

Emerging Risks

<http://dcs.ics.forth.gr>

Emerging Risks in Network and Information Systems Security

Evangelos Markatos
FORTH-ICS, Crete, Greece

in collaboration with
Louis Marinou
ENISA

Roadmap

<http://dcs.ics.forth.gr>

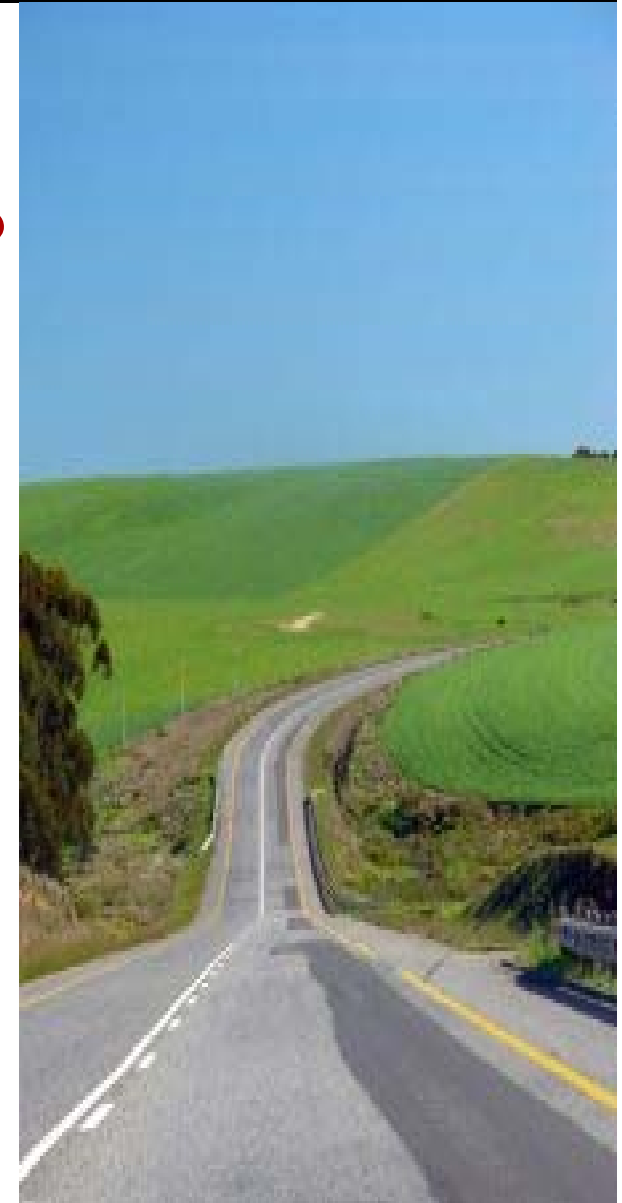
- Motivation
 - Why is this work important?
- Which are the drivers of the emerging threats?
 - Technical Dimensions
 - New Applications
 - Market Trends
- Which are the Risks?
 - Current, Emerging, and Future
- Scenarios
 - Objectives
 - How do you come up with one? Examples



Roadmap

<http://dcs.ics.forth.gr>

- **Motivation**
 - Why is this work important?
- Which are the drivers of the emerging threats?
 - Technical Dimensions
 - New Applications
 - Market Trends
- Which are the Risks?
 - Current, Emerging, and Future
- Scenarios
 - Objectives
 - How do you come up with one? Examples



Motivation

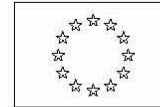
<http://dcs.ics.forth.gr>

- Prepare for the future
- Anticipate the emerging risks
 - you can prepare better
 - you can inform beneficiaries
 - you may be one step ahead in the security “arms race”

A strategy for a Secure Information Society

<http://dcs.ics.forth.gr>

- one of the cornerstones in developing a culture of security is **improving our knowledge of the problem.**
- ... to facilitate effective responses to **existing and emerging threats** to electronic networks...



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, [...]
 COM(2006) 251

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

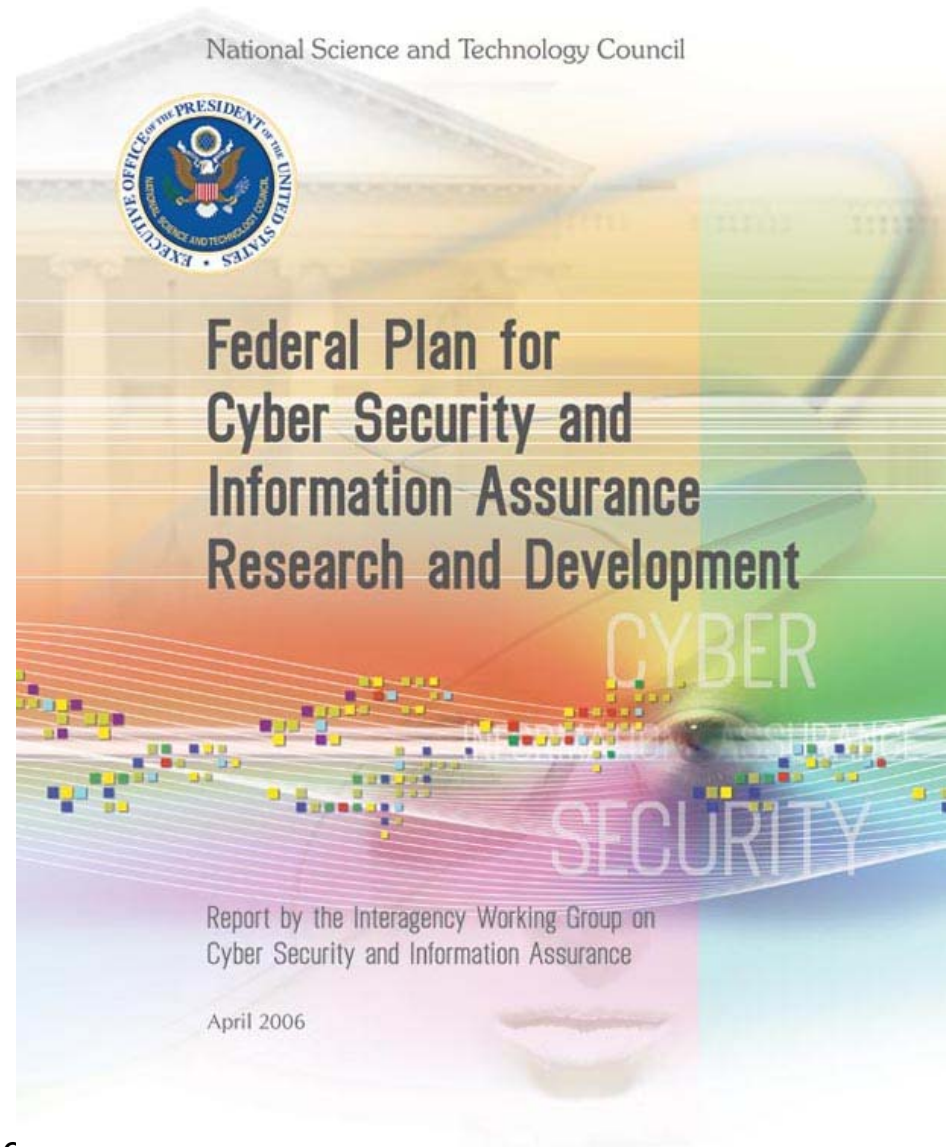
A strategy for a Secure Information Society – “Dialogue, partnership and empowerment”

{SEC(2006) aaa}

Federal Plan for Cybersecurity

<http://dcs.ics.forth.gr>

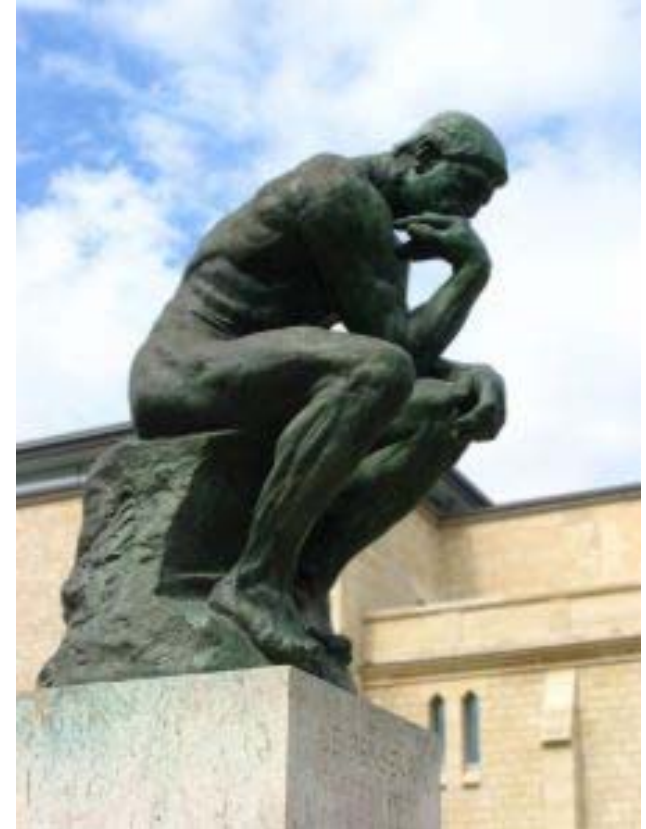
- We need to
 - **Assess security implications of emerging information technologies**
 - Develop and apply **new metrics to assess cyber security** and information assurance
- They found that:
 - Integration of **emerging technologies** into the IT infrastructure increases the breadth of and access to vulnerabilities.
 - **emerging technologies** will present more information than can reasonably be analyzed with existing capabilities.
 - A particularly difficult problem is **finding trends and patterns in attacks**



So...

<http://dcs.ics.forth.gr>

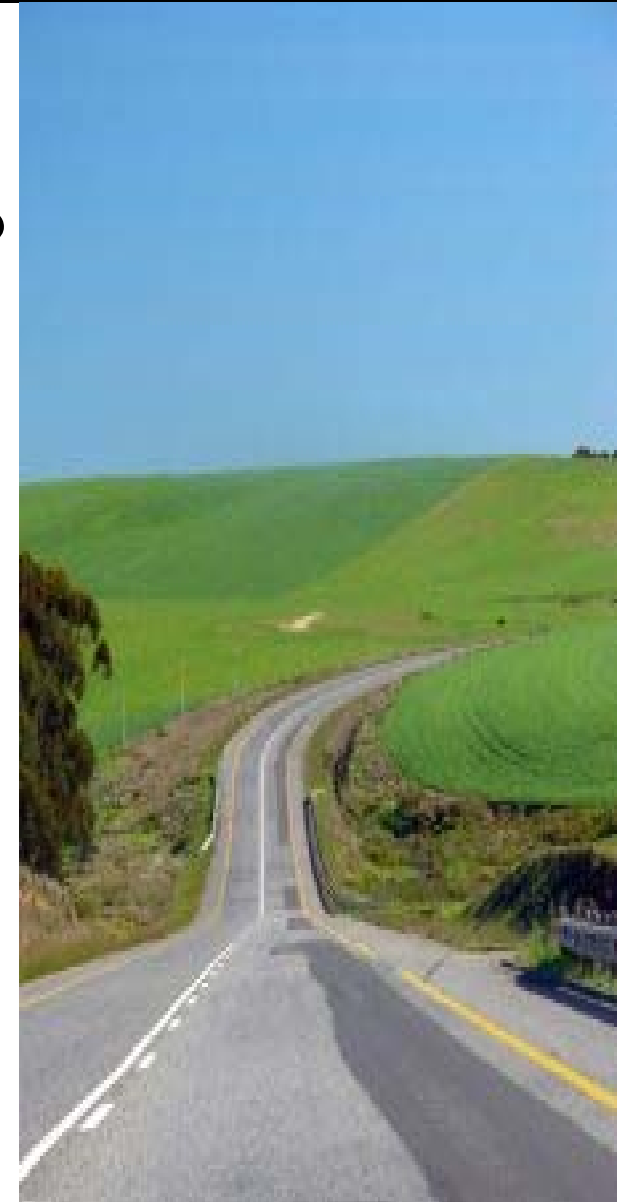
- We need to
- Collect information for
 - Current,
 - Emerging, and
 - Future threats and vulnerabilities in
 - Network and information systems security
- Current threats: now
- Emerging threats: next 3 years
- Future threats: 3 years after that



Roadmap

<http://dcs.ics.forth.gr>

- Motivation
 - Why is this work important?
- Which are the drivers of the emerging threats?
 - Technical Dimensions
 - New Applications
 - Market Trends
- Which are the Risks?
 - Current, Emerging, and Future
- Scenarios
 - Objectives
 - How do you come up with one? Examples



What drives emerging threats?

<http://dcs.ics.forth.gr>

- Technical Dimensions
 - What will be the technologies of the future?
- Application Dimensions
 - What will be the applications of the future?
- Future Market Trends and Dimensions
 - What are the trends in the market?



Drivers: Technical Dimensions

<http://dcs.ics.forth.gr>

- Which technical dimensions drive future threats?
 - Wireless Networks
 - Wireless networks could potential be eavesdropped
 - Wireless devices may become more transparent
 - Less visible – more integrated with other appliances
 - Proliferation of Broadband Networks
 - i.e. **compromised computers have more firepower today.**
 - e.g. a 1 Mbps DSL computer can send
 - 10 Gbytes of information per day
 - One million (1,000,000) SPAM email messages
 - 10 million attack packets
 - 10 years ago a computer on a 28.8Kbps modem
 - Had two-three orders of magnitude less firepower



Drivers: Technical Dimensions (II)

<http://dcs.ics.forth.gr>

- Which technical dimensions drive future threats?
 - Device miniaturization
 - Devices will not remind of a traditional computer
 - They will be integrated into other devices (doors, kitchens, etc.)
 - They may not run (properly configured) protection software (e.g. Antivirus)
 - Digital identities (e.g. RFID)
 - More products will have a digital ID
 - People will frequently carry (or wear) products with digital IDs
 - Digital ID readers will proliferate (in public buildings, etc.)



Drivers: Applications

<http://dcs.ics.forth.gr>

- Smart Mobile Phones
 - Eavesdropping, Loss of privacy, stalking
- E-banking, e-commerce, e-everything
 - Financial loss, attacks to banking system, attacks to the stock market, etc.
- Smart Home – Aml
 - Lots of wireless potential vulnerable devices
- Smart Vehicles
 - What if the computer that controls the brakes is compromised?



Drivers: Applications (II)

<http://dcs.ics.forth.gr>

- E-health
 - What if the computer which controls a medical device gets compromised?
 - What if our medical record is stored in a compromised computer?
- E-government
 - More and more of our personal information will be stored on-line
- Blogs
 - Blogs encourage people, including minors, to publish their information on the web
 - This may be used for stalking today
 - It may be used to invade their privacy, etc.



Drivers: Future Market Trends and Dimensions

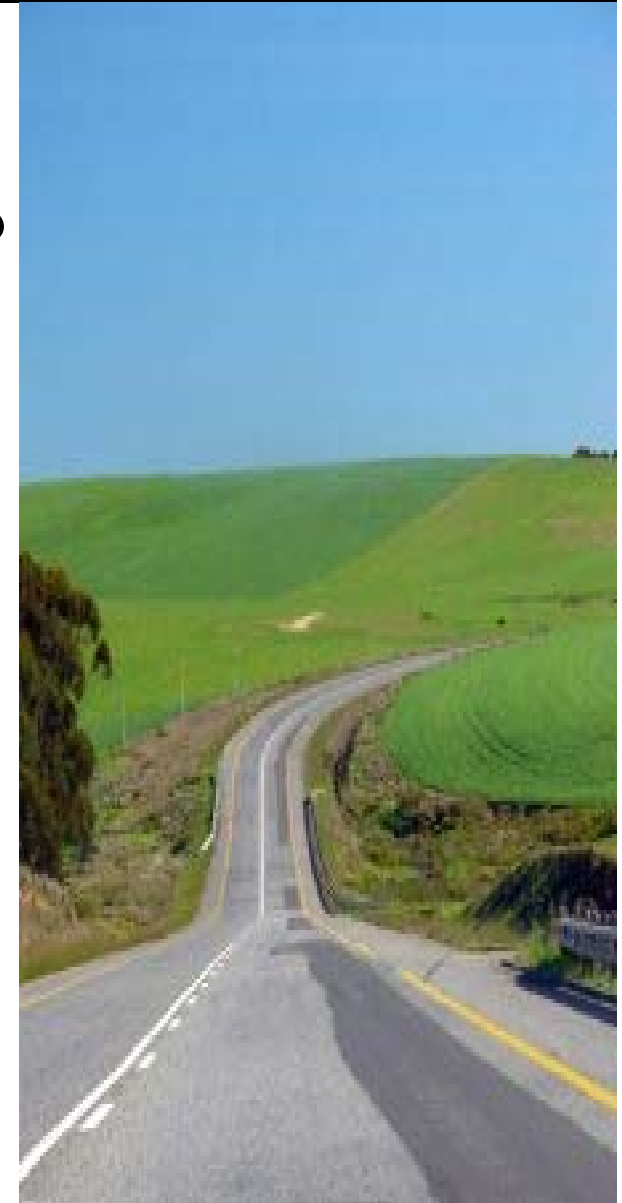
<http://dcs.ics.forth.gr>

- **On-line services will become more common**
 - Online services: commerce, entertainment, news, etc.
 - Even a “second-life” is possible on-line
- **Mobile phone use will prevail**
 - People are “on the go” – mobile phones are needed to support our mobile world
 - Much like electricity supports industrialized nations
- **Service-oriented information society**
 - European Economy moves away from “traditional products” and steps into new forms of “services”
 - The Internet enables these services to be composed to create even fancier ones
 - E.g. find a doctor who has an opening at a date a time compatible with your schedule and your mother’s schedule and who is located nearby

Roadmap

<http://dcs.ics.forth.gr>

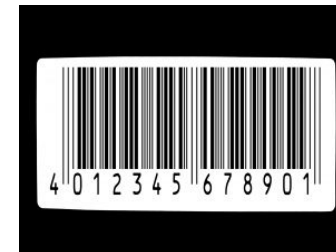
- Motivation
 - Why is this work important?
- Which are the drivers of the emerging threats?
 - Technical Dimensions
 - New Applications
 - Market Trends
- Which are the Risks?
 - Current, Emerging, and Future
- Scenarios
 - Objectives
 - How do you come up with one? Examples



Current Risks

<http://dcs.ics.forth.gr>

- SPAM
 - to email addresses, phones, etc.
- Botnets
 - “zombie” computers
- Phishing
 - Using more means (phones, SMS)
 - More targeted
 - (“Hi Pal. We met at the IST conf. Let me tell you about...”)
- Identity theft
 - Login/password
- Route hijacking
 - Divert/Intercept traffic from the Internet
- Instant Messaging
 - Chat, etc. SMS, etc.



Current Risks

<http://dcs.ics.forth.gr>

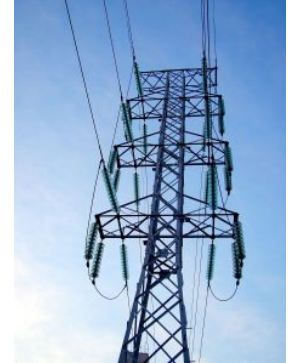
- Peer-to-peer systems
 - File sharing systems
 - Download malware
- Malware on Cell Phones
 - Through SMS, MMS, (free) games
- Hackers in Stock Market
 - Through compromised bank accounts
- Software Vulnerabilities
 - Software is getting larger and more complex
- No protection (e.g. antivirus) in some devices
 - Mobile phones
 - Printers,
 - Refrigerators, kitchens, stoves, etc.



Emerging Risks

<http://dcs.ics.forth.gr>

- SCADA
 - Supervisory Control And Data Acquisition
- Increased home automation
 - A hacker may penetrate the computer which controls the front door
- Massive collections of personal data
- Invisible data collection in public places
- Invisible data collection in private premises
- Security is more an art rather than a science



Emerging Risks (II)

<http://dcs.ics.forth.gr>

- DoS attack to the home telephone
 - Image hackers/SPAMers calling all the time on the telephone
- Hacking home heat and/or air-conditioning system
 - Turn on/off the stove while the owner is away...
- Internet users are younger, less experienced, and more prone to targeted attacks
- Internet users may not have strong motives to clean up their compromised computers
- Malware over multiple networks (GSM, GPRS, Internet, Bluetooth)



Future Risks

<http://dcs.ics.forth.gr>

- **Manageability**

- Currently we manage a few digital devices:
 - Computer, PDA, mobile phone, laptop
- In the future we will have 10's if not 100's of such devices most of which will be hidden



- **Over-use of ICT**

- People use ICT even when not needed
 - They send email instead of talking to people
 - They use e-voting systems when traditional “raise your hand” votes work just fine
 - Such approaches open the road to cyber attackers



- **Use home appliances to attack infrastructures**

- Use thousands of compromised phones to jam the telephone network
- Use thousands of compromised Air-conditioning units to overload the electric power GRID



Roadmap

<http://dcs.ics.forth.gr>

- Motivation
 - Why is this work important?
- Which are the drivers of the emerging threats?
 - Technical Dimensions
 - New Applications
 - Market Trends
- Which are the Risks?
 - Current, Emerging, and Future
- Scenarios
 - Objectives
 - How do you come up with one? Examples



Scenarios: Objectives

<http://dcs.ics.forth.gr>

- Goals:
 - Present easy to say story
 - Set the stage by an example
 - Explain
 - Who may be the victims?
 - Who may be the attackers?
 - What is the magnitude of the attack?
 - Is there any way we could have prevented it?



Scenarios: How do you come up with one?

<http://dcs.ics.forth.gr>

- Think...
 1. Ask “what if” questions
 - “What if an attacker manages to compromise X?”
 - “What if an attacker manages to get my login and password for my bank”
 - She would be ample to empty my bank account
 2. Combine them with real-life events
 - “What of an attacker manages to compromise X at a time of Y?”
 - What if an attacker manages to get my login and password for my bank at the time of my Christmas bonus?”
 - She would be able to get more money

Scenarios: How do you come up with one? II

<http://dcs.ics.forth.gr>

3. Explore the dimension of scale

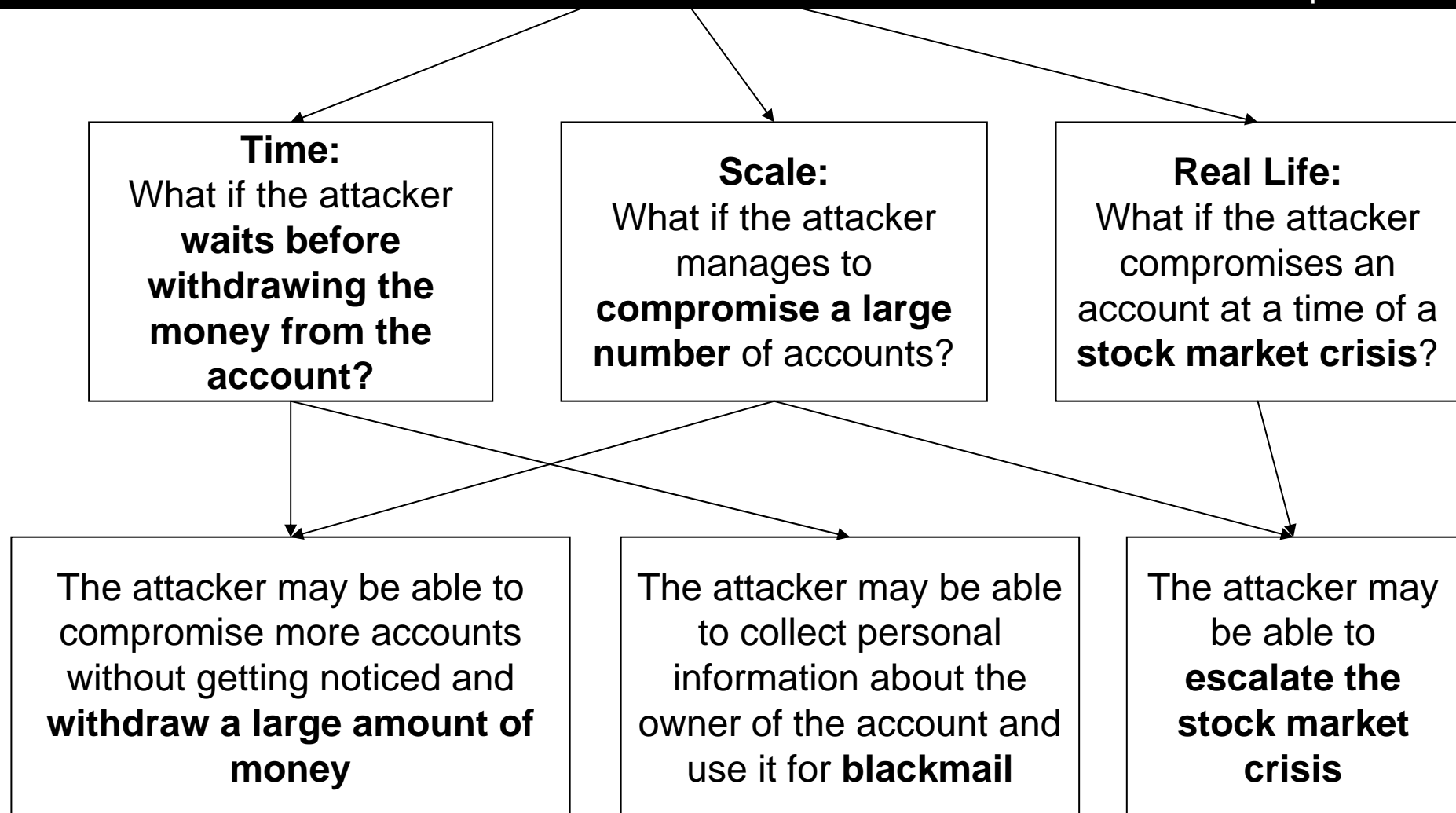
- “What if an attacker manages to compromise X?”
- “What if an attacker manages to compromise lots of Xes?”
 - e.g. “what if an attacker manages to compromise 1000 bank accounts?”
 - She may be able to steal 1000 times more money
 - She may be able to shutter the credibility of the bank
- “What if an attacker manages to compromise lots of accounts in several different banks”
 - She may be able to undermine the credibility of the banking system



Bank Compromization:

What if an attacker manages to **compromise** one bank account?

<http://dcs.ics.forth.gr>



Scenario I: Stock Market Manipulation

<http://dcs.ics.forth.gr>

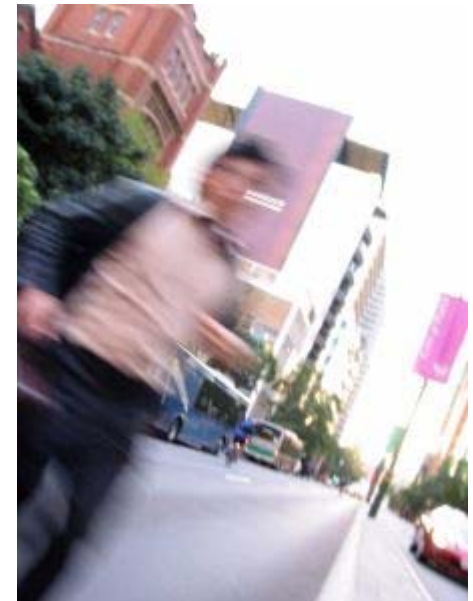
- **Mr Smith subscribes to an stock-market alerting SMS service** which informs him of promising stock
- One day **he received an alert for a large rise in OILUC** (Oil United Consortium) and he decided to immediately sell some of his OILUC stock through his mobile phone.
- The day after he realized that there was no rise in the price of OILUC
- Actually **thousands of people sold their OILUC stock at rock bottom price as a result of the fake SMS messages** they received



Scenario I: Stock Market Manipulation

<http://dcs.ics.forth.gr>

- Dimensions of the problem
 - Phishing:
 - Mr Smith received a fake SMS for an alleged increase in his stock
 - m-banking
 - Mr. Smith was able to sell stock via his mobile phone
 - Mobile way of life
 - People “on the go” make important financial decisions without having the time to thoroughly double-check them



Scenario II: Bank Crash

<http://dcs.ics.forth.gr>

- John Cracker managed to get the personal data (names, phones, and email addresses) of 100.000 customers of the Western European Credit Bank
- He sent a phishing email to half of them inviting them to check out the alleged new features of the web site of the bank.
- John managed to collect usernames and passwords for about 500 accounts.
- Then he launched a double attack:
 - He **robbed the accounts**
 - He **send the telephone numbers of the victims to reporters** alerting them of the fact



Scenario II: Bank Crash

<http://dcs.ics.forth.gr>

- Most of the victims **found themselves learning about the phishing scam live on the evening news.**
- The impact was so huge that **all the bank's customers demanded to withdraw their money.**
- To avoid crashing, next day the bank remain closed until people calm down.
- Then John released the second part of his attack.
- He sent email to the rest of the bank's customers seemingly on behalf of the Bank president where he:
 - Apologized for the problem
 - Told them that although the bank is closed, the web site of the bank is open and that through it they can transfer their money to an account of their choice...

Scenario II

<http://dcs.ics.forth.gr>

- Dimensions of the problem:
 - Phishing
 - The customers of the bank were tricked by email messages
 - E-banking
 - People used e-banking to transfer money
 - The media
 - The extend of the problem was aggravated by the media and this eventually resulted in panic
 - Two-phase attack
 - The first phase creates panic through a small number of compromised accounts
 - The second phase harvests more money from people in panic



In closing...

<http://dcs.ics.forth.gr>

- The dimensions that drive emerging risks are:
 - New technology
 - Wireless networks, residential broadband networks, device miniaturization, etc.
 - New applications
 - Mobile phones, e-banking, e-government, etc.
 - Social Engineering
 - Phishing, etc.
- We need to
 - Understand the dimensions of the problem
 - Work towards addressing current, emerging and future risks.

Emerging Risks

<http://dcs.ics.forth.gr>

Emerging Risks in Network and Information Systems Security

Evangelos Markatos
FORTH-ICS, Crete, Greece

in collaboration with
Louis Marinou
ENISA

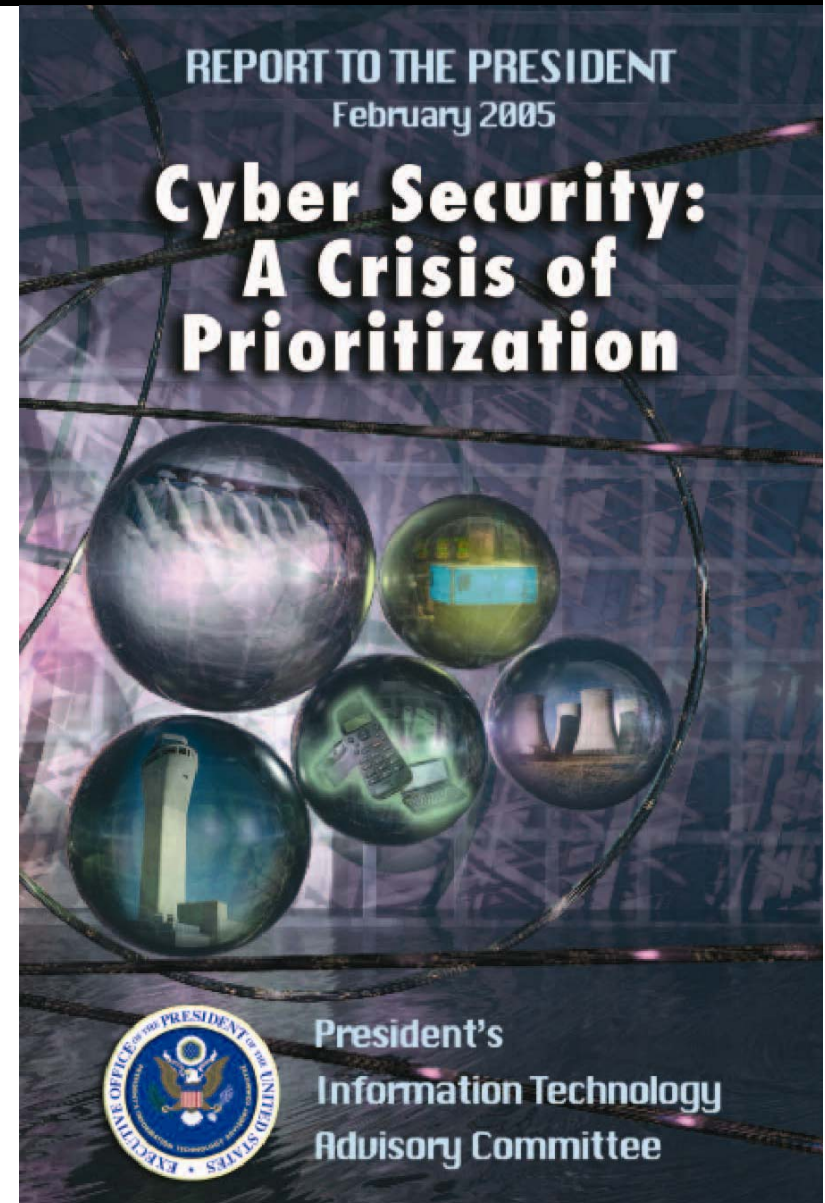
Back up Slides

<http://dcs.ics.forth.gr>

PITAC's Report

<http://dcs.ics.forth.gr>

- 2005 US Report Findings:
 - Funding for fundamental research in civilian cyber security should also be substantially increased at other agencies, most notably DHS and DARPA.
 - As a result, the PITAC recommends that the Federal government strengthen its **cyber security technology transfer partnership with the private sector**.
 - Specifically, the Federal government should place greater emphasis on the **development of metrics, models, datasets, and testbeds so that new products and best practices can be evaluated**;



Things to remember

<http://dcs.ics.forth.gr>

- What is the most important thing I would like you to remember
 - **P**rivacy
 - **P**ervasiveness
 - ICT **I**ntegration
 - Social **E****N****G**ineering
 - **PPING**

Scenarios (III)

<http://dcs.ics.forth.gr>

- Exploit both scale and real-life events
 - What if an attacker manages to compromise one traffic light?
 - She may be able to obstruct traffic in one intersection
 - She may even cause accidents, which will obstruct traffic even further
 - What if an attacker manages to compromise several traffic lights?
 - She may be able to obstruct traffic in a whole city
 - What if an attacker manages to compromise several traffic lights during rush hour?
 - She may create chaos

