# Konsep Keamanan Jaringan dan Kejahatan Internet

# Sekilas Tentang Jaringan Komputer

# Jaringan komputer

- Adalah sekelompok komputer otonom yang saling berhubungan antara yang satu dengan lainnya,
- Menggunakan suatu protokol komunikasi melalui media komunikasi sehingga dapat saling berbagi dan bertukar informasi

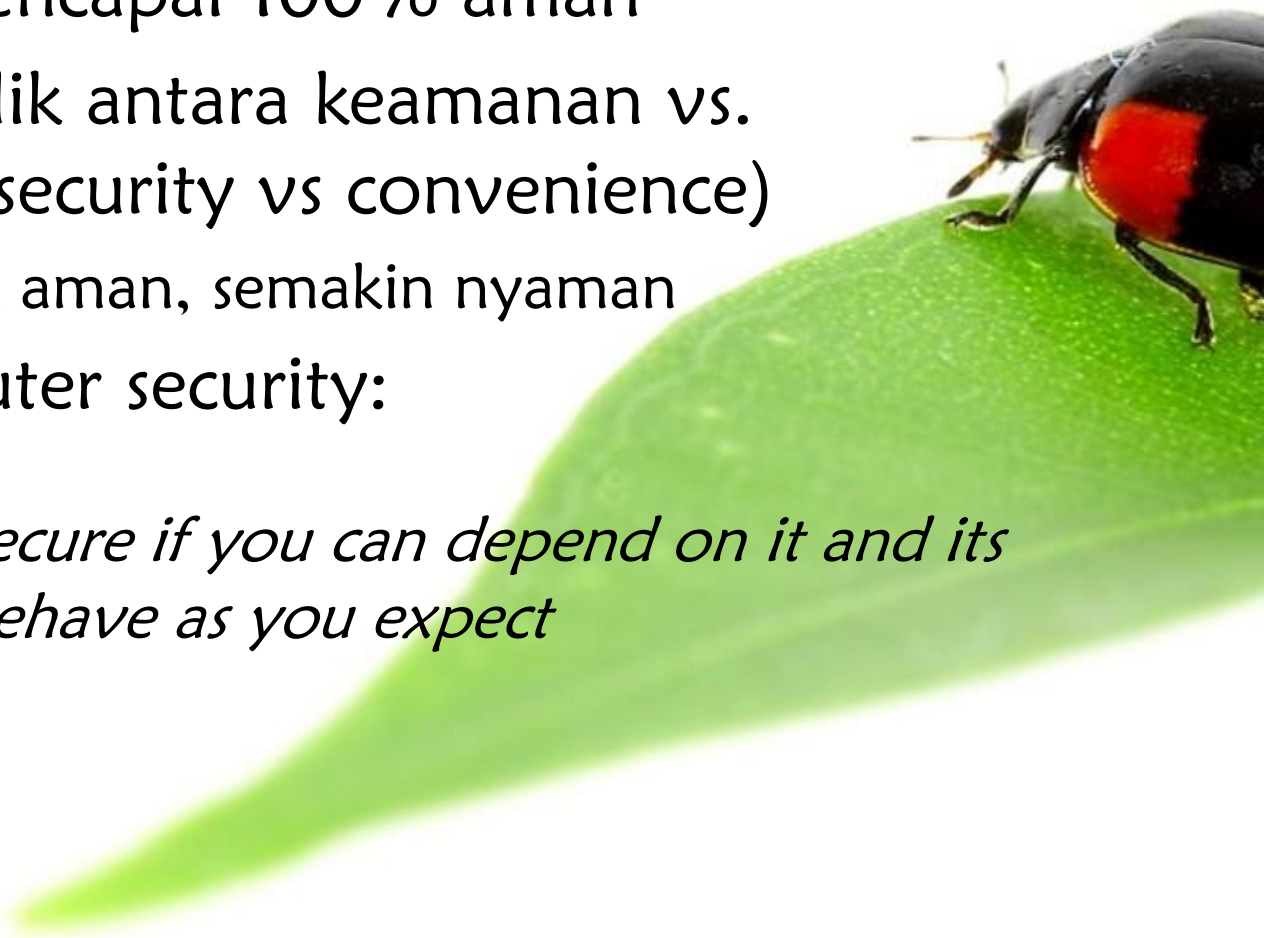
# Manfaat Jaringan Komputer

- Berbagi sumber daya (*sharing resources*)
- Media komunikasi
- Integrasi data
- Pengembangan dan pemeliharaan
- Keamanan data
- Sumber daya lebih efisien dan informasi terkini.

# Mungkinkah aman?

- Sangat sulit mencapai 100% aman
- Ada timbal balik antara keamanan vs. kenyamanan (security vs convenience)
  - Semakin tidak aman, semakin nyaman
- Definisi computer security:
  (Garfinkel & Spafford)

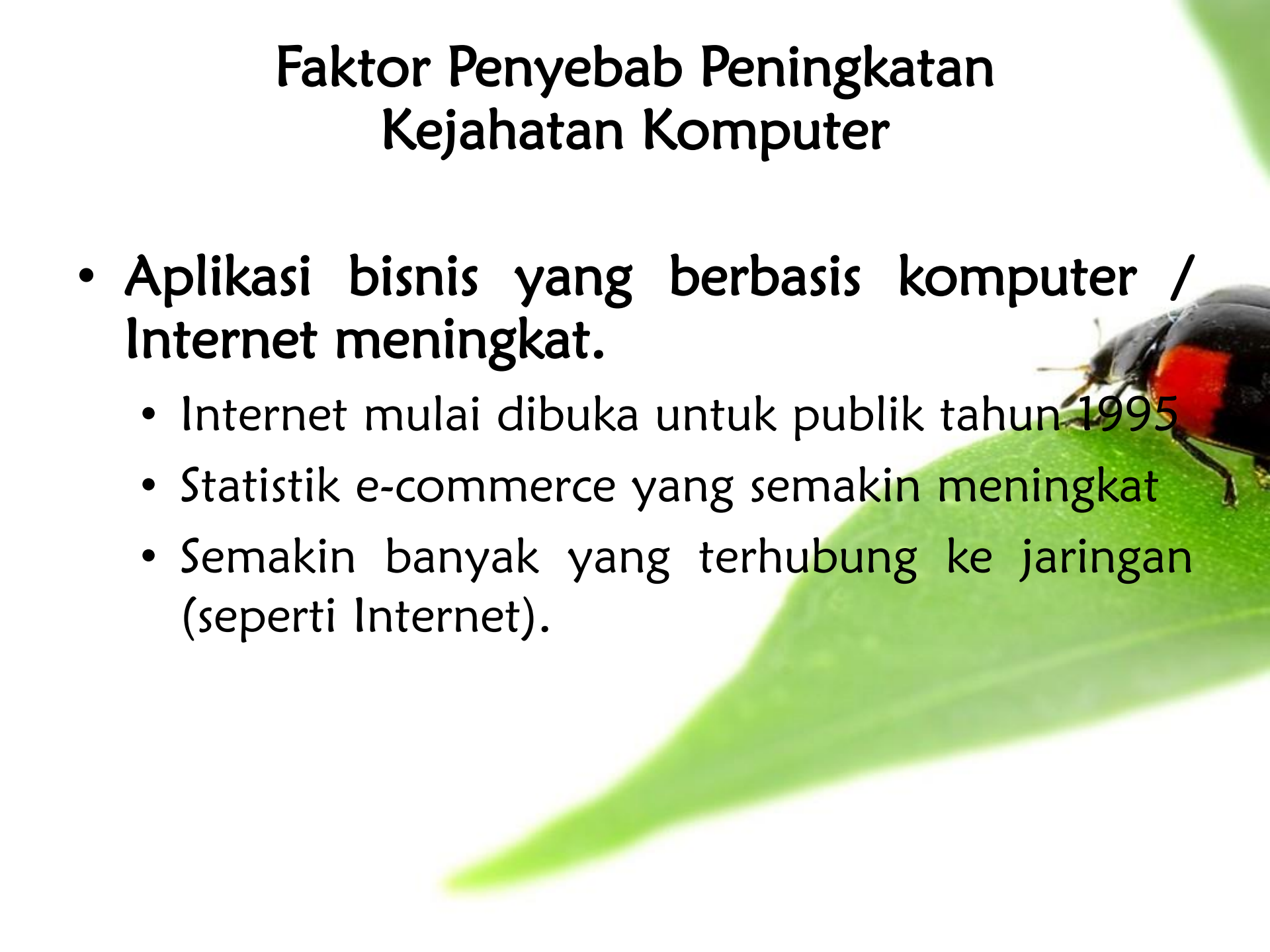
  *A computer is secure if you can depend on it and its software to behave as you expect*



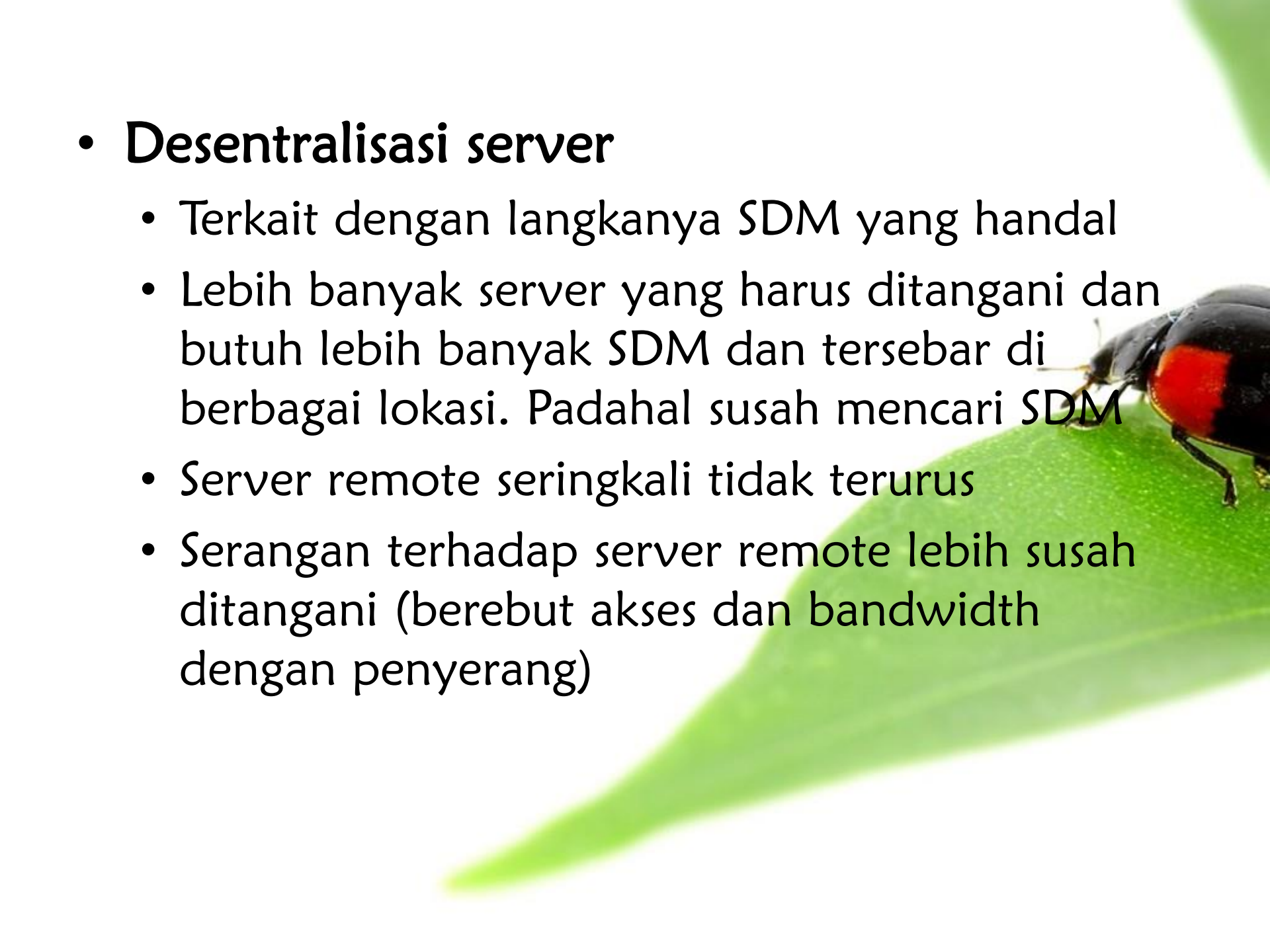
# Kejahatan Internet

# Faktor Penyebab Peningkatan Kejahatan Komputer

- **Aplikasi bisnis yang berbasis komputer / Internet meningkat.**
  - Internet mulai dibuka untuk publik tahun 1995
  - Statistik e-commerce yang semakin meningkat
  - Semakin banyak yang terhubung ke jaringan (seperti Internet).

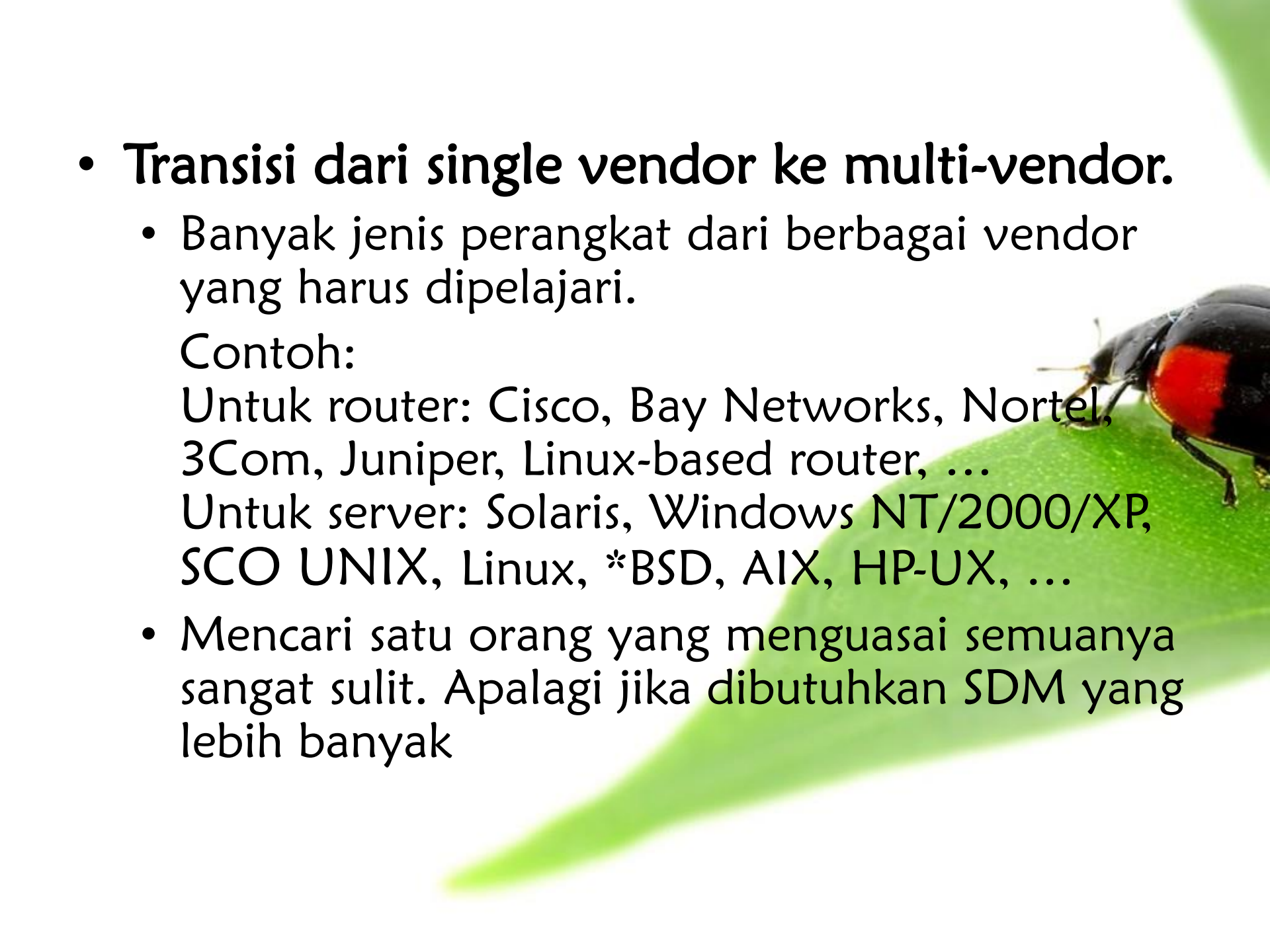


- **Desentralisasi server**
  - Terkait dengan langkanya SDM yang handal
  - Lebih banyak server yang harus ditangani dan butuh lebih banyak SDM dan tersebar di berbagai lokasi. Padahal susah mencari SDM
  - Server remote seringkali tidak terurus
  - Serangan terhadap server remote lebih susah ditangani (berebut akses dan bandwidth dengan penyerang)



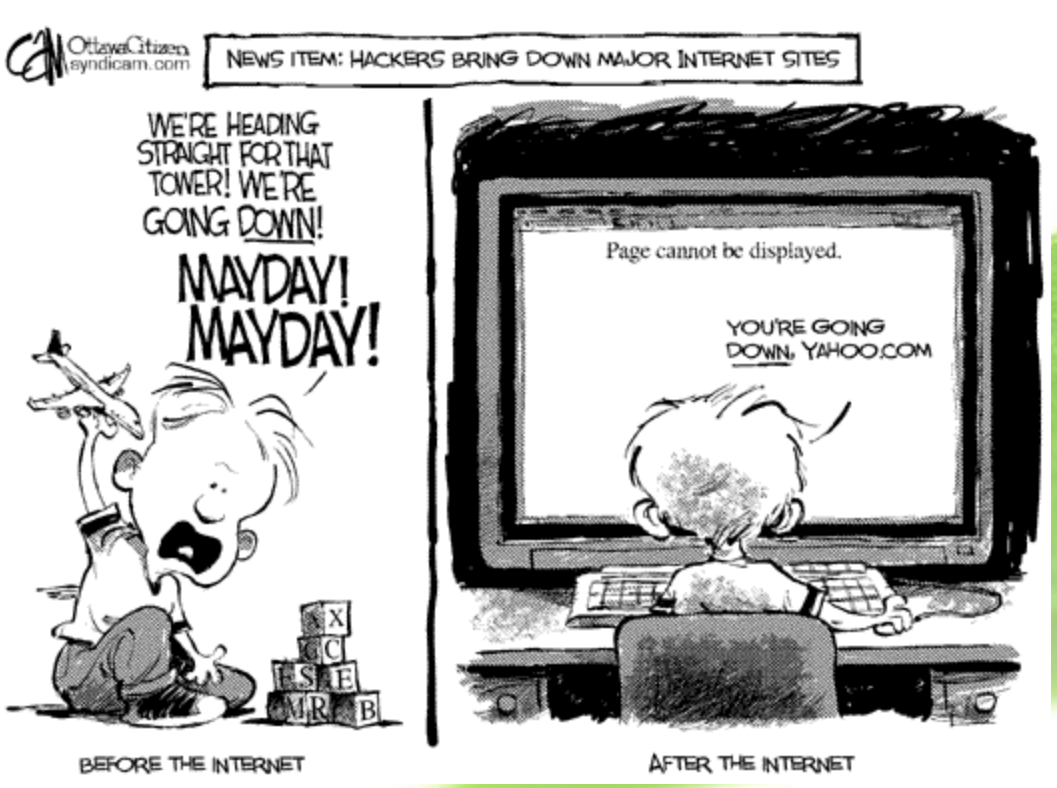
- **Transisi dari single vendor ke multi-vendor.**
  - Banyak jenis perangkat dari berbagai vendor yang harus dipelajari.

    Contoh:
    Untuk router: Cisco, Bay Networks, Nortel, 3Com, Juniper, Linux-based router, …
    Untuk server: Solaris, Windows NT/2000/XP, SCO UNIX, Linux, *BSD, AIX, HP-UX, …
  - Mencari satu orang yang menguasai semuanya sangat sulit. Apalagi jika dibutuhkan SDM yang lebih banyak



- **Pemakai makin melek teknologi dan kemudahan mendapatkan software.**
  - Ada kesempatan untuk menjajal. Tinggal download software dari Internet. *(Script kiddies)*
  - Sistem administrator harus selangkah di depan.

# Hacker kecil (1)




# Hacker kecil (2)


- **Kesulitan penegak hukum untuk mengejar kemajuan dunia telekomunikasi dan komputer**
  - Cyberlaw belum matang
  - Tingkat *awareness* masih rendah
  - *Technical capability* masih rendah

- **Meningkatnya kompleksitas sistem**

# Aspek / Pilar Keamanan

- Privacy / confidentiality
- Integrity
- Authenticity
- Availability
- Non-repudiation
- Access control

# Privacy / confidentiality

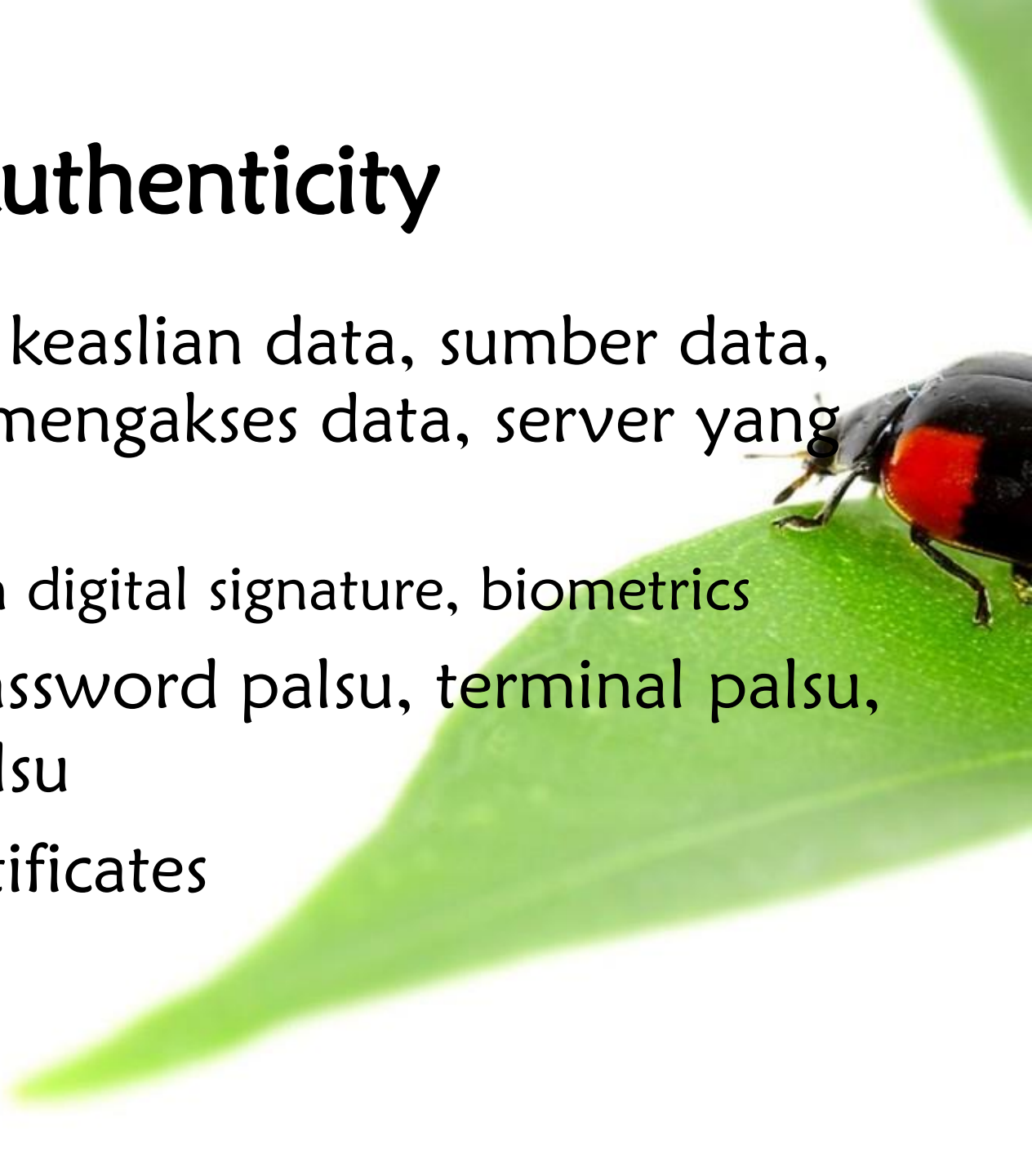
- Proteksi data [hak pribadi] yang sensitif
  - Nama, tempat tanggal lahir, agama, hobby penyakit yang pernah diderita, status perkawinan
  - Data pelanggan
  - Sangat sensitif dalam e-commerce, *healthcare*
- Serangan: sniffer
- Proteksi: enkripsi

# Integrity

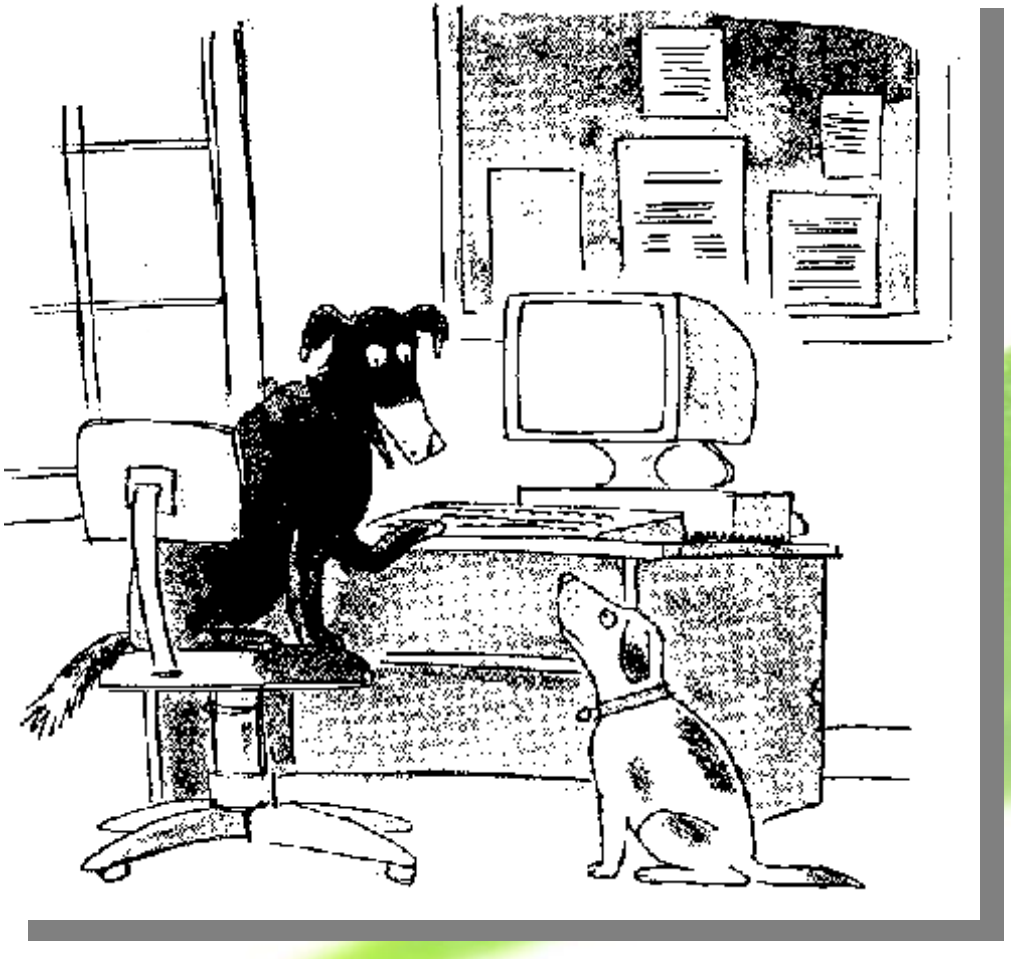
- Informasi tidak berubah tanpa ijin (tampered, altered, modified)
- Serangan: spoof, virus, trojan horse, man in the middle attack
- Proteksi: signature, certificate, hash

# Authenticity

- Meyakinkan keaslian data, sumber data, orang yang mengakses data, server yang digunakan
  - penggunaan digital signature, biometrics
- Serangan: password palsu, terminal palsu, situs web palsu
- Proteksi: certificates

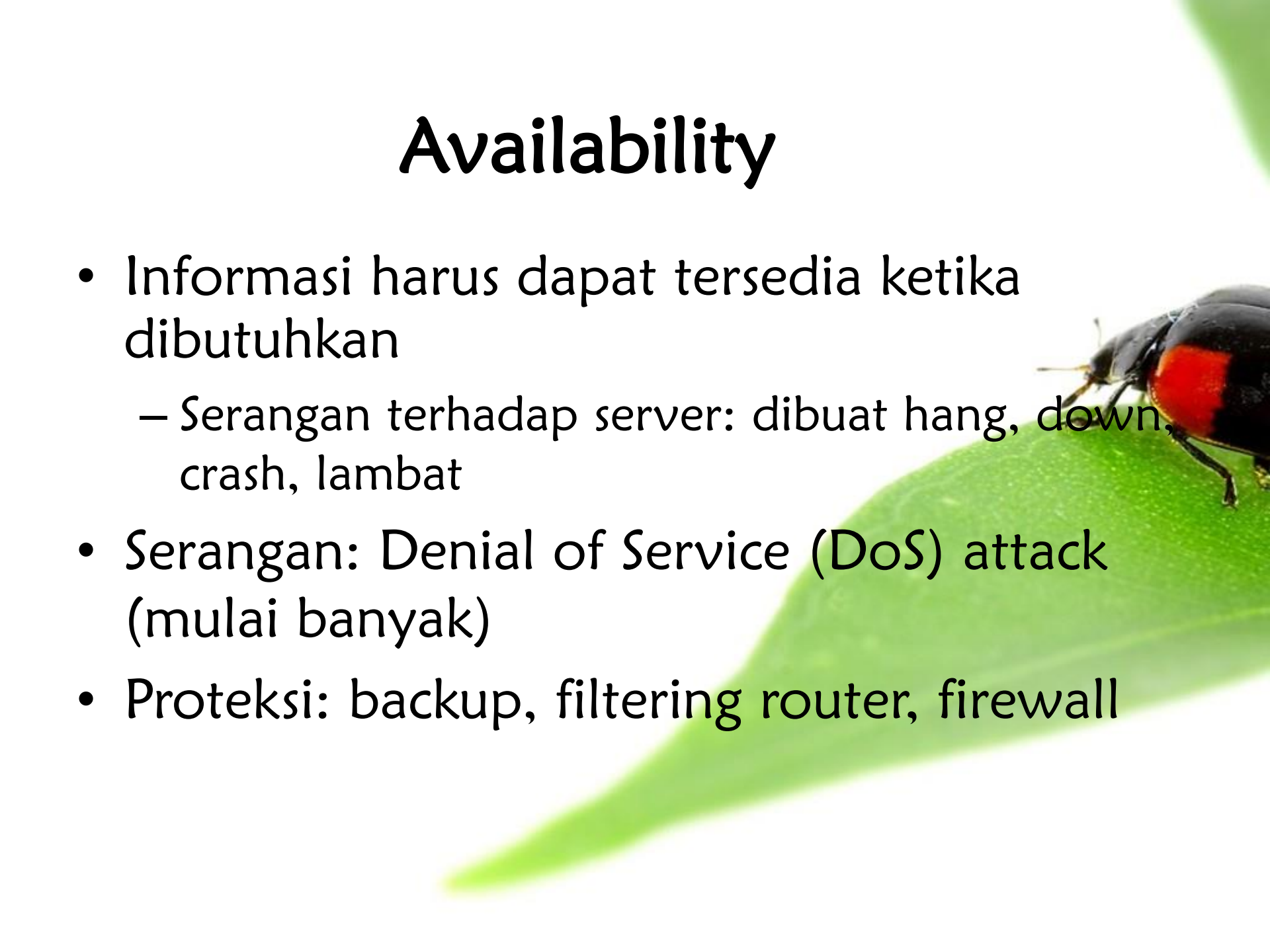


# On the Internet nobody knows you're a dog



# Availability

- Informasi harus dapat tersedia ketika dibutuhkan
  - Serangan terhadap server: dibuat hang, down, crash, lambat
- Serangan: Denial of Service (DoS) attack (mulai banyak)
- Proteksi: backup, filtering router, firewall



# Non-repudiation

- Tidak dapat menyangkal (telah melakukan transaksi)
  - menggunakan digital signature / certificates
  - perlu pengaturan masalah hukum (bahwa digital signature sama seperti tanda tangan konvensional)

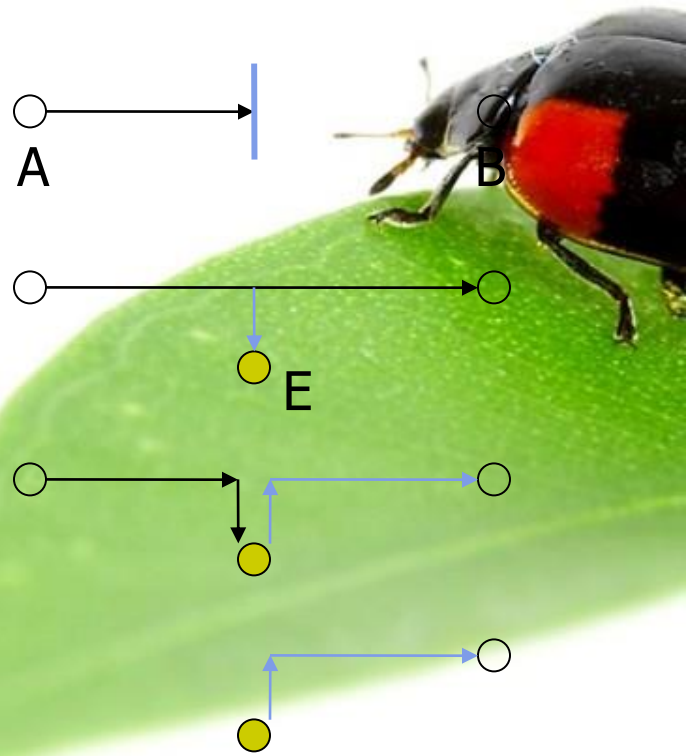
# Access Control

- Mekanisme untuk mengatur siapa boleh melakukan apa
  - biasanya menggunakan password, token
  - adanya kelas / klasifikasi pengguna dan data

# Jenis Serangan (attack)

- Menurut W. Stallings

- Interruption(gangguan)
  DoS attack, network flooding
- Interception(penahanan)
  Password sniffing
- Modification(perubahan)
  Virus, trojan horse
- Fabrication(pemalsuan)
  spoffed packets

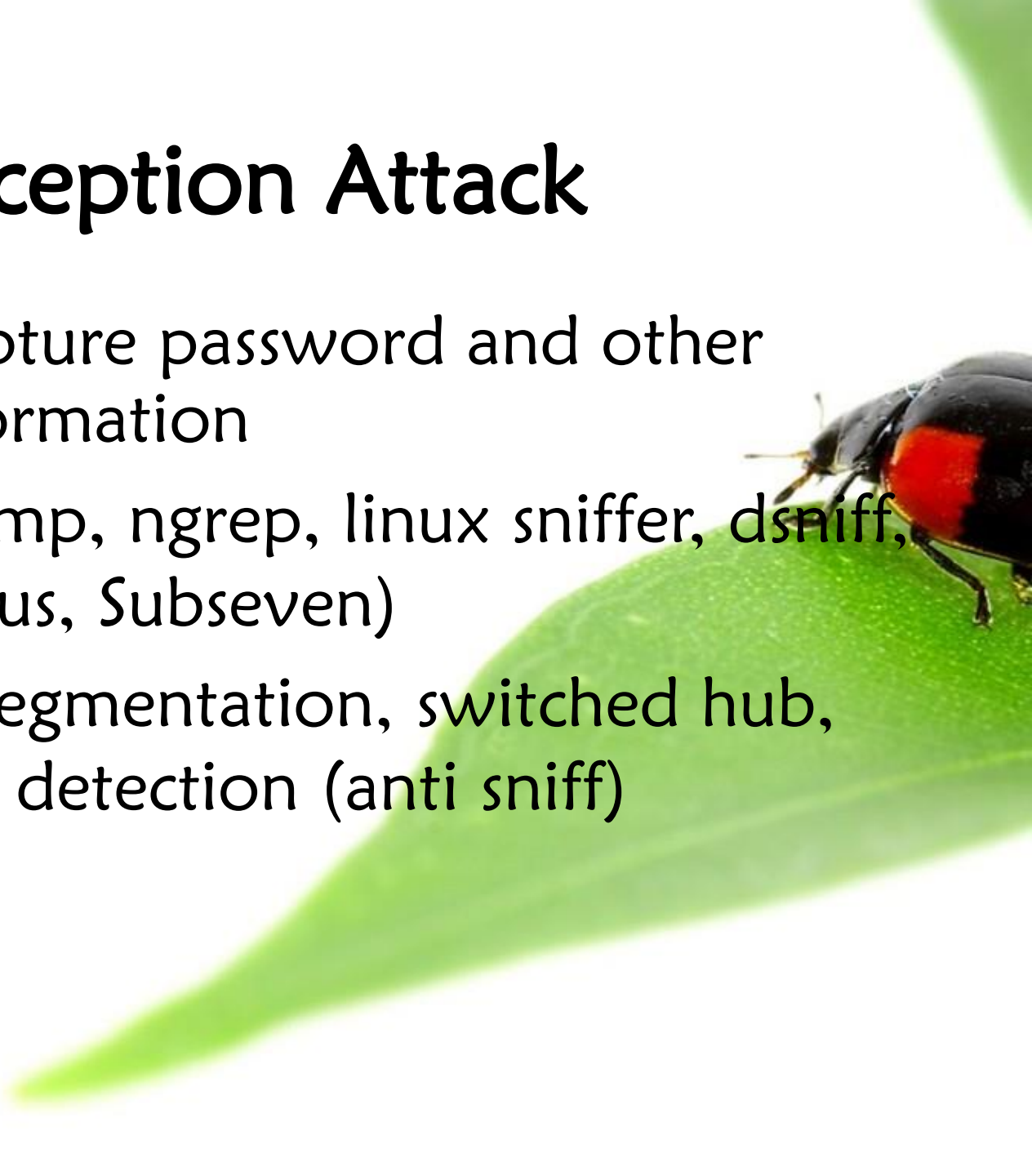


# Interruption Attack

- Denial of Service (DoS) attack
  - Menghabiskan bandwith, network flooding
  - Memungkinkan untuk spoofed originating address
  - Tools: ping broadcast, smurf, synk4, macof, various flood utilities
- Proteksi:
  - Sukar jika kita sudah diserang
  - Filter at router for outgoing packet, filter attack orginiating from our site

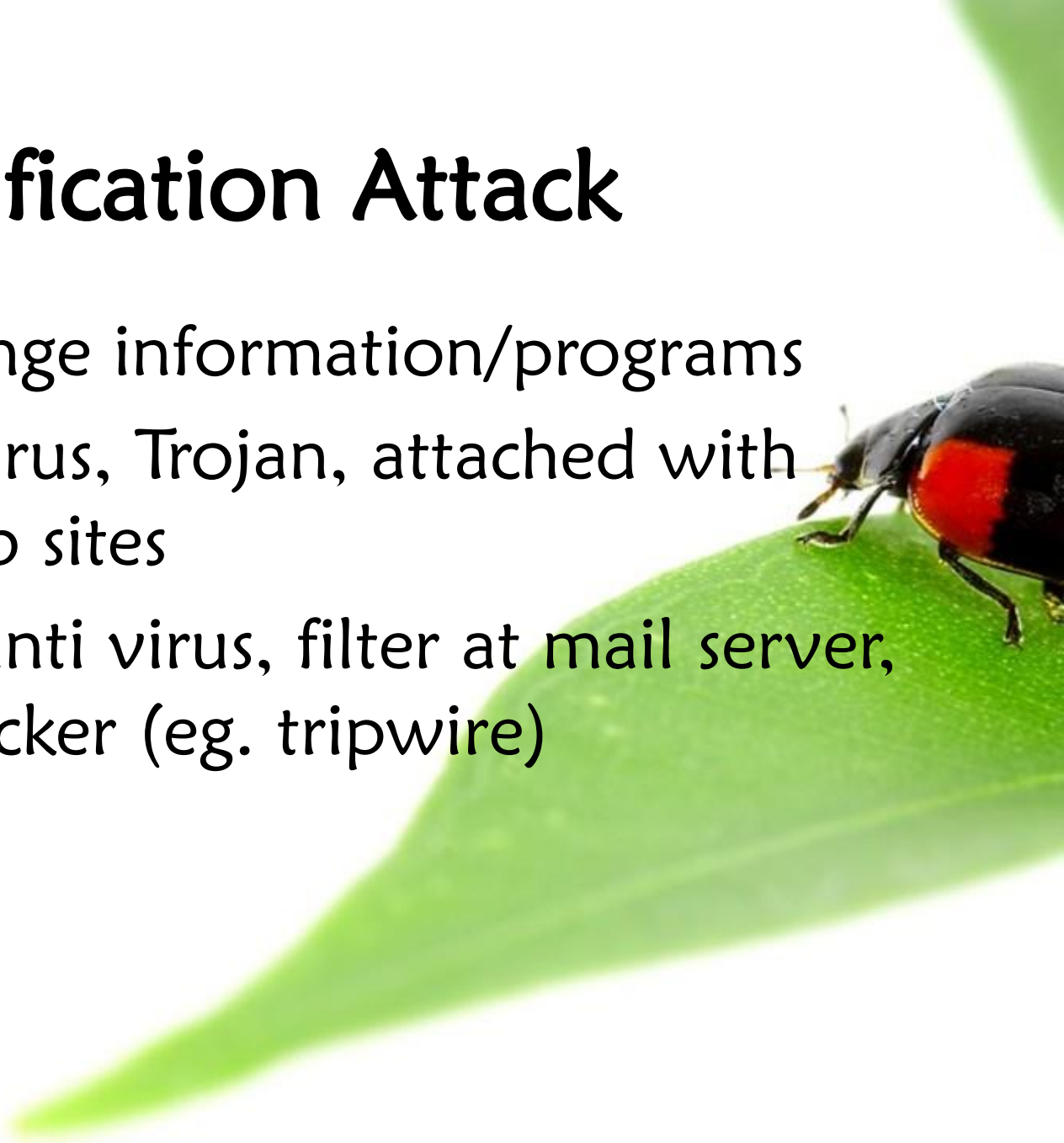
# Interception Attack

- Sniffer to capture password and other sensitive information
- Tools: tcpdump, ngrep, linux sniffer, dsniff, trojan (Netbus, Subseven)
- Protection: segmentation, switched hub, promiscuous detection (anti sniff)



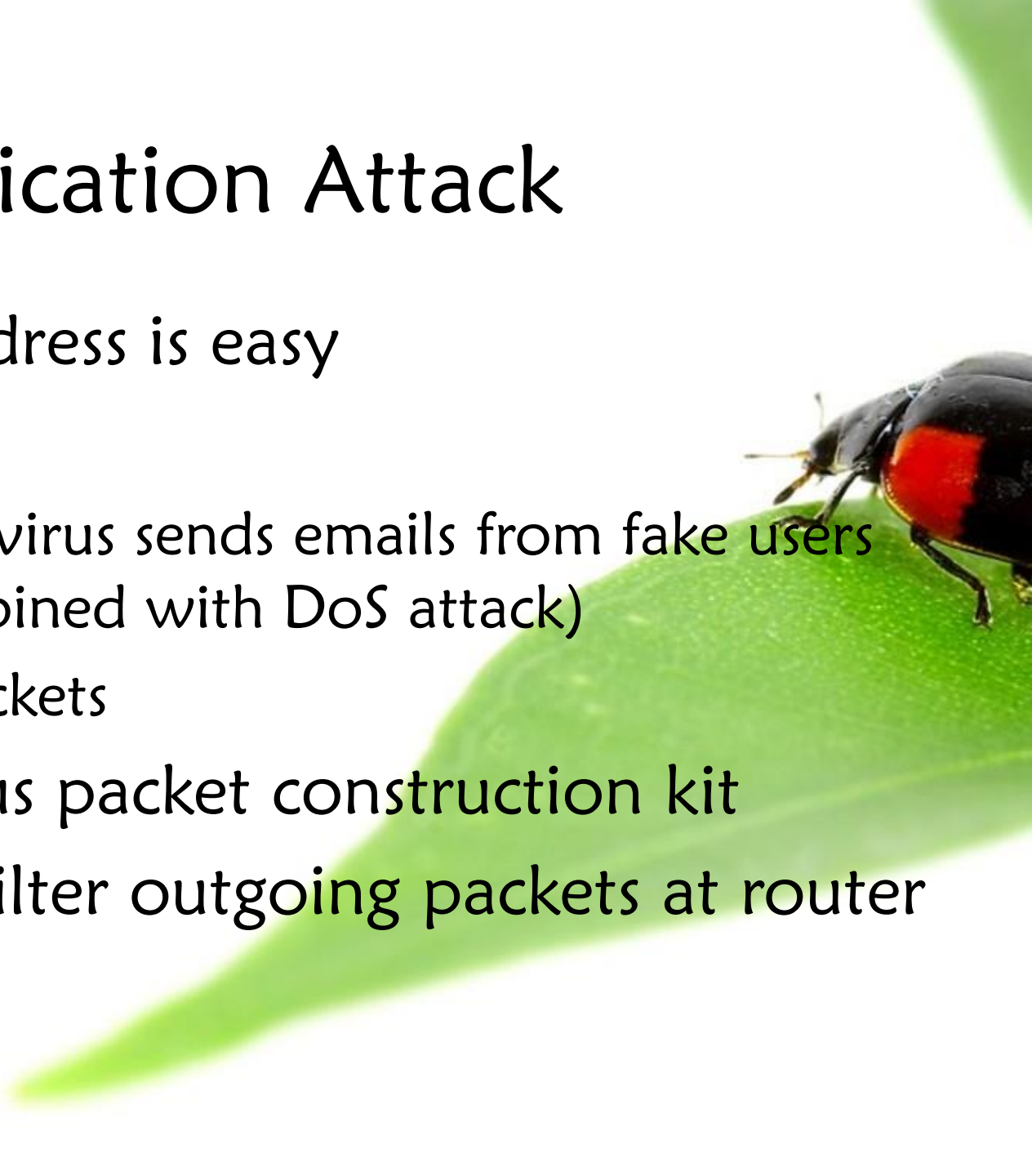
# Modification Attack

- Modify, change information/programs
- Examples: Virus, Trojan, attached with email or web sites
- Protection: anti virus, filter at mail server, integrity checker (eg. tripwire)



# Fabrication Attack

- Spoofing address is easy
- Examples:
  - Fake mails: virus sends emails from fake users (often combined with DoS attack)
  - spoofed packets
- Tools: various packet construction kit
- Protection: filter outgoing packets at router

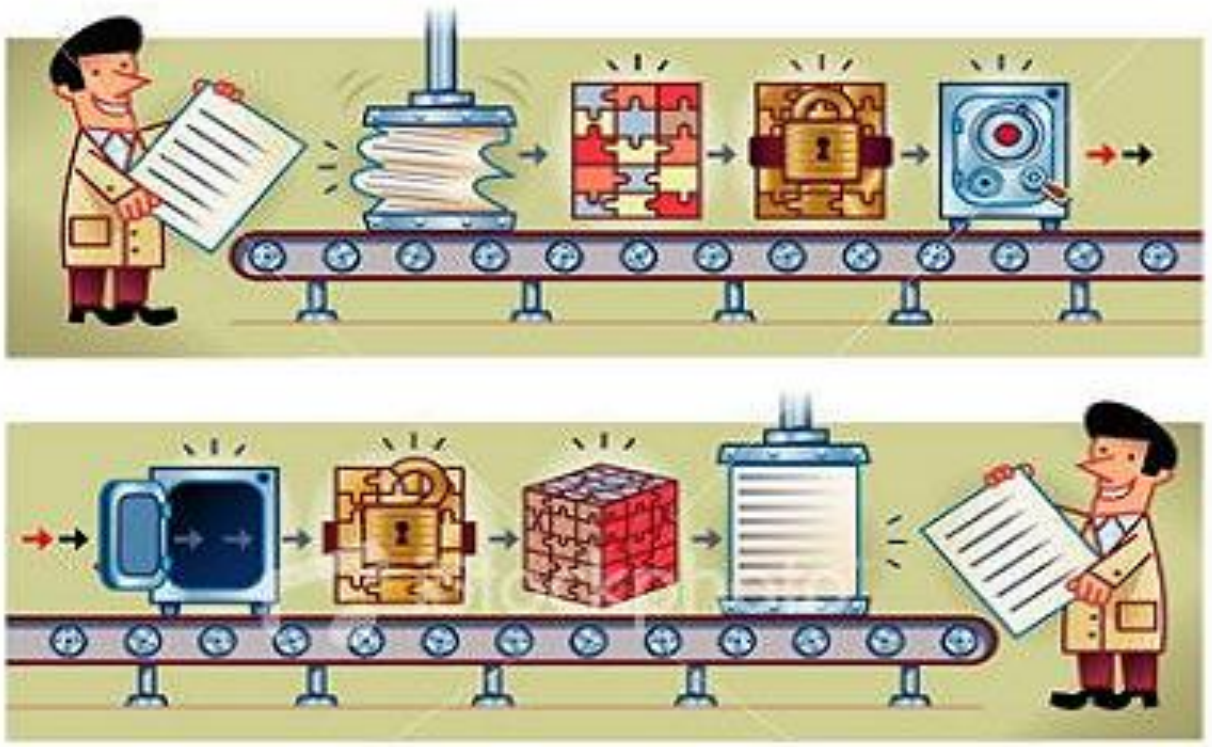


# Teknologi Kriptografi

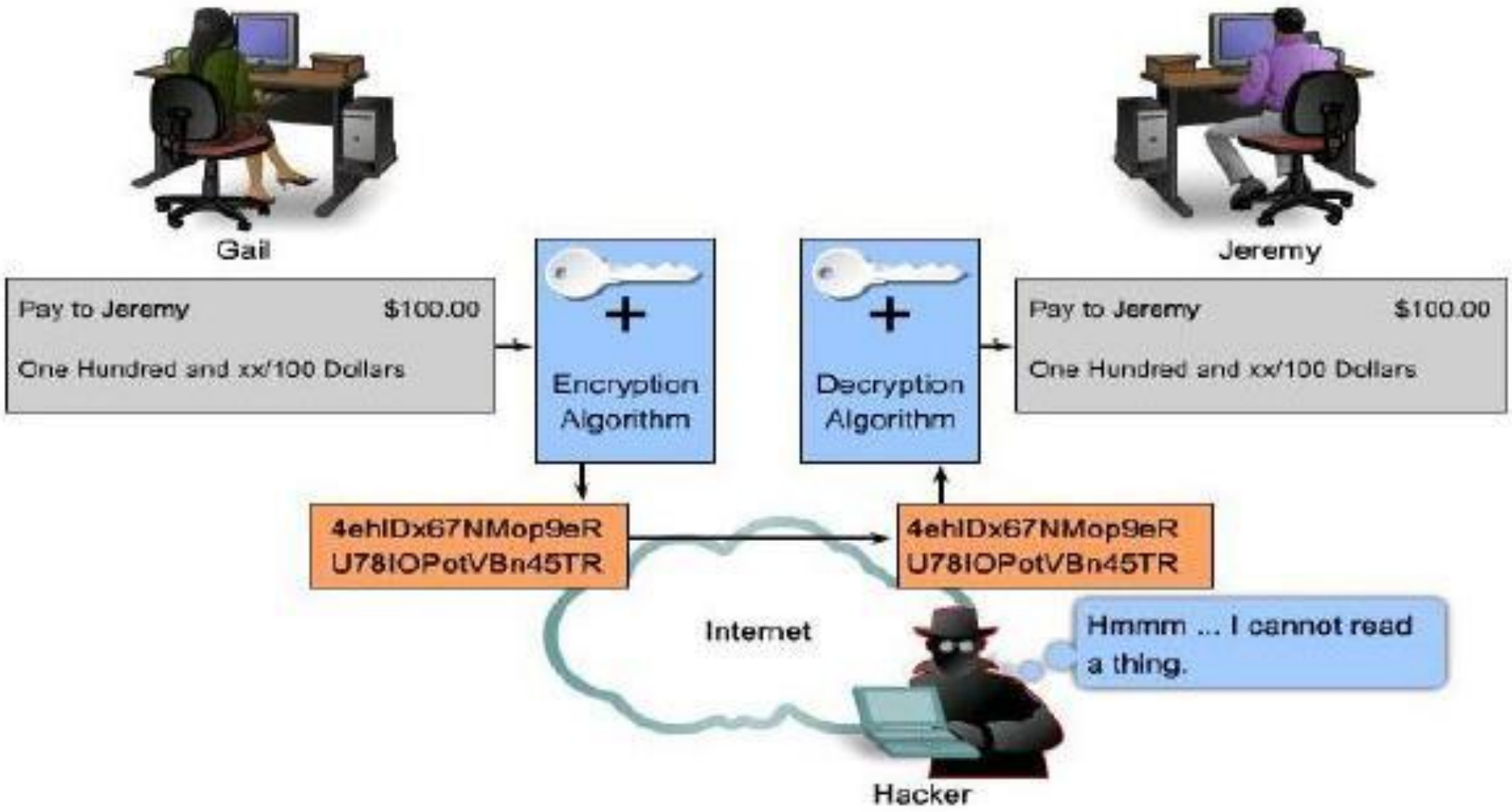
- Penggunaan enkripsi (kriptografi) untuk meningkatkan keamanan
- Private key vs public key
- Contoh: DES, IDEA, RSA, ECC

# Ekripsi vs Dekripsi

- **Enkripsi** berarti mengkodekan data ke format tertentu menggunakan kunci rahasia
- **Dekripsi** mendekodekan data yang terenkripsi ke format asli



# Fungsi Enkripsi dalam menjamin kerahasiaan data



# Terima kasih