EVALUASI LAYANAN KRIPTOGRAFIPADA PERANGKAT BERBASIS ANDROID

Setiyo Cahyono[1)], Prasetyo Adi W.P[2)]
[1]Program Studi Teknik Persandian, [2]Program Studi Manajemen Persandian,
Sekolah Tinggi Sandi Negara
Jl. Raya Haji Usa, Desa Putat Nutug, Bogor, Jawa Barat, 16330
HP : +62 857 21369938
E-mail : setyo18@yahoo.com[1)], padiwp@gmail.com[2)]

Abstrak

Penelitian ini bertujuan untuk mengetahui layanan kriptografi apa saja yang didukung oleh semua perangkat berbasis android dan Android Virtual Device (AVD). Penelitian dilakukan dengan cara membuat aplikasi yang akan digunakan untuk mengevaluasi fungsi kriptografi yang didukung oleh perangkat berbasis android, menjalankan aplikasi tersebut pada android sdk dan perangkat berbasis android lalu menganalisis data hasil percobaan tersebut untuk mendapatkan kesimpulan. Sebagai hasil penelitian terdapat enam class yang menjadi layanan kriptografi yaitu Crypto, Signature, Message Digest, Mac, Key Agreement dan SSL Context. Delapan Layanan algoritma kriptografi yaitu AES, DES, HMACMD, HMACSHA, Diffie Hellman, SHA-384, SHA-512, DSA dan SHA With RSA ditemukan di setiap AVD dan perangkat berbasis android.

Kata kunci: *evaluasi, layanan kriptografi, android*

Abstract

This study aimed to determine the cryptographic services that supported by all android based devices and Android Virtual Device (AVD). The study was conducted by making an application to see the cryptographic services available on the android system then compared the results of several Android-based devices and Android Virtual Device (AVD) to see what's cryptographic services on all devices and AVD. As a result we found six classes of the cryptographic services: Crypto, Signature, Message Digest, Mac, and SSL Context Key Agreement. Eight cryptographic algorithm are found in every AVD and Android-based devices : AES, DES, HMACMD, HMACSHA, Diffie Hellman, SHA-384, SHA-512, SHAWithDSA and RSA.

Key Words: *evaluation, cryptographic services, android*

1. PENDAHULUAN

Fenomena *Bring Your Own Device (BYOD)* telah berkembang dari sebuah tren menjadi kebutuhan kerja [1]. Gartner memprediksi setengah dari perusahaan akan membutuhkan pegawainya untuk membawa perangkat komputasi sendiri untuk keperluan pekerjaan [3]. Istilah BYOD adalah merujuk kepada pegawai yang membawa dan menggunakan perangkat komputasi miliknya seperti smartphone, laptop, PDA atau tablet ke tempat kerjanya. Tren BYOD meningkatkan resiko keamanan bagi perusahaan karena pegawai dapat mengakses sumber daya perusahaan menggunakan perangkatnya sendiri. Sebagian besar perusahaan memiliki perhatian khusus terhadap resiko kehilangan data dan akses data oleh pihak yang tidak sah [5].

Sistem operasi untuk perangkat bergerak yang banyak digunakan adalah Android, iOS, Windows Phone, Blackberry OS, Linux dan Symbian. Berdasarkan International Data Corporation (IDC) Worldwide Quarterly Mobile Phone Tracker, Android menempati urutan pertama dan iOS urutan kedua dalam *shipment* pada kwartal pertama tahun 2013. Android menguasai 75% sedangkan iOS menguasai 17,3% pangsa pasar yang ada [4].

Android merupakan platform yang menarik bagi pengguna dan pengembang aplikasi. Filosofi yang digunakan bertolak belakang dengan iOS, iOS bersifat *closed source* sedangkan Android bersifat *open source*. Pada Mei 2013, jumlah perangkat Android yang diaktifkan sebesar 900 juta dan jumlah aplikasi yang diinstall dari Google Play Store sebesar 48 milyar [2].

Faktor keamanan merupakan salah satu kebutuhan yang harus diperhatikan dalam penggunaan aplikasi pada perangkat bergerak. Perangkat bergerak memiliki sumber daya yang terbatas, seperti kemampuan pemrosesan, kapasitas memori dan media penyimpanannya. Pengembang aplikasi perlu mengetahui

fungsi-fungsi kriptografi yang didukung pada perangkat berbasis android untuk dapat membuat aplikasi yang menyediakan layanan keamanan. Oleh karena itu perlu adanya penelitian untuk mengevaluasi layanan kriptografi yang didukung oleh Android.

Penelitian ini memiliki 3 tujuan. Pertama, untuk mengetahui layanan kriptografi apa saja yang didukung oleh perangkat berbasis android. Kedua, untuk mengetahui layanan kriptografi apa saja yang didukung oleh semua perangkat berbasis andoid. Ketiga, untuk mengetahui apakah layanan kriptografi yang ada pada *Android Virtual Device (AVD)* diimplementasikan juga pada perangkat berbasis android.

Penelitian ini dilakukan dengan menggunakan metodologi yang terbagi menjadi 3 bagian. Pertama, kami membuat aplikasi yang akan digunakan untuk mengevaluasi layanan kriptografi yang didukung oleh perangkat berbasis android. Kedua, kami menjalankan aplikasi tersebut pada AVD dan perangkat berbasis android. Ketiga, kami menganalisis data hasil eksperimen tersebut untuk mendapatkan kesimpulan.

2. DETAIL PERMASALAHAN

Seringkali pengguna perangkat Android tidak mengetahui apa yang dapat dilakukan oleh perangkat miliknya. Pengguna hanya mengerti bagaimana cara menggunakan aplikasinya saja, sehingga tidak ada masalah jika ia tidak mengetahui layanan kriptografi apa yang didukung oleh perangkat Androidnya. Namun tren BYOD menyebabkan banyaknya penggunaan perangkat bergerak untuk mendukung pekerjaan mereka di berbagai perusahaan. Hal ini menimbulkan kekhawatiran bagi perusahaan, karena para pekerjanya menggunakan perangkat tersebut untuk mengakses sumber daya perusahaan yang mungkin bersifat terbatas atau berklasifikasi rahasia. Untuk dapat mengatasi permasalahan tersebut, maka perlu dikembangkan aplikasi untuk perangkat tersebut yang dapat mengakses sumber daya perusahaan dengan cara yang aman atau memperhatikan faktor-faktor keamanan.

Untuk mengembangkan aplikasi yang menyediakan layanan keamanan pada perangkat berbasis Android, maka pengembang harus mengetahui layanan kriptografi apa saja yang didukung oleh perangkat tersebut. Dengan mengetahui layanan-layanan tersebut, para pengembang dapat memberdayakan layanan yang sudah disediakan pada perangkat tersebut tanpa harus membuat fungsi-fungsi itu sendiri. Hal ini membantu para pengembang sehingga dapat mempercepat pembuatan aplikasinya.

3. METODOLOGI

Pada bagian ini kami akan menjelaskan metodologi yang digunakan dalam penelitian ini. Secara umum metodologi yang kami gunakan dapat dibagi menjadi 3 bagian. Pertama, kami mencari dan mengetahui layanan kriptografi yang didukung oleh Android *Application Programming Interface (API)*. Kedua, kami melakukan eksperimen baik pada *Android Virtual Device (AVD)* maupun perangkat berbasis Android. Ketiga, kami melakukan analisis terhadap data-data hasil eksperimen yang telah didapatkan untuk mendapatkan kesimpulan.

3.1Evaluasi Layanan Kriptografi

Untuk dapat melakukan evaluasi layanan kriptografi pada perangkat berbasis Android, kita harus terlebih dahulu mendapatkan semua daftar algoritma kriptografi yang didukung oleh perangkat tersebut. Android menggunakan beberapa pustaka kriptografi, antara lain Openssl dan Bouncy Castle. Namun mungkin tidak semua algoritma kriptografi yang ada pada pustaka tersebut diimplementasikan pada Android API. Hal ini karena keterbatasan kemampuan pemrosesan dan media penyimpanan pada perangkat berbasis android. Saat penelitian ini dilakukan tidak ada informasi dari pengembang resmi Android terkait hal tersebut, sehingga kami harus melakukannya sendiri.

Salah satu cara yang dapat dilakukan untuk mengetahui penyedia pustaka dan algoritma kriptografi yang didukung oleh pustaka tersebut adalah dengan menelusuri kode sumber dari Android API. Namun hal ini tidak optimal dan memakan waktu yang cukup lama. Sehingga kami membuat suatu aplikasi yang dapat menampilkan semua daftar penyedia pustaka kriptografi dan algoritma kriptografi yang didukung oleh setiap pustaka kriptografi tersebut.

3.2Eksperimen

Setelah aplikasi untuk melakukan evaluasi layanan kriptografi dibuat, kami melakukan eksperimen baik pada AVD maupun perangkat berbasis Android. Kami menjalankan aplikasi pada AVD yang menggunakan android image mulai dari API level 3 sampai API level 16. Sedangkan untuk eksperimen pada perangkat berbasis Android, kami menyebarkan aplikasi tersebut ke rekan-rekan kami yang memiliki perangkat berbasis Android. Hasil dari eksperimen tersebut dikirimkan melalui email.

3.3 Pengumpulan dan Pengolahan Data

Pengumpulan data hasil ekperimen yang dilakukan oleh rekan-rekan kami dilakukan berdasarkan e-mail yang masuk. Pengumpulan data dilakukan mulai tanggal 26 April 2013 sampai 18 Juni 2013. Berdasarkan data yang terkumpul diperoleh sebanyak 16 perangkat berbasis android berupa *smartphone* dan *tablet*. Kami juga menjalankan aplikasinya pada 11 AVD dengan API level yang berbeda-beda. Jumlah dan sebaran data dalam penelitian ini dapat dilihat pada tabel 1. Data-data hasil ekperimen tersebut kemudian diolah dan disajikan dalam bentuk tabel untuk memudahkan proses analisis.

Tabel 1. Sebaran Data Penelitian

Platform Version	API Level	Perangkat	AVD
Android 1.5	3		1
Android 1.6	4		1
Android 2.1	7		1
Android 2.2	8	1	1
Android 2.3.3	10	4	1
Android 3.1	12		1
Android 3.2	13		1
Android 4.0.2	14		1
Android 4.0.4	15	10	1
Android 4.1.2	16	1	1
Android 4.2.2	17		1
Jumlah		**16**	**11**

4. DATA

Aplikasi yang kami gunakan untuk pengumpulan data dapat berjalan baik di semua versi android baik pada AVD maupun perangkat fisik. Aplikasi tersebut menampilkan daftar penyedia *(provider)* layanan kriptografi dan algoritma yang ada pada sebuah perangkat berbasis android. Berdasarkan data yang diperoleh, ditemukan ada 5 pustaka kriptografi yaitu AndroidOpenSSL, DRLCertFactory, Bouncy Castle, Crypto, dan HarmonyJJSE. Pada Tabel 2 terlihat contoh data tiga pustaka yang diperoleh dari perangkat berbasis android dan AVD. Melalui data AVD yang lebih detail dapat dilihat jenis layanan kriptografis yang disediakan masing-masing algoritma.

Pengujian terhadap 11 versi android mendapatkan 20 layanan kriptografi yang sudah didefinisikan oleh android. Layanan kriptografi yang diperoleh dari perangkat berbasis Android adalah :

a. Signature
b. Secret Key Factory
c. Message Digest
d. Mac
e. Key Store
f. KeyPair Generator
g. Key Generator
h. Key Factory
i. Key agreement
j. Cipher
k. Cert Store
l. Cert Path Validatior
m. Cert Path Builder
n. Certification Factory
o. Algorithm Parameter
p. Algorithm Parameter Generator
q. Trust Manager Factory
r. SSL Context
s. Key Manager Factory
t. Secure Random

Tabel 2. Contoh Data Penelitian dari Perangkat dan AVD

Contoh Data Dari Perangkat	Contoh Data Dari AVD	Data AVD lebih Detail
Model Device GT-S5360 Versi Kernel 2.6.35.7 Versi SDK 10 Versi SDK RELEASE 2.3.6	Model Device SDK Versi Kernel 2.6.35.7 Versi SDK 10 Versi SDK RELEASE 2.3.6	Model Device SDK Versi Kernel 2.6.35.7 Versi SDK 10 Versi SDK RELEASE 2.3.6
A. Crypto Provider : AndroidOpenSSL Crypto Algorithm : Default MD5 SHA-1 SHA-256 SHA-384 SHA-512 SSL SSLv3 TLS TLSv1	A. Crypto Provider : AndroidOpenSSL Crypto Algorithm : Default MD5 SHA-1 SHA-256 SHA-384 SHA-512 SSL SSLv3 TLS TLSv1	Crypto Provider: AndroidOpenSSL version 1.0 Crypto Algorithm : MessageDigest : MD5 MessageDigest : SHA-1 MessageDigest : SHA-256 MessageDigest : SHA-384 MessageDigest : SHA-512 SSLContext : Default SSLContext : SSL SSLContext : SSLv3 SSLContext : TLS SSLContext : TLSv1
D. Crypto Provider : Crypto Crypto Algorithm : DSA SHA-1 SHA1PRNG SHA1withDSA	D. Crypto Provider : Crypto Crypto Algorithm : DSA SHA-1 SHA1PRNG SHA1withDSA	Crypto Provider: Crypto version 1.0 Crypto Algorithm : KeyFactory : DSA MessageDigest : SHA-1 SecureRandom : SHA1PRNG Signature : SHA1withDSA
E. Crypto Provider : HarmonyJSSE Crypto Algorithm : SSL SSLv3 TLS TLSv1 X509	E. Crypto Provider : HarmonyJSSE Crypto Algorithm : SSL SSLv3 TLS TLSv1 X509	Crypto Provider: HarmonyJSSE version 1.0 Crypto Algorithm : KeyManagerFactory : X509 SSLContext : SSL SSLContext : SSLv3 SSLContext : TLS SSLContext : TLSv1 TrustManagerFactory : X509

Berdasarkan hasil uji coba baik pada AVD maupun perangkat berbasis Android diperoleh data bahwa terdapat sebanyak 117 algoritma yang sudah disediakan dan sebagian besar disediakan oleh pustaka Bouncy Castle. Beberapa algoritma bukan merupakan algoritma publik dan bahkan menggunakan kode angka sebagai nama. Banyaknya algoritma yang diidentifikasi tidak mengindikasikan banyaknya algoritma sebenarnya karena beberapa data algoritma hanya merupakan *Object Identifier (OID)* dari algoritma publik yang ada. Sebagai contoh AES memiliki OID 2.16.840.1.101.3.4.1.

5. ANALISIS

Kriptografi didefinisikan sebagai sebuah ilmu yang mempelajari teknik matematis terkait dengan keamanan informasi seperti *confidentiality*, *data integrity*, *entity authentication* dan *data origin authentication*. Layanan kriptografi didefinisikan sebagai empat tujuan utama kriptografi yaitu *Confidentiality*, *Authentication*, *Data Integrity*, dan *Non-Repudiation [6]*.

Layanan Kriptografi didefinisikan berbeda oleh Android, yaitu sebagai *Engine ClassName* (Nama dari *Abstract Class*). Nama Class ini sudah didefinisikan sebelumnya oleh *Java Cryptography Architecture* (JCA). Pada perkembangannya, Android mengadopsi *engine* Java termasuk JCA [7]. Dua puluh nama class diantaranya dapat diidentifikasi oleh aplikasi penelitian ini. Selanjutnya, Kedua puluh layanan kriptografi tersebut dipetakan dengan layanan kriptografi yang sudah didefinisikan [6]. Pemetaan didasarkan pada kesesuaian definisi, hasil pemetaan dapat dilihat pada Tabel 3. Dari analisis berhasil diidentifikasi 7 layanan kriptografi Android yang memiliki kesesuaian dengan layanan kriptografi yang didefinisikan oleh 13 layanan kriptografi yang didefinisikan Android merupakan penunjang 7 layanan utama seperti *Secret Key Factory* dan *Key Generator* untuk mendukung layanan *Cipher*.

Tabel 3. Dukungan Layanan Kriptografi

Confidentiallty	Authentication	Data Integrity	Non-Repudiation
Cipher	Signature	Message Digest Mac	Key Agreement SSL Context

Android memberikan nama lain (alias) untuk algoritma kriptografi sehingga penelitian menghasilkan 117 algoritma kriptografi sedangkan algoritma yang beredar di publik tidak sebanyak itu. Selanjutnya dicari algoritma yang selalu ada di setiap versi Android khususnya di 6 layanan kriptografi yang sudah diidentifikasi di Tabel 3. Sebaran algoritma di masing-masing level API dapat dilihat pada Tabel 4. Berdasarkan data sebaran algoritma tersebut, diperoleh 8 algoritma yaitu :

a. Cipher : AES
b. Cipher : DES
c. Mac : HMACMD dan HMACSHA
d. Key Agreement : Diffie Hellman
e. MessageDigest : SHA-384
f. MessageDigest : SHA-512
g. Signature : DSA
h. Signature : SHA With RSA

Setelah diperoleh pustaka, layanan kriptografi dan algoritma pada level API. Dibandingkan data algoritma pada masing-masing pustaka di setiap level API. Perbadingan dilakukan pada 5 level API perangkat berbasis android yang menjadi responden penelitian. Tabel 5. Memperlihatkan bahwa semua algoritma di semua pustaka diimplementasikan pada perangkat berbasis android.

Tabel 4. Sebaran Algoritma pada Pustaka Layanan Kriptografi

Pustaka dan Algoritma Kriptografi		API Level										
		3	4	7	8	10	12	13	14	15	16	17
Cipher	AES	x	x	x	x	x	x	x	x	x	x	x
	ARC4					x	x	x	x	x	x	x
	BLOWFISH					x	x	x	x	x	x	x
	BrokenIES	x	`	x	x							
	DES	x	x	x	x	x	x	x	x	x	x	x
	IES	x	x	x	x							
	RSA	x	x	x	x	x	x	x	x	x	x	x
KeyAgreement	DH	x	x	x	x	x	x	x	x	x	x	x
	ECDH						x	x	x	x	x	x
Mac	DESEDEMAC	x	x	x	x							
	HMACMD / HMACSHA	x	x	x	x	x	x	x	x	x	x	x
	ISO9797ALG3MAC	x	x	x	x							
	PBEWITHHMACSHA1	x	x	x	x	x	x	x	x	x	x	x
MessageDigest	MD5	x	x	x	x							
	SHA-256	x	x	x	x							
	SHA-384	x	x	x	x	x	x	x	x	x	x	x
	SHA-512	x	x	x	x	x	x	x	x	x	x	x
Signature	DSA	x	x	x	x	x	x	x	x	x	x	x
	ECDSA						x	x	x	x	x	x
	MD2WithRSAEncryption	x										
	MD4WithRSAEncryption	x	x	x	x							
	MD5WITHRSA											x
	MD5withRSA/ISO9796-2	x	x	x								
	MD5WithRSAEncryption	x	x	x	x	x	x	x	x	x		
	SHAwithDSA	x	x	x	x							
	SHAWITHRSA	x	x	x	x	x	x	x	x	x	x	x
	SHAWITHECDSA						x	x	x	x	x	x
SSLContext	SSL										x	x
	SSLv3										x	x
	TLS	x	x	x	x						x	x
	TLSv1										x	x

Tabel 5. Perbandingan Jumlah Algoritma Kriptografi AVD dengan Perangkat berbasis Android

Provider	Versi 8		Versi 9		Versi 10		Versi 15		Versi 16	
	AVD	Perangkat	AVD	Perangkat	AVD	Perangkat	AVD	Perangkat	AVD	Perangkat
AndroidOpenSSL	0	0	10	10	10	10	10	10	20	20
DRLSertFactory	1	1	1	1	1	1	1	1	1	1
Bouncy Castle (BC)	106	106	59	59	59	59	65	65	65	65
Crypto	4	4	4	4	4	4	4	4	4	4
HarmonyJJSE	6	6	5	5	5	5	6	6	6	6

6. SIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan dapat diambil kesimpulan sebagai berikut :

a. Terdapat kesamaan layanan kriptografi dan jumlah algoritma kriptografi untuk setiap level API yang sama
b. Semua algoritma kriptografi yang disediakan pada Android SDK diimplementasikan persis sama oleh pabrikan perangkat berbasis Android
c. Melihat jenis algoritma kriptografinya, semua layanan kriptografi sudah didukung di semua perangkat Android
d. Algoritma kriptografi yang didukung oleh seluruh versi Android adalah AES, DES, HMACMD, HMACSHA, Diffie Hellman, SHA-384, SHA-512, DSA dan SHAWithRSA
e. Pada API level 8 kebawah tidak menyediakan layanan kriptografi dari pustaka AndroidOpenSSL namun demikian keberadaan pustaka sudah ada.
f. Provider BC versi 1.34 menyediakan nama lain algoritma lebih banyak dari versi yang lain sehingga seolah-olah Android API level 8 memiliki algoritma kriptografi lebih banyak dari API level lain.

7. DAFTAR RUJUKAN

[1] Arik Hesseldahl, 2013. *"Bring Your Own Device" Evolving From Trend to Requirement.* [Online] (Updated 01-05-2013) Available at: http://allthingsd.com/20130501/bring-your-own-device-evolving-from-trend-to-requirement/. [Accessed 12-06-2013].

[2] Dana Wollman, 2013. *There have been 900 million Android activations, 48 billion app installs to date*. [Online] (Updated 15-05-2013) Available at: http://www.engadget.com/2013/05/15/900-million-android-activations/. [Accessed 12-06-2013]

[3] Gartner, Inc., 2013. *Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes.*[Online] (Updated 01-05-2013) Available at: http://www.gartner.com/newsroom/id/2466615. [Accessed 12-06-2013].

[4] IDC, 2013. *Android and iOS Combine for 92.3% of All Smartphone Operating System Shipments in the First Quarter While Windows Phone Leapfrogs BlackBerry, According to IDC*. [Online] (Updated 16-05-2013) Available at: http://www.idc.com/getdoc.jsp?containerId=prUS24108913. [Accessed 12-06-2013].

[5] Ken Hess, 2013. *The top 5 trends in mobile and BYOD security*. [Online] (Updated 18-04-2013) Available at: http://www.zdnet.com/the-top-five-trends-in-mobile-and-byod-security-7000014226/. [Accessed 12-06-2013].

[6] Menezes, 1996. *Handbook of Applied Cryptography*. Ontario. CRC Press

[7] Oracle, 2011. *Java ™ Cryptography Architecture (JCA) Reference Guide*. [Online] Available at : http://docs.oracle.com/javase/6/docs/technotes/guides/security/crypto/CryptoSpec.html. [Accessed 12-06-2013]