Everyday Security Problems

- Viruses
- Unauthorised access
- Sniffing
- Password cracking
Why do security problems appear?

- People, the weakest link
- Security holes in mainstream products
  - Word
  - Excel
  - Outlook
  - Windows
  - Sendmail
  - Apache
- Insecure networking
- Insecure storage
- Inefficient authentication of users
Unencrypted data

- If you can touch a computer, you can steal the data on it
- Stealing laptops becoming more and more common
- Windows NT offers no protection
Passwords

• Password is like a toothbrush
  – Exchange regularly
  – Do not share with others

• A good password...
  – is over 13 characters long
  – contains special characters
  – can't be found from any dictionary
  – easy to remember
    —> use a passphrase
  – "stupid&boringJob!", "My_Boss_Smells_Bad..."
Social Engineering

- "Here's the IT Manager from the New York department. What the heck is wrong in your systems! I can't access our order database and clients are waiting in the meeting room!"
Kevin Mitnick damages 1993-1994

- Sun, USA; Solaris source code: $80M
- NEC, Japan; Mobile phone sources: $1.75M
- Nokia, Suomi; HD760 project: FIM 2.5M
- Nokia, UK; "Mobile software": $135M
- Novell, USA; Netware sources: $75M
- Fujitsu, USA; PCX phone sources: $2.1M

Source: http://www.hackernews.com/orig/letters.html
Kevin Mitnick sentence

- Sentence issued on August 9th, 1999
- Total damage: $296,000,000
- Mitnick ordered to pay: $4,125
- And to serve 46 months in prison
- Will be released around January 2000
Number of viruses (9/1999)

- **PC:** Over 43,000
  - Windows 3.x: 15
  - Windows 95: 210
  - Windows NT: 50
- **Word:** ~4100
- **Excel:** ~700
- **Powerpoint:** 5
- **Macintosh:** 50
- **Linux:** 5
Costs of viruses

- "Businesses worldwide have lost a total of US$7.6 billion in the first two quarters of 1999 because of viruses"
  - Wired, Computer Economics Inc.

Why are viruses written?

- Anarchy
- Curiosity
- Challenge
- Fame
- Power
What do virus writers look like?

David L. Smith, 30, USA

Christopher Pile, 27, UK

Chen Ing-Hau, 24, Taiwan
Demos...

- Word macro viruses
- Excel macro viruses
- Cracking passwords
- Sniffing
NT-aware virus

The virus infects a single NT machine
NT-aware virus

Virus starts to sniff network traffic
NT-aware virus

And collects the admin password hash
NT-aware virus

Virus starts to crack the password
What if...

- If all stored information is strongly encrypted...
- If all information in the network is strongly encrypted
- If viruses are stopped at every level...

You have solved 99% of your security problems
- Firewalls and intrusion detection products become secondary priorities
Security Drivers

- Increasing Workforce Mobility
- Growth of EDI / EC / Extranets
- Need for Global Access to Info
- Outsourcing Trend for IT Services

Confidential information is increasingly created and stored outside corporate LANs and is accessible over public non-secure networks.

Corporate information needs to be protected everywhere, all the time.
Critical Problem

How can a corporation ensure that corporate information, the lifeblood of the organization, is protected every minute of every day, everywhere around the world, when the workforce is increasingly mobile and the methods of communication are inherently insecure?
Management vs. Distribution

Centralized, Policy Based

Fragmented, Device Based

Enjoy centralized management - but only within the “perimeter”

Distributed stand-alone products - but difficult to deploy and manage

Secure the “Perimeter”

Secure every device

Distributed stand-alone products - but difficult to deploy and manage
The F-Secure Solution - Management and Distribution

- Centralized, Policy Based
- Fragmented, Device Based

Management

Secure the “Perimeter”
Secure every device

Distribution

- Firewalls, Existing VPNs, Intrusion Detection
- Router ACL, Gateway AV
- Standalone AV, Point Security Apps
- F-Secure applications protect corporate information everywhere all the time
## Security Solution Alternatives

<table>
<thead>
<tr>
<th>Management</th>
<th>Secure the “Perimeter”</th>
<th>Secure every device</th>
</tr>
</thead>
</table>
| Centralized, Policy Based | - doesn’t protect against inside intruders  
- no way to efficiently secure mobile users  
- FW are becoming less efficient due to HTTP  
- doesn’t happen where information is created and processed  
- no broadband outside the LAN |  
| | **Increased security (coverage)**  
- protects from inside attacks  
- faster reaction to new security threats  
- enables mobility (people and devices)  
- enables the truly distributed organization  
- enables the use of broadband  
- enables Security as a Service™ — both external and internal |  
| Fragmented, Device Based | - doesn’t provide granularity  
- hard to enforce extensive security  
- hard to manage  
- security settings become static  
- no way to secure mobile users  
- doesn’t protect against inside intruders |  
| | - complexity of deployment, updates and management  
- complexity can lead to security holes  
- hard and expensive to manage  
- security settings become static  
- impossible to enforce  
- no way to efficiently secure mobile users |
Choose one: management or distribution

Management
- Enjoy centralized management – but only of the systems within the “perimeter”

Distribution
- Buy standalone point products, but live with the burden of separately maintaining each system, forget all about unobtrusiveness, allow the end-users to uninstall the applications etc. etc.
F-Secure applications enable the provision of Security as a Service™ by:
- Making security invisible, automatic and non-intrusive to end-users
- Enabling the administrator to simply push a button to define, install, control and manage security

This service can be provided by:
- internal IT departments
- third-party service providers
  - ISPs for SOHO customers
  - Facility Management companies and Application Service Providers for corporate customers
Security as a Service™

DF
Distr. Server

Sonera
Distr. Server

Any SP
Distr. Server

Push, HTTP Information Channels

Applications, updates, Information, virus alerts
SUHU customers
Corporate customer
Email + hotline support
Centrally Managed Security – Without Boundaries

• Data Fellows brings security that is

  – **Widely distributed**
    • Automatic installation on hundreds of thousands of systems
    • Automatic updating of virus and security information, corporate policies

  – **Centrally managed**
    • Centralized, hierarchical policy management
    • Common management interface for all products
    • Centralized alarms and alerts

  – **Transparent to end users**
    • Users don’t need to do anything
    • No danger of users removing or bypassing security

ANYTHING ELSE IS JUST A COMPROMISE!
F-Secure Applications and Framework

Security as a Service™

- Policies, Applications
- Alerts, reports
- Push
- HTTP

Control
Scalability
Execution

An Extensible, Highly Integrated Solution

- F-Secure Anti-Virus
- F-Secure FileCrypto
- F-Secure VPN+
- F-Secure SSH
- 3rd Party Product

Workstations, Servers, Gateways, new Platforms

F-Secure Mgmnt Servers

F-Secure Anti-Virus
F-Secure FileCrypto
F-Secure VPN+
F-Secure SSH
3rd Party Product

F-Secure Anti-Virus
F-Secure FileCrypto
F-Secure VPN+
F-Secure SSH
3rd Party Product

Workstations, Servers, Gateways, new Platforms

F-Secure Mgmnt Servers

F-Secure Anti-Virus
F-Secure FileCrypto
F-Secure VPN+
F-Secure SSH
3rd Party Product

Workstations, Servers, Gateways, new Platforms

F-Secure Mgmnt Servers

F-Secure Anti-Virus
F-Secure FileCrypto
F-Secure VPN+
F-Secure SSH
3rd Party Product

Workstations, Servers, Gateways, new Platforms

F-Secure Mgmnt Servers

F-Secure Anti-Virus
F-Secure FileCrypto
F-Secure VPN+
F-Secure SSH
3rd Party Product

Workstations, Servers, Gateways, new Platforms

F-Secure Mgmnt Servers

F-Secure Anti-Virus
F-Secure FileCrypto
F-Secure VPN+
F-Secure SSH
3rd Party Product

Workstations, Servers, Gateways, new Platforms

F-Secure Mgmnt Servers

F-Secure Anti-Virus
F-Secure FileCrypto
F-Secure VPN+
F-Secure SSH
3rd Party Product

Workstations, Servers, Gateways, new Platforms

F-Secure Mgmnt Servers

F-Secure Anti-Virus
F-Secure FileCrypto
F-Secure VPN+
F-Secure SSH
3rd Party Product

Workstations, Servers, Gateways, new Platforms

F-Secure Mgmnt Servers

F-Secure Anti-Virus
F-Secure FileCrypto
F-Secure VPN+
F-Secure SSH
3rd Party Product

Workstations, Servers, Gateways, new Platforms

F-Secure Mgmnt Servers

F-Secure Anti-Virus
F-Secure FileCrypto
F-Secure VPN+
F-Secure SSH
3rd Party Product

Workstations, Servers, Gateways, new Platforms

F-Secure Mgmnt Servers

F-Secure Anti-Virus
F-Secure FileCrypto
F-Secure VPN+
F-Secure SSH
3rd Party Product

Workstations, Servers, Gateways, new Platforms

F-Secure Mgmnt Servers

F-Secure Anti-Virus
F-Secure FileCrypto
F-Secure VPN+
F-Secure SSH
3rd Party Product

Workstations, Servers, Gateways, new Platforms

F-Secure Mgmnt Servers

F-Secure Anti-Virus
F-Secure FileCrypto
F-Secure VPN+
F-Secure SSH
3rd Party Product

Workstations, Servers, Gateways, new Platforms

F-Secure Mgmnt Servers

F-Secure Anti-Virus
F-Secure FileCrypto
F-Secure VPN+
F-Secure SSH
3rd Party Product

Workstations, Servers, Gateways, new Platforms
Data Fellows’ Solution

Policy based management: F-Secure Framework

Malicious code protection: F-Secure Anti-Virus

Network encryption: F-Secure VPN+

File encryption: F-Secure FileCrypto

Secure remote management: F-Secure SSH

New F-Secure products
Leading global provider of centrally-managed, widely distributed solutions for enterprise security — enabling the provision of security as a service
History of Data Fellows

1988  Founded by R. Siilasmaa & Co
1990  Focus on Anti-Virus products
1996  Entered into encryption, F-Secure SSH launched
1997  Data Fellows Inc. established in Silicon Valley
      F-Secure VPN+ launched, Hot Product of the Year (Data Communications Magazine)
1998  Global expansion: regional sales offices established in US, UK, Germany, France and Canada;
      F-Secure Framework project
      F-Prot brand name changed to F-Secure
1999  Regional sales offices opened in Japan and Greater China
      F-Secure Framework launched
Best-of-Breed Applications

- F-Secure Workstation Suite 4.0 5/5 “Components are seamlessly integrated, centralized control of the network, 5/5 overall rating” (Secure Computing - July 1999)
- F-Secure VPN+ “the fastest software-based IPSec-compliant VPN” (Sonera - April 1999)
- F-Secure Anti-Virus “The Editor’s Choice” (PC Professionell magazine - July 1999)
- “F-Secure Anti-Virus detected more viruses “in the wild” than any other product, superior in macro virus detection” (Virus Test Center - March 1999)
- “The best product to detect known viruses” (Virus Bulletin - January 1999)
Government
DoD, French Army, IRS, NASA Headquarters, Naval Air Warfare Center, U.S. Army Medical

- **Leading universities**
  Harvard University, University of California Berkeley
- **Research**
  Cogema, Lawrence Livermore National Lab, Los Alamos National Lab, Oak Ridge National Lab, San Diego Supercomputer Center, Sandia National Lab
- **Banking**
  Charles Schwab, Credit Agricole, Daiwa Bank, DresdnerBank, E*TRADE, Fuji Bank, Merita-Nordbanken, Sumitomo Bank
- **Information Technology**
  Andersen Consulting, EDS, First Data Corp, Fujitsu, IBM, Siemens, Unisys
- **Telecommunication manufacturing**
  Cisco, Ericsson, Motorola, Nokia
- **Internet**
  Amazon.com, Digital Island, eBay, Entrypoint (Pointcast), Yahoo
- **Telecommunications**
  AT&T Wireless, British Telecom, Cegetel, Concert, Deutsche Telekom, GTE, NTT, Sonera, Telecom Italia, Telia, US West
- **Other**
  BMW, Boeing, DaimlerChrysler, Volkswagen