TUGAS MAKALAH

EL6115 – OPERASI KEAMANAN DAN RESPON INSIDEN

OPERASI KEAMANAN PADA PERANGKAT SELULER BISNIS UNTUK MENCEGAH SPIONASE DIGITAL

MOCHAMAD BETA AUDITAMA

23215125

MAGISTER TEKNIK ELEKTRO

SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA

INSTITUT TEKNOLOGI BANDUNG

2015

ABSTRAK

OPERASI KEAMANAN PADA PERANGKAT SELULER BISNIS UNTUK MENCEGAH SPIONASE DIGITAL

Oleh

MOCHAMAD BETA AUDITAMA

NIM : 23215125

PROGRAM STUDI TEKNIK ELEKTRO

Belakangan ini, ancaman *cyber* berupa praktik spionase digital sering terjadi, terutama di sektor bisnis. Tujuan *attacker* melakukan spionase digital adalah memperoleh informasi-informasi rahasia milik entitas dan/atau personal tertentu untuk kepentingannya sendiri, seperti finansial, politik, dan lain-lain. Praktik spionase digital dapat dilakukan melalui dua metoda, yaitu menggunakan agen terlatih untuk memperoleh informasi secara fisik, atau menginfiltrasi sistem komputer secara ilegal (*hacking*). Perolehan informasi melalui *hacking* lebih mudah untuk dilakukan apabila dibandingkan dengan menggunakan agen terlatih karena sifatnya yang fleksibel (serangan dapat dilakukan secara lintas negara selama jaringan-jaringan komputer terkoneksi satu sama lain), cepat, dan dapat dilakukan secara masif. Salah satu perangkat jaringan yang dapat dijadikan target spionase digital adalah perangkat seluler bisnis. Sebelum *attacker* mengakuisisi informasi-informasi rahasia yang tersimpan di perangkat seluler, *attacker* harus mengendalikan perangkat seluler terlebih dahulu dengan meng-*compromise* perangkat seluler melalui perangkat lunak dan perangkat keras. Proses *compromise* perangkat seluler melalui perangkat lunak dapat dilakukan dengan beberapa cara, yaitu dengan memasukkan *malware*, melakukan *spear phising*, mengekploitasi sosial media yang dimiliki oleh pengguna perangkat seluler, dan memasang aplikasi jahat. Proses *compromise* perangkat seluler melalui perangkat keras dapat dilakukan dengan beberapa cara, di antaranya mengeksploitasi *audio jack* dan memasang cip mata-mata pada perangkat seluler. Makalah ini akan membahas mengenai operasi keamanan pada perangkat seluler bisnis dengan melibatkan konsep-konsep tata kelola perangkat seluler bisnis secara terpusat.

Kata kunci: Spionase Digital, *Hacking*, Perangkat Seluler, Tata Kelola Perangkat Seluler Bisnis secara Terpusat, dan Operasi Keamanan pada Perangkat Seluler Bisnis..

Daftar Isi

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Berdasarkan [21], belakangan ini, ancaman *cyber* berupa praktik spionase digital sering terjadi, terutama di sektor bisnis. Tujuan *attacker* melakukan spionase digital adalah memperoleh informasi-informasi rahasia milik entitas dan/atau personal tertentu untuk kepentingannya sendiri, seperti finansial, politik, dan lain-lain. Oleh karena itu, *attacker* bersedia untuk mengalokasikan waktu dan sumber daya yang dimilikinya untuk mengetahui informasi yang dimiliki oleh pihak tertentu. Namun, perlu diperhatikan di sini, *attacker* melakukan spionase digital bukanlah untuk memperoleh seluruh informasi yang dimiliki oleh pihak yang dijadikan target spionase, melainkan *attacker* menganggap target spionase berpotensi memiliki informasi-informasi yang berkaitan atau bermanfaat bagi *attacker*. Oleh karena itu, *attacker* tidak akan melakukan praktik spionase secara serta-merta.

Praktik spionase digital dapat dilakukan melalui dua metoda, yaitu menggunakan agen terlatih untuk memperoleh informasi secara fisik, atau menginfiltrasi sistem komputer secara ilegal (*hacking*) [21]. Perolehan informasi melalui *hacking* lebih mudah untuk dilakukan apabila dibandingkan dengan menggunakan agen terlatih karena sifatnya yang fleksibel (serangan dapat dilakukan secara lintas negara selama jaringan-jaringan komputer terkoneksi satu sama lain), cepat, dan dapat dilakukan secara masif [21]. Salah satu contoh riil praktik spionase digital, yaitu sebagai berikut :

Menurut [6], lima negara di benua Eropa Utara (disebut *Nordic states*), antara lain, Denmark, Finlandia, Islandia, Norwegia, dan Swedia, mengalami serangan *cyber* yang merugikan sektor pemerintahan dan industri dari kelima negara tersebut. Serangan *cyber* dilakukan dalam bentuk spionase digital. Spionase digital ini dilakukan oleh grup APT Rusia dan Tiongkok yang didanai dan didukung oleh masing-masing negara. Motif serangan *cyber* adalah memperoleh data rahasia negara, data personal yang bersifat sensitif, data keuangan, dan hak kekayaan intelektual milik industri dan pemerintah *Nordic states*. Kemungkinan, data yang diperoleh akan digunakan oleh pemerintah Rusia dan Tiongkok untuk kepentingan ekonomi,

militer, dan politiknya. Dengan memiliki produk-produk serta teknologi milik negara pesaing, Rusia dan Tiongkok dapat mempercepat perkembangan industri domestiknya serta memonopoli transaksi jual-beli di pasar global.

Salah satu perangkat jaringan yang dapat dijadikan target spionase digital adalah perangkat seluler bisnis. Pernyataan ini sesuai dengan [25] yang menyatakan bahwa perangkat seluler saat ini terintegrasi sangat baik dengan internet, memiliki lebih banyak fungsionalitas apabila dibandingkan dengan perangkat seluler sebelumnya, dan menyimpan banyak informasi sensitif, baik itu informasi milik organisasi maupun personal. Dengan demikian, perangkat seluler bisnis menjadi target yang menarik bagi *attacker* untuk dieksploitasi *resource*-nya [25]. Sebelum *attacker* mengakuisisi informasi-informasi rahasia yang tersimpan di perangkat seluler, *attacker* harus mengendalikan perangkat seluler terlebih dahulu dengan meng-*compromise* perangkat seluler melalui perangkat lunak dan perangkat keras. Berikut beberapa contoh *attacker* dapat meng-*compromise* perangkat seluler melalui perangkat lunak dan perangkat keras sebagai berikut :

- Flame [2].

  Malware Flame memiliki ukuran *file* yang cukup besar. Besarnya ukuran *file malware* ini diiringi dengan banyaknya fungsionalitas yang dimiliki oleh Flame. Flame terdiri atas beberapa modul, tetapi modul-modul tersebut hanya dibagi menjadi dua kategori, yaitu modul utama dan modul pendukung (modul yang lebih kecil dari modul utama). Modul utama Flame merupakan *file* berformat DLL yang diberi nama `mssecmgr.ocx`. Saat menginfeksi sistem komputer, `mssecmgr.ocx` dapat berwujud *big version* atau *small version*. Untuk *big version*, ukuran *file* `mssecmgr.ocx` adalah 6 MB karena modul utama pada versi ini juga membawa modul-modul pendukung. Untuk *small version*, ukuran *file* `mssecmgr.ocx` hanya 900 KB karena tidak membawa modul-modul pendukung. Setelah proses pemasangan dilakukan, *file* `mssecmgr.ocx` *small version* baru mengunduh modul-modul pendukung dengan cara melakukan koneksi ke *server Command and Control* (C&C). Perlu diketahui, nama modul utama dapat saja bukan `mssecmgr.ocx` karena penamaan modul utama ini tergantung pada metoda infeksi dan *internal state* dari Flame saat ini, seperti instalasi, replikasi, atau *upgrade*. Contoh nama lain dari `mssecmgr.ocx`, yaitu `wavesup3.drv`, `~zff042.ocx`, dan `msdclr64.ocx`.

Tabel 1. Tiga Unit *Malware* Flame [2].

Unit	Deskripsi
Beetlejuice	*Bluetooth* : Mengenumerasi perangkat-perangkat yang terdapat di sekitar laptop atau *desktop* yang telah terinfeksi. Laptop atau *desktop* dapat mengaktifkan "suar" secara otomatis : Meng-umumkan laptop atau *desktop* sebagai perangkat yang *discoverable* dan meng-*encode* status *malware* yang terdapat pada informasi perangkat menggunakan base64.
Microbe	Merekam suara audio yang berasal dari perangkat keras laptop atau *desktop* tertentu : Mengenumerasi seluruh perangkat multimedia yang dimiliki, menyimpan konfigurasi lengkap dari setiap perangkat multimedia, dan memilih perangkat rekaman yang diinginkan.
Infectmedia	Menginfeksi media, seperti *Universal Serial Bus* (USB) *disk*, menggunakan metoda Autorun_infector atau Euphoria.

Tahap pertama instalasi Flame adalah proses inisiasi (*running*) *file* `mssecmgr.ocx` oleh salah satu dari dua jenis fitur eksternal, yaitu penggunaan *file* MOF oleh Windows WMI apabila memanfaatkan kerentanan MS10-061, atau menggunakan *file* BAT sbb :

```
s1 = new ActiveXObject("Wscript.Shell");
s1.Run("%SYSTEMROOT%system32rundll32.exe msdclr64.ocx, DDEnumCallback");
```

Setelah proses inisiasi selesai, `mssecmgr.ocx` melakukan registrasi dirinya sendiri sebagai *custom authentication package* di *registry* Windows :

```
HKLM_SYSTEMCurrentControlSetCOntrolLsa
Authentication Packages = mssecmgr.ocx [added to existing entries]
```

Tujuan dari proses registrasi di atas adalah menjalankan modul utama Flame secara otomatis oleh sistem operasi pada sistem *booting* berikutnya. Setelah proses registrasi selesai, `mssecmgr.ocx` mengekstraksi dan memasang modul-modul pendukung yang masih dalam kondisi terenkripsi dan terkompresi pada *resource* 146. *Resource* 146 juga berisi opsi-opsi konfigurasi untuk `mssecmgr.ocx` dan nilai-nilai parameter yang akan diberikan ke modul-modul pendukung (misal kunci dekripsi) agar modul-modul tersebut dapat dijalankan. Setelah instalasi modul-modul pendukung selesai, `mssecmgr.ocx` menjalankan *thread-thread* tertentu menggunakan modul-modul pendukung untuk membangun komunikasi dengan *server* C&C, *host interpreter* Lua, dan fitur-fitur lainnya, tergantung dari opsi konfigurasi `mssecmgr.ocx` yang dipilih. Fungsionalitas Flame, atau lebih tepatnya, fungsionalitas dari modul-modul Flame dipecah menjadi beberapa unit. Tiga unit dari dua puluh unit yang tersedia diperlihatkan pada Tabel 1.

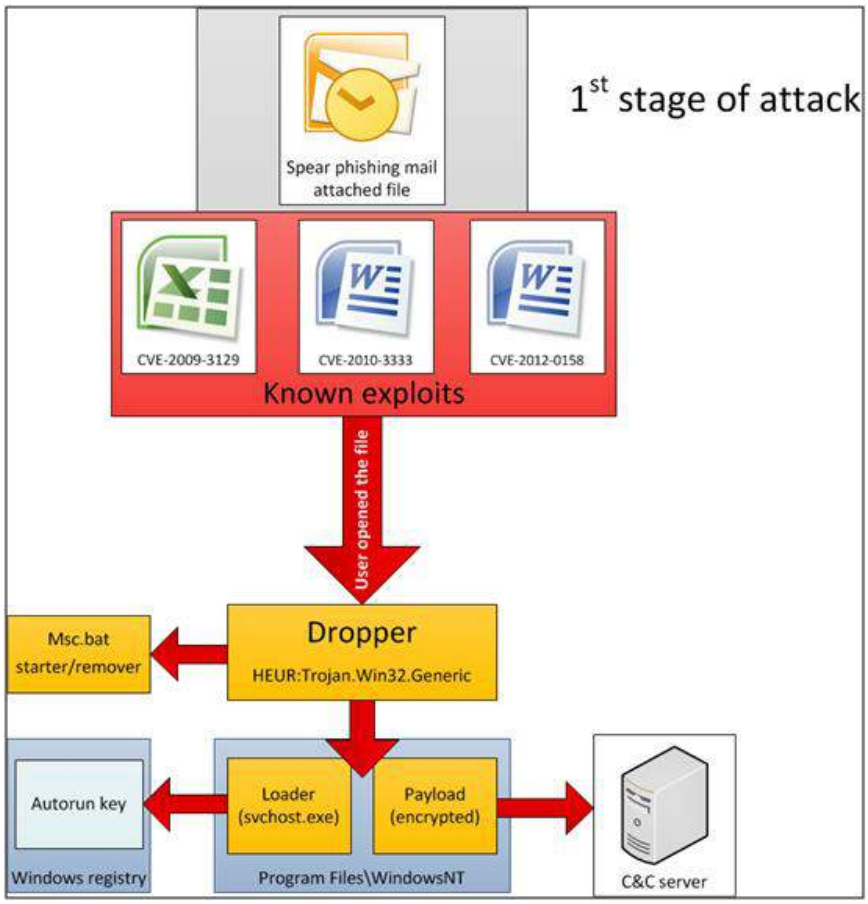
Gambar 1. Negara-negara Korban Red October [11].

- Red October [11].

  Selama lima tahun, suatu aksi spionase digital telah berhasil menginfiltrasi jaringan komputer diplomatik, pemerintah, dan organisasi riset sains dengan tujuan mengambil data yang tersimpan di perangkat seluler, sistem komputer, dan perangkat jaringan tertentu (misal *router*). Target serangan spionase digital adalah negara-negara Eropa Barat, Eropa Timur, mantan anggota USSR, Asia (termasuk negara Indonesia), dan Amerika Utara (lihat Gambar 1). Aksi spionase digital ini dinamakan Red October yang mana data yang diperoleh dikirim ke *server* C&C melalui konfigurasi yang hampir sama dengan Flame.

  Beberapa hal yang perlu diperhatikan terkait serangan Red October :

  - *Attacker* menanamkan *botnet* pada target jaringan komputernya. *Botnet* ini digunakan untuk mengifeksi suatu jaringan komputer agar dapat dikendalikan secara jarak jauh. Dalam mengendalikan jaringan komputer yang telah diinfeksi, *attacker* membuat enam puluh nama domain dan beberapa *server hosting* di beberapa negara, terutama Rusia dan Jerman. Hal ini dilakukan untuk mengimplementasikan konfigurasi C&C-nya, yaitu *framework* berupa rantai *server* yang beroperasi sebagai *proxy* untuk menyembunyikan lokasi dari *server* "kapal induk" C&C yang sebenarnya.



Gambar 2. Tahap Pertama Serangan Red October [11].

- *Attacker* mendesain konfigurasi C&C sedemikian rupa sehingga dapat mengumpulkan informasi secara cepat. Selain itu, konfigurasi yang dibuat juga bertujuan agar tetap memperoleh informasi melalui kanal komunikasi yang lain apabila *server* C&C yang sebenarnya dihentikan operasinya.
- Informasi yang diambil oleh *attacker* tidak hanya dari *workstation*, tetapi juga informasi yang tersimpan di media-media berikut :
  - ✓ perangkat seluler, seperti *smartphones* (iPhone, Nokia, dan Windows mobile);
  - ✓ perangkat jaringan milik organisasi (misal konfigurasi *router* Cisco);
  - ✓ *removable disk drives*, termasuk informasi yang telah dihapus;
  - ✓ *server remote* POP/IMAP atau media penyimpanan Outlook yang dijadikan tempat *database e-mail*; dan
  - ✓ *server* lokal FTP yang menyimpan *file-file* internal organisasi.
- Tahap pertama yang dilakukan attacker dalam menginfeksi jarigan komputer adalah menyebarkan *malware* pada jaringan komputer tersebut. Penyebaran *malware* memanfaatkan kerentanan CVE-2009-3129 (MS Excel), CVE-2010-3333 (MS Word), dan CVE-2012-0158 (MS Word) (lihat Gambar 2).

- Setelah berhasil memasukkan *malware*, atau dengan kata lain, menanamkan *botnet* pada target jaringan komputer, langkah selanjutnya yang dilakukan oleh *attacker* adalah menjalankan dua modul penyerangan. Modul penyerangan yang pertama adalah mengakses sistem sebagai administrator menggunakan salah satu dari dua metoda yang tersedia, yaitu memindai jaringan lokal untuk mencari apakah sistem memiliki kerentanan MS08-067, yaitu kelemahan *server* yang mengizinkan dijalankannya kode-kode perintah secara jarak jauh, atau menggunakan *database* kata sandi yang telah dibuat sendiri oleh *attacker* untuk mengakses sistem. Modul penyerangan yang kedua adalah mengumpulkan informasi-informasi tertentu dari jaringan komputer yang telah diinfeksi untuk menginfeksi *host* lain secara jarak jauh.

- Operasi Pawn Storm [14].

  Operation pawn storm bertujuan untuk melakukan spionase digital pada pengguna perangkat iOS dengan cara menginfeksi perangkat iOS tersebut melalui *malware*. Target entitas serangan operasi pawn storm, antara lain militer, pemerintah, industri pertahanan, dan media. *Malware* yang disebarkan pada operasi pawn storm merupakan generasi lanjut dari *malware* SEDNIT yang terdapat pada sistem operasi Windows. *Malware* disebarkan pada perangkat iOS dalam bentuk dua jenis aplikasi, yaitu aplikasi XAgent dan aplikasi permainan Madcap. Tujuan dari kedua *malware* ini, termasuk juga SEDNIT, adalah mencuri data personal, merekam suara audio, membuat *screenshot*, dan mengirimkan informasi-informasi tersebut ke *server* C&C.

  Terdapat dua metoda untuk menyebarkan aplikasi XAgent, yaitu sebagai berikut :

  - *attacker* dapat menyebarkan aplikasi XAgent selain dari AppStore, yaitu dengan menggunakan *custom provisioning profile*, sehingga pengguna perangkat iOS dapat mengunduh dan memasang aplikasi XAgent dalam versi *beta*; atau
  - aplikasi XAgent disebar ke perangkat iOS ketika perangkat iOS tersebut dihubungkan ke komputer yang telah terinfeksi.

  Setelah dipasang pada perangkat iOS 7, *icon* aplikasi XAgent di-*hidden* dan aplikasi dioperasikan secara *background*. Ketika aplikasi dihentikan, aplikasi akan beroperasi kembali secara otomatis. Apabila aplikasi dipasang pada perangkat iOS 8, *icon* aplikasi XAgent tidak di-*hidden* dan tidak dapat dioperasikan secara otomatis. Hal ini menunjukkan bahwa aplikasi XAgent dibuat ketika perangkat iOS masih dalam versi iOS 7.

Lebih spesifik, informasi-informasi yang diambil oleh aplikasi XAgent untuk dikirim ke *server* C&C, antara lain pesan teks, daftar kontak, foto/gambar, *geo-location*, rekaman suara audio (*malware* dapat merekam suara audiosecara otomatis), daftar aplikasi yang dipasang pada perangkat, daftar proses yang dijalankan oleh perangkat, dan status Wi-Fi. Aplikasi permainan Madcap hanya berfokus pada pengambilan informasi berupa rekaman suara audio saja. Perbedaan yang lain antara Madcap dan XAgent adalah Madcap hanya dapat diperasikan pada perangkat iOS yang telah di-*jailbreak*, sedangkan XAgent dapat dioperasikan pada perangkat iOS yang belum di-*jailbreak*.

- Spionase Digital via *Audio Jack* Perangkat Seluler [1].

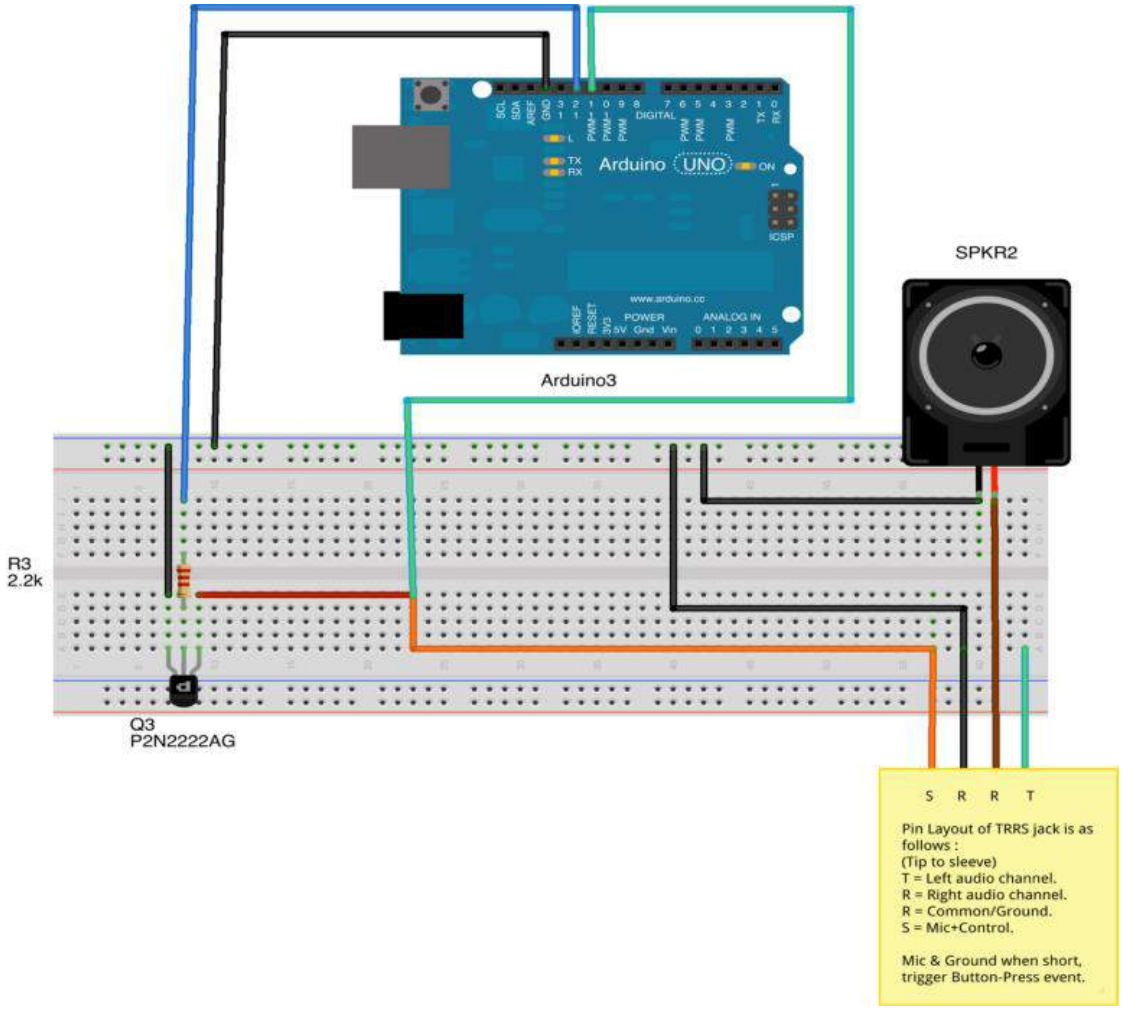
  Proses *compromise* melalui perangkat keras merupakan salah satu alternatif yang dapat digunakan untuk melakukan spionase digital. Berdasarkan tren saat ini, proses *compromise* melalui perangkat lunak semakin sulit karena perangkat seluler didukung oleh sistem keamanan berbasis perangkat lunak yang semakin canggih. Terdapat suatu cara untuk menyerang perangkat seluler (iPhone, Android, Windows Phone, dan BlackBerry) dengan mengombinasikan fitur *voice dialing* yang dimiliki oleh perangkat seluler dengan mikrokontroler, seperti Arduino. Serangan ini bertujuan untuk melakukan beberapa hal berikut :

  - menginisiasi panggilan keluar tanpa diketahui oleh pengguna perangkat seluler;
  - mencatat durasi panggilan keluar yang telah dilakukan; dan
  - mendeteksi adanya panggilan masuk/keluar dan SMS.

  Dengan memodifikasi serangan, beberapa hal di bawah ini juga dapat dilakukan oleh *attacker*, meskipun masih sulit untuk dilakukan :

  - merekam nomor telepon yang dimasukkan oleh pengguna perangkat seluler;
  - memperoleh seluruh kontak yang tersimpan di perangkat seluler;
  - merekam panggilan keluar/masuk yang dilakukan oleh pengguna perangkat seluler; dan
  - melakukan seluruh *compromise* di atas secara jarak jauh.

  Penyerangan dilakukan dengan meniru cara kerja perangkat lunak perangkat seluler dalam mengakuisisi suara manusia menjadi suatu perintah. Hal ini dilakukan dengan memanfaatkan mikrokontroler untuk mengendalikan *audio jack* perangkat seluler. Dengan mengendalikan *audio jack* perangkat seluler, pengguna perangkat seluler tidak akan menyadari bahwa perangkat selulernya sedang di-*hack* karena nada suara yang menjadi penanda utama adanya panggilan keluar/masuk atau SMS dinonaktifkan oleh mikrokontroler. Selain itu, *attacker* juga dapat melakukan panggilan keluar melalui mikrokontroler tanpa diketahui oleh pengguna perangkat seluler. Rangkaian mikrokontroler untuk mengendalikan *audio jack* perangkat seluler dapat dilihat pada Gambar 3.



Gambar 3. Rangkaian Mikrokontroler untuk Mengendalikan *Audio Jack* Perangkat Seluler [1].

- *Backdoor* pada Prosesor MediaTek MT6582 [26].

  Pada tanggal 13 Pebruari 2016, Justin Case, seorang peneliti di bidang keamanan, menemukan adanya *backdoor* berbahaya yang terdapat di prosesor MediaTek MT6582 (lihat *link* https://twitter.com/jcase/status/687151870255755264). Prosesor ini banyak ditemukan pada perangkat seluler berbasis *Operating System* (OS) Android 4.4 KitKat. *Backdoor* pada prosesor Mediatek MT6582 merupakan *debug tool* yang dibiarkan terbuka bagi publik. Seharusnya, *debug tool* ini hanya dibuka untuk *carrier* yang ingin menguji coba kualitas jaringannya pada perangkat seluler. Akibatnya, *attacker* dapat memperoleh informasi-informasi pengguna perangkat seluler, seperti kontak pribadi, pesan teks, foto, dan video, dengan memanfaatkan *debug tool* yang terbuka bagi publik ini.

  Walaupun kasus *backdoor* ini tidak dilakukan secara sengaja oleh MediaTek, kasus ini memperlihatkan adanya potensi dipasangnya *backdoor* secara sengaja pada perangkat keras dan/atau perangkat lunak perangkat seluler. Dugaan ini terbukti pada CoolReaper.

- CoolReaper [4].

  Coolpad merupakan salah satu manufaktur *smartphone* terbesar di dunia. Namun, Coolpad menciderai kepercayaan konsumennya dengan memasang *backdoor* perangkat lunak secara sengaja pada produk *smartphone* Android-nya. *Backdoor* ini dinamakan CoolReaper. Tujuan dari CoolReaper adalah melakukan beberapa hal-hal ilegal berikut :

  - mengunduh, memasang, atau mengaktivasi aplikasi Android tanpa diketahui oleh pengguna perangkat seluler;
  - menghapus data milik pengguna perangkat seluler, menghapus aplikasi Android yang telah terpasang, atau menghentikan proses aplikasi sistem;
  - menipu pengguna perangkat seluler agar memasang aplikasi jahat dengan memberikan notifikasi *update* perangkat palsu;
  - mengirim dan/atau menambah isi pesan teks/gambar tanpa seizin pengguna;
  - melakukan panggilan keluar; dan
  - mengunggah informasi-informasi sensitif, seperti lokasi perangkat lunak, *log* penggunaan aplikasi, *history* panggilan keluar/masuk, dan *history* pesan teks/gambar, ke *server* Coolpad.

  Backdoor CoolReaper diimplementasikan dengan memodifikasi OS Android pada seluruh ROM perangkat seluler, tepatnya memberikan tanda tangan digital resmi Coolpad pada *file-file backdoor*, sehingga komponen-komponen serta aktivitas-aktivitas CoolReaper tidak diketahui oleh pengguna perangkat seluler dan program *antivirus*. Tanda tangan digital resmi Coolpad mengeksploitasi kelemahan *whitelist* yang dimiliki oleh *antivirus* dan perangkat keamanan jaringan lainnya. Meskipun *antivirus* dapat mendeteksi CoolReaper, *file-file backdoor* tidak dapat dihapus karena *file-file backdoor* ini terdapat di sistem aplikasi yang membutuhkan akses *root* untuk menghapusnya.

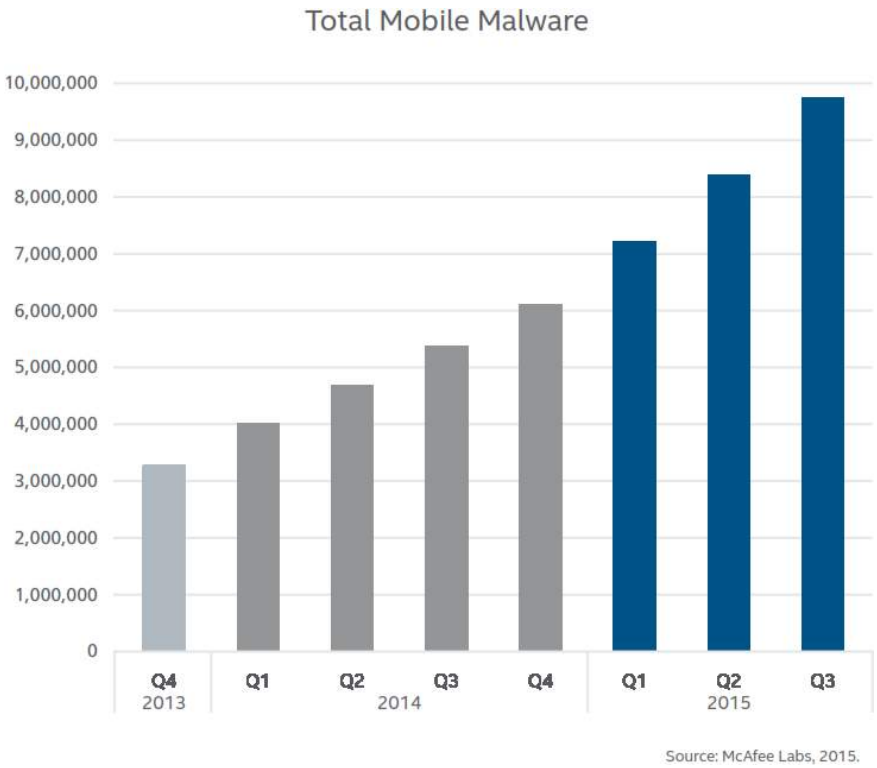
  Backdoor ini dilaporkan oleh beberapa pengguna perangkat seluler Coolpad setelah perangkat selulernya melakukan pemasangan aplikasi yang tidak diinginkan oleh pengguna secara otomatis dan menerima notifikasi palsu mengenai *update* perangkat. Tentu saja, laporan ini tidak ditanggapi dan dihapus oleh Coolpad. Coolpad baru menerima dan merespon laporan dari seorang peneliti di bidang keamanan mengenai adanya kerentanan pada sistem kendali *back-end*-nya, tepatnya peneliti tersebut mengetahui Coolpad mengendalikan *backdoor* CoolReaper.

- Spionase Digital via Media Sosial [5, 15].

  Media sosial merupakan cara bagi seseorang untuk berkomunikasi dan bertukar informasi dengan pihak lain secara *online* (saling terhubung satu sama lain melalui jaringan komputer). Saat ini, penggunaan media sosial sudah sangat masif karena manfaat yang dirasakan oleh banyak entitas atau personal. Salah satu perangkat yang digunakan untuk mengakses media sosial adalah perangkat seluler karena perangkat ini bersifat *portable* sehingga memudahkan pengguna untuk mengakses media sosial di berbagai waktu dan tempat.

  Banyaknya pengguna media sosial menyebabkan media sosial ini menjadi wadah baru bagi *attacker* untuk melakukan praktik spionase digital. Beberapa tindakan di bawah ini merupakan ancaman terhadap layanan media sosial.

  - *Spamming* : *Attacker* membuat dan menyebarkan *malware* ke banyak pihak dengan memanfaatkan rekan-rekan yang dimiliki oleh seseorang.
  - *Tools* : Dengan menggunakan *tools* tertentu, akun media sosial milik seseorang dapat di-*compromise* sehingga data personal, termasuk daftar kontak teman, dapat diketahui oleh *attacker*. Selanjutnya, *attacker* dapat menggunakan akun tersebut untuk melakukan *spamming malware* dan aksi-aksi ilegal lainnya.
  - *Spear phising* : *Attacker* dapat mengirim *e-mail* atau menulis komentar yang seakan-akan pengaturannya tersebut merupakan pihak yang dapat dipercaya. Pesan atau komentar tersebut dapat berupa URL atau permintaan untuk memberikan informasi personal. Apabila instruksi yang diberikan oleh *attacker* ini diikuti oleh pengguna sosial media, informasi-informasi sensitif milik pengguna sosial media dapat diketahui.
  - Pencurian Identitas : *Attacker* dapat mengumpulkan informasi-informasi tentang pengguna sosial media dan/atau rekannya yang dipublikasi di akun sosial medianya. Dengan menggunakan informasi-informasi ini, *attacker* berpotensi untuk mengetahui tantangan keamanan atau kata sandi *e-mail*, kartu kredit, dan akun bank milik pengguna sosial media dan/atau rekannya.
  - Aplikasi pihak ketiga : Mayoritas media sosial mengizinkan pengguna untuk menggunakan aplikasi pihak ketiga. Agar aplikasi pihak ketiga ini dapat digunakan, aplikasi pihak ketiga mengharuskan sosial media untuk menyediakan beberapa informasi personal milik pengguna. Tentu saja, hal ini berpotensi menimbulkan bahaya karena pengguna tidak mengetahui informasi-informasi personal apa saja yang diberikan ke aplikasi pihak ketiga.



Gambar 4. Tren Pertumbuhan *Malware* pada Perangkat Seluler [20].

Serangan-serangan yang telah dijelaskan sebelumnya memperlihatkan bahwa perangkat seluler bisnis saat ini telah memiliki ancaman spionase digital yang cukup banyak dan masih terus berkembang. Gambar 4 menunjukkan bahwa tren pertumbuhan ancaman spionase digital pada perangkat seluler, terutama melalui *malware*, terus meningkat. Dengan demikian, organisasi perlu melakukan suatu tindakan untuk mengatasi ancaman-ancaman keamanan yang dihadapi oleh perangkat seluler bisnis, terutama ancaman spionase digital.

NIST SP 800-124 *Revision* 1 : *Guidelines for Managing the Security of Mobile Devices in the Enterprise* merupakan pedoman yang dikembangkan oleh National Institute of Standards and Technology (NIST) mengenai tata kelola perangkat seluler bisnis yang dilakukan secara terpusat untuk mengatasi ancaman-ancaman keamanan, seperti spionase digital. Perangkat seluler bisnis yang dicakup oleh pedoman NIST adalah perangkat seluler milik organisasi dan perangkat seluler milik pribadi, atau biasa disebut dengan perangkat seluler *Bring Your Own Device* (BYOD). Dengan menjadikan NIST SP 800-124 *Revision* 1 sebagai acuan utama dan beberapa sumber lain sebagai referensi pendukung dan/atau pelengkap, makalah ini dibuat, terutama, untuk membahas operasi keamanan pada perangkat seluler bisnis; dimulai dari perangkat seluler bisnis digunakan pertama kali di organisasi hingga perangkat seluler bisnis tersebut dibuang atau dipindah tangankan; dengan melibatkan konsep-konsep tata kelola perangkat seluler bisnis secara terpusat.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dipaparkan maka dapat dirumuskan beberapa pokok masalah yang diangkat pada makalah kali ini, yaitu sebagai berikut :

1. Apa saja kerentanan-kerentanan dan variasi jenis serangan yang dialami oleh perangkat seluler sehingga praktik spionase digital dapat dilakukan pada perangkat seluler bisnis?
2. Apa itu tata kelola perangkat seluler bisnis secara terpusat? Apa saja komponen, bentuk arsitektur, dan kapabilitas dari tata kelola perangkat seluler bisnis secara terpusat?
3. Bagaimana bentuk struktur dari operasi keamanan pada perangkat seluler bisnis?

1.3 Tujuan Makalah

Adapun tujuan yang ingin dicapai pada penelitian ini adalah sebagai berikut ini.

1. Mendeskripsikan kerentanan-kerentanan dan variasi jenis serangan yang dialami oleh perangkat seluler bisnis.
2. Memberikan pandangan umum tentang tata kelola perangkat seluler bisnis secara terpusat serta mendeskripsikan komponen, arsitektur, dan kapabilitas dari tata kelola perangkat seluler bisnis secara terpusat.
3. Mendeskripsikan bentuk struktur dari operasi keamanan pada perangkat seluler bisnis.

1.4 Manfaat Makalah

Manfaat yang ingin diperoleh dari makalah ini adalah mengetahui kerentanan-kerentanan dan variasi jenis serangan yang dihadapi oleh perangkat seluler bisnis sehingga rentan terhadap praktik spionase digital. Selain itu, manfaat lain yang ingin diperoleh adalah memahami operasi keamanan pada perangkat seluler bisnis dengan melibatkan konsep-konsep tata kelola perangkat seluler bisnis secara terpusat. Oleh karena itu, makalah ini juga menjelaskan pandangan umum, komponen, arsitektur, dan kapabilitas dari tata kelola perangkat seluler bisnis secara terpusat.

1.5 Batasan Masalah

Berikut batasan-batasan masalah dari makalah ini :

1. Deskripsi tentang kerentanan-kerentanan dan variasi jenis serangan yang dihadapi oleh perangkat seluler bisnis sesuai dengan NIST SP 800-124 *Revision* 1 dan referensi [23, 24].

2. Definisi tata kelola perangkat seluler bisnis secara terpusat yang dibahas pada makalah ini mayoritas merujuk pada definisi tata kelola perangkat seluler bisnis secara terpusat sebagaimana dijelaskan pada NIST SP 800-124 *Revision* 1. Tata kelola perangkat seluler bisnis secara terpusat yang berasal dari sumber lain juga digunakan, tetapi tetap sejalan dengan definisi tata kelola perangkat seluler bisnis secara terpusat sebagaimana dijelaskan pada NIST SP 800-124 *Revision* 1. Sumber lain hanya digunakan sebagai pelengkap dan/atau pendukung.
3. Struktur dari operasi keamanan pada perangkat seluler bisnis yang akan dibahas pada makalah ini sesuai dengan fase-fase pada siklus hidup penggunaan perangkat seluler bisnis pada NIST 800-124 *Revision* 1.

1.6 Metodologi

Metodologi yang digunakan memiliki tahapan sebagai berikut.

1. Studi Literatur
   Studi literatur yang dilakukan adalah dengan mempelajari pedoman/standar milik badan yang diakui secara internasional maupun negara (misal NIST dan GAO), laporan dari entitas tertentu (misal Kaspersky dan McAfee), sumber-sumber internet, maupun segala tulisan yang berkaitan serta membantu dalam pengerjaan makalah ini.
2. Penulisan Dokumen
   Penulisan makalah dilakukan untuk mendokumentasikan hasil yang telah diperoleh dari studi literatur yang telah dilakukan.

1.7 Sistematika Penulisan

Penulisan laporan proposal penelitian ini terdiri dari tiga bagian yaitu pendahuluan, tinjauan pustaka, dan perancangan awal dari implementasi sistem.

BAB 1. PENDAHULUAN

Bab ini memuat latar belakang, perumusan masalah, tujuan dan manfaat makalah, ruang lingkup dan batasan masalah, metodologi, serta sistematika penulisan makalah.

BAB 2. ANCAMAN-ANCAMAN TERHADAP PERANGKAT SELULER BISNIS

Bab ini menjelaskan tentang kerentanan-kerentanan dan variasi jenis serangan yang dialami oleh perangkat seluler bisnis sehingga praktik spionase digital dapat dilakukan.

BAB 3. TATA KELOLA PERANGKAT SELULER BISNIS SECARA TERPUSAT

Bab ini memberikan pandangan umum mengenai tata kelola perangkat seluler bisnis secara terpusat sesuai definisi NIST SP 800-124 *Revision* 1 serta menjelaskan komponen, arsitektur, dan kapabilitas dari tata kelola perangkat seluler secara terpusat.

BAB 4. OPERASI KEAMANAN PADA PERANGKAT SELULER BISNIS

Bab ini menjelaskan tentang operasi keamanan pada perangkat seluler bisnis. Operasi keamanan dijelaskan dalam bentuk siklus atau tahapan-tahapan penggunaan perangkat seluler bisnis yang aman di organisasi. Materi-Materi yang telah dibahas 3 sangat digunakan di sini.

BAB 5. KESIMPULAN DAN BAHAN PEMBAHASAN LEBIH LANJUT

Bab ini menjawab pertanyaan-pertanyaan yang ada pada rumusan masalah sesuai penjelasan yang terdapat di BAB 2, 3, dan 4. Selain itu, saran mengenai pengembangan selanjutnya dari makalah ini diberikan.

BAB 2

ANCAMAN-ANCAMAN TERHADAP PERANGKAT SELULER BISNIS

2.1 Tujuan Keamanan pada Perangkat Seluler Bisnis

NIST SP 800-124 *Revision* 1 menyatakan perangkat seluler memiliki tiga tujuan yang sama dengan sistem kriptografi pada umumnya, yaitu CIA *Triad*.

- Kerahasiaan. Menjamin bahwa data yang ditransmisikan dan disimpan tidak dapat diakses atau dibaca oleh pihak yang tidak berwenang, termasuk *attacker*.
- Integritas. Mendeteksi adanya perubahan-perubahan yang terjadi pada data yang ditransmisikan dan disimpan, baik itu perubahan data yang dilakukan secara sengaja maupun tidak sengaja,
- Keteradaan. Menjamin bahwa pengguna perangkat seluler dapat mengakses *resource* melalui perangkat selulernya kapanpun pengguna tersebut ingin lakukan.

Untuk mencapai tiga tujuan keamanan perangkat seluler di atas, ancaman-ancaman yang dialami oleh perangkat seluler bisnis wajib ditangani. Ancaman-Ancaman ini muncul akibat dari semakin canggihnya fitur-fitur yang dimiliki oleh perangkat seluler. Fitur-Fitur perangkat seluler yang semakin canggih menyebabkan perangkat seluler memiliki banyak kerentanan. Tentunya, banyaknya kerentanan yang dimiliki oleh perangkat seluler ini diiringi dengan semakin banyaknya jenis serangan yang dapat dilakukan terhadap perangkat seluler. Oleh karena itu, sisa pembahasan pada bab ini akan menjelaskan tentang fitur-fitur perangkat seluler, kerentanan yang dimiliki oleh perangkat seluler, dan jenis serangan yang dapat dilancarkan oleh *attacker* terhadap perangkat seluler. Bab ini juga menjelaskan tentang *attacker* yang merupakan sumber utama terjadinya ancaman-ancaman yang dialami oleh perangkat seluler.

2.2 Fitur-Fitur Perangkat Seluler

Seperti yang telah diketahui, fitur perangkat seluler yang semakin banyak membuat ancaman-ancaman yang dihadapi oleh perangkat seluler semakin banyak pula. Menurut [18], fitur perangkat seluler selalu berubah sehingga ancaman terhadap perangkat seluler dan kendali kea-

manan untuk mengatasi ancaman tersebut juga selalu berubah. Oleh karena itu, perlu didefinisikan suatu fitur dasar perangkat seluler, yaitu fitur yang dimiliki oleh setiap perangkat seluler. Berikut fitur dasar perangkat seluler yang digunakan [18] :

- perangkat keras yang terdapat pada perangkat seluler, terutama *motherboard*, termasuk ke dalam kategori *Small Form Factor* (SFF);
- memiliki sedikitnya satu antarmuka jaringan nirkabel yang berfungsi untuk menghubungkan perangkat seluler ke jaringan komputer (misal Wi-Fi atau jaringan *provider* lokal);
- memiliki tempat penyimpanan data yang *non-removable*;
- memiliki OS, tetapi tidak sekompleks OS *desktop* atau laptop; dan
- perangkat seluler dapat memasang aplikasi melalui beberapa metoda, salah satunya *server* pihak ketiga (misal Google Play Store, Apple App Store, Amazon, dan Humble Bundle).

Terdapat fitur lain yang dimiliki oleh perangkat seluler yang terkait dengan keamanan, tetapi fitur ini tidak termasuk ke dalam fitur dasar perangkat seluler di atas. Fitur ini dapat disebut juga sebagai fitur opsional. Fitur opsional perlu diperhatikan apabila perangkat seluler memiliki fitur opsional ini. Berikut beberapa contoh fitur opsional perangkat seluler [18] :

- memiliki sedikitnya satu antarmuka jaringan lokal (misal *Bluetooth* atau *Near-field Communications* (NFC));
- memiliki sedikitnya satu antarmuka jaringan yang berfungsi untuk melakukan panggilan keluar/masuk (misal jaringan *provider* lokal);
- memiliki modul Global Positioning System (GPS);
- memiliki sedikitnya satu perangkat kamera untuk mengambil foto atau merekam video;
- *microphone*;
- mendukung *removable* media;
- mendukung penggunaan sebagian memori *built-in* sebagai *removable storage* untuk keperluan proses komputasi yang lain;
- memiliki fitur *built-in* yang berfungsi untuk melakukan sinkronisasi data dengan perangkat lain, seperti *desktop*, laptop, *server* organisasi, *server* pihak ketiga, dan *server provider* telekomunikasi.

2.3 *Attacker* sebagai Inisiator Ancaman

Menurut [24], sumber ancaman perangkat seluler berasal dari grup atau individu berikut :

- Operator *Botnet*. Operator *botnet* mendistribusikan *malware* ke banyak perangkat seluler dan sistem elektronik lainnya sehingga *attacker* dapat melakukan serangan terhadap perangkat-perangkat ini secara jarak jauh. Pendistribusian *malware* dapat dilakukan ke *website-website* atau melalui skema-skema tertentu, seperti *phishing*, *spamming*, dan lain-lain.
- Sindikat Kriminal *Cyber*. Sindikat criminal *cyber* biasanya menyerang perangkat seluler untuk kepentingan finansial. Sindikat tersebut dapat menggunakan *phising*, *spamming*, *spyware*, atau *malware* untuk memperoleh akses ke informasi yang tersimpan di dalam perangkat seluler. Informasi yang diperoleh ini dapat digunakan oleh sindikat kriminal *cyber* untuk mencuri identitas, penipuan, dan pemerasan. Serangan yang dilakukan oleh sindikat kriminal *cyber* dapat dilakukan di tingkat korporasi, badan pemerintahan, dan institusi-institusi besar lainnya. Selain faktor finansial, serangan yang dilakukan di level yang tinggi ini dilakukan untuk melakukan spionase digital dan pencurian kekayaan intelektual.
- Pemerintah Negara Lain. Badan intelijen negara lain menyerang perangkat seluler sebagai bagian dari operasi mereka dalam mengumpulkan informasi sensitif dan aksi spionase digital. Dengan demikian, negara lain dapat mengembangkan kemampuannya dalam berbagai hal, salah satunya teknologi di bidang pertahanan.
- *Hacker*. *Hacker* menyerang perangkat seluler untuk memperlihatkan kemampuannya dan memperoleh gengsi tersendiri di komunitas *hacker*. Meskipun praktik *hacking* memerlukan kemampuan khusus di bidang komputer, praktik *hacking* ini marak terjadi karena *hacker* dapat mengunduh skrip jahat dari internet untuk menyerang perangkat seluler.
- Teroris. Teroris menyerang perangkat seluler untuk menghancurkan, mengekploitasi, atau melemahkan infrastruktur milik suatu industri atau negara tertentu. Serangan yang dilakukan oleh teroris dapat berupa skema *phising* atau *spyware*/*malware* untuk mengumpulkan informasi sensitif atau mengumpulkan uang.

Sumber ancaman perangkat seluler ini menunjukkan bahwa ancaman-ancaman terbesar dialami oleh perangkat seluler bisnis, bukan personal, akibat dari pentingnya dan banyaknya data sensitif yang dimiliki oleh perangkat seluler bisnis tersebut.

2.4 Kerentanan dan Jenis Serangan terhadap Perangkat Seluler

Seperti yang telah dijelaskan di bagian 1.1, *attacker* dapat mengakuisisi informasi-informasi rahasia yang tersimpan di perangkat seluler setelah *attacker* mengendalikan perangkat seluler terlebih dahulu dengan meng-*compromise* perangkat seluler tersebut. Dua faktor yang menyebabkan perangkat seluler dapat di-*compromise*, yaitu kerentanan yang dimiliki oleh perangkat seluler dan jenis serangan yang dilancarkan oleh *attacker* terhadap perangkat seluler.

Kerentanan yang Dimiliki oleh Perangkat Seluler :

Menurut [23], terdapat banyak sekali kerentanan yang dmiliki oleh perangkat seluler. Namun, NIST SP 800-124 *Revision* 1 merangkum kerentanan-kerentanan tersebut menjadi lima jenis kerentanan. Berikut lima jenis kerentanan yang mayoritas dimiliki oleh perangkat seluler menurut NIST SP 800-124 *Revision* 1 :

- Serangan secara Fisik. Perangkat seluler biasanya digunakan di banyak tempat yang lokasinya di luar kendali organisasi, seperti rumah karyawan, kafe, hotel, dan konferensi. Meskipun perangkat seluler digunakan di lingkungan organisasi sekalipun, perangkat seluler sering berpindah dari satu fasilitas ke fasilitas lainnya. Perpindahan perangkat seluler seperti ini menyebabkan informasi-informasi sensitif yang diakses melalui perangkat seluler berada dalam risiko ter-*compromise*. Dengan demikian, ketika mendesain kebijakan dan kendali keamanan perangkat seluler, organisasi wajib mengasumsikan bahwa perangkat seluler sewaktu-waktu dapat dicuri oleh *attacker*. Jika perangkat seluler jatuh ke tangan *attacker*, informasi-informasi sensitif milik pribadi dan/atau organisasi dapat dicuri, baik secara langsung (mengambil informasi-informasi sensitif yang tersimpan di dalam perangkat seluler) maupun tidak langsung (mengakses informasi-informasi sensitif yang terdapat di *server* organisasi secara jarak jauh menggunakan perangkat seluler yang dicuri).
- Perangkat Seluler yang Digunakan Tidak Dapat Dipercaya. Mayoritas perangkat seluler saat ini, terutama perangkat seluler BYOD, tidak memiliki *trust feature*, seperti *Trusted Platform Modules* (TPMs), yang saat ini banyak di-*built-in* ke laptop dan perangkat lainnya. Selain itu, praktik *jailbreak* dan *rooting* terhadap perangkat seluler kerap terjadi sehingga batasan-batasan keamanan, penggunaan OS, dan lain-lain di-*bypass*. Dengan demikian, organisasi wajib mengasumsikan bahwa seluruh perangkat seluler sebagai perangkat yang tidak dapat dipercaya, kecuali organisasi tersebut telah memasang sistem keamanan pada perangkat seluler serta memonitor sistem keamanan ini secara berkelanjutan, terutama saat aplikasi atau *resource* milik organisasi sedang diakses.

- Jaringan Komputer yang Digunakan Tidak Dapat Dipercaya. Perangkat seluler hampir selalu menggunakan jaringan non-organisasi untuk mengakses internet, sedangkan organisasi tidak memiliki kendali keamanan pada jaringan non-organisasi ini. Karena akses internet pada perangkat seluler menggunakan mekanisme nirkabel, seperti Wi-Fi dan jaringan *provider* lokal, informasi-informasi sensitif yang ditransmisikan selama proses komunikasi berlangsung berada dalam risiko ter-*compromise* akibat serangan, seperti *eavesdropping* atau *Man-In-The-Middle* (MITM) *attack*. Dengan demikian, organisasi wajib mengasumsikan bahwa jaringan komputer yang digunakan oleh perangkat seluler dan organisasi untuk saling berhubungan satu sama lain tidak dapat dipercaya, kecuali organisasi tersebut telah yakin perangkat seluler menggunakan jaringan komputer yang dapat dikendalikan keamanannya oleh organisasi (dapat dipercaya).
- Aplikasi yang Digunakan Tidak Dapat Dipercaya. Perangkat seluler didesain sedemikian rupa agar mudah dalam mencari, mengunduh, memasang, dan/atau menggunakan aplikasi pihak ketiga yang berasal dari *application store*. Hal ini menimbulkan risiko keamanan, terutama untuk *platform* perangkat seluler dan *application store* yang tidak memiliki ketentuan-ketentuan atau batasan-batasan keamanan pada aplikasi pihak ketiga yang dipublikasi. Dengan demikian, organisasi wajib mengasumsikan bahwa aplikasi pihak ketiga yang dicari, diunduh, dipasang, dan/atau digunakan pada perangkat seluler tidak dapat dipercaya.
- Interaksi Perangkat Seluler dengan Sistem Ter-*compromise*. Perangkat seluler dapat berinteraksi dengan sistem lain dalam rangka pertukaran dan penyimpanan data. Terdapat dua jenis interaksi antara perangkat seluler dengan sistem lain, yaitu interaksi sistem secara lokal dan interaksi sistem secara jarak jauh. Interaksi sistem secara lokal, antara lain menghubungkan perangkat seluler dengan *desktop* atau laptop via kabel atau jaringan nirkabel, dan internet *tethering*. Interaksi sistem secara jarak jauh seringnya berbentuk aktivitas *backup* data secara otomatis ke tempat penyimpanan data berbasis *cloud*. Apabila seluruh jenis interaksi sistem ini dapat dikendalikan oleh organisasi, risiko yang dihadapi organisasi terkait interaksi perangkat seluler dengan sistem yang lain dapat diterima. Namun, seringnya, beberapa jenis interaksi sistem tidak berada di bawah kendali organisasi. Berikut beberapa contoh skenario interaksi sistem yang berada di luar kendali organisasi :
  - menghubungkan perangkat seluler BYOD ke laptop milik organisasi;
  - menghubungkan perangkat seluler milik organisasi ke laptop BYOD;
  - mengakses layanan *backup* secara *remote* dari perangkat seluler atau laptop organisasi;

- mengisi daya baterai menggunakan alat pengisi yang tidak dapat dipercaya; dan
- pertukaran data antar-perangkat seluler.

Skenario-skenario di atas memperlihatkan *resource* milik organisasi berada dalam risiko karena interaksi sistem tidak berada di dalam kendali organisasi. Selain itu, skenario-skenario di atas juga memperlihatkan potensi tersebarnya *malware*.

Jenis Serangan yang Dilancarkan oleh Attacker terhadap Perangkat Seluler :

Seperti yang telah diketahui, banyaknya kerentanan yang dimiliki oleh perangkat seluler diiringi dengan semakin banyaknya jenis serangan terhadap perangkat seluler. Beberapa jenis serangan telah diberikan di Bagian 1.1. Berikut daftar jenis serangan yang umumnya digunakan untuk menyerang perangkat seluler [24] :

- Eksploitasi *Browser*. Eksploitasi jenis ini memanfaatkan kerentanan fitur yang terdapat pada perangkat lunak, yaitu fitur untuk mengakses *website*. Fitur ini disiipi oleh suatu skrip yang nantinya akan dijalankan untuk mengakses *website* atau membuka tautan tertentu. Dengan mengunjungi *website* dan/atau membuka tautan ini, eksploitasi *browser* dapat beroperasi sehingga *malware* atau hal merugikan lainnya masuk ke perangkat seluler.
- Pencegatan Data. Pencegatan data dapat terjadi ketika melakukan *eavesdropping* saat komunikasi data sedang berlangsung dari atau ke perangkat seluler. *Eavesdropping* dapat dilakukan melalui beberapa teknik, sebagai berikut :
  - MITM *Attack*. Serangan ini dapat dilakukan ketika perangkat seluler terhubung ke jaringan Wi-Fi yang tidak aman lalu *attacker* mencegat dan mengubah komunikasi data.
  - Wi-Fi *Sniffing*. Serangan ini dapat dilakukan ketika data dikirim dari atau ke perangkat seluler melalui jaringan yang tidak aman (misal jaringan yang tidak menggunakan teknologi enkripsi) sehingga *eavesdropper* dapat memonitor dan merekam informasi-informasi yang dipertukarkan.
- Pencatatan Penekanan Tombol. *Malware* jenis ini merekam tombol-tombol perangkat seluler yang ditekan untuk memperoleh informasi-informasi sensitif, seperti nomor kartu kredit. Biasanya, catatan penekanan tombol dikirim ke *website* atau *e-mail attacker*.
- *Malware*. Malware sering dipalsukan sebagai aplikasi permainan, *patch*, *utility*, atau aplikasi perangkat lunak yang penting. Jenis-jenis *malware*, termasuk *spyware* (perangkat lunak yang dipasang secara diam-diam di perangkat komputer yang berguna untuk mengumpulkan informasi-informasi milik personal atau organisasi tanpa sepengetahuan pengguna

perangkat seluler), virus (program yang dapat mereplikasi diri dan menginfeksi sistem perangkat seluler tanpa seizin atau sepengetahuan pengguna perangkat seluler), dan Trojan (*file* yang meniru sebagai *file* yang legal atau *file* yang disisipkan di dalam *file* yang legal). Setelah *malware* dipasang, *malware* dapat menyebarkan diri ke perangkat komputer yang lain (misal *repackaging*) dan melakukan berbagai jenis serangan, seperti mengetahui lokasi pengguna, mengetahui informasi-informasi sensitif, memperoleh akses untuk membaca atau menulis ke *history browsing* pengguna, melakukan panggilan keluar, mengaktifkan *microphone* dan kamera tanpa sepengetahuan pengguna, dan mengunduh aplikasi-aplikasi jahat lainnya.

- Pelacakan Lokasi secara Ilegal. Pelacakan lokasi berfungsi untuk mengetahui dan memonitor keberadaan perangkat seluler. Pelacakan lokasi dapat dilakukan secara terbuka maupun secara diam-diam. Informasi tentang lokasi perangkat seluler dapat diketahui melalui aplikasi tertentu atau dengan memasukkan *malware* ke perangkat seluler.
- Eksploitasi Jaringan. Ekploitasi jenis ini memanfaatkan kelemahan perangkat lunak tertentu yang dilakukan ketika perangkat seluler terhubung dengan jaringan lokal, seperti *Bluetooth* atau Wi-Fi, atau jaringan *provider* lokal. Eksploitasi jaringan dapat dilakukan tanpa perlu adanya interaksi dengan pengguna sehingga eksploitasi jaringan ini berbahaya karena dapat menyebar *malware* secara otomatis. Dengan *tools* tertentu, *attacker* dapat memperoleh informasi kredensial milik pengguna melalui jaringan Wi-Fi kemudian menyalahgunakan informasi kredensial ini. Serangan lain yang dapat dilakukan oleh *attacker*, yaitu bluesnarfing. Bluesnarfing adalah serangan yang memanfaatkan kelemahan perangkat seluler yang memiliki fitur *Bluetooth*.
- *Phising*. Tindakan yang biasa dilakukan oleh *attacker* melalui *e-mail* atau pesan *pop-up* dengan tujuan untuk menipu seseorang sehingga orang tersebut memberikan informasi-informasi sensitif miliknya. *E-mail* atau pesan *pop-up* berfungsi sebagai umpan untuk pengguna perangkat seluler agar informasi sensitif milik pengguna perangkat seluler, seperti kata sandi dan data finansial, dapat diperoleh oleh *attacker*.
- *Spamming*. *Spam* merupakan iklan komersial mengenai suatu produk, layanan, dan *website* yang biasanya dikirim via *e-mail*. Spam dapat digunakan sebagai media untuk menyebarkan perangkat lunak jahat. *Spam* dapat berupa pesan teks, selain berupa *e-mail*. *Spam* dapat dimanfaatkan untuk menambah efektivitas dan efisiensi dari *phising*.

- *Spoofing*. *Attacker* membuat *website* palsu yang menirukan atau "*spoof*" *website* yang asli kemudian menggunakan *website* palsu tersebut untuk menyebarkan *malware* ke perangkat seluler. *Spoofing* via *e-mail* dilakukan dengan mengganti alamat *e-mail* pengirim dan bagian-bagian tertentu dari *header e-mail* sehingga *e-mail* yang dikirim oleh *attacker* seakan-akan dari orang yang terpercaya. *Spoofing* menyembunyikan sumber pengiriman *e-mail* dan menyisipkan *malware* pada *e-mail*.
- Pencurian/hilang. Karena perangkat seluler memiliki ukuran yang kecil dan sering digunakan di luar organisasi, perangkat seluler lebih rentan untuk dicuri atau hilang dibandingkan dengan laptop atau sejenisnya. Apabila perangkat seluler dicuri atau hilang, akses informasi yang tersimpan di dalam perangkat seluler relatif mudah untuk dilakukan.
- *Zero-day Exploit*. Eksploitasi jenis ini menyerang kerentanan yang dimiliki oleh perangkat lunak sebelum *update* atau *patch* untuk memperbaiki kerentanan tersebut dibuat dan diimplementasikan. Tindakan *attacker* dalam percobaannya menulis skrip untuk mengeksploitasi kerentanan perangkat lunak merupakan ancaman bagi perangkat seluler karena perangkat lunak tersebut belum dilakukan *update* atau *patch* untuk mencegah percobaan eksploitasi yang dilakukan oleh *attacker*.

Dengan menggabungkan kerentanan-kerentanan yang dimiliki oleh perangkat seluler dengan berbagai jenis serangan yang dapat dilakukan terhadap perangkat seluler, risiko ter-*compromise*-nya perangkat seluler bisnis menjadi semakin tinggi. Dengan demikian, organisasi memerlukan suatu cara untuk mengendalikan perangkat seluler bisnis supaya risiko ter-*compromise*-nya perangkat seluler dapat ditekan. Seperti yang akan dijelaskan pada bab selanjutnya, NIST SP 800-124 *Revision* 1 merekomendasikan penggunaan tata kelola perangkat seluler bisnis secara terpusat sebagai solusi keamanan perangkat seluler yang tepat.

BAB 3

TATA KELOLA PERANGKAT SELULER BISNIS SECARA TERPUSAT

Tata kelola perangkat seluler secara terpusat, atau biasa disebut dengan *Mobile Device Management* (MDM), merupakan solusi untuk mengendalikan perangkat seluler milik organisasi dan BYOD. Selain mengelola konfigurasi dan keamanan dari perangkat seluler bisnis, MDM juga menyediakan akses yang aman ke *resource* organisasi.

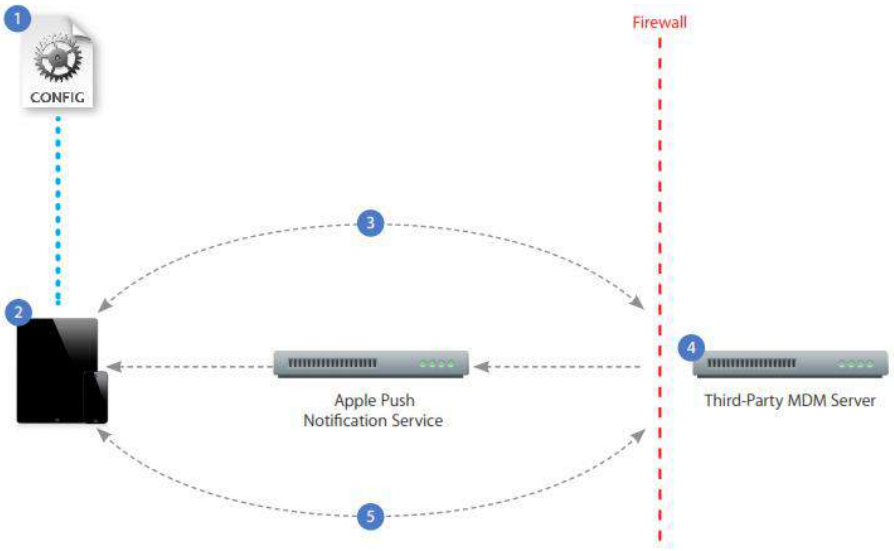
3.1 Komponen, Arsitektur, dan Kapabilitas MDM

Komponen dan Arsitektur [17] :

Terdapat dua jenis MDM yang dapat digunakan, yaitu menggunakan MDM buatan pihak manufaktur dari perangkat seluler yang digunakan oleh organisasi (misal BlackBerry Enterprise Server), atau menggunakan MDM buatan pihak ketiga (misal VMware AirWatch MDM). Dukungan terhadap perangkat seluler yang dibuat oleh pihak manufaktur lebih *robust* apabila dibandingkan dengan dukungan yang dibuat oleh pihak ketiga karena fokus MDM buatan pihak manufaktur hanya pada OS perangkat seluler buatannya, sedangkan MDM buatan pihak ketiga memiliki cakupan OS perangkat seluler yang lebih luas. Namun, NIST SP 800-124 *Revision* 1 tidak mengharuskan organisasi untuk menggunakan MDM buatan pihak manufaktur karena MDM buatan pihak ketiga juga dapat menyediakan dukungan yang *robust* terhadap perangkat seluler.

Secara arsitektur, kedua jenis MDM memiliki kemiripan pada arsitektur *server-client*-nya. Organisasi memiliki satu atau lebih *server* yang berfungsi untuk mengelola perangkat seluler secara terpusat, dan memiliki satu atau lebih aplikasi *client* yang dipasang pada setiap perangkat seluler yang dikonfigurasi sedemikian rupa sehingga aplikasi tersebut dapat beroperasi secara *background*. Gambar 5 memperlihatkan contoh arsitektur *server-client* untuk perangkat seluler berbasis iOS. Apabila perangkat seluler milik organisasi yang digunakan, aplikasi *client* didesain agar dapat mengelola konfigurasi dan keamanan untuk seluruh bagian perangkat seluler. Apabila perangkat seluler BYOD yang digunakan, aplikasi *client* didesain agar hanya mengelola konfigurasi dan keamanan dari aplikasi itu sendiri beserta *resource*-nya. Aplikasi *client* beserta *resource*-nya ini harus di-*sandboxed* supaya keduanya berada di tempat yang

aman dari pengaruh aplikasi dan *resource* perangkat seluler yang lain. Apabila *sandboxed* ini tidak dilakukan, *attacker* dapat meng-*compromise resource* milik organisasi yang terdapat di perangkat seluler, dan mengeksploitasi aktivitas atau data milik pengguna perangkat seluler (merusak privasi pengguna).



1. A Configuration Profile containing Mobile Device Management server information is sent to the device. The user is presented with information about what will be managed and/or queried by the server.
2. The user installs the profile to opt in to the device being managed.
3. Device enrollment takes place as the profile is installed. The server validates the device and allows access.
4. The server sends a push notification prompting the device to check in for tasks or queries.
5. The device connects directly to the server over HTTPS. The server sends commands or requests information.

Gambar 5. Arsitektur MDM pada Perangkat Seluler Berbasis iOS [3].

Kapabilitas [16] :

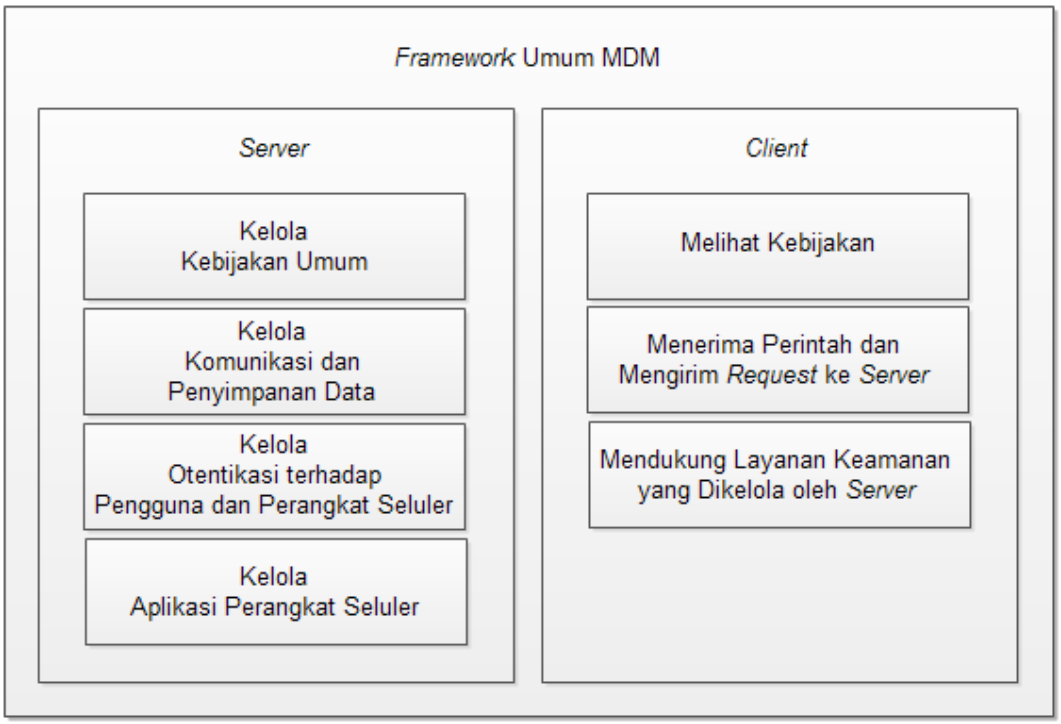
Bagian ini menjelaskan mengenai kapabilitas, atau lebih tepatnya layanan keamanan, yang ditawarkan oleh MDM. Layanan keamanan ini dapat disediakan oleh OS perangkat seluler, perangkat lunak MDM, atau kendali keamanan lainnya. Layanan keamanan ini dapat diimplementasikan di seluruh bagian perangkat seluler atau hanya pada *sandbox*. Layanan keamanan ini dapat digunakan juga untuk tata kelola perangkat seluler yang dilakukan secara individual (bukan secara terpusat). Berikut empat jenis layanan keamanan yang ditawarkan oleh MDM :

- Kebijakan Umum. MDM dapat memaksa organisasi untuk membuat dan mengimplementasikan kebijakan keamanan perangkat seluler. Berikut ketentuan-ketentuan atau batasan-batasan yang wajib ada pada kebijakan keamanan perangkat seluler :
  - mengelola antarmuka jaringan nirkabel (misal Wi-Fi dan *Bluetooth*);

- membatasi akses pengguna dan aplikasi ke perangkat keras perangkat seluler (misal kamera digital, modul GPS, antarmuka *Bluetooth*, antarmuka USB, dan *removable storage*;
- membatasi akses pengguna dan aplikasi ke layanan *native* OS (misal kalender, *built-in web browser*, *e-mail client*, kontak, dan layanan untuk instalasi aplikasi);
- secara otomatis memonitor, mendeteksi, melaporkan, dan menindaklanjuti pelanggaran kebijakan yang terjadi (misal mengubah konfigurasi keamanan tanpa izin); dan
- membatasi atau mencegah akses ke layanan organisasi berdasarkan versi OS perangkat seluler (termasuk juga perangkat seluler yang telah di-*rooting* atau di-*jailbreak*), *vendor* perangkat seluler, model perangkat seluler, atau versi perangkat lunak *client* MDM (apabila pembatasan atau pencegahan ke layanan organisasi berdasarkan versi perangkat lunak *client* dapat dilakukan);

- Komunikasi dan Penyimpanan Data. MDM wajib memiliki beberapa kapabilitas terhadap komunikasi dan penyimpanan data sebagai berikut :
  - Menggunakan teknologi enkripsi yang kuat pada komunikasi data antara perangkat seluler dengan organisasi. Biasanya, hal ini diimplementasi dalam bentuk *Virtual Private Network* (VPN) walaupun sebenarnya dapat menggunakan protokol dan teknologi enkripsi yang lain.
  - Menggunakan teknologi enkripsi yang kuat pada media penyimpanan data, baik itu media penyimpanan *built-in* maupun *removable storage*. Khusus untuk *removable storage*, penggunaan *removable storage* dapat dikombinasikan dengan suatu perangkat dekripsi sehingga informasi terenkripsi yang tersimpan di dalam *removable storage* hanya dapat dibaca ketika *removable storage* ini dihubungkan ke perangkat dekripsi; dengan demikian, risiko terjadinya penyerangan secara *offline* dapat dimitigasi.
  - Hapus seluruh data yang tersimpan di dalam perangkat seluler sebelum perangkat seluler dipindah tangakan, dibuang, atau dilakukan tindakan-tindakan lainnya.
  - Hapus seluruh data yang tersimpan di dalam perangkat seluler secara jarak jauh apabila terdapat dugaan bahwa perangkat seluler telah hilang, dicuri, atau jatuh ke pihak yang tidak berwenang sehingga terdapat risiko ter-*recovery*-nya data oleh pihak yang tidak dapat dipercaya.
  - Perangkat seluler dikonfigurasi sedemikian rupa sehingga data yang tersimpan di dalamnya dihapus secara otomatis apabila proses otentikasi gagal sebanyak jumlah percobaan tertentu.

- Otentikasi terhadap Pengguna dan Perangkat Seluler. MDM wajib memiliki beberapa kapabilitas otentikasi terhadap pengguna dan perangkat seluler berikut ini :
  - Menggunakan kata sandi dan/atau proses otentikasi yang lain, seperti *token-based authentication*, *network-based device authentication*, dan *domain authentication*, sebelum mengakses *resource* organisasi. Hal ini termasuk menentukan parameter, seperti kekuatan kata sandi dan batasan jumlah percobaan otentikasi tanpa adanya konsekuensi negatif (misal mengunci akun pengguna atau menghapus data perangkat seluler).
  - Apabila akun pengguna telah terkunci atau lupa kata sandi, administrator dapat melakukan *reset* secara *remote* sehingga pengguna dapat kembali mengakses perangkat seluler.
  - Mengunci perangkat seluler secara otomatis apabila perangkat seluler dalam kondisi diam selama waktu tertentu, misal lima menit.
  - Di bawah arahan administrator, perangkat seluler dikunci secara jarak jauh apabila terdapat dugaan bahwa perangkat seluler berada di lokasi yang tidak aman dan berada dalam keadaan tidak terkunci.
- Aplikasi Perangkat Seluler. MDM wajib memiliki beberapa kapabilitas terhadap aplikasi perangkat seluler sebagai berikut :
  - membatasi *application store* mana saja yang boleh digunakan;
  - membatasi pemasangan aplikasi perangkat seluler melalui *blacklisting* atau *whitelisting* (*whitelisting* lebih banyak digunakan);
  - membatasi izin, seperti akses kamera dan akses lokasi, untuk seluruh aplikasi perangkat seluler;
  - menggunakan mekanisme *safeguard* ketika memasang, meng-*update*, dan/atau menghapus aplikasi perangkat seluler serta selalu menyimpan inventaris saat ini yang dimiliki oleh seluruh aplikasi yang terpasang pada perangkat seluler;
  - membatasi penggunaan OS dan layanan sinkronisasi aplikasi (misal sikronisasi layanan secara jarak jauh dan sinkronisasi antar-perangkat lokal);
  - melakukan verifikasi tanda tangan digital pada aplikasi perangkat seluler untuk memeriksa integritas dari *source code* aplikasi menjamin bahwa hanya aplikasi yang berasal dari entitas yang telah dipercaya saja yang terpasang pada perangkat seluler; dan
  - Mendistribusikan aplikasi-aplikasi organisasi via *application store* yang telah ditentukan oleh organisasi.



Gambar 6. *Framework* Umum MDM.

3.2 *Framework* Umum MDM dan Kapabilitas *Server-Client* MDM

Berdasarkan penjelasan mengenai komponen, arsitektur, dan kapabilitas MDM sebelumnya, *framework* umum MDM dapat diperoleh (lihat Gambar 6). Sebelum menjelaskan pengertian dari *framework* umum MDM, alangkah baiknya untuk mengetahui terlebih dahulu pengertian dari *framework*. Berikut beberapa pengertian *framework* yang diperoleh dari [13] :

- Pengertian ke-1 : *Framework* adalah suatu aplikasi *semi complete* yang digunakan kembali dan dapat dimodifikasi untuk menghasilkan aplikasi tertentu.
- Pengertian ke-2 : *Framework* adalah kerangka dari suatu aplikasi yang dapat dimodifikasi dan disesuaikan oleh pengembang aplikasi.
- Pengertian ke-3 : *Framework* adalah sekumpulan kelas yang saling bekerja sama membentuk suatu desain yang mana desain ini dapat digunakan kembali untuk menghasilkan perangkat lunak tertentu.

Dengan demikian, pengertian *framework* umum MDM adalah kerangka yang dapat diimplementasikan di berbagai sistem (atau arsitektur) MDM dan dapat dimodifikasi sesuai keinginan pihak tertentu, seperti organisasi atau penyedia produk MDM. *Framework* umum MDM terdiri dari *server* dan *client* beserta masing-masing kapabilitasnya. Kapabilitas *server* dan

client yang akan diperlihatkan di bagian ini tidak hanya meliputi empat layanan keamanan MDM yang telah dijelaskan sebelumnya, tetapi juga meliputi persyaratan-persyaratan keamanan *server* yang ditentukan oleh Defense Information Systems Agency (DISA) dan persyaratan-persyaratan keamanan hasil penelitian [12]. Tabel 2 memperlihatkan daftar kapabilitas dari *server* dan *client*.

Tabel 2. Kapabilitas *Server* dan *Client*.

Keterangan : *Server* di sini dapat berupa *server* yang dipasang secara fisik di *data center* dan *server* yang dipasang secara *virtual* (misal *server cloud*).

Nomor	Kapabilitas
1	Kapabilitas *server* dalam mendukung tata kelola kebijakan umum : • *Server* wajib mendaftarkan perangkat seluler ke sistem MDM. • *Server* wajib mengelola kebijakan organisasi, terutama kebijakan keamanan perangkat seluler. Contoh pengelolaan kebijakan, yaitu membuat kebijakan baru, memodifikasi kebijakan, dan/atau menghapus kebijakan yang tidak sesuai. • *Server* wajib mendeteksi adanya pelanggaran terhadap kebijakan, terutama kebijakan keamanan perangkat seluler, seperti memodifikasi, menonaktifkan, dan/atau mem-*bypass* kebijakan. • Server wajib mengirimkan notifikasi ke perangkat seluler apabila terdeteksi adanya modifikasi ilegal terhadap konfigurasi keamanan yang dipasang di perangkat seluler tersebut. • *Server* wajib memiliki kapabilitas untuk melakukan *update* versi OS dan aplikasi perangkat seluler menggunakan mekanisme *over-the-air* (OTA). • *Server* wajib mengatur akses perangkat seluler ke layanan organisasi berdasarkan versi OS perangkat seluler (termasuk juga perangkat seluler yang telah di-*rooting* atau di-*jailbreak*), *vendor* perangkat seluler, model perangkat seluler, atau versi perangkat lunak *client* MDM (apabila pembatasan atau pencegahan ke layanan organisasi berdasarkan versi perangkat lunak *client* dapat dilakukan). • *Server* wajib mengatur penggunaan *Bluetooth*. • *Server* wajib mengatur penggunaan GPS. • *Server* wajib mengatur penggunaan *internet tethering*. • *Server* wajib mengatur penggunaan kamera. • *Server* wajib mengatur penggunaan layanan *native* OS, seperti kalender, *built-in web browser*, e-mail client, kontak, dan layanan untuk instalasi aplikasi. • *Server* wajib mengatur penggunaan *microphone*. • *Server* wajib mengatur penggunaan NFC. • *Server* wajib mengatur penggunaan *removable storage*. • *Server* wajib mengatur penggunaan kartu *Subscriber Identity Module* (SIM), seperti memasang atau mengganti kartu SIM. • *Server* wajib mengatur penggunaan USB. • *Server* wajib mengatur penggunaan Wi-Fi. • *Server* wajib membuat *audit trail* terkait proses sistem MDM secara menyeluruh yang mana hasil-hasil audit yang diperoleh ditulis menggunakan format tertentu. • *Server* wajib menyimpan catatan tentang perubahan konfigurasi keamanan yang dilakukan pada perangkat seluler di *log* audit.

2	Kapabilitas *server* dalam mendukung tata kelola komunikasi & penyimpanan data : • *Server* wajib menggunakan teknologi enkripsi yang kuat pada komunikasi data antara perangkat seluler dengan *server* (misal VPN). • *Server* wajib mengenkripsi *data-in-transit*, seperti *e-mail* beserta *attachment*-nya, kunci enkripsi perangkat seluler, sertifikat PKI *server*, dan *database* perangkat seluler, dengan menggunakan teknologi enkripsi yang telah divalidasi oleh standar FIPS 140-2. • *Server* wajib mengenkripsi seluruh *data-in-transit* menggunakan AES 128-bit (minimum) atau AES 256-bit (direkomendasikan). • *Server* wajib memiliki dan mengimplementasi mekanisme tertentu untuk memfasilitasi aktivitas *monitoring* dan kendali terhadap metoda yang digunakan untuk melakukan akses secara jarak jauh. • *Server* wajib memiliki kapabilitas untuk mentransmisikan perintah penghapusan data ke perangkat seluler yang dikelola. • *Server*, atau lebih tepatnya admin, memiliki kapabilitas untuk menghapus seluruh data yang tersimpan di dalam perangkat seluler sebelum perangkat seluler tersebut dipindah tangankan, dibuang, atau dilakukan tindakan-tindakan lainnya.
3	Kapabilitas *server* dalam mendukung tata kelola otentikasi terhadap pengguna dan perangkat seluler : • *Server* wajib mengidentifikasi perangkat seluler yang dikelolanya sebelum *server* melakukan koneksi dengan perangkat seluler tersebut. • *Server* wajib menonaktifkan akses komponen-komponen *server* yang ilegal ke jaringan atau melaporkan kejadian ini ke petugas organisasi. • *Server* wajib menggunakan kata sandi, *mutual authentication*, dan/atau proses otentikasi lainnya, seperti *token-based authentication*, *network-based authentication*, dan *domain authentication*, sebelum *server* melakukan koneksi ke perangkat seluler yang dikelolanya secara OTA. • *Server* wajib memiliki kapabilitas untuk mengaktifkan dan menonaktifkan perangkat seluler yang dikelolanya. • *Server* wajib mengelola beberapa ketentuan dan/atau batasan keamanan di bawah ini secara terpusat. ➢ mengaktifkan atau menonaktifkan penggunaan kata sandi unuk mengunci perangkat seluler yang dikelola; ➢ menentukan kekuatan kata sandi minimum yang boleh digunakan; ➢ waktu maks. penggunaan kata sandi dibatasi (rekomendasi 30/90/180 hari); ➢ menentukan banyaknya jumlah percobaan memasukkan kata sandi yang diperbolehkan (direkomendasikan 3-10 percobaan); dan • *Server* wajib mengunci akun pengguna perangkat seluler atau menghapus seluruh data yang terdapat di perangkat seluler, baik itu data yang terdapat di memori internal maupun memori eksternal, apabila kata sandi untuk membuka perangkat seluler gagal sebanyak jumlah percobaan tertentu. • *Server* wajib memiliki kapabilitas untuk melakukan *reset* secara jarak jauh untuk menangani kejadian pengguna perangkat seluler lupa kata sandi atau akun pengguna telah terkunci. • *Server* wajib mengunci perangkat seluler secara jarak jauh apabila terdapat dugaan bahwa perangkat seluler berada di lokasi yang tidak aman dan berada dalam keadaan tidak terkunci.

4	Kapabilitas *server* dalam mendukung tata kelola aplikasi perangkat seluler : • *Server* wajib mendeteksi dan melaporkan versi OS, device driver, dan aplikasi perangkat lunak yang terpasang pada perangkat seluler yang dikelola. • *Server* wajib memiliki kapabilitas untuk mengaktifkan dan menonaktifkan akses perangkat seluler ke *application store* atau *repository* tertentu. • Server wajib membatasi pemasangan aplikasi perangkat seluler melalui *white-listing* (direkomendasikan) dan *blacklisting*. • *Server* wajib mencegah pengunduhan aplikasi yang dilakukan oleh perangkat seluler yang berasal dari sumber yang tidak dapat dipercaya; gunakan sumber yang telah dipercaya oleh organisasi. • *Server* wajib membatasi akses aplikasi perangkat seluler ke perangkat keras perangkat seluler, seperti kamera, GPS, *Bluetooth*, dan lain-lain. • *Server* wajib menggunakan mekanisme *safeguard* ketika memasang, meng-*update*, dan/atau menghapus aplikasi perangkat seluler serta selalu menyimpan inventaris saat ini yang dimiliki oleh seluruh aplikasi yang terpasang pada perangkat seluler. • *Server* wajib membatasi penggunaan OS dan layanan sinkronisasi aplikasi, seperti sinkronisasi layanan *cloud* secara jarak jauh dan sinkronisasi antar-perangkat lokal. • *Server* wajib memeriksa integritas dari aplikasi perangkat seluler dan komponen sistem perangkat seluler lainnya melalui mekanisme tertentu (misal pemeriksaan integrtas *source code* melalui tanda tangan digital) untuk menjamin bahwa hanya aplikasi yang berasal dari entitas yang telah dipercayai oleh organisasi saja yang terpasang pada perangkat seluler dan mendeteksi apakah perangkat seluler telah di-*rooting* atau di-*jailbreak*.
5	Pengguna dapat melihat kebijakan yang berlaku pada perangkat selulernya.
6	Pengguna dapat menerima perintah dari *server* dan mengirim *request* ke *server*.
7	Pengguna dan/atau perangkat seluler wajib mendukung layanan keamanan yang dikelola oleh *server*. Berikut beberapa ketentuan-ketentuan dan/atau batasan-batasan yang wajib diikuti oleh pengguna dan/atau perangkat seluler : • Mengonfigurasi perangkat seluler agar komunikasi data antara perangkat seluler dengan *server* menggunakan teknologi enkripsi yang kuat (misal VPN). • Menggunakan teknologi enkripsi yang kuat pada media penyimpanan data, baik itu *built-in storage* maupun *removable storage*. • Penggunaan removable storage dikombinasikan dengan suatu perangkat dekripsi sehingga informasi terenkripsi yang tersimpan di dalam *removable storage* hanya dapat dibaca ketika *removable storage* ini dihubungkan ke perangkat dekripsi. • Mengonfigurasi perangkat seluler agar data yang tersimpan di dalamnya dihapus secara otomatis apabila proses otentikasi gagal sebanya jumlah percobaan tertentu. • Mengunci perangkat seluler secara otomatis apabila perangkat seluler berada dalam kondisi diam selama rentang waktu tertentu (misal lima menit).

BAB 4

OPERASI KEAMANAN PADA PERANGKAT SELULER BISNIS

Bagian ini akan menjelaskan mengenai operasi keamanan pada perangkat seluler bisnis sesuai NIST SP 800-124 *Revision* 1. Seperti yang akan diperlihatkan nanti, operasi keamanan pada perangkat seluler bisnis mencakup proses pengamanan perangkat seluler bisnis selama periode penggunaannya di organisasi. Dengan kata lain, operasi keamanan yang akan dijelaskan nanti terdiri atas beberapa fase penggunaan perangkat seluler bisnis. Masing-masing fase operasi keamanan akan melibatkan konsep-konsep MDM yang telah dijelaskan pada bab sebelumnya.

4.1 Siklus Penggunaan Perangkat Seluler Bisnis

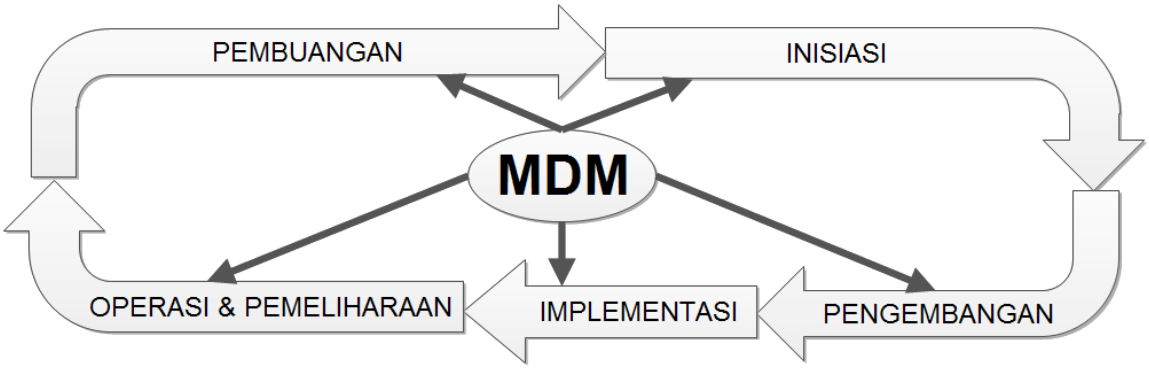
Menurut [19], ada lima fase operasi keamanan pada perangkat seluler selama siklus penggunaannya. Berikut kelima fase operasi keamanan yang dimaksud :

- Fase 1 : Inisiasi. Pada fase ini, organisasi perlu melakukan tugas-tugas tertentu sebelum mendesain solusi keamanan perangkat seluler, antara lain mengidentifikasi kebutuhan-kebutuhan perlu dimiliki oleh perangkat seluler, menyediakan pandangan umum mengenai bagaimana solusi keamanan perangkat seluler dapat mendukung misi organisasi, membuat strategi yang tepat untuk mengimplementasi solusi keamanan perangkat seluler, mengembangkan kebijakan keamanan perangkat seluler, serta menentukan persyaratan-persyaratan bisnis dan fungsional untuk mendukung solusi keamanan perangkat seluler.
- Fase 2 : Pengembangan. Pada fase ini, teknis dari solusi keamanan perangkat seluler beserta komponen-komponen lain yang berkaitan dengan solusi keamanan tersebut ditentukan. Penentuan teknis solusi keamanan perangkat seluler termasuk menentukan metoda otentikasi serta mekanisme kriptografi untuk melindungi komunikasi dan penyimpanan data. Tipe perangkat seluler, seperti *vendor*, OS, dan lain-lain, yang akan diotorisasi juga perlu diperhatikan pada fase ini karena tipe perangkat seluler dapat memengaruhi kebijakan keamanan yang dibuat. Fase pengembangan juga memerhatikan bagaimana menjamin kebijakan keamanan perangkat seluler yang dibuat selalu ditegakkan oleh seluruh *cli-*

ent yang terotorisasi. Pada bagian akhir fase, komponen-komponen pembangun dan pendukung solusi keamanan perangkat seluler diperoleh.

- Fase 3 : Implementasi. Pada fase ini, seluruh komponen yang digunakan oleh perangkat seluler dikonfigurasi supaya memenuhi persyaratan-persyaratan operasional dan keamanan yang telah ditentukan oleh organisasi, seperti kebijakan keamanan perangkat seluler yang telah dikembangkan oleh organisasi. Kemudian, sebelum diimplementasi secara riil, seluruh perlengkapan ini dipasang dan diuji sebagai pilot (percobaan). Selain itu, fase implementasi juga mengimplementasi kendali dan teknologi keamanan yang diperlukan, seperti *security event logging* dan *server* otentikasi.
- Fase 4 : Operasi dan Pemeliharaan. Operasi dan Pemeliharaan. Pada fase ini, organisasi perlu melakukan tugas-tugas tertentu yang dilakukan secara terus menerus setelah solusi keamanan perangkat seluler telah berhasil diimplementasi dan berada pada tahap operasi. Contoh beberapa tugas yang dimaksud adalah *patching*, peninjauan ulang *data log*, dan deteksi serangan.
- Fase 5 : Pembuangan. Pada fase ini, organisasi perlu melakukan tugas-tugas tertentu ketika solusi keamanan perangkat seluler atau beberapa komponennya sudah tidak akan digunakan lagi. Contoh beberapa tugas yang dimaksud adalah menjaga informasi sesuai ketentuan hukum yang berlaku, menghapus media, dan membuang perlengkapan-perlengkapan sebagaimana mestinya.

Seperti yang telah disebutkan sebelumnya, setiap fase operasi keamanan pada perangkat seluler bisnis akan melibatkan konsep-konsep MDM. Gambar 7 menunjukkan *framework* umum dari siklus penggunaan perangkat seluler bisnis yang mana organisasi atau pihak ketiga dapat memodifikasi fase-fase yang terdapat di dalam siklus penggunaan perangkat seluler bisnis sesuai dengan kebutuhannya. Selanjutnya akan dijelaskan mengenai hal-hal apa saja yang wajib dilakukan oleh organisasi atau pihak ketiga di setiap fase operasi keamanan perangkat seluler.



Gambar 7. Framework Umum Siklus Penggunaan Perangkat Seluler Bisnis.

4.1.1 Fase 1 : Inisiasi

Pada fase inisiasi, beberapa persiapan dilakukan, seperti mengidentifikasi kebutuhan-kebutuhan yang diperlukan pada saat ini dan di masa yang akan datang, serta menentukan persyaratan performansi, fungsionalitas, dan keamanan. Bagian yang paling kritis pada fase inisiasi adalah pengembangan kebijakan keamanan perangkat seluler. Pada kebijakan keamanan perangkat seluler, hal-hal yang perlu ditentukan adalah jenis-jenis *resource* organisasi apa saja yang boleh diakses oleh perangkat seluler, jenis-jenis perangkat seluler apa saja yang boleh digunakan untuk mengakses resource organisasi, level hak akses untuk masing-masing jenis perangkat seluler yang digunakan (misal penentuan level hak akses untuk perangkat seluler milik organisasi dan BYOD), dan bagaimana menangani penyediaan yang diperlukan. Selain itu, kebijakan keamanan perangkat seluler juga wajib menentukan bagaimana cara mengelola *server* yang digunakan pada MDM, bagaimana ketentuan untuk meng-*update* kebijakan terkait *server* tersebut, dan persyaratan-persyaratan MDM lainnya. Kebijakan keamanan perangkat seluler wajib didokumentasi pada rencana keamanan sistem. Sedapat mungkin kebijakan keamanan perangkat seluler yang dikembangkan konsisten dan melengkapi kebijakan keamanan non-perangkat seluler.

- Ketentuan-Ketentuan dan/atau Batasan-Batasan pada Perangkat Seluler Bisnis dan Penentuan Level Hak Akses :

  Salah satu persyaratan yang terdapat pada kebijakan keamanan perangkat seluler adalah membatasi jenis-jenis perangkat seluler yang dapat digunakan untuk mengakses *resource* organisasi. Pembatasan ini dilakukan berdasarkan beberapa alasan, seperti mengamankan *resource* organisasi dari berbagai jenis ancaman dan keterbatasan teknologi (misal perangkat seluler jenis tertentu tidak memiliki fitur keamanan yang ditentukan oleh organisasi). Contoh pembatasan jenis-jenis perangkat seluler, yaitu suatu organisasi hanya mengizinkan penggunaan perangkat seluler milik organisasi saja. Di beberapa organisasi lain, penggunaan perangkat seluler ditentukan level hak aksesnya, yaitu perangkat seluler milik organisasi diizinkan untuk mengakses mayoritas *resource* organisasi, sedangkan perangkat seluler BYOD yang menggunakan perangkat lunak *client* MDM diizinkan untuk mengakses *resource* organisasi secara terbatas, dan perangkat seluler BYOD yang lain hanya diizinkan untuk mengakses beberapa *resource* organisasi berbasis *web* (misal *e-mail*). Dengan mempraktikkan kebijakan keamanan perangkat seluler seperti ini, organisasi dapat menekan risiko yang dialaminya karena organisasi dapat mengendalikan akses yang dilakukan oleh perangkat seluler bisnis ke *resource* organisasi. Organisasi juga dapat mene-

kan risiko dengan membuat daftar jenis perangkat seluler yang diperbolehkan untuk digunakan di organisasi. Daftar jenis perangkat seluler dibuat berdasarkan versi OS, *vendor* perangkat seluler, model perangkat seluler, dan lain-lain.

Setiap organisasi wajib menentukan level hak akses untuk seluruh jenis perangkat seluler yang digunakan di organisasi. Berikut ini beberapa faktor yang perlu diperhatikan oleh organisasi ketika mengembangkan kebijakan keamanan perangkat seluler terkait penentuan level hak akses :

- Tingkat Sensitivitas Pekerjaan. Sebagian pekerjaan memerlukan akses ke *resource* organisasi, sedangkan sebagian pekerjaan yang lain tidak. Organisasi dapat mengeluarkan persyaratan-persyaratan tambahan bagi pekerjaan yang memerlukan akses ke *resource* organisasi (misal hanya mengizinkan perangkat seluler milik organisasi saja yang dapat mengakses ke *resource* organisasi). Organisasi juga perlu memerhatikan tentang penghapusan *resource* organisasi yang tersimpan di dalam perangkat seluler BYOD secara jarak jauh.
- Tingkat Keyakinan untuk Mematuhi Kebijakan Keamanan Perangkat Seluler. Memenuhi banyak persyaratan yang terdapat pada kebijakan keamanan perangkat seluler dapat dijamin apabila organisasi mengendalikan konfigurasi perangkat seluler. Untuk perangkat seluler yang tidak dipasang perangkat lunak *client* MDM, persyaratan-persyaratan yang terdapat pada kebijakan keamanan perangkat seluler dapat diverifikasi melalui mekanisme pemeriksaan status keamanan yang dilakukan secara otomatis oleh *server* MDM ketika perangkat seluler tersebut melakukan koneksi dengan *server* MDM. Tapi, sayangnya, mekanisme seperti ini tidak dapat melakukan verifikasi untuk seluruh persyaratan-persyaratan yang terdapat pada kebijakan keamanan perangkat seluler, hanya sebagian persyaratan saja yang dapat diverifikasi. Dengan demikian, apabila diperlukan tingkat keamanan yang tinggi, organisasi dapat membuat keputusan agar setiap perangkat seluler wajib menggunakan perangkat lunak *client* MDM.
- Biaya. Biaya yang dikeluarkan untuk keperluan keamanan perangkat seluler bervariasi tergantung dari kebijakan keamanan perangkat seluler yang dikembangkan. Biaya yang secara langsung dikeluarkan oleh organisasi adalah biaya untuk memproduksi perangkat seluler milik organisasi dan perangkat lunak *client*, sedangkan biaya yang secara tidak langsung dikeluarkan oleh organisasi adalah biaya untuk memelihara keamanan pada perangkat seluler bisnis dan menyediakan dukungan teknis terkait keamanan yang diperuntukkan bagi pengguna perangkat seluler.

- Lokasi Kerja. Risiko penggunaan perangkat seluler yang hanya dapat digunakan di area organisasi akan lebih kecil daripada risiko penggunaan perangkat seluler yang dapat digunakan di berbagai lokasi.
- Batasan-Batasan Teknis. Tidak semua jenis perangkat seluler beserta OS-nya dapat digunakan untuk mengoperasikan aplikasi-aplikasi *client*, seperti perangkat lunak *client* MDM. Oleh karena itu, organisasi perlu membatasi jenis OS dan perangkat seluler agar aplikasi-aplikasi *client* dapat dioperasikan di perangkat seluler bisnis.
- Kepatuhan terhadap Kebijakan Lainnya. Organisasi wajib menyesuaikan persyaratan-persyaratan yang akan dituangkan ke dalam kebijakan keamanan perangkat seluler dengan kebijakan organisasi lainnya. Sebagai contoh, salah satu persyaratan yang terdapat pada kebijakan organisasi tertentu menyatakan bahwa organisasi wajib untuk membatasi penggunaan perangkat seluler di luar negeri karena dapat mengancam organisasi. Untuk itu, persyaratan yang akan dituangkan ke dalam kebijakan keamanan perangkat seluler, yaitu larangan untuk menggunakan perangkat seluler di luar negeri atau kewajiban untuk menggunakan jasa penyewaan perangkat seluler.

Banyak organisasi yang menggunakan kendali keamanan yang ketat untuk kondisi kerja yang memiliki risiko yang tinggi, seperti hanya mengizinkan penggunaan perangkat seluler milik organisasi atau perangkat seluler yang aman saja ketika bekerja, dan menggunakan otentikasi multifaktor saat pengguna ingin mengakses perangkat seluler dan *resource* organisasi. Kendali keamanan yang lain yang mungkin dapat dilakukan oleh organisasi adalah memindahkan *resource* organisasi yang memiliki risiko tinggi ke suatu *server* yang bertanggung jawab untuk melindungi *resource* tersebut. Misal, perangkat seluler diwajibkan melakukan koneksi ke *server* untuk mengakses *resource* organisasi sehingga tidak lagi menyimpan *resource* organisasi di dalam perangkat seluler. Organisasi juga dapat mengurangi risiko dengan melarang perangkat seluler untuk mengakses informasi-informasi tertentu, seperti informasi sensitif mengenai identitas seseorang.

Karena fitur perangkat seluler, ancaman terhadap perangkat seluler, dan kendali keamanan yang diberikan pada perangkat seluler selalu berubah, organisasi wajib melakukan penilaian ulang terhadap kebijakan keamanan perangkat seluler secara periodik, mempertimbangkan untuk mengganti jenis perangkat seluler, menentukan level hak akses pengguna perangkat seluler, dan menentukan kendali-kendali keamanan apa saja yang dibutuhkan untuk mengatasi risiko yang sedang dihadapi. Organisasi juga wajib untuk mempertimbangkan penggunaan solusi keamanan perangkat seluler yang baru, memperhatikan MDM yang baru, dan menjamin kebijakan organisasi selalu di-*update* setiap saat.

- Persyaratan Tambahan bagi Pengguna Perangkat Seluler Bisnis :

  Biasanya, organisasi mempertimbangkan faktor-faktor keamanan tambahan untuk perangkat seluler yang mana faktor-faktor kemanan tambahan ini dapat membantu untuk memitigasi risiko. Namun, organisasi tidak dapat mengimplementasikan faktor-faktor keamanan tambahan ini secara langsung karena organisasi wajib terlebih dahulu memberikan pendidikan kepada pengguna perangkat seluler mengenai faktor-faktor keamanan tambahan yang akan diimplementasikan oleh organisasi serta mendefinisikan tanggung jawab pengguna perangkat seluler ketika mengimplementasikan faktor-faktor keamanan tambahan pada kebijakan organisasi dan dokumen persetujuan penggunaan perangkat seluler.

  Salah satu faktor keamanan yang dipertimbangkan meliputi *Wireless Personal Area Network* (WPAN) yang mana WPAN ini merupakan jaringan nirkabel skala kecil yang tidak memerlukan infrastruktur tertentu untuk beroperasi. Beberapa contoh teknologi WPAN adalah *keyboard* dan *mouse* yang dihubungkan secara nirkabel dengan komputer, *wireless printing*, sinkronisasi perangkat seluler secara nirkabel dengan komputer, dan *headset* atau *earpiece* yang dihubungkan secara nirkabel dengan perangkat seluler. Biasanya, operasional teknologi WPAN didukung oleh *Bluetooth* dan NFC. Apabila perangkat seluler sedang berada di lokasi yang dekat dengan ancaman, pengguna perangkat seluler wajib menggunakan teknologi WPAN secara tepat untuk mencegah terjadinya penyalahgunaan oleh pihak-pihak yang tidak berwenang.

4.1.2 Fase 2 : Pengembangan

Setelah kebijakan keamanan perangkat seluler telah selesai dikembangkan, kebutuhan-kebutuhan perangkat seluler telah seluruhnya diidentifikasi, dan persiapan-persiapan lainnya juga telah dilakukan, langkah selanjutnya adalah menentukan jenis MDM yang akan digunakan dan mendesain solusi keamanannya. Terdapat beberapa hal yang perlu dipertimbangkan ketika mendesain solusi keamanan, antara lain :

- Arsitektur. Dalam mendesain arsitektur MDM, beberapa hal yang perlu dilakukan antara lain memilih perangkat lunak *server* dan *client* MDM, penempatan *server* MDM beserta komponen-komponen lainnya yang terkait dengan MDM, dan penentuan arsitektur VPN.

- Otentikasi. Ketika mendesain proses otentikasi yang akan digunakan pada MDM, terdapat dua hal yang dilibatkan, yaitu memilih perangkat seluler dan menentukan metoda otentikasi, termasuk menentukan prosedur untuk mendistribusikan serta me-*reset* otentikator dan prosedur untuk menyediakan otentikator tersebut ke pengguna perangkat seluler. Selain itu, desain proses otentikasi juga termasuk dua hal berikut : a) mengatur akses ke sistem otentikasi organisasi yang telah ada; dan b) cara mengintegasikan proses otentikasi yang sedang didesain ke sistem otentikasi organisasi yang telah ada.
- Kriptografi. Keputusan-keputusan terkait kriptografi yang wajib dibuat, antara lain penentuan algoritma untuk menunjang enkripsi dan integritas pada komunikasi data yang dilakukan oleh perangkat seluler, dan pengaturan kekuatan kunci untuk algoritma kriptografi yang mendukung berbagai jenis ukuran kunci. Algoritma kriptografi yang telah disetujui FIPS dapat digunakan untuk melindungi *resource*.
- Persyaratan-Persyaratan Konfigurasi. Beberapa jenis konfigurasi yang perlu dilakukan, antara lain menentukan standar keamanan minimum untuk perangkat seluler (misal tindakan-tindakan yang wajib dilakukan untuk mengamankan suatu *host*), dan menentukan kendali-kendali keamanan yang perlu ditambahkan pada perangkat seluler (misal *client* VPN).
- Penyediaan Perangkat Seluler. Solusi keamanan ini membahas cara menyediakan perangkat lunak *client*, otentikator, konfigurasi-konfigurasi tertentu, dan lain sebagainya ke perangkat seluler yang telah ada dan masih digunakan maupun perangkat seluler yang baru.
- Pemeriksaan dan Pengujian terhadap Aplikasi. Solusi keamanan ini menentukan persyaratan-persyaratan keamanan, performansi, dan persyaratan lainnya yang wajib dimiliki oleh aplikasi. Setelah persyaratan-persyaratan telah ditentukan, aplikasi diuji kepatuhannya terhadap persyaratan-persyaratan tersebut.

Aspek-aspek keamanan yang terdapat pada desain solusi keamanan perangkat seluler wajib didokumentasikan di dalam rencana keamanan sistem. Organisasi juga wajib mendesain dan mendokumentasi respon insiden terkait solusi keamanan perangkat seluler.

4.1.3 Fase 3 : Implementasi

Setelah desain solusi keamanan perangkat seluler telah selesai dibuat, langkah selanjutnya adalah menguji desain solusi keamanan perangkat seluler tersebut sebagai *pilot* sebelum desain tersebut diimplementasi secara riil. Berikut aspek-aspek solusi keamanan perangkat seluler yang perlu dievaluasi untuk setiap jenis perangkat seluler :

- Konektivitas. Pengguna perangkat seluler dapat membangun dan memelihara koneksi ke organisasi dari lokasi yang diperbolehkan. Pengguna dapat mengakses *resource* organisasi yang diizinkan dan tidak dapat mengakses *resource* organisasi yang lain.
- Proteksi. Informasi yang disimpan di dalam perangkat seluler dan komunikasi data antara perangkat seluler dengan organisasi harus dilindungi sesuai persyaratan-persyaratan yang telah dikembangkan.
- Otentikasi. Proses otentikasi harus dapat diimplementasi, tidak dapat di-*compromise*, dan atau tidak dapat dihindari. Seluruh kebijakan terkait proses otentikasi terhadap perangkat seluler, pengguna, dan domain harus ditegakkan.
- Aplikasi. Aplikasi-aplikasi yang digunakan pada solusi keamanan perangkat seluler harus berfungsi sebagaimana mestinya. Ketentun-ketentun dan/atau batasan-batasan yang dikenakan pada proses instalasi dan penghapusan aplikasi harus ditegakkan.
- Tata Kelola. Administrator dapat mengonfigurasi dan mengelola seluruh komponen dari solusi keamanan perangkat seluler secara efektif, mudah, dan aman. Selain itu, perlu dipehartikan juga mengenai kemampuan pengguna dalam mengubah pengaturan perangkat lunak perangkat seluler yang mana hal ini dapat menimbulkan kerentanan pada keamanan perangkat seluler.
- *Logging*. *Security event logging* pada perangkat seluler harus berfungsi sesuai dengan persyaratan-persyaratan yang terdapat pada kebijakan keamanan perangkat seluler. Perlu diperhatikan, kapabilitas perangkat seluler dalam melakukan *security event logging* berbeda-beda. Menurut [22], terdapat delapan jenis *data logging* yang dapat digunakan untuk menangani insiden, seperti *phising* melalui *e-mail*. Berikut kedelapan jenis *data logging* tsb :
  - *Web traffic log* (termasuk *proxy log*) : Melakukan *data logging* pada *web browsing* tepatnya sesi komunikasi yang menggunakan protokol HTTP (TCP *port* 80) dan HTTPS (TCP *port* 443).
  - NetFlow : *Data logging* ini menyimpan *traffic* jaringan yang terjadi pada sistem secara menyeluruh. *Traffic* jaringan yang diperoleh biasanya berbentuk suatu pola yang dapat dianalisis untuk diperoleh gambaran umum tentang insiden, seperti cakupan serangan spionase digital beserta waktu kejadiannya. Untuk data *log*-nya sendiri, setiap data memiliki *metadata* yang berisi informasi-informasi, misal alamat IP internal-eksternal *client* dan *timestamp-size* dari sesi komunikasi yang dilakukannya.
  - DNS *log* atau *passive monitoring* : *Data logging* ini memperlihatkan pasangan alamat IP dan nama *domain*-nya. DNS yang masuk ke dalam sistem dapat berbeda-beda, tetapi data historik suatu domain yang berasosiasi dengan alamat IP-nya adalah faktor krusial

dalam mengungkap pelaku insiden spionase digital. Untuk kasus tertentu, aktivitas *attacker* yang tidak terdeteksi oleh *web traffic log* dapat dideteksi oleh DNS *log*.

- *Web server log* : *Data logging* ini memperlihatkan apakah suatu sesi komunikasi merupakan *web-access* atau *web-error*. Apabila sesi komunikasi merupakan *web-access*, hal ini merepresentasikan bahwa proses *request* valid. Sebaliknya, apabila sesi komunikasi merupakan *web-error*, hal ini merepresentasikan bahwa proses *request* tidak valid. Dengan menulusuri hasil ke-valid-an proses *request* ini (*web-access* atau *web-error*), terdapat kemungkinan praktik spionase digital yang dilakukan oleh *attacker* terhadap sistem diketahui. Misal, dengan menggunakan informasi pada *web server log*, serangan *e-mail spearphising* terhadap karyawan dapat ditelusuri.
- *Authentication log* : *Data logging* ini memberi informasi mengenai aktivitas pengguna yang mengakses layanan sistem. Dengan menganalisa data *logging* ini, aktivitas *login* yang mencurigakan dapat dideteksi. Aktivitas *login* dapat dicurigai apabila menyimpang dari aktivitas *login* yang normal. Misal, data *logging* memperlihatkan adanya dua pengguna yang sama mengakses layanan sistem secara jarak jauh di tempat yang berbeda dan letaknya berjauhan, tetapi selisih waktu antar-pengaksesannya relatif singkat.
- *Administration log* : *Data logging* ini mendokumentasikan perubahan-perubahan administratif sistem yang umumnya dilakukan oleh sistem administrator. Kegunaan data *logging* ini pada insiden spionase digital adalah mendeteksi apakah *attacker* telah membuat atau memodifikasi (meningkatkan level hak akses) akun pengguna untuk mengakses sistem atau objek sistem secara ilegal. Misal, *attacker* membuat akun pengguna baru dengan level hak akses yang tinggi kemudian menghapusnya setelah berhasil menyerang sistem atau memperoleh objek sistem yang diinginkan.
- *Security log* : Produk-produk keamanan, baik itu perangkat keras maupun perangkat lunak, umumnya akan membuat *data logging* ketika beroperasi untuk keperluan penanganan insiden. Sebagian dari produk-produk keamanan ini akan menghentikan aktivitas-aktivitas yang tidak diinginkan dan memberikan semacam tanda pada aktivitas-aktivitas tersebut. Selain itu, jika memungkinkan, produk-produk keamanan tersebut juga akan memasukkan data yang mencurigakan yang terbawa bersamaan dengan aktivitas-aktivitas yang dihentikan ke dalam karantina untuk keperluan analisis.
- *E-mail log* : *E-mail* sering digunakan sebagai tempat untuk melakukan spionase digital. Analisis terhadap informasi teknis, seperti alamat *e-mail* pengirim, topik *e-mail*, dan nama *attachment*, sangat diperlukan untuk mengatasi insiden spionase digital. Hasil analisis yang diperoleh berguna untuk mengetahui metodologi dan infrastruktur yang

digunakan oleh *attacker*. Oleh karena itu, *e-mail log* harus dibuat sedemikian rupa sehingga efektif untuk mencari *e-mail* yang mencurigakan berdasarkan informasi teknis.

- Performansi. Seluruh komponen solusi keamanan perangkat seluler wajib memiliki performansi yang baik selama penggunaan normal dan puncak. Perangkat-perangkat *intermediate* juga perlu diperhatikan performansinya, seperti *router* dan *firewall*.
- Keamanan saat Proses Implementasi Solusi Keamanan Perangkat Seluler. Proses implementasi solusi keamanan perangkat seluler itu sendiri dapat memiliki kerentanan dan kelemahan yang dapat dieksploitasi oleh *attacker*. Organisasi yang membutuhkan keamanan yang tinggi dapat melakukan penilaian terhadap kerentanan yang dimiliki oleh masing-masing komponen solusi keamanan perangkat seluler. Apabila penilaian terhadap kerentanan komponen-komponen solusi keamanan perangkat seluler tidak dilakukan, organisasi setidaknya wajib meng-*update* komponen dengan *patch* terbaru yang tersedia dan melakukan konfigurasi ulang sesuai praktik-praktik keamanan yang terbaik. Organisasi juga wajib melakukan tindakan-tindakan untuk mencegah terjadinya pengelakkan penggunaan fitur-fitur keamanan perangkat seluler, termasuk praktik *jailbreak* dan *rooting* (apabila mekanisme untuk mendeteksi kedua praktik ini mudah dilakukan).
- Pengaturan *Default*. Untuk masing-masing versi OS perangkat seluler, pihak yang mengimplementasikan solusi keamanan perangkat seluler wajib memahami setiap pengaturan yang terdapat pada perangkat seluler dan mengubah setiap pengaturan ini sesuai persyaratan-persyaratan keamanan yang telah ditentukan. Pihak yang mengimplementasikan solusi keamanan perangkat seluler juga wajib memastikan agar pengaturan-pengaturan solusi keamanan perangkat seluler yang telah diimplementasikan tidak kembali lagi menjadi pengaturan-pengaturan *default* yang tidak aman.

Organisasi wajib mengamankan perangkat seluler milik organisasi secara menyeluruh sebelum digunakan oleh karyawan. Setiap perangkat seluler yang telah dan masih digunakan, tetapi belum diimplementasikan dengan solusi keamanan perangkat seluler saat ini, perangkat-perangkat seluler tersebut wajib dikonfigurasi untuk mendukung MDM yang diadopsi oleh organisasi. Kendali-kendali keamanan yang lain perlu diimplemetasikan ketika muncul suatu risiko yang signifikan, seperti perangkat lunak *antivirus* dan teknologi untuk mencegah hilangnya data, atau biasa disebut *Data Loss Prevention* (DLP) *technologies*.

4.1.4 Fase 4 : Operasi dan Pemeliharaan

Berikut proses-proses operasional yang wajib dilakukan secara periodik untuk memelihara keamanan perangkat seluler :

- Memeriksa apakah ada *update* atau *patch* terbaru untuk komponen-komponen solusi keamanan perangkat seluler, seperti komponen-komponen infrastruktur perangkat seluler, OS perangkat seluler, dan aplikasi-aplikasi perangkat seluler, kemudian melakukan pengujian dan pengimplementasian terhadap *update* atau *patch* tersebut.
- Menjamin waktu yang digunakan oleh masing-masing komponen infrastruktur perangkat seluler, seperti *server* MDM, *server* otentikasi, dan komponen-komponen lainnya, berasal dari sumber waktu yang sama sehingga *timestamp* dari komponen-komponen tersebut sesuai dengan waktu pada sistem lainnya;
- Mendeteksi dan mendokumentasi anomali-anomali yang ditemukan pada infrastruktur perangkat seluler, termasuk adanya konfigurasi perangkat seluler yang dilakukan oleh pihak yang tidak memiliki otorisasi, melalui proses pengawasan yang dilakukan secara berkelanjutan. Selain itu, anomali-anomali yang ditemukan juga harus dilaporkan ke administrator-administrator sistem yang berkaitan.
- Memelihara inventaris aktif dari setiap data perangkat seluler, data pengguna, dan data aplikasi-aplikasi perangkat seluler.
- Melakukan aktivitas-aktivitas *awareness* dan memberikan pelatihan kepada pengguna perangkat seluler mengenai berbagai jenis ancaman yang dapat dihadapi dan rekomendasi praktik-praktik keamanan yang dapat dilakukan untuk mengatasi ancaman-ancaman tersebut.
- Mencabut akses atau menghapus aplikasi yang dianggap memiliki risiko yang tinggi.
- Menghapus data sensitif yang disimpan di dalam perangkat seluler sebelum perangkat seluler tersebut dipindah tangankan ke pengguna yang lain.

Organisasi wajib melakukan penilaian secara periodik terhadap kebijakan, proses, dan prosedurnya untuk memastikan bahwa ketiga hal ini telah dilakukan sebagaimana mestinya. Proses penilaian dapat dilakukan secara pasif, seperti meninjau ulang data *log*, maupun secara aktif, seperti melakukan *vulnerability scans* dan *penetration testing*.

4.1.5 Fase 5 : Pembuangan

Sebelum perangkat seluler keluar dari organisasi secara permanen (misal *server* yang disewa telah habis masa sewanya atau perangkat seluler yang sudah usang ingin didaur ulang) atau dipindah tangankan ke pengguna lain, organisasi wajib menghapus seluruh data yang disimpan di dalam perangkat seluler. Seringnya, proses penghapusan data yang terdapat di dalam *hard drive* dan *memory card* sulit dilakukan karena data yang disimpan tidak berada di satu lokasi (data tersebar) dan penggunaan *memori flash* sebagai media penyimpanan lebih banyak digunakan apabila dibandingkan dengan penggunaan *magnetic disk*.

BAB 5

KESIMPULAN DAN BAHAN PEMBAHASAN LEBIH LANJUT

5.1 Kesimpulan

Berikut beberapa kesimpulan yang dapat diperoleh :

1) Fitur-Fitur perangkat seluler semakin canggih sehingga kerentanan-kerentanan yang dialami oleh perangkat seluler semakin banyak. Tentunya, kerentanan-kerentanan yang semakin banyak ini menyebabkan jenis serangan yang dapat dilakukan terhadap perangka seluler semakin banyak. Berdasarkan penjelasan pada BAB 2, berikut daftar kerentanan-kerentanan dan jenis-jenis serangan yang dapat dilakukan terhadap perangkat seluler :
   - Kerentanan-Kerentanan yang dialami oleh Perangkat Seluler Bisnis :
     - kurangnya kendali terhadap keamanan fisik perangkat seluler;
     - penggunaan perangkat seluler yang tidak dapat dipercaya;
     - penggunaan jaringan komputer yang tidak dapat dipercaya;
     - penggunaan aplikasi yang tidak dapat dipercaya;
     - interaksi perangkat seluler dengan sistem yang lain; dan
     - penggunaan layanan lokasi.
   - Jenis-Jenis Serangan terhadap Perangkat Seluler Bisnis : Eksploitasi *browser*, pencegatan data, pencatatan penekanan tombol, *malware*, pelacakan lokasi secara ilegal, eksploitasi jaringan, *phising*, *spamming*, *spoofing*, pencurian/hilang, dan *zero-day exploit*.
2) Terkait MDM, berikut beberapa poin yang perlu diperhatikan :
   - MDM merupakan solusi keamanan perangkat seluler yang digunakan untuk mengendalikan perangkat seluler milik organisasi dan BYOD dengan cara mengonfigurasi perangkat seluler, mengelola keamanan perangkat seluler, dan menyediakan akses yang aman.
   - Komponen MDM teridiri dari satu/lebih *server* dan satu/lebih *client* yang saling terhubung satu sama lain melalui suatu arsitektur tertentu. *Server*, *client*, beserta arsitekturnya digabungkan dan didesain sedemikian rupa agar MDM dapat menyediakan layanan-layanan keamanan berikut : Kebijakan umum; komunikasi dan penyimpanan data; otentikasi terhadap pengguna dan perangkat seluler; dan aplikasi perangkat seluler.

Spesifik arsitektur MDM tidak berikan, tetapi *framework* umum MDM diberikan supaya organisasi dapat mengembangkan MDM sesuai kebutuhannya sendiri dengan tetap menjamin bahwa layanan-layanan keamanan MDM terpenuhi. Realisasi layanan-layanan kemanan ini juga perlu didukung oleh kapabilitas-kapabilitas *server* dan *client* sebagaimana dijelaskan pada Tabel 2.

3) Struktur operasi keamanan pada perangkat seluler bisnis terdiri dari lima fase, yaitu inisiasi; pengembangan; implementasi; operasi dan pemeliharaan; dan pembuangan. Kelima fase ini saling terhubung, seperti yang diperlihatkan pada Gambar 7. Setiap fase mendukung sistem MDM yang digunakan oleh organisasi. Tapi, fase inisiasi dan pengembangan merupakan fase yang paling penting bagi terealisasinya MDM karena dua poin berikut :
   - Pada fase inisiasi, organisasi menentukan kebijakan keamanan perangkat seluler yang merupakan bagian terpenting supaya MDM dapat terealisasi. Terdapat beberapa elemen yang wajib ada pada kebijakan keamanan perangkat seluler supaya memenuhi fungsi bisnis dan keamanan organisasi. Elemen-Elemen yang dimaksud dapat dilihat di BAB 4 Bagian 4.1.1.
   - Pada fase pengembangan, teknis mengenai penyediaan tiga dari empat layanan keamanan MDM, yaitu komunikasi dan penyimpanan data; otentikasi terhadap pengguna dan perangkat seluler; dan aplikasi perangkat seluler, ditentukan. Dengan demikian, organisasi wajib berhati-hati dalam mendesain ketiga layanan keamanan MDM tersebut agar memenuhi ketentuan-ketenuan dan/atau batasan-batasan yang terdapat pada kebijakan keamanan perangkat seluler dan kebutuhan-kebutuhan MDM lainnya.

   Meskipun fase inisiasi dan pengembangan merupakan titik paling penting bagi terealisasinya MDM, fase-fase lainnya juga memegang peranan penting karena bertugas untuk mendukung dan menjamin bahwa layanan-layanan MDM yang diinginkan oleh organisasi terlaksana sebagaimana mestinya. Secara singkat, fase implementasi berfungsi untuk menguji atau mengevaluasi desain solusi keamanan perangkat seluler yang dibuat sebagai *pilot*; fase operasi dan pemeliharaan berfungsi untuk memonitor proses-proses operasional MDM secara periodik supaya solusi keamanan perangkat seluler yang telah diimplementasi tetap terpelihara; dan fase pembuangan berfungsi untuk menghapus seluruh *resource* organisasi dan data sensitif lainnya yang terdapat di perangkat seluler bisnis ketika suatu pengguna tidak akan lagi menggunakan perangkat seluler bisnis tersebut.

5.2 Bahan Pembahasan Lebih Lanjut

Terdapat satu topik yang dapat dijadikan bahan pembahasan selanjutnya, yaitu operasi keamanan pada perangkat seluler bisnis ketika sistem MDM dan/atau atau perangkat seluler bisnis *offline*. Seperti yang dijelaskan pada BAB 3 Bagian 4.1.3 mengenai "Keamanan saat Proses Implementasi Solusi Keamanan Perangkat Seluler", sistem MDM itu sendiri dapat memiliki kerentanan dan kelemahan sendiri yang mana salah satunya, yaitu sistem MDM dan/atau perangkat seluler bisnis menjadi *offline* sehingga *server* dan client tidak saling terhubung satu sama lain. Dengan demikian, organisasi tidak dapat mengendalikan perangkat seluler secara jarak jauh dan keamanan perangkat seluler hanya bergantung pada konfigurasi serta sistem keamanan yang terpasang di perangkat seluler bisnis itu sendiri. Meskipun konfigurasi dan sistem keamanan yang diterapkan oleh organisasi pada perangkat seluler bisnis diasumsikan sudah kuat, organisasi tetap butuh kepastian bahwa *resource* organisasi atau data sensitif lainnya tidak tersebar ke pihak tidak berwenang, terutama *attacker*. Kepastian ini baru dapat diketahui ketika *server* telah terhubung kembali ke *client* dan/atau perangkat seluler bisnis berada di jangkauan organisasi.

DAFTAR PUSTAKA

[1] A. Alex. (2012, November 25). *The Pied Piper*. [online]. Available : http://www.slideshare.net/Aodrulez/the-pied-piper-15340675?from_action=save

[2] A. Gostev. (2012, May 30). *Flame: Bunny, Frog, Munch and BeetleJuice…* [online]. Available : https://securelist.com/blog/incidents/32855/flame-bunny-frog-munch-and-beetlejuice-2/

[3] Apple Inc, "Process Overview" in *Deploying iPhone and iPad : Mobile Device Management, Apple Inc*, pp 8.

[4] C. Xiao and R. Olson. (2014, December 17). *COOLREAPER: The Coolpad Backdoor* [PDF]. Available : https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-cool-reaper.pdf

[5] C. Wüest, "Spamming in social networks" in *The Risks of Social Networking*, Security Response of symantec(TM), ch.2, pp. 3.

[6] FireEye Inc. "Targeting Key Industries for Economic Espionage" in *Cyber Threats To The Nordic Region*, FireEye Inc, pp. 10-11.

[7] ForeScout Technologies Inc. "Applications – Requirements from the MDM SRG" in *Addressing NIST and DOD Requirements for Mobile Device Management*, ForeScout Technologies Inc., ch. 7, pp. 9.

[8] ForeScout Technologies, Inc. "Communications and Storage – Requirements from the MDM SRG" in *Addressing NIST and DOD Requirements for Mobile Device Management*, ForeScout Technologies, Inc., ch. 5, pp. 7.

[9] ForeScout Technologies, Inc. "Managing Policies – Requirements from the MDM SRG" in *Addressing NIST and DOD Requirements for Mobile Device Management*, ForeScout Technologies, Inc., ch. 4, pp. 5.

[10] ForeScout Technologies Inc. "User and Device Authentication – Requirements from the MDM SRG" in *Addressing NIST and DOD Requirements for Mobile Device Management*, ForeScout Technologies Inc., ch. 6, pp. 8.

[11] GreAT. (2013, January 14). *The "Red October" Campaign – An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies* [online]. Available : https://securelist.com/blog/incidents/57647/the-red-october-campaign/

[12] K. Anggriani et al. “ANALISIS DOMAIN” in *Perancangan Framework Mobile Device Management pada Platform Android*, Informatika ITB, ch. III, pp. 3.

[13] K. Anggriani et al. “Framework” in *Perancangan Framework Mobile Device Management pada Platform Android*, Informatika ITB, ch. II, sec. II.1, pp. 1.

[14] L. Sun *et al*. (2015, February 04). *Pawn Storm Update: iOS Espionage App Found* [online]. Available : http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-ios-espionage-app-found/

[15] M. McDowell and D. Morda. “Attacks and Unintended Information Disclosure” in *Socializing Securely: Using Social Networking Services*, US-CERT, pp 2.

[16] M. Souppaya and K. Scarfone. “Capabilities” in *NIST Special Publication 800-124 Revision 1 – Guidelines for Managing the Security of Mobile Devices in the Enterprise*, National Institute of Standards Technology, ch. 3, sec. 3.1, pp. 8-9.

[17] M. Souppaya and K. Scarfone. “Components and Architectures” in *NIST Special Publication 800-124 Revision 1 – Guidelines for Managing the Security of Mobile Devices in the Enterprise*, National Institute of Standards Technology, ch. 3, sec. 3.1, pp. 7-8.

[18] M. Souppaya and K. Scarfone. “Defining Mobile Device Characteristics” in *NIST Special Publication 800-124 Revision 1 – Guidelines for Managing the Security of Mobile Devices in the Enterprise*, National Institute of Standards Technology, ch. 2, sec. 2.1, pp. 2.

[19] M. Souppaya and K. Scarfone. “Security for the Enterprise Mobile Device Solution Life Cycle” in *NIST Special Publication 800-124 Revision 1 – Guidelines for Managing the Security of Mobile Devices in the Enterprise*, National Institute of Standards Technology, ch. 4, pp. 10-15.

[20] McAfee Inc, “Threat Statistics” in *McAfee Labs : Threats Reports November 2015*, McAfee Inc, pp 49.

[21] Nasjonal Sikkerhetsmyndighet, “HVA ER DIGITAL SPIONASJE?” in *Hvordan forebygge, oppdage og håndtere dataangrep*, Nasjonal Sikkerhetsmyndighet, pp. 4.

[22] Nasjonal Sikkerhetsmyndighet, “Hvordan oppdage forsøkene?” in *Hvordan forebygge, oppdage og håndtere dataangrep*, Nasjonal Sikkerhetsmyndighet, pp. 6-8.

[23] United States Government Accountability Office, “A Range of Vulnerabilities” in *GAO-12-757 – INFORMATION SECURITY : Better Implementation of Controls for Mobile Devices Should Be Encouraged*, United States Government Accountability Office, pp. 17-22.

[24] United States Government Accountability Office, “Source of Threats and Attack Methods Vary” in *GAO-12-757 – INFORMATION SECURITY : Better Implementation of Controls for Mobile Devices Should Be Encouraged*, United States Government Accountability Office, pp. 14.

[25] US-CERT, “Overview” in *Technical Information Paper-TIP-10-105-01 Cyber Threats to Mobile Devices*, U.S. Department Of Homeland Security, pp. 1.

[26] W. Wei. (2016, February 01). *Hacking Smartphones Running on MediaTek Processors* [online]. Available : http://thehackernews.com/2016/02/mediatek-hacking-mobile.html