Pengantar Open Source dan Aplikasi

Aspek Keamanan Open Source

Rusmanto at gmail.com

Rusmanto at nurulfikri.ac.id

Twitter @ruslinux

Topik

a) Isu-isu keamanan software Open Source dari sisi kode program dan *cracking*.

b) Keamanan dari gangguan virus, worm, dan sejenisnya.

c) Beberapa kesalahan orang dan cara atau prosedur yang baik untuk menjaga keamanan software atau sistem informasi.

Tujuan

a) Mampu menjelaskan isu-isu keamanan software Open Source dari sisi ketersediaan kode program.

b) Mampu menjelaskan software Open Source “relatif lebih aman” terhadap virus dan worm dibandingkan software proprietary.

c) Mampu menjelaskan prosedur yang baik dalam menjaga keamanan software/sistem.

Pendahuluan

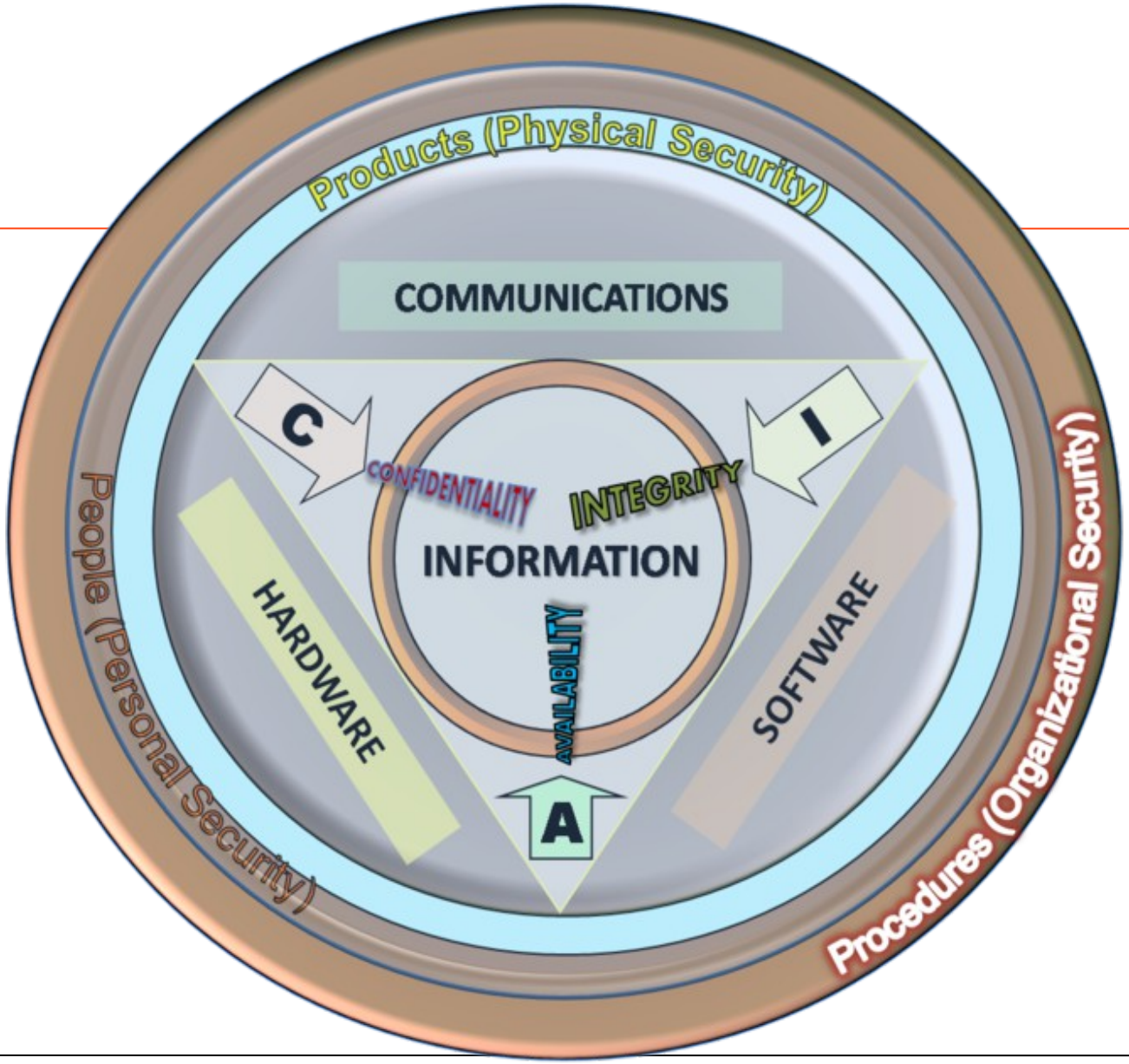
- Ketersediaan kode sumber *(source code)* tidak berarti membuat produk Open Source tidak aman, dan sebaliknya tidak berarti pasti aman.
- Ketersediaan kode sumber memungkinkan banyak orang dapat memperbaiki jika ditemukan kelemahan.
- Banyak faktor yang menentukan keamanan software, antara lain **produk** software itu sendiri, **orang** yang menggunakan dan merawat, dan **prosedur** keamanan yang seharusnya dijalankan.

Pengantar: Keamanan Komputer

- Keamanan komputer *(computer security)* disebut juga keamanan IT *(information technology security)* atau keamanan saiber *(cyber security)*, yakni penerapan keamanan informasi *(information security)* pada komputer dan jaringan komputer.
- Keamanan informasi penting untuk menjaga CIA: *confidentiality* (kerahasiaan dan privasi), *integrity* (keutuhan), dan *availability* (ketersediaan), serta *control* (pengendalian) dan *audit* (evaluasi).

Pengantar: 3 Jenis Keamanan Informasi

- *Physical Security* atau *Product*, yang mencakup teknologi hardware, software, dan komunikasi.
- *Personal Security* atau *People*, yang mencakup pengguna biasa (staf hingga pemimpin) dan bagian IT (system/network/database administrator, programmer, dll.)
- *Organizational Security* atau *Procedure*, yang mencakup panduan/pedoman/aturan untuk menjalankan sistem keamanan informasi.


Products (Physical Security)
COMMUNICATIONS
C
CONFIDENTIALITY
INTEGRITY
I
INFORMATION
AVAILABILITY
HARDWARE
SOFTWARE
A
People (Personal Security)
Procedures (Organizational Security)

Pengantar: Bentuk Gangguan Keamanan (1)

- **Program**: Virus, worm, dan lain-lain yang termasuk malware *(malicious software)* adalah program yang dibuat untuk mengganggu atau merusak. Program disebut virus atau worm karena bisa menular atau menyebar dari satu komputer ke komputer lain.
- **Penyerang**: *Attacker* atau *cracker* (hacker jahat), yakni orang yang mencari kelemahan suatu sistem IT atau komputer, lalu memanfaatkan kelemahan itu untuk menyerang atau merusak.

Pengantar: Bentuk Gangguan Keamanan (2)

- **Defacing** (pengrusakan tampilan), karena penyerang tahu ada kelemahan yang belum diperbaiki/ditutup.
- **Planting malware** (pemasangan program jahat atau berbahaya, malicious software) atau Trojan.
- **Phishing** (penipuan), berasal dari kata *fishing* (memancing), yakni cara untuk mendapatkan nama dan password, misal untuk akses ke suatu program, kartu kredit, dan lain-lain yang dapat merugikan pengguna (yang terpancing) atau sistem.

Pengantar: Bentuk Gangguan Keamanan (3)

- **Exploit**: program yang khusus dibuat untuk menyerang keamanan komputer tertentu.
- **Brute Force** (serangan brutal): salah satu metode dalam penjebolan keamanan password dengan menebak semua password yang mungkin.
- **Password Cracking**: teknik untuk Brute Force.
- **DoS (Denial of Service)**: mengirim data yang sangat besar ke komputer atau jaringan agar komputer tidak bekerja normal (tidak dapat diakses).

Mengapa Open Source Relatif Lebih Aman?

- Dalam kasus virus/worm, sistem operasi Open Source seperti Linux relatif lebih aman karena sistem otentikasi yang lebih ketat dan sebagian besar virus/worm dibuat untuk selain Linux.
- Ketersediaan kode sumber memungkinkan banyak orang membuat perbaikan *(patch)* jika ditemukan kelemahan, sehingga ketersediaan update bisa lebih cepat. Sedangkan produk proprietary hanya dapat diperbaiki oleh pengembang atau pemilik program.

Beberapa Koreksi terhadap Mitos (123)

Mitos 1: Open Source PASTI aman atau PASTI TIDAK aman. Koreksi: Keamanan tidak hanya ditentukan ada atau tidaknya kode sumber.

Mitos 2: Ada kode sumber PASTI banyak penjaga. Koreksi: belum tentu banyak yang mengaudit.

Mitos 3: Orang jahat bisa melihat kode sumber PASTI menjadikan software tidak aman. Koreksi: keamanan ditentukan oleh siapa yang menggunakan dan menjaga keamanannya.

Beberapa Koreksi terhadap Mitos (456)

Mitos 4: Siapa pun boleh tahu kode sumber PASTI membuat tidak aman. Koreksi: Produk bagus telah melalui seleksi siapa saja pengembang yang terlibat.

Mitos 5: Produk yang dinyatakan “Open Source” pasti dapat dimodifikasi agar jadi aman. Koreksi: ada produk “Open Source” yang mengandung paten.

Mitos 6: Semua software pasti telah melalaui proses audit/evaluasi keamanan sebelum digunakan. Koreksi: tidak semua software harus diaudit/dievaluasi.

Beberapa Kesalahan terkait Keamanan (1)

- Tidak memasang antivirus, misal di server yang dijadikan perantara pertukaran data (server email, server file, dan gateway internet).
- Membuka attachment email yang tidak dikenal, atau mengikuti petunjuk email penipuan *(phising)*.
- Tidak mengikuti berita keamanan produk.
- Tidak segera melakukan *security patch*.
- Tidak membuat dan menguji sistem backup.

Beberapa Kesalahan terkait Keamanan (2)

- Menyambungkan sistem ke internet sebelum sistem itu dibuat sangat aman *(hardening)*.
- Menyambungkan sistem ke internet dengan password bawaan atau password mudah ditebak.
- Menjalankan program server (daemon) yang tidak aman seperti *telnetd* (harusnya sshd yang menggunakan enkripsi password).
- Menjalankan program yang tidak dibutuhkan sehingga membuka celah keamanan lebih banyak.

Beberapa Kesalahan terkait Keamanan (3)

- Tidak segera mengupdate program atau sistem jika ditemukan lubang keamanan *(security hole)* atau kelemahan/kutu *(bug)*.
- Tidak menerapkan sistem *firewall* yang bagus untuk mencegah masuknya orang atau program jahat. Firewall = dinding api untuk membakar penjahat.
- Tidak menerapkan sistem pendeteksian intrusi atau usaha pihak lain yang ingin masuk ke jaringan atau komputer.

Beberapa Kesalahan terkait Keamanan (4)

- Tidak melakukan update virus pada program antivirus secara otomatis.
- Tidak membuat panduan yang baik untuk diajarkan kepada pengguna dalam hal keamanan sistem yang dibuat atau dikelolanya.
- Memberikan password kepada pengguna melalui telepon atau saluran komunikasi yang kurang aman.

Penutup

- Ketersediaan kode sumber *(source code)* tidak berarti membuat produk Open Source tidak aman, dan sebaliknya kode tertutup tidak menjamin produk Proprietary pasti aman, karena keamanan ditentukan oleh pengguna dan penjaga keamanan.
- Ketersediaan kode sumber memungkinkan banyak orang dapat mempelajari dan memperbaiki jika ditemukan kelemahan, namun tidak bisa dipastikan ada orang yang selalu mengaudit dan membuat perbaikan, sehingga pengguna harus tetap waspada.