Tietoturvaohjelmistojen toteutus

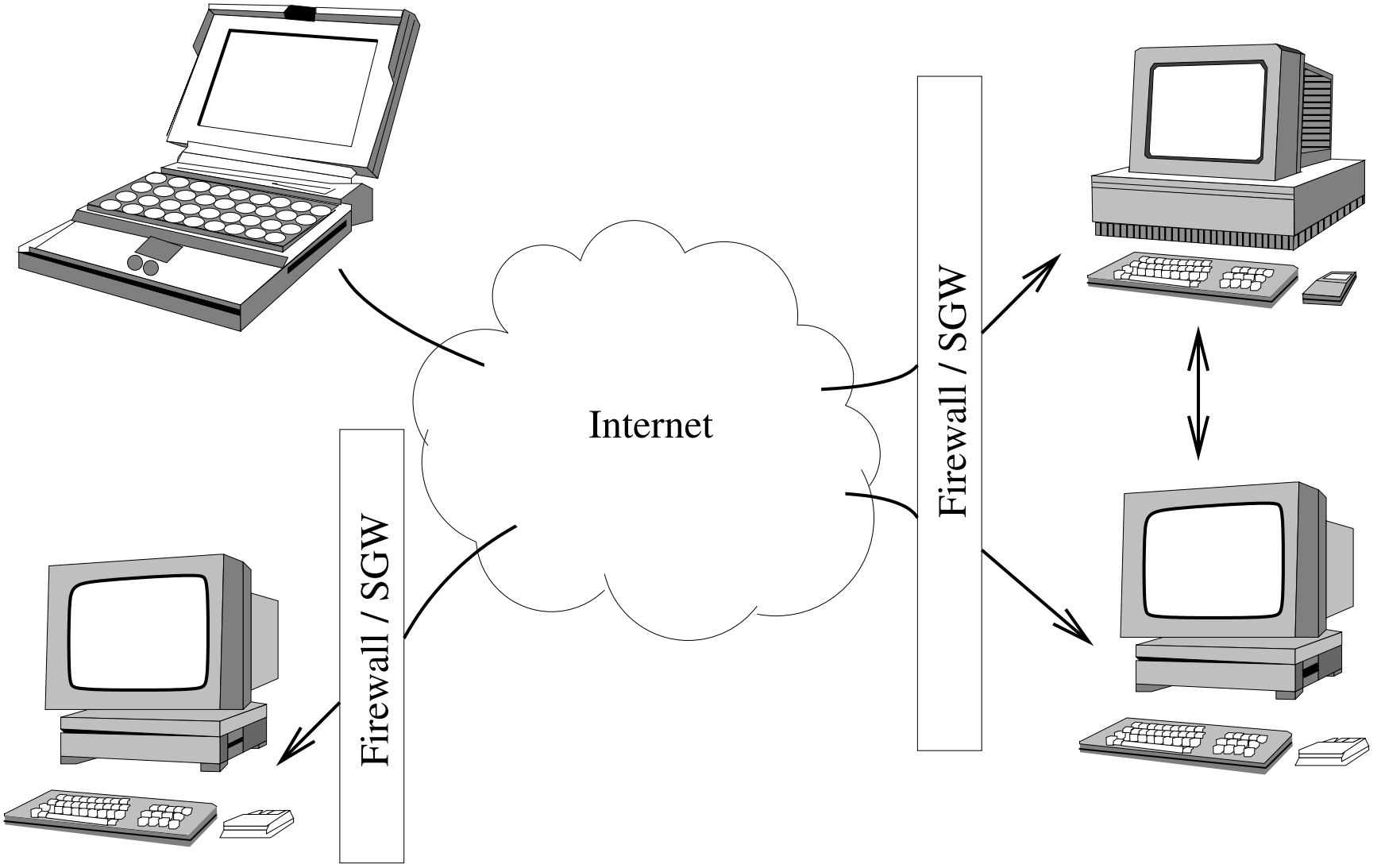
Markku Rossi

mtr@ssh.com

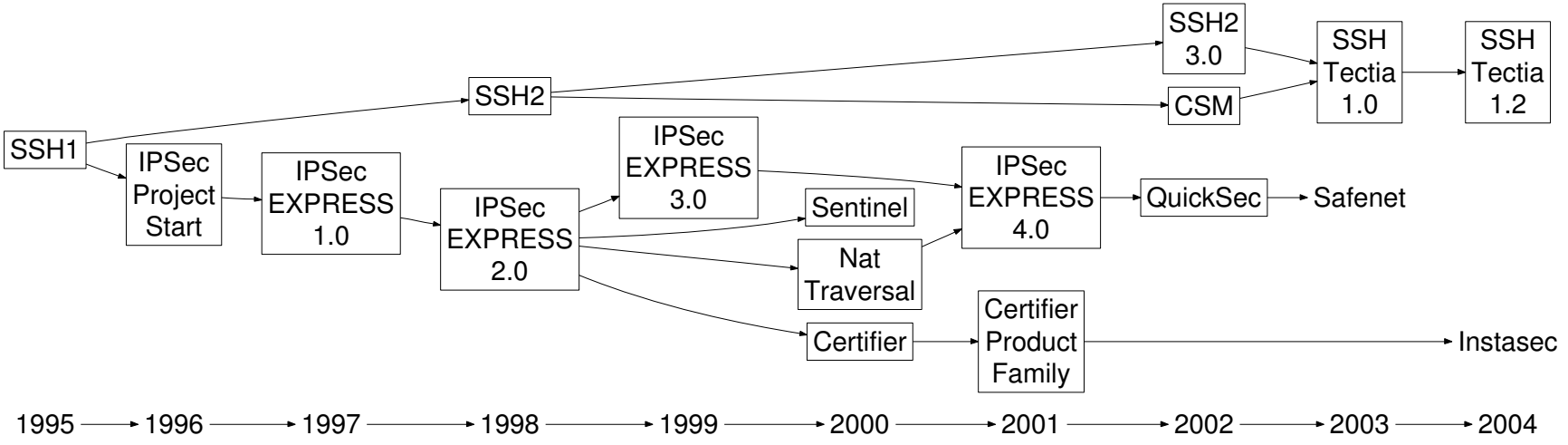
Agenda

- Tietoturva, mitä se on?
- SSH Communications Security 1995–2004
- Toimintaympäristön vaatimukset ja rajoitteet
- Ohjelmistotuotanto käytännössä

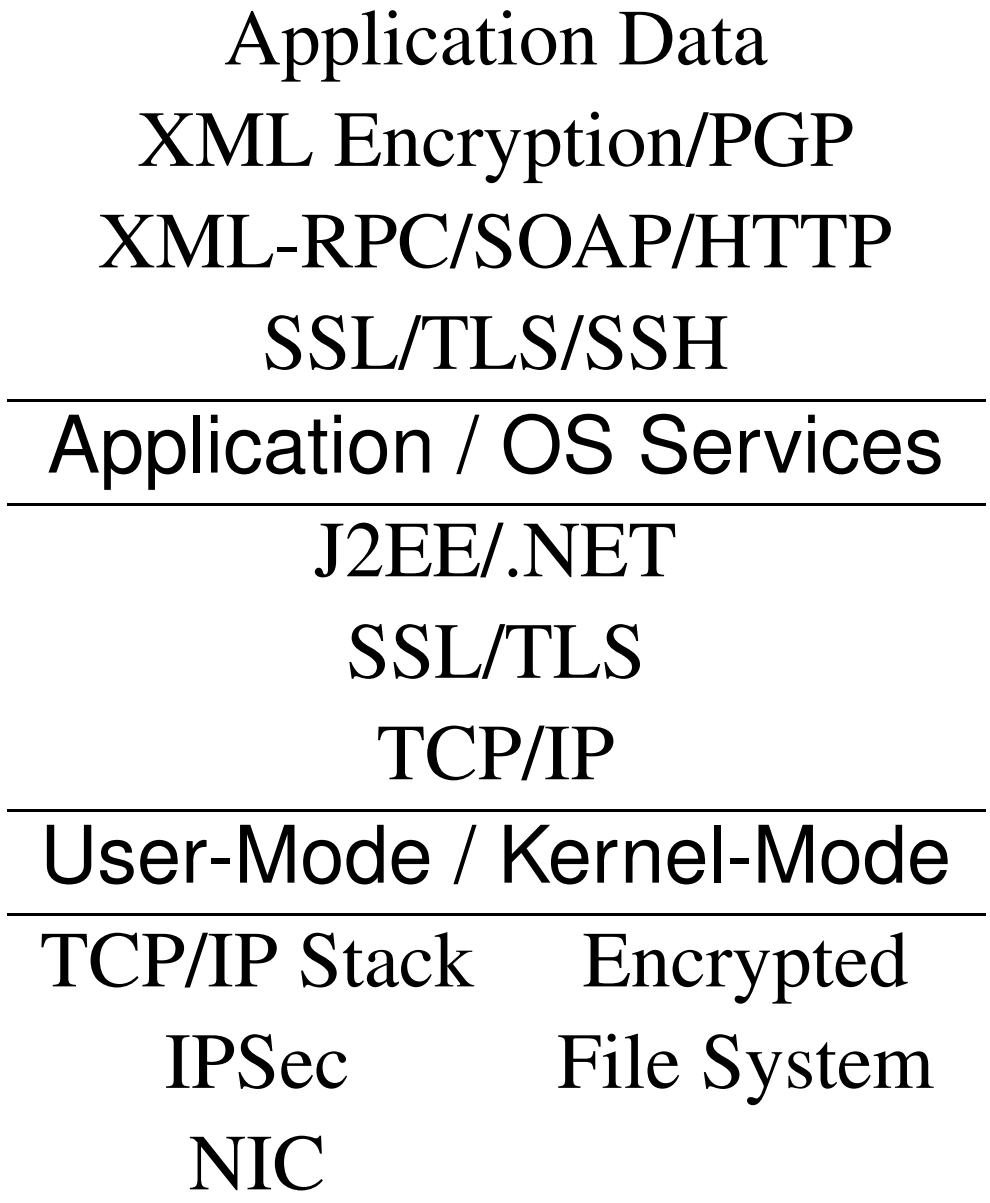
Tietoturva



SSH Communications Security



Sovellus ja käyttöjärjestelmä



Toimintaympäristö

- Yleiskäyttöiset käyttöjärjestelmät
  - Windows 95,98,Me,NT,2000,2003,XP
  - Solaris, HP/UX, AIX, Tru64
  - Linux 2.2 $\rightarrow$
- Sulautetut järjestelmät
  - VxWorks
  - NetBSD, FreeBSD
  - Nucleus
  - Linux
  - Symbian

Käytettävissä olevat resurssit

- Muisti: 5MB $\rightarrow$ 256MB
- Pino: 2048B $\rightarrow$ 4096B $\rightarrow$ 128kB
- Säikeet [a]: 16 / prosessi $\rightarrow$
- CPU cyclet: 0.01% $\rightarrow$ 95% koneen laskentatehosta

[a] Ei tuettu kaikilla alustoilla.

Vaatimukset

- Wire-speed
- Guaranteed response (real-time systems)
- Zero bugs
- Tuki kaikille käyttöjärjestelmille mitä asiakkaalla on käytössä
- ...

Ohjelmat: IPSec

QuickSec Access 2.0 Toolkit

MODULE	LOC
Policy Management	46000
Application Gateways	26000
IKE	32000
Certificate Management	55000
Other Libraries	290000
Packet Processing Engine	50000
Total	499000

Ohjelmat: ssh-4.1.5.5

SSH-4.1.5.5-commercial

MODULE	LOC
`zlib`	6700
Certificate Management	80000
Crypto Library	50000
Math Library	11000
Other Libraries	101000
`apps/ssh`	99000
Total	347700

Ohjelmistotuotanto

- Tässä on speksi:
  - RFC 2401, RFC 2402, RFC 2403, RFC 2404, RFC 2405, RFC 2406, ...
- Mikset jo koodaa?

```
$ emacs mokkula.c
  M-x compile
^Z
[1]+  Stopped                 emacs
$ ./mokkula
Segmentation fault (core dumped)
$ fg
  M-x gdb mokkula mokkula.core
```

Ohjelmistotuotanto

- Software business as usual
- Paitsi että
  - Tietoturva on välttämätön paha jos sitäkään
    - Ei business hyötyä sellaisenaan
    - Nykyisin säädökset auttavat:
      - Gramm–Leach–Bliley Act (GLBA)
      - Health Insurance Portability and Accountability Act (HIPAA)
      - Sarbanes–Oxley Act (SOX)
      - Basel II
      - California SB 1386
  - (Tietoturva)ohjelmistossa on aina varauduttava pahimpaan

Mitä tehdään ja kenelle?

- Requirement engineering
- Asiakkaalta kannattaa todellakin kysyä...
- ...mutta vastuu jää kysyjälle ts. asiakas ei tiedä mitä hän haluaa
- Tietoturva voi olla vaikea asia selittää ja ymmärtää

Arkkitehtuuri

- Huomioi toimintaympäristön kirjavuus
  - suunnittele järjestelmä joko yhdelle
  - tai n:lle platformille
- Selkeät rajapinnat käyttöjärjestelmäspecifiselle koodille
- Varaudu vaatimusten muutoksiin ja laajennuksiin
  - Asiakaslähtöiset muutokset
  - Teknologialähtöiset muutokset
    - algoritmien haavoittuvuudet (DES, MD5)
    - uudet hyökkäykset

Varaudu pahimpaan

- “Dirty data”
  - Kaikki “ulkoa” (verkosta, levyltä, yms.) tuleva data on rikkinäistä ja vahingollista.
- “Denial of Service” hyökkäykset
  - Tietoliikenneprotokollien rajoitteet ja mahdollisuudet (IKEv1 / IKEv2)
  - Algoritmien valinta, toteutus
  - Rate-limiting connections per host
  - black-listing hosts

Millä tehdään?

- C, C++, Java, Visual-Basic, Perl, Scheme, ...
- Miksi C:
  - Toimii kaikissa käyttöjärjestelmissä
  - Suorituskyky
  - Kernel ohjelmointi
  - Muistinhallinta
  - Rajapinnat muihin järjestelmiin helppoja
- Miksi ei C:
  - Muistinhallinta
  - Pinon ylivuoto
  - Bufferien ylivuodot

Toteutus

- KISS
  - Tehokkaat algoritmit
  - Yksinkertainen “käsiala” ja toteutus
- Ylläpidettävyys
  - Coding style
  - Standard coding idioms
- Testattavuus

Coding Idioms

- Virheiden käsittely
- Muistin varaus ja vapautus

Code Reviews

- Self review. *Watts S. Humphrey:*

  Code reviews are from three to five times more efficient in finding bugs than unit tests.

- Peer reviews

Optimointi

Michael Jackson:

- The First Rule of Program Optimization:

  Don’t do it.

- The Second Rule of Program Optimization (for experts only):

  Don’t do it yet.

Optimointeja

- Vältä datan kopiointia
- `cc -pg`
- $O(n)$ vs. $O(n^2)$

Jatkuva oppiminen

- Oppiminen toimintaympäristöstä:
  - malloc, snprintf, memcmp
- Oppiminen virheistä
- Ammattitaidon ylläpito

Asenne

Ei kirjoiteta niitä bugeja!

Ammattiylpeys

Minä tein tämän!