguna lain jika tersedia.
    b. Berhati-hatilah dengan tautan yang Anda terima dalam email dan pesan teks yang mungkin menipu Anda untuk memasang aplikasi dari pihak ketiga atau sumber yang tidak dikenal.
    c. Selalu baca dengan cermat izin aplikasi sebelumnya.

2. Jangan mengklik tautan atau lampiran di email atau pesan teks yang tidak diminta
    a. Hapus mereka segera setelah Anda menerimanya.

b. Periksa ulang URL yang dipersingkat dan kode QR, mereka dapat mengarah ke situs web berbahaya atau langsung mengunduh malware ke perangkat Anda.

3. Keluar dari situs setelah Anda melakukan pembayaran
    a. Jangan pernah menyimpan nama pengguna dan sandi di browser atau aplikasi seluler Anda. Setelah transaksi selesai, logout dari situs, bukan hanya menutup browser.
    b. Jangan bank atau berbelanja online menggunakan koneksi Wi-Fi publik.
    c. Periksa ulang URL situs - Pastikan alamat web sudah benar sebelum masuk atau mengirim informasi sensitif. Pertimbangkan untuk mengunduh aplikasi resmi bank Anda.

4. Selalu perbarui sistem operasi dan aplikasi Anda
    a. Unduh pembaruan perangkat lunak untuk sistem operasi perangkat seluler Anda segera setelah Anda diminta.

5. Matikan Wi-Fi, layanan lokasi dan Bluetooth jika tidak digunakan
    a. Penjahat dunia maya dapat mengakses informasi Anda jika koneksi tidak aman.
    b. Jangan izinkan aplikasi menggunakan layanan lokasi Anda kecuali jika diperlukan.
    c. Pastikan Bluetooth Anda dimatikan sepenuhnya dan tidak hanya pada mode tak terlihat.

6. Hindari memberikan informasi pribadi
    a. Jangan pernah mengirimkan informasi pribadi Anda sebagai tanggapan atas pesan teks atau email yang mengaku dari bank Anda atau bisnis sah lainnya.
    b. Tinjau laporan seluler Anda secara teratur untuk memeriksa biaya yang mencurigakan.

7. Jangan melakukan jailbreak pada perangkat Anda
    a. Jailbreak dapat melemahkan keamanannya secara signifikan, membuka lubang keamanan yang mungkin belum terlihat.

8. Cadangkan data Anda
    a. Konsultasikan opsinya tergantung pada sistem operasi perangkat Anda. Dengan membuat cadangan untuk ponsel cerdas atau tablet Anda, Anda dapat dengan mudah memulihkan data pribadi Anda jika perangkat hilang, dicuri, atau rusak.

9. Pasang aplikasi keamanan seluler
    a. Jika tersedia, gunakan solusi keamanan seluler yang mendeteksi dan mencegah malware, spyware, dan aplikasi berbahaya, di samping fitur privasi dan anti-pencurian lainnya.

7.4. Kesimpulan

Pertama-tama, ini karena pertumbuhan yang stabil dalam jumlah Malware yang menargetkan perangkat seluler. Kedua, karena pengguna jahat pindah ke Android sebagai platform target utama mereka.

Tugas dan Diskusi:

1. Bisakah Malware memengaruhi kerja perangkat seluler?
2. Apa penyebab Mobile Malware
3. Bagaimana kerja dari Mobile Malware

Referensi:

Mobile malware attacks and defense. Dunham, Ken. Burlington, MA: Syngress/Elsevier.
2009. ISBN 9780080949192. OCLC 318353699.

Preston Gralla (2005). *PC Pest Control: Protect Your Computers from Malicious Internet Invaders*. *"O'Reilly Media, Inc.". p.* 237. ISBN 978-0-596-00926-7.

"Mobile Phones Swamped by E-Mail Virus". ecommercetimes.com. 7 June 2000.

Malware Goes Mobile, Mikko Hyppönen, Scientific American, November 2006, pp. 70–77.

Richard Hantula (2009). How Do Cell Phones Work?. Infobase Publishing. p. 27. ISBN 978-1-4381-2805-4.

Suarez-Tangil, Guillermo; Juan E. Tapiador; Pedro Peris-Lopez; Arturo Ribagorda (2014). "Evolution, Detection and Analysis of Malware in Smart Devices" (PDF). IEEE Communications Surveys & Tutorials. **16** (2): 961–987. doi:10.1109/SURV.2013.101613.00077. Archived from the original (PDF) on 2017-10-31. Retrieved 2013-11-11.

"How to Remove an Android Virus". Latest Gadget. 2019-03-24. Retrieved 2019-07-15.

"What Is A Backdoor and How to Protect Against It | Safety Detective". Safety Detective. Retrieved 2018-11-22.

Mobile virus hack Google Play user on Brazil

Samuel Gibbs. "HummingBad malware infects 10m Android devices". Retrieved 2016-07-06.

BAB IX.

MOBILE SPYWARE

9.1. Pendahuluan

Spyware menjelaskan perangkat lunak dengan perilaku berbahaya yang bertujuan untuk mengumpulkan informasi tentang seseorang atau organisasi dan mengirimkan informasi tersebut ke entitas lain dengan cara yang merugikan pengguna; misalnya dengan melanggar privasi mereka atau membahayakan keamanan perangkat mereka. Perilaku ini mungkin ada di malware dan juga di perangkat lunak yang sah. Situs web juga dapat terlibat dalam perilaku spyware seperti pelacakan web . Perangkat keras mungkin juga terpengaruh. Spyware sering kali dikaitkan dengan periklanan dan melibatkan banyak masalah yang sama . Karena perilaku ini sangat umum, dan dapat memiliki kegunaan yang tidak berbahaya, memberikan definisi yang tepat tentang spyware adalah tugas yang sulit

Bahan kajian pembelajaran pada bab adalah penjelasan secara komprehensif tentang definisi **Mobile Spyware.**

Sub Capaian pembelajaran mata kuliah dalam dalam pertemuan ini adalah mahasiswa diharapkan dapat **Mengetahui dan memahami tentang Mobile Sspyware..**

Indikator pencapaian dalam pertemuan ini adalah mahasiswa dapat mendeskripsikan, **mampu menjelaskan dan mempraktekkan mengenai penanganan dan pencegahan Mobile Spyware.**

Penyampaian materi adalah dengan **ceramah, diskusi, dan praktek**

9.2. Apa Itu Spyware?

Spyware berasal dari kata spy dan ware. Dimana spy berarti mata mata dan ware barang atau perangkat. Adapun spyware masuk ke dalam perangkat jahat atau malware yang merugikan orang lain. Jadi Spyware adalah jenis malware yang menginfeksi komputer atau perangkat mobile dan mengumpulkan informasi tentang penggunanya[1].

Informasi tersebut seperti situs web yang dikunjungi, hal hal yang diunduh, nama pengguna dan kata sandi, informasi pembayaran, dan email Anda mengirim dan menerima atau dengan kata lain segala sesuatu yang dilakukan diperangkat tersebut.

Bahkan yang sangat mengejutkan anda mungkin sebagai pengguna komputer atau smartphone secara tidak sengaja mengizinkan spyware untuk menginstal sendiri ketika menyetujui syarat dan ketentuan program yang tampaknya sah tanpa membaca catatan dari developer. Sangat licik bukan?

Apa pun cara spyware menginfeksi di komputer anda, metode operasinya adalah berjalan diam diam secara backgroud atau demon sehingga tidak terdeteksi. Selain itu aplikasi atau tool spyware tidak memberikan fitur uninstal yang mudah sehingga diperlukan aplikasi pihak ketiga untuk uninstal nya.

9.3. Cara Kerja Spyware

Gambar 9.1 Siklus Kerja Spyware

[1] Wienbar, Sharon. "The Spyware Inferno". News.com. August 13, 2004

Penjelasan Silus Kerja Spyware pada Gambar 9.1 diatas:

1. Pelanggan menyetujui persyaratan dan menginstal Mobile Spy ke telepon yang mereka miliki dan memiliki persetujuan yang tepat untuk memantau. Program konfigurasi pelanggan.
2. Anak atau karyawan melakukan aktivitas pesan SMS, penelusuran URL, dan panggilan. Mobile Spy mencatat aktivitas dan memasukkan log tersebut ke akun Mobile Spy milik pelanggan.
3. Pelanggan masuk ke akun online mereka dari browser web mana pun tempat mereka dapat melihat semua aktivitas yang dicatat hampir secara real time.

9.4. Bagaimana Bisa Terinfeksi Spyware

Spyware dapat menginfeksi sistem komputer dengan cara yang sama seperti bentuk malware lainnya. Berikut adalah beberapa teknik utama spyware untuk menginfeksi komputer atau perangkat mobile. Celah keamanan yang bisa dimanfaatkan untuk menanamkan back door dan eksploitasi dapat disalahgunakan untuk mendapatkan akses yang tidak sah. Celah keamanan pada perangkat lunak juga dikenal sebagai bug.

Bug.

Kesalahan dalam develop aplikasi terjadi dan terdapat bug yang bisa digunakan sebagai jalan masuk ke dalam aplikasi yang digunakan pengguna. Setelah masuk spyware akan menanamkan backdoor untuk akses cepat ke dalam sistem. Namun hacker lebih sering untuk menggunakan exploit untuk masuk ke dalam sistem kemudian memasang backdoor.

Phishing Dan Spoofing.

Kedua ancaman ini sering digunakan bersama sama. **Phishing** terjadi setiap kali hacker mencoba membuat target melakukan semacam tindakan seperti meng klik tautan ke situs web yang sarat dengan malware, membuka lampiran email yang terinfeksi atau mail spam kemudian diminta untuk login menggunakan username dan password. **Spoofing** mengacu pada tindakan menyamarkan email

dan website phishing sehingga tampaknya berasal dari dan oleh individu dan organisasi yang bisa dipercaya padahal bukan. Untuk mengetahui phishing dan tekniknya bisa membaca artikel teknik hacking phishing ini ya.

Aplikasi Pengguna.

Pencipta spyware sering menyajikan aplikasi spyware sebagai alat yang bermanfaat oleh pengguna atau target sehingga pengguna tergoda untuk mengunduh. Aplikasi seperti akselerator download Internet, pengelola unduhan baru, pembersih hard disk drive, atau layanan pencarian web alternatif. Waspadalah terhadap umpan jenis aplikasi ini. Karena memasang aplikasi tersebut dapat mengakibatkan infeksi spyware yang tidak disengaja. Dan bahkan jika telah diuninstal spywre masih ada di dalam sistem dan terus menginfeksi.

Freeware.

Siapa yang tidak suka perangkat lunak gratis freeware? Padahal di dalam nya bisa saja terdapat program jahat yang menyembunyikan add on, ekstensi, atau plugin berbahaya. Bundleware atau freeware mungkin terlihat seperti aplikasi yang diperlukan, tetapi sesungguhnya mereka adalah spyware yang sangat berbahaya. Dan lebih parahnya anda setuju untuk memasang spyware tersebut karena asal klik tanpa membaca informasi petuntuk penginstalan terlebih dahulu.

Trojans.

Secara umum, malware bisa bertindak sebagai Trojan. Karena sebagian besar Trojan saat ini digunakan untuk mengirimkan bentuk malware lain, seperti cryptojackers, spyware, ransomware, virus dan lain lain.

9.5. Jenis Spyware

Berikut ini adalah jenis spyware berdasarkan fungsionalitasnya;

#1. Spyware Password.

Dalam sebagian besar kasus, fungsionalitas ancaman spyware tergantung pada niat penulisnya. Misalnya, beberapa fungsi khas yang dirancang ke dalam spyware seperti spyware untuk mencuri kata sandi, adalah aplikasi yang dirancang untuk mengambil kata sandi dari komputer atau perangkat smartphone yang terinfeksi.

Jenis kata sandi yang dikumpulkan dapat mencakup identitas yang tersimpan dari browser web, login sistem, dan bermacam macam kata sandi penting lainnya. Kata sandi ini dapat disimpan di lokasi yang dipilih penyerang pada mesin yang terinfeksi atau dapat dikirim ke server jarak jauh untuk pengambilan.

#2. Spyware Perbankan.

Spyware atau Trojans Perbankan misalkan Emotet adalah aplikasi yang dirancang untuk memanen kredensial dari lembaga keuangan. Mereka mengambil keuntungan dari kerentanan dalam keamanan browser untuk memodifikasi halaman web, memodifikasi konten transaksi, atau menyisipkan transaksi tambahan, semuanya dengan cara rahasia sepenuhnya tidak terlihat oleh aplikasi web pengguna.

Trojans Perbankan dapat menargetkan berbagai lembaga keuangan, termasuk bank, broker, portal keuangan online, atau dompet digital. Mereka mungkin juga mengirimkan informasi yang dikumpulkan ke server untuk pengambilan.

Infostealer adalah aplikasi yang memindai komputer yang terinfeksi dan mencari berbagai informasi, termasuk nama pengguna, kata sandi, alamat email, riwayat browser, file log, informasi sistem, dokumen, spreadsheet, atau file media lainnya.

Seperti Trojans perbankan, pengiklan dapat mengeksploitasi kerentanan keamanan browser untuk mengumpulkan informasi pribadi di layanan dan forum online, kemudian mengirimkan informasi ke server atau menyimpannya di komputer anda secara lokal untuk diambil.

#3. Keylogger.

Keylogger juga disebut monitor sistem, adalah aplikasi yang dirancang untuk merekam aktivitas komputer, termasuk penekanan tombol, website yang dikunjungi, riwayat penelusuran, diskusi email, dialog ruang obrolan, dan kredensial sistem. Mereka biasanya mengumpulkan rekaman layar dari jendela saat ini pada interval yang dijadwalkan. Untuk mengetahui keylogger dan tekniknya bisa membaca artikel teknik hacking keylogger ini ya.

Keylogger juga dapat mengumpulkan fungsionalitas, memungkinkan untuk menangkap dan mengirim gambar dan audio dan video secara diam diam dari perangkat yang terhubung. Mereka bahkan mungkin mengizinkan penyerang untuk mengumpulkan dokumen yang dicetak pada printer yang terhubung, yang kemudian dapat dikirim ke server atau disimpan secara lokal di komputer target.

Serangan spyware pada smartphone umumnya terjadi dalam tiga cara, yaitu;

Free WIFI.

Free wi fi atau wi fi gratis yang berada di umum seperti bandara dan kafe merupakan jaringan yang tidak aman. Jika anda masuk ke jaringan yang tidak aman, orang jahat dapat melihat semua yang Anda lakukan saat terhubung. Perhatikan pesan peringatan yang mungkin diberikan ke perangkat Anda, terutama jika itu menunjukkan bahwa identitas server tidak dapat diverifikasi. Maka lindungi diri dengan menghindari koneksi yang tidak aman tersebut.

Kelemahan Sistem Operasi.

Celah keamanan pada sistem operasi dapat membuat penyerang menginfeksi perangkat mobile. Vendor smartphone sering merilis pembaruan OS untuk melindungi pengguna, itulah sebabnya pengguna harus menginstal pembaruan segera setelah tersedia.

Malware.
Aplikasi yang berbahaya seperti malware bersembunyi di aplikasi yang tampaknya sah, terutama ketika mereka diunduh dari situs web seperti website warez. Di sini penting untuk melihat pesan peringatan saat memasang aplikasi, terutama jika mereka meminta izin untuk mengakses email Anda atau informasi pribadi lainnya. Intinya agar tetap aman adalah menggunakan sumber tepercaya untuk aplikasi mobile dan menghindari aplikasi pihak ketiga.

9.6. Siapa Target Spyware

Tidak seperti beberapa jenis malware lainnya, pembuat spyware tidak benar benar menargetkan kelompok atau orang tertentu. Sebaliknya, sebagian besar serangan spyware menyebarkan aplikasi secara luas untuk mengumpulkan sebanyak mungkin calon korban, ini dijelaskan pada Gambar 9.2. Dan itu membuat semua orang menjadi target spyware, karena informasi sekecil apa pun mungkin akan bisa dijual.

Misalnya, spammer akan membeli alamat email dan kata sandi untuk mendukung spam jahat atau bentuk kejahatan lainnya. Serangan spyware pada informasi keuangan dapat menguras rekening bank atau dapat mendukung bentuk penipuan lainnya menggunakan rekening bank yang sah.

Informasi yang diperoleh melalui dokumen, gambar, video, atau barang digital curian lainnya bahkan dapat digunakan untuk tujuan pemerasan. Jadi, pada akhirnya tidak ada yang kebal dari serangan spyware, dan penyerang biasanya tidak peduli tentang siapa yang mereka terinfeksi, karena semua hal bisa mengungkan.

9.7. Bagaimana Cara Menghilangkan Spyware

Jika anda curiga atau ingin mengetahui apakah sistem komputer atau smartphone telah diinfeksi spyware, hal berikut ini yang bisa dilakukan, yaitu;

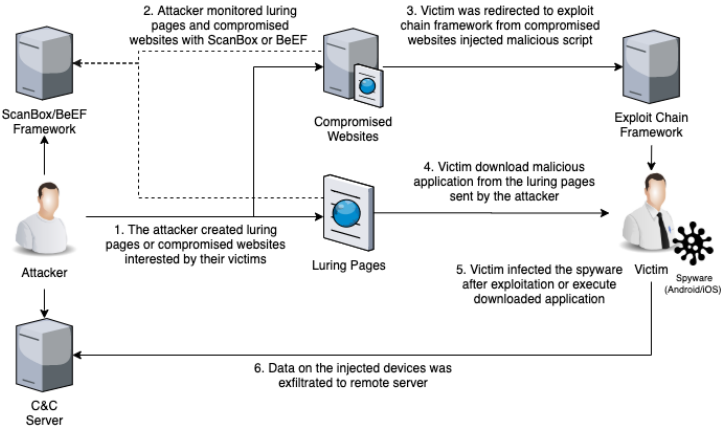
1. Yang pertama harus dilakukan adalah membersihkan perangkat yang terinfeksi seperti PC atau smartphone. Buat password baru kemudian pasang aplikasi anti spyware dari sumber yang

terpercaya. Bisa juga memasang anti virus dan perangkat keamanan lainnya.
2. Setelah membersihkan sistem, yang selanjutnya dilakukan adalah memperbaharui akun keuangan. Bisa jadi akun bank sudah diketahui oleh spyware dan perlu di ganti.
3. Jika informasi yang dicuri adalah informasi sensitif atau melibatkan pengumpulan dan transmisi gambar, audio dan video, maka anda harus menghubungi pihak penegak hukum setempat untuk melaporkan adanya pencurian data dan potensi pelanggaran hukum.
4. Hal terakhir adalah jika akun telah dicuri seperti akun keuangan, maka tindakan pembekuan akun keuangan adalah tindakan yang tepat. Kemudian menggan semua informasi tentang akunnya.

9.8. Bagaimana Melindungi Diri Dari Spyware

Bagaimana cara melindungi diri dari ancaman spyware? Cara terbaik mencegah dan melindungi diri dari ancaman spyware adalah dengan sadar akan bahaya spware. Sadar akan keberadaan spyware, bahayanya dan cara spyware menginfeksi. Berikut ini adalah cara agar terhindar dari bahaya spyware, yaitu;

1. Tidak sembarangan membuka email dari pengirim yang tidak dikenal.
2. Tidak mengunduh file kecuali berasal dari sumber tepercaya.
3. Tidak mengklik tautan atau link website yang tidak sesuai dengan url pada umumnya.
4. menggunakan program keamanan siber terkemuka untuk melawan spyware.
5. Gunakan anti spyware perlindungan real time.
6. Memblokir lalu lintas jaringan atau fitur pengiriman data spyware ke server.



Gambar 9.2. Teknik Mobile Spyware

Sumber: https://www.semanticscholar.org/paper/Techniques-Used-for-Detection-of-Mobile-Spyware-Kaur/

9.9. Kesimpulan

Spyware tersebar luas di seluruh web, dan selalu ada di perangkat seluler dan desktop saat ini. Anda harus selalu waspada terhadap keamanan dan menghindari mengklik tautan yang mencurigakan atau mengunduh perangkat lunak yang tidak dikenal. Sebaiknya Anda juga menggunakan perangkat lunak keamanan agar Anda selalu terlindungi

Tugas dan Diskusi:

1. Bagaimana cara kerja spyware pada ponsel?
2. Apa saja contoh mobile spyware?
3. Apa saja tanda-tanda mobile spyware?
4. Apakah mobile spyware dapat dideteksi?

Referensi:

Wienbar, Sharon. "The Spyware Inferno". News.com. August 13, 2004.

Kim, Taejin; Yi, Jeong Hyun; Seo, Changho (January 2014). "Spyware Resistant Smartphone User Authentication Scheme". International Journal of Distributed Sensor Networks. 10 (3): 237125. doi:10.1155/2014/237125. ISSN 1550-1477. S2CID 12611804.

BAB X.

SECURE MOBILE APP DEVELOPMENT

10.1. Pendahuluan

Keamanan aplikasi seluler berfokus pada postur keamanan perangkat lunak aplikasi seluler di berbagai platform seperti Android, iOS, dan Windows Phone. Ini mencakup aplikasi yang berjalan baik di ponsel maupun tablet. Aplikasi seluler adalah bagian penting dari keberadaan online bisnis dan banyak bisnis mengandalkan sepenuhnya pada aplikasi seluler untuk terhubung dengan pengguna dari seluruh dunia. Lebih banyak pengguna daripada sebelumnya yang mengandalkan aplikasi seluler untuk sebagian besar tugas digital mereka daripada aplikasi desktop tradisional.

Bahan kajian pembelajaran pada bab adalah penjelasan secara komprehensif tentang definisi **Secure Mobile App Development**.

Sub Capaian pembelajaran mata kuliah dalam dalam pertemuan ini adalah mahasiswa diharapkan dapat **Mengetahui dan memahami tentang Secure Mobile App Development.**

Indikator pencapaian dalam pertemuan ini adalah mahasiswa dapat mendeskripsikan, **mampu menjelaskan dan mempraktekkan mengenai konsep pengembangan aplikasi mobile yang aman.**

Penyampaian materi adalah dengan **ceramah, diskusi, dan praktek**

10.2. Apa itu Keamanan Aplikasi Seluler

Keamanan aplikasi seluler berfokus pada postur keamanan perangkat lunak aplikasi seluler di berbagai platform seperti Android, iOS, dan Windows Phone. Ini mencakup aplikasi yang berjalan baik di ponsel maupun tablet. Ini melibatkan penilaian aplikasi untuk masalah keamanan dalam konteks platform tempat mereka dirancang untuk dijalankan, kerangka kerja yang mereka kembangkan, dan kumpulan pengguna yang diantisipasi (misalnya, karyawan vs. pengguna akhir). Aplikasi seluler adalah bagian penting dari keberadaan online bisnis dan banyak bisnis bergantung sepenuhnya pada aplikasi seluler untuk terhubung dengan pengguna dari seluruh dunia[1].

Lebih banyak pengguna daripada sebelumnya yang mengandalkan aplikasi seluler untuk sebagian besar tugas digital mereka daripada aplikasi desktop tradisional. Pada 2015 di AS saja, pengguna menghabiskan 54% waktu media digital mereka di perangkat seluler secara aktif menggunakan aplikasi seluler. Aplikasi ini memiliki akses ke sejumlah besar data pengguna, sebagian besar merupakan data sensitif dan harus dilindungi dari akses yang tidak sah.

Semua platform seluler populer menyediakan kontrol keamanan yang dirancang untuk membantu pengembang perangkat lunak membangun aplikasi yang aman. Namun, pengembang sering kali harus memilih dari banyak sekali opsi keamanan. Kurangnya pemeriksaan dapat menyebabkan penerapan fitur keamanan yang dapat dengan mudah dielakkan oleh penyerang.

Masalah umum yang memengaruhi aplikasi seluler meliputi:

1. Menyimpan atau secara tidak sengaja membocorkan data sensitif sedemikian rupa sehingga dapat dibaca oleh aplikasi lain di ponsel pengguna.
2. Menerapkan pemeriksaan otentikasi dan otorisasi yang buruk yang dapat dilewati oleh aplikasi atau pengguna jahat.

[1] Crussell, Johnathan; Gibler, Clint; Chen, Hao (2012). Attack of the Clones: Detecting Cloned Applications on Android Markets (PDF) (Dissertation). University of California, Davis

3. Menggunakan metode enkripsi data yang diketahui rentan atau dapat dengan mudah dipatahkan.
4. Mengirimkan data sensitif tanpa enkripsi melalui Internet.

Masalah ini dapat dieksploitasi dengan berbagai cara; misalnya, oleh aplikasi hasad pada perangkat pengguna, atau oleh penyerang yang memiliki akses ke jaringan WiFi yang sama sebagai pengguna akhir.

10.3. Apa itu Pengujian Keamanan Aplikasi Seluler

Pengujian keamanan aplikasi seluler melibatkan pengujian aplikasi seluler dengan cara yang akan dicoba oleh pengguna jahat untuk menyerangnya. Pengujian keamanan yang efektif dimulai dengan pemahaman tentang tujuan bisnis aplikasi dan jenis data yang ditangani. Dari sana, kombinasi analisis statis , analisis dinamis , dan pengujian penetrasi menghasilkan penilaian holistik yang efisien untuk menemukan kerentanan yang akan terlewatkan jika teknik tidak digunakan bersama secara efektif. Proses pengujian meliputi:

1. Berinteraksi dengan aplikasi dan memahami cara aplikasi menyimpan, menerima, dan mengirimkan data.
2. Mendekripsi bagian terenkripsi dari aplikasi.
3. Mendekompilasi aplikasi dan menganalisis kode yang dihasilkan.
4. Menggunakan analisis statis untuk menunjukkan kelemahan keamanan dalam kode yang didekompilasi.
5. Menerapkan pemahaman yang diperoleh dari rekayasa balik dan analisis statis untuk mendorong analisis dinamis dan pengujian penetrasi.
6. Memanfaatkan analisis dinamis dan pengujian penetrasi untuk mengevaluasi efektivitas kontrol keamanan (misalnya, kontrol otentikasi dan otorisasi) yang digunakan dalam aplikasi.

Ada sejumlah alat keamanan aplikasi seluler gratis dan komersial yang tersedia yang menilai aplikasi menggunakan metodologi pengujian statis atau dinamis dengan berbagai tingkat efektivitas. Namun, tidak ada satu alat pun yang memberikan penilaian menyeluruh atas aplikasi tersebut. Sebaliknya, kombinasi pengujian statis dan dinamis dengan tinjauan manual diperlukan untuk memberikan cakupan terbaik.

Pengujian keamanan aplikasi seluler dapat dianggap sebagai pemeriksaan pra-produksi untuk memastikan bahwa kontrol keamanan dalam aplikasi berfungsi seperti yang diharapkan, sambil menjaga dari kesalahan implementasi. Ini dapat membantu menemukan kasus edge (yang berubah menjadi bug keamanan) yang mungkin tidak diantisipasi oleh tim pengembangan. Proses pengujian memperhitungkan masalah kode dan konfigurasi dalam lingkungan seperti produksi untuk memastikan bahwa masalah ditemukan sebelum ditayangkan.

10.4. Kesimpulan

Aplikasi seluler dan pelanggaran keamanan terkait menerima banyak perhatian media

- Anda tidak bisa 100% aman, tetapi Anda bisa berhasil memnuatnya sulit - Defense in Depth
- Ketahui data Anda, ketahui platform dan penggunaan Anda pengetahuan itu untuk melindungi aplikasi Anda

Tugas dan Diskusi

Kekhawatiran Pengembang Seluler: Menurut Anda, apa tiga masalah keamanan terbesar itu pengembang aplikasi seluler harus mempertimbangkan dalam desain dan implementasinya? Gambarkan masing-masing masalah ini secara rinci, dan membuat argumen untuk kepentingannya atas keamanan.

Referensi:

Crussell, Johnathan; Gibler, Clint; Chen, Hao (2012). Attack of the Clones: Detecting Cloned Applications on Android Markets (PDF) (Dissertation). University of California, Davis

BAB XI.

Mobile SMS Security

11.1. Pendahuluan

Mobile SMS Security sedang meningkat, dengan bisnis kecil dan perusahaan tingkat perusahaan menyadari potensi otentikasi layanan pesan singkat dan keamanan grup dengan media yang cepat dan andal ini. Sebagai pengembang aplikasi dengan audiens untuk dipikirkan, bagaimana Anda akan menggunakan SMS untuk mengamankan informasi pribadi pengguna Anda?

Selama bertahun-tahun, SMS seluler telah membantu melindungi dan mengamankan data yang dipertukarkan antara pengguna aplikasi dan pengembang aplikasi. Apakah Anda mengoptimalkan keamanan SMS Anda?

Bahan kajian pembelajaran pada bab adalah penjelasan secara komprehensif tentang definisi **Mobile SMS Security.**

Sub Capaian pembelajaran mata kuliah dalam dalam pertemuan ini adalah mahasiswa diharapkan dapat **Mengetahui dan memahami tentang SMS security**.

Indikator pencapaian dalam pertemuan ini adalah mahasiswa dapat mendeskripsikan, **mampu menjelaskan dan mempraktekkan mengenai keamanan SMS.**

Penyampaian materi adalah dengan **ceramah, diskusi, dan praktek**

11.2. Celah Keamanan SMS

Sebuah studi tentang keamanan infrastruktur SMS mengungkapkan bahwa pesan SMS dikirim dariInternet dapat digunakan untuk melakukan serangan Distributed Denial of Service (DDoS) terhadap infrastruktur telekomunikasi seluler kota besar. Serangan tersebut mengeksploitasi penundaan dalam pengiriman pesan untuk membebani jaringan.

Serangan potensial lainnya dapat dimulai dengan telepon yang mengirimkan MMS ke telepon lain, dengan lampiran. Lampiran ini terinfeksi virus. Setelah menerima MMS, pengguna dapat memilih untuk membuka lampiran. Jika dibuka, telepon terinfeksi, dan virus mengirimkan MMS dengan lampiran terinfeksi ke semua kontak di buku alamat. Ada contoh dunia nyata dari serangan ini: virus Commwarrior menggunakan buku alamat dan mengirimkan pesan MMS termasuk file yang terinfeksi ke penerima. Seorang pengguna menginstal perangkat lunak, seperti yang diterima melalui pesan MMS. Kemudian, virus mulai mengirim pesan ke penerima yang diambil dari buku alamat[1].

Ada perubahan yang sangat unik yang terjadi dalam ceruk keamanan setiap tahun, dan hal ini belum terlihat lebih jelas daripada di ruang seluler. SMS telah berkembang menjadi lebih dari sekadar alat 'perpesanan massal'. Ini juga merupakan alat pemberitahuan waktu-nyata yang canggih, sistem peringatan komunitas, dan cara bagi Anda untuk membantu basis pengguna Anda.

Mari kita lihat lebih dekat 5 cara ampuh yang dapat Anda gunakan untuk menggunakan SMS untuk keamanan :

Pemberitahuan pengguna aplikasi

1 untuk masalah keamanan dengan aplikasi Anda. Jika aplikasi Anda diretas dan bug atau mengalami masalah teknis di seluruh pengguna (tidak mau masuk, atau memantulkan pengguna kembali

[1] Finn Trosby, "the strange duckling of GSM SMS" Archived 2007-09-25 at the Wayback Machine, Telektronikk Vol.3 200

ke layar beranda), dan informasi pribadi orang-orang mulai muncul online - Anda dalam masalah. Tindakan terbaik Anda adalah mengirimkan SMS seluler yang memperingatkan semua orang tentang ancaman keamanan baru dan mengontrol penghapusan massal aplikasi Anda.

Bagaimana cara kerjanya? Ponsel selalu diretas , begitu pula aplikasi individu. Tanpa alasan yang jelas, keamanan aplikasi yang digunakan secara global dapat dikompromikan karena peretas ini. SMS adalah cara terbaik untuk mengontrol jatuhnya jumlah pengguna saat ini terjadi!

2: SMS seluler dapat digunakan untuk otentikasi dua faktor. Saat Anda masuk ke situs, aplikasi, atau program penting secara online - satu-satunya cara untuk masuk adalah jika Anda mengakses pin satu kali (OTP) khusus yang dikirimkan situs ke ponsel Anda, dan kode ini dapat kedaluwarsa segera setelah digunakan .

Bagaimana cara kerjanya? Otentikasi dua faktor diatur sehingga hanya pengguna yang dituju yang dapat mengakses profil mereka. Saat masuk, mereka akan menerima pin satu kali (OTP) di ponsel mereka, yang akan mereka gunakan untuk mendapatkan akses ke situs, dan informasi mereka.

3: Pengiriman mata uang dalam aplikasi yang aman semakin populer. Untuk pengalaman SMS seluler berlapis, yang menjamin pengiriman mata uang pengguna Anda segera setelah pembayaran, di jaringan yang aman - SMS seluler adalah jawabannya.

Bagaimana cara kerjanya? Pengguna aplikasi Anda membeli beberapa kode curang untuk aplikasi Anda. Kode dikirimkan melalui SMS seluler dalam hitungan detik setelah pembayaran. Itu pelayanan yang bagus!

4: Lebih banyak keamanan tersedia untuk pengguna SMS seluler yang memiliki rencana pemasaran 'area eksklusif'. Setelah pengguna

aplikasi Anda mencapai level tertentu dalam game, atau dalam aplikasi, mereka membuka SMS khusus yang dikirimkan kepada mereka dengan alamat URL yang sebelumnya tersembunyi, tempat mereka dapat berinteraksi dengan anggota 'elit' lainnya.

Bagaimana cara kerjanya? SMS seluler berfungsi bersama dengan aplikasi Anda untuk hanya mengizinkan orang tertentu masuk ke forum / blog atau situs keanggotaan online Anda yang aman. SMS ideal dalam situasi ini karena memungkinkan anggota Anda melakukan kontak instan - dengan jaminan harga terbuka 98% . Sebagai perbandingan, email tertinggal dengan rasio terbuka 20%.

5: Gunakan SMS seluler untuk membayar item dalam aplikasi secara langsung. Buat pengguna Anda membayar melalui SMS premium, sehingga uangnya dipotong dari airtime prabayar mereka, atau ditambahkan ke tagihan telepon mereka di akhir bulan. Untuk pembelian dalam aplikasi yang murah, ini sangat aman karena tidak ada detail yang perlu dimasukkan atau dibagikan.

Bagaimana cara kerjanya? Sistem bekerja melalui penukaran kode atau dengan mengakses aplikasi atau situs Anda. SMS seluler dikirim ke pengguna Anda, yang kemudian mengirimkan kode kembali kepada Anda, memungkinkan mereka membayar ekstra aplikasi tanpa harus menambahkan detail pembayaran mereka.

11.3. Kesimpulan

SMS memainkan peran penting dalam sistem komunikasi seluler. Sisi pengirim bertindak seperti server untuk sisi penerima yang menerima layanan pesan singkat di sisi penerima. SMS tidak menyertakan prosedur untuk memberikan keamanan untuk teks yang dikirim sebagai data. Mayoritas aplikasi untuk perangkat seluler dirancang dan diterapkan tanpa mempertimbangkan keamanan. Pesan SMS biasanya tidak dienkripsi secara default. Kerahasiaan adalah gagasan untuk memastikan bahwa data tidak dapat diakses atau diekspos kepada orang yang tidak berwenang. Enkripsi adalah pendekatan utama untuk kerahasiaan. Enkripsi

simetris dan asimetris dapat digunakan. Karena kerahasiaan adalah tujuan awal kriptologi, bab ini diperkenalkan sebagai pendekatan kerahasiaan data untuk SMS di Android.

Tugas dan Diskusi

1. Apakah pesan teks telepon aman?
2. Mengapa SMS tidak aman?
3. Apakah Algoritma 2FA SMS aman?

Referensi:

Finn Trosby, "the strange duckling of GSM SMS" Archived 2007-09-25 at the Wayback Machine, Telektronikk Vol.3 200

BAB XII.

Mobile Phishing

12.1. Pendahuluan

Phishing adalah upaya penipuan untuk mendapatkan informasi atau data sensitif , seperti nama pengguna, sandi, dan detail kartu kredit , dengan menyamar sebagai entitas yang dapat dipercaya dalam komunikasi elektronik . Biasanya dilakukan melalui spoofing email , pesan instan , dan pesan teks, phishing sering kali mengarahkan pengguna untuk memasukkan informasi pribadi di situs web palsu yang sesuai dengan tampilan dan nuansa situs resmi.

Bahan kajian pembelajaran pada bab adalah penjelasan secara komprehensif tentang definisi **Mobile Phishing.**

Sub Capaian pembelajaran mata kuliah dalam dalam pertemuan ini adalah mahasiswa diharapkan dapat **Mengetahui dan memahami tentang Mobile Phishing.**

Indikator pencapaian dalam pertemuan ini adalah mahasiswa dapa **mendeskripsikan, mampu menjelaskan dan mempraktekkan mengenai penanganan dan pencegahan Mobile Phishing**

Penyampaian materi adalah dengan **ceramah, diskusi, dan praktek**

Sebagian besar mengira "email" saat mendengar kata "phishing", tetapi berbeda di perangkat seluler. Phishing seluler melampaui email hingga SMS, MMS, platform perpesanan, dan aplikasi media sosial. Serangan secara teknis sederhana tetapi baru dalam pendekatannya. Mereka berusaha untuk mengeksploitasi

kepercayaan manusia di sepanjang jejaring sosial menggunakan konteks pribadi.

12.2. Taktik Umum Mobile Phishing

Ada beberapa teknik yang digunakan penjahat dunia maya mereka lebih efektif di perangkat seluler penjelasan pada Gambar 2.1. untuk membuat teknik serangan phishing pada gambar 12.2 Di bawah ini adalah beberapa taktik yang lebih umum digunakan:

URL padding adalah teknik yang menyertakan domain nyata dan sah dalam URL yang lebih besar tetapi melapisinya dengan tanda hubung untuk mengaburkan tujuan sebenarnya. Misalnya, hxxp: //m.facebook.com----------validate----step1.rickytaylk [dot] com / sign_in.html menyembunyikan domain sebenarnya dari situs berbahaya, rickytaylk, hanya menyisakan m.facebook.com seperti yang terlihat di bilah alamat pada [1]perangkat. Perhatikan, bahwa situs phishing 'rickytaylk' sudah berumur beberapa tahun, tidak aktif lagi, dan hanya digunakan di sini misalnya..

Tiny URLs adalah URL singkat yang dapat digunakan oleh penyerang untuk mengarahkan pengguna ke konten berbahaya. Karena sifatnya yang singkat, mereka cocok untuk serangan SMS phishing dan sering digunakan dalam serangan 'smishing' berskala besar..

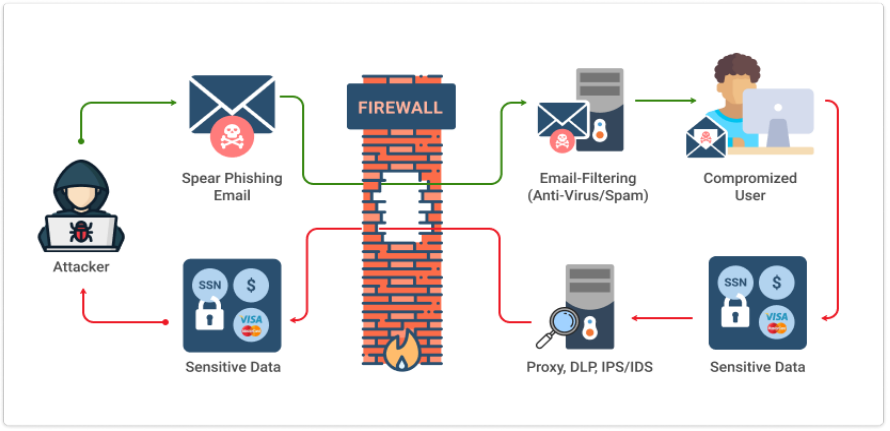
Screen overlays memungkinkan aplikasi mereplikasi halaman login aplikasi seluler yang sah untuk menangkap kredensial otentikasi pengguna. Jenis serangan ini sering digunakan oleh penipuan phishing dan terbukti sangat efektif dan menguntungkan bagi peretas yang menargetkan aplikasi pembayaran dan perbankan seluler..

Mobile verification mengacu pada kode yang disematkan di situs phishing dan dirancang untuk memverifikasi bahwa perangkat yang mengakses tautan adalah perangkat seluler. Ini menyiratkan

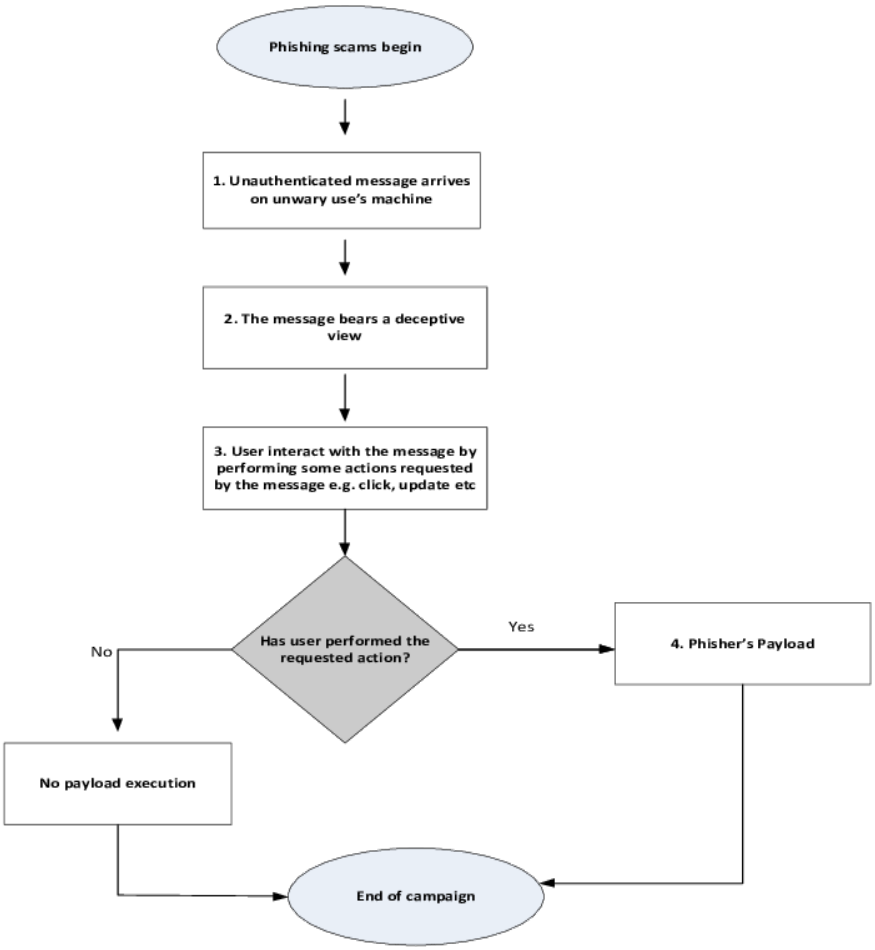
[1] Ramzan, Zulfikar (2010). "Phishing attacks and countermeasures". In Stamp, Mark; Stavroulakis, Peter (eds.). Handbook of Information and Communication Security. Springer. ISBN 978-3-642-04117-4

bahwa penyerang mengonfirmasi bahwa targetnya adalah seluler untuk menyebarkan serangan khusus seluler..

SMS spoofing menggunakan **over-the-air (OTA)** dalah serangan phishing seluler di mana pesan teks palsu menipu pengguna untuk mengklik link. Pesan ini sering kali datang dalam bentuk pemberitahuan pembaruan konfigurasi sistem. Jika diklik, tautan tersebut dapat memicu intersepsi email atau lalu lintas web ke dan dari ponsel Android.



Gambar 12.1. Teknik Mobile Phishing
Sumber: https://www.msp360.com/resources/blog/types-of-phishing/



Gambar 12.2. Siklus Mobile Phishing
Sumber : https://www.sciencedirect.com/science/article/pii/

12.3. Kesimpulan

1. Phishing adalah ketika seseorang berpura-pura menjadi orang lain untuk mencuri uang atau data, atau informasi untuk mendapatkan uang. Phishing adalah cara yang paling umum di mana kebocoran berskala organisasional terjadi.

2. Secara umum, siapa pun yang memiliki data berharga dapat menjadi target phishing.

Tugas dan Diskusi

1. Apa yang diinginkan pelaku phising?
2. Siapa target phishing?
3. Apa dampak phising bagi saya?
4. Apa yang bisa saya lakukan untuk tetap aman?
5. Sepertinya saya telah terkena phising! Apa yang harus saya lakukan sekarang?

Referensi:

Ramzan, Zulfikar (2010). "Phishing attacks and countermeasures". In Stamp, Mark; Stavroulakis, Peter (eds.). Handbook of Information and Communication Security. Springer. ISBN 978-3-642-04117-4.

Van der Merwe, A J, Loock, M, Dabrowski, M. (2005), Characteristics and Responsibilities involved in a Phishing Attack, Winter International Symposium on Information and Communication Technologies, Cape Town, January 2005.

BAB XIII.

MOBILE NETWORK EXPLOITS

13.1. Pendahuluan

Eksploitasi adalah kode yang memanfaatkan kerentanan perangkat lunak atau kelemahan keamanan. ... Saat digunakan, eksploitasi memungkinkan penyusup mengakses jaringan dari jarak jauh dan mendapatkan hak istimewa yang lebih tinggi, atau masuk lebih dalam ke jaringan. Dalam beberapa kasus, exploit dapat digunakan sebagai bagian dari serangan multi-komponen..

Bahan kajian pembelajaran pada bab adalah penjelasan secara komprehensif tentang definisi **Mobile network exploits.**

Sub Capaian pembelajaran mata kuliah dalam dalam pertemuan ini adalah mahasiswa diharapkan dapat **Mengetahui dan memahami tentang mobile network exploits.**

Indikator pencapaian dalam pertemuan ini adalah mahasiswa dapat mendeskripsikan, **Mahasiswa mampu menjelaskan dan mempraktekkan mengenai exploits pada mobile network.**

Penyampaian materi adalah dengan **ceramah, diskusi, dan praktek**

13.2. Serangan berdasarkan jaringan GSM

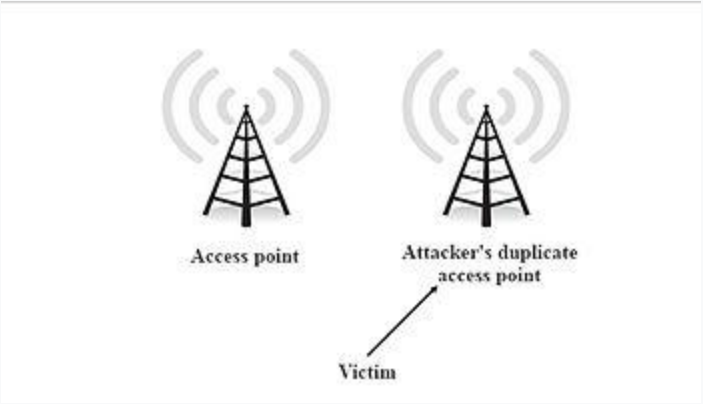
Penyerang mungkin mencoba memecahkan enkripsi jaringan seluler. The GSM algoritma enkripsi jaringan milik keluarga algoritma yang disebut A5 . Karena kebijakan keamanan melalui ketidakjelasan , belum mungkin untuk menguji ketahanan algoritme

ini secara terbuka. Awalnya ada dua varian algoritme: A5 / 1 dan A5 / 2 (stream cipher), di mana yang pertama dirancang agar relatif kuat, dan yang terakhir dirancang agar lemah dengan tujuan untuk memungkinkan pembacaan sandi dan penyadapan yang mudah. ETSI memaksa beberapa negara (biasanya di luar Eropa) untuk menggunakan A5 / 2. Karena algoritme enkripsi dipublikasikan, terbukti dimungkinkan untuk memecahkan enkripsi: A5 / 2 dapat dipatahkan dengan cepat, dan A5 / 1 dalam waktu sekitar 6 jam. [15] Pada bulan Juli 2007, 3GPP menyetujui permintaan perubahan untuk melarang penerapan A5 / 2 di telepon seluler baru, yang berarti bahwa itu telah dinonaktifkan dan tidak lagi diterapkan di telepon seluler. Algoritme publik yang lebih kuat telah ditambahkan ke standar GSM , A5 / 3 dan A5 / 4 (Block cipher), atau dikenal sebagai KASUMI atau UEA1 diterbitkan oleh ETSI. Jika jaringan tidak mendukung A5 / 1, atau algoritma A5 lainnya yang diimplementasikan oleh telepon, maka base station dapat menentukan A5 / 0 yang merupakan algoritma null, dimana lalu lintas radio dikirim tanpa enkripsi. Bahkan jika ponsel dapat menggunakan 3G atau 4G yang memiliki enkripsi lebih kuat daripada 2G GSM , stasiun pangkalan dapat menurunkan versi komunikasi radio ke 2G GSM dan menentukan A5 / 0 (tanpa enkripsi). [17] Ini adalah dasar untuk serangan penyadapan di jaringan radio seluler menggunakan stasiun pangkalan palsu yang biasa disebut penangkap IMSI .

Selain itu, penelusuran terminal seluler sulit karena setiap kali terminal seluler mengakses atau diakses oleh jaringan, identitas sementara baru (TMSI) dialokasikan ke terminal seluler. TMSI digunakan sebagai identitas terminal seluler saat mengakses jaringan di lain waktu. TMSI dikirim ke terminal seluler dalam pesan terenkripsi.

Setelah algoritma enkripsi GSM rusak, penyerang dapat mencegat semua komunikasi tidak terenkripsi yang dibuat oleh smartphone korban.

13.3. Serangan berdasarkan Wi-Fi



Gambar 13.1. Spoofing Titik Akses

Penjelasan Gambar 13.1 : Penyerang dapat mencoba menguping komunikasi Wi-Fi untuk mendapatkan informasi (mis. Nama pengguna, sandi). Jenis serangan ini tidak hanya terjadi pada ponsel cerdas, tetapi mereka sangat rentan terhadap serangan ini karena seringkali Wi-Fi menjadi satu-satunya alat komunikasi yang mereka miliki untuk mengakses internet. Keamanan jaringan nirkabel (WLAN) dengan demikian merupakan subjek penting. Awalnya, jaringan nirkabel diamankan dengan kunci WEP . Kelemahan WEP adalah kunci enkripsi pendek yang sama untuk semua klien yang terhubung. Selain itu, beberapa pengurangan dalam ruang pencarian kunci telah ditemukan oleh para peneliti. Sekarang, sebagian besar jaringan nirkabel dilindungi oleh protokol keamanan WPA . WPA didasarkan pada " Protokol Integritas Kunci Temporal(TKIP) "yang dirancang untuk memungkinkan migrasi dari WEP ke WPA pada peralatan yang telah digunakan. Perbaikan utama dalam keamanan adalah kunci enkripsi dinamis. Untuk jaringan kecil, WPA adalah" kunci yang dibagikan sebelumnya "yang didasarkan pada kunci bersama. Enkripsi dapat menjadi rentan jika panjang kunci bersama pendek. Dengan kesempatan input yang terbatas (yaitu hanya keypad numerik), pengguna ponsel mungkin menentukan kunci enkripsi pendek yang hanya berisi angka. Hal ini meningkatkan kemungkinan penyerang

berhasil dengan serangan brute force. Penerus WPA, yang disebut WPA2 , seharusnya cukup aman untuk menahan serangan brute force.

Seperti halnya GSM, jika penyerang berhasil memecahkan kunci identifikasi, maka akan mungkin untuk menyerang tidak hanya telepon tetapi juga seluruh jaringan yang terhubung dengannya.

Banyak ponsel cerdas untuk LAN nirkabel mengingat bahwa mereka telah terhubung, dan mekanisme ini mencegah pengguna untuk mengidentifikasi ulang dengan setiap koneksi. Namun, penyerang dapat membuat kembaran titik akses WIFI dengan parameter dan karakteristik yang sama dengan jaringan asli. Menggunakan fakta bahwa beberapa ponsel cerdas mengingat jaringan, mereka dapat mengacaukan dua jaringan dan menyambung ke jaringan penyerang yang dapat mencegat data jika tidak mengirimkan datanya dalam bentuk terenkripsi. [18] [19] [20]

Lasco adalah worm yang awalnya menginfeksi perangkat jarak jauh menggunakan format file SIS . Format file SIS (Software Installation Script) adalah file script yang dapat dijalankan oleh sistem tanpa interaksi pengguna. Dengan demikian, smartphone percaya bahwa file tersebut berasal dari sumber tepercaya dan mengunduhnya, menginfeksi mesin.

13.4. Serangan berbasis Bluetooth

Masalah keamanan yang terkait dengan Bluetooth pada perangkat seluler telah dipelajari dan menunjukkan banyak masalah pada ponsel yang berbeda. Satu kerentanan yang mudah dieksploitasi : layanan yang tidak terdaftar tidak memerlukan otentikasi, dan aplikasi yang rentan memiliki port serial virtual yang digunakan untuk mengontrol telepon. Penyerang hanya perlu terhubung ke port untuk mengambil kendali penuh atas perangkat. Contoh lain: telepon harus dalam jangkauan dan Bluetooth dalam mode penemuan. Pada Gambar 13.2 dijelaskan Penyerang mengirimkan file melalui Bluetooth. Jika penerima menerima, virus ditularkan. Contoh: Cabir adalah worm yang menyebar melalui koneksi Bluetooth. Worm mencari ponsel

terdekat dengan Bluetooth dalam mode yang dapat ditemukan dan mengirimkan dirinya sendiri ke perangkat target. Pengguna harus menerima file yang masuk dan menginstal program. Setelah dipasang, worm menginfeksi mesin[1].

Gambar 13.2. Contoh Serangan menggunakan Bluetooth
Sumber: http://itsmyviewofthings.blogspot.com/2011/03/bluetooth-attacks.html

13.5. Kesimpulan

1. Keamanan jaringan (mobile network security) terdiri dari kebijakan dan praktik untuk mencegah dan memantau akses yang tidak sah, penyalahgunaan, maupun penolakan yang terjadi di jaringan komputer.
2. Mobile Network melibatkan otorisasi akses ke data di dalam jaringan, yang dikendalikan oleh administrator jaringan. Pengguna (users) memilih atau diberi ID dan password atau informasi otentikasi lain yang memungkinkan mereka untuk

[1] http://docs.lucidinteractive.ca/index.php/Cracking_WEP_and_WPA_Wireless_Networks

mengakses informasi dan program dalam wewenang mereka sendiri.

3. Mobile Network mencakup berbagai jaringan komputer, baik publik maupun pribadi, yang digunakan dalam pekerjaan sehari-hari; melakukan transaksi dan komunikasi di antara bisnis, instansi pemerintah dan individu. Jaringan tersebut dapat bersifat pribadi, seperti di dalam perusahaan, dan lainnya yang mungkin terbuka bagi akses publik.
4. Mobile Network terlibat dalam organisasi, perusahaan, dan jenis lembaga lainnya. Seperti bagaimana mengamankan jaringan, serta melindungi dan mengawasi operasi yang dilakukan. Dimana cara paling umum dan sederhana untuk melindungi sumber daya jaringan (network resource) adalah dengan menetapkan nama yang unik dan password yang sesuai.

Tugas dan Diskusi:

1. Apa yang dimaksud dengan Network And Internet Defense
2. Komponen-komponen apa saja yang ada pada Network And Internet Defense
3. Mengapa diperlukannya Network And Internet Defense
4. Berikan contoh keuntungan yang diperoleh dari keberadaan Network And Internet Defense
5. Berikan contoh kerugian yang diperoleh jika tidak memiliki Network And Internet Defense
6. Jelaskan unit organisasi yang bertanggung jawab dalam mengembangkan Network And Internet Defense
7. Jelaskan batasan teritori organisasi yang terikat atau harus patuh terhadap Network And Internet Defense
8. Jelaskan waktu yang tepat bagi sebuah organisasi untuk menyusun Network And Internet Defense

Referensi:

http://www.wi-foo.com/
http://docs.lucidinteractive.ca/index.php/Cracking_WEP_and_WPA_Wireless_Networks

DAFTAR PUSTAKA

Bishop, Matt (2004). Introduction to Computer Security. Addison Wesley Professional. ISBN 978-0-321-24744-5.

Dunham, Ken; Abu Nimeh, Saeed; Becher, Michael (2008). Mobile Malware Attack and Defense. Syngress Media. ISBN 978-1-59749-298-0.

Rogers, David (2013). Mobile Security: A Guide for Users. Copper Horse Solutions Limited. ISBN 978-1-291-53309-5.

Becher, Michael (2009). Security of Smartphones at the Dawn of Their Ubiquitousness (PDF) (Dissertation). Mannheim University.

Becher, Michael; Freiling, Felix C.; Hoffmann, Johannes; Holz, Thorsten; Uellenbeck, Sebastian; Wolf, Christopher (May 2011). Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices (PDF). 2011 IEEE Symposium on Security and Privacy. pp. 96–111. doi:10.1109/SP.2011.29. ISBN 978-1-4577-0147-4.

Bilton, Nick (26 July 2010). "Hackers With Enigmatic Motives Vex Companies". The New York Times. p. 5.

Cai, Fangda; Chen, Hao; Wu, Yuanyi; Zhang, Yuan (2015). AppCracker: Widespread Vulnerabilities in Userand Session Authentication in Mobile Apps (PDF) (Dissertation). University of California, Davis.

Crussell, Johnathan; Gibler, Clint; Chen, Hao (2012). Attack of the Clones: Detecting Cloned Applications on Android Markets (PDF) (Dissertation). University of California, Davis.

Dagon, David; Martin, Tom; Starder, Thad (October–December 2004). "Mobile Phones as Computing Devices: The Viruses are Coming!". IEEE Pervasive Computing. 3 (4): 11. doi:10.1109/MPRV.2004.21. S2CID 14224399.

Dixon, Bryan; Mishra, Shivakant (June–July 2010). On and Rootkit and Malware Detection in Smartphones (PDF). 2010 International Conference on Dependable Systems and Networks Workshops (DSN-W). ISBN 978-1-4244-7728-9.

Gendrullis, Timo (November 2008). A real-world attack breaking A5/1 within hours. Proceedings of CHES '08. Springer. pp. 266–282. doi:10.1007/978-3-540-85053-3_17.

Gupta, Sugandha (2016). Vulnebdroid: Automated Vulnerability Score Calculator for Android Applications. International Symposium on Security in Computing and Communication. Springer. doi:10.1007/978-981-10-2738-3_40.

Guo, Chuanxiong; Wang, Helen; Zhu, Wenwu (November 2004). Smart-Phone Attacks and Defenses (PDF). ACM SIGCOMM HotNets. Association for Computing Machinery, Inc. Retrieved March 31, 2012.

Halbronn, Cedric; Sigwald, John (2010). Vulnerabilities & iPhone Security Model (PDF). HITB SecConf 2010. Archived from the original (PDF) on 2013-02-02. Retrieved 2012-04-21.

Hogben, Giles; Dekker, Marnix (December 2010). "Smartphones: Information security Risks, Opportunities and Recommendations for users". ENISA.

Jøsang, Audun; Miralabé, Laurent; Dallot, Léonard (2015). "Vulnerability by Design in Mobile Network Security" (PDF). Journal of Information Warfare (JIF). 14 (4). ISSN 1445-3347.

Malik, Jyoti (2016). CREDROID: Android malware detection by network traffic analysis. Proceedings of the 1st ACM Workshop on Privacy-Aware Mobile Computing. Association for Computing Machinery, Inc. pp. 28–36. doi:10.1145/2940343.2940348.

Mickens, James W.; Noble, Brian D. (2005). Modeling epidemic spreading in mobile environments. WiSe '05 Proceedings of the 4th ACM workshop on Wireless security. Association for

Computing Machinery, Inc. pp. 77–86. doi:10.1145/1080793.1080806.

Mulliner, Collin Richard (2006). Security of Smart Phones (PDF) (M.Sc. thesis). University of California, Santa Barbara.

Pandya, Vaibhav Ranchhoddas (2008). Iphone Security Analysis (PDF) (Thesis). San Jose State University.

Raboin, Romain (December 2009). La sécurité des smartphones (PDF). Symposium sur la sécurité des technologies de l'information et des communications 2009. SSTIC09 (in French).

Racic, Radmilo; Ma, Denys; Chen, Hao (2006). Exploiting MMS Vulnerabilities to Stealthily Exhaust Mobile Phone's Battery (PDF) (Dissertation). University of California, Davis.

Roth, Volker; Polak, Wolfgang; Rieffel, Eleanor (2008). Simple and Effective Defense Against Evil Twin Access Points. ACM SIGCOMM HotNets. doi:10.1145/1352533.1352569. ISBN 978-1-59593-814-5.

Ruff, Nicolas (2011). Sécurité du système Android (PDF). Symposium sur la sécurité des technologies de l'information et des communications 2011. SSTIC11 (in French).

Ruggiero, Paul; Foote, Jon. Cyber Threats to Mobile Phones (PDF) (thesis). US-CERT.

Schmidt, Aubrey-Derrick; Schmidt, Hans-Gunther; Clausen, Jan; Yüksel, Kamer Ali; Kiraz, Osman; Camtepe, Ahmet; Albayrak, Sahin (October 2008). Enhancing Security of Linux-based Android Devices (PDF). Proceedings of 15th International Linux Kongress.

Schmidt, Aubrey-Derrick; Schmidt, Hans-Gunther; Batyuk, Leonid; Clausen, Jan Hendrik; Camtepe, Seyit Ahmet; Albayrak, Sahin (April 2009a). Smartphone Malware Evolution Revisited: Android Next Target? (PDF). 4th International Conference on Malicious and Unwanted Software (MALWARE). ISBN 978-1-4244-5786-1. Retrieved 2010-11-30.

Shabtai, Asaf; Fledel, Yuval; Kanonov, Uri; Elovici, Yuval; Dolev, Shlomi (2009). "Google Android: A State-of-the-Art Review of Security Mechanisms". arXiv:0912.5101v1 [cs.CR].

Thirumathyam, Rubathas; Derawi, Mohammad O. (2010). Biometric Template Data Protection in Mobile Device Using Environment XML-database. 2010 2nd International Workshop on Security and Communication Networks (IWSCN). ISBN 978-1-4244-6938-3. Archived from the original on 2013-02-12.

Töyssy, Sampo; Helenius, Marko (2006). "About malicious software in smartphones". Journal in Computer Virology. 2 (2): 109–119. doi:10.1007/s11416-006-0022-0. S2CID 9760466.

European Telecommunications Standards Institute (2011). "3GPP Confidentiality and Integrity Algorithms & UEA1 UIA1". Archived from the original on 12 May 2012.

CIGREF (October 2010). "Sécurisation de la mobilité" (PDF) (in French).

Chong, Wei Hoo (November 2007). iDEN Smartphone Embedded Software Testing (PDF). Fourth International Conference on Information Technology, 2007. ITNG '07. doi:10.1109/ITNG.2007.103. ISBN 978-0-7695-2776-5.

Jansen, Wayne; Scarfone, Karen (October 2008). "Guidelines on Cell Phone and PDA Security: Recommendations of the National Institute of Standards and Technology" (PDF). National Institute of Standards and Technology. Retrieved April 21, 2012.

Murugiah P. Souppaya; Scarfone, Karen (2013). "Guidelines for Managing the Security of Mobile Devices in the Enterprise". National Institute of Standards and Technology 2013. doi:10.6028/NIST.SP.800-124r1.

Lee, Sung-Min; Suh, Sang-bum; Jeong, Bokdeuk; Mo, Sangdok (January 2008). A Multi-Layer Mandatory Access Control Mechanism for Mobile Devices Based on Virtualization. 5th IEEE Consumer Communications and Networking Conference, 2008. CCNC 2008. doi:10.1109/ccnc08.2007.63. ISBN 978-1-4244-1456-7.

Li, Feng; Yang, Yinying; Wu, Jie (March 2010). CPMC: An Efficient Proximity Malware Coping Scheme in Smartphone-based Mobile Networks (PDF). INFOCOM, 2010 Proceedings IEEE. doi:10.1109/INFCOM.2010.5462113.

Ni, Xudong; Yang, Zhimin; Bai, Xiaole; Champion, Adam C.; Xuan, Dong (October 2009). Distribute: Differentiated User Access Control on Smartphones. 6th IEEE International Conference on Mobile Adhoc and Periodic Sensor Systems, 2009. MASS '09. ISBN 978-1-4244-5113-5.

Ongtang, Machigar; McLaughlin, Stephen; Enck, William; Mcdaniel, Patrick (December 2009). Semantically Rich Application-Centric Security in Android (PDF). Annual Computer Security Applications Conference, 2009. ACSAC '09. Annual Computer Security Applications Conference (Acsac). ISSN 1063-9527.

Schmidt, Aubrey-Derrick; Bye, Rainer; Schmidt, Hans-Gunther; Clausen, Jan; Kiraz, Osman; Yüksel, Kamer A.; Camtepe, Seyit A.; Albayrak, Sahin (2009b). Static Analysis of Executables for Collaborative Malware Detection on Android (PDF). IEEE International Conference Communications, 2009. ICC '09. Communications, 2009. Icc '09. IEEE International Conference on. ISSN 1938-1883.

Yang, Feng; Zhou, Xuehai; Jia, Gangyong; Zhang, Qiyuan (2010). A Non-cooperative Game Approach for Intrusion Detection Systems in Smartphone systems. 8th Annual Communication Networks and Services Research Conference. doi:10.1109/CNSR.2010.24. ISBN 978-1-4244-6248-3.

GLOSARIUM

A

Advertising Click Fraud *adalah jenis malware yang memungkinkan penyerang membajak perangkat untuk menghasilkan pendapatan melalui klik iklan palsu.*

Algoritma *adalah suatu upaya dengan urutan operasi yang disusun secara logis dan sistematis untuk menyelesaikan suatu masalah untuk menghasilkan suatu output tertentu · 8*

Android SDK *adalah adalah sekumpulan alat yang dapat digunakan oleh pembuat aplikasi untuk mengembangkan aplikasi yang dikustomisasi untuk ditambahkan, atau dihubungkan dengan, program lain. Dengan SDK, programmer dapat mengembangkan aplikasi untuk platform tertentu*

Android Studio *adalah Integrated Development Environment (IDE) resmi untuk pengembangan aplikasi Android, yang didasarkan pada IntelliJ IDEA*

B

Backdoor *adalah Metode rahasia untuk melewati batasan keamanan untuk mendapatkan akses tidak sah ke sistem komputer. Dengan kata sederhana, pintu belakang adalah bagian kode yang memungkinkan orang lain masuk dan keluar dari sistem tanpa terdeteksi*

Broadcast Receiver *adalah komponen di aplikasi Android yang menunggu sebuah pesan broadcast (atau event yang terjadi) dari beberapa sumber: Aplikasi itu sendiri. Dari sistem. Atau dari aplikasi lain*

Bug*. adalah error yang menyebabkan aplikasi/software tak berjalan*

dengan semestinya. Mulai dari tiba-tiba hang atau freeze, layar jadi hitam atau biru, hingga aplikasi tertutup dengan sendirinya.

BYOD . *Bring Your Own Device* adalah sebuah kebijakan yang mengizinkan para pegawai untuk membawa gadget pribadi mereka masing-masing seperti laptop, tablet, dan smartphone untuk digunakan di tempat kerja serta digunakan untuk mengakses data perusahaan serta aplikasinya menggunakan device pribadi mereka.

C

C# *adalah atau yang dibaca C sharp adalah bahasa pemrograman sederhana yang digunakan untuk tujuan umum, dalam artian bahasa pemrograman ini dapat digunakan untuk berbagai fungsi misalnya untuk pemrograman server-side pada website, membangun aplikasi desktop ataupun mobile, pemrograman game dan sebagainya. Selain itu C# juga bahasa pemrograman yang berorientasi objek, jadi C# juga mengusung konsep objek seperti inheritance, class, polymorphism dan encapsulation.*

C++ *adalah bahasa pemrograman komputer yang dibuat oleh Bjarne Stroustrup, yang merupakan perkembangan dari bahasa C dikembangkan di Bell Labs. Pada awal tahun 1970-an, bahasa itu merupakan peningkatan dari bahasa sebelumnya*

Class *yaitu cetakan dari object. Sebuah class berisi kode-kode yang menjelaskan bagaimana sebuah object akan berperilaku dan berinteraksi satu sama lain. Class dalam pemrograman diartikan seperti sebuah cetakan atau template. ·*

Confidentiality *adalah (kerahasiaan) aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan*

Content Provider *adalah sebuah mekanisme penyimpanan di Android. Ia merupakan sebuah antarmuka untuk menjadikan aplikasi sebagai*

penyedia data bagi aplikasi lain di dalam sebuah peranti.

Cyber Threat adalah hal yang dilakukan oleh orang-orang yang tidak bertanggung jawab dengan memanfaatkan celah teknologi untuk kepentingan pribadi yang merugikan orang lain. Dengan maraknya kejahatan dunia maya, beberapa pihak telah melakukan upaya yang membentengi dan mencegah kejahatan maya terjadi.

D

Data Privacy adalah adalah mengenai apa yang dapat dan harus dilakukan oleh lembaga atau perusahaan yang telah mengumpulkan data pribadi seseorang secara sah, dan kontrol apa yang pemilik data miliki atas penyimpanan dan penggunaan data tersebut

Dekripsi (Decrypt) *a*dalah cara merubah kembali data yang tadinya telah di enkripsi menjadi sebuah kode tertentu kemudian dikembalikan ke bentuk semula, contohnya seperti kode-kode yang berbentuk hash dan binary.

Delphi sebuah IDE Compiler untuk bahasa pemrograman Pascal dan lingkungan pengembangan perangkat lunak yang digunakan untuk merancang suatu aplikasi program. Delphi juga dapat di artikan sebagai Suatu bahasa pemrograman yang menggunakan visualisasi sama seperti bahasa pemrograman Visual Basic (VB)

Digital Signature adalah jenis tanda tangan elektronik khusus yang dibuat menggunakan aplikasi eSign khusus. Tanda tangan digital ini menggunakan kriptografi untuk melindungi dokumen dan juga menyematkan detail seperti alamat email Anda, kapan dan di mana Anda menandatangani dokumen apa pun, dan perangkat apa yang Anda gunakan untuk melakukannya. Ini menciptakan sidik jari digital yang membuat dokumen itu unik dan jejak kertas yang dapat diverifikasi secara independen jika, katakanlah, pernah ada kasus pengadilan.

E

Enkapsulasi (Pembungkusan) *Merupakan pelindung program dan data yang sedang diolah. Enkapsulasi mendefinisikan perilaku dan melindungi program dan data*

agar tidak diakses secara sembarangan oleh orang lain

Enkripsi (Encrypt) ·adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus.

European Telecommunications Standards Institute - ETSI *adalah organisasi standarisasi independen, nirlaba di bidang informasi dan komunikasi. ETSI mendukung pengembangan dan pengujian standar teknis global untuk sistem, aplikasi, dan layanan yang mendukung TIK*

F

Faster Development Metode ini didukung oleh banyak library objek, sehingga mempercepat penyelesaian program dan juga projek berikutnya.

Free WIFI. ·adalah jaringan internet gratis

Freeware. · perangkat lunak, biasanya milik perorangan dan dilindungi hak cipta, yang didistribusikan ke pengguna akhir secara cuma-cuma dan tidak memungut bayaran apa pun

*Fungsi Hash a*dalah yaitu fungsi yang menerima string dengan panjang sembarang dan mengkonversinya menjadi string keluaran yang panjangnya tetap (fixed). pesan (message), maka sembarang pesan M berukuran bebas dikompresi oleh fungsi hash H melalui persamaan : h = H(M)

Fungsi Hashing adalah fungsi yang secara efisien mengubah string input dengan panjang berhingga menjadi string output dengan panjang tetap yang disebut nilai hash

G

H

I

Improved Software Development Productivity *adalah Sistem program yang dapat dimodifikasi tanpa melibatkan banyak modul dimana hanya objek saja yang terlibat. Selain itu sistem program dapat dikembangkan sampai skala paling kompleks.*

Improved Software Maintainability adalah *Bagian dari software dapat dengan mudah di maintenance jika ada perubahan meskipun dalam skala yang cukup besar.*

Integritas *adalah Merupakan aspek dimana keaslian pesan terjaga walaupun dikirim melalui jaringan yang rentan terhadap serangan, namun dapat dipastikan bahwa data atau informasi yang dikirim tidak diubah oleh orang yang tidak berhak.*

iOS *adalah sistem operasi perangkat lunak yang dikembangkan oleh Apple, secara khusus untuk mendukung pengoperasian produk mobile device atau perangkat genggam. iOS tidak hanya dipakai pada ponsel iPhone, melainkan juga di perangkat genggam apple lainnya, seperti tablet iPad dan pemutar musik iPod*

J

Jailbreak *adalah proses rooting di untuk perangkat Android, jailbreak merupakan sebuah metode yang bisa digunakan oleh pengguna untuk mendapat kebebasan lebih dalam mengelola perangkatnya*

Java · *adalah salah satu bahasa pemrograman populer yang digunakan untuk mengembangkan aplikasi mobile, desktop, hingga website. Beberapa website besar dunia seperti, Yahoo!, LinkedIn, dan Spotify ternyata juga telah menggunakan Java untuk mengembangkan websitenya.*

K

Kata sandi non-teks, *adalah simbol atau gambar dapat dipilih dari bidang yang dibuat secara acak.*

Keamanan jaringan (mobile network security) *adalah kebijakan dan praktik untuk mencegah dan memantau akses yang tidak sah, penyalahgunaan, maupun penolakan yang terjadi di jaringan komputer.*

Key Management · *adalah proses penerapan standar tertentu untuk memastikan keamanan kunci kriptografi dalam suatu organisasi yang berurusan dengan pembuatan, pertukaran, penyimpanan, penghapusan, dan penyegaran kunci. Mereka juga menangani akses anggota dari kunci*

Kriptografi *adalah ilmu yang mempelajari bagaimana membuat suatu pesan yang dikirim pengirim dapat disampaikan kepada penerima dengan aman .*

Kunci Aktivasi *adalah sistem*

yang mencegah orang lain menggunakan perangkat Anda yang terhapus dari jarak jauh.

L

Logika atau bom waktu *adalah teknik pintu belakang klasik yang memicu aktivitas berbahaya berdasarkan peristiwa, penggunaan perangkat, atau waktu tertentu .*

M

Malware*. · adalah perangkat lunak apa pun yang sengaja dirancang untuk menyebabkan kerusakan pada komputer, peladen, klien, atau jaringan komputer Berbagai jenis malware ada, termasuk virus komputer, cacing komputer, kuda troya, perangkat pemeras, perangkat pengintai, perangkat lunak beriklan, dan scareware*

Mobile Authentication *adalah verifikasi identitas pengguna melalui penggunaan perangkat seluler dan satu atau beberapa metode autentikasi untuk akses aman. Mobile Authentication dapat digunakan untuk mengotorisasi perangkat seluler itu sendiri atau sebagai bagian dari skema otentikasi multifaktor untuk masuk ke lokasi dan sumber daya yang aman.*

Mobile Malware*, dalah perangkat lunak berbahaya yang dirancang khusus untuk menargetkan perangkat seluler, seperti ponsel cerdas dan tablet, dengan tujuan memperoleh akses ke data pribadi. ·*

Mobile Security *adalah perlindungan ponsel pintar, tablet, laptop, dan perangkat komputasi portabel lainnya, dan jaringan tempat mereka terhubung, dari ancaman dan kerentanan yang terkait dengan komputasi nirkabel. Mobile Security juga dikenal sebagai Wireless Security.*

N

Non-repudiasi, *atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.*

Non-repudiation *Merupakan aspek yang berhubungan dengan keaslian pengirim pesan, dapat dipastikan bahwa pengirim adalah orang*

yang sebenarnya diharapkan mengirimkan data.

O

Object *dalam dunia pemrograman objek diartikan sebagai bagian dari sebuah program. Dimana di dalamnya dihubungkan beberapa variable dan method yang salin berkaitan satu sama lain*

Otentikasi out of band*, adalah sebuah kondisi di mana pengguna melakukan panggilan untuk mendapatkan otentikasi.*

P

Perangkat seluler *· perangkat lain yang dibuat untuk portabilitas, dan karenanya kompak dan ringan*

Perangkat Virtual Android *· adalah sebuah konfigurasi yang menetapkan karakteristik ponsel dan tablet Android, Wear OS, Android TV, atau perangkat Automotive OS yang ingin Anda simulasikan dalam Android Emulator.*

Perl *· adalah adalah bahasa pemrograman untuk segala keperluan, dikembangkan pertama kali oleh Larry Wall di mesin Unix. Perl dirilis pertama kali pada tanggal 18 Desember 1987*

Phishing *adalah ketika seseorang berpura-pura menjadi orang lain untuk mencuri uang atau data, atau informasi untuk mendapatkan uang. Phishing adalah cara yang paling umum di mana kebocoran berskala organisasional terjadi.*

PHP *adalah singkatan rekursif untuk "PHP: Hypertext Preprocessor", yaitu bahasa pemrograman yang digunakan secara luas untuk penanganan pembuatan dan pengembangan sebuah situs web dan bisa digunakan bersamaan dengan HTMLPlatform Android SDK · 20, 21*

Platform Android SDK *adalah Kit pengembangan perangkat lunak (SDK) adalah sekumpulan alat yang dapat digunakan oleh pembuat aplikasi untuk mengembangkan aplikasi yang dikustomisasi untuk ditambahkan, atau dihubungkan dengan, program lain. Dengan SDK, programmer dapat mengembangkan aplikasi untuk platform tertentu.*

Prinsip Keamananan Data *adalah usaha melindungi sistem informasi agar terpelihara integritas (integraty), ketersediaaan (availability), dan kerahasiannya atau kepercayaanya (confidentiality).*

Privasi informas*i adalah hubungan antara pengumpulan dan penyebaran data , teknologi , ekspektasi publik terhadap privasi , dan masalah hukum dan politik yang mengelilinginya. Ini juga dikenal sebagai privasi data atau perlindungan data . · 86*

Property *adalah merupakan variable yang dideklarasikan di dalam sebuah class, tetapi tidak berada di dalam fungsi atau method dari suatu class. · 46*

Python *· adalah bahasa pemrograman interpretatif yang dapat digunakan di berbagai platform dengan filosofi perancangan yang berfokus pada tingkat keterbacaan kode dan merupakan salah satu bahasa populer yang berkaitan dengan Data Science, Machine Learning, dan Internet of Things (IoT). Keunggulan Python yang bersifat interpretatif juga banyak digunakan untuk prototyping, scripting dalam pengelolaan infrastruktur, hingga pembuatan website berskala besar*

R

RSA · *(Rivest Shamir Adleman)* *adalah sebuah algoritma pada enkripsi publik key. RSA merupakan salah satu metode enkripsi yang paling banyak digunakan.*

Runtime *adalah fase terakhir dari siklus hidup program komputer, di mana kode tersebut dijalankan pada unit pemroses pusat komputer sebagai kode mesin. Dengan kata lain, "runtime" adalah fase menjalankan program.*

S

Schnorr signature *adalah tanda tangan digital yang dihasilkan oleh algoritme tanda tangan Schnorr yang dijelaskan oleh Claus Schnorr.*

Single sign-off *atau* ***single log-out*** *(* **SLO** *) adalah properti di mana satu tindakan keluar akan menghentikan akses ke beberapa sistem perangkat lunak.*

***Secure Hash Algorithm* (SHA)** *· adalah keluarga fungsi hash kriptografi yang diterbitkan*

oleh Institut Nasional Standar dan Teknologi sebagai Standar Pemrosesan Informasi Federal AS, termasuk: SHA-0: Sebuah retronim yang diterapkan pada versi asli dari fungsi hash 160-bit yang diterbitkan pada tahun 1993 dengan nama "SHA"

***Sensor** · perangkat yang menerima dan menanggapi sinyal atau stimulus." Definisi terlihat cukup luas, contoh saja mata manusia yang kemudian dapat digunakan untuk memicu suatu tindakan tertentu*

***Sertifikat digital menggunakan infrastruktur kunci publik. · Public Key Infrastructure (PKI) adalah sebuah metode bagi otentikasi, pengamanan data dan perangkat anti sangkal. Secara teknis, PKI adalah implementasi dari berbagai teknik kriptografi yang mempunyai tujuan bagi mengamankan data, memastikan keaslian data maupun pengirimnya dan mencegah penyangkalan*

***Single Sign-On.** · akses ke beberapa software yang terpisah dan berdiri sendiri, tetapi dimiliki oleh satu pengguna yang sama.*

***Spoofing** adalah salah satu bentuk penipuan online yang dilakukan dengan cara menyamar sebagai seseorang / pihak tertentu. Biasanya, penipu akan berkedok sebagai individu atau organisasi yang memang sudah Anda kenal..*

T

***Taksonomi** · adalah ilmu yang memperlajari identifikasi, tatanama dan klasifikasi suatu objek*

***Tanda tangan digital (S**) didekripsikan dengan kunci publik yang telah diberikan kepada penerima. Proses ini akan menghasilkan MD (Message Digest). · 82*

***Tiny URLs** adalah URL singkat yang dapat digunakan oleh penyerang untuk mengarahkan pengguna ke konten berbahaya. Karena sifatnya yang singkat, mereka cocok untuk serangan SMS phishing dan sering digunakan dalam serangan 'smishing' berskala besar.. ·*

***Token otentikasi (yaitu yang OAuth) adalah layanan web yang disimpan di penyimpanan sistem untuk berbagi antar aplikasi.*

Trojans. · *adalah sebuah perangkat lunak berbahaya yang dapat merusak sebuah sistem atau jaringan. Tujuan dari Trojan adalah memperoleh informasi dari target, dan mengendalikan target.*

Two Factor Authentication. · *adalah lapisan keamanan tambahan untuk melindungi akun Anda lebih jauh, dengan memastikan bahwa orang yang berusaha untuk mengakses akun adalah Anda. Pertama, Anda memasukkan nama pengguna dan kata sandi. Setelah itu, Anda tidak akan langsung masuk, tapi harus menyediakan informasi tambahan*

U

Ubuntu · *adalah adalah salah satu proyek andalan Debian. Sasaran awal Ubuntu adalah menciptakan sistem operasi desktop Linux yang mudah dipakai. Ubuntu dijadwalkan dirilis setiap 6 bulan sehingga sistem Ubuntu dapat terus diperbarui.*

USB Debugging *adalah suatu tindakan untuk memeriksa adanya kemungkinan cacat atau bug pada pengoperasian sistem android. Sebelumnya tindakan ini hanya bisa dilakukan oleh pihak developer. Namun dengan seiring berkembangnya zaman, user saat ini juga bisa untuk melakukan tindakan atau operasi ini.*

V

W

Y

Z

INDEKS

A

Acrivity & Intent · VII, 49

Acrivity & Intent 32 · VII, 23

Activity pada Aplikasi Android 32 · XII

Advertising Click Fraud *adalah jenis malware yang memungkinkan penyerang membajak perangkat untuk menghasilkan pendapatan melalui klik iklan palsu.* · 95

akses internet . · 67

Akses ke antarmuka komunikasi (termasuk pengenal perangkat keras dan kekuatan sinyal jika berlaku, dan permintaan untuk mengaktifkannya), seperti Bluetooth , Wi-Fi , Komunikasi jarak dekat (NFC), dan lainnya. · 67

Akses ke kamera internal dan / atau mikrofon perangkat . · 67

Akses ke penyimpanan dan informasi pribadi, seperti kontak , janji temu kalender, dll. · 67

Akses ke sensor biometrik , termasuk pembaca sidik jari dan sensor kesehatan lainnya .. · 67

Alat React Native memerlukan beberapa variabel lingkungan untuk disiapkan untuk membangun aplikasi dengan kode asli. · 22

Algoritma Hashing Populer · 79

Algoritma Message Digest (MD) · 79

Algoritme · 83, 116

Algoritme Pointcheval–Stern signature · 83

Alhamdulillah, segala puji selalu Kami **Security***' dengan lancar tanpa kendala berarti.* · III

android · XII, 19, 23, 30, 33, 51, 53

Android SDK versi terbaru · 24

Android Studio menginstal Android SDK terbaru secara default. Membangun

aplikasi React Native dengan kode asli, bagaimanapun, membutuhkan Android 9 (Pie) SDK secara khusus. Android SDK tambahan dapat diinstal melalui SDK Manager di Android Studio. · 20
Aspek Keamanan · 82
Aturan dan tanggungjawab, merupakan proses menyusun aturan dan penanggungjawab, yang mengatur kegiatan sebagai upaya untuk menurunkan risiko keamanan informasi yang bersumber dari ancaman dan kelemahan. · 17
Availability · V, 1, 4, 71
Availability 4 · V

B

Backdoor
Metode rahasia untuk melewati batasan keamanan untuk mendapatkan akses tidak sah ke sistem komputer. Dengan kata sederhana, pintu belakang adalah bagian kode yang memungkinkan orang lain masuk dan keluar dari sistem tanpa terdeteksi. [12] · 94
Broadcast Receiver · VII, 52
Broadcast Receiver 34 · VII
Bug. · 100

C

C# · 45
C++ · 45
Class
yaitu cetakan dari object. Sebuah class berisi kode-kode yang menjelaskan bagaimana sebuah object akan berperilaku dan berinteraksi satu sama lain. Class dalam pemrograman diartikan seperti sebuah cetakan atau template. · 46
Confidentiality / Privacy · V, 3
Confidentiality / Privacy 3 · V
Content Provider · VII, 53
Content Provider 35 · VII
Cyber Threat & Mobile Threat · 5

D

Data Privacy · VIII, 87, 89
Data Privacy 62 · VIII
Hogben, Giles · 122
Dekripsi (Decrypt) · VIII, 75
Dekripsi (Decrypt) adalah cara merubah kembali data yang tadinya telah di enkripsi menjadi sebuah kode tertentu kemudian dikembalikan ke bentuk semula, contohnya seperti kode-kode yang berbentuk hash dan binary. · 75
Dekripsi (Decrypt) 53 · VIII

Delphi · 45
Digital Signature · VIII, XIII, 80
Digital Signature 57 · VIII

E

Enkapsulasi (Pembungkusan)
Merupakan pelindung program dan data yang sedang diolah. Enkapsulasi mendefinisikan perilaku dan melindungi program dan data agar tidak diakses secara sembarangan oleh orang lain. · 46
Enkripsi (Encrypt) · VIII, 75
Enkripsi (Encrypt) 52 · VIII
Ethical Challenges in Information thics · VI, 9, 10, 13
Ethics 8 · V
European Telecommunications Standards Institute (2011). · 123
Expander

F

Faster Development
Metode ini didukung oleh banyak library objek, sehingga mempercepat penyelesaian program dan juga projek berikutnya. · 44
Free WIFI. · 102
Freeware. · 101
Fungsi Hash 56 · XIII
Fungsi Hashing
Inti dari Algoritma Hashing · 77

G

H

Higher Quality Software
Faster developmentpun akan memberikan lebih banyak waktu dan sumberdaya untuk proses verifikasi software. · 45
Hindari memberikan informasi pribadi · 96
http
//docs.lucidinteractive.ca/index.php/Cracking_WEP_and_WPA_Wireless_Networks · 120
//www.wi-foo.com/ · 120

I

Improved Software Development Productivity
Sistem program dapat dimodifikasi tanpa melibatkan banyak modul dimana hanya objek saja yang terlibat. Selain itu sistem program dapat dikembangkan sampai skala paling kompleks. · 44
Improved Software Maintainability

Bagian dari software dapat dengan mudah di maintenance jika ada perubahan meskipun dalam skala yang cukup besar. · 44
In Code
instal aplikasi hanya dari sumber tepercaya · 96
Instalasi SDK 19 · XII
Integritas
Merupakan aspek dimana keaslian pesan terjaga walaupun dikirim melalui jaringan yang rentan terhadap serangan, namun dapat dipastikan bahwa data atau informasi yang dikirim tidak diubah oleh orang yang tidak berhak. · 83
Integrity · V, 1, 4
Integrity 3 · V
iOS memberlakukan persyaratan serupa untuk izin yang akan diberikan pada waktu proses, dengan kontrol tertentu ditawarkan untuk mengaktifkan Bluetooth, Wi-Fi, dan pelacakan lokasi. [5] [6] · 68
Istilah-Istilah Dalam Pemrograman Berorientasi Objek · 44, 46
Itulah bahasan ringkas mengenai pemrograman berorientasi objek. Untuk lebih lengkapnya kamu bisa mencari referensi buku-buku atau ebook tentang OOP JAVA, PHP, dan bahasa pemrograman lainnya. · 47

J

Jailbreak dapat melemahkan keamanannya secara signifikan, membuka lubang keamanan yang mungkin belum terlihat. · 97
Java · 2, 45
Jelaskan batasan teritori organisasi yang terikat atau harus patuh terhadap Network And Internet Defense · 120
Jelaskan Jenis-jenis ancaman terhadap Keamanan Data dan Informasi · 92
Jelaskan salah satu metode otentikasi multi-faktor dan diskusikan pro dan kontra penggunaan otentikasi multi-faktor. · 70
Jelaskan unit organisasi yang bertanggung jawab dalam mengembangkan Network And Internet Defense · 120
Jelaskan waktu yang tepat bagi sebuah organisasi untuk menyusun Network And Internet Defense · 120
Jenis Broadcast pada Aplikasi Android 35 · XII
Jenis Intent Pada Aplikasi Android 33 · XII

Jenis Malware Seluler · IX, 94
Jenis Malware Seluler 68 · IX
Jenis Servis pada Aplikasi Android 34 · XII
Jenis Spyware · IX, 101
Jenis Spyware 75 · IX

K

Kata sandi non-teks, di mana simbol atau gambar dapat dipilih dari bidang yang dibuat secara acak. · 69
Kata sandi satu kali (OTP) *melalui aplikasi telepon atau pesan* SMS. · 70
Keamanan jaringan (mobile network security) terdiri dari kebijakan dan praktik untuk mencegah dan memantau akses yang tidak sah, penyalahgunaan, maupun penolakan yang terjadi di jaringan komputer. · 119
Kelemahan Pemrograman Berorientasi Objek · 44
Kelemahan Sistem Operasi. · 102
Keluar dari situs setelah Anda melakukan pembayaran · 96
Keunggulan Pemrograman Berorientasi Objek · 44
Key Management · VIII, XIII, 79
Key Management 57 · VIII
Komponen-komponen apa saja yang ada pada Network And Internet Defense · 120
Konflik kepentingan · 10
Konsultasikan opsinya tergantung pada sistem operasi perangkat Anda. Dengan membuat cadangan untuk ponsel cerdas atau tablet Anda, Anda dapat dengan mudah memulihkan data pribadi Anda jika perangkat hilang, dicuri, atau rusak. · 97
Kriptografi adalah ilmu yang mempelajari bagaimana membuat suatu pesan yang dikirim pengirim dapat disampaikan kepada penerima dengan aman . · 73
Kunci Aktivasi *mencegah orang lain menggunakan perangkat Anda yang terhapus dari jarak jauh.* · 58

L

Locate - Lock · VII, 56
Locate - Lock 38 · VII
Logika atau bom waktu adalah teknik pintu belakang klasik yang memicu aktivitas berbahaya berdasarkan peristiwa, penggunaan perangkat, atau waktu tertentu . · 7

M

MALICIOUS ACTIVITY *by* ATTACKER: · 5

Malware. · 102
Manajemen kunci menyangkut kunci di tingkat pengguna, baik di antara pengguna atau sistem. Ini berbeda dengan penjadwalan kunci , yang biasanya mengacu pada penanganan internal kunci dalam pengoperasian sandi. · 80
Method
yaitu fungsi yang ada di dalam class. Method dapat diakses dengan tiga jenis user atau modifier. Dalam pemrograman objek method dapat menyimpan state dalam variabel dan mengimplementasikan behaviournya menggunakan method. · 46
MIT IST. "OpenID Connect Authorization". · 72
Mobile Authentication adalah verifikasi identitas pengguna melalui penggunaan perangkat seluler dan satu atau beberapa metode autentikasi untuk akses aman. · 69
Mobile Authentication dapat digunakan untuk mengotorisasi perangkat seluler itu sendiri atau sebagai bagian dari skema otentikasi multifaktor untuk masuk ke lokasi dan sumber daya yang aman. · 69
***Mobile Malware**, dalah perangkat lunak berbahaya yang dirancang khusus untuk menargetkan perangkat seluler, seperti ponsel cerdas dan tablet, dengan tujuan memperoleh akses ke data pribadi.* · 92
MOBILE SECURITY · I
Mobile Security adalah perlindungan ponsel pintar, tablet, laptop, dan perangkat komputasi portabel lainnya, dan jaringan tempat mereka terhubung, dari ancaman dan kerentanan yang terkait dengan komputasi nirkabel. · 1
Mobile Security juga dikenal sebagai Wireless Security. · 2
Mobile Threat 8 · XII
Mobile virus hack Google Play user on Brazil · 98

N

Net · 45
Mickens, James W.
Non-repudiasi, atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya

suatu informasi oleh yang mengirimkan/membuat. · 74
Non-repudiation
Merupakan aspek yang berhubungan dengan keaslian pengirim pesan, dapat dipastikan bahwa pengirim adalah orang yang sebenarnya diharapkan mengirimkan data.[5] · 83

O
Object
dalam dunia pemrograman objek diartikan sebagai bagian dari sebuah program. Dimana di dalamnya dihubungkan beberapa variable dan method yang salin berkaitan satu sama lain · 46
Objek-objek dalam dunia nyata memiliki 2 karakteristik yaitu status dan perilaku. Contoh
Sepeda mempunya status (Jumlah pedal, gir, dan ban). Sedangkan perilakunya (Mengerem, Mempercepat, dan Ubah gir). · 45
OS X · 27
Otentikasi out of band, di mana pengguna melakukan panggilan untuk mendapatkan otentikasi. · 70
Overview Malware 67 · XIII

P
Pasang aplikasi keamanan seluler · 97
0
pemberitahuan desktop · 68
Pemberitahuan pengguna aplikasi · 109
Pemisalan Objek dalam Pemrograman Beriorientasi Objek · 44, 45
Perangkat seluler · 6, 8, 56, 66, 70
Perangkat Virtual Android · 20, 23
Performa (Intel ® HAXM) · 20
Periksa ulang URL situs - Pastikan alamat web sudah benar sebelum masuk atau mengirim informasi sensitif. Pertimbangkan untuk mengunduh aplikasi resmi bank Anda. · 96
Periksa ulang URL yang dipersingkat dan kode QR, mereka dapat mengarah ke situs web berbahaya atau langsung mengunduh malware ke perangkat Anda. · 96
Perl · 45
Perlakukan penghapusan jarak jauh sebagai upaya terakhir kecuali jika datanya cukup sensitif dan / atau ponsel sudah lama hilang dan dibuka kuncinya. · 58

Permission · VIII, 66
Permission 46 · VIII
Phishing adalah ketika seseorang berpura-pura menjadi orang lain untuk mencuri uang atau data, atau informasi untuk mendapatkan uang. Phishing adalah cara yang paling umum di mana kebocoran berskala organisasional terjadi. · 115
Phishing Dan Spoofing. · 100
PHP · 45
Pilih tab · 21
Platform Android SDK · 20, 21
Platform Android SDK 28 · 21
Prinsip Keamananan Data 3 · XII, 3
Prioritas aksi tersebut sebagai pengaman untuk menjaga kerahasiaan, keutuhan dan ketersediaan informasi, dengan penentuan control keamanan yang sesuai dengan tujuan dan sasaran yang diinginkan. · 17
Privasi informasi adalah hubungan antara pengumpulan dan penyebaran data , teknologi , ekspektasi publik terhadap privasi , dan masalah hukum dan politik yang mengelilinginya. Ini juga dikenal sebagai privasi data atau perlindungan data . · 86
Property
merupakan variable yang dideklarasikan di dalam sebuah class, tetapi tidak berada di dalam fungsi atau method dari suatu class. · 46
Python · 45

R

RSA · 79, 83
RSA kombinasi SHA · 83
Ruby · 45
h). · 122
Run · 23
Running Device Path 26 · XII, 38
Runtime program lebih lambat · 45

S

Schnorr signature · 83
SDK Android · 20, 22
SDK diinstal, secara default, di lokasi berikut: · 22
SDK Manager dapat diakses dari layar · 20
SDK Manager juga dapat ditemukan dalam dialog · 21
***single sign-off** atau **single log-out** (**SLO**) adalah properti di mana satu tindakan keluar akan menghentikan akses ke beberapa sistem perangkat lunak.* · 61

Secure Hash Algorithm (SHA) · 79
sensor · 10, 68
Serangan berbasis Bluetooth · 118
Serangan berbasis Bluetooth 92 · XI
Serangan berdasarkan jaringan GSM · 116
Serangan berdasarkan jaringan GSM 90 · XI
Serangan berdasarkan Wi-Fi · 117
Serangan berdasarkan Wi-Fi 91 · XI
Serangan spyware pada smartphone umumnya terjadi dalam tiga cara, yaitu; · 102
Sertifikat digital menggunakan infrastruktur kunci publik. · 69
Services · VII, 51, 72, 124
Services 33 · VII
SHA. Baik SHA1, SHA2, atau SHA3. · 83
Siapa target phishing? · 115
Siapa Target Spyware · IX, 102
Siapa Target Spyware 77 · IX
Siemens (2010). · 123
Halbronn, Cedric · 121
Siklus Kerja Spyware 74 · XIII
Siklus Mobile Phishing 88 · XIII
Single Sign-On yang benar memungkinkan pengguna untuk masuk sekali dan mengakses layanan tanpa memasukkan kembali faktor otentikasi. · 61
Single Sign-On. · VII, 61
Single Sign-On. 41 · VII
Situs · 65, 98, 123
Spoofing Titik Akses 91 · XIII
).

T

Taksonomi · IX, 93
Taksonomi 68 · IX
Taktik Umum Mobile Phishing · XI, 112
Taktik Umum Mobile Phishing 86 · XI
Tanda tangan digital (S) didekripsikan dengan kunci publik yang telah diberikan kepada penerima. Proses ini akan menghasilkan MD (Message Digest). · 82
Tanda tangan digital (S) diletakkan pada pesan M. · 82
Teknik Mobile Phishing 87 · XIII
Teknik Mobile Spyware 78 · XIII
Think Like A Hacker · VI, 16
Think Like A Hacker 14 · VI
Threat · V, XII, 5
Threat 4 · V
***Tiny URLs** adalah URL singkat yang dapat digunakan oleh penyerang untuk mengarahkan pengguna ke konten berbahaya. Karena*

sifatnya yang singkat, mereka cocok untuk serangan SMS phishing dan sering digunakan dalam serangan 'smishing' berskala besar.. · 112
Token otentikasi (yaitu yang OAuth) dari layanan web yang disimpan di penyimpanan sistem untuk berbagi antar aplikasi. · 67
Trojans Perbankan dapat menargetkan berbagai lembaga keuangan, termasuk bank, broker, portal keuangan online, atau dompet digital. Mereka mungkin juga mengirimkan informasi yang dikumpulkan ke server untuk pengambilan. · 101
Trojans. · 101
***Tugas dan Diskusi:** · 17, 47, 53, 59, 70, 84, 91, 97, 104, 120*
Tuliskan langkah-langka pengerjaannya · 47
Two Factor Authentication. · VIII, 63
Two Factor Authentication. 43 · VIII

U

Ubuntu · 27, 28
USB Debugging-2 24 · XII, 27
USB Debuging 23 · XII

V

VULNERABILITY: · 7

W

WebPermissions · 68
Wipe · VII, 57
Wipe 38 · VII

Y

Z