PERTEMUAN 18:

MOBILE SECURITY

A. TUJUAN PEMBELAJARAN

Pada bab ini akan dijelaskan mengenai keamanan sistem operasi jaringan, Anda harus mampu:

1.1 Risiko data storage

1.2 Android

1.3 Blackberry

B. URAIAN MATERI

Tujuan Pembelajaran 1.1:
Mobile Security

Risiko Data Storage

Risiko Keamanan Perangkat Kekuatan komputasi laptop tentu tak sama dengan komputasi ponsel. Saat ini program enkripsi data pada ponsel masih belum sematang sama dengan aset-aset lainnya, perangkat mobile 1 program enkripsi pada laptop.

Risiko Fisik

- Risiko fisik menjadi risiko paling mendasar yang dimiliki oleh perangkat mobile.
- Risiko fisik ini mulai dari akses oleh orang yang tak berhak hingga risiko kehilangan.
- Mengaksesnya menjadi persyaratan untuk keamanan perangkat mobile.

Risiko Strong Password

Aplikasi Internet Banking diharuskan memiliki password yang kuat. Akses oleh orang yang tak berhak pada perangkat yaitu password dengan minimal panjang karakter mobile.Dapat berupa:

- Seseorang yang berpura-pura,
- Mengatakan ingin meminjam melakukan telepon atau mengirim SMS
- Kombinasi huruf besar/kecil
- Kombinasi alfanumerik dan simbol, , atau perangkat tentu akan dengan mudah.

Penyerang saat berada di dekatnya.

- Format pengetikan password di aplikasi mobile yang mengatakan URL tersebut adalah URL
- Risiko kehilangan sebaiknya dari awal sudah ada di pikiran pengguna perangkat mobile saat mengacu pada situs yang ia buat sendiri, dengan memutuskan menggunakannya. Berbeda dengan server yang bisa diletakkan pada ruangan terkunci, tidak ada mekanisme pengamanan akses.

Fisik untuk perangkat mobile. Mobile namun tetap memungkinkan bagi aplikasi untuk bagaimana ia akan mengetikkan delapan karakter ponselnya? Tentu akan lebih sulit dilakukan pada sudah diluncurkan.

Berikut ini adalah beberapa keyboard ponsel:

- model ketik tiga kali ABC,
- prinsip-prinsip keamanan dalam mendesain model QWERTY
- Keyboard virtual touch aplikasi mobile: screen

Akibatnya ia akan memilih untuk tidak menggunakan aplikasi Internet Banking mobile saja dan dari sisi bank akan kehilangan penggunanya.

Risiko Internet Browsing

Identifikasi dan Proteksi Data Sensitif pada Perangkat Mobile. Sebelum mendesain aplikasi mobile, lakukan identifikasi terhadap semua data yang akan diproses. Tentukan tingkat sensitivitas data. Data yang bersifat publik tidak perlu mendapatkan mekanisme pengamanan. Data yang bersifat confidential harus mendapatkan mekanisme dapat dikatakan nyaris takkan bisa. Hal ini akan pengamanan. Sedapat mungkin, desain aplikasi dengan data confidential tidak tersimpan diperangkat mobile. Jika tidak memungkinkan, data confidential yang tersimpan pada perangkat mobile harus terlindungi. URL shortener, untuk mengarahkan ke situs palsu.

- Risiko Privasi Lokasi
- Pastikan Data Sensitif Terlindungi Saat Transit

Perangkat mobile memiliki beragam mode

Bagi Gayus Tambunan saat kabur dari penjara isu koneksi untuk tersambung ke Internet: apakah lokasi akan menjadi sangat kritikal. Tentu ia tak BIS, GPRS, Edge, WiFi, dst. Tidak semua mode mau tertangkap basah saat kabur dari penjara. koneksi ini terenkripsi, contoh paling sederhana Bagaimana apabila ponsel yang digunakan Gayus adalah public wifi. Selalu mengirimkan posisi koordinat GPS-nya?

Saat ini isu privasi lokasi menjadi isu yang hangat menggunakan TLS/SSL (Transport Layer dibicarakan. Ponsel iPhone dan Android Security/Secure Socket Layer) saat dikabarkan mengirimkan lokasinya. mengirimkan/menerima data sensitif.

Jalankan Aplikasi dengan Hak Akses Minimum

sistem operasinya tentu akan memilikinya Desain klien aplikasi mobile yang dapat risikonya sendiri-sendiri. Baik Android, iPhone, dijalankan dengan hak akses minimum yang BlackBerry, Symbian, Windows Phone, masing- diperlukan. Contohnya aplikasi cukup bisa masing memiliki risiko. Risiko sistem operasi ini dijalankan user biasa, tidak harus sebagai melekat pada perangkat mobile tersebut. Contoh admin/root; jika aplikasi tidak membutuhkan risiko sistem operasi adalah jailbreak atau akses ke servis kamera, maka tak perlu diberikan berusaha mendapatkan akses root pada perangkat. akses ke servis kamera. Model hak akses minimum ini akan meminimalisir risiko akses yang tak perlu dan memastikan aplikasi bisa

Ikuti Praktik Secure Coding

Keamanan seharusnya diawali dari awal, bukan dikembangkan pada aplikasi mengikuti praktik secure didasarkan pada pengujian di akhir saat aplikasi coding.Misalnya: input validation, output. Layar ponsel tidak sebesar layar laptop. Jadi menampilkan URL secara lengkap pada ponselmembuat serangan phishing semakin mudah.

Pengguna tidak dapat selalu melihat URL yang diaksesnya. Penyerang hanya perlu memancing pengguna membuka, misalnya menggunakan encoding. Pengembang perlu melakukan static analysis dalam proses SDLC untuk mengetahui keamanan source code .

Lainnya, tanda tangani aplikasi saat akan mengupload (signed application) untuk menjaga integritas aplikasi.

Pada bagian ini akan dijelaskan metodologi pengujian keamanan aplikasi mobile.

- Metodologi Umum

Berikut ini adalah metodologi umum dalam melakukan pengujian aplikasi mobile.
1. Memahami proses bisnis aplikasi (Understanding application business process). Langkah pertama yang perlu dilakukan dan akan menjadi pondasi dalam melakukan pengujian adalah dengan memahami proses bisnis aplikasi. Misalnya dengan mengetahui karakteristik aplikasi apakah berupa aplikasi transaksional atau aplikasi informasional. Aplikasi yang bersifat transaksional akan memiliki risiko finansial sementara aplikasi informasional akan memiliki risiko integritas data. Apabila penyerang memiliki motif ekonomi dalam melakukan penyerangan maka aplikasi transaksional akan dipilih untuk diserang.

2. Menguraikan aplikasi (Decomposing application)
Setelah memahami proses bisnis dilanjutkan dengan menguraikan komponen penyusun aplikasi. Apabila pengujian dilakukan dengan cara black box maka penguraian aplikasi dilakukan dengan cara fingerprinting.
Dengan melakukan penguraian aplikasi dapat dilakukan analisis terhadap desain dan arsitektur aplikasi mobile ini.

Komponen server apa saja yang terlibat, berikut bagaimana aplikasi mobile didistribusikan.

- Mengembangkan skenario serangan (Developing attack scenarios)

Susun skenario serangan-serangan yang mungkin dilakukan berikut penjelasan kondisi yang diperlukan untuk melakukan serangan tersebut. Faktor kemungkinan dan dampak dari serangan juga perlu dijelaskan agar risiko setiap serangan dapat terlihat dengan jelas.
Misalnya dari hasil penguraian aplikasi diketahui bahwa terdapat 2 server yang terlibat berikut aplikasi mobile.
Skenario serangan pertama adalah melakukan serangan pada sisi server misalnya dengan melakukan: penetration testing, vulnerability assessment, web application testing, dst. Selanjutnya diikuti dengan skenario kedua yaitu mobile application assessment.

- Menentukan prioritas risiko (Prioritizing risks)

Umumnya pengujian dilakukan dengan batasan waktu. Tentu tak semua skenario dapat dilakukan. Oleh karena itu perlu ditentukan skenario yang menjadi prioritas.

- Melakukan pengujian (Conducting tests)

Skenario dieksekusi dengan prioritas. adalah skenario yang memiliki risiko tertinggi. Perhitungan risiko dihitung dari perkalian kemungkinan dengan dampak dari setiap skenario serangan.

- Menganalisis hasil pengujian (Analyzing test results)

Selanjutnya hasil pengujian dianalisis, skenario serangan yang menghasilkan temuan.

- Merekomendasikan perbaikan (Recommending fixes).

Menyusun rekomendasi perbaikan dari temuan yang ditemukan.

- Mobile Security Assessment

Mobile security assessment dapat dilakukan dengan melakukan pengujian pada aplikasi yang sedang dijalankan atau pada aplikasi yang sedang tidak dijalankan.

Dinamis

Pengujian dengan metode analisis dinamis berlaku umum tanpa melihat sistem operasi pada pengujian dinamis, pengujian perangkat mobile. Untuk dapat menganalisis dilakukan pada aplikasi yang sedang network traffic disusun skenario berikut: gunakan berjalan. Pengujian dinamis dapat intercepting proxy untuk melakukan analisis dilakukan dengan cara: terhadap network traffic aplikasi mobile dengan servernya.

Debugging dapat dilakukan langsung pada Konfigurasikan koneksi perangkat mobile agar perangkat ataupun pada emulator. melalui interepting proxy terlebih dahulu sebelum menuju server. Lakukan analisis terhadap traffic yang lalu-lalang. Perhatikan apakah data sensitif

Melakukan analisis remote services yang terkirim dalam keadaan tak terenkripsi. seperti HTTP/SOAP/dll

Menganalisis request & respond scan/fuzz, jika intercepting proxy yang digunakan menggunakan intercepting proxy. memiliki fitur scan/fuzz. Intercepting proxy yang dapat digunakan antara lain: Paros Proxy.

Analisis Statis (Static Analysis)

Pada pengujian statis, pengujian dilakukan dengan kondisi aplikasi tidak OWASP ZAP Proxy, Burp Proxy.

Pengujian dengan Analisis Statis dijalankan

Pengujian statis dilakukan Pengujian dengan metode analisis statis dilakukan dengan menganalisis source code aplikasi. dengan menganalisis source code. Pada binary Pengujian statis dilakukan dengan cara aplikasi dilakukan reversing code untuk sebagai berikut: mendapatkan source code aplikasi tersebut.

1. Ekstrak aplikasi dari perangkat atau dapatkan paket aplikasi dari pengembang
2. Melakukan source code review. Jika source code memang tersedia maka tak perlu melakukan reverse engineering ataupun disassembling namun keduanya tetap boleh dilakukan untuk mengetahui risiko

Android

Jack Maninno dalam blognya menulis bagaimana cara melakukan reversing code aplikasi Android. Kebocoran dan terlalu banyak data yang terungkap seperti: kredensial, kunci enkripsi, sumber daya pada sisi server; pada sisi klien merupakan hal yang berpotensi menjadi risiko. Dengan melakukan reversing code aplikasi akan

a. Melakukan debugging pada aplikasi.
b. Melakukan analisis network traffic

Perhatikan webservices yang dieksekusi. Lakukan didapatkan source code aplikasi. Selanjutnya dari iPhone source code ini dilakukan analisis untuk mencari Aplikasi untuk iPhone ditulis menggunakan bahasa objective-C. Untuk melakukan reversing Tools yang perlu digunakan untuk melakukan code pada aplikasi iPhone dapat menggunakan reversing code aplikasi Android adalah: tool otool atau class-dump-x.

Perangkat mobile.

- Langkah pertama adalah melakukan pull berkas ini dapat memberikan gambaran secara utuh APK aplikasi Android. mengenai keamanan perangkat mobile.
- Program untuk mengekstrak berkas ZIP. Tulisan ini dibuat dengan mengacu pada setelah mengekstrak berkas APK, perhatikan berkas manifest dan berkas DEX. Pada berkas manifest terdapat beragam informasi seperti: permission, intent filters .
- Gunakan dex2jar untuk mengkonversi berkas dengan format DEX menjadi JAR. Selanjutnya, buka kompresi file hasil konvers dex2jar.
- Langkah terakhir gunakan java decompiler untuk Bolsen. Coddec mendapatkan source code aplikasi.

Tool lain untuk melakukan pengujian keamanan c-released/

Aplikasi Android adalah c-ray. C-ray adalah scanner security untuk aplikasi Android. Hasil analisis c-ray akan menunjukkan tingkat keamanan interface aplikasi Android. Denim Group merilis program smartphone dumbapps yang berisi script perl untuk melakukan reversing code mobile application secara otomatis. Versi saat ini sudah mendukung aplikasi Android dan iPhone.

BlackBerry

Dr Olsen telah merilis program coddec untuk melakukan reversing code aplikasi BlackBerry. Coddec merupakan kependekan dari cod decompiler. Cod adalah ekstensi berkas aplikasi BlackBerry.

C. SOAL LATIHAN/TUGAS

1. Jelaskan mengembangkan skenario serangan ?
2. Pengujian keamanan c-released ?

DAFTAR PUSTAKA

Buku

Bambang Hariyanto. 1997. Sistem Operasi, Bandung:Informatika Bandung.

Dali S. Naga. 1992. Teori dan Soal Sistem Operasi Komputer,Jakarta: Gunadarma.

Silberschatz Galvin. 1995. 4 Edition Operating System Concepts: Addison Wesley.

Sri Kusumadewi. 2000. Sistem Operasi. Yogyakarta: J&J Learning.

Setiawan Agung.2005, Pengantar Sistem Komputer Edisi Revisi, Bandung: Informatika

Tanenbaum, A.1992. Modern Operating Systems.New York: Prentice Hall

Link and Sites:

Unswagati. 2010. Keamanan Jaringan Komputer.
http://unswagati-crb.ac.id/component/option,com_phocadownload/Itemid,73/download, 55/id,11/view,category/ . Tanggal akses 10 November 2012.
http://www.ilmukomputer.com
http://vlsm.bebas.org
http://www.wikipedia.com