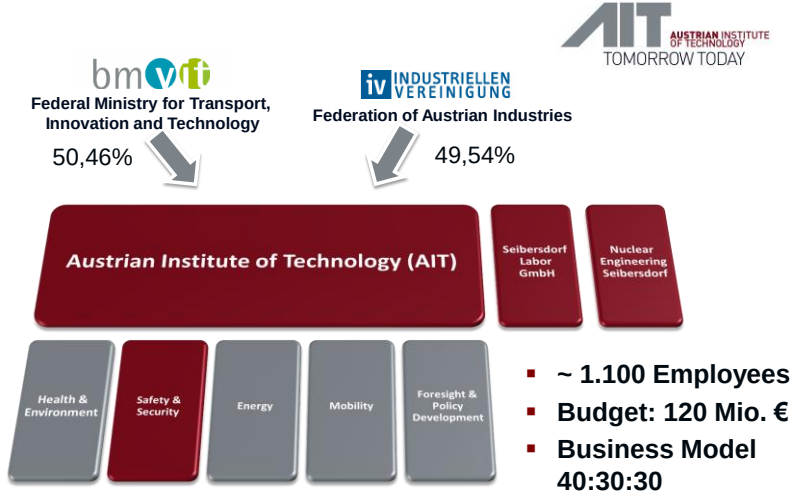
ICT Security Research @ AIT

Anomaly Detection and Incident Info Sharing

Thomas Bleier
Dipl.-Ing. MSc zPM CISSP CEH CISM
Thematic Coordinator ICT Security
Digital Safety & Security Department
AIT Austrian Institute of Technology GmbH



Safety & Security Department

Intelligent Vision Systems (IVS)

Surveillance & Protection

Multi-Camera Vision

Intelligent Camera Networks
3D Vision and Modelling

High Speed Imaging

High Performance Vision
New Sensor Technologies

Highly Reliable SW and Systems (HRS)

Highest System Reliability

Assessment and Testing of Autonomous and Safety-Critical Systems

Verification & Validation

Future Networks and Services (FNS)

Large Scale Networked Systems

Secure Inf. Access in Distr. Systems

ICT Security
Optical Quantum Technologies

Next-Gen Content Mgmt Systems

Big Data & Open Data
Quality Assurance & Recommender Systems

Advanced Apps in Sensor Networks

Health Information Systems
Biosignal Processing
Environmental and Crisis & Disaster Management

From key scientific competences to focused applied research

The problem…

- The complexity of ICT systems is increasing
  - Landing on the moon with 7.500 Lines of Code
  - Today: F-35 fighter jet: 5,7 Mio; Boeing 787: 6,5 Mio; Mercedes S-Class: 20 Mio; Chevrolet Volt: 100 Mio.
- Systems are getting more and more interconnected
  - Internet-of-Things, Always-on, Pervasive Computing
  - M2M (Machine-to-Machine) Communication
  - Virtual Infrastrucutures (Cloud), etc.
- Industry trend towards open network architectures
  - Open protocols (e.g. IP)
  - Increased number of „third parties“
- The dependency on ICT systems is increasing
  - Smart Grid, Smart Home, Smart City, Smart Phone
  - eGovernment, eCommerce, eHealth, eMobility

Increased Number of Vulnerabilities

Increased Risk

Increased Impact

General Approach

Basic Secure System Design Methods

New Approaches

Application-oriented Research

Application Domain Know-How

Methodologies and Tools for Secure System Design

Research Topics

Main Application Areas

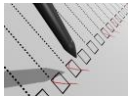
Smart Grid & SCADA Security

High Assurance Clouds

(National) Cyber Security

Fundamental Technologies

Info Sharing & Event Correlation



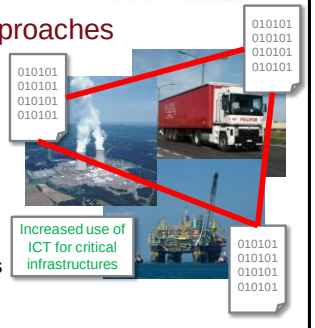
Risk Management

Privacy & Identities

Next Gen Crypto

Motivation for Novel Cyber Defense Approaches

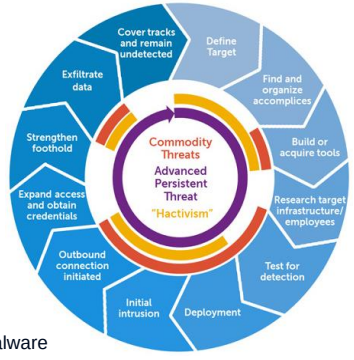
- Our **society** is highly **dependent on ICT**
- **Cyber crime** has become a profitable business
- **Cyber terrorism** and cyber war are reality!
  - Large-scale distributed denial of service attacks (DoS)
  - Targeted and highly specialized (Stuxnet)
- **Private** organizations run **critical infrastructures**
  - 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**.



New Approaches to Cyber Security required!

What is an **A**dvanced **P**ersistent **T**hreat?

- Traditional attacks are…
  - Objectives: spam, DoS, ID theft
  - Target: machines with certain config.
  - Scope: promiscuous
  - Timing: fast
  - Control: automated malware
- Advanced persistent threats are…
  - Objectives: espionage, control, IPR theft
  - Target: users, companies, organizations
  - Scope: specific
  - Timing: slow
  - Control: manual intervention, customized malware
- Discovery of attacks
  - **Know what is normal in your system …**
  - **… to understand what might be (the result of) an attack.**



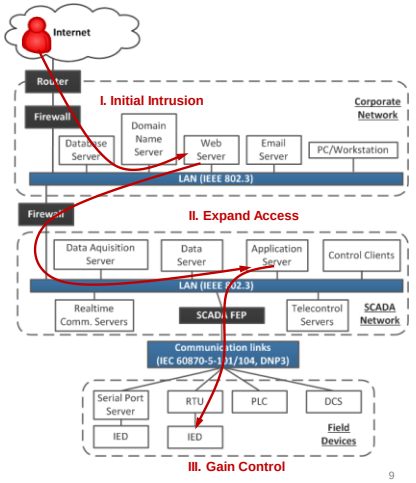
Establishing *Cyber Situational Awareness* is the key!

The Anatomy of an APT: An Example from a Smart Grid

I. Initial Intrusion
- Exploit weaknesses (configuration error, SW vulnerability (e.g., RDP))

II. Expand Access and Strengthen Foothold
- Access control system from within the trusted environment

III. Gain Control
- Send fabricated control messages



What does that mean ..?

- Security breaches are not preventable – too complex, customized …
- New tactics are required:
  - Accept security incidents (to a certain degree)
  - BUT: minimize effects of (successful) attacks


TECHNOLOGY

Symantec Develops New Attack on Cyberhacking

Declaring Antivirus Software Dead, Firm Turns to Minimizing Damage From Breaches

Email Print Comments

By DANNY YADRON CONNECT

Updated May 4, 2014 10:41 p.m. ET

Symantec Corp. invented commercial antivirus software to protect computers from hackers a quarter-century ago. Now the company says such tactics are doomed to failure.

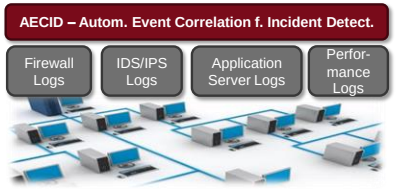
Shift from preventive to reactive defense strategies!

Establishing Cyber Situational Awareness

- **Understand**
  - Structure of networks and service interdependencies
  - Availability of services
  - Ongoing business and operations
- **Detect** and **predict**
  - Undesired activities and their current or future impact on services, operation, or infrastructure
- **Observe** and **analyze**
  - Responsive actions, such as mitigation strategies, and their success
  - Effectiveness of service recovery procedures

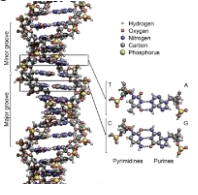
Effective Defense through Distributed Anomaly Detection

- (Future) Issue: Highly sophisticated and coordinated distributed attacks
  - Each of those single attacks are often below security thresholds
  - Looking at isolated systems or single points in a network not sufficient any longer
  - Infiltration of systems through social engineering
- Solution: Introduction of an **additional security layer**, spanning various services/systems in numerous departments/organizations to:
  - harness **log data from various systems and services** on different layers
  - **understand** the "normal" system utilization and behavior
  - detect **behavior deviations resulting from unknown(!) attacks**
  - detect attacks using **multiple attack vectors**



Massive Event Correlation – Models from Bioinformatics

- Main Objective:
  - Harvest operational data (**logs**) of systems describing the dynamic behavior
  - Continuously analyze this data, even across different systems, to build a system model and understand the mode of operation and dependencies
  - Use an applicable **anomaly detection** schema to detect signs of an attack/intrusion
- Applied Concepts:
  - **Fingerprinting:** pattern mining for data reduction
    - Mining of repetitive sequences
    - Extraction of characteristic attributes
    - Not depending on predefined rules
  - **Alignment:** Near real-time discovery of fingerprints in continuous log data streams



Source: Wikipedia, Licensed under Creative Commons.

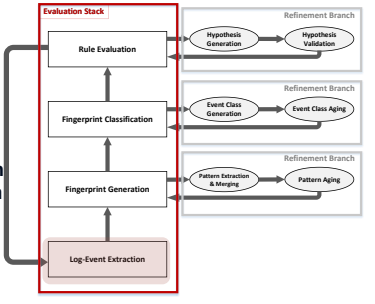
AAB24823
TYHMCQFHCRYVNNHSGEKLYECNERSKAFSCPSHLQCHKRRQIGEKTHEHNQCGKAFFT 60
----------YECNQCGKAFAQHSSLKCHYKTHIGEKPYECNQCGKAFSK 40
PSHLQYHERTHTGEKPYECHQCGQAFKKCSLLQRHKRTHTGEKPYE-CNQCGKAFAQ- 116
HSHLQCHKRTHTGEKPYECNQCGKAFSQHGLLQRHKRTHTGEKPYMNVINMVKPLHNS 98

Similar to anomaly detection in biology, we use available algorithms for anomaly detection in large-scale computer networks.

AIT Patents: ÖPA A 50292 2013, AT 514.215

AECID Anomaly Detection Approach in a Nutshell

1. **Collect log files** from various systems and process them, **timely ordered**, **line-by-line**
2. Generate a **fingerprint** (a **bit-vector** representation **of matching and un-matching patterns**) of each log-line
3. **Classify fingerprints** and trigger **synthetic events**
4. **Create hypothesis and evaluate if-then rules** to detect significant deviations from normal system behavior
5. **Point** human investigator **to anomalous behavior**



$$H_1 = \langle C_1, C_2, +10s \rangle$$

Time	Q_1	
10:30:40	$\langle 10:30:35, C_1 \rangle$	
10:30:42	$\langle 10:30:41, C_2 \rangle$	$\langle 10:30:35, C_1 \rangle$
10:30:50	$\langle 10:30:45, C_1 \rangle$	
10:30:57	$\langle 10:30:57, C_2 \rangle$	$\langle 10:30:45, C_1 \rangle$
10:30:59		

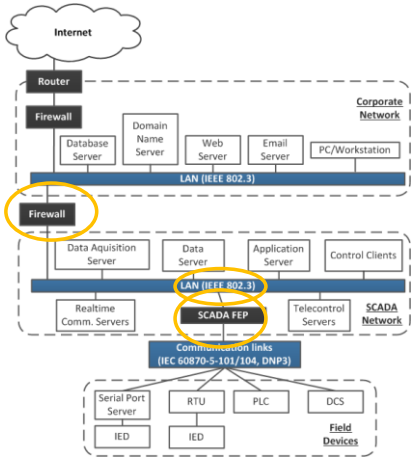
	P_4
v3ls13	1
	0
	0

Slot 3	Buffer	Sl_3									
Slot 2	Sl_2										
Slot 1	Sl_1										

pos	1	2	3	4	5	6	7	8	9	10	11	12
10:30:40	1	1	0	1	1	1	1	1	1	1	1	
10:30:50	1	1	1	0	1	1	1	1	1	1	1	
10:30:59	0	1	1	1	0	1	1	1	1	1	1	

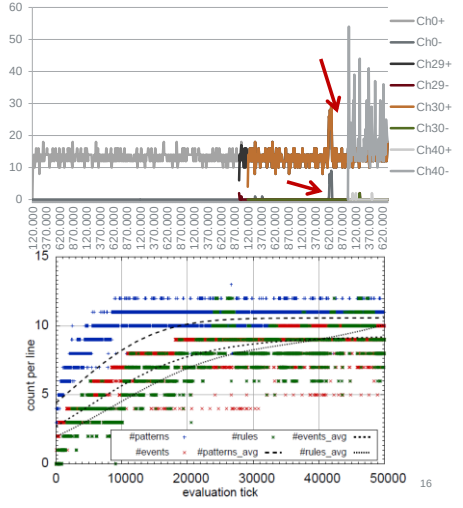
Real World Use Case: SCADA System Setup

- Testbed from an AUT DSO
- Evaluation data
  - 200.000 log lines per hour
  - Over 3 days of operations
- Testbed structure
  - Corporate LAN
  - Firewall
  - Switch
  - SCADA system



Real World Use Case: SCADA System Results and Performance

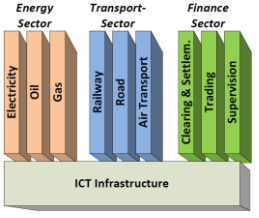
- Eval. complexity
  - 200.000 lines per hour
  - After 7.000 we capture all events
  - After 50.000 we have a stable set of hypotheses
- Model metrics
  - 11-13 patterns per line
  - 7-9 events per line
  - > 5 hypotheses per line
- Evaluation scenario
  - Anomaly injection: bypass firewall and cause all firewall hypotheses to fail.



Cyber Incident Information Sharing

- **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 incident report analysis techniques

Motivation for Cyber Incident Information Exchange



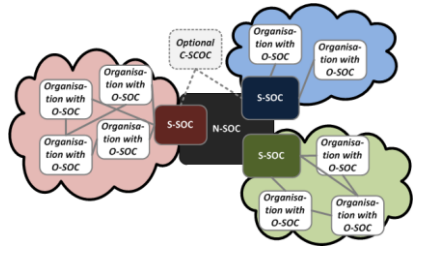
- **Connecting single organizations** to enable them to:
  - Exchange information about **cyber incidents**
    - → collaborative early warning system
  - Report **exploited vulnerabilities**
    - → national impact analysis
  - Apply **mutual aid**
    - → mitigate effects of an attack for the welfare 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.

Challenges in Cyber Incident Information Sharing

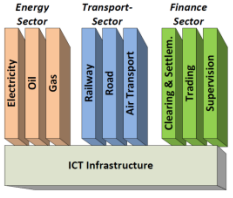
- Pure **hierarchical sharing systems** have **not proven useful** in the past because organizations are reluctant to share sensitive/critical information.
- They **fear**…
  - to **become** even **more vulnerable** (e.g., detailed information about ICT assets and their configuration is top secret)
  - **exploitation through competitors**, especially in emergency situations (e.g., when under attack)
  - **bad publicity** and loss of reputation (e.g., stolen customer data)
  - **high efforts/costs** but no or minimal gain (detailed reporting of incidents without any impact)
  - leakage of IPR, business data, in general: **privacy concerns**

Preliminary Approaches 1: 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



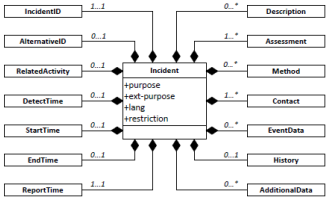
Preliminary Approaches 2: Sharing Incentive Model

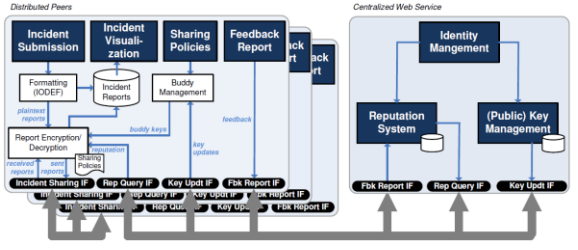


- **Connecting single organizations** to enable them to:
  - Exchange information about **cyber incidents**
    - → collaborative early warning system
  - Report **exploited vulnerabilities**
    - → national impact analysis
  - Apply **mutual aid**
    - → mitigate effects of an attack for the welfare 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 3: Applicable Software Framework

- Scalable architecture using both centralized entities and p2p structures
- Formats for attack reports: IODEF, STIX,…
- Proof of Concept using PKI, SOA
- Integration of social networking concepts: trust and reputation

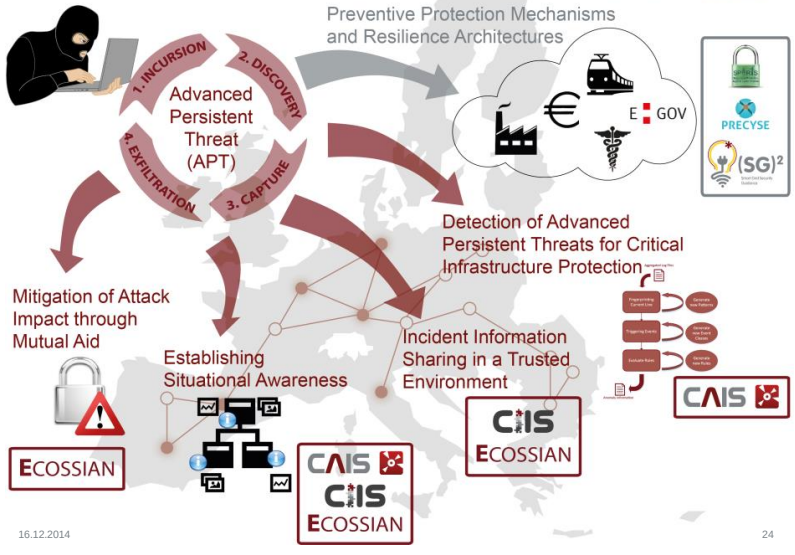




Conclusion: Prevention, Detection and Reaction…

- Prevention is of limited use without detection and reaction!
  - AECID – where to look for attacks?
- Increasing System Complexity
- Situational awareness through
  - Data collection
  - Big data analytics
  - Information fusion
  - Information sharing

Cyber Defense and Situational Awareness

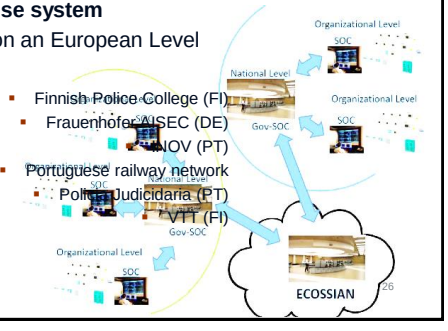


Project Cyber Attack Information System (CAIS)

- *National research project*
  - Partly funded by the Federal Ministry for Transport, Innovation and Technology
- *Project duration:* 2 years, 2011-2013; ***finished***.
- *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
- *Web:* http://ercim-news.ercim.eu/en91/ri/cybercrime-and-the-security-of-critical-infrastructures

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 SISEC (DE)
  - INOV (PT)
  - Portuguese railway network
  - Polícia Judiciária (PT)
  - VTT (FI)



AIT Austrian Institute of Technology

your ingenious partner

Thomas Bleier
Dipl.-Ing. MSc zPM CISSP CEH CISM
Thematic Coordinator ICT Security
Research Area Future Networks and Services
Digital Safety & Security Department
thomas.bleier@ait.ac.at | +43 664 8251279 | www.ait.ac.at/ict-security