Keamanan Sistem Komputer

Latar Belakang

- Kondisi trafik 1960an :
  - Mayoritas voice (>95%)
  - Data umumnya berisi trafik teleks, belum ada konsep pertukaran file antara komputer, pertukaran file dilakukan dengan cara transmisi

- Advance Research Pro Agency (ARPA) – Lembaga riset Dept. of Defense (DoD) (1969) membiayai projek ARPANet bekerja sama dengan universitas-universitas terkemuka di Amerika seperti Stanford University

- ARPA ← Penemu LAN pertama kali

- ARPANet ← penukaran data menggunakan paket switching, yang berhasil beroperasi di dunia. Bukan yang pertama

Latar Belakang

- Konsep perancangan jaringan data ARPA : Sesederhana mungkin, Handal (paket pasti di**terima** dengan **benar**)
- Pengguna ARPANet : Pemerintahan, akademisi, & militer
- Dikembangkan konsep RFC (Req. for Comment) dimana pengguna berhak mengusulkan perubahan yang dianggap perlu dan akan ditanggapi oleh pengguna lain dan tim pengembang

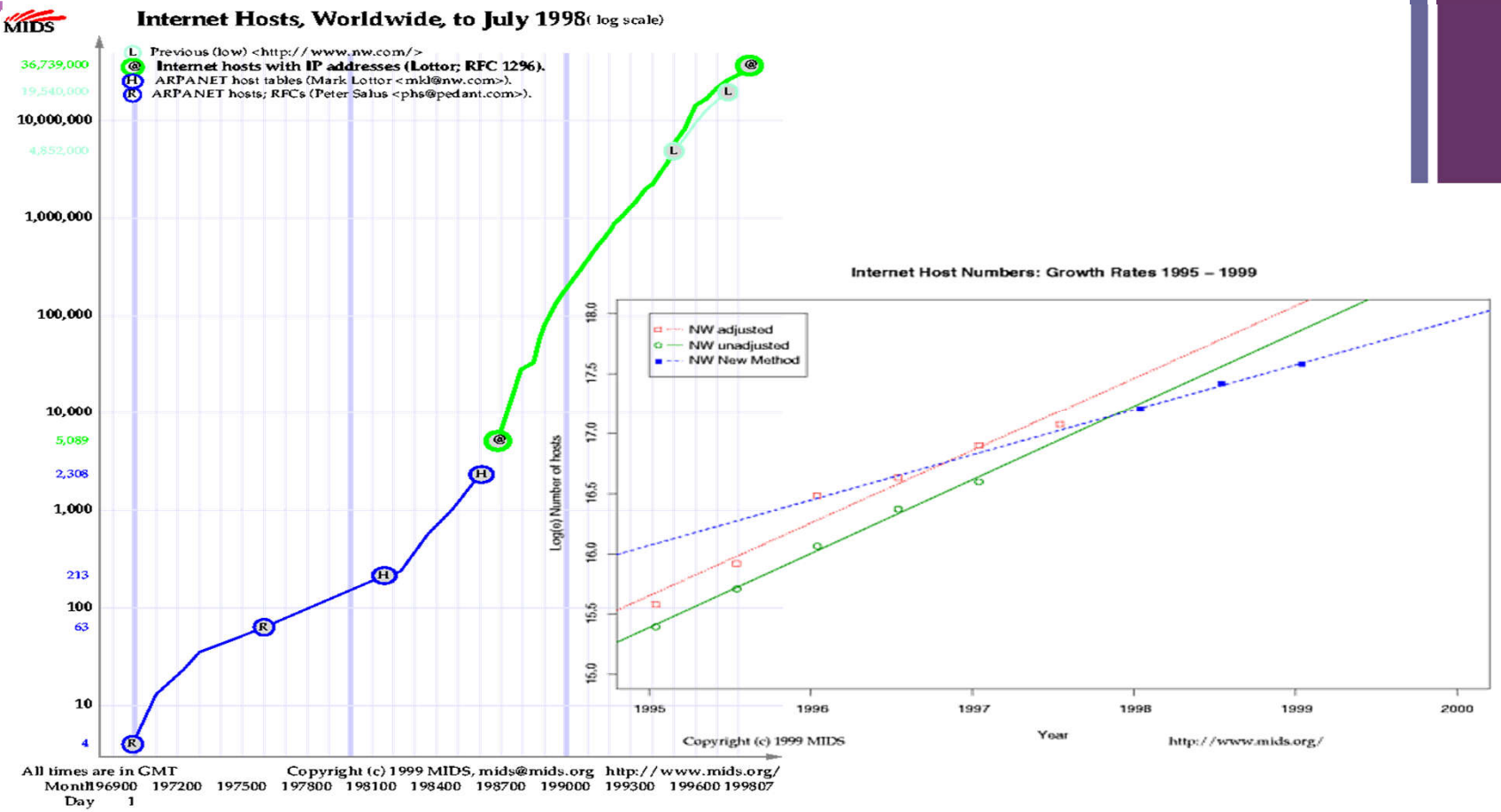
Evolusi Internet

- 1969 : ARPANet
- 1980s : NSFnet (US), CA*net (Canada)
- 1991 : HTML (CERN) → WWW
- 1993 : Mosaic → Netscape

Akademia → Bisnis → Publik

Pertumbuhan Internet

- Eksponensial
- *"**Internet is changing all the time**. Two things, in our opinion, have marked it's evolution recently: **the social web and mobile technology**. These two innovations have changed the way people use the Internet. People have found in the social web a new way to communicate: **since** it's creation in **2004** Facebook has grown into a worldwide web of **nearly 900 million subscribers**. **Mobile technology**, on the other hand, has made possible a much greater reach of the Internet, **increasing the number of Internet users everywhere**."*
  http://www.internetworldstats.com/emarketing.htm


Internet Hosts, Worldwide, to July 1998 (log scale)
MIDS
L Previous (low) <http://www.nw.com/>
@ Internet hosts with IP addresses (Lottor; RFC 1296).
H ARPANET host tables (Mark Lottor <mkl@nw.com>).
R ARPANET hosts; RFCs (Peter Salus <phs@pedant.com>).
36,739,000
19,540,000
10,000,000
4,852,000
1,000,000
100,000
10,000
5,089
2,308
1,000
213
100
63
10
4
All times are in GMT
Copyright (c) 1999 MIDS, mids@mids.org http://www.mids.org/
Month 196900 197200 197500 197800 198100 198400 198700 199000 199300 199600 199807
Day 1
Internet Host Numbers: Growth Rates 1995 – 1999
NW adjusted
NW unadjusted
NW New Method
Log(e) Number of hosts
18.0
17.5
17.0
16.5
16.0
15.5
15.0
1995
1996
1997
1998
1999
2000
Year
Copyright (c) 1999 MIDS
http://www.mids.org/

Pertumbuhan Internet

- Internet secara rancangan dasar tidak bisa mengatasi masalah – masalah yang timbul kemudian, karena
  - Kesederhanaannya, yang hanya berfokus pada kemampuan menyampaikan data dengan "benar"
  - Tidak disiapkan untuk menghadapi kemajuan disisi perangkat lunak yang bisa 'memanipulasi' kelemahan protokol internet
- Terjadi serangan ke internet yang semakin hari semakin banyak, dan merusak.

Ancaman (Threat)

- *Ancaman keamanan* adalah kemungkinan kebijakan keamanan bisa dibobol (misal hilangnya keutuhan atau kerahasiaan).
- *Layanan keamanan* adalah cara mengatasi ancaman (misal perlengkapan kerahasiaan).
- Mekanisme keamanan adalah alat untuk menyediakan layanan (misal enkripsi, tanda tangan digital)

Ancaman (Threat)

- Sebuah *ancaman*:
  - seseorang, sesuatu, kejadian atau ide yang berpotensi membahayakan suatu aset (dalam bentuk kerahasiaan, keutuhan, ketersediaan atau penggunaan yang sah).
- Serbuah *serangan* adalah realisasi dari ancaman.
- *Perlindungan* = cara (misal kendali, prosedur) untuk perlidungan atas ancaman.
- *Titik Lemah* = kelemahan pada perlidungan.

Ancaman Dasar

- Empat ancaman dasar (Kerahasiaan / Confidentiality, Keutuhan / Integrity, Ketersediaan / Availability (CIA) + penggunaan sah)
  - Kebocoran informasi,
  - Gangguan keutuhan,
  - Penolakan layanan (DoS),
  - Penggunaan tidak sah

Ancaman Primer

- Realisasi dari ancaman - ancaman ini dapat langsung menuju ke realisasi ancaman dasar :
  - Penyamaran (Masquerade)
  - Pemotongan kendali
  - Pelanggaran autorisasi
  - Kuda Troya
  - Jebakan

Jim Geovedi (satelit hack)

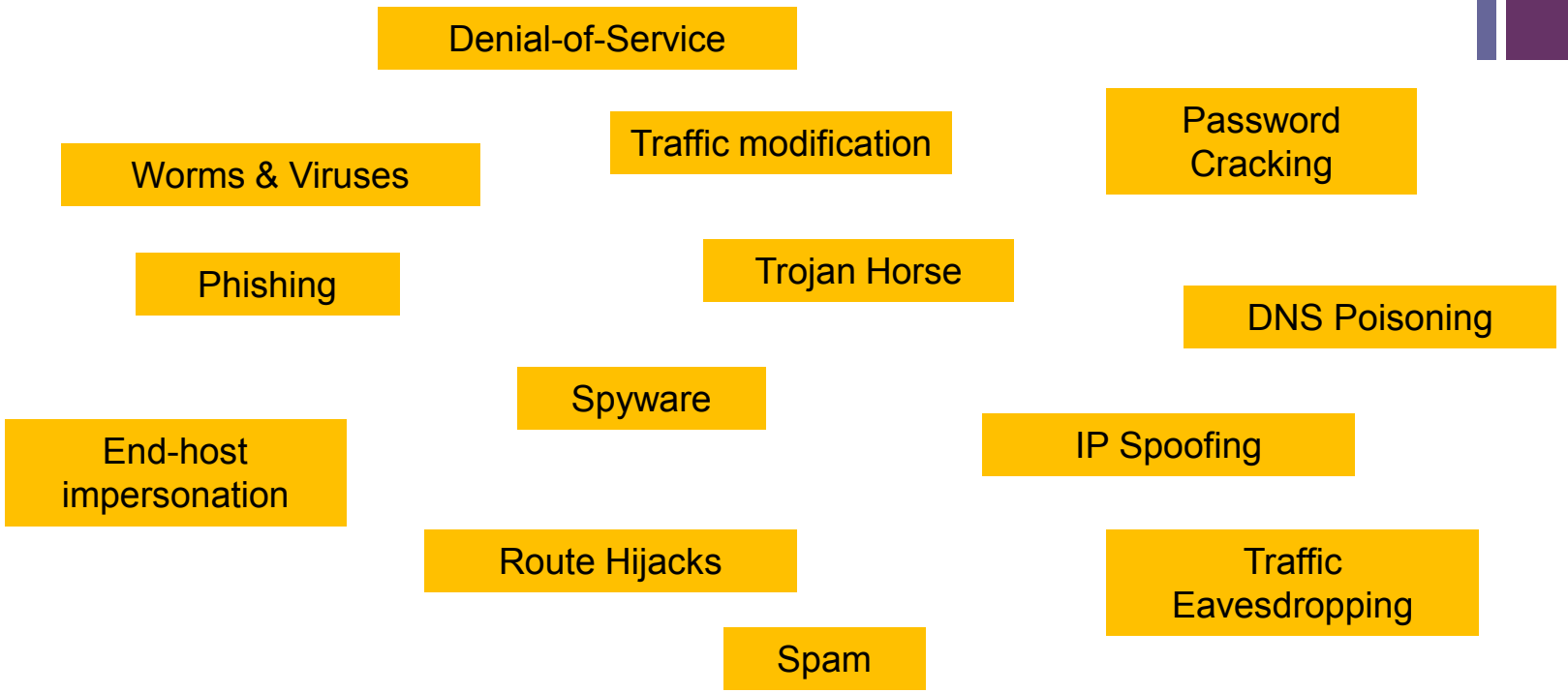
- "Kalau mau saya bisa mengontrol internet di seluruh Indonesia," kata Jim dalam percakapan dengan *Deutsche Welle*.

- "Saya tidak pernah meng*hack*…kalaupun ya, saya tidak akan mengungkapkannya dalam wawancara, hehehe. Tapi saya banyak dibayar untuk melakukan uji coba sistem keamanan. Saya punya konsultan perusahaan keamanan untuk menguji aplikasi dan jaringan. Klien saya mulai dari perbankan, telekomunikasi, asuransi, listrik, pabrik rokok dan lain-lain."

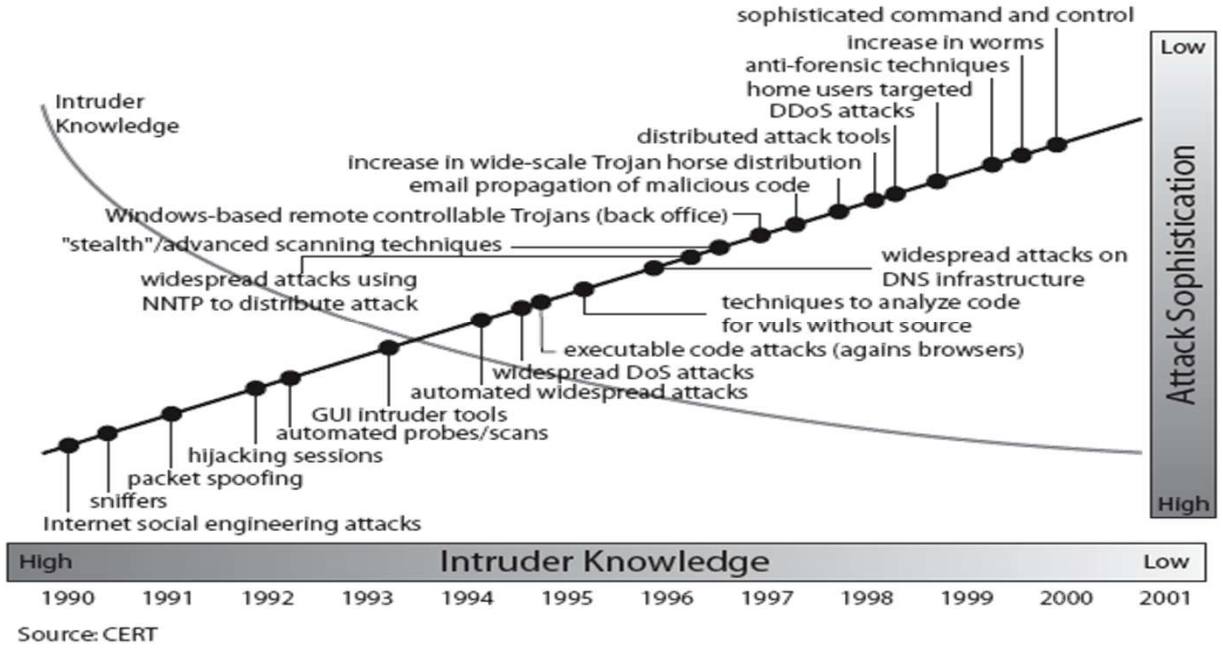
http://www.dw.de/jim-geovedi-meretas-satelit-di-langit/a-16564273

Artikel 2013

Serangan Internet

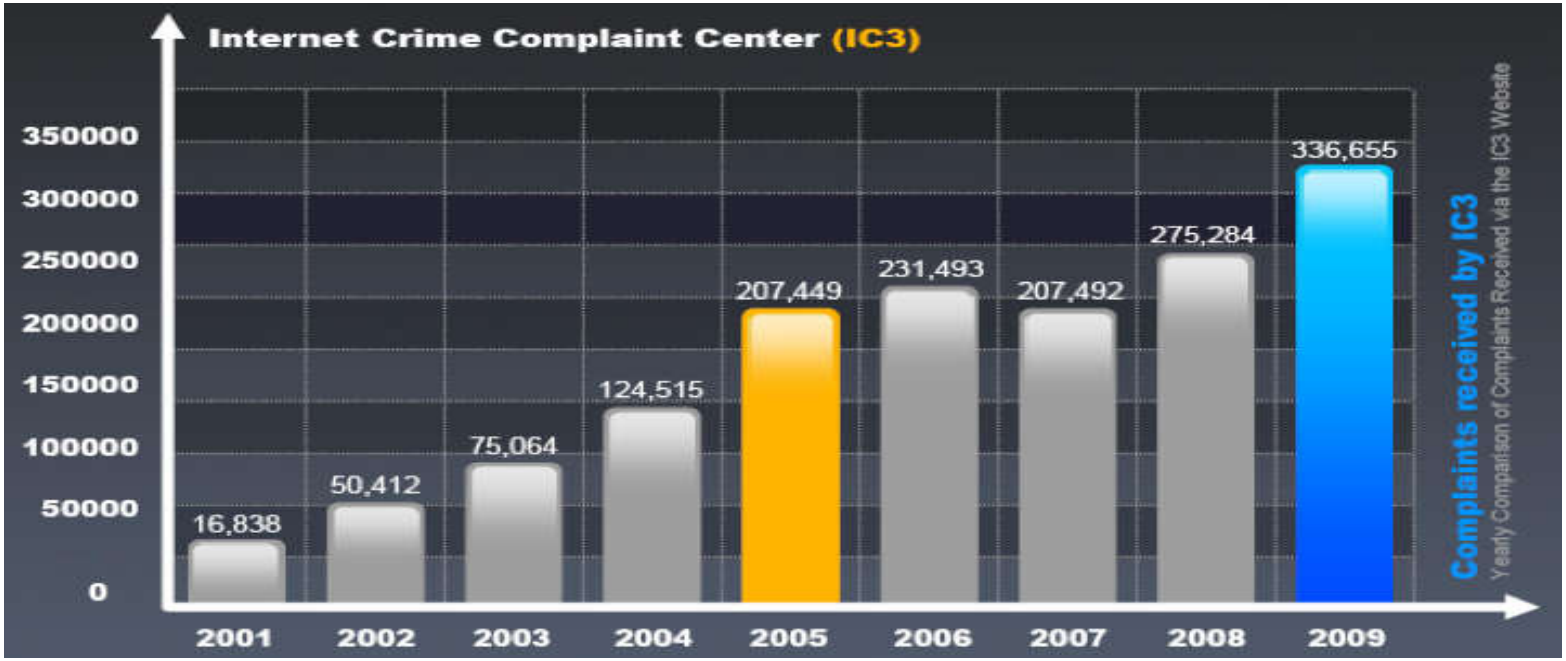


Trend Keamanan



Source: CERT

IC3 report 2009

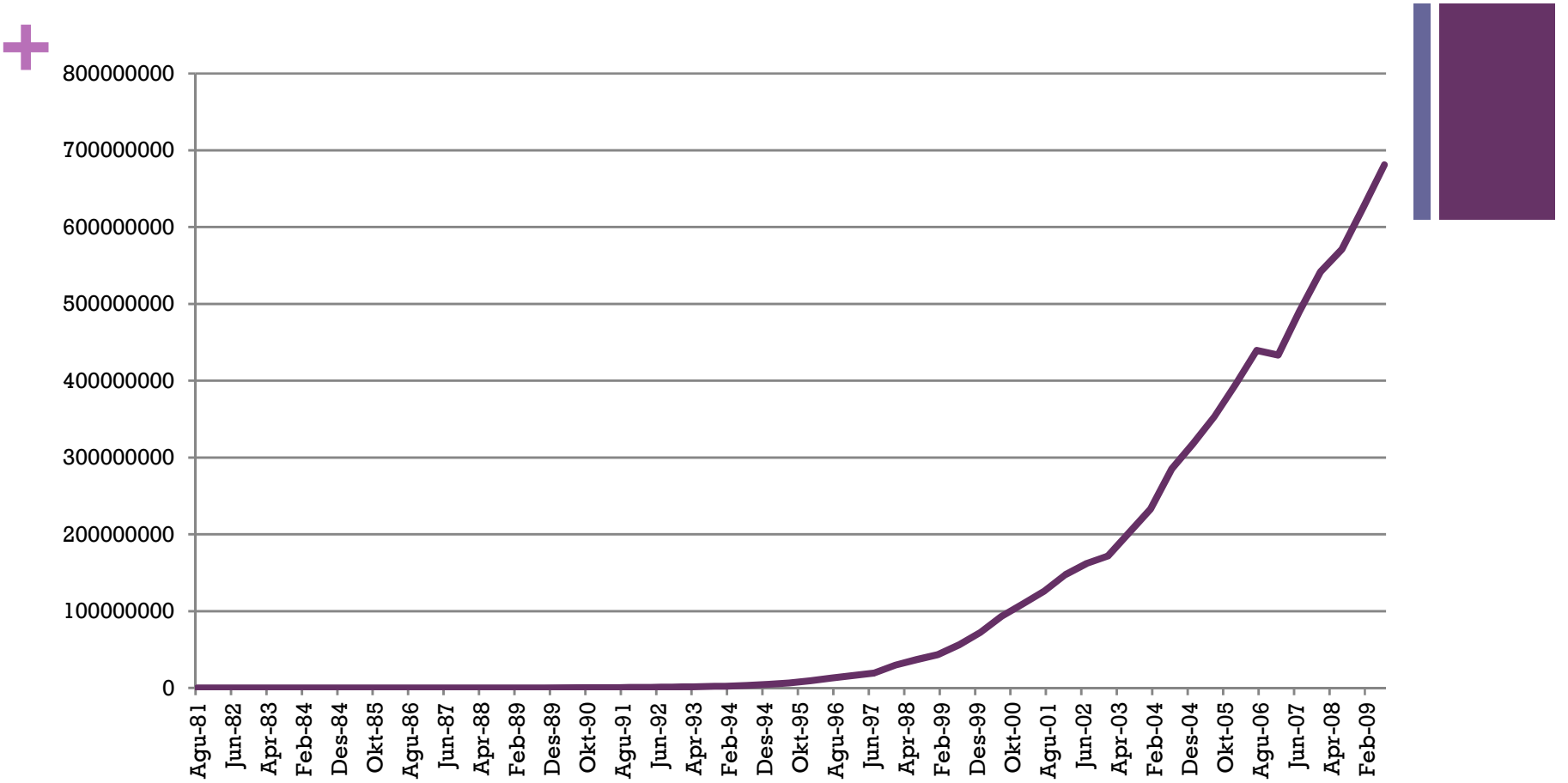


Evolusi metoda serangan

- Serangan satu ke satu mendominasi sampai akhir 90an
  - Membutuhkan kemampuan pengetahuan pemrograman yang sangat tinggi dan serangan harus dilakukan secara real-time
  - Membutuhkan kesabaran untuk melakukan monitoring dalam rangka mencari kelemahan dari sistem
- Serangan memanfaatkan script dan program mulai marak mulai pertengahan tahun 90an
  - Masih serangan satu-ke-satu
  - Keahlian yang dibutuhkan lebih rendah, bisa dilakukan oleh ABG
- Munculnya scanner 1988 menyebabkan serangan gaya baru muncul
  - Secara dramatis mempercepat dan mempermudah serangan dengan munculnya daftar sistem yang rentan terhadap serangan dan jenis serangannya
  - Munculnya DSL sebagai sarana akses broadband menyebabkan sistem yang rentan tersedia 24/7

Evolusi metoda serangan

- Ekploitasi script otomatis digabungkan dengan scanner kelemahan sistem
  - Serangan kebanyak sistem bisa dilakukan secara mudah dengan menekan beberapa tombol saja
  - Banyak serangan saat ini dilakukan secara otomatis
- Kebangkitan WORM
  - Isi scanner di modifikasi untuk mendownload, install, dan menjalankan dirinya sendiri → menjadi seekor cacing (worm)
  - Suatu kode baru, dari saat diluncurkan bisa jalan berbulan-bulan atau tahunan


800000000
700000000
600000000
500000000
400000000
300000000
200000000
100000000
0
Agu-81
Jun-82
Apr-83
Feb-84
Des-84
Okt-85
Agu-86
Jun-87
Apr-88
Feb-89
Des-89
Okt-90
Agu-91
Jun-92
Apr-93
Feb-94
Des-94
Okt-95
Agu-96
Jun-97
Apr-98
Feb-99
Des-99
Okt-00
Agu-01
Jun-02
Apr-03
Feb-04
Des-04
Okt-05
Agu-06
Jun-07
Apr-08
Feb-09

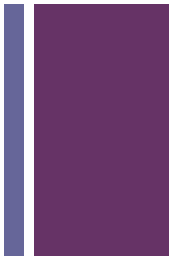
Evolusi metoda serangan

- Perang kanal IRC mendorong pengembangan bot dan DoS
  - Kegunaan IRC sebagai sarana komunikasi menjadi menurun oleh serangan ke infrastruktur servernya
  - Server IRC yang sah menjadi sangat tidak handal sehingga Bot Herder menbuat jaringan server IRC nya sendiri

Worm Pertama

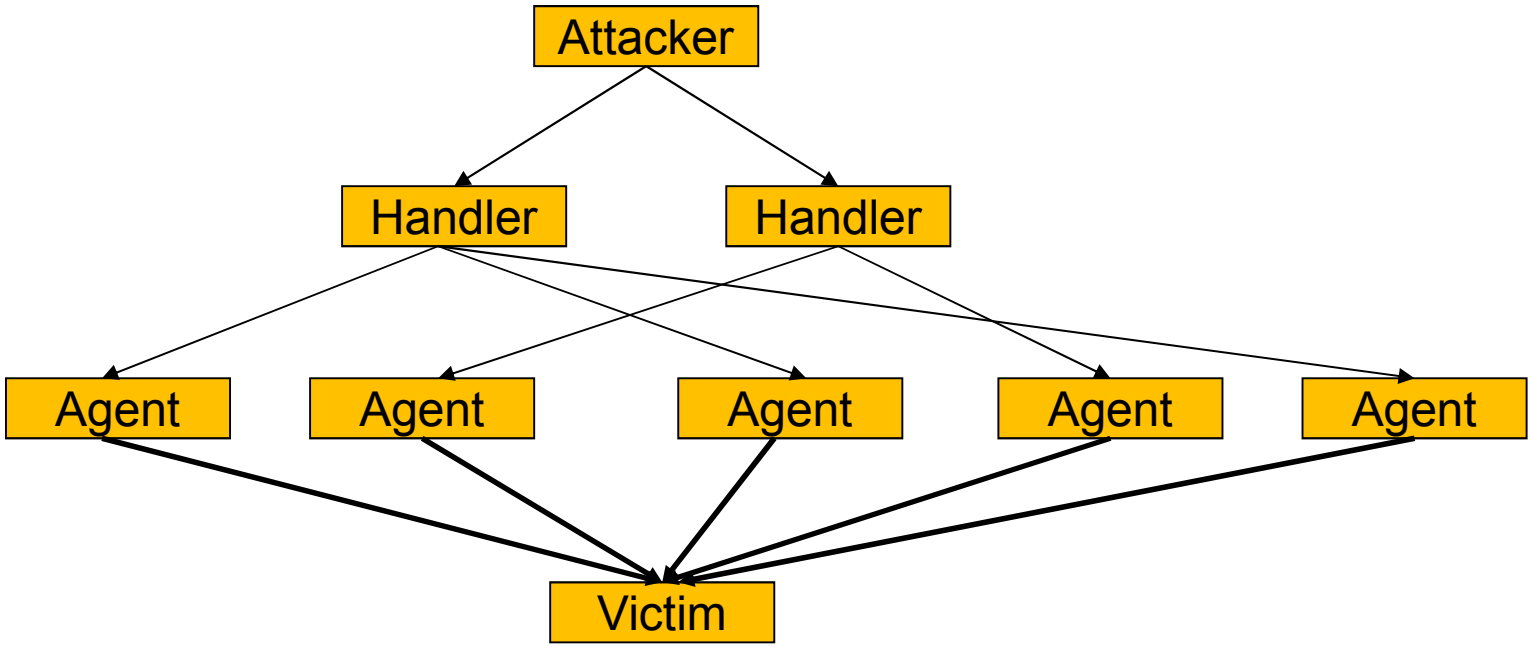
- Apakah Worm Morries th 1988 merupakan serangan pertama DDoS?
  - Ratusan sistem yang terinfeksi masing-masing mencoba menyerang tetangganya
  - Pertumbuhan yang tidak terkendali disebabkan kesalahan programming.

Diikuti oleh DoS

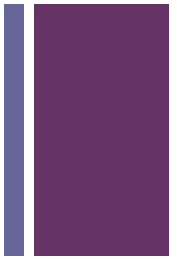


- Umumnya serangan masih satu ke satu
  - Bom e-mail (mailbox flooding) dengan banyak file berukuran besar
  - Menghabiskan resource host (memori, tabel proses dll)
  - Mengeksploitasi stack OOB (ping of death)

DDoS / Distributed-DoS



Sesuatu yang baru di 95..



- Syn flood
  - Menggunakan fitur protokol lapis bawah sebagai alat DoS, masih yang paling efektif dan paling susah untuk dikalahkan
  - Serangan berbasis protokol lain jika mulai muncul seperti : sequence guessing, RST flood
  - Masih merupakan serangan DoS terpopuler

Dan Yang Baru Muncul

- Beserta munculnya jaringan besar bot , DDoS baru muncul di akhir 1997, yaitu ICMP amplifier atau serangan Smurf

- Tugas : cari tau apa itu serangan smurf, jangan hanya copy-paste, pahami, berikan komentar anda mengenai serangan ini. Kumpul max pertemuan berikutnya

Hacking

- Etika Hacking
  - Pro : semua informasi adalah free
  - Kontra : jika semua informasi free, yang mana yang privasi?
- Aspek Keamanan
  - Pro : "*intrusion*" adalah ilustrasi kelemahan sistem
  - Kontra : tidak perlu jadi pencuri untuk menunjukkan pintu yang tidak terkunci
- Idle Machines
  - Pro : hacking hanya pada idle machines!
  - Kontra : "*idle machines*" itu milik siapa?
- Science Education
  - Pro : hanya membobol tapi tidak merusak
  - Kontra : "*hacker wannabe*" berpotensi sangat besar untuk merusak

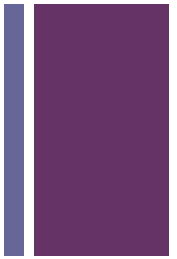
Fungsi Etika Hacking Apa??

- Melihat network security dari sudut pandang "*attackers*"
- Meningkatkan kewaspadaan staff IT terhadap bahaya yang mungkin terjadi setiap waktu
- Membangun desain network yang cenderung aman
- Merencanakan langkah antisipasi terhadap setiap insiden

Serangan Khas

- Serangan Buffer Overflow
  - Korban : aplikasi yang ditulis dengan tidak baik
  - Memanfaatkan kesalahan programming untuk mengeksekusi sisipan kode
  - Dapat dieksploitasi secara remote atau lokal, tergantung aplikasi
  - Spesifik pada prosesor dan OS tertentu
- Denial of Service
  - Menjadikan service tidak dapat dipergunakan
  - Target DoS :
    - Koneksi jaringan penghubung antar servis dan user
    - OS yang digunakan
    - Aplikasi yang menyediakan service

Serangan Khas



- Serangan Distributed Denial of Service (DDoS)
  - Sama seperti DoS, namun menggunakan banyak host untuk menyerang satu target
  - Host yang digunakan untuk menyerang biasanya host yang telah berhasil dikuasai
  - Eksekusi DDoS dilakukan serentak (menggunakan master host)
  - Efek yang ditimbulkan lebih berbahaya

Serangan Khas

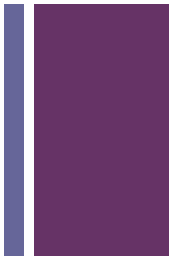
- Penyalahgunaan Trust
  - Hanya berlaku pada jaringan berskala kecil dan menggunakan tipikal arsitektur jaringan yang lama
  - Memanfaatkan trust antar host/sistem
  - Sulit dibedakan antara intruder dan user biasa
- Serangan Brute Force
  - Secara berulang melakukan percobaan autentifikasi
  - Menebak username dan password
  - *Cracking* password file

Serangan Khas

- Serangan CGI / WWW
  - Terbagi dalam 3 kategori
    - Buffer overflow : tidak melakukan validasi pada user input
    - Command execution : dapat mengeksekusi perintah tambahan
    - Subverting client-side scripting : dapat dimanfaatkan untuk mengeksekusi buffer overflow dan command execution disisi client
- Backdoor & Kuda Troya
  - Memperdayai user atau sysadmin untuk memberikan password mereka tanpa diketahui
  - Dapat berupa program yang umum dikenal dan sering digunakan sehingga tidak menimbulkan kecurigaan

Laporan Investigasi

Fase Hacking



- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Clearing Track

Reconnaissance

- Tahap persiapan untuk penyerang untuk mendapatkan informasi dari seorang target sebelum dilakukannya penyerangan
- Mengetahui kapasistas dari target disaat terdapat penyerangan berikutnya
- Mengetahui cakupan dari target, bisa saja klien sebuah perusahaan, pegawai, jaringan, dan sebagainya.

Tipe Reconnaissance

- Pasif
  - Informasi didapatkan tanpa berinteraksi langsung dengan target
  - i.e. : public records atau news releases

- Aktif
  - Informasi didapatkan dengan sengaja melakukan interaksi langsung dengan target
  - i.e. : menghubungi help desk sebuah perusahaan

Scanning

- Melakukan penyaringan data untuk mengetahui informasi detail dari target
- Melakukan penyaringan seperti : dialers, port scanner, network mapping, sweeping, vulnerability, dsb..
- Melakukan ekstraksi dari informasi yang didapatkan, seperti nama komputer, alamat IP, akun pengguna, dsb..

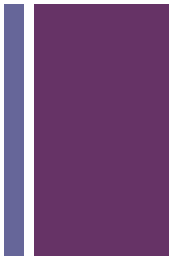
Gaining Access

- Penyerang sudah melakukan akses ke sistem operasi atau aplikasi pada sebuah komputer atau jaringan
- Penyerang mendapatkan hak akses untuk mengakses sistem operasi, aplikasi, ataupun jaringan
- Penyerang mendapatkan hak untuk menguasai sistem kontrol dari sebuah sistem
- Dapat dilakukan dengan melakukan password cracking, buffer overflows, DoS, session hijacking, dsb..

Maintaining Access

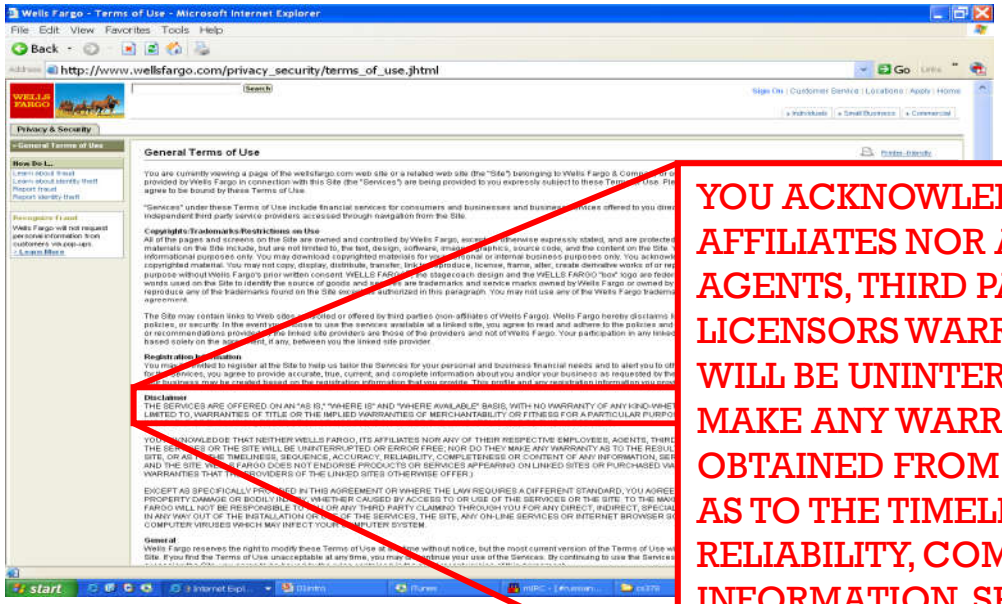
- Melakukan pengaturan pada komputer korban yang sudah di*hack*, sehingga kelak penyerang akan mengakses komputer tersebut, metode yang dilakukannya jauh lebih sederhana
- Rootkits, Backdoor, dsb..
- Penyerang dapat meng*upload*, men*download*, manipulasi data, dan mengubah konfigurasi sistem.

Clearing Track

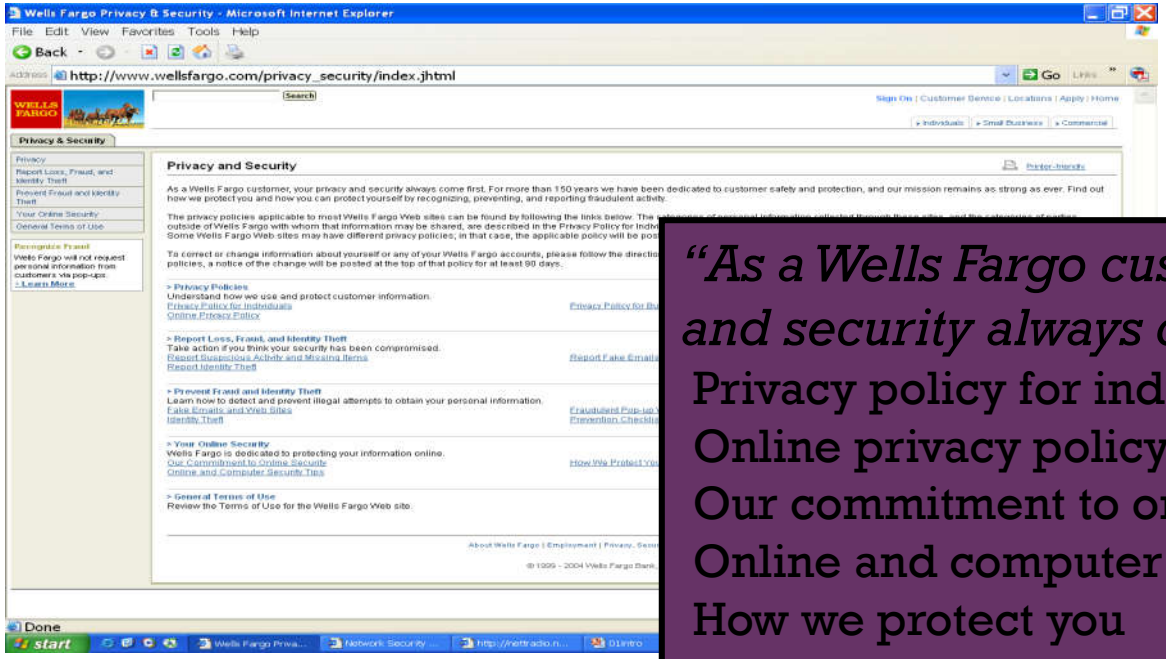


- Menyembunyikan perilaku menyimpang pada sistem
- Overwrite log server, sistem dan aplikasi untuk menutupi kecurigaan
- Hapus semua bukti, file aneh, dsb..

Kutipan dari "General Terms of Use"



Privasi dan Keamanan



"As a Wells Fargo customer, your privacy and security always come first."

Privacy policy for individuals
Online privacy policy
Our commitment to online security
Online and computer security tips
How we protect you
General terms of use

Properti Keamanan Ideal

- Autentifikasi
- Kerahasiaan
- Keutuhan
- Ketersediaan
- Pertanggung-jawaban dan tanpa penyangkalan
- Kenyamanan
- Kendali Akses
- Privasi dari informasi yang dikumpulkan
- Kesatuan routing dan infrastruktur DNS