Managing Emerging Threats in ICT Infrastructures

Motivation

forward

- Security research in Europe is fragmented
- ICT security is a complex field
  - involves many domains and changes rapidly
  - affects systems outside the network
- forward is a coordination action to bring together
  - academics,
  - industry, and
  - policymakers …

  who are interested in emerging threats to ICT infrastructures

Motivation

forward

- The security research community is ill-prepared to deal with new types of Internet threats
  - It takes time for experts to come together, study the problem domain, form alliances, obtain funding ...
  - It takes even longer before practical solutions are developed
  - All too often, the response comes too late
- There is a clear gap between academic and industrial security research

The Flash Worms Example

forward

- The first years of the millennium were characterized by the spreading of fast, loud, and destructive worms
  (Code Red I/II, NIMDA, Slammer, Blaster...)
- Millions of Euros were spent on research projects to develop defense mechanisms against flash worms
- By the time the first solutions were proposed, malware writers had already shifted their focus to more stealthy and sneaky attacks (botnets)

We Need to Look Forward

forward

- Which trends in technology are likely to lead to new types of attack?
- What is the nature of such attacks?
- What would be needed to address the problem?
- Which groups are active in a particular field and how can we bring them together?

Forward Consortium

forward

Industrial Advisory Board

forward

Atos Consulting
Combitech
Deutsche Telekom Labs
Ericsson
Forthnet
France Telecom
Hispasec Sistemas
Ikarus Software
Lindholmen Science Park
Secode
VirtualTrip
Volvo

Main Objectives

forward

- Organize workshops
  - bring together players for face-to-face exchange
  - foster community building
- Establish working groups
  - focused effort to perform deep analysis of different ICT threats
- Set up community platform
  - continuous review of threat landscape and dissemination of results
- Compile threat scenarios
  - summarize working group findings
  - outline future research roadmaps (white book)

Website & Workshop

forward

- Website (www.ict-forward.eu)
  - Project objectives and results
  - Public wiki
  - Forward blog

- First workshop
  (co-located with the “Threats on the Internet” seminar)
  - 61 attendees (27 from industry) and 30 presentations
  - working group topics:
    - Smart Environments
    - Malware & Fraud
    - Critical Systems

Smart Environments

- Ubiquitous networking and device mobility is changing the threat landscape that users and organizations have to face
- Analyze upcoming threats in the areas of wireless networks, ambient intelligence environments, cellular telephony, vehicular networks, RFID, network monitoring

Smart Environments

forward

- Threats to privacy
  - How do you protect users from being tracked?
- Security in smart devices
  - How do you define security policies for mobile devices, home appliances, and sensors?
- Threats to and from wireless networks
  - How do you protect the countless wireless networks that are emerging?
- Cross network attacks
  - How do you protect the Internet infrastructure from malicious mobile hosts?

Malware & Fraud

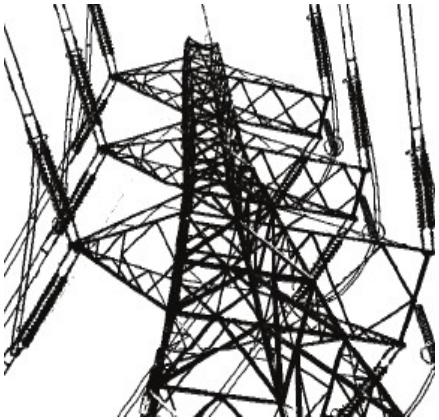
- The activities of malware authors and online fraudsters have converged, creating a vibrant and dangerous underground economy
- This underground economy is responsible for the tremendous increase of criminal activity on the Internet, the resulting significant financial losses to companies and end users, and the decrease of trust in the security of online transactions

Malware & Fraud

forward

- Spreading of malicious code
  - What are the malware emerging propagation vectors?
- Malware code
  - What techniques are used to develop malware?
- How does malware thwart detection and analysis?
  - How is malware used once a machine is infected?
- Information gathering
  - Which information is interesting for criminals and how is this information obtained?
- Exploiting information and control
  - What are the schemes to convert information into profit?

Critical Systems



- Discuss society's dependence of critical infrastructures and the consequences of disruption of the services from these infrastructures
- Identify the possible reasons for such disruption and how to guarantee that the critical services are continually and correctly delivered

Critical Systems

forward

- Internet is by far the most critical system in society. The implications of this must be investigated
- How do we deal with terrorist action?
- How should we cope with cascading effects between different systems?
- What kind of data can we gather that would help us draw the right conclusions?
- Critical infrastructure protection is not only technical
  - Cooperation between authorities
  - Information dissemination
  - Training
  - Planning for recovery actions