Forskning inom datasäkerhet
Tomas Olovsson

Facts and Figures

• Employees at department: 160
  – Faculty members: 75
  – PhD students: 70

• Full time students: 1100 (360 GU)
• 120 courses at 20 programmes
• Thirty nationalities represented
Research Groups

- Algorithms
- Bioinformatics
- Computer Architecture
- Computer Graphics
- Communications and Computer Networks
- Computer Security
- Dependable Real-Time Systems
- Distributed Computing
- Embedded and Networked Processors
- Formal Methods
- Functional Programming
- Language Technology
- Programming Logic
- Software Engineering
- Telecommunication Theory
- VLSI Circuit Design

Networks and Systems security group

Erland Jonsson  Tomas Olofsson  Philippas Tsigas  Marina Papatriantafilou  Magnus Almgren

Wolfgang John  Elad Schiller

Asrin Javaheri  Farnaz Moradi  Laleh Pirzadeh  Pierre Kleberger  Andreas Larsson  Zhang Fu
Security Arena Lindholmen
Forskning och Utveckling i TRIPLE HELIX-miljö

- Akademi
- Industri
- Samhälle

European Network of Excellence in
Managing Threats and Vulnerabilities in the Future Internet

- A Network of Excellence (2010-2014) to work towards solutions and collaborate
- European level
  - Poli. di Milano (IT)
  - Vrije Universiteit (NL)
  - Institute Eurecom (FR)
  - IPP (Bulgaria)
  - TU Vienna (Austria)
  - Chalmers U (Sweden)
  - UEKA (Turkey)
  - FORTH – ICS (Greece)
- and with international colleagues around the world
- Focus
  - Research into malware & fraud, smart environments, and cyber attacks
  - Develop a curriculum for system security, and
  - Report and describe large threats in a yearly report.

http://www.syssec-project.eu/
Security projects at Chalmers

- Quantitative modeling and evaluation of security
- Security and dependability modelling
- Intrusion Detection Systems
- Intelligent security logging and monitoring
- Programming language support for security
- Formal methods for programming languages
- Malicious Internet traffic (attacks, spam, ...)
- Denial of Service mitigation techniques
- Secure sensor networks
- Decision support systems
- Safety and Security in transport systems
- ...

Security Metrics and Modelling

Erland Jonsson
Laleh Pirzadeh
(Vilhelm Verendel)
**What is the problem?**

- **Reliability:**
  - Own research field
  - Deals with random events – failing components, etc.
  - Can with good precision predict how and when a system fails
  - MTTF: Mean time to failure

- **Security:**
  - No randomness in events
  - Events are malicious
  - The presence of just one vulnerability can be enough for an attacker
  - Attacks can be tested off-line
  - No measure for security. Certifications and standard compliance used instead

---

**System-related Security Metrics**

Metrics are decomposed into protective, behavioural and correctness:

- A **protective metric** describes the ability of a system to resist attacks during operation.
- A **behavioural metric** describes to what extent the system delivers its service to its authorized users and denies service to non-authorized users.
- **Correctness** describes how correct a system is wrt to some reference (very hard).
Network defence against spam

Farnaz Moradi
Tomas Olovsson
Philippas Tsigas

Why Do We Care About Spam?

- Today, as much as 90% of inbound email is spam
  - More than 120 billion spam messages is sent per day
- Estimated cost of spam in 2007 was on order of $100 billion
What Is Our Goal?

- Traditional methods remove spam after it has been received
  - Spam identification software requires large computational resources

- Goal: Provide network-based protection
  - Stop spam as close to its source as possible
  - To be implemented in small networked devices

- Method:
  - Study spam characteristics
  - Network-level data
  - No inspection of contents should be needed
  - *Use social network techniques* to find statistical differences

Small-world networks – Clustering

Social network: All other nodes can be reached by a small number of steps
Possible to identify “outliers”, nodes with different clustering behavior.
Spam differs from Ham

Differences are visible within minutes. Spamming nodes can then be identified! Many more characteristics are available and can be used.

Degree distribution for Ham and Spam (i.e. frequency of number of friends)
Ham follows a power law: $C \times k^\gamma$

Securing the Connected Car

Project: SIGYN II (Vinnova)
Volvo Cars, Chalmers, KnowIT, Viktoriainstitutet, SP, Semcon, Alkit
Introductory Example

• Possible explanations for the crash

- Bad weather
- Bambi
- Too much to drink...
- Road conditions

OR...
Perhaps a piece of malicious code?
Modern Vehicles

• Contain 50-100 computers
  – Electronic control units (ECUs)
  – Internal network used – replaces all old cables
  – Network of the size of an office!

• Why use computers and software?
  – Easy to reproduce, update functionality
  – Supports flexible, advanced functionality:
    ABS, ESP, ...
  – Diagnostics and software updates
  – App-store

Securing the Connected Car

• A car today consists of 50-100 networked computers
• And tomorrow it will be connected to the Internet...
• Complementing safety issues with security aspects
Examples of Services

- Remote diagnostics
  - Read diagnostic trouble codes
  - Determine what is wrong with the vehicle
  - Control functionality (test hardware and software)

- Remote software update
  - Install new software in an ECU
  - Provide improved functionality
  - Patch software (bugs)
    Can we wait 3 years for a patch?
Why remote software updates?

Volvo recalls 26,000 cars worldwide:

Reason: Problems with the software controlling the fuel injection pump. It can under some circumstances render the car impossible to start.

Affected models are Volvo S 80, S 60, XC 60, XC 70 and V 70 from 2008 to 2010, all with the T6 turbo engine.

This is not a Volvo specific problem. All vendors recall cars due to software and other problems.

Risks and Consequences

- Execution of arbitrary code
  - Successful impersonation of portal, intrusion to vehicle
    - Issue arbitrary diagnostics requests or software
    - Update ECU with modified software

- Disclosure of information
  - Successful intrusion to portal, impersonation of vehicle
    - Gain access to private data

- Denial of service
  - Targeting portal, communication link or vehicle
    - Cause software updates to fail, diagnostics to report incorrect values
    - Prevent legitimate users from updating potentially vulnerable software
Summary: Current security projects

- Quantitative modeling and evaluation of security
- Security and dependability modelling
- Intrusion Detection Systems
- Intelligent security logging and monitoring
- Programming language support for security
- Formal methods for programming languages
- Malicious Internet traffic (attacks, spam, ...)
- Denial of Service mitigation techniques
- Secure sensor networks
- Decision support systems
- Safety and Security in transport systems
- ...