Trustworthy Incident Information Sharing for Collaborative Cyber Defense

Florian Skopik
AIT Austrian Institute of Technology, AT

October 07, 2013
Vienna
Motivation for Collaborative Cyber Defense

- **Our society** is highly dependent on ICT
- **Cyber crime** has become a profitable business
- **Cyber terrorism** and cyber war are reality!
  - Large-scale distributed denial of service attacks (DoS)
  - Targeted and highly specialized (Stuxnet)
- **Private** organizations run **critical infrastructures**
  - Varying security standards
  - Multitude of new attack vectors
- **Infrastructure** providers get **increasingly interconnected**, resulting in more and more **interdependencies and larger attack surfaces**
- A **critical service outage** (energy, water, transportation, finance) can cause **serious situations for the whole society**.

The security of organizations’ ICT assets becomes a major concern!
Collaborative Cyber Defense – Research Questions

How can we collaboratively …

- support SMEs who deliver critical services to secure their corporate systems?
- set up an effective early warning system on a national level (national cyber security system)?
- detect distributed and coordinated attacks targeting multiple organizations simultaneously?
- protect critical (national) assets through knowledge sharing about incidents?
- investigate and mitigate the impact of attacks on a national level?
Collaborative Cyber Defense – AIT’s Research Agenda

- Linking and coordinating existing initiatives
  - Military initiatives (e.g., ministry of defense etc.)
  - Civil initiatives, e.g., from crisis management
  - ICT: Computer Emergency Response Teams (CERTs)
  - Individual trainings for SMEs
- Facilitating public-private partnerships
  - Private organizations deliver public services
  - Definition of roles, responsibilities, obligations etc.
- Activating inter-organizational collaboration
  - Information exchange regarding exploited vulnerabilities
  - Mutual aid in securing systems against current threats
- Establishing situational awareness on a national level
  - Using advanced anomaly detection approaches
Preliminary Approaches 1: Anomaly Detection Algorithm

- Detect abnormal behavior which might be the effect of an attack
  - Anomaly = a statistically-relevant deviation from the "typical behavior"
  - Typical behavior = the dominant event pattern observed in the past
- Novelties*:
  - Not counting single events on packet layer
  - Instead: extensive temporal analysis of co-occurring high level events
  - Not based on predefined signatures and 3rd party patterns (IDSs)
  - Instead: Adaptive and self-learning approach
- Algorithm design:
  I. Dynamic baseline construction: learn typical behavior of co-occurring events due to system utilization at timespan \( t_{12} \) from past events
  II. Detection: test current events against elements in the baseline

* Patent pending: „Algorithmus zur Anomalie-Detektion“, A50292/2013
Preliminary Approaches 2: Efficient Sharing Structure

- **A hybrid sharing model** unifying p2p-aspects and hierarchical ones.
  - Increase trust between organizations by enabling them to regulate information flows on a p2p-basis.
  - Let organizations decide: what and with whom to share.
  - Enable a national authority to still establish situational awareness.

- **Establish Security Operation Centers (SOCs)**
  - Organizational Level
  - Sectoral Level
  - Cross-Sectoral Level
  - National and European Level

- **A trusted SOC** cares for
  - Incident information storage, distribution, lawful disclosure
  - Maintains contact to national authorities
Preliminary Approaches 3: Sharing Incentive Model

- **Connecting single organizations** to enable them to:
  - Exchange information about **cyber incidents**
    - → collaborative early warning system
  - Report **exploited vulnerabilities**
    - → national impact analysis
  - Apply **mutual aid**
    - → mitigate effects of an attack for the welfare of the country
- … has also several **positive effects on contributing organizations:**
  - **Cut** of security **expenditures**
    - → Collaboration might enable the earlier detection of APTs
    - → Receive hints “what to look for” and “where to take care”
  - **Risk Mitigation**
    - → Being part of an alliance enables one to count on help/support of others.
Preliminary Approaches 4: Applicable Software Framework

- Scalable architecture using both centralized entities and p2p structures
- Formats for attack reports: IODEF, x-Arf
- Proof of Concept using PKI, SOA
- Integration of social networking concepts: trust and reputation
Outlook and (some!) Business Opportunities

- Capture and manage **critical interdependencies** between different CIs
- Deal with Cyber vulnerabilities of CIs and **detection of highly sophisticated attacks** (anomaly detection)
- Improve information handling and **incident management & decision support** (Common Operational Picture contents, visualization, assessment)
- Improve **public-private cooperation** /PPP
- Study the framework applicability from an **organizational and technical perspective**
- Perform systematic capturing and evaluation of usable **best practices**
- Study **societal acceptance**, economic, organizational & **legal viability**
Thank you!

DDr. Florian Skopik
IT Security
Business Unit Information Management & eHealth
Safety & Security Department

florian.skopik@ait.ac.at  |  +43 664 8251495  |  www.ait.ac.at/it-security
Backup Slides
Project Cyber Attack Information System (CAIS)

- **National research project**
  - Partly funded by the Federal Ministry for Transport, Innovation and Technology
- **Project duration:** 2 years, 2011-2013
- **Aim:** to study concepts, models and approaches for **setting up a national cyber center** in order to keep track of ongoing incidents on a national level and establish/maintain **situational awareness**.
- **Partners:** from research, industry, and the government
  - AIT Austrian Institute of Technology
  - Bundeskanzleramt Österreich (The Federal Chancellery)
  - Bundesministerium für Landesverteidig. u. Sport (Ministry of Defence and Sports)
  - Bundesministerium für Inneres (Federal Ministry for the Interior)
  - FH St. Pölten (University of Applied Sciences)
  - OIIP Österreichisches Institut für Internationale Politik
  - T-Mobile Austria
  - T-Systems Austria
  - NIC.AT / CERT.AT
FP7 Sec 2013.2.5-3 ECOSSIAN
European Control System Security Incident Analysis Network

- Large-scale Integrated Project on an European Level
- Development of an organizational and technical framework for a secure, trustworthy information sharing system which protects the anonymity and privacy of all participants
- Development of anomaly detection to enable organizations, governments and transnational bodies to defend their critical infrastructures with respect to a cross border incident response system
- Successor of KIRAS Project CAIS on an European Level
- Project Participants
  - Technikon (AT)
  - Austrian Institute of Technology (AT)
  - Cambrensis (UK)
  - Cassidian (DE/FR)
  - EADS Innovation Works (DE/UK)
  - espion (IE)
  - Finnish Police College (FI)
  - Frauenhofer AISEC (DE)
  - INOV (PT)
  - Portuguese railway network
  - Policia Judiciaria (PT)
  - VTT (FI)