Serba Serbi
Keamanan Sistem Informasi

Rahmat M. Samik-Ibrahim
http://rms46.vLSM.org/2/130.pdf
(revisi 2005.11.29.00)

Dikembangkan dengan OpenOffice.org 2.0 berbasis distro De2.UI
Versi awal dibuat oleh Arrianto Mukti Wibowo.

Memperkenal Diri

- Rahmat M. Samik-Ibrahim
  - **UI** (1984 - ?)
  - **vLSM.org** (1996 - ...)
- WebPages:
  - **http://rms46.vLSM.org/**
  - **http://rmsui.vlsm.org/rms46/**
  - **http://komo.vLSM.org/** (560 Gbytes)
  - **http://kambing.vLSM.org/** (1000 Gbytes)
  - **http://bebas.vLSM.org/** (Dokumen)
  - **http://gtm.vLSM.org/** (Grounded Theory)
  - **http://de2.vlsm.org/** (De2.UI: distroLinux)

Latar Belakang

- Keamanan Sistem Informasi merupakan:
  - hal yang rumit namun dapat dipelajari
  - cakupan yang sangat luas
  - aspek yang universal
- Lebih dari 90% permasalahan:
  - serupa untuk sistem operasi **apa pun**
  - serupa untuk berbagai distribusi (distro)
- Kurang dari 10% permasalahan:
  - merupakan hal-hal spesifik (umpama Debian)
  - sering berubah dari waktu ke waktu
  - perlu dipantau secara terus menerus

Tujuan

- Memperkenalkan aspek keamanan Sistem Informasi secara umum
- Mengungkapkan hal-hal yang spesifik pada keluarga distribusi (distro) Debian GNU/Linux.
- Memahami bahwa solusi tanggung/tidak lengkap dapat berakibat fatal.
- Memahami bahwa solusi hari ini belum tentu cocok diterapkan dikemudian hari
- Memahami bahwa aspek non-teknis sama pentingnya dengan aspek teknis

Ilustrasi Kasus Keamanan

- Pihak yang tidak bertanggung-jawab:
  - memodifikasi situs Internet.
  - memanfaatkan kartu-kredit untuk belanja.
  - memalsukan email.
  - memalsukan transaksi e-commerce.
  - membuat virus komputer.
  - menyerang/memacetkan saluran internet.
- Hal-hal yang "**teknis**" di atas, bersama yang "**non-teknis**" harus dipahami secara menyeluruh (holistik)

Isyu Keamanan Sistem Informasi

- Keperluan Sistem Informasi
  - penjaminan **INTEGRITAS** informasi.
  - pengamanan **KERAHASIAN** data.
  - pemastian **KESIAGAAN** sistem informasi.
  - pemastian **MEMENUHI** peraturan, hukum, dan bakuan yang berlaku.

Bidang/Domain Keamanan Sistem Informasi

- Aspek keamanan Sistem Informasi sedemikian luasnya, sehingga dapat dibagi menjadi 11 bidang/domain/sudut pandang.
- Ke-11 bidang ini bersifat universal, sehingga pada prinsipnya serupa untuk berbagai sistem operasi dan distribusi (distro).
- Selintas yang **"ditinjau"** ialah itu-itu juga; namun dari sebelas sudut pandang yang berbeda!

11 Domain Keamanan (1)

- **Pelaksanaan Pengelolaan Keamanan** (*Security Management Practices*).
- **Sistem dan Metodologi Pengendalian Akses** (*Access Control Systems and Methodology*).
- **Keamanan Telekomunikasi dan Jaringan** (*Telecommunications and Network Security*)
- **Kriptografi** (*Cryptography*).
- **Model dan Arsitektur Keamanan** (*Security Architecture & Models*).

11 Domain Keamanan (2)

- **Keamanan Pengoperasian** (*Operations Security*).
- **Keamanan Aplikasi dan Pengembangan Sistem** (*Application and Systems Development Security*).
- **Rencana Kesinambungan Usaha dan Pemulihan Bencana** (*Disaster Recovery and Business Continuity Plan -- DRP/BCP*).
- **Hukum, Investigasi, dan Etika** (*Laws, Investigations and Ethics*).
- **Keamanan Fisik** (*Physical Security*).
- **Audit** (*Auditing*).

1. Pelaksanaan Pengelolaan Keamanan (1)

- *Security Management Practices*
- Mempelajari:
  - mengidentifikasi asset (informasi) perusahaan
  - menentukan tingkat pengamanan asset tersebut
  - menaksir anggaran keamanan yang diperlukan
  - menyelaraskan antara anggaran yang tersedia dengan asset yang akan dilindungi.

1. Pelaksanaan Pengelolaan Keamanan (2)

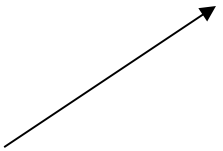
- Cakupan:
  - alur pertanggung-jawaban
  - administrasi
  - model keamanan organisasi
  - keperluan keamanan untuk bisnis
  - pengelolaan risiko
  - analisa risiko
  - prosedur
  - bakuan
  - kebijaksanaan
  - lapisan/ring keamanan
  - klasifikasi data
  - sosialisasi aspek keamanan

Mulai dari mana?

Nilai "Information Asset"

Resiko
(kemungkinan terjadi, kemungkinan kerugian per kasus, dll)

	Kecil	Sedang	Tinggi
Kecil			
Sedang			
Tinggi			



Fokuskan pengamanan mulai dari sini

1. Pelaksanaan Pengelolaan Keamanan (4)

- Ilustrasi Klasifikasi Berkas:
  - Pengguna: r w x
  - Group: r w x
  - Umum: r w x
- Ilustrasi Ancaman:
  - Ancaman: Kebakaran/Api
  - Masalah: Tidak Ada Pemadam Kebakaran
  - Akibat: Kerusakan Sistem

2. Sistem dan Metodologi Pengendalian Akses (1)

- *Access Control Systems & Methodology*
- Mempelajari:
  - mekanisme/metode pengendalian akses
  - identifikasi, otentifikasi dan otorisasi
  - pemantauan penggunaan sistem

2. Sistem dan Metodologi Pengendalian Akses (2)

- Cakupan:
  - Identifikasi
  - Otentikasi
  - Otorisasi
  - Model-model Pengendalian Akses
  - Teknik Kendali Akses
  - Metoda Pengendalian Akses
  - Administrasi Pengendalian Akses
  - Ancaman-ancaman Pengendalian Akses

2. Sistem dan Metodologi Pengendalian Akses (3)

- Ilustrasi
  - Identifikasi:
    - User-Name
    - Sidik-Jari
    - Tanda-tangan
    - Kartu Anggota
  - Otentifikasi:
    - Password
    - Tanya-Jawab
  - Otorisasi:
    - Akses
    - Ubah
    - Hapus Berkas.

3. Keamanan Telekomunikasi dan Jaringan (1)

- *Telecommunications and Network Security*
- Mempelajari:
  - teknologi dan protokol jaringan
  - perangkat jaringan terkait
  - aspek keamanan terkait yang terkait

3. Keamanan Telekomunikasi dan Jaringan (2)

- Ruang Lingkup
  - model tujuh lapisan jaringan ISO/OSI
  - model rujukan protokol TCP/IP
  - topologi LAN, MAN, WAN, VPN
  - perangkat jaringan
  - perangkat nirkabel
  - *firewall*
  - aspek keamanan

3. Keamanan Telekomunikasi dan Jaringan (3)

- Ilustrasi **'allow'**

```
# Berkas:  /etc/hosts.allow
# service: hostname : options

ipop3d: ALL: ALLOW

ALL: ALL@192.168.124.1  : ALLOW
ALL: ALL@192.168.124.10 : ALLOW
```

- Ilustrasi **'deny'**

```
# Berkas:  /etc/hosts.deny
ALL: ALL
```


4. Kriptografi (1)

- *Cryptography*
- Mempelajari:
  - metoda dan teknik penyembunyian

4. Kriptografi (2)

- Cakupan:
  - kriptografi simetrik
  - kriptografi asimetrik
  - kekuatan kunci
  - system kriptografi
  - PKI: Public Key Infrastruktur
  - fungsi satu arah
  - fungsi hash
  - pengelolaan kunci
  - serangan kriptografi
  - tandatangan digital

4. Kriptografi (3)

- Ilustrasi fungsi password (satu arah)

```
# passwd user1
Enter new UNIX password:  [rahasia]
Retype new UNIX password: [rahasia]
```

- Ilustrasi berkas **/etc/shadow**

```
...
user1:$1$ADaQTYGz$xjHux3HCLvq.zw3Yq1Sit.:13115:0:99999:7:::
...
```


4. Kriptografi (4)

- Ilustrasi Membuat Kunci **GnuPG**

```
# gpg --gen-key
[...]
gpg: /home/dummy/.gnupg/trustdb.gpg: trustdb created
gpg: key A8F128EE marked as ultimately trusted
public and secret key created and signed.
[...]
pub   1024D/A8F128EE 2005-11-29
      Key fingerprint = D8F8 D13D 3CBC 6990 FF47  5B15 7873 7940 A8F1 28EE
uid   Dummy <dummy@dummy.com>
sub   2048g/8BEEDC59 2005-11-29
```

- Tanda-tangan berkas “Release” dengan GnuPG

```
# gpg -b --armor -o Release.gpg Release
```


5. Model dan Arsitektur Keamanan (1)

- *Security Architecture & Models*
- Mempelajari
  - konsep, prinsip dan standar untuk merancang dan mengimplementasikan aplikasi, sistem operasi, dan sistem yang aman.

5. Model dan Arsitektur Keamanan (2)

- Cakupan:
  - keamanan arsitektur komputer
  - hak minimum
  - domain
  - model keamanan
    - *state machine*
    - *Bell-LaPadula*
    - *Biba*
    - *Clark-Wilson*
  - Buku *Orange*
  - FIPS
  - BS/ISO 17799
  - Sistem terbuka vs. sistem tertutup.
  - Sertifikasi vs. Akreditasi
  - Ancaman terhadap model dan arsitektur keamanan

5. Model dan Arsitektur Keamanan (3)

- Prinsip-prinsip
  - hak minimum *(least previlage*)
  - pertahanan berlapis (*defense in depth*)
  - pembatasan gerbang (*choke point*)
  - titik terlemah (*weakest link*)
  - pengamanan kegagalan (*fail-safe stance*)
  - partisipasi total (*universal participation*)
  - aneka pertahanan (*diversity of defense*)
  - kesederhanaan (*simplicity*)

6. Keamanan Pengoperasian (1)

- *Operations Security*
- Mempelajari:
  - teknik-teknik kontrol pada operasi personalia, sistem informasi dan perangkat keras.

6. Keamanan Pengoperasian (2)

- Cakupan
  - pemisahan tugas dan wewenang
  - alur pertanggung-jawaban (*accountability*)
  - perekrutan Sumber Daya Manusia
  - pengendalian keluaran/masukan
  - pengendalian pengelolaan perubahan
  - penyerangan (*attack*)
  - penyusupan (*intrusion*)
  - penanggulangan virus dan cacing

7. Keamanan Aplikasi dan Pengembangan Sistem (1)

- *Application & Systems Development Security*
- Mempelajari:
  - berbagai aspek keamanan serta kendali yang terkait pada pengembangan sistem informasi.

7. Keamanan Aplikasi dan Pengembangan Sistem (2)

- Cakupan:
  - Tingkatan Kerumitan Fungsi dan Aplikasi
  - Data
  - Pengelolaan Keamanan BasisData
  - SDLC: Systems Development Life Cycle
  - metodology pengembangan aplikasi
  - pengendalian perubahan perangkat lunak
  - program bermasalah

7. Keamanan Aplikasi dan Pengembangan Sistem (3)

- Ilustrasi Debian
  - Dari mana asal paket ".deb" anda?
  - Apakah tanda-tangan paket terdaftar di "key-ring"?
  - Apakah menggunakan paket dari sumber resmi?

8. Rencana Kesinambungan Usaha dan Pemulihan Bencana (1)

- *Disaster Recovery & Business Continuity Plan* -- DRP & BCP
- Mempelajari:
  - bagaimana aktifitas bisnis dapat tetap berjalan meskipun terjadi gangguan atau bencana.

8. Rencana Kesinambungan Usaha dan Pemulihan Bencana (2)

- Cakupan:
  - Indentifikasi Sumber Daya Bisnis
  - Penentuan Nilai Bisnis
  - Analisa Kegagalan (*impact*) Bisnis (BIA)
  - Analisa Kerugian
  - Pengelolaan Prioritas dan Krisis
  - Rencana Pengembangan
  - Rencana Implementasi
  - Rencana Pemeliharaan

8. Rencana Kesinambungan Usaha dan Pemulihan Bencana (3)

- Ilustrasi:
  - Apa yang akan dilakukan jika X tertabrak becak?
  - Apakah ada rencana jelas?
  - Apakah rencana tersebut tertulis.

9. Hukum, Investigasi, dan Etika (1)

- Mempelajari:
  - berbagai jenis aturan yang terkait dengan kejahatan komputer dan legalitas transaksi elektronik, serta membahas masalah etika dalam dunia komputer.

9. Hukum, Investigasi, dan Etika (2)

- Cakupan:
  - Hukum, Aturan, dan Etika
  - Transaksi Elektronis
  - Hak Kekayaan Intelektual
  - Pembajakan
  - Undang-undang keamanan dan eksport
  - Penyelidikan Kejahatan Komputer
  - Privasi

10. Keamanan Fisik (1)

- *Physical Security*
- Mempelajari:
  - berbagai ancaman, resiko dan kontrol untuk pengamanan fasilitas sistem informasi.

10. Keamanan Fisik (2)

- Cakupan:
  - Kawasan Terbatas
  - Kamera Pemantau dan Detektor Pergerakan
  - Bunker (dalam tanah)
  - Pencegahan dan Pemadaman Api
  - Pemagaran
  - Peralatan Keamaman
  - Alarm
  - Kunci Pintu

11. Audit (1)

- *Auditing*
- Memperkenalkan:
  - konsep dasar auditing sistem informasi terkait dengan masalah keamanan sistem informasi.

11. Audit (2)

- Cakupan:
  - Rencana Audit
  - Kendali
  - Tujuan Kendali
  - Metoda Audit
  - Testing
  - Pengumpulan Bukti
  - Teknik Audit Berbantuan Komputer

Ilustrasi Debian GNU/Linux (1)

- Berlangganan milis: “Debian Security Announce”, **`http://lists.debian.org/`**.
- UPDATE -- UPDATE -- UPDATE, **`http://security.debian.org/`**.
  - update aplikasi
  - update *library*
  - update kernel
  - update perangkat keras/BIOS
- Pencegahan Boot Yang Tidak Sah
  - set BIOS
  - set Loader (GRUB/LILO)

Ilustrasi: Debian GNU/Linux (2)

- Pemanfaatan PAM (Pluggable Authentication Modules).
- Pembatasan Jumlah Konsul *SuperUser*
- Pembatasan Hak Reboot Sistem
- Pembatasan Hak Pada Disk Yang Dimount
  - noexec
  - read-only
- Konfigurasi Pembatasan `/etc/security/limits.conf`
- Pemantauan “Kelakuan Para Pengguna”
  - set log terkait

Ilustrasi: Debian GNU/Linux (3)

- Pergantian PASSWORD yang teratur
- Logout user idle
- Pemantauan Berkala

Penutup

- Demikian serba-serbi dari ke-11 domain keamanan Sistem Informasi.
- Informasi Lanjut dapat dipelajari pada rujukan berikut ini.

Rujukan

- Ronald L. Krutz dan Russell D. Vines: The CISSP Prep Guide, Wiley Pub, 2003.
- Javier Fernández-Sanguino Peña: Securing Debian Manual, 2005, URL:

  `http:/www.debian.org/doc/manuals/`

Ucapan Terimakasih

- Versi awal dari bahan ini dibuat oleh Arrianto Mukti Wibowo dan Johny Moningka.

