forward

Future and Emerging Threats in ICT

www.ict-forward.eu

Edita Djambazova

Institute for Parallel Processing

Bulgarian Academy of Sciences

Description

ICT-FORWARD is a Coordination Action that aims at promoting collaboration and partnership between researchers from academia and industry involved in the protection of ICT infrastructures against cyber threats.

Consortium

TU WIEN
Technische Universität Wien
Vienna University of Technology

Tekniska Högskola · Chalmers · Göteborg

EURECOM
Sophia Antipolis

IPP BAS

vrije Universiteit amsterdam

FORTH

Motivation

- Security research in Europe is fragmented.
- **FORWARD** is a Coordination Action aimed at bringing together academics, industry experts, and policy makers who are actively working on addressing emerging threats in ICT infrastructures.
- ICT is a complex field that involves many domains and affects systems outside the network.
- The ICT landscape is rapidly and constantly changing.
- To counter the emerging and future ICT threats there is need for coordinated research activity and multi-domain cooperation.

Objectives

forward

- Establish focused ***working groups*** to perform in-depth analysis of emerging and future ICT threats.
- Set up a ***community platform*** to enable continuous review of threat landscape and disseminate the results.
- Foster community building by organizing face-to-face ***workshops*** involving leading experts in the field.
- Compile threat scenarios to summarize the working group findings and outline future ***research roadmaps***.

FORWARD's activity

forward

- Working groups:
  - Malware and Fraud
  - Smart Environments
  - Critical Systems
- Workshops
  - First FORWARD Workshop in Goteborg, Sweden, April 2008
  - Second FORWARD Workshop in Saint-Jean-Cap-Ferrat, France, May 2009
- In-person meetings, teleconferences, mailing lists
- Dissemination through dedicated panels at security-related events, newsletters and papers
- Web site and blog

Threat identification procedure

forward

- First FORWARD Workshop, 60 experts from academia, industry, and government
- Three working groups, including field experts, communicating through mailing lists, teleconferences, in-person meetings of each WG
- Discussions on the emerging and future threats
- Threat lists delivered by each working group
- Discussions on the identified threats at the Second FORWARD Workshop, feedback from 100 experts
- Consolidated threat list

Threat identification procedure 2

forward

- Ranking of threats by impact, likelihood, awareness, R&D needed
- Threat scenarios to demonstrate how a threat could actually be materialized
- White book with realistic threat scenarios
- Research roadmap

Working groups

- **Malware and Fraud.** Malware and fraud-related threats on the Internet. Topics range from novel malware developments over botnets to cyber crime and Internet fraud.
- **Smart Environments.** Ordinary environments that have been enhanced by interconnected computer equipment. There is general expectation that a large number of small devices such as sensors and mobile phones will be interconnected.
- **Critical Systems.** Critical systems whose disruption of operation can lead to significant material loss or threaten human life.

Threat drivers

- **New technologies:** Technical advances that provide new functionality. By extrapolation we can foresee much faster networks (both wired and wireless), a substantial increase in parallelism (multi-core machines), and better energy and battery technology. Also, computing devices will become increasingly smaller and cheaper. As a result, they will become more widespread and they can support more and richer applications.
- **New applications:** Completely new uses of technology, uses that typically did not exist before or do not have a counterpart in the real world. Social networks, tools that have rapidly reached a significant fraction of the population and that support social interactions among large user groups. Software as a service. Applications are hosted by providers on a large-scale computing infrastructure, such as a cloud. This deployment and computing model is profoundly different from the traditional client-server model, and thus, we need to consider its security implications.
- **New business models:** Certain services or applications that might exist already in some form increasingly start to rely on a working ICT infrastructure. For example, online shopping, online banking, and even e-government.
- **New social dynamics and the human factor:** Possible changes in the way that people approach and use technology and certain applications.

Threats list

forward

- Hardware security and threats
- Outsourcing
- Cyber physical systems
- Cyber warfare
- Attacks against virtualization
- IPv6 and direct reachability of hosts
- Advanced botnets
- Naming, the role of domain registrars, fast-flux networks
- Attacks against the network backbone and infrastructure
- Abuse of social network privacy and trust in online communities
- Underground economy
- Attacks against the financial sector/banks
- New vectors to reach victims
- Targeted attacks, spear phishing
- 'Smart' phones and braindead zombies
- RFID-related threats
- Threats due to malicious hardware
- Threats due to false sensor data
- Threats to system maintainability and verifiability
- Attacks on office equipment that is not a traditional computer
- Threats to home automation
- Threats to aviation security
- Multicore-related threats.
- Threats to the wireless plane
- Privacy threats: spyware in the bedroom
- Threats due to scale
- Valuable Resources in Online Gaming

Threats list (cont.)

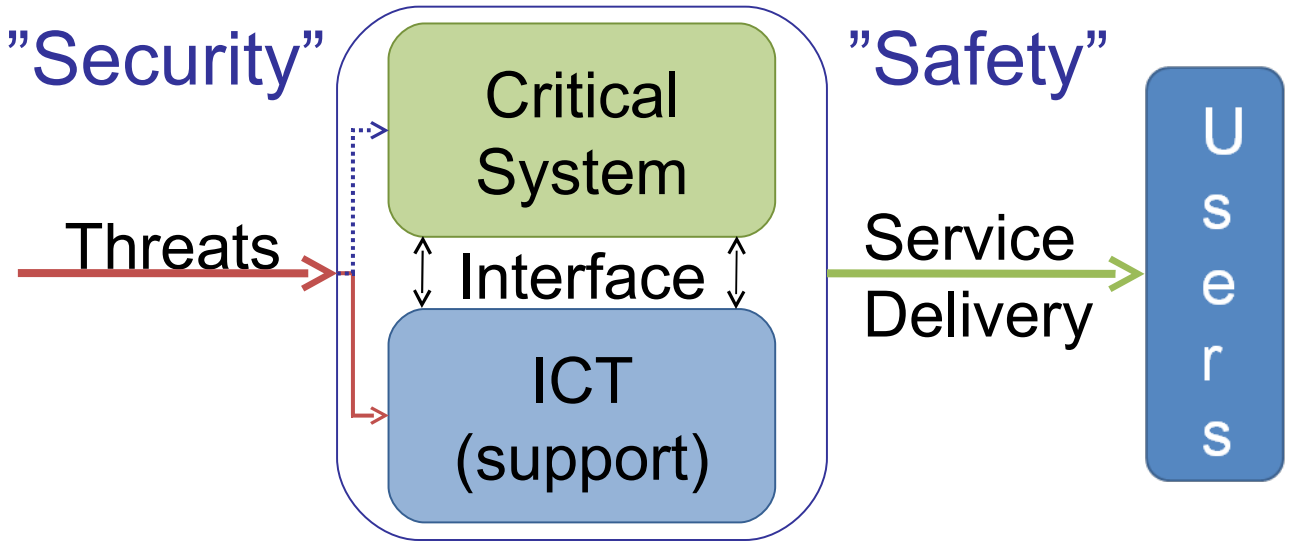
forward

- Sensors as the “New Computing Class”
- New Generation Networks bring new security challenges
- Wireless communications in critical industrial applications
- Unforeseen cascading effects
- Hidden functionality
- Retrofitting security to legacy systems
- The use of COTS components and systems
- Safety takes priority over security
- The human factor
- The insider threat to critical infrastructures
- Cultural differences between control and security communities

Scope of the Critical Systems Working Group

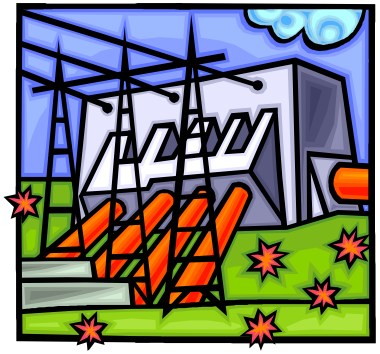
forward

- Critical Systems working group considers the special requirements of ICTs when applied to critical systems and critical infrastructures.

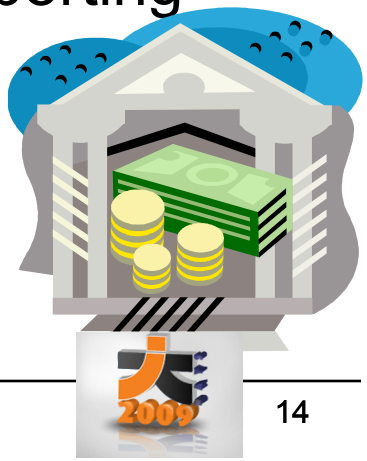


The service delivery must not be interrupted

Examples of critical systems



- ***"Traditional" critical infrastructures***
  - electricity, water, telecommunications, etc.
- ***SCADA systems***
  - Used in almost all Critical Infrastructures
  - Efforts are already ongoing to protect such systems
- ***Financial systems*** are critical infrastructures that are hardly distinguishable from their ICT supporting component.
  - Many access points
  - Availability to many and diverse users



“Emerging” critical systems

forward

- ***Data centers*** are becoming common and these can be seen as CIs in that they provide data necessary for more traditional CIs
(Ex. future air traffic management, cloud computing, etc.)

- ***In-vehicle automation*** and ICT, with remote diagnostics and software updates for vehicles.
  - Embedded (automobile) systems connected to open networks.
  - Some of the problems related to any embedded system are also valid for the ***connected car***.

Sensor networks

- The convergence of control with communication and computation will make sensor networks the new dominant “computing class.”
- This computational shift is going to bring a big shift on computer security issues.
- Common security mechanisms may not be applicable because of limited resources.
- An attacker can have much more powerful hardware and software than the nodes being attacked.

New Generation Networks

- The general idea behind NGN is that one network transports all information and services (voice, data, other media) by encapsulating them into packets.
- Openess and easy access of these non-regulated networks lead to an increased number of vulnerabilities, something that calls for large attention to security.
- NGN is designed to meet complex requirements, which complicates security architecture.
- Security solutions will differ from those of ”normal” networks.

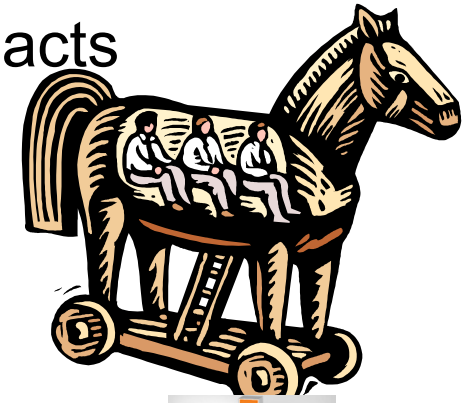
Wireless communications in critical industrial applications

forward

- Today, wireless communications are not yet widely used for closed-loop control.
- Compelling technology because of its many advantages: operator mobility, safety, access security for visualization and optimization, and the immediate benefits of their deployment.
- Prediction that within 10 years, even critical control communications will be wireless.

Hidden functionality

- One threat of paramount importance is that of hidden functionality in systems, and in particular, in software (e.g. secret/undocumented entries to a system).
- Insertion vector is unknown and its existence difficult to verify.
- This functionality is totally uncontrolled and can lead to a large range of very detrimental impacts on the system.



Retrofitting security to legacy systems

forward

- Security can seldom be retrofitted to an existing system, but economical constraints might still make this necessary.
- A better understanding is needed of how to best adapt security to such systems. Analysis of what new features can be added without unnecessary risk. Study the dependability of the different parts.

Use of COTS components

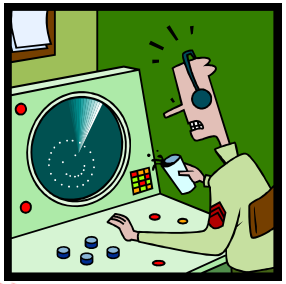
- Commercial Of The Shelf (COTS) components could be general-purpose or specialized software/hardware that is built separately of the system. Used in critical applications to reduce cost and time for design.
- Use of COTS components in a context never intended for them.
- Compositional effects of putting COTS systems together have never been tested.
- The designer has no real control over the product he is introducing into his system.
- There is no guarantee that there is no hidden functionality.
- Use COTS components with some fault-tolerant approaches (replication, diversity approach); apply only in non-critical areas; manage heterogeneity; use of compact and trusted application base.

Safety takes priority over security

- In the domain of critical systems both safety and security are important but in certain scenarios, safety takes priority.
  If the underlying process is about to become critical, security should not block or delay appropriate remedies or counteractions.
  - Should there be a fail-safe system that disables the security (e.g. password requirement) at the local console when parameters in the system indicate a catastrophic event?

- A better understanding of the domain for the IT security experts is necessary.

The Human factor



- Human is considered to be the weakest point in a critical system. The roles include operators in control rooms, engineers taking technical decisions, managers and decision-makers for future strategy development.

- Education and training, raising awareness of security risks; sound and evolving security policy; modeling the user (“cognitive modeling”) and user-interactive properties. Rely on automatic procedures!

The insider threat to critical infrastructures

forward

- Insiders are employees with experience of and knowledge about the CS.
- Attacks of this kind have already taken place.
- Some interesting results from a study on the insider threat show that a negative work-related event is most likely the trigger to most insiders' attacks.
- Effective strategies for discovering an "insider" is an open research question.

Conclusions

- We have identified ***a number of threat areas*** that need further attention.
- We will scrutinize the final list of threats and describe some ***threat scenarios and research directions*** to counter the threats.
- The results will be published in a ***white book*** to be presented at the end of the project.
- We would like to capitalize on the large group of experts gathered by FORWARD to build a strong ***security research community*** in Europe.