 ISSN : 2338-2899

SISTEM KEAMANAN SMARTPHONE DALAM APLIKASI MOBILE LEARNING

Sy. Yuliani[1)], **Apri Junaidi**[2)]

[1), 2)] *Teknik Informatika, Fakultas Teknik, Universitas Widyatama*
Unversitas Widyatama
Jl. Cikutra No. 204 A Bandung
Email : sy.yuliani@widyatama.ac.id[1)], apri.junaidi@widyatama.ac.id[2)]

Abstrak

Berkembang pesatnya perangkat mobile atau yang sering di sebut dengan Smartphone, dengan segala kemudahan dan fasilitas teknologi yang ditawarkan, sehingga smartphone tidak hanya berfungsi sebagai alat berkomunikasi, tapi juga dapat digunakan dalam proses pembelajaran yang kemudian dikenal dengan nama Mobile Learning.

Dalam penggunaan sehari hari faktor keamanan dalam mobile learning juga terhadap sistem smartphone juga sangat diperhatikan, dalam paper ini, penulis memaparkan beberapa bentuk serangan terhadap sistem smartphone, arsitektur sistem mobile learning, serta mengusulkan sebuah sistem keamanan dalam mobile learning.

Kata kunci: *mobile learning, keamanan sistem mobile learning, android, keamanan sistem android, smartphone..*

1. Pendahuluan

Perkembangan perangkat mobile *(smartphone)* yang berkembang pesat memberikan dampak pada perkembangan dunia pendidikan seperti Perkembangan elearning. Dalam proses pembelajaran menggunakan smartphone. Ada beberapa sistem operasi yang digunakan dalam smartphone seperti : Symbian OS, Windows Mobile, Android and iPhone OS [1]. Dalam sistem Mobile learning perlu dipertimbangkan masalah keamanan, yang dapat menggangu proses pembelajarann dan penggunaan aplikasi yang di gunakan dalam smartphone atau sistem lain.

Penjualan perangkat mobile juga mencapai angka 420 juta smartphone. [1], dengan penggunaan smartphone yang begitu banyak memang perlu dipertimbangkan penggunaan smartphone dalam kegiatan proses pembelajaran.

2. Landasan Teori

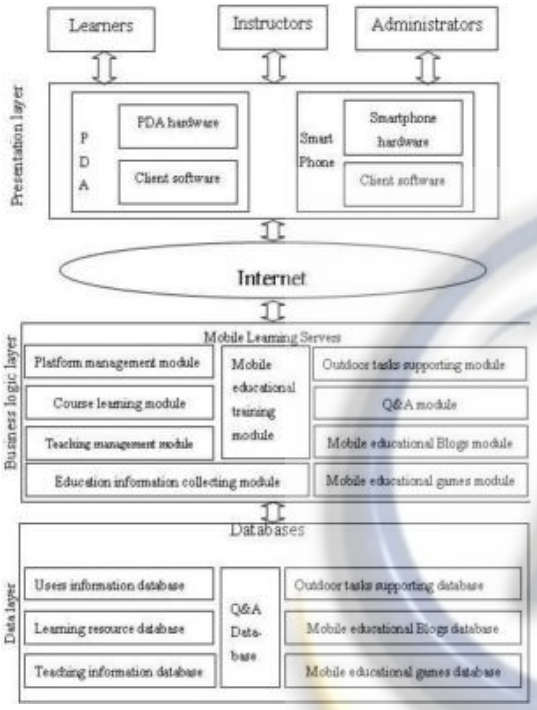
a. Pendidikan

Beberapa jenjang pendidikan secara normalnya ditempuh dalam beberapa tingkatan, sekolah dasar, sekolah menengah pertama, sekolah menengah atas serta perguran tinggi atau memasuki Universitas. Setiap fase pendidikan yang disebutkan diatas, interakasi guru dan murid hanya dapat berlangsung selama berada disekolah, selanjutnya peran orang tua menggantikan peran guru dirumah, mengawasi, mengontrol semua proses pendidikan anak anak di sekolah. Pemerintah Indonesia sangat mendukung proses pendidikan seperti tersedia sarana pembelajaran, beasiswa untuk anak anak yang berprestasi sehingga dapat menghasilkan siswa yang berkualitas dan memiliki keilmuan yang bagus. Perkembangan teknologi informasi memberikan dampak dalam dunia pendidikan, pendidikan yang biasa diajarkan secara formal dikelas, saat ini bisa menggunakan teknologi yang di sebut pendidikan jarak jauh[2][3][4] tanpa mengesampingkan peran orang tua dan guru sebagai pemberi pendidikan serta mengawasi proses pembelajaran

b. Mobile Learning

Mobile learning saat ini menjadi suatu yang hal yang penting yang mengacu pada penggunaan perangkat mobile seperti Personal Data Assistant (PDA), handphone, smartphone, laptop dan tablet PC dan proses belajar mengajar, dapat juga disebut mobile learnig adalah bagian mobile computing dan e-learning[5] Mobile learning juga bisa diartikan suatu proses belajar mengajar yang baru dan memiliki prinsip, siapapun, dimanapun dan kapanpun informasi yang dibutuhkan dalam mendukung pembelajaran dapat digunakan[6]. Beberapa kelebian dari mobile learning: Mobility, Real Time, Interactive, Virtualization, Digitization, Individuation. Mobile Learning adalah sesuatu cara pembelajaran yang baru, baik peserta didik, siapapun, dimanapun, kapanpun bisa mendapatkan informasi yang diperlukan dalam proses belajar mengajar, pendapat lain tentang mobile learning yaitu media pembelajaran yang

memungkinkan perserta didik dapat belajar kapan saja dan dimana saja dengan menggunakan perangkat smarthpone sebagai terminal penerima informasi, sehingga pembelajaran lebih interaktif, efisien dalam berkomunikasi antara pengajar dan peserta didik [6]. Gambar 1. Merupakan bentuk arsitektur mobile learning dengan beberapa komponen seperti : perserta didik, instruktur, administrator, jaringan internet, mobile learning service serta database sebagai tempat pengolahan data.



Gambar 1. *Arsitektur Mobile Learning*

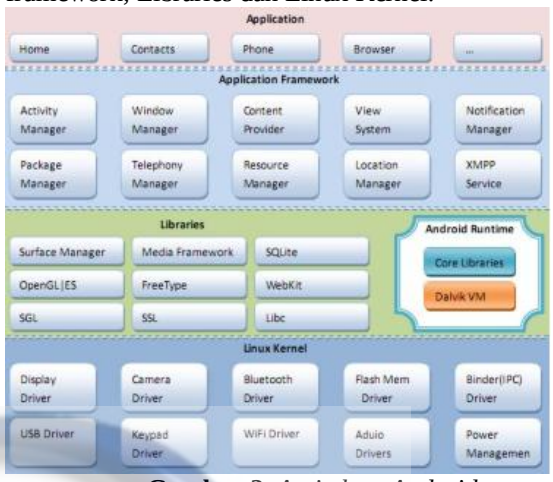
c. Android

Sejak diluncurkan pada 2008, Android telah berkembang menjadi salah satu smartphon terlaris. Tiga alasan utama bahwa Sistem operasi Android adalah keterbukaan platform android, aplikasi mudah didapat di Google Play Store; dan kompatibilitas perangkat dengan aplikasi dari pihak ketiga vendor [7].

Android platform yang menggunakan bahasa pemrograman Java, juga merupakan software stack untuk perangkat mobile yang mencakup sistem operasi, middleware dan kunci aplikasi. Android SDK menyediakan alat dan API diperlukan untuk mulai mengembangkan aplikasi [8].

d. Arsitektur Android

Berikut arsitektur android dalam bentuk bagan yang terdiri dari beberapa lapisan: Application, Application framework, Libraries dan Linux Kernel.



Gambar 2. *Arsitektur Android*

e. Sistem Operasi Smarthphone

Dalam perkembangan teknologi komunikasi saat ini hadirlah berbagai macam alat komunikasi yang kita kenal dengan nama smartphone, untuk berinteraksi dengan user smartphone tersebut memiliki sistem operasi yang khusus di rancang untuk peralatan kecil seperti smartphone, berikut sistem operasi yang mendukung smartphone: Android, Symbian, iOS, Reseach In Motion, Microsoft Windows Mobile, Linux dan lain lain.[9][1].

f. Keamanan Smarthphone Android

Android merupakan sistem operasi yang sangat populer saat ini, dan beberapa teknik pengamanan untuk sistem operasi ini dijabarkan sebagai berikut:

1. Sandboxing Mechanism : dimana android mampu memabatasi satu aplikasi dengan aplikasi yang lainnya, serta mengatur ID dari setiap aplikasi yang sedang berjalan.
2. Application Permission Mechanism: Android juga menggunakan sistem pengamanan pada level aplikasi, seperti izin untuk mengkakses sebuah sumber daya dideklarasikan pada saat sebuah aplikasi akan di install, seperti izin akses internet, akses kamera, menulis sms dan lain lain [9].

Dalam penelitian lain, ada beberapa strategi yang digunakan untuk mengamankan aplikasi android seperti: Mobile Malware, Secure Mobile Coding, Cryptography on Mobile Device, Access Control, Mobile Privacy[10]

g. Mobile Malware

Malware adalah sejenis musuh yang mengganggu, perangkat lunak atau kode program seperti Trojan, rootkit dan backdoor. Penyebaran malware sering di lakukan dalam bentuk spam, dalam file lampiran email atau dalam link sebuah website [1].

Berikut beberapa malware yang dikenal: virus, worm, Trojan, rootkits dan bootnet [1]. Tabel 1. Menampilkan daftar malware yang dikenal saat ini.

3. Keamanan dalam Mobile Learning

Berdasarkan daftar pustaka yang dipelajar, keamanan yang ada dalam smartphone android dapat di terapkan pada aplikasi mobile learning. Seperti dengan menanamkan unsur keamanan dalam aplikasi seperti memperbaiki dari sisi mobile code, cryptography, enkrispi, steganography serta teknik penyembunyian data lainnya.
Berikut penulis sampaikan usulan bentuk infrastruktur keamanan dalam mobile learning.

Gambar 3. *Arsitektur Mobile Learning Security*

4. Kesimpulan

Berisi berbagai kesimpulan yang di ambil berdasarkan penelitian yang telah dilakukan, penulis mengusulkan suatu cara untuk mengamankan sistem mobile learning dalam bentuk rancangan infrastruktur, dengan menggunakan smartphone berbasiskan Android serta memperhatikan sisi keamanan, maka sebuah sitem mobile learning yang aman bisa didapatkan. Pengembangan tentang keamanan mobile leaning ini bisa diterapkan pada sistem operasi yang lain seperti iOS, Windows Mobile dan lain lain.

Daftar Pustaka

[1] M. La Polla, F. Martinelli, and D. Sgandurra, "A Survey on Security for Mobile Devices," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 1, pp. 446–471, 2013.

[2] R. J. Wardoyo and N. Mahmud, "Benefits and Barriers of Learning and Using ICTs at Open University : A Case Study of Indonesian Domestic Workers in Singapore," 2013.

[3] R. Reis, P. Escudeiro, and N. Escudeiro, "Educational Resources for Mobile Wireless Devices: A Case Study," *2012 IEEE Seventh Int. Conf. Wireless, Mob. Ubiquitous Technol. Educ.*, pp. 264–267, Mar. 2012.

[4] S. Interactions, "Mobile Computing Research and Education : Bridging the Gap between Academia and Industry Ontario College of Art and Design Theme :," pp. 407–408.

[5] G. Liu and Z. Jiao, "The Design of Mobile Learning System for Teachers' Further Education," *2010 Second Int. Work. Educ. Technol. Comput. Sci.*, pp. 730–732, 2010.

[6] Y. Jin, "Research of One Mobile Learning System," *2009 Int. Conf. Wirel. Networks Inf. Syst.*, pp. 162–165, Dec. 2009.

[7] T. Oh, B. Stackpole, E. Cummins, C. Gonzalez, and R. Ramachandran, "Best security practices for android, blackberry, and iOS," *2012 First IEEE Work. Enabling Technol. Smartphone Internet Things*, pp. 42–47, Jun. 2012.

[8] H. Bing, "Analysis and Research of System Security Based on Android," *2012 Fifth Int. Conf. Intell. Comput. Technol. Autom.*, pp. 581–584, Jan. 2012.

[9] S. Khan, M. Nauman, A. T. Othman, and S. Musa, "How secure is your smartphone: An analysis of smartphone security mechanisms," *Proc. Title 2012 Int. Conf. Cyber Secur. Cyber Warf. Digit. Forensic*, pp. 76–81, Jun. 2012.

[10] M. Guo, P. Bhattacharya, K. Qian, and L. Yang, "Authentic learning of mobile security with case studies," *2013 IEEE Front. Educ. Conf.*, pp. 1519–1521, Oct. 2013.

Tabel 1. *Daftar Serangan Malware Smartphone[1]*

Name	Time	Type	Method of Infection	Effects	OS
Liberty Crack	2000	Trojan	Pretend to be a hack	Remove third-party software	Palm OS
Cabir	2004	Worm	Bluetooth connection and copies itself	Continuous scan of Bluetooth, drain phone's battery	Symbian OS
Dust	2004	Virus	File Infector	Infect all executables in root DIR	Windows Mobile
Brador	2004	Trojan	Copy itself in to the startup folder	Open a backdoor	Windows Mobile
Mosquitos	2004	Trojan	Embedded in a game	Send SMS to premium-rate numbers	Symbian OS
Skulls	2004	Trojan	Vulnerability in overwriting system files	DoS	Symbian OS
MetalGear	2004	Trojan	Vulnerability in overwriting system files	Disable virus scanner	Symbian OS
CommWarrior	2005	Worm	Replicates via Bluetooth and MMS	MMS charging	Symbian OS
Doomboot	2005	Trojan horse	Doom 2 video game	Prevents booting and installs Cabir and CommWarrior	Symbian OS
Lasco	2005	Virus	File infection	Add itself to install packages	Symbian OS
Lockinf	2005	Trojan	Vulnerability in OS	Create entries for a new application	Symbian OS
Fakkr	2005	Worm	SMS message	Send SMS to all contacts	Symbian OS
Cardblock	2005	Virus	Fake SIS application	Encrypt memory card with a random password	Symbian OS
CardTrap	2005	Cross-Platform Virus	Auto-start of removable storage	Copy WinKill on the phone	Symbian/Windows OS
Blankfont	2005	Trojan	Replace font files	Fonts not displayed	Symbian OS
Crossover	2006	Cross-Platform Virus	CIL vulnerabilities	Copy to/from mobile/PC	Windows/Mobile OS
Lanum	2006	Worm	E-Mail spreading	Infect registry	Windows Mobile
Fontal	2006	Trojan	Vulnerability in overwriting system files	Device not restart after reboot	Symbian OS
Mobler	2006	Cross-Platform Worm	Dropping Mechanisms	Disable antivirus and infect removable storage	Symbian/Windows OS
Redbrowser	2006	Trojan	Fake Browser	Send SMS continuously	OS-Independent (J2ME)
Wesber	2006	Trojan	Fake Browser	Send SMS to premium-rate numbers (Russia only)	OS-Independent (J2ME)
Acallno	2006	Spyware	Fake Commercial Software	Gather and send information about user's activities	Symbian OS
Lasco	2007	Worm	A worm that spreads over Bluetooth networks	Searching and infecting other phones	Symbian OS
Feak	2007	Worm	Proof-of-concept worm	Sending SMS to contact list with URL	Symbian OS
Flocker	2007	Trojan	It claims to be an ICQ application to trick the user	Sending SMS to a hard coded phone number	Symbian OS
Beselo	2008	Worm	Via MMS and Bluetooth fake application	MMS charging	Symbian OS
InfoJack	2008	Trojan	Attach itself to installation packages	Disable security settings	Windows Mobile
Pmcryptic	2008	Worm	Memory card spreading	Dialing premium-rate numbers	Windows Mobile
Yxe	2009	Worm	SMS containing malicious URL	Send contact lists to external server	Symbian OS
Yxes	2009	Worm/Botnet	SMS containing malicious URL	Send contact lists to external server	Symbian OS
Ikee	2009	Worm	Scanning a IP ranges and SSH	Alter wallpaper	iPhone
ExxiSpy	2009	Spyware	Fake Application	Tracking/log of device's usage	Symbian
Curse of Silence	2009	SMS Exploit	Vulnerabilities in e-mail parsing	Disable SMS functionalities	Symbian OS
ZeuS MitMo	2010	Worm	Fake SMS	Steal bank account information	Cross-Platform
iSAM	2011	Multifarious malware	Scanning IP and connecting to SSH	Collect private information, send malicious SMS, DoS	iPhone