

TUGAS AKHIR
EC 7010 KEAMANAN SISTEM LANJUT

**ANALISA KEAMANAN PADA SISTEM OPERASI PALM
DAN KEAMANAN TERHADAP ANCAMAN KODE
YANG MENGGANGGU (MALICIOUS CODE)**

oleh

BAMBANG NOOR AK
NIM : 23203101



PROGRAM MAGISTER TEHNIK ELEKTRO
BIDANG KHUSUS TEKNOLOGI INFORMASI DIKMENJUR
INSTITUT TEKNOLOGI BANDUNG

2004

ABSTRAK

ANALISA KEAMANAN PADA SISTEM OPERASI PALM DAN KELEMAHANNYA TERHADAP ANCAMAN KODE YANG MENGGANGGU (*MALICIOUS CODE*)

Oleh

Bambang Noor AK

Kemajuan teknologi informasi sudah sangat dirasakan, yang dapat dimanfaatkan sebagai bentuk komunikasi yang dapat membantu disegala bidang aspek kegiatan baik social maupun bisnis. Salah satunya alat komunikasi adalah *Personal Digital Assistant (PDAs)*, peralatan ini sangat fleksibel, praktis dan mudah dibawa kemana-mana (*portable divice*) namun alat ini masih rentan terhadap kode yang mengganggu (*malicious code*), karena memang alat ini didesain dan dirancang tidak dilengkapi dengan system keamanan. Disamping itu PDAs digunakan pada implementasi yang sangat luas dengan system yang kurang memperhatikan keamanan. PDA pada umumnya menggunakan aplikasi yang mengarah pada penyimpanan data/informasi seperti, data medical, rahasia perusahaan dan *e-commerce* yang menerakap generasi aplikasi *one-time-password*. Pengguna alat ini biasanya tidak menyadari bahwa alat ini rentan terhadap serangan virus, disamping itu alat inipun tidaklah mungkin akan menggunakan aplikasi yang aman diatas pondasi yang tidak aman. Sistem operasi (SO) pada palm mendekati 80 persen yang dapat mendukung keamanan pada PDA. Oleh karena itu SO pada palm dan hardware yang mendukung system keamanan perlu dianalisa baik dari segi kelemahan maupun segi perlindungan data/informasi.

KATA PENGANTAR

Syukur Alhamdulillah kami panjatkan kehadiran Illahi Robby yang telah memberikan rahmat dan hidayahnya, sehingga penulis bisa menyelesaikan tugas akhir mata kuliah EC.7010 Keamanan Sistem Lanjut dengan baik. Tugas akhir ini dibuat sebagai salah satu persyaratan dalam akhir mata kuliah Teknik Elektro, bidang khusus Teknologi Informasi Institut Teknologi Bandung.

Penulis menyadari sepenuhnya bahwa di dalam menyelesaikan pembuatan tugas akhir ini, banyak mendapatkan kendala dan kesulitan namun berkat bimbingan dan dorongan dari berbagai pihak, akhirnya penulis dapat menyelesaikan tugas akhir ini dengan baik. Sehubungan dengan hal itu, penulis mengucapkan rasa terima kasih kepada :

1. Bapak Dr. Ir. BUDI RAHARDJO sebagai dosen sekaligus pembimbing dalam kami menyelesaikan tugas akhir ini.
2. Tema-teman senasib dan seperjuangan di Batch 2 Teknologi Informasi Dikmenjur yang telah banyak membantu serta memberi masukan sehingga kami bisa dengan mudah dan lancar menyelesaikan tugas akhir ini.

Kami hanya bisa berdoa kepada alloh SWT, semoga amal dan budi baik dari Bapak dan Ibu sekalian mendapat pahala dan ridlo dari Alloh SWT amin.

Hormat Kami

Bambang Noor AK

ANALISA KEAMANAN PADA SISTEM OPERASI PALM DAN KELEMAHANNYA TERHADAP ANCAMAN KODE YANG MENGGANGGU (*MALICIOUS CODE*)

1. Latar Belakang

Teknologi jaringan nirkabel Wi-Fi sekarang sudah menjadi sebuah perangkat penting yang mewarnai perkembangan digitalisasi dunia. Banyak tempat di belahan dunia mulai mengarah pada pembangunan *hot-spot* sebagai wahana baru dunia digitalisasi. Perkembangan teknologi informasi yang begitu cepat telah mempengaruhi segala aspek kehidupan manusia, dengan suatu kebutuhan informasi yang tidak bisa lepas dari ke-hidupan manusia.

Kemajuan teknologi informasi sudah sangat dirasakan, dimana teknologi ini dapat dimanfaatkan sebagai bentuk komunikasi yang dapat membantu disegala aspek kehidupan baik kegiatan sosial maupun bisnis. Salah satu alat komunikasi yang dapat membantu adalah *Personal Digital Assistant (PDAs)*, peralatan ini sangat fleksibel, praktis dan mudah dibawa kemana-mana (*portable device*) serta mudah digunakan sebagai alat yang dapat menyimpan sejumlah data/informasi. Alat ini juga dilengkapi dengan sistem metode jaringan nirkabel yang dapat mengakses internet tanpa dibatasi oleh jarak, waktu dan tempat. namun alat ini masih rentan terhadap kode yang mengganggu, karena memang pada dasarnya alat ini dirancang dan di desain tidak dilengkapi dengan adanya perlindungan atau keamanan yang dapat melindungi data/informasi yang disimpannya. Sehingga alat ini masih perlu sekali metode system operasi yang dapat melindungi baik data/informasi yang disimpannya maupun jaringan nirkabelnya.

Serangan virus pada jaringan nirkabel pada (PDAs) pada umumnya tidak dimasukkan ke dalam desktop, namun seolah olah hanya merupakan merupakan serangan virus tempelan saja, tetapi sangat berbahaya terhadap data/informasi yang telah disimpannya. Untuk mengatasi hal tersebut diatas perlu adanya peningkatan

aplikasi keamanan terhadap serangan virus. Kemampuan yang ditambahkan pada alat ini adalah inframerah (IR) dan frekuensi radio (RF). Walaupun pada alat ini sudah ditambahkan IR dan RF namun serangan model baru dari kode malicious ternyata tidak bisa dideteksi oleh suatu metode tertentu, sehingga perlu adanya tambahan system yang bisa melindunginya, ternyata bahwa arsitektur jaringan pada jaringan utama, justru membuka peluang baru bagi serangan dan ancaman dari malicious pada jaringan PDA secara paralel.

Sebenarnya banyak para pengguna PDA yang tidak mengerti dan memahami sama sekali terhadap arsitektur jaringan dan operasi pada PDA bahkan mereka juga tidak mengerti bahwa informasi/data yang disimpan pada PDA merupakan jaringan/jalur terbuka dan tidak aman, karena dapat secara mudah diketahui oleh para pengguna yang lainnya yang tidak syah/tidak terdaftar, pada intinya bahwa data/informasi yang tersimpan di PDA sama halnya dengan data/informasi yang disimpan di desktop/komputer (PC). Oleh karena itu, sistem keamanan yang belum dirancang dan didesain pada operasi sistem palm perlu lebih dikaji lagi, sehingga para pemakai PDA merasa nyaman dan aman dalam menggunakannya. Walaupun sebenarnya system operasi palm tidak begitu memberikan jaminan keamanan pada sitem operasi kinerja, jika PDA digunakan sebagai alat komunikasi pada tingkat komunikasi rahasia atau jalinan kerjasama kepada para koleganya untuk tujuan keamanan data/informasi yang disampaikannya terdapat banyak sekali resiko terhadap keamanan data dan inforrmasi.

Sistem operasi palm menawarkan suatu aplikasi keamanan yang bisa digunakan sebagai penangkal serangan dan ancaman virus. Sistem aplikasi keamanan yang ditawarkan adalah system keamanan yang menyatu (built-in). Walaupun sebenarnya sistem palm tidak memberikan jaminan keamanan pada sistem operasi/kinerja, jika alat digunakan untuk tujuan keamanan, pada tingkat komunikasi/informasi data yang sangat pribadi atau rahasia. Sebagai contoh, bahwa sistem palm menawarkan aplikasi keamanan yang menyatu (built-in), bentuk aplikasi keamanan ini diberikan kepada para pengguna yang sah/terdaftar adalah *password*. Dimana *password* dapat sedikit banyak dapat menjamin keamanan untuk menyembunyikan data/informasi

yang tersimpan dari gangguan tangan jahil yang tidak bertanggung jawab terutama pada para pengguna yang tidak sah/ terdaftar. Sistem aplikasi penerapan *password* ini merupakan operasi keamanan yang menyatu. Dalam aplikasi dasar password yang menyatu itu adalah : nama, alamat, tanggal, dan keterangan pribadi. Data data tersebut bisa dijadikan *password* pribadi untuk keamanan pada data/informasi yang dibutuhkan. Contoh yang lain adalah dengan sistem "*Beam Bit*" yaitu merupakan bendera dimana setiap bendera berisi aplikasi database, yang dapat digunakan untuk mencegah informasi dari *transfer*, atau "*beamed*" ke alat yang lain melalui IR. Sistem *Beam Bit* semata-mata merupakan operasi yang benar benar terbuka dalam mengeksekusi sebuah tugas/aplikasi. Mekanisme sederhana ini seolah olah dapat memanjakan para pengguna i dan beberapa pengembang ke dalam suatu rasa aman, yang sebenarnya rasa aman itu adalah semu atau palsu.

Aplikasi keamanan yang berdasarkan pada sistem operasi palm, seperti yang terdapat pada perangkat lunak , kriptografi dan enkripsi masih memerlukan suatu sistem keamanan agar informasi/data dapat diimplementasikan. Tanpa mekanisme perlindungan yang sesuai pada tempatnya, aplikasi keamanan yang melindungi komponen rahasia sungguh merupakan risiko yang sangat besar. Propertis dari kode malicious, dapat digolongkan dalam empat langkah, yaitu :

1. infeksi
2. penyimpanan
3. triggers
4. actions.

dimana sistem palm akan menganalisa dari masing masing langkah diatas. Sehingga dengan langkah tersebut di atas sejumlah kelemahan dan vektor serangan dapat secara mudah dikenali baik yang klasik maupun yang mempunyai area teknologi baru.

Kita dapat menyimpulkan bahwa PDAs merupakan salahh satu alat komunikasi dan penyimpanan data/informasi yang canggih namun tidak dilengkapi sistem keamanan untuk serangan virus atau ancaman dari kode malicious. Sebagai tambahan, bahwa

model serangan dan model ancaman pada PDA memang dirancang dan didesain oleh perusahaan adanya keamanan serangan virus.

Dengan penuh harapan, semoga tulisan/ makalah ini dapat menjadikan sebuah pemikiran untuk kemajuan produksi PDA ini ke arah masa depan yang lebih baik dengan dilengkapi sebuah perancangan sistem keamanan guna melindungi keamanan data/informasi yang telah disimpan.

BAB I

PERSONAL DIGITAL ASSSISTANTS (PDAs)

1.1 Pengertian PDAs

PDAs merupakan sebuah alat yang dapat digunakan untuk menyimpan sejumlah data dan informasi penting, yang dapat dibawa kemana mana karena bentuknya yang sangat praktis (*portable*). PDAs merupakan computer mini yang juga dilengkapi dengan keyboard dan sebuah pena untuk menulisnya. Dalam mengakses data atau informasi PDAs dapat melalui jalur internet, karena PDA itu sendiri sudah dilengkapi dengan koneksi jaringan, dengan menggunakan sistem nirkabel. Jadi para pengguna PDAs dapat mengakses data dan informasi dimana saja berada tanpa dibatasi oleh ruang, jarak dan waktu. Dalam proses penerimaan data dan informasi PDAs akan berjalan dalam beberapa sistem, antara lain;

1. PDAs dengan sistem palm
2. PDAs dengan sistem palm V
3. PDAs dengan sistem pocket PC
4. PDAs dengan sistem IE
5. PDAs dengan sistem iPAQ pocket PC

Pada dasarnya bahwa fungsi dan kegunaan PDAs sangat luas dan kompleks, namun dalam pembahasan makalah ini, akan diuraikan tentang fungsi PDAs yang ada hubungan dan kaitan erat dengan penerimaan data dan informasi, karena dengan menggunakan sistem penerimaan data dan informasi banyak yang perlu dikaji, antara lain : koneksi atau jaringan, akses internet dan virus yang menyerang pada data dan informasi. Beberapa fungsi dan kegunaan PDAs, antara lain :

1. membaca dan menulis *file pdf* dengan *Microsoft word*,
2. mem-*back up* data dan *file memory card*
3. menggunakan extra memory pada flash ROM
4. mengatasi rusaknya file data *player*

5. mengembalikan data yang hilang
6. *power on password*
7. *multiple windows* dengan paket IE

1.1.1 Membaca dan Menulis *File pdf* dengan *Microsoft word*,

Penggunaan PDAs , baik palm sistem ataupun yng lainnya, sudah menjadi trend masa kini utnuk dijadikan sebagai perpustakaan pribadi. Hal ini semakin marak karena praktis dan sangat menyenangkan, selain itu masih dilengkapi dengan adanya *e-book* di berbagai situs/web yang banyak mendorong maraknya PDAs sebagai gudang buku elektronik.

Di internet kita akan mudah menemukan berbagai macam informasi dan data yang kita inginkan termasuk jjuga *e-book* baik yang secara Cuma-Cuma ataupun dengan cara membayar. Namun biasanya *file-file* tersebut disimpan dalam bentuk *pdb* (*Palm Data Base*) yang hanya dapat dibaca oleh palm reader. Namun demikian, meskipun bahan bacaan tersedia melimpah ruah di internet, kita masih mempunyai kendala di dalam mengakses data dan informasi yang kita maksud. Problem yang timbul adalah :bahannya ada , tetapi masih berbentuk buku atau berupa file dengan format yang umum.

Documen *word* (doc atau rtf) memang dapat dengan mudah ditransfer dalam sistem palm, tetapi tidak semudah apa yang kita lakukan. Atau tidak semudah jika file tersebut disimpan dalam bentuk file *pdb*. Demikian pula dengan file text (txt) yang dapat dibaca oleh note pad. *File acrobat* (pdf) juga demikian halnya. Selain memerlukan memerlukan aplikasi yang berbeda untuk setiap jenis file, saat kita membaca file-file pada umumnya kita selalu menekan *up* dan *down* untuk berpindah halaman tidak seperti pada palm *reader* yang cukup dengan sentuhan (tab) di layer. Agar supaya kita dapat membuat file pdf sendiri, kita haruslah menembah file sendiri yang namanya *pdoc* (dulunya *palmdoc*), dengan jalan menambahkan aplikasi *pdoc* pada window help yang ber guna untuk memudahkan membaca dan membuat *file palm database* (pdf) yang dimengerti oleh *palm reader*. Aplikasi kecil ini dijlankan

dalam platform windows dan dapat bekerja dengan baik dengan *microsoft word97*, *word2000* dan *wordXP*.

1.1.2 Mem-back up data dan file memory card

PDA's yang berbasis palm OS telah menerapkan teknologi VFS (*Virtual File System*) dengan menggunakan memory card eksternal (*expansion card*) mulai diperkenalkan. Pengguna tidak lagi dibatasi oleh kapasitas memory internal PDA's. Pengguna dapat menginstal dan menyimpan lebih banyak program dan data di *memory card* hingga kapasitas maksimal. Akan tetapi, fasilitas *expansion card* ini juga menimbulkan masalah baru. Seperti diketahui, fungsi *Hotsync* pada PDA hanya mensinkronisasikan atau mem *back up* semua file dan data yang ada di *memory internal* saja. Oleh karena itu, tidak heran apabila kebanyakan pengguna menyimpan file atau datanya di *memory card* merasa was-was dan khawatir apabila memori card akan rusak atau hilang, otomatis semua data dan infoemasi penting juga akan hilang. Trend aplikasi yang kini mulai mendukung VFS menjadikan hal ini semakin kritis. Namun ada program yang mendukung program *back up* yang mendukung VFS seperti; *BlueSync*. Program baru ini memungkinkan kita dapat melakukan back up data atau semua isi *memory card* ke dalam hardisk PC melalui proses *HotSync*. Apabila card rusak atau hilang, kita dapat menggunakan card yang lain dan mengembalikan isi *memory card* yang lama ke dalam card yang baru. Memori juga bisa disinkronisasikan dengan sebuah folder di PC, sehingga file dapat disalin ke dalam folder tersebut. Kemudian melakukan *HotSync* untuk mentranfes file langsung ke *memory card*.

Interface BlueSync terdiri dari tiga bagian;

1. *BlueSync Conduit* untuk mengatur aksi *HotSync*
2. *BlueSync Destop*, yaitu browser yang dapat digunakan untuk melihat isi memori yang telah di back up
3. *BlueSync Palm OS Application* berfungsi sebagai browser untuk PDA

Setelah instalasi ketiga interface akan muncul di PC dan PDA. Untuk melakukan proses proses *back up*, pertama kali pengguna cukup melakukan *HotSync* yang pertama, *BlueSync* hanya akan mentransfer file-file yang berubah saja.

BlueSync 1.0.0.3 hanya bisa dijalankan dalam lingkungan *platform windows 95/98/ME/NT/2000/XP* dan bisa digunakan disemua PDA palm yang mendukung VFS. Palm yang mendukung VFS adalah; palm m125 m500 dan m550. Menurut produsen *BlueSquirrel*, versi *BueSync* yang dapat kompatibel dengan PDA adalah : *Sony Clie, Handera*.

1.1.3 menggunakan *extra memory* pada *flash ROM*

PDA palm mempunyai dua jenis memori yaitu :

1. Flash ROM

Yaitu tempat menyimpan sistem operasi dan aplikasi *built in*

2. RAM

Yaitu untuk menyimpan program tambahan dan data, kapasitas 4 -8 MB

PDA palm yang dijual diluar Amerika dilengkapi dengan 5 bahasa yang dimasukkan ke dalam *flash ROM* , yang disebut dengan EFIGS (*English, French, Italian, German, Spanish*) ini hamper menyita sebagian besar kapasitas ROM. Dengan menghapus bahasa yang tidak diperlukan kita dapat mendapatkan tambahan memori sekitar 1,7MB. Untuk menghapus program bbahsa tersebut dibutuhkan dua program yaitu : dari Brayder Technology, yaitu Jack Sprat 2.0b1 dan Jack Flash 2.3.3. Kedua program ini bisa didapatkan di www.brrayder.com atau www.palmgear.com

Untuk mem-*back up* isi ROM, jalankan dahulu program *Jack Sprat* dan tap tombol reset pada tampilan konfirmasi. Dalam tampilan utama jack sprat lakukan untuk *Back Up ROM*. Back up ini penting sekali guna mengembalikan isi *flash ROM*. Dalam mem back up sebaiknya menggunakan methoda *hotsync* agar lebih terjamin. Sedangkan untuk mendapatkan extra memori, jalankan kembali *jack sprat* dan lakukan "*remove Language*" untuk menghapus bahasa yang tidak diperlukan. Setelah

melakukan penghapusan bahasa yang sudah tidak terpakai, maka memori akan bertambah sekitar 1,7 MB di *Flash ROM*, dimana memori nantinya dapat digunakan dengan melalui Jack Flash.

1.1.4 mengatasi rusaknya file data *player*

Salah satu keunggulan pocket PC dibandingkan dengan PDA jenis lain terletak pada kemampuannya dalam menampilkan grafis yang sangat baik. Ini sangat bermanfaat, terutama dalam aplikasi multimedia/hiburan seperti game. Salah satu game yang cukup menarik dan masuk dalam kategori unggulan adalah game pocket tennis. Game ini adalah game kategori sport yang sangat baik, dalam hal kualitas tampilan maupun game play. Kebetulan setelah memainkan game ini beberapa waktu, CHIP mengalami masalah. Layar yang seharusnya me load data dari pemain ternyata kosong. Pocket tennis sendiri tidak hilang, hanya saja gagal me load data dari para pemain.

Solusinya, chip mencari file “player.dat” di direktori tempat game diinstal. Hapus atau rename file ini menjadi file dengan nama lain, misalnya «player_dat», kemudian coba jalankan lagi pocket tennis. Seharusnya Pocket tennis sudah dapat berjalan dengan baik, walaupun infoemasi pemain yang pernah dibuat akan kembali pada kondisi awal seperti pertama kali menginstalnya.

1.1.5 mengembalikan data yang hilang

Tidak sengaja kita melakukan satu kesalahan sehingga tanpa sengaja file penting terhapus dengan sendirinya. Kita masih dapat mengembalikan file yang hilang lewat data back up active Sync. Perlu diingat bahwa langkah ini akan berhasil jika kita belum membuka atau melakukan back up setelah file disimpan. Data back up akan disimpandi folder

C:\windows\aplikationdata\microsoft\activesync\profile\<devicename>\synchronized files backup,

Jika menggunakan windows 200 file yang hilang dapat dicari di folder :

C:\document and setting\[username]\aplikation

data\microsoft\activesync\profile\<devicename>\synchronized file back up

1.1.6 power on password

Apabila data dan informasi penting tersimpan dengan aman, maka solusinya adalah menggunakan on-password yang telah tersedia pada sistem operasi pocket pc 2002, tersedia dua macam tingkat keamanan, pertama adalah simple dengan menggunakan 4 digit password, dimana pengguna dapat memasukkan 4 angka sebagai password. Berikutnya adalah strong alphanumeric password, yang dapat menggunakan gabungan angka dan huruf. Tingkat keamanan akan lebih terjamin. Sesuai seperti standar windows 2000. Pada menu password tersebut, pengguna dapat pula mengatur jangka waktu yang bertujuan untuk mengingat password yang digunakan.

1.1.7 multiple windows dengan paket IE

browsing merupakan salah satu kegiatan yang wajib saat ini. Bagi sebagian orang, satu hari saja tidak browsing rasanya ada yang kurang. Berkat hadirnya layanan GPRS dari IM3, para pengguna pocket PC dapat melakukan browsing dengan lebih mudah dan nyaman. Kelebihan lainnya adalah bahwa layanan GPRS ini masih relative murah bahkan masih gratis. Tidak heran jika semua pengguna Pocket PC menggunakan ponsel GPRS dan pocket PCnya untuk browsing internet. Salah satu kelemahan dari browsing pocket IE adalah ketidak mampuan untuk menampilkan multiple window. Artinya bahwa kita dapat membuka satu site dalam satu waktu, tentunya hal ini sangatlah menyebalkan, karena kita tidak bisa membuka site yang lain pada satu waktu. Namun berkat adanya multi IE atau semacam program add-on yang memungkinkan pocket IE untuk dapat membuka banyak windows pada satu waktu

BAB II

TIPE KODE MALICIOUS

2.1 Kode Malicious

Sifat dan karakter dari malicious merupakan virus yang mengancam pada sistem operasi palm, seperti yang terdapat pada perangkat lunak , kriptografi dan enkripsi masih memerlukan suatu sistem keamanan agar informasi/data dapat diimplementasikan. Tanpa mekanisme perlindungan yang sesuai pada tempatnya, aplikasi keamanan yang melindungi komponen rahasia sungguh merupakan risiko yang sangat besar. Karakter/sifat dari kode malicious, dapat digolongkan dalam empat tingkatan, yaitu : infeksi, penyimpanan, triggers dan actions. Sistem palm akan menganalisa dari masing masing langkah/tingkatan diatas. Sehingga dengan langkah tersebut di atas sejumlah kelemahan dan vektor serangan dapat secara mudah dikenali baik yang klasik maupun yang mempunyai area teknologi baru. Pada dasarnya kode malicious dibagi menjadi 3 (tiga), yaitu :

1. *a virus*
2. *a. trojan horse*
3. *a worm*

Ad. 1. A Virus

Merupakan segmen kode yang bisa mereplikasi dengan sendirinya dalam arti bahwa virus ini dapat berdiri sendiri, sehingga tatkala kita mengirimkan informasi disertai *attachment*, kode ini dapat di *attachment* ke dalam *host*. Ketika *host* kita eksekusi, secara otomatis pula kode virus juga akan dieksekusi pula, dengan demikian bahwa virus trojan ini dengan mudah akan masuk kedalam data atau informasi yang kita eksekusi. Namun sangat memungkinkan bahwa kode virus ini juga akan mereplikasi dengan sendirinya dengan mengalihkan pada eksekusi program yang lainnya. Kode virus ini kemungkinan besar akan

bertambah pada saat kita menjalankan trigger apabila kondisinya memungkinkan.

Ad. 2. A Trojan Horse

Merupakan kode malicious yang bersifat *masquerading* yang juga merupakan aplikasi yang sudah dilegimitasi. Tujuan utama dari kode ini adalah untuk memberikan pengertian kepada para pengguna agar percaya bahwa operasi pelaksanaan kode adalah standard, atau eksekusi kode ini akan berjalan pada aplikasi yang tidak berbahaya apabila pelaksanaan merupakan aktivitas yang tersembunyi. Dengan demikian, ada banyak cara guna menghindari dari serangan virus apabila para pengguna percaya akan pelaksanaan operasi kode ini. Sebenarnya *a Trojan horse* sama dengan virus pada umumnya, kecuali bila Trojan horse ini tidak berupa kode yang direplikasi.

Ad.3. A Worm

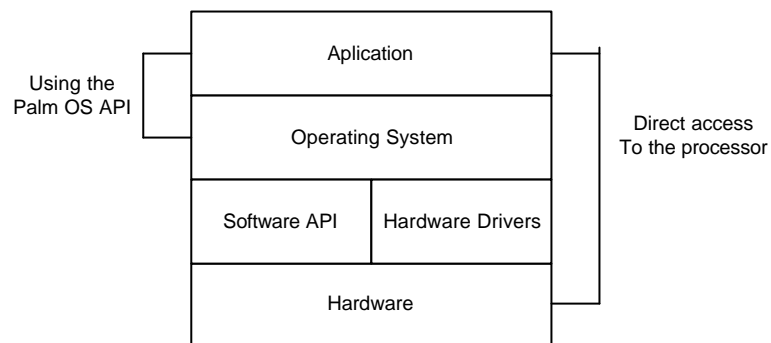
Merupakan sebuah program yang dapat mereplikasi dengan sendirinya. Karena worm dapat mengisi/masuk ke dalam host secara otomatis tanpa diminta oleh host. Program ini muncul dan masuk dalam host dikarenakan pelaksanaan eksekusi, dan tidak ada intervensi dari para pengguna. Biasanya worm bekerja pada layanan jaringan, karena worm berfungsi sebagai penyebar jaringan kepada sistem komputer lainnya.

2.2 Arsitektur *Operating system* (OS) Palm

OS palm merupakan level tertinggi dalam arsitektur sistem palm, dan pada dasarnya sistem yang ada pada PDAs dapat dibagi menjadi 3 bagian ;

1. layer aplikasi,
2. sistem operasi,
3. hardware.

Ketiga bagian tersebut tidak dapat dipisahkan satu dengan yang lainnya karena ke tiga bagian tersebut membentuk satu kesatuan yang dapat mendukung dalam sistem operasi palm. Sedangkan sistem operasi palm itu sendiri menggunakan sistem *Aplikation Programming Interface* (API) dimana sistem ini mampu menyediakan pengembangan aplikasi dengan perkiraan hardware yang independen serta menyediakan layer yang abstraksi/layer yang dapat berpindah pindah.



Gambar 1.1. Arsitektur PDAs

Apabila API digunakan sesuai dengan kinerja, penyusunan dari aplikasi merupakan hal yang sangat penting dalam upaya menjalankan OS Palm, dimana OS palm berdasar/berbasis pada hardware yang berbeda. Hal ini sangat penting guna menguji akan kelemahan/kejelekan dan serangan vector yang barangkali akan dapat ditemukan pada interfase pemrograman pada OS.

Akses prosesor secara langsung dapat menghindari interfacce dengan melalui OS yang memperbolehkan pada pengembang untuk memperoleh banyak fungsi dan control pada prosesor. Resiko dari lgimitasi yang menggunakan akses langsung akan memperangaruhi hilangnya kecocokan/kesesuaian pada model masa depan. Sebagai cotnoh Pada OS Palm sistem versi terdahulu, tidak cocok (support) pada penggunaan LCD melalui OS palm API. Walaupun demikian proses hardware menolak pada capbilitinya. Dengan melalui interface dan menunjuk pada fungsionalitas, prosesor secara langsung akan memperbaiki proses ini . Idealnya dalam menyediakan beberapa kesamaan akses control dan keamanan, hanya operating sistem akan memiliki akses pada hardware yang dibuthkan saja.

Mengikuti aplikasi pada akses langsung, hardware akan menyediakan sebuah kesempatan untuk serangan malicious.

2.2.1 Operating Sistem

Operasi sistem pada Palm sudah didesain sedemikian rupa sehingga OS ini terbuka (open source) dan modularnya selalu support pada aplikasi pengembangan, aplikasi pengembangan ini dapat dibagi menjadi 3 bagian. Layer dugaan atau file yang berbasis akses control yang pada khususnya . Hal ini tidaklah begitu mengejutkan bahwa pada semua program code dan data dapat di akses dan di modifikasi oleh para pengguna atau aplikasi yang lainnya. Pada kenyataannya secenario memory akses, sangat sulit dibedakan antara legimitasi dan aplikasi melicious dari memori membaca dan memari menulis dan berbagai sistem calling (panggil). Berikut ini merupakan file sistem dan struktur aplikasi :

1. operasi sistem palm tidak menggunakan file dengan sistem flat yang tradisioanal. Data disimpan pada memori chunk yang sudah dikenal dengan sebutan "record" dimana record tersebut dikelompokkan dalam sebuah basis data. Untuk dapat mengirim Basis data ke dalam file. Basis data harus berbentuk analog, sehingga pengiriman tersebut bisa lancer dan masuk ke dalam file. Guna menghindari serta mengganti terjadinya penumpukan penyimpanan di memori *chunk*, maka basis data harus dibagi dalam beberapa multi record. Dengan demikian penumpukan penyimpanan dapat dihindari sehingga informasi yang kita butuhkan akan mudah untuk diproses atau dieksekusi.
2. aplikasi OS palm pada umumnya merupakan pelayanan single/tunggal, kecuali pada program driven. OS hanya dapat dieksekusi atau dijalankan pada satu program pada waktu yang sama. Setiap aplikasi hanya mempunyai satu fungsi yang sama pada program utama di drive C. Untuk meyebarkan aplikasi, OS palm memanggil Pilot utama untuk mengirim pada luncuran kode. The *launch* ini bersifat specific bahwa aplikasi akan menjadi aktif dan

display pada setiap interface para pengguna.. Sasaran dan fungsi main pilot adalah menerima kode *launch* dan meresponnya. Guna merubah aplikasi OS dalam pengembangan di masa yang akan datang, dapat dilakukan dengan cara mengikuti 3 bagian dari aplikasi ke multi thread;

3. Aplikasi palm dapat mengirim kode *launch* kepada sistem yang lainnya. Karena OS palm kemungkinan besar akan menjadi *launch* dengan memperhatikan dari sistem yang sedang dijalankan . Sebuah aplikasi dapat menggunakan kode *launch*, apabila kita menginginkan untuk meminta aplikasi yang lainnya, yang nantinya dapat membentuk sebuah aktifitas atau memodifikasi data.

2.2.2 Hardware

Semua OS palm device, termasuk handspring, sony, IBM, Kyocera, QUALCOMM, Franklin Covey, TRG dan simbol teknologi lainnya, semuanya itu menggunakan Motorola Dragon Ball MC68328 , yang merupakan famili dari microprosesor. Proses dari hardware tersebut di atas semua berdasar pada sistem yang ada pada Motorola MC68EEC000 core2 Pada Prosesor DragonBall merupakan hardware yang *low-speed*, Dragon Ball hanya mampu berjalan pada rentang 16 mhz, sampai 33 MHz, itupun masih tergantung pada tipe (MC68328, EZ328, atau VZ328). Guna meningkatkan daya kerja dari drogon Ball dapat ditambahkan sistem ARM *limited arsitektur microprosesor*, ARM merupakan produk dari perusahaan, nirkabel dan keamanan jaringan, yang diharapkan mampu untuk diimplementasikan pada OS palm.

Pada OS palm dan sistem embaded menggunakan battery Backed random access memary (RAM) untuk mengirim aplikasi dan data pengguna..Pada operating sistem dan operating yang lainnya (non transient) komponen sering di simpan pada Rad only Memory (ROM). Walaupun device baru akan bergerak menuju flash memory, ini khusus untuk component yang statis, seperti pada operating sistem. Memory Flash merupakan non volatile, berarti data yang telah disimpan akan utuh dan tidak akan hilang apabila kehabisan battery atau dengan cara di reset. Operating sistem palm berbasis pada ROM atau penyimpanan flash dan dengan sistem reset.

2.3 Retrieval Of password

Sangat memungkinkan, dengan menggunakan angka dan metoda, kita dapat mengekstrak data dari device portable, namun hal yang perlu diingat adalah kita harus menyakinkan bahwa data tersebut sudah di *back up*. Karena data yang dibaca adalah data mentah atau data yang diambil langsung dari *host*. Tidak menutup kemungkinan bahwa system yang tengah dijalankan akan mendapat serangan. Penyerangan data ini akan didapat kembali dalam data dan file atau data data penting lainnya, seperti password, financial, medical atau perusahaan yang lainnya atau informasi personal tatkala sistem dijalankan. Namun penyerangan kembali dan pengambilan data tersebut haruslah ada persetujuan dari *official scan*, atau pengarang/pembuat. Guna melindungi data dan informasi penting lainnya, pengguna haruslah mempunyai *password*, guna menemukan data dan informasi yang kita butuhkan. Dengan adanya *password* secara tidak langsung kita juga mengamankan dan menjaga data pada PDA, berarti juga para pengguna telah menjaga aset perusahaannya.

Salah satu contoh, pada aplikasi keamanan tingkat tinggi adalah data medical/kesehatan. Penyimpanan data ini sangat penting artinya bagi seorang dokter dalam memahami status pasien atau penderita, sehingga para dokter dapat menganalisa penyakit si pasien dengan tepat dan akurat, hanya dengan mengakses data informasi tentang penderita/pasien. Dengan demikian para dokter dapat mengantisipasi pada keadaan, situasi pada status pasien yang gawat. Namun banyak para pengacau rumah sakit mempunyai sejumlah data dan kesempatan guna menyerang pada suatu tiang penyangga data pasien yang tidak diproteksi dari OS palm device. Guna menghindari hal tersebut di atas, perlu kiranya menggunakan *password*, sebagai sistem keamanan enkripsi dan akses kontrol pada OS palm device. Namun penggunaan *password* tidak selama aman. Sejarah telah mengingatkan adanya kelemahan atau kejelekan pemilihan atau penyimpanan dengan *password*. Seperti yang ditunjukkan pada *Morris Worm*. Pengguna pada portable device, khususnya pada pengguna yang tidak memiliki keyboard dan penerimaan input data hanya dengan menggunakan pena. Memilih menggunakan

password dengan jumlah karakter yang terpendek, karena dengan menggunakan karakter yang pendek, akan mendapatkan suatu kemudahan, praktis, simpel dan familiar. Disamping itu karakter yang pendek akan berada pada posisi yang baik pada tingkat keamanannya. Dengan hal ini, bahwa malicious akan mendeteksi/mengenal *password* yang dipakai oleh para pengguna pada local device, pada koneksi jaringan dan pada sistem jaringan yang lainnya. Usaha ini untuk mendapatkan akses pada sistem yang lain dengan menggunakan nama pengguna dan *password* yang sudah dikenal.

2.3.1 Password decoding Details

Password diatur/dibuat dengan mengingat akan legimitasi antara pengguna dengan aplikasi keamanan. Panjang maksimum standart ASCII untuk *password* adalah 13 karakter. Tanpa memperhatikan panjang maksimum dari ASCII, mengakibatkan code/sandi selalu memblok 32 byte. Ada dua methoda yang digunakan dalam mengkodekan password pada ASCII, namun hal ini tergantung panjang karakter *password* yang digunakan. Pada penggunaan password 4 karakter atau kurang, kalkulasi index akan berdasar panjang dari karakter password yang digunakan dan penggunaan string adalah XORed yang berlawanan dengan penggunaan 32 byte. Untuk password yang lebih dari 4 karrakter , string mengisi pada 32 byte dan berjalan menuju 4 putaran dari sebuah fungsi bahwa XORs berlawanan dengan 64 byte pada konstan blok. Dengan pengertian pada skema code, hal ini memungkinkan untuk berjalan pada rutinitas untuk melawan decode dari pada *password*.

Software palm digunakan pada Serial Link Protokol (SLP) untuk menstransfer data dan information pada palm device. Setiap SLP terdiri dari beberapa paket, diantaranya; paket header, paket footer dan paket client data dengan berbagai ukuran variabel. Selama HotSyancnegoation Process, satu particular dari SLP yaitu paket client akan membentuk sebuah struktur yang berisi tentang encode blok *password*. Untuk lebih jelasnya, dapat dilihat pada *source code* dibawah ini.

Struck {

```

UInt8 header [4] ;
UInt8 exec_buf [6] ;
In32 userID;
In32 vieweID;
In32 lastSyncPC;
Time_t successfulSyncDate;
Time_t lastsyncDate;
UInt8 userlan ;
UInt8 passwordlan ;
UInt8 username[userLen+1] ;
UInt8 password [passwordLen+1] ;
};

```

Gambar 1.2 struktur proses encoding password blok.

Apabila kita menggunakan *Password* yang terdiri dari 4 karakter atau kurang dari 4 karakter, dengan membandingkan pada encode blok dari variasi *password* yang mempunyai karakter pendek, (lihat contoh pada gambar 1.3) dimana diketahui bahwa 32 byte constant (gambar 4) merupakan hal yang sangat simple/ringkas dari XORed melawan ASCII password blok. Source code dibawah ini menggambarkan penggunaan karakter pendek.

A = ASCII password

B = 32 byte constant blok

C = encode password blok

Pada awal index, j masuk pada consatan blok dimana operasi XOR akan mulai menghitung dengan cara :

$$J = (A[0] + \text{strlen}(A) \% 32);$$

Untuk encode password blok, sebagai berikut :

```

For (I = 0; I < 32; ++I, ++j)
{
If (j == 32) j = 0;
C[i] = A[i] XOR B[j];
}

```

56	8C	D2	3E	99	4b	0F	88	009	02	13	45	07	04	13	44
0C	08	13	5A	32	15	13	5D	D2	17	EA	D3	B5	0F	55	63

Gambar 1.3 encode password blok ASCII password test

Penggunaan *Password* lebih dari 4 karakter

Skema dari encode untuk *password* yang menggunakan karakter panjang panjang atau menggunakan 4 karakter lebih,

09	02	13	45	07	04	13	44	0C	08	13	5A	32	15	13	5D
D2	17	EA	D3	B5	DF	44	63	22	E9	A1	4A	99	4B	0F	88

Gambar 1.4 32 byte constant blok untuk 4 karakter lebih

Karakter dengan panjang 31 ini lebih complex daripada yang karakter pendek, walaupun dalam prakteknya bisa dan dapat ditukar balikan.

A = ASCII password

B = 64 – byte constant blok

C = encode password blok

Pertama A diisi dengan 32 byte , seperti terlihat dibawah ini,

```
J = strlen (A);
```

```
While (j<32)
```

```
{
```

```
For (I = j; i < j * 2; ++i)
```

```

// nilai increment ASCII adalah j
A[i] = A[I - j] + j;

J = j * 2
}

```

Akibat dari array 32 byte, A, yang kemudian diberikan 4 putaran pada fungsi XORs melawan 64 byte constant. Gambar 1.5. k adalah merupakan index yang mulai dari {2,16,24,8} pada setiap 4 putaran.

```

J = (A[k] + A[k+1]) & 0x3F;
// 6 SLB
Shift = (A[k + 2 ] + A [k + 3]) & 0x07;
// 3 SLB

```

```

For (I = 0; I < 32; ++I, ++j, ++k)
{
//menjaga putaran untuk mulai

If (j == 64) = 0;
If (k == 32) k = 0;
temp = B[j]; // xy
temp = << 8;
temp |= B [j]; // xyxy
temp >> = shift

C[k] XOR = (unsigned char) temp;
}

```

Akibat password blok 32 byte (example gambar 6) tidak akan mendapatkan secara cepat sissa dari constant blok seperti pada karakter pendek. Waloupin hal itu masih dapat di balikan dengan minimal daya pada computer.

B1	56	35	1A	9C	98	80	84	37	A7	3D	61	7F	2E	E8	76
2A	F2	A5	84	07	C7	EC	27	6F	7D	04	CD	52	1E	CD	5B
B3	29	76	66	D9	5E	4B	CA	63	72	6F	D2	FD	25	E6	7B
C5	66	B3	D3	45	9A	AF	DA	29	86	22	6E	B8	03	62	BC

Gambar 1.5 ; 64 byte constant blok untuk 4 karakter lebih

18	Oa	43	3a	17	7d	A3	Ca	D7	9d	75	D2	D3	C8	A5	CF
F1	71	07	03	5A	52	4B	B9	70	2D	B2	D1	DF	A5	54	

Gambar 1. 6 ; encode password blok dari ASCII password “testa”

2.4 Rekomendasi

OS palm 4.0 yang disosialisaikan pada tahun 2001. diharapkan dapat memecahkan berbagai persoalan pada password. Walaupun hal ini telah direkomendasikan melalui analisa dari os 4.0 yang berlangsung sebelum adanya keamanan yang dapat melindungi informasi penting.

Pada suatu tempat direkomendasikan bahwa OS palm tidak bisa dipercaya untuk menyimpan berbagai informasi yang penting. dalam masalah ini baik pengguna ataupun vendor berbesar hati untuk mengikuti petunjuk guna peningkatan keamanan password.

2.4.1 Mekanisme Respon

Mekanisme respon ini akan meminimalkan potensi dalam melawan kumpulan password melalui monitoring dari medium transport. Transfer untuk komponen rahasia, seringkali merupakan encode, yang bisa diterima buses (contoh pada; serial, IR, nirkabel atau jaringan) yang merupakan pengambilan keputusan yang rawan atau tidak baik. Sayangnya,, hal ini merupakan hal yang wajar bahwa aplikasi pemilihan pada *password* yang simpel dan praktis akan lebih bermakna dan

dapat dijadikan keamanan data dan informasi yang baik dari pada memilih enkripsi sebagai sistem keamanan data dan informasi..

2.4.2 Enkripsi dan kepercayaan pada sistem penyimpanan

Obfuscation yang simple dan transformasi yang dapat diputar balik menyebabkan pada pengguna dapat terbuai untuk masuk pada suatu kesalahan yang tidak terduga pada segi keamanan data dan informasi. Hal ini ditunjukkan pada simultan yang tak dicermati oleh para pengguna mengenai keamanan yang diberikan oleh para vendor. Penggunaan dari keamanan sistem garam (salt) bekerjanya sama seperti pada sistem palm, yaitu dengan diawali oleh; nama pengguna, ID pengguna. Disamping itu bahwa serial number yang bersifat unique pada device palm, akan meminimalkan kemungkinan bahwa *password* akan dapat dimunculkan pada multi sistem dengan *hash* yang sama.

2.4.3 Teknik implementasi untuk mengunci pada sistem enkripsi

Aplikasi keamanan pada OS palm sistem menyediakan “sistem pengunci” pada fungsi sistem ini device palm tidak akan dapat beroperasi dan berjalan dengan baik selama password yang diberikan tidak benar, pemberian password yang benar akan mempercepat dan memperlancar proses. Hal ini menunjukkan bahwa guna mencegah kepada para pengguna yang tidak terdaftar akan bisa masuk untuk membaca data, menulis data atau membuka aplikasi pada device. Walaupun sistem keamanan ini dapat di dicegat dipertengahan jalan, karena sistem ini menyediakan sebuah layer yang dapat diproses pada layer berikutnya, layer ini berada dan berjalan pada fakta keterangan deployment. Dengan demikian enkripsi data dapat dicapai dengan menggunakan 3 bagian dari aplikasi. Dengan proses yang demikian ini akan dapat di ambil alih pada variasi penyimpanan keamanan dari komponen enkripsi.

BAB III

KESIMPULAN DAN PENUTUP

3.1. Kesimpulan

Dengan telah selesainya makalah ini, maka dapat ditarik kesimpulan :

1. PDAs merupakan alat komunikasi yang canggih, dalam bentuk yang portable yang dapat di bawa kemana mana dan dapat mengakses data dan informasi tanpa dibatasi oleh jarak, ruang dan waktu;
2. Dengan adanya system OS palm, dapat dijadikan suatu jaminan keamanan untuk data dan informasi dengan menggunakan PDAs;
3. Dengan memahami kelemahan system malicious, kita dapat memanfaatkannya untuk meningkatkan keamanan jaringan dalam mengakses data dan informasi;
4. Sistem keamanan dalam hal penyimpanan data dan informasi dapat dijamin berkat adanya system OS palm dan malicious code;.
5. Terdapat beberapa Sistem yang digunakan pada PDA, antara lain OS palm, pocket PC, Pocket IE, dan iPAQ Pockety PC.

3.2. Penutup

Makalah ini dibuat untuk melengkapi tugas akhir mata kuliah Sistem Keamanan Lanjut. Penulis yakin dan sadar bahwa makalah ini jauh dari sempurna, oleh karena itu kami mengharapkan kritik dan saran guna penyempurnaan makalah untuk masa yang akan datang. Atas perhatian dan pemberian kritik dan saran yang membangun, penulis mengucapkan beribu terima kasih. Semoga Alloh SWT memberikan pahala dan ridlo untuk kita semua. amin

Daftar Pustaka

1. D. Balfanz and E. Felten “Hand-Held computers can be better smart card”, 8th USENIX Security Symposium, Washington D.C august 1998.
2. ARM Ltd., “Motorola’s Dragon Ball prosesor Portfolio to Include ARM Architecture in 2001,” Press release, Desember 11, 2000.
3. Palm. Inc, Palm OS *Programmer’s Development Tool Guide* DN 3011 – 002
4. Palm. Inc, Palm OS *Programmer’s Companion* DN 3001 – 003
5. Palm. Inc, Palm OS SDK Reference DN 3003 – 003