BAB II

STUDI LITERATUR

2.1 TINJAUAN PUSTAKA

2.1.1 Tinjauan Pustaka

Sosial media semakin berkambang untuk saat ini dan memungkinkan kita selalu terhubung dengan semua hal baik itu pertemanan, berita, maupun berbelanja secara online. Hal ini menimbulkan bagaimana keamana data dari sosial media dan juga *web browser* memungkinkan data kita secara aman.

Dalam bagian ini akan dipaparkan bagaimana keamanan dari berbagai aplikasi *browser* pada android dan iOS dan juga aplikasi yang sosial media dari android dan iOS. Virvilis (2015) mengemukakan bagaimana bahaya data yang yang bisa dicuri dari *web browser* baik dari Android maupun dari iOS sendiri (Virvilis et al. 2015). Dan Gronli (2014) membandingkan bagaimana aplikasi dapat berjalan disetiap *platform* masing-masing sistem operasi (Gronli et al. 2014).

2.1.2 Pembahasan Pustaka

Penggunaan *web browser* saat ini dikalangan pengguna android dan iOS sangat penting untuk mengakses segala jenis sosial media mupun pencarian dari data.

	iOS 7.1.1	Android 4.0.4	Windows 7
Safari Mobile	X		
Chrome Mobile	X	X	
Opera Mini	X	X	
Browser†		X	
Firefox Mobile		X	
Opera Mobile		X	
Chrome			X
Firefox			X
Internet Explorer			X
Opera			X

Gambar 2.1. *Browser* masing-masing *platform* (Virvilis et al. 2015)

Pada Gambar 2.1 terlihat beberapa *web browser* yang ter-*install* di berbagai macam *platform* dan *Chrome mobile* merupakan *web browser* yang terdapat pada iOS dan juga android. Hasil studi yang dilakukan oleh Virvilis (2015) ditemukan beberapa *web browser* yang memberikan perlindungan untuk akses dan juga keamanan data pengguna. Pada iOS *web browser* memberikan perlindungan data sedangkan pada Android *web browser* sebaliknya tidak memberikan perlindungan data (Virvilis et al. 2015).

OS	Browser name	Phishing protection†
Android	Browser††	N
	Chrome Mobile	N
	Firefox Mobile	Y
	Opera Mobile	Y
	Opera Mini	N
iOS	Chrome Mobile	N
	Opera Mini	N
	Safari Mobile	Y

OS	Browser name	Malicious sites protection†
iOS	Safari Mobile	N
	Chrome Mobile	N
	Opera Mini	N
Android	Browser††	N
	Firefox Mobile	Y
	Chrome Mobile	N
	Opera Mobile	Y
	Opera Mini	N

Gambar 2.2. *Phishing* protection test dan malicious site test (Virvilis et al. 2015)

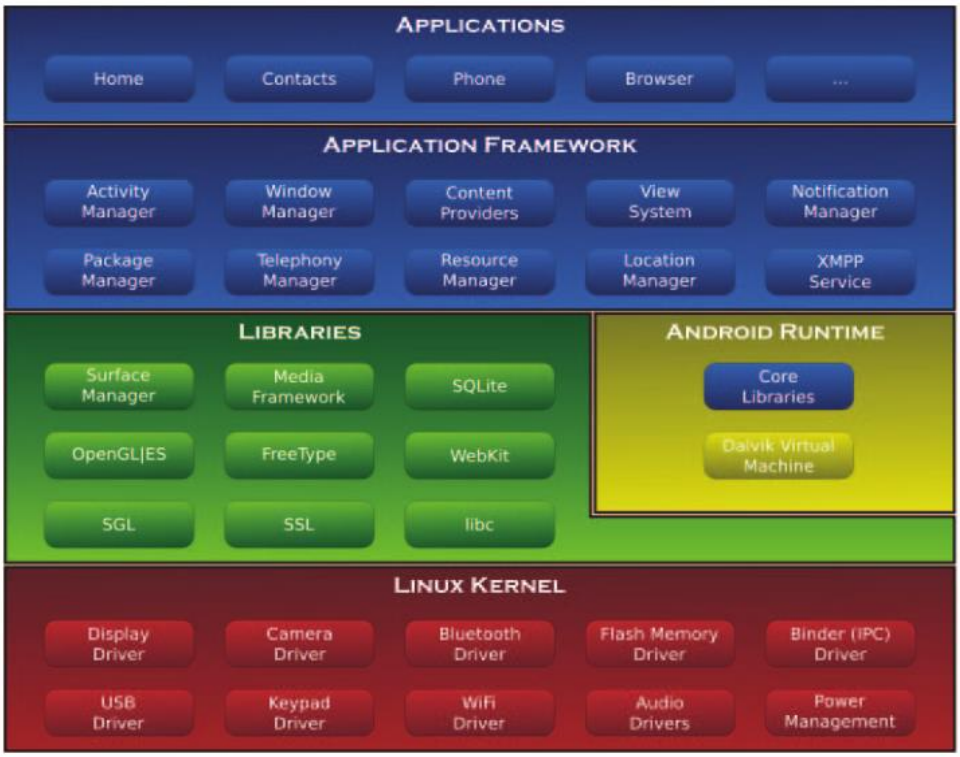
Pada *Gambar 2.2* menjelaskan beberapa *web browser* memberikan perlindungan untuk *phishing* dan situs-situ yang berbahaya misalnya untuk *mozilla firefox* dan opera. Sedangkan untuk iOS *safari* memberikan perlindungan untuk *web-web* yang bisa menimbulkan *phishing*.

2.2 LANDASAN TEORI

2.2.1 Android

Android merupakan OS (Operating System) yang di desain untuk pengguna *smartphone* (Gronli et al. 2014). Android dengan cepat menjadi populer di kalangan komunitas pengembang (*developer*) karena bersifat *open source* dan dapat adopsi oleh penyedia telekomunikasi di seluruh dunia. *Android* berbasis *Linux*. *Android* berfokus pada aplikasi, dan sebagian besar fungsi inti dari telepon diterapkan sebagai aplikasi sehingga bisa lebih dikembangkan oleh pihak lain (*developer*) sebagai pihak ketiga.

Platform Android tidak hanya menyediakan sistem operasi *mobile* yang dapat dikembangkan, namun juga menyediakan mesin virtual built-in (Dalvik Virtual Machine) agar aplikasi dapat berjalan sebaik *middleware* antara kode dan sistem operasi. API (*Application Programming Interface*) terus berkembang dan terus ditingkatkan dari awalnya versi 1.0 sampai saat ini menjadi versi 8.1.0 (*oreo*) merupakan peningkatan yang sangat besar dimana jumlah fitur-fiturnya semakin banyak dan memberikan kemudahan bagi para pengguna maupun pengembang (*developer*). Karena Android adalah sistem operasi mobile *open source*, pilak lain (*developer*) diharapkan bisa untuk berkolaborasi dalam pengembangan sistem operasi ini untuk lebih meningkatkan kinerjanya baik dalam sistem operasi dan API (*Application Programming Interface*).



Gambar 2.3. *Android Architecture* (Gronli et al. 2014)

Pada Gambar 2.3 menjelaskan arsitektur *layer* pada android yang terdari dari aplikasi, aplikasi *framework*, *libraries* yang berisikan *source code* dan yang terakhir berisikan *kernel-kernel* yang mengakses langsung pada perangkat keras masing-masing seperi kamera dan *bluetooth*.

2.2.2 iOS

IOS adalah sistem operasi dikembangkan untuk perangkat *Apple*, salah satu yang paling penting adalah *Iphone* (Gronli et al. 2014). *IPhone* dirilis pada tahun 2007 dan mengubah pasar penjualan *smartphone* dengan menbuat trobosan baru dalam bentuk layar sentuh yang besar besar dan untuk perangkat keras dan spesifikasi dari *smartphone* termasuk yang mengesankan.

Aplikasi untuk iOS dari dibuta dalam bentuk *Objective*-C yang menggunakan *library Cocoa Touch*. Objective-C adalah perpanjangan dari bahasa C,

sedangkan *Cocoa Touch* adalah kumpulan *class*. Sementara C# dan Java (yang digunakan pada Android dan *Windows Phone*) cukup mirip dalam sintaks, *libraries* Objective-C. Objective-C menggunakan bahasa pemrograman berorientasi obyek. Bahasa dan *platform* telah terus meningkat selama bertahun-tahun, dan satu perubahan yang sangat penting datang dengan diperkenalkannya ARC (*Automatic Reference Counting*). Untuk melakukan pengembangan dalam aplikasi di iOS memerlukan komputer yang menjalankan Mac OS. Aplikasi yang biasa digunakan untuk menulis aplikasi iOS adalah *Xcode*. Aplikasi ini merupakan aplikasi untuk editor, alat analisis, simulator iOS dan SDK.

Gambar 2.4. iOS *Architecture* (Gronli et al. 2014)

Pada Gambar 2.4 merupakan arsitektur untuk iOS yang terdiri dari *layer* aplikasi, *core service, security service* dam *core* OS. Pada layer *security service*

sudah diberikan beberapa pengamanan untuk menjalankan iOS di interaksi di internet.

2.2.3 Sosial Media

Jaringan Sosial membuat pengguna menampilkan informasi pribadi mereka yang dapat dilihat oleh semua orang (Wicaksono et al. 2017). Situs jejaring sosial online seperti facebook sangat populer di kalangan masyarakat. Jaringan Sosial adalah struktur di mana individu atau organisasi memberikan jaringan yang terhubung oleh satu atau lebih jenis interkoneksi tertentu, seperti persahabatan dan hubungan pertukaran keuangan. Jaringan Sosial adalah suatu bentuk jaringan baik individu maupun kelompok ke dalam jenis komunitas kecil yang terhubung melalui jaringan internet. Mereka terhubung ke jaringan internet dan berinteraksi dengan individu maupun kelompok. (Robi'in et al. 2017).

Situs Jaringan Sosial seperti *facebook*, *Twitter*, dan *Instagram* memungkinkan individu untuk menceritakan tentang diri mereka sendiri, dan menjalin hubungan dengan orang lain. Situs ini sangat berguna untuk menjaga hubungan dan menghubungkan individu-individu dengan minat seperti musik atau olahraga.

Orang yang telah menggunakan situs-situs jaringan sosial ini secara intens sering melakukan komunikasi dan bertemu di internet untuk saling menghibur dan berinteraksi. Situs-situs ini menyediakan layanan untuk berkomentar dan juga mengunggah foto maupun video ke jejaring sehinga bisa dilihat oleh pengguna lain. Banyak orang menggunakan situs jejaring sosial untuk tetap terhubung dengan teman-teman lama dari berbagai sekolah atau

universitas. Karena banyaknya pengguna yang memberikan data-data pribadi mereka yang di-*share* ke jejaring sosial membuat kemungkian ancaman terhadap data-data pribadi tersebut sehingga mendeteksi serangan terhadap privasi data pengguna individual merupakan tantangan yang besar.

2.2.4 Wireless

Komunikasi *wireless* (nirkabel) menggunakan gelombang elektromagnet untuk mengirimkan sinyal jarak jauh. Biasanya penggunaan *wireless* digunakan untuk mengkases *Web browser*, e-*mail*, dan aplikasi jaringan sosial. Jaringan ini sedikit berbeda dengan jaringan yang menggunakan kabel *ethernet* namun secara keseluruhan hampir sama. Standarisasi untuk wireless di publikasi oleh IEEE yaitu IEEE 802.11 (Hiertz et al. 2010). Standar tersebut kemudian dibagi menjadi beberapa jenis menurut frekuensi dan kecepatan transfer data yang digunakan. Pembagian tersebut yaitu:

- IEEE 802.11 yaitu standart pertama yang bekerja pada frekuensi 2,4 GHz dengan kecepatan transfer data maksimum 2 Mbps.
- IEEE 802.11b masih menggunakan frekuensi 2,4 GHz dengan kecepatan trasfer datanya mencapai 11 Mbps dan jangkau sinyal sampai dengan 30 m.
- IEEE 802.11a bekerja pada frekuensi 5 GHz dengan kecepatan transfer datanya mencapai 58 Mbps.
- IEEE 802.11g gabungan dari standart 802.11b yang menggunakan frekuensi 2,4 GHz namun kecepatan transfer datanya bisa mencapai 54 Mbps.
- IEEE 802.11n yaitu standart bekerja pada frekuensi 2,4 Ghz dan dikabarkan kecepatan transfer datanya mencapai 100-200 Mbps.

2.2.5 Teknik Serangan

Berbagai jenis serangan yang memungkinkan terjadi pada jaringan *wireless* yang dapat memberikan dampak kerugian pada hilangnya data atau informasi dari pengguna jaringan. Berbagai jenis serangan yang mungkin bisa ter jadi pada jaringan *wirelesss* yaitu.

2.2.5.1 *Web Phishing*

Sebuah serangan yang mambuat sebauh halaman domain *web* palsu yang mirip dengan aslinya untuk menggelabuhi pengguna untuk mendapatkan data seperti *username* dan *password* dari pengguna. Biasanya serangan ini dilakukan saat aktifitas *login* pada sosial media atau bahkan *login* untuk masuk kedalam jaringan *wifi* yang membutuhkan *username* dan *password*. Biasanya teknik ini memfokuskan pada teks dan gambar yang menyerupai halaman *web* aslinya. Serangan ini bisa dideteksi dari halaman *web* tersebut maupun URL yang sebenarnya mengarah kehalaman lain yang bukan halaman dari *web* tersebut (Zhang et al. 2013).

2.2.5.2 *Bruto Force*

Serangan ini merupakan percobaan untuk mengetahui semua kunci yang digunakan untuk masuk dalam sebuah jaringan *wireless*, bisa juga dalam *server* atau *workstation* (Jo & Won Yoon 2015). Serangan ini dilakukan biasanya untuk mencoba masuk secara paksa kedalam suatu jaringan tersebut. Secara sederhananya serangan ini menggunakan semua kombinasi yang mungkin untuk menebak *username* dan *password*. Penggunaan *password* yang sederhana bisa memudahkan penggunaan melakukan serangan ini karena *password*

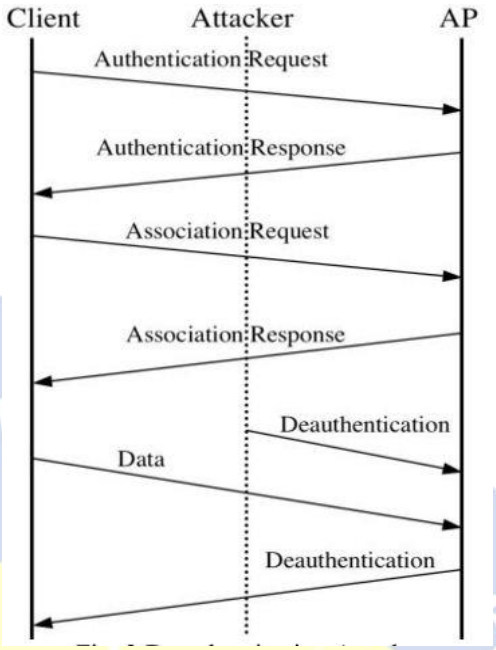
yang telalu sederhana. namun bisa juga serangan ini gagal atau memakan waktu yang cukup lama karena untuk memecahkan kombinasi *password* termasuk sangat rumit (Liu 2015).

2.2.5.3 MITM (*Man In The Middle Attack*)

Sebuah serangan dari pihak ketiga yang secara diam-diam mencoba mengendalikan komunikasi di antara keduah belah pihak yang saling berintetarsi didalam suatu jaringan. Serangan ini mencoba mencegat, memodifikasi dan mengubah atau mengganti lalu lintas komunikas dari pihak yang berinteraksi ke pihak ke tiga atau pihak penyerang. Jenis serangan ini menyebabkan pihak yang berinteraksi tidak akan menyadari dari serangan dan menganggap jaringan dalam keadaan amam dan terpercaya. Sasaran yang biasanyan ingin dicapai dari serangan ini bukan hanya serangan terhadapat data tetapi kerahasian data dan juga intergritas dari data itu sendiri (Conti et al. 2016).

2.2.5.4 *Deauthentication attack*

Biasanya serangan ini sering dikatakan dengan serangan DDoS atau *Distributed-Denial-of-Service Attack*. Serangan ini biasanya dilancarkan untuk menyerang *server* dengan menghabiskan *resource* dari suatu *server* atau komputer sehingga layanannya tidak bisa akses. Serangan jenis ini juga bisa dilakukan untuk menyerang aksess poin atau *router wifi*. Serangan ini memaksa jalur akses untuk *autentikasi* pengguna kedalam jaringan wifi.



Gambar 2.5. Deauthentication Attack (Noman et al. 2015)

Secara garis besar serangan ini dapat dilihat pada Gambar 2.5 dimana penyerang melakukan blok terhada authentikasi dari pengguna ke akses point.

2.2.5.5 *Arp Poisoning*

Serangan ini menitik-beratkan pada ARP (*Address Resolution Protocol*) dimana serangan yang memanipulasi paket ARP sehingga paket yang seharunya diterima oleh pihak lain dilewatkan terlebih dahulu ke penyerang dan dari penyerang baru dikirim ke tujuan. Serangan ini mencegat *frame* data dan memodifikasi lalu lintas jaringan atau bisa mengentikan lalu lintas jaringan. Secara teknis serangan ini memamfaatkan kelemahan dari ARP broadcast dengan menyebarkan MAC *address* (*Media Access Control*) palsu dari permintaan ARP pihak lain yang saling berinteraksi didalam jaringan (Kaur & Malhotra 2015).

2.2.5.6 DNS Spoofing

Serangan ini hampir sama dengan serangan ARP *poisoning* namun menggunakan DNS (*domain names server*) yang dimanipulasi IP-nya oleh penyerang. Serangan ini bisa dikatakan sebagai serangan yang hampir sama dengan phising, hanya pada aksesnya serangan tidak dilanjutkan kehalaman domain yang dituju oleh penerima. Tujuannya untuk mengalihkan *website* ke IP yang telah tentukan sebelumnya (Zhang & Xia 2013).

2.2.5.7 DHCP Spoofing

Serangan ini juga dikatakan sama dengan serangan DNS *spoofing* yang memamfaatkan alamat IP yang di lakukan secara otomatis sehingga mengalihkan IP ke alamat IP penyerang (Zhang & Xia 2013).

2.2.5.8 Enkripsi dan dekripsi

Data yang lewat didalam jarinagn bisanya terenkripsi sesua dengan protokol yang dilaluinya misal untuk email bisalnya mengunakan protokol SSL ataupun penagunaan HTTPS pada penggunaan sosial media (Kabetta et al. 2012).