ANALISIS ANCAMAN *SMISHING* PADA *SMARTPHONE* MENGGUNAKAN *STRIDE* SEBAGAI PEMODELAN ANCAMAN

Andriyan Dwi Putra[1)] **Joko Dwi Santoso**[2)] **Muhammad Yuga Nugraha**[3)]
Ipung Ardiyansyah[4)]
Program Studi Sistem Informasi[1)]
Program Studi Teknik Komputer [2) 3) 4)]
Fakultas Ilmu Komputer, Universitas AMIKOM, Yogyakarta, Indonesia[1) 2) 3) 4)]
andriyan.putra@amikom.ac.id

ABSTRACT

Phishing attacks are often encountered in everyday life, both computer and mobile devices. Different types of Phishing attacks are aimed at end users who have little knowledge of security awareness, making mobile devices a target for threats. The portability of mobile devices makes it easier for someone to use phishing Short Message Service (SMS) attacks on behalf of the message as an E-Commerce company or Internet Service Provider so that end users become targets for crimes such as data theft and fraud. In the discussion of this paper, it will be discussed how the pattern of attacks that occur and the mitigation that can be done when end users receive SMS Phishing (smishing).

Keywords*: Mobile, Threat, Threat Modeling, STRIDE, Smishing*

ABSTRAK

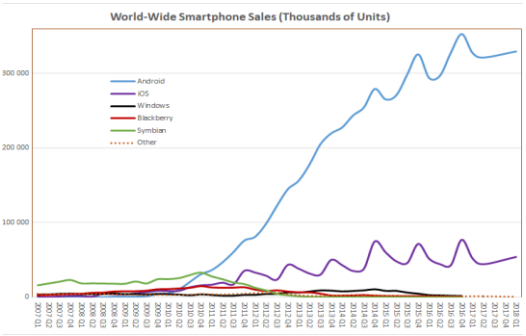
Serangan Phising seringkali kita temui di kehidupan sehari-hari baik perangkat komputer maupun mobile. Berbagai jenis serangan Phising ditujukan kepada end user yang memiliki sedikit pengetahuan mengenai security awareness, sehingga perangkat mobile menjadi target ancaman. Portabilitas dari perangkat mobile memudahkan seseorang untuk menggunakan serangan Short Message Service (SMS) phising yang mengatasnamakan pesan sebagai perusahaan E-Commerce maupun Internet Service Provider sehingga end-user menjadi target tindak kejahatan seperti pencurian data dan penipuan. Dalam pembahasan paper ini akan dibahas bagaimana pola serangan yang terjadi serta mitigasi yang dapat dilakukan ketika end-user mendapatkan SMS Phising (smishing).

Kata Kunci : *Mobile, Threat, Threat Modeling, STRIDE, Smishing*

PENDAHULUAN

Perkembangan teknologi menghasilkan berbagai jenis perangkat keras (*hardware*) seperti komputer, laptop, tablet, *smartphone* yang dapat mendukung kebutuhan masyarakat akan informasi di dalam internet baik komunikasi dalam sehari-hari[1]. Informasi dapat didapatkan secara mudah menggunakan perangkat yang ada, baik informasi positif yang membawa keuntungan maupun informasi negatif yang memberikan dampak negatif bagi seseorang maupun organisasi. Hal ini memicu perkembangan tindak kejahatan secara digital atau *cyber crime* dengan memanfaatkan informasi yang luas dan memanfaatkannya kedalam tindakan kejahatan atau hal negatif. Keamanan perangkat keras (*hardware*) perlu ditingkatkan seiring banyaknya tindak kejahatan digital yang memanfaatkan berbagai jenis teknik serangan untuk memberikan dampak kecil maupun besar dalam kehidupan sehari-hari.

Keamanan di dunia digital merupakan tindakan dalam mencegah pengguna perangkat keras (*hardware*) agar terhindar dari serangan tindak kejahatan digital (*cyber crime*) seperti yang dinyatakan oleh Gollmann (2006) dalam bukunya yang berjudul "*Computer Security*"[2]. Ancaman yang terjadi menggunakan teknik yang beragam seperti halnya Phising yang memanfaatkan teknologi yang tersedia sebagai alat untuk melakukan serangan dan *Social Engineering* untuk memanfaatkan kelemahan dari keadaan psikologi seseorang agar dapat melakukan pencurian data melalui website, e-mail, maupun SMS[3]. Smartphone menjadi perangkat keras (hardware) yang banyak digunakan oleh masyarakat diseluruh dunia karena sangat *portable* sehingga memudahkannya untuk dibawa kemana saja, cara kerja *smartphone* sama seperti halnya komputer yang dengan arsitektur perangkat yang berbeda. Pada Gambar 1 terdapat grafik yang menunjukan pengguna sistem operasi yang dari seluruh dunia.



Gambar 1. Grafik pengguna sistem operasi di dunia dari tahun 2007-2018.

Dari grafik diatas kita dapat mengetahui ancaman keamanan dunia digital akan mendominasi pada sistem operasi Android atau perangkat smartphone[4]. Smartphone banyak digunakan oleh masyarakat sebagai sarana komunikasi baik internet, telepon, sms, e-mail, e-banking maupun kebutuhan lainnya sehingga akan semakin banyak ancaman yang memanfaatkan media komunikasi untuk mendapatkan data yang sensitif[5]. Hal ini akan berdampak pada beberapa aspek keamanan pada sistem diantaranya:

Privacy / Confidentiality

Kerahasiaan, menjaga informasi pribadi atau seseorang dari siapapun yang tidak memiliki izin yang sah. Pada sebuah perusahaan umumnya data sensitif yang dikelola hanya diperuntukkan oleh orang tertentu yang berhak untuk mengaksesnya secara internal dan tidak boleh mempublikasikannya kepada pihak external seperti keluarga, teman, perusahaan lain.

Integrity

Integritas, menjaga atau melindungi data agar tidak terjadi perubahan data untuk menjaga keaslian dari data. Ketika data akan dikirimkan melalui sebuah komunikasi maka diperlukannya beberapa metode untuk menjaga keaslian data seperti enkripsi saat terjadinya komunikasi antar pihak.

Authentication

Autentikasi, proses validasi pengguna ketika hendak melakukan pengaksesan pada sumber daya yang ada seperti jaringan, komputer, dan perangkat lainnya. Hal ini dilakukan agar sistem mengetahui seseorang yang hendak mengakses suatu resources apakah memiliki identitas yang jelas atau tidak.

Availability

Ketersediaan, aspek yang menjamin bahwa data yang ada harus selalu tersedia dalam berbagai kondisi baik bencana alam, kesalahan teknis, maupun ketika terjadi sebuah serangan. Aspek ini menentukan bahwa diperlukannya sistem cadangan (backup system) yang dapat digunakan ketika terjadi insiden pada sistem yang sedang berjalan.

Access Control

Kontrol akses, memastikan seorang pengguna memiliki autoriasi dengan hak akses yang sudah ditentukan. Dalam penerapan kontrol akses, dibutuhkan klasifikasi tertentu untuk menentukan grup akses dengan penggunaan *resources* yang dibatasi setiap grupnya.

Non-repudiation

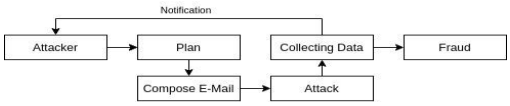
Mencegah salah satu pihak melakukan penyangkalan terhadap aktifitas yang sudah dilakukannya dan rekaman dari komunikasi antar pengguna direkam ke dalam sebuah file

agar dapat melihat aktifitas antar pengguna ketika sedang melakukan komunikasi.

Aspek diatas akan menentukan bagaimana sebuah sistem pemodelan ancaman (*threat modelling*) merupakan metode yang digunakan untuk mengidentifikasi kelemahan pada sebuah sistem beserta memberikan informasi dari dampak yang ditimbulkan[6]. Pemodelan ancaman memiliki berbagai macam jenisnya dengan berdasarkan pada kasus dan kondisi yang sedang terjadi. Dengan menggunakan pemodelan, maka akan mempermudah dalam mengetahui seberapa besar dampak yang disebabkan oleh jenis serangan SMS Phising pada pengguna *smartphone* serta bagaimana cara meminimalisir dampaknya maupun langkah-langkah agar tidak menjadi target serangan tersebut.

TINJAUN PUSTAKA

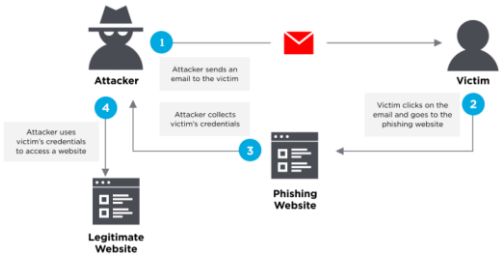
Phishing, merupakan jenis serangan dengan motif mencuri informasi rahasia pengguna dengan akses yang tidak sah dan memanfaatkan Social Engineering dalam aksinya. Informasi yang bisa didapatkan dari kegiatan ini adalah berupa password account e-mail maupun sosial media dan nomor kartu kredit pada perangkat. Serangan phising memanfaatkan website yang berisikan konten spesifik untuk mendapatkan data pengguna seperti halaman login atau pendaftaran dengan memanfaatkan bentuk konten pada platform terpercaya dan dibuat dengan sama persis sehingga pengguna akan kesulitan untuk mengetahui website yang diaksesnya merupakan website phising. Dalam melakukan serangan phising, penyerang menggunakan tahapan seperti pada Gambar 2.



Gambar 2. Tahapan dalam melakukan serangan phising

Cara Kerja Phising

Attacker akan menggunakan email untuk membuat sebuah pesan yang sudah disusun untuk menghindari pesan yang dikirimnya masuk sebagai spam seperti memanipulasi Header pada bagian email dengan mengatasnamakan organisasi maupun pemerintah, serta mencantumkan pesan-pesan untuk melakukan Social Engineering pada pengguna seperti informasi untuk melakukan reset password, mengisikan sebuah form dan sebagainya. Hal ini dalam upaya untuk memanfaatkan pengguna agar mempercayai pesan yang dibawakan oleh penyerang dan biasanya tercantum sebuah dokumen ataupun URL yang berfungsi untuk mendapatkan informasi pengguna secara tidak sadar. Ketika pengguna berhasil memasukkan informasi pribadinya, penyerang akan mendapatkan balasan kembali dari website phising yang sudah dibuatnya sehingga berbagai data akan berhasil didapatkan dengan mudahnya.



Gambar 3. Cara kerja serangan phising

Pada Gambar 3 menjelaskan proses kerja dari serangan phising pada umumnya, adapun klasifikasi serangan phising berdasarkan target dan metode yang digunakannya sebagai berikut

Deceptive Phishing

Serangan phishing yang paling populer digunakan para pelaku kepada korbannya. Deceptive Phishing digunakan untuk mendapatkan informasi rahasia dari para korban. Misalnya, dengan mengirimkan link palsu ke e-mail korban.

Spear Phishing

Serangan phishing yang dilakukan dengan hanya menargetkan individu tertentu dengan memanfaatkan situs sosial media. Ciri khas dari serangan ini yaitu para pelaku mencantumkan informasi personal seputar korbannya seperti nama, jabatan, dan nomor teleponnya.

Whaling

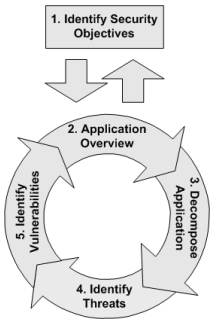
Serangan phishing yang dilakukan dengan menargetkan para CEO perusahaan atau orang terkemuka. Penyerangan ini sering menghabiskan banyak waktu profiling target untuk menemukan momen yang tepat dalam mencuri kredensial login dan informasi sensitif.

Pharming

Serangan yang mirip dengan phishing, pharming mengirim pengguna ke situs web palsu yang tampaknya sah. Namun, dalam kasus ini, korban bahkan tidak perlu mengklik tautan jahat untuk dibawa ke situs palsu. Penyerang dapat menginfeksi komputer pengguna atau server DNS situs web dan mengarahkan pengguna ke situs palsu bahkan jika URL yang benar dimasukkan.

Threat Modelling

Dalam mengidentifikasi serangan phising, diperlukan sebuah pendekatan agar dapat dianalisis dan menghasilkan informasi dengan pemodelan ancaman yang disebut dengan *Threat Modelling.* Dalam pemodelan ancaman terdapat berbagai jenis yang dapat digunakan berdasarkan ancaman yang akan dianalisis dan mengevaluasinya dapat berupa penilaian maupun dokumentasi. Untuk menentukan jenis pemodelan ancaman yang dapat digunakan, kita dapat menggunakan tahapan pada Gambar 4 dalam melakukan pemodelan sebuah ancaman.



Gambar 4. Proses dalam membuat Threat Modeling

Mengidentifikasi aspek keamanan yang akan ditinjau dari serangan Phishing yaitu smartphone, bagaimana cara kerja aplikasi ketika melakukan komunikasi antar perangkat yang satu dengan yang lain, dan komponen-komponen yang saling berhubungan dengan aplikasi saat melakukan interaksi. Kemudian meninjau beberapa jenis framework threat modelling yang sesuai dengan hasil analisis sebelumnya, sehingga didapatkan framework STRIDE untuk melakukan tinjauan lebih jauh secara mudah dalam cakupan objek yang simpleks. Adapun masing-masing komponen yang terdapat pada STRIDE terdapat pada Gambar 5.

	Threat	Property Violated	Threat Definition
S	Spoofing identify	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

Gambar 5. Komponen pada STRIDE

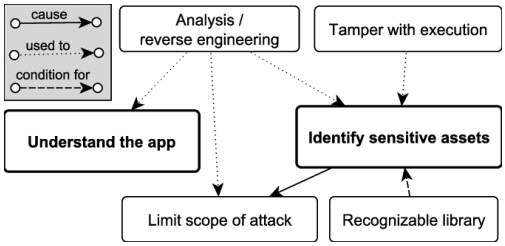
Spoofing

Serangan yang memanfaatkan identitas yang sah seperti menggunakan nama customer services ISP maupun perusahaan E-Commerce dengan tujuan mengirim pesan yang sudah dimanipulasi agar pengguna dapat percaya pada isi pesan dari pengirim seperti pada Gambar 6.

Gambar 6. Salah satu contoh serangan SMS Phising

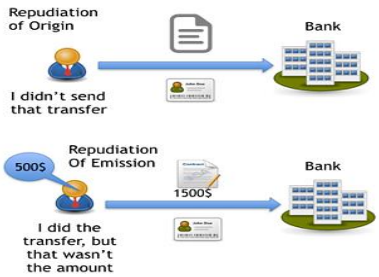
Tampering Data

Jenis serangan yang dapat memodifikasi data dengan menghapus, membuat, maupun menambahkan data ketika melakukan *intercept* saat terjadi komunikasi.



Repudiation

Merupakan serangan dimana seorang pengguna tidak bisa membuktikan transmisi data yang sudah dijalankan dengan pengguna lainnya, sehingga penerima data dapat mengetahui pengguna yang mengirimkan data tersebut.



Gambar 7. Contoh repudiation

Information Disclosure

Privacy breach atau *data leak* diartikan sebagai kebocoran data terjadi ketika sebuah aplikasi mempunyai kerentanan yang memungkinkan untuk mendapatkan hak akses secara tidak sah untuk melihat informasi yang bersifat sensitif sehingga ancaman ini dapat mengancam aspek keamanan dalam hal kerahasiaan (*confidentiality*).

Denial of Service (DoS)

Merupakan serangan yang terjadi pada jaringan, berpotensi untuk membuat sebuah program atau *services* yang sedang berjalan pada sistem menjadi *crash* bahkan sampai terhenti sehingga dapat mengancam aspek keamanan yaitu ketersediaan (*availability*).

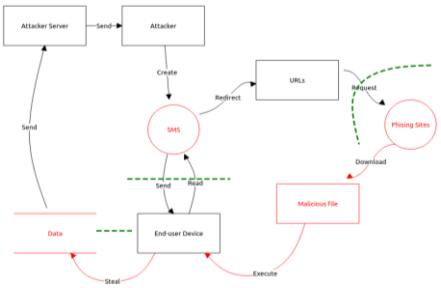
Elevation of Privileges

Mendapatkan akses tertinggi pada sebuah sistem dengan memanfaatkan user yang ada pada sistem. Beberapa aplikasi yang terdapat baik komputer, laptop maupun android memiliki spesifik user untuk menjalankannya dengan pembatasan akses tertentu yang dapat dilakukan ketika aplikasi sedang berjalan. Proses ini dapat menyebabkan penyerang mengambil alih perangkat secara penuh baik untuk mendapatkan data sensitif, mengintai aktivitas yang dilakukan pengguna, memanipulasi komunikasi yang dilakukan sehingga ancaman ini dapat mengancam aspek keamanan yaitu autorisasi.

METODE PENELITIAN

Tujuan dalam penulisan paper ini adalah untuk mengidentifikasi aset yang terdapat pada perangkat, proses yang digunakan saat terjadi serangan Smishing (SMS Phishing), serta menganalisa ancaman yang ditimbulkan menggunakan framework pemodelan ancaman (*threat modelling*) STRIDE, dan digambarkan berupa Data Flow Diagram beserta flowchart pemodelannya pada Gambar 8 dan Tabel 1. Dalam membuat sebuah flow untuk pemodelan maka diperlukan *software* pendukung agar lebih mudah dalam membuat rangkaian aset dan tahapan pada ancaman, penulis menggunakan

OWASP Threat Dragon untuk membuat gambar diatas dengan menambahkan informasi berupa warna merah sebagai ancaman pada entitas, proses maupun data store sehingga dapat ditinjau pada Tabel 1.



Gambar 8. Flow serangan Smishing

Elements	**S**	**T**	**R**	**I**	**D**	**E**
Entity						
Data Flow		✓		✓		
Data Store		✓		✓		
Process	✓	✓	✓	✓		✓

Tabel 1. Data Flow Diagram

Tabel diatas menunjukkan jenis beberapa komponen yang terdapat pada serangan smishing berdasarkan pada Gambar 8 bahwa selain komponen **D** (*Denial of Service*) terlibat dalam setiap tahapannya dari awal serangan terjadi sampai attacker berhasil mendapatkan informasi sensitif yang ada pada smartphone korban. Ancaman DoS tidak banyak dijumpai dalam serangan Phising karena sifatnya yang cukup intrusif kepada sistem sehingga dapat membuat smartphone korban mengalami crash pada service maupun mati total pada sistem.

Pembahasan

Serangan Phising diawali dengan attacker yang membuat sebuah server khusus bertujuan sebagai *hosting* sebuah website phising serta untuk memberikan notifikasi pada e-mail attacker ketika data berhasil diperoleh dari korban phising. Setelah persiapan awal telah selesai maka attacker akan menggunakan nomor telepon sebagai perantara dalam menyebarkan website phising, biasanya berupa pesan SMS yang berisikan informasi hadiah untuk korban atau bahkan form pendaftaran undian. Nomor yang digunakan oleh attacker adalah acak karena serangan phishing ini tidak selalu ditargetkan pada organisasi khusus untuk memperoleh data, SMS yang diterima kemudian akan dibaca oleh korban atau bahkan sampai melakukan interaksi dengan link yang ada pada SMS dan dilakukan redirect pada website phising, untuk melakukan validasi sebuah website termasuk phising atau bukan perlu melihat beberapa aspek kembali tidak hanya dari sisi keamanan website seperti SSL di browser tetapi diperlukan filter baik dari konten yang ada, URLs serta informasi lainnya sebagai pendukung.

Website phising yang telah dibuat oleh attacker biasanya akan dimasukkan juga program seperti malware ads, trojan atau bahkan ransomware. Hal ini tentunya akan merugikan korban dengan adanya sebuah program tidak sah berada pada smartphone pengguna, bahkan tidak banyak yang dapat melakukan akses lebih jauh lagi ketika program sudah terpasang pada perangkat seperti trojan yang terpasang karena pengguna mengizinkan instalasi dari sebuah program yang sudah terdownload sehingga malware akan ikut terpasang pada sistem smartphone dan melakukan komunikasi dengan server dari attacker untuk melakukan Remote Control dan memperoleh beberapa informasi yang sifatnya sensitif, tindak kejahatan (*fraud*) dapat dilakukan dengan melakukan provokasi melalui akun korban yang sudah diambil alih dan diteruskan kepada pengguna lainnya.

SIMPULAN

Smishing (SMS phishing) adalah jenis serangan phishing dilakukan dengan menggunakan SMS (Short Message Service) pada ponsel. Penggunaan pemodelan STRIDE dalam analisis smishing menunjukan serangan smishing dengan berbagai komponen – komponen proses yaitu spoofing, tampering data, repudiation, Information Disclosure, dan Elevation of Privileges. Harapannya penelitian

selanjutnya lebih mendalam ke arah mitigasi smishing.

DAFTAR PUSTAKA

[1] S. Permatasari, A. I. Gufroni, and D. N. Widiyasono, "Analisis Mobile Forensic dengan Menggunakan Metode Hybrid Evidence Investigation pada Smartphone," *Univ. Siliwangi Tasikmalaya*, pp. 1–6, 2015.

[2] D. Rachmawati, "Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber," *J. Ilm. Saintikom, Univ. Sumatera Utara, Medan*, vol. 1978–6603, pp. 209–216, 2014.

[3] C. F. M. Foozy, R. Ahmad, and M. A. Faizal, "A practical rule based technique by splitting SMS phishing from SMS spam for better accuracy in mobile device," *Int. Rev. Comput. Softw.*, vol. 9, no. 10, pp. 1776–1782, 2014.

[4] M. S. MAHMOD, "SMS-Phishing on Android Smart Phone," *J. Educ. Sci.*, vol. 27, no. 3, pp. 120–135, 2018, doi: 10.33899/edusj.2018.159322.

[5] M. Computing, "a Review on Phishing," vol. 4, no. 2, pp. 166–170, 2015.

[6] R. Khan, K. Mclaughlin, D. Laverty, and S. Sezer, "STRIDE-based Threat Modeling for Cyber-Physical Systems," 2018.