MINISTRY OF TRANSPORT
AND COMMUNICATIONS FINLAND

What is the Right Level of Data Security

Telecom Forum 2005

Kristiina Pietikäinen/ 29.11.2005

Content of the presentation

- Background
  - situation
  - initiatives and projects
- Contradictions between basic rights and security needs
- Challenges:
  - legislation
  - skills and awareness
  - balancing between basic rights and security threats

Situation

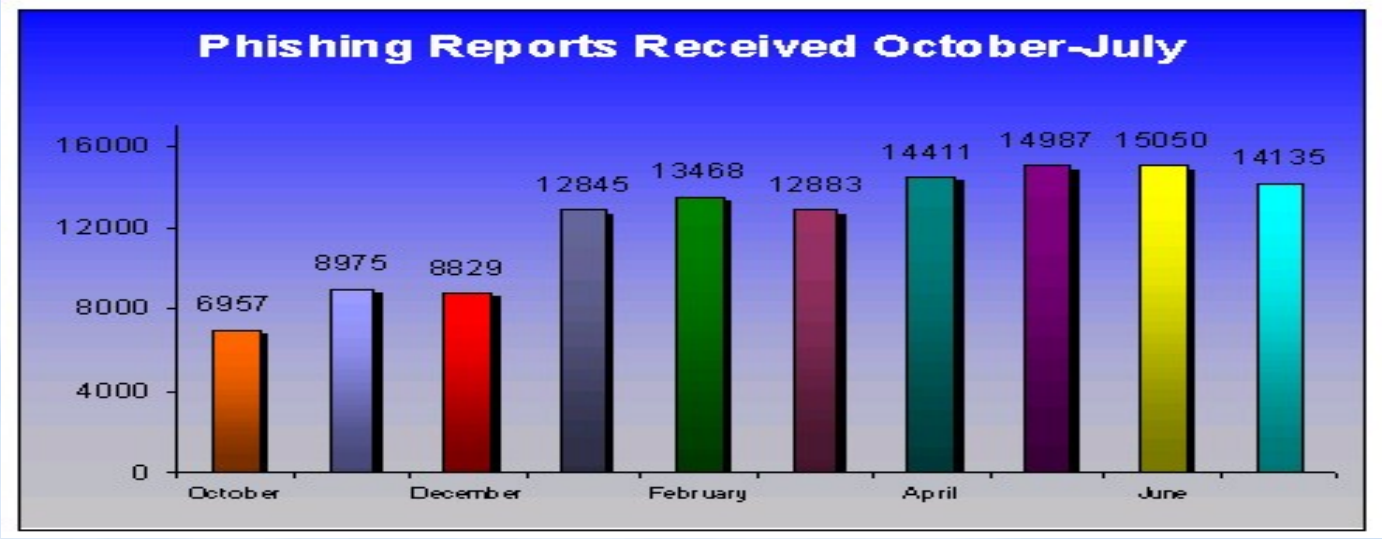
- Current major issues:
  - Internet is observed as more and more a playground for organised crime
  - Botnet phenomena – massive automated exploitation of vulnerable internet-attached computers as
    - vulnerability scanning platforms
    - spamm transmission
    - DDoS for hire attack platforms
- Tie between malware developers, botneck operators and spammers
- Worldwide: 5-10 million computers in the hands of botneck operators
- Finland: hundreds of IP-addresses

New threats

- Intelligent mobile devices
  - Symbian, Pocket PC, PalmOS
- Mobile device malware development has already moved from “proof-of-concept” to “production”
- Spreading has signs of distribution patterns in biological hazards
  - Bluetooth does not need network support
- Moving to MMS distribution can speed up distribution radically
- No really destructive malware – yet
  - Think of 50000 phones calling 112..

Current security threats:
Phishing

- Phishing attacks use both social engineering and technical means to steal consumers' personal identity data and financial account credentials.



Anti- Phishing work group, 2005

Phishing

- From english-speaking countries (Australia, UK, US, Canada) to Europe and Scandinavia
- First significant cases in Sweden during the last months
- Does the move to Scandinavia indicate that the European anglo-american market for phishing is drying?
- 28.10 at 20.40 Case Nordea

Botnet

- Netherlands in October: arrested 2 people who run a botneck of a million computers and using it for blackmail and spamming
- In Finland according to CERT.fi constantly running about 100 botnet contaminated systems
- Luckily no signs of botnets run from Finland

WLAN + MOBILE

- More common in companies and at home
- Increased risk of maluse, cause no protection such as passwords used
- www.cert.fi ; information on how to protect the personal WLAN environment
- Mobile: new challenges emerge as equipment has more programming capabilities
- Symbian- environment
- In the future:
  - M2M
  - Always on ip mobile terminals

Megatrends

- New tecnologies, mobility, no time to react, better targeted threats
- Less and less skills to prevent the threats: new protocols, new systems
- The greater dependence on the technologies in societies in general
- Economic productivity requirements: more with less
- mobility

Intiatives and projects

- Security is a two fold issue:
  - general security policy issues
  - information security issues
- Closely linked together and cannot be dealt with separately
- Therefore every security issue has both sides technical and general (= policy, economic)

Current threats and their implications

- Terrorism -> surveillance, data retention, registration, new methods for authentification, new powers to authorities, new control regimes
- illegal and harmfull contents -> control of content, blocking of access and connections, filtering
- spamm, viruses, phishing -> technical control, filtering, access control
- company security -> employee control, monitoring of emails and webb-usage, itemized bills etc.
- IPR -> need to control the p2p networks

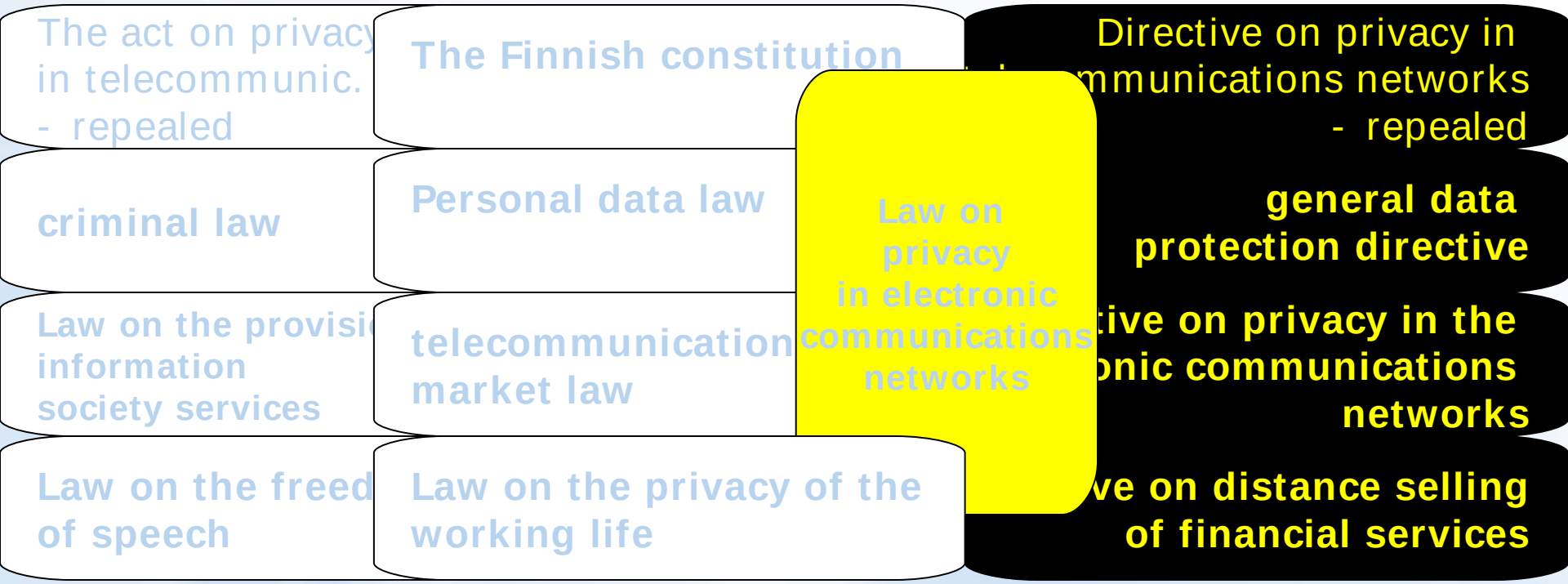
Ongoing

- EU:
  - Data retention initiative: framework decision + directive
  - Spamm: OECD task force on spamm, EU´s proposals?
  - EU`s data security strategy

Ongoing

- Finland:
  - updating the dataprotection legislation
  - blocking access to child porno sites
  - fighting spamm
  - biometric passports
  - registering the prepaid sim-cards
  - critical infrastructure protection
  - resources + organisation for information security work (CERT, CIP etc.)

About legislation



Finnish ”peculiarities” on confidentiality

- **Strong confidentiality of communications**
- corporate or association subscriber (means a **company or organization** which subscribes to a communications service or a value added service and which handles users’ confidential messages, identification data or geographic information in its communications network **as a third party)**
- **confidentiality of email in the working life**
- **confidentiality of internet usage** (traffic data relating to internet usage is confidential)
- **filtering of spamm is allowed under certain circumstances**

Needs to update the legislation

- Strong need to allow more processing of traffic data within companies (fraud detection, misuse of resources, security)
- Strong need to submit more traffic data to security officials for criminal investigations and prevention of criminal offences (location data, data retention, false basestations)
- Strong need to limit acces to certain sites and content to protect minors (child porno, rasism)
- Strong need to get the traffic data related to copyright insults to the ipr- holders

The user approach

- Security is a key element in the information society
- Information security threats are increasing
- The attacks are more systematatic and aim towards real benefits (= money)
- It is more and more difficult to protect oneself from misuse of information and resources
- Protections requires skills
- Protection requires resources (= money, staff)

What is the right level of security

- Technically speaking:
  - as much as possible, but limitations come from interoperability, costs, resources, skills,
  - how much can be foreseen in advance
- Speaking about principles:
  - how much data can be processed and collected in the spirit of respecting the basic rights (freedom of speech, confidentiality of communications, privacy protection) -> trust and acceptance from the users
- Taking into consideration the usability of services
- **Privacy and information security protection are not exclusive but complementary; both are needed**

Thingking ahead: ”Ubiquitous Society”

- Internet of things (IPV6)
- NGN (next generation networks)
- Rfid + plus other authentication and surveillance techonogies
- Sensors, chips, integrated intelligent devices
- Embedded systems
- Wireless technologies (WLAN, WiMax, 3G)
- Consumer electronics (digital television)
  - New requirements also for security
  - New elements of misstrust (bigbrother is watching)
  - Much more potential harm done with security attacks
  - Easy to use????
  - Real ability to protect the systems and users?
  - Economic benefits (innovations and competitivenes of the society)
- Information society for everyday life????

Examples of how to enhance security

- The Finnish information security strategy
- National Information Security Day
- The programme for enhancing security in the field of electronic entertainment services (LUOTI)
- Security requirements for biometric information
- U-strategy?
- Authority cooperation; CERT-functions, CIP cooperation
- Spamm-guide (www.xxxx.) to be opened

National Information Security Strategy

Strategic objectives

The national information security strategy helps Finland become an information-secure society. Objectives of the strategy are to:

promote national and international information security cooperation;

promote national competitiveness and the operating environment for Finnish information and communication operators;

improve information security risk management;

safeguard the fundamental rights and protect the nation's knowledge capital

increase awareness of and competence in information security.

MINISTRY OF TRANSPORT
AND COMMUNICATIONS FINLAND

The high level
National Information Security Advisory Board has task to

1. **ensure coordination** of the actions implementing Finland's National Information Security Strategy

3. **monitor the Strategy implementation** through to the end of its term in May 2007

5. **submit an annual report to the Government** on the implementation of the Strategy and on the need to update it

7. **provide a broad-based forum** for the purpose of improving cooperation between the different actors and organizations involved in information security.

MINISTRY OF TRANSPORT
AND COMMUNICATIONS FINLAND

The priority projects in 2005

2. Information- secure electronic services

Guiding principle: 'Promoting information-secure PC, mobile phone and digital TV services for the consumer.'

2. Analysis of national information security risks

Guiding principle: 'Correct transmission of the right information will reduce anxiety and uncertainty.'

3. National Information Security Day

Guiding principle: 'Learning about information security begins at school.'

At the same time, the other 17 projects (inc. almost 200 FIN professionals) are arranged into groups, each **supporting** one of the above priority projects.

MINISTRY OF TRANSPORT
AND COMMUNICATIONS FINLAND

One of the priorities in 2004 and 2005

National Information Security Day 2005

Guiding principle: ‘Learning about information security begins at school.’

Finland’s National Information Security Day is **an annual event** held in February.

It is **organized jointly** by various public-sector bodies, private-sector businesses and other organizations.

The purpose is **to increase awareness** of current threats to information security and the practical ways of protecting against these threats.

MINISTRY OF TRANSPORT
AND COMMUNICATIONS FINLAND

ENISA (European Network and Information Society Agency)

- An independent centre of expertise at European level, providing guidance and, when called upon, assistance to the European Parliament, Commission and any competent body appointed by member states.
- to build the ”culture of security”
- to raise awareness and promote best practise on security matters
- to network differend actors in the field of security

LIIKENNE- JA
VIESTINTÄMINISTERIÖ

Tasks:

- Collecting and analysing data on security events and trends
- Providing assistance when called upon
- Promoting risk assesment and risk management methods
- Raise awareness and promote best practise
- Enhance co-operation
- Monitor and track the development of standards

Agency´s tasks should not pre-empt, impede or overlap with relevant tasks conferred on:

the national regulatory authorities

the European standardisation bodies

the national supervisory authorities of the MS relating to protection of individuals with the regard to the processing of personal data

National security which falls into the sphere of III pillar