STANDAR NASIONAL INDONESIA UNTUK KEAMANAN APLIKASI *MOBILE*

Yumarsono Muhyi
Sistem Komputer, STMIK Indonesia
Jl. Siantar No. 6, Cideng – Gambir, Jakarta 10150 – Indonesia
email: muhyi@stmik-indonesia.ac.id, y.muhyi@gmail.com

Abstrak *– Pemerintah Indonesia telah mulai membuat Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang di dalamnya terdapat beberapa amanat perundangan lanjtan. Pemerintah Indonesia juga telah membuat beberapa peraturan dan standar, terkait dengan UU ITE ini. Namun dengan munculnya Next-Generation Network (yaitu konvergensi: pengguna, perangkat handphone, aplikasi, dan sistem/layanan) dandengan semakin meningkatnya jumlah dan kualitas kasus kriminalitas di dunia Internet, Pemerintah Indonesia perlu segera membuat suatu standar kemanan aplikasi* handphone*, yaitu berupa Standar Nasional Indonesia Untuk Keamanan Aplikasi* Mobile*, untuk melindungi aplikasi para pengguna* handphone *di Indonesia dari serangan kriminal di Internet.*

Kata Kunci*: SNI, standar, keamanan, aplikasi, mobile*

I. PENDAHULUAN

Istilah ”*security*” atau ”keamanan” telah menjadi bagian dari publik, sejak perkembangan pesat Internet dan *handphone*. Banyak aspek telah dicakup dalam keamanan Internet, termasuk informasi. Pemerintah Indonesia telah membuat sebuah langkah besar untuk ikut kepatutan dalam masalah keamanan Internet, dengan membuat Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagai perundangan dasar.

Banyak peraturan lain muncul berdasarkan UU ITE ini: peraturan-peraturan penyelenggaraan layanan elektronik, peraturan-peraturan perangkat/hardware, peraturan-peraturan isi informasi, standar-standar keamanan, dan masih banyak lagi. Ini menggambarkan fokus Pemerintah Indonesia akan keamanan publik.

Dalam tulisan ini, penulis mengajukan sebuah aspek penting yang perlu diurus: aplikasi-aplikasi *mobile/handphone*. Dengan mengeksplorasi dan menganalisa aspek ini lebih dalam, semoga dapat membuka kesadaran Pemerintah Indonesia akan pentingnya keamanan aplikasi *mobile*, dan membuat sebuah standar keamanan untuk itu, berupa Standar Nasional Indonesia (SNI) Untuk Keamanan Aplikasi *Mobile*.

Metode penelitian yang penulis gunakan dalam tulisan ini adalah studi literatur dan observasi umum. Adapun aspek kajian yang penulis ambil adalah bidang kajian hukum dan perundangan, bukan aspek penelitian teknis atau aspek empiris. Analisa yang dilakukan adalah berupa *gap analysis* (analisis kesenjangan) yang masih awal dan relatif sederhana, untuk melacak apa yang kurang dan perlu dipenuhi, terkait dengan keamanan aplikasi *mobile*, yang kini sedang sangat tren dan sudah menjadi bagian dari kehidupan penduduk Indonesia secara umum.

Pembahasan dan analisa kesenjangan dalam tulisan ini penulis bagi menjadi 3 (tiga) bagian: (1) peraturan dan perundangan yang telah dibuat oleh pemerintah Indonesia (dimasukkan dalam bagian Landasan Teori), (2) perkembangan mutakhir (dan prediksi masa depan) tentang aplikasi *mobile* (dimasukkan dalam bagian Pembahasan) dan serangan dalam dunia Internet, dan (3) aspek keamanan aplikasi *mobile* yang belum ada dan perlu dibuatkan diadopsi dalam peraturan dan perundangan di Indonesia (dimasukkan dalam kesimpulan).

II. LANDASAN TEORI

2.1. Permasalahan Umum Keamanan Informasi

Keamanan informasi dalam dunia Internet memiliki kaidah umum, bahwa ada 3 (tiga) hal yang harus dijaga dalam jejaring komputer [4], yaitu:

1. *Confidentiality* atau kerahasiaan data.
2. *Integrity* atau keutuhan/kebenaran data.
3. *Availability* atau ketersediaan data.

Ketiga hal di atas itulah yang menjadi ukuran keamanan informasi. Apabila terjadi serangan, maka tujuan dari serangan tidak lain adalah salah satu, atau beberapa hal, atau mungkin semua dari ketiga aspek penjagaan tersebut.

Ada pun teknik-teknik dalam menghadapi serangan (atau *countermeasure*) [4] adalah:

1. *Preventive* atau pencegahan sebelum terjadinya serangan.
2. *Detective* atau pelacakan serangan ketika sedang terjadi.
3. *Corrective* atau perbaikan ketika serangan telah terjadi.

2.2. Peraturan dan Perundangan Indonesia di Bidang Informasi

Pemerintah RI sejauh ini telah melakukan beberapa kemajuan besar dalam melakukan perlindungan dari bahaya serangan terhadap data, yaitu dengan menerbitkan dua peraturan penting [2]:

1. Undang-undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).
2. Surat Edaran Menteri KOMINFO No. 05/SE/M.KOMINFO/07/2011 tentang, ”Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik”.

Dari UU ITE tersebut, maka dapat diturunkan 9 (sembilan) amanat yang harus dibuat dan direalisasikan oleh Pemerintah RI berupa Peraturan Pemerintah (PP) [2], yaitu:

1. Lembaga Sertifikasi Keandalan: pasal 10 ayat 2.
2. Tanda Tangan Elektronik: pasal 11 ayat 2.
3. Penyelenggaara Sertifikasi Elektronik: pasal 13 ayat 6.
4. Penyelenggaa Sistem Elektronik: pasal 16 ayat 2.
5. Penyelenggara Transaksi Eletronik: pasal 17 ayat 3.
6. Penyelenggara Agen Elektronik: pasal 22 ayat 2.
7. Pengelolaan Nama Domain: pasal 24.
8. Tata Cara Intersepsi: pasal 31 ayat 4.
9. Peran Pemerintah dalam Pemanfaatan TIK (Teknologi informasi dan komunikasi): pasal 40.

2.3. Standar-Standar Keamanan Informasi di Indonesia

Dari Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik [5], Pemerintah RI telah memetakan beberapa hal penting terkait informasi yang harus diamankan. Pementaan ini kemudian dibakukan menjadi Standar Sistem Manajemen Keamanan Informasi (SMKI).

Standar SMKI ini sebetulnya adakan penyelearasan atau penyesuaian (*conformity*) atas standar-standar kemanan informasi yang telah dibuat sebelumnya di dunia internasional berupa *Information Security Management Systems* (ISMS), dan diadopsi oleh Badan Standarisasi Nasional (BSN) untuk menjadi Standar Nasional Indonesia (SNI).

Standar-standar internasional atas keamanan informasi itu adalah [5]:

1. ISO/IEC 27000:2009 ISMS Overview and Vocabulary
2. ISO/IEC 27001:2005 ISMS Requirements.
3. ISO/IEC 27002:2005 Code of Practice for ISMS.
4. ISO/IEC 27003:2010 ISMS Implementation Guidance.
5. ISO/IEC 27004:2009 ISMS Measurements.
6. ISO/IEC 27005:2008 Information Security Risk Management.
7. ISO/IEC 27006: 2007 ISMS Certification Body Requirements.
8. ISO/IEC 27007 Guidelines for ISMS Auditing.

Tujuan inti dari SMKI ini adalah melindungi aset informasi instansi penyelenggara layanan publik dari segala bentuk ancaman, baik eksternal maupun internal, sengaja atau tidak [5].

Yang termasuk aset informasi di sini adalah (tapi tidak terbatas pada):

1. Data dan Informasi.
2. *Software.*
3. *Hardware.*
4. Perangkat Jaringan Komunikasi.
5. Fasilitas Pendukung.
6. Sumber Daya Manusia.

Kemudian ditetapkanlah suatu standar penilaian atas perlindungan aset informasi, berupa Indeks Keamanan Informasi (disingkat menjadi KAMI). Indeks KAMI menganalisa 5 (lima) aspek [5]:

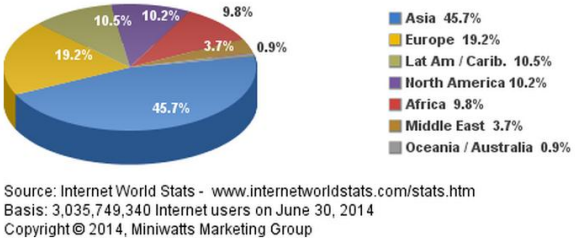
1. Tata Kelola Keamanan Informasi.
2. Pengelolaan Risiko Keamanan Informasi.
3. Kerangka Kerja Keamanan Informasi.
4. Pengelolaan Aset Informasi.
5. Teknologi dan Keamanan Informasi.

Indeks KAMI ini memiliki tingkat-tingkat kematangan, yang menggambarkan kesiapan suatu Penyelenggara Pelayanan Publik dalam menjaga keamanannya. Tingkat-tingkat kematangan itu mengacu ke COBIT (*Control Objective for Information and related Technology*) atau CMMI (*Capability Maturity Model for Integration*) sebagai landasan penilaiannnya [5], yaitu:

1. Tingkat 0: Tidak Diketahui (PASIF).
2. Tingkat I: Kondisi Awal (REAKTIF).
3. Tingkat II: Penerapan Kerangka Kerja Dasar (AKTIF).
4. Tingkat III: Terdefinisi dan Konsisten (PRO AKTIF).
5. Tingkat IV: Terkelola dan Terukur (TERKENDALI).
6. Tingkat V: Optimal (OPTIMAL).

III. PEMBAHASAN

3.1. Kondisi Akses Publik Indonesia Akan Informasi



Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 3,035,749,340 Internet users on June 30, 2014
Copyright © 2014, Miniwatts Marketing Group

Gambar 1. Pengguna Internet Dnnia

Dari seluruh penduduk dunia yang lebih dari 7 miliar manusia, maka tidak kurang dari 42% dari mereka adalah pengguna Internet, atau lebih dari 3 miliar orang pengguna Internet. Dan dari seluruh pengguna Internet itu, Indonesia memiliki porsi tidak kurang dari 5% sebagai pengguna Internet dunia [1].

China *	1,355,692,576	22,500,000	**642,261,240**	47.4 %	46.3 %	633,300
Georgia	4,935,880	20,000	**2,188,311**	44.3 %	0.2 %	911,900
Hong Kong *	7,112,688	2,283,000	**5,751,357**	80.9 %	0.4 %	4,034,560
India	1,236,344,631	5,000,000	**243,000,000**	19.7 %	17.5 %	62,713,680
Indonesia	253,609,643	2,000,000	**71,190,000**	28.1 %	5.1 %	51,096,860
Japan	127,103,388	47,080,000	**109,626,672**	86.2 %	7.9 %	17,196,080

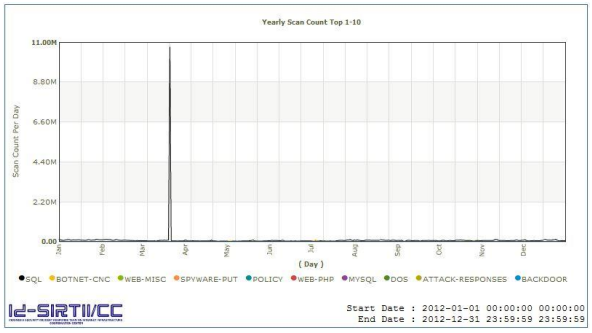
Gambar 2. Pengguna Internet Indonesia

Dengan porsi sebesar ini, maka Indonesia menduduki peringkat ke-4 pengguna Internet terbesar di Asia. Berturut-turut peringkat di atas Indonesia adalah: Cina (46,3%), India (17,5%), dan Jepang (7,9%) [1]. Angka ini tentu merupakan prestasi dan potensi positif yang sangat besar untuk Indonesia dalam mengembangkan dirinya dan memposisikan dirinya di dunia Internasional. Berbagai wacana telah digulirkan untuk membahas potensi positif ini.

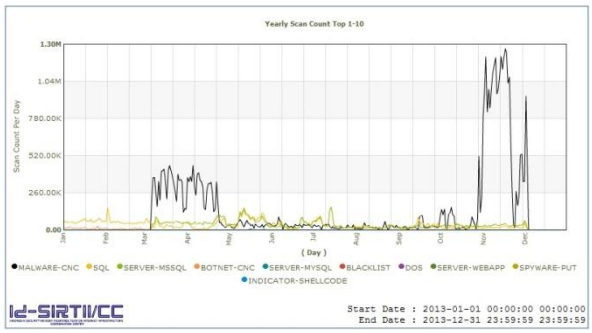
3.2. Kondisi Kejahatan Dunia Maya di Indonesia

Tapi di sisi lain, ada efek negatif dan potensi negatif yang telah ada dan menghadang di depan, yaitu: kriminalitas di dunia *cyber*/maya (Internet) atau disebut *cyber crime*. *Cyber crime* ini semakin drastis peningkatannya, seiring dengan semakin banyaknya pengguna Internet di Indonesia [2]. Menurut data pemantauan *Indonesia Security Incident Response Team on Internet and Infrastructure/Coordination Center* (Id-SIRTII/CC) [3], sejak tahun 2012 hingga tahun 2015, terlihat pola kenaikan yang konstan dan mungkin bisa dikategorikan darurat masa depan.

Dari gambar-gambar pemantauan Id-SIRTII/CC berikut ini, akan terlihat pola yang sangat mengkhawatirkan. Bila pada tahun 2012 hanya ada serangan Internet pada satu waktu peak atau puncak, dan dengan durasi yang sangat pendek, hanya beberapa hari di bulan Maret tahun 2012. Tapi bila kita lihat pada tahun 2013, maka para kriminal Internet ini telah 'belajar' dan semakin bersungguh-sungguh melakukan kejahatan. Pada tahun 2013, serangan Internet terjadi di sepanjang bulan Maret dan April 2013.

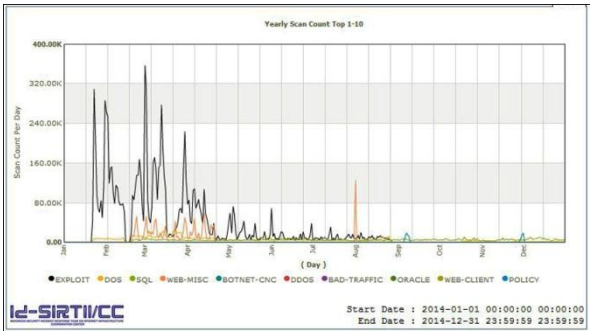


Gambar 3. Serangan Tahun 2012

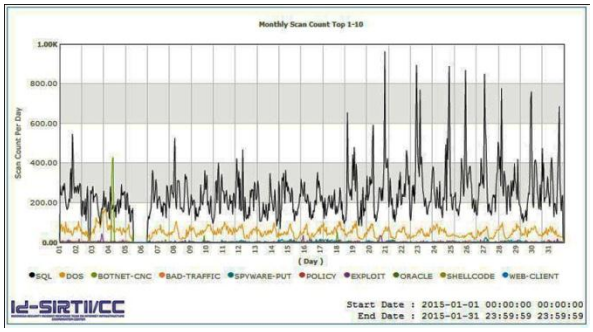


Gambar 4. Serangan Tahun 2013

Pada tahun 2014 memang sempat terjadi penurunan yang signifikan di akhir tahun, setelah di awal hingga pertengahan tahun 2014 tetap terjadi serangan. Kemungkinan di akhir tahun 2014 ini serangan Internet menurun, karena aktivitas pemantauan Internet oleh Kepolisian Republik Indonesia (RI) sangat ketat, berkaitan dengan Pemilihan Presiden 2014 yang cukup menarik perhatian masyarakat Indonesia pada waktu itu. Namun pada bulan Januari 2015 terlihat bahwa ternyata serangan Internet menjadi jauh lebih gencar lagi, dan lebih konsisten.



Gambar 5. Serangan Tahun 2014

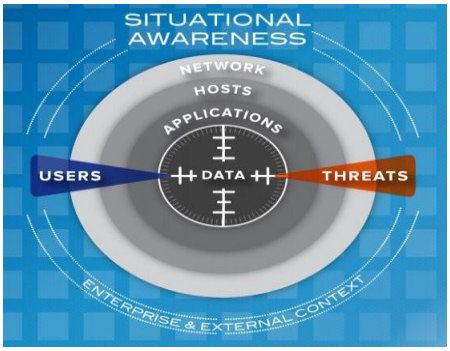


Gambar 6. Serangan Bulan Januari Tahun 2015

Data ini semua menggambarkan bahwa kriminalitas di dunia Internet sangat membahayakan, dan darurat masa depan. Polanya sangat jelas sekali, bahwa peningkatan aktivitas serangan Internet terus meningkat dengan sangat tajam. Dan ini tidak hanya membahayakan Pemerintah RI, tapi juga seluruh masyarakat Indonesia secara luas.

Serangan yang terjadi ini bukan hanya banyak dari sisi kuantitas, tapi juga banyak dari sisi jenis serangannya. Dari gambar di bawah ini terlihat, bahwa dari semua jenis serangan itu, yang terbanyak [2] adalah:

1. *Web defacement*, yaitu serangan terhadap basis data suatu web server, dengan tujuan mengubah atau merusak tampilan suatu laman web.
2. *Malware/malicious code*, yaitu serangan virus yang kebanyakan adalah virus lokal.
3. *Scam*, yaitu penipuan berupa berita bohong yang sengaja disebarkan atau dikirim oleh pelakunya demi mendapatkan keuntungan (dengan makna yang luas, tidak hanya finansial).
4. *Spam*, yakni masuknya informasi yang tidak diinginkan ke dalam jalur komunikasi, yang dulu hanya lewat surel (surat elektronik atau *email*), kini telah masuk ke media seluler melalui SMS dan MMS.

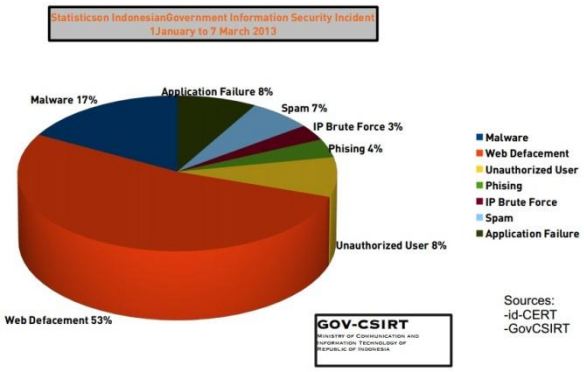


Gambar 7. Serangan Terhadap Data

3.3. *Next-Generation Network* (NGN)

Sudah sejak lama berbagai peneliti di dunia TIK terus berusaha melacak dan memperkirakan arah perkembangan TIK, bahkan ini telah dilakukan sejak pertama kali arsitektur komputer itu dibuat oleh Von Neumann tahun 195, hingga sekarang ini. Berbagai buku teks tentang sejarah dan pengantar TIK di Amerika Serikat telah merekam upaya-upaya para peneliti dari berbagai bidang, untuk memperkirakan perkembangan TIK di masa depan.

Di era TIK moderen sekarang ini, umumnya analisa perkiraan perkembangan TIK di masa depan sudah semakin akurat dan mendekati kebenaran. Para peneliti kini merumuskan, bahwa kesemua aspek TIK akan semakin konvergen ke arah tertentu, yang disebut sebagai *Next-Generation Network* (NGN), sebagai mana pada Gambar 9.

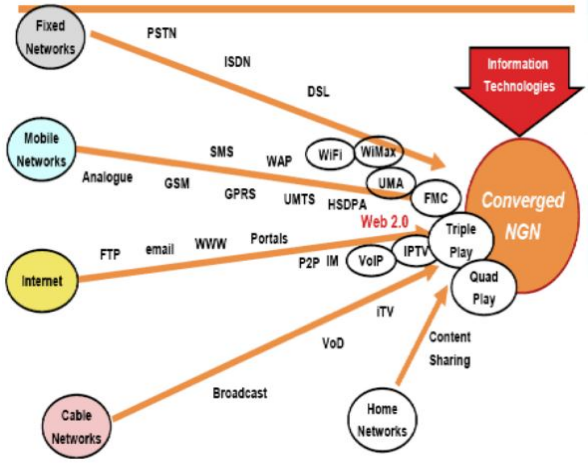


Gambar 8. Tipe Serangan Terbanyak

Konvergensi dari banyak faktor ini kemudian dikategorikan menjadi 4 (empat) faktor dominan [6], yaitu:

1. *Ubiquitous connectivity*, orang saling terhubung karena teknologi yang semakin pribadi.
2. *Increasingly smart device*, semakin banyaknya perangkat cerdas.
3. *Pervasive content*, materi-materi yang semakin pribadi.
4. *Customer demand*, permintaan pelanggan.

Keempat faktor ini saling berharmonisasi yang akhirnya menciptakan masa depan baru: jejaring dalam jumlah yang luar biasa dan saling berkaitan, sebagaimana digambarkan di bawah ini, ke suatu kondisi yang disebut sebagai "*Tera-Play*" [6].



Gambar 9. ***Next-Generation Network***

Pada tahun 2009, Amdocs memprediksi dengan cukup akurat (dengan kenyataan di tahun 2014 lalu) bahwa [6]:

- Pada tahun 2011, pengguna biasa dari Internet akan mengkonsumsi data 20 GB (*giga bytes*) setiap harinya.
- Miliaran unduhan untuk lagu dan *mobile apps*.
- Pada tahun 2012 di setiap orang 16 negara akan memiliki lebih dari satu akses *wireless broadband*.
- *Blackberry* dan *iPhone* hanya awal saja, nanti yang terhubung ke jejaring dunia tidak lagi hanya *handphone*.
- Konsumen pada tahun 2012 akan membayar total sebesar US$ 700 miliar, hanya untuk bertahan agarg bisa terkoneksi online.
- Pada tahun 2012 diperkirakan akan ada 1,4 miliar pengguna Internet yang *mobile* (menggunakan *handphone* atau piranti bergerak lainnya). Pada tahun 2013 diperkirakan 64% penggunakan *mobile* Internet adalah untuk video.

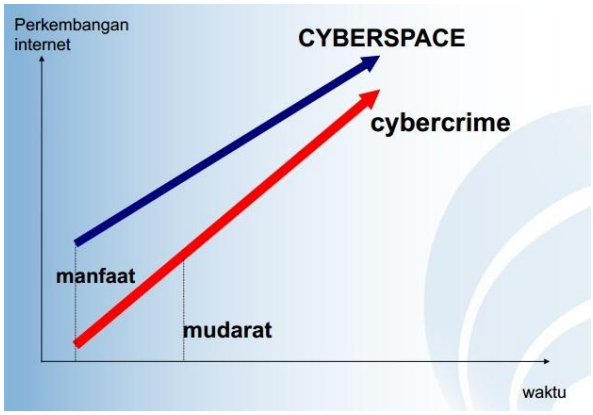
Gambar 10. Faktor-Faktor NGN

3.4. Keamanan Aplikasi *Mobile*

Dari analisa-analisa terkait dengan NGN, baik dari sisi: konvergensi TIK, teknologi yang semakin pribadi, maupun prediksi tingginya jumlah pengguna *mobile* Internet, maka dapat disimpulkan bahwa semua akan berfokus bukan lagi ke publik secara kelompok, tapi ke individu atau orang per orang pengguna Internet. Ini tentu merupakan hal yang positif dan memiliki potensi positif yang luar biasa, baik untuk individu atau pun untuk negara Indonesia dan Pemerintah RI.

Pertumbuhan jumlah pengguna Internet yang sangat signifikan, juga mendorong kerawanan yang signifikan. Bahkan diperkirakan bahwa potensi kerawanan terjadinya kriminalitas itu memiliki kecenderungan (tren) pertumbuhan yang lebih cepat dari kecenderungan pertumbungan jumlah pengguna Internet itu sendiri [2]. Yang artinya bahwa akan ada suatu waktu, jika tidak diantisipasi dengan serius, tingkat kejadian kriminalitas akan ’meledak’ jauh melebihi jumlah pengguna Internet itu sendiri.

Karena teknologi semakin konvergen dan semakin pribadi, maka kejahatan Intenet pun juga akan lebih dan sangat fokus ke pribadi-pribadi pengguna Intenet. Dan ini adalah ancaman serius atau potensi negatif yang sangat tinggi. Karena dari beberapa tatanan hukum yang sedikit diulas dalam tulisan ini, dan produk-produk hukum terkait Internet yang dilahirkan oleh Pemerintah RI melalui Kementerian Komunikasi dan Informatika, Pemerintah Indonesia berfokus kepada pengamanan instansi pemerintah dan lembaga layanan publik. Sementara para individu pengguna Internet, yang merupakan subjek dan objek paling dominan dalam urusan akses Internet, masih kurang diperhatikan.



Gambar 11. Kemajuan Internet vs Kejahatan Internets

IV. KESIMPULAN

Dari pembahasan dalam tulisan ini, tentang perkembangan pengguna Internet yang tinggi serta semakin meningkatnya kriminalisme dalam dunia Internet, terlihat bahwa aplikasi *mobile* kini menjadi aspek yang sangat penting untuk diatur dalam peraturan dan perundangan di Indonesia.

Cara paling jitu dalam mengantisipasi sejak dini akan adanya 'ledakan' kriminalitas di dunia Internet yang sangat ramai dengan penggunanya, adalah dengan bertindak secara preventif untuk mencegah terjadinya serangan secara perorangan atau individu. Diharapkan dengan langkah ini, kejahatan Intenet dapat dicegah dan dilacak keberadaan pelakunya untuk ditindak.

Para pengguna mobile Internet ini dapat dipastikan mereka mengaksesnya dari aplikasi mobile. Karena pintu masuk kejahatan Internet ini dari jalur mobile dan pribadi, maka Pemerintah RI perlu mengupayakan suatu standar pengamanan untuk pribadi *mobile* dan pribadi dari pengguna Internet. Pola analisanya sama dengan analisa SMKI dan Indeks HAKI, hanya saja kini pembahasannya adalah aplikasi *mobile*.

ISO (*International Standardization Organization*) sendiri masih belum memiliki aturan yang pas untuk menjamin kemanan aplikasi *mobile*. Namun ada beberapa ISO terkait aplikasi *mobile* yang bisa direferensikan untuk dijadikan bahan kajian SNI Keamanan Aplikasi *Mobile*. Beberapa ISO itu secara urut berdasarkan relevansi adalah:

1. ISO 25000 Series [7] [8], yang membahas tentang *Software Quality Requirements* (KebutuhanKebutuhanKualitas Aplikasi), dimana aspek keamanan merupakan salah satu variabel perhitungan kualitas. ISO ini sangat tepat dijadikan kerangka acuan dan diadopsi untuk menyusun SNI Keamanan Aplikasi Mobile. ISO ini sudah tuntas sejak 2004, dan sudah matang untuk diadopsi menjadi SNI.
2. ISO/IEC 27034-1:2011 [9], yang membahas tentang keamanan proses pembuatan/ pengembangan sistem/*software*. Konsep dari ISO ini sangat baik, dimana proses pembuatan software pun dianalisa aspek keamanannya. Ini semakin menjamin keamanan software ketika sudah sedang dikembangkan hingga selesai, yang diharapkan juga dapat menjamin keamanan software-nya nanti. ISO ini masih tahap 1, dan belum berkembang ke tahapan selanjutnya.
3. ISO/IEC 24727 [10], yang sebetulnya membahas mengenai *interfacing* untuk ID (*identity*) cards. Tapi karena ada bagian yang relevan dengan kemanan aplikasi mobile terutama dari sisi web, maka bisa dijadikan bahan kajian juga.

Semoga dengan tulisan yang singkat ini, dapat mendorong Pemerintah RI untuk mengusulkan dan mengundangkan peraturan tentang keamanan aplikasi *mobile*. Yang kemudian hal ini ditindaklanjuti oleh institusi/lembaga terkait untuk membuat SNI Kemanan Aplikasi *Mobile*. Semoga dengan adanya SNI Kemanan Aplikasi *Mobile*, maka pengguna Internet di Indonesia tidak lagi perlu khawatir dengan pencurian data pribadi lewat handphone, SMS/MMS *spam*, penipuan (*scam*), dan ancaman kejahatan Internet lainnya.

Penelitian aspek hukum dan perundangan ini masih penelitian yang sangat awal tentang perlunya SNI Aplikasi *Mobile*, namun sangat relevan untuk ditindaklanjuti dengan beberapa penelitian lanjutan, di antaranya adalah:

1. Penelitian empiris tentang statistik pengguna aplikasi *mobile* di Indonesia.
2. Penelitian empiris tentang lalu lintas transaksi ITE di Indonesia.
3. Penelitian empiris tentang kriminalisme ITE di Indonesia.
4. Kajian ilmiah dan empiris tentang relevansi perlunya SNI Keamanan Aplikasi *Mobile*.

DAFTAR REFERENSI

[1] (2015, 25 Februari) Internet world stats. [Online]. Available: http://www.internetworldstats.com.

[2] B. H. Tjahjono, "Kebijakan nasional keamanan informasi menghadapi ancaman dan tantangan global," STIKOM Bali, Indonesia, 2013.

[3] (2015, 25 Februari) Id-SIRTII/CC. [Online]. Available: http://idsirtii.or.id..

[4] R. J. Boyle and R. R. Panko, Corporate Computer Network Security, 3rd ed. New Jersey, USA: Pearson Education, 2013.

[5] T. D. K. Informasi, Panduan Penerapan Tata Kelola Keamanan In-formasi bagi Penyelenggara Pelayanan Publik. Republik Indonesia: Kementerian Komunikasi dan Informatika, 2011.

[6] Amdocs, Leading the Way to Tera-Play. Singapore: Amdocs, 2009.

[7] P. T. W. G. Dave Zubrow, Software Quality Requirements and Evalua-tion, the ISO 25000 Series. Pittsburgh, USA: Carnegie Mellon Software Engineering Institut, 2004.

[8] J. Amsenga, "An introduction to standards related to information secu-rity," University of Johannesburg, South Africa, 2008.

[9] R. C. Group, The Emergence of Software Security Standards: ISO/IEC 270341:2011 and Your Organization. Reavis Consulting Group, 2013.

[10] D. H. M. B. Jan Eichholz, Detlef Houdeau, "ISO/IEC 24727 for secure mobile web applications," http://www.w3.org, 2008.

Biodata Penulis

Yumarsono Muhyi, lahir di Jakarta pada 21 Februari 1978. Lulus tahun 2001 dari program sarjana Institut Teknologi Bandung (ITB), jurusan Teknik Elektro, konsentrasi Telekomunikasi. Tahun 2010 penulis lulus dari Universitas Pembangunan Veteran (UPNJ) Jakarta, program Magister Manajemen. Penulis pada tahun 2014 mengambil lagi program Magister Komputer di STMIK Nusa Mandiri, Jakarta.

Minat penulis mempelajari dan mengajarkan agama, membimbing penulis sempat mengecap program diploma jurusan Bahasa Arab di *Ma'had Al-Imaaraat* di Bandung pada tahun 2014.

Penulis kini juga beasiswa program sarjana Ilmu Syariah (Fikih) di Lembaga Ilmu Pengetahuan Islam dan Arab (LIPIA) atau *Ma'had Al-'Uluum Al-Islaamiyyah wa Al-'Arabiyyah*, di Jakarta pada tahun 2014, untuk program Pembelajaran Jarak Jauh (*ta'liim an bu'd*), kini masuk semester ke-4 dari 9 semester di kampus berkurikulum internasional ini.