Study on Emerging Risks

"It takes a brave man or else a fool to predict the future. But without any vision of the future, Man is doomed to act like the proverbial drunken sailor".

Jani Arnell

Expert – Risk Management

Technical Department

Unit Risk Management

www.enisa.europa.eu

ENISA Regulation

(EC No 460/2004 "Establishing the European Network and Information Security Agency")

- "To understand better the challenges in the network and information security field, there is a need for a *Agency to analyse* ***Current and Emerging Risks*** and for that purpose the Agency may collect appropriate information"…
- … ***"Emerging Risks should be understood as issues already visible as possible future risks to network and information security".***

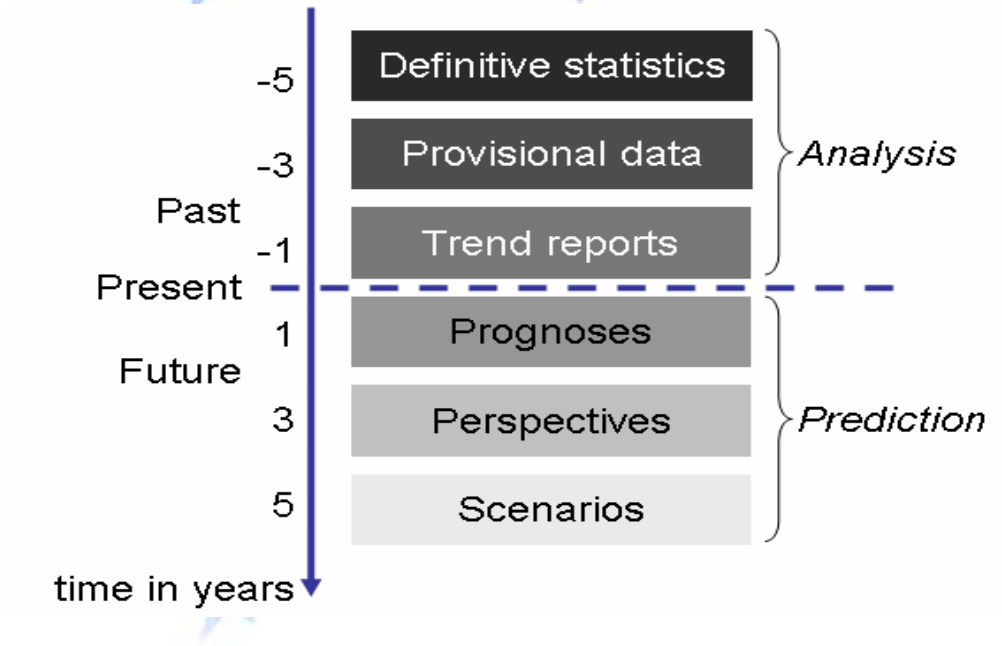
ENISA and Emerging Risks

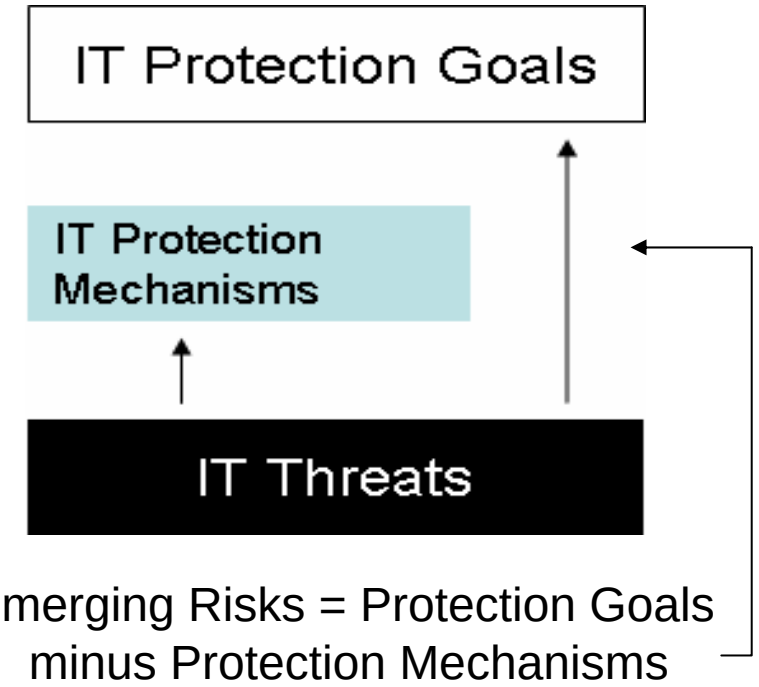
- Which kinds of Emerging Risks there will be in the future?
- Is there a way to identify Emerging Risks?
- Are there methods or tools to assess and/or manage Emerging Risks?
- What are those factors (not only technical) leading to Emerging Risks?
- Are there any suggestions how to gather, handle and disseminate Emerging Risks related information?
- Are there some practical examples of Emerging Risks for different stakeholders?

Study on Emerging Risks

- Initializing study for the upcoming Emerging Risk related work in ENISA
- Helps to understand the Emerging Risks context
- Identifies some future modes of computing
- Preliminary investigation of possible RM/RA methods
- Gives some examples of the future risk scenarios
- Gives overview for the privacy concerns of the future
- Study was made with cooperation of University of Freiburg Germany (Thanks to Guenter and Lutz!)

Assessing Emerging Security and Privacy Risks in IT





Emerging Risks = Protection Goals minus Protection Mechanisms

Layered Risk Model

- In the future IT causes risks on more than just the technical layer

Societal Risks	• Cyper Terrorism, Information Warfare
Business Risks	• Sales and reputation losses
Individual Risks	• Privacy, Phishing, Identity theft
Technical Risks	• Malware, SW Attacks, HW attacks

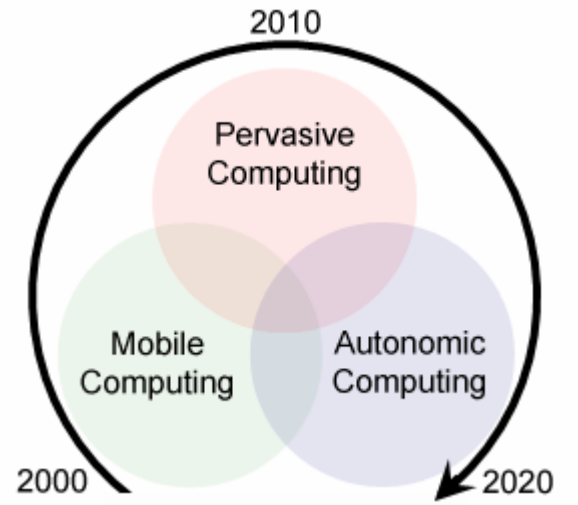
Three Computing Paradigms (1/2)

- The mainframe age: *"Insiders are good, outsiders are bad"*
  - Data storage and processing is realized in centralized manner
  - Whoever is inside the system is considered to be good
  - Outsiders are considered to be bad
  - Concentrated on access control
- The Internet age: *"Look who is talking to whom"*
  - Everybody is considered to be an outsider
  - How to identify good users?
  - Concentrated on Authentication (e.g. Digital Signature and Biometrics)

Three computing paradigms (2/2)

- The Ubiquitous Computing: *"Security xor privacy"*
  - Future systems will connect dynamically and be known "infrastructuless"

Mobile Computing: location free services



Pervasive Computing: mobility + context awareness

Autonomic Computing: heterogeneous, dynamic and decentralized control

Computing paradigms and some of their properties

- Mobile Computing is open but adaptability is only rudimentary, because, typically Network Provider controls security of networks and by that devices.
- Pervasive Computing systems are open and they offer an increased degree of adaptability which results from capturing and processing of context data. Bar codes will be replaced by RFID chips.
- Autonomic Computing has property to be open and being able to adapt changes. Machines interact with machines without human interaction.

George the Security:

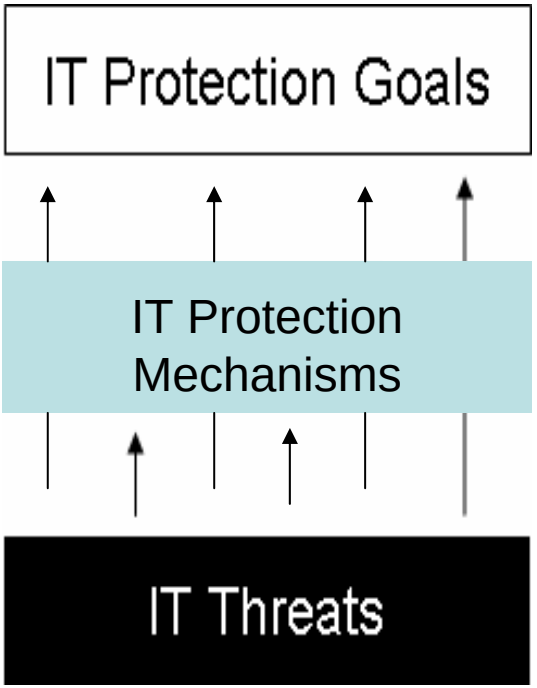
I can still manage this!

How about Privacy?!

Hey come on!, how I can manage this?

Computing paradigms and safeguards

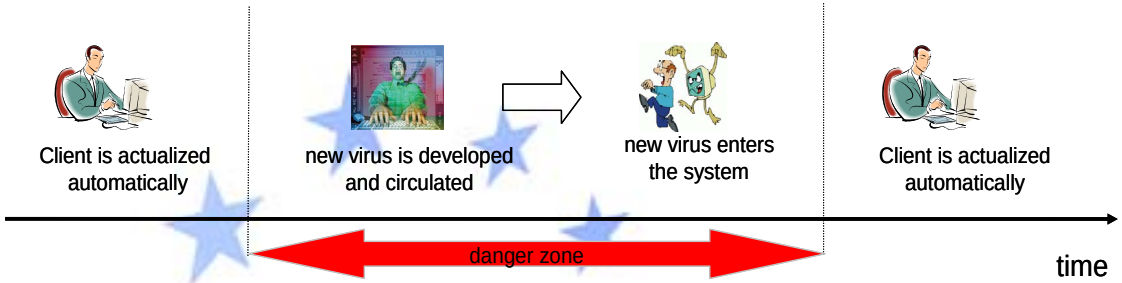
- Computing paradigms have their specific threat and risk-coping protection mechanisms. Mostly though, security and privacy mechanisms have ex-ante perspective
- ***Today's protection mechanisms are insufficient for security and privacy in highly dynamic systems and ubiquitous computing***

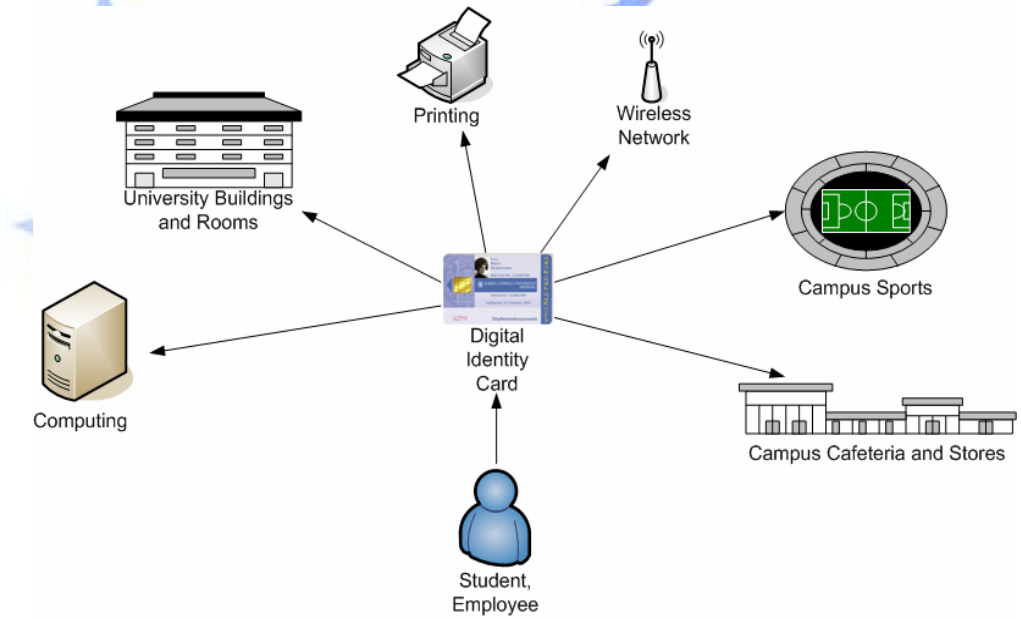


Some examples of the Risk Scenarios in Emerging Computing Modes (1/2)

	Short scenario description	**Used technology**	**Security and privacy problem**	**Estimated realization**
A: "Malware"	Employee Internet access	WWW and email clients, antivirus software	Amount and speed of new malware	Today
B: "ID cards"	ID cards on university campus	PKI, biometric identification	Imperishability of biometric data	In 1-3 years
C: "E-Health"	Electronic health records	PKI, distributed storage	Data collection w/o users consent, delegation of rights	In 2-3 years
D: "RFID-Store"	Personalized shopping in stores	RFID, WLAN, Bluetooth	Massive data collection w/o users consent	In 3-4 years


Username:
Password:


Client is actualized automatically
new virus is developed and circulated
new virus enters the system
Client is actualized automatically
danger zone
time


Printing
Wireless Network
University Buildings and Rooms
Campus Sports
Digital Identity Card
Computing
Campus Cafeteria and Stores
Student, Employee

How to manage Emerging Risks? Example approach (1/2)

- Phase 1: Identification of Security and Privacy Risks
  - Set protection goals for assets
  - Define Attacker model
  - Search vulnerabilities
  - Model Threats
- Phase 2: Quantification of Security and Privacy Risks
  - Estimate potential losses
  - Prioritize threats
- Phase 3: Controlling of Security and Privacy Risks
  - Select protection mechanisms
  - Implement protection mechanisms

How to manage Emerging Risks? Example approach (2/2)

- Phase 4: Monitoring of Security and Privacy Risks
  - Review identification results
  - Review quantification results
  - Review controlling results
  - Create stakeholder report
- Challenges:
  - Validity of the Results of this approach are heavily dependent for the fact how well one is able to build up ***valid scenarios*** (technical expertise, predictions of the future applications and vulnerabilities, possible impacts on future society etc.)

ENISA's Conclusions (1/3)

- With the high degree of openness and adaptability of future IT systems, relevant assets can be hard to detect
- Open and adaptable future systems do not allow for an easy determination of the risks because of the large number of devices
- Statistics are not going to provide support when identifying Emerging threats of future. Analysis must rely more on analytic expertise
- Monitoring becomes more important for future IT systems than it is for current ones.

ENISA's Conclusions (2/3)

Window of opportunity = Short	Window of opportunity = Intermediate	Window of opportunity = Long

Present time

- *Technology exists*
- *Applications exists*
- *Vulnerability exists*
- *Exploits exist or not*
- *RM/RA methods exist*

- *Technology exists*
- *Future applications*
- *Vulnerability exists or not*
- *No exploits*
- *RA/IT methods*

- *Future technologies*
- *Future applications*
- *No RM/RA/IT methods*

Future

Current Risks ≤ 6 months – 1 year	**Emerging Risks** ≥ 1 year – 5 years	**Emerging Risks** ≥ 5 years - 15 years

ENISA's Conclusions (3/3)

- ENISA needs to know what to do next and who has done what (e.g. SWAMI project, SERENITY project). Ongoing project: Roadmap for Emerging Risks (2006)
- ENISA needs to know which kind of information is needed to be able to identify Emerging Risks. On going project: Emerging Risks related Information collection and Dissemination (2006)
- Are there RM/RA methods to assess or manage Emerging Risks? Upcoming project (2007)
- ENISA has to provide Emerging Risks related information to it's stakeholders. Upcoming whitepapers (2007)

Contact Details

Jani Arnell
Expert - Risk Management
jani.arnell@enisa.europa.eu
(+30) 2810 391358

Louis Marinos
Senior Expert – Risk Management
louis.marinos@enisa.europa.eu
(+30) 2810 391359

Thank You!

Questions, please?