Real-time SEC&DEP monitoring: make it a bundle

Luigi Romano

64th IFIP WG 10.4 Meeting

June 27-30, 2013 Visegrád, Hungary

Roadmap

- Problem Statement and Proposed Approach
- SEC&DEP monitoring building blocks and enabling technologies: SOTA review & Gap Analysis
- Action Points towards integrated real-time SEC&DEP monitoring technology
- Selected Case Studies
- Acknowledgements & pointers to additional info
- Contact Info

Problem Statement and Proposed Approach

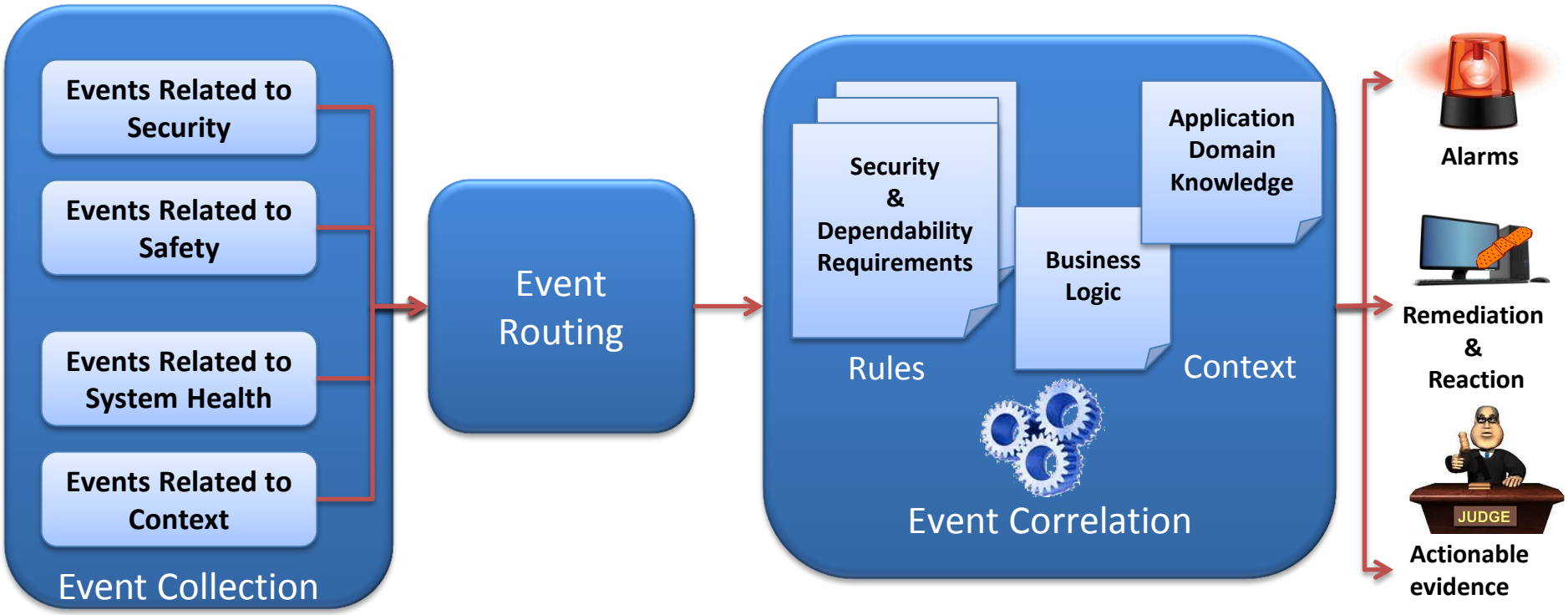
Problem Statement – 1/2

- A plethora of technologies exists (will review them in a second), that individually represent a (potentially) effective building block of a real-time SEC&DEP monitoring facility
- Regrettably, they very much lack integration
- A significant advancement in the convergence of such technologies is needed
- Convergence here means:
  - Effective cooperation - i.e. coordinated and results-oriented capability of working together- among previously disjointed functions
- Recently some achievements have been made - e.g. SEM and SIM have merged into SIEM, LACS and PACS have merged into IM, SOC technology has improved significantly - but much is yet to be done

Problem Statement – 2/2

- In order for remediation to be effective, the right actions must be taken at the right time
- That means SEC&DEP monitoring facilities must be implemented as dependable (i.e. accurate, timely, and trustworthy) functions
- The availabilty of Fault- and Intrusion- Detection and Diagnosis facilities is the precondition for performing appropiate remediation actions
- Enhanced situation awareness is needed to allow dependable detection and diagnosis of faults and attacks
- Since there will always be faults and intrusions, SEC&DEP monitoring facilities must be designed as a resilient system

Integrated real-time SEC&DEP monitoring: Conceptual View and Main Issues



- **Data volumes**
- **Data heterogeneity**
- **Key technologies not (well) supported**
- **Scalability**
- **Protection of critical flows**
- **Understanding the context**
- **Extracting KPIs**
- **Intrusiveness**

Proposed Approach - 1

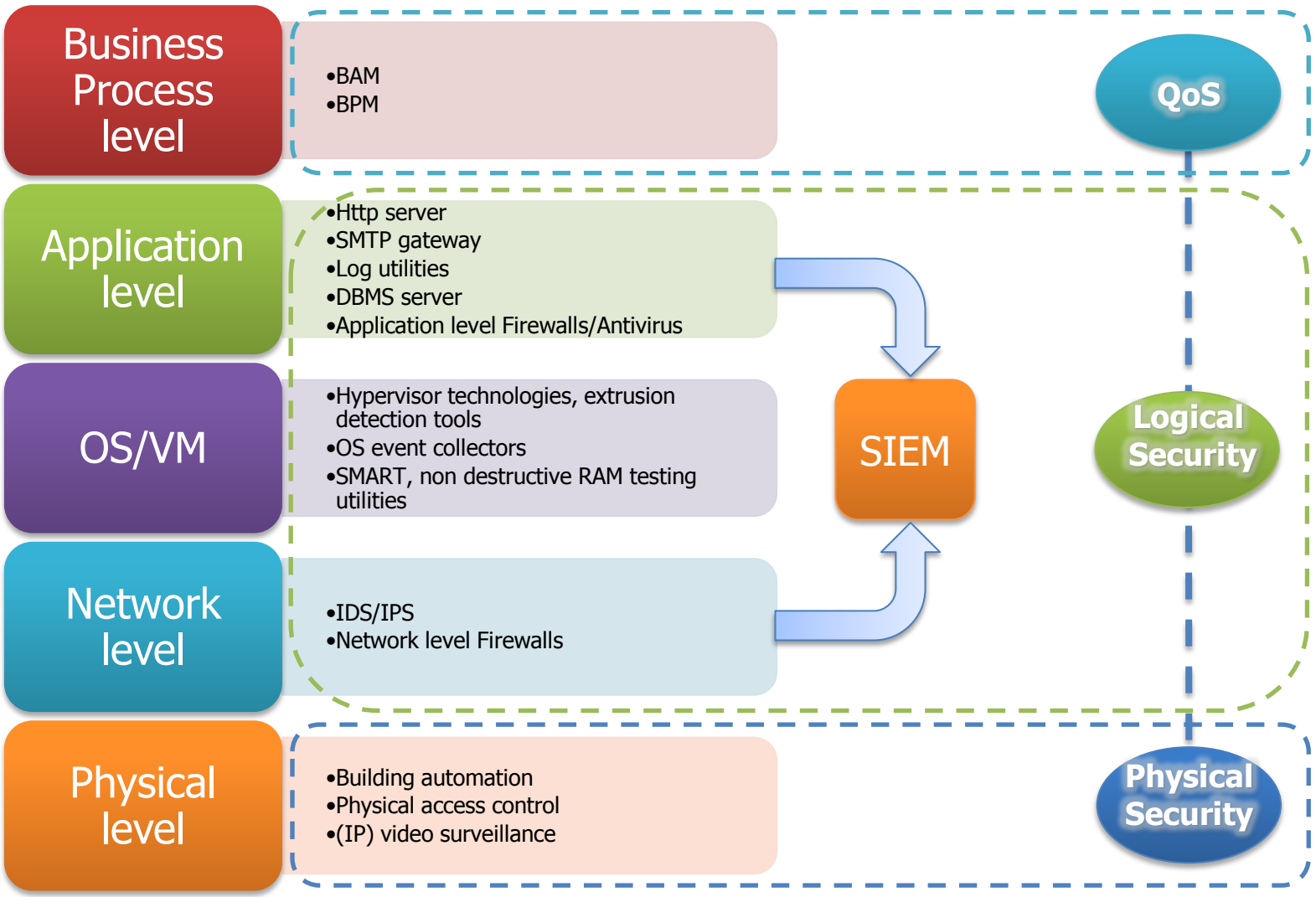
- Collect information at several architectural levels (namely: Physical, Network, Operating System*, Data Base, Application, and Business Process)
- Use multiple security probes, which are deployed as a distributed architecture
- Use effective techniques/technologies (e.g. grammar-based approaches and compiler-compiler technologies) to handle data heterogeneity
- Escalate from fault/intrusion symptoms to the adjudged cause of the fault/intrusion, and estimate the damage to individual system components

***also VM if we are in the cloud**

Proposed Approach - 2

- Improve the performance of the detection process, i.e. to achieve higher detection rates and lower false positives rates
- Perform sophisticated correlation analysis of SEC&DEP-related data, using effective technologies, specifically: Complex Event Processing (CEP)
- Improve the support for widespread legacy technologies (e.g. SCADA) as well as for emerging technologies (e.g. WSN and PMU)
- Combine edge-side and core-side processing

Event Collection Technologies: Architectural View



Putting this talk in context

- Excerpt from Paulo's message:
  - I would like to challenge you to talk about research
    - yours and/or other's
    - the one you think you'd like to do
    - or that should be done by someone
    - or that you predict will become relevant in the future, in our area
  - But in so doing, I would like you as well to frame your talk within one of the following boundaries:
    - SURVEY of an R&D AREA (PAST)
    - ONGOING or RECENT R&D (PRESENT)
    - VISIONS for SEC&DEP R&D (FUTURE)
- Not much of research aiming at developing a new technology. More of finding how to use existing technologies in a smarter way

SEC&DEP monitoring technologies: SOTA review & Gap Analysis

IDS/IPS in a nutshell

- An Intrusion Detection System (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations
- IDSes typically record information related to observed events, notify security administrators of important observed events, and produce reports
- Many IDSes can also respond to a detected threat by attempting to prevent it from succeeding → Intrusion Detection & Prevention System (IDPS)
- Though they both relate to network security, an intrusion detection system (IDS) differs from a firewall in that:
  - A firewall looks outwardly for intrusions in order to stop them from happening.
  - Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network.
  - An IDS evaluates a suspected intrusion once it has taken place and signals an alarm.
  - An IDS also watches for attacks that originate from within a system.
  - An IDS observes network communications, identifying heuristics and patterns (often known as signatures) of common computer attacks

IDS/IPS market

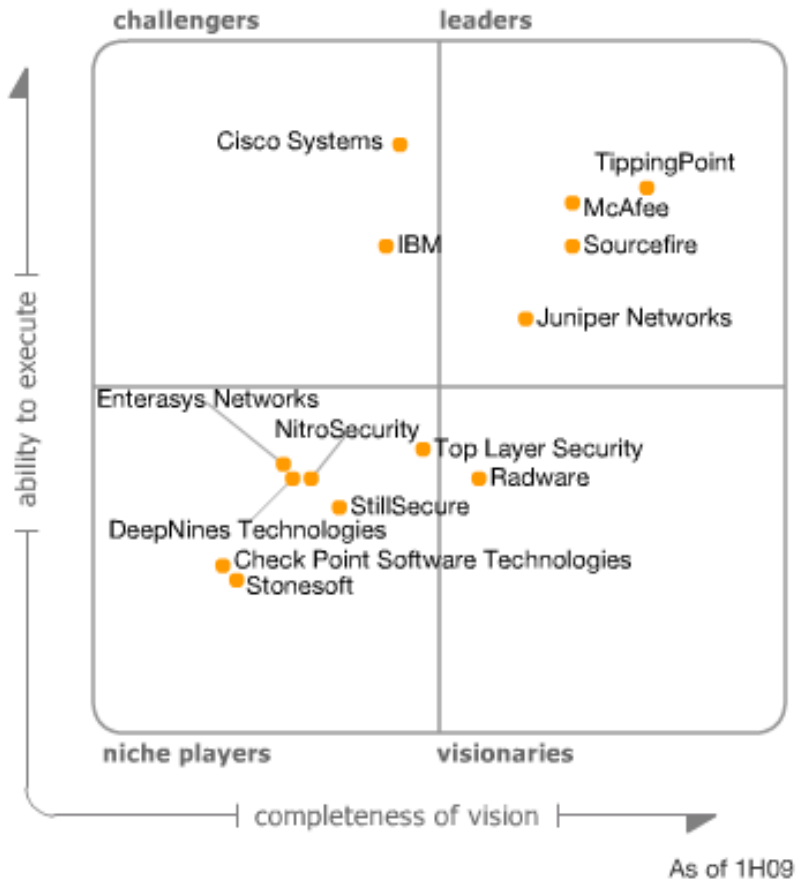
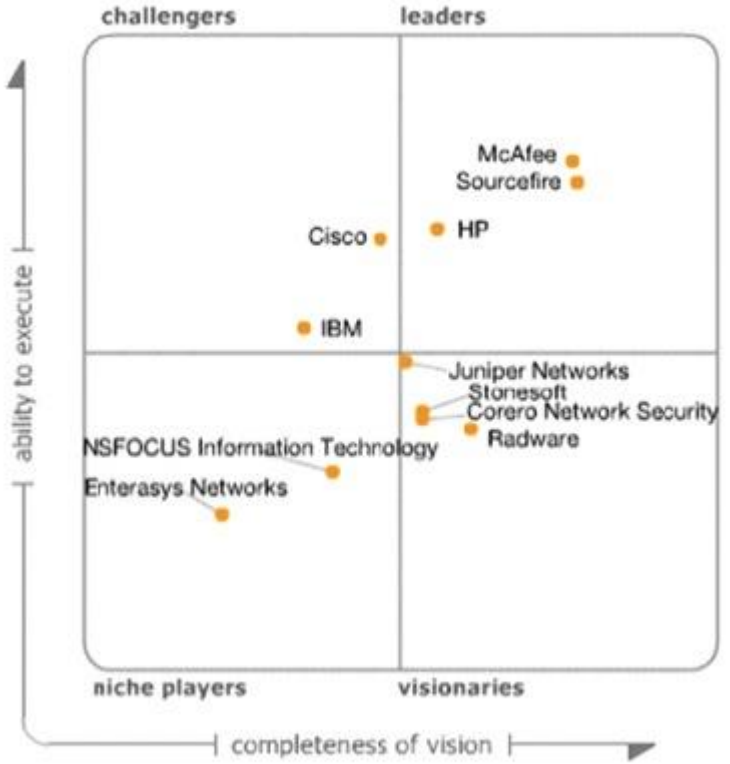


Figure 1. Magic Quadrant for Intrusion Prevention Systems



Source: Gartner (July 2012)

Overall Evaluation and Way Ahead

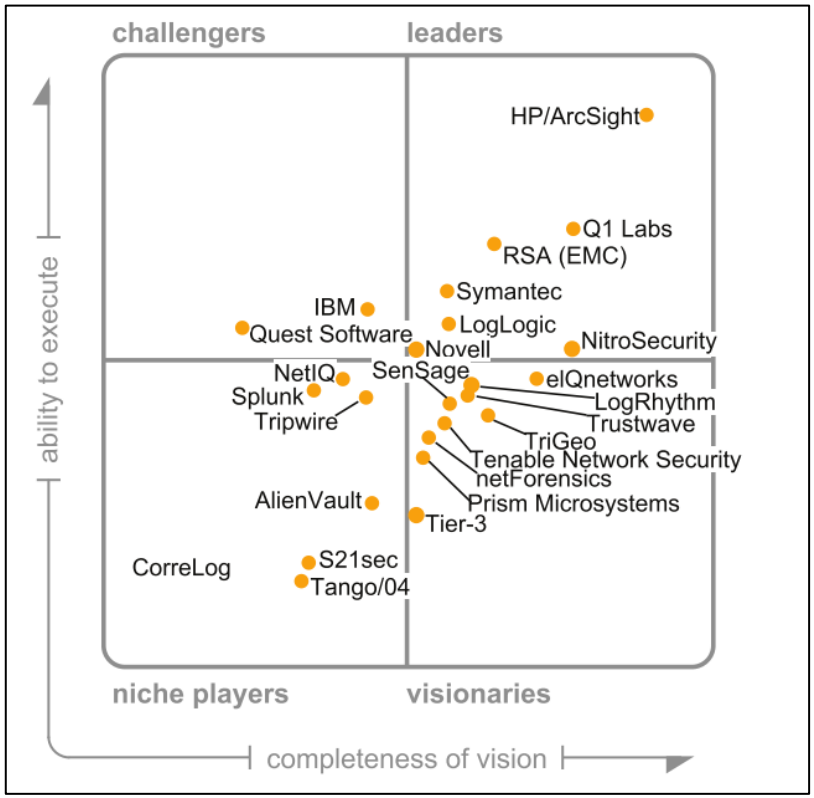
- Poor Detection Accuracy
- Rate of false positives is high -> unacceptable for several application domains (e.g. Telco)
- Limited scalability
- Deployments should scale to enterprise wide extensions … on top of Gigabit network connections
- Growing Evasion
- Current techniques often fail to detect emerging attacks
- Very limited diagnostic facilities
- Who defends the defender? (Despite IDS/IPS are themselves potential targets of intruders' attacks, current products are not designed to be fault- and intrusion-tolerant

SIEM in a nutshell

- A Security Information and Event Management (SIEM) solution effectively combines elements of Security Information Management (SIM) with Security Event Management (SEM)
- SIEM solutions typically correlate, analyze, 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

BPM in a nutshell

- Business Process Management (BPM) has been referred to as a "holistic management" approach to aligning an organization's business processes with the wants and needs of clients
- Since BPM attempts to improve processes continuously, it can be defined as a "process optimization process"
- As a managerial approach, BPM sees processes* as strategic assets of an organization that must be understood, managed, and improved to deliver value-added products and services to clients
- While it is arguable whether BPM enables organizations to be more efficient, more effective and more capable of change (than a functionally focused, traditional hierarchical management approach), they surely process a whole lot of information that is related – sometimes quite closely indeed – to SEC & DEP

***These processes are critical to the organization, as they i) can generate revenue, and ii) often represent a significant proportion of costs**

BAM in a nutshell

- Business Activity Monitoring (BAM) is software that aids in monitoring of business activities, as those activities are implemented in computer systems
- It provides near real-time monitoring of business activities, measurement of Key Performance Indicators (KPIs), their presentation in dashboards, and automatic and proactive notification in case of deviations
- A business activity can either be a business process that is orchestrated by BPM software, or a business process that is a series of activities spanning multiple systems and applications
- BAM is an enterprise solution primarily intended to provide a real-time summary of business activities to operations managers and upper management

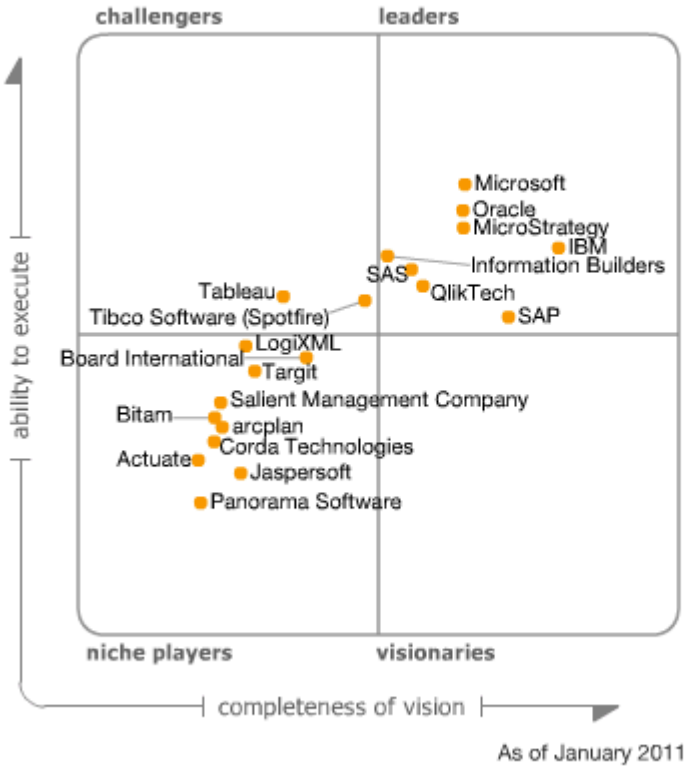
BPM market

Figure 1. Magic Quadrant for Business Process Management Suites

Source: Gartner (October 2010)

BAM Market

Figure 1. Magic Quadrant for Business Intelligence Platforms



Source: Gartner (January 2011)

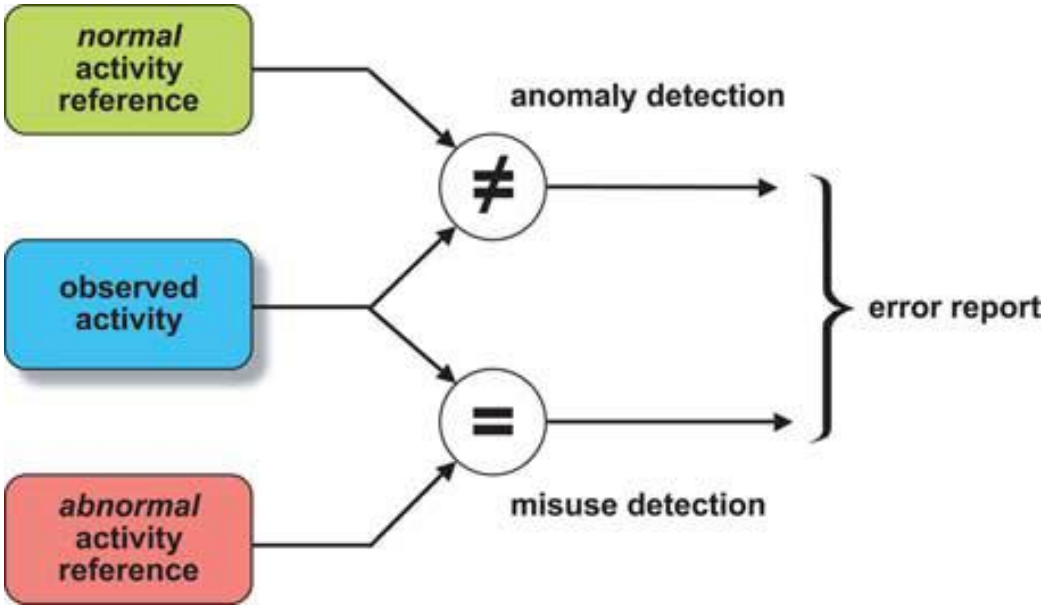
Overall Evaluation and Way Ahead

- BPM/BAM are used (almost) exclusively for monitoring the QoS at the application level
- Since many emerging attacks, which evade current IDS/IPS technology, have clear symptoms in terms of QoS degradation, BPM has a great potential in terms of performance improvement of the detection process
- By understanding the Business Process Logic, it would also be possible to detect new categories of faults/attacks, e.g.:
  - Faults related to orchestration flaws
  - Attacks related to exploitation of misuse cases

Taking SEC&DEP monitoring beyond SOTA: Improving detection

Limitations of current IDS/IPS approaches

- 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

Attack Relevance (2007-2010)

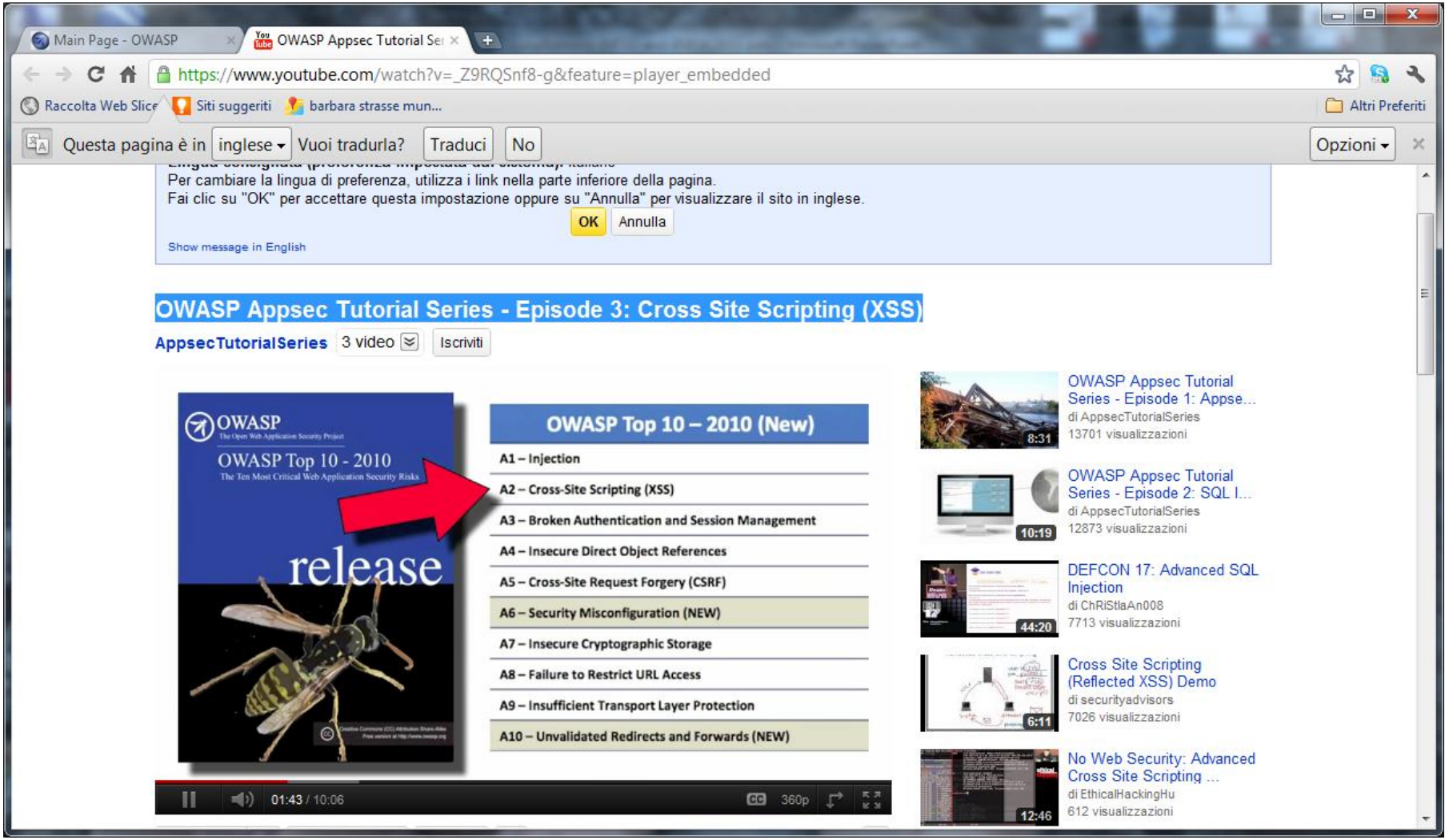
OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	A1 – Injection
A1 – Cross Site Scripting (XSS)	A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session	A3 – Broken Authentication and Session
A8 – Insecure Cryptographic Storage	A9 – Insecure Cryptographic Storage
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

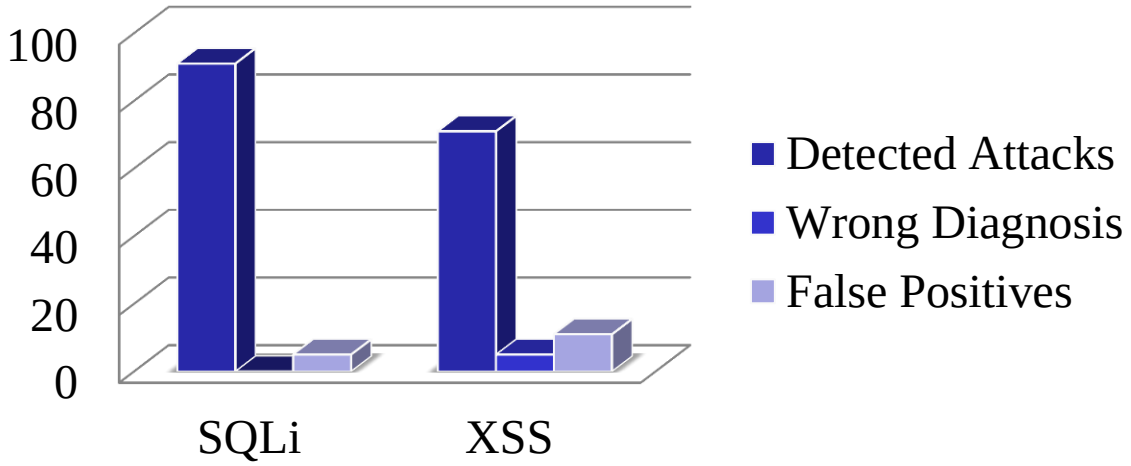
OWASP Top 10 Web attacks, Sep. 2008:
http://www.owasp.org/index.php/Top 10 2007

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)



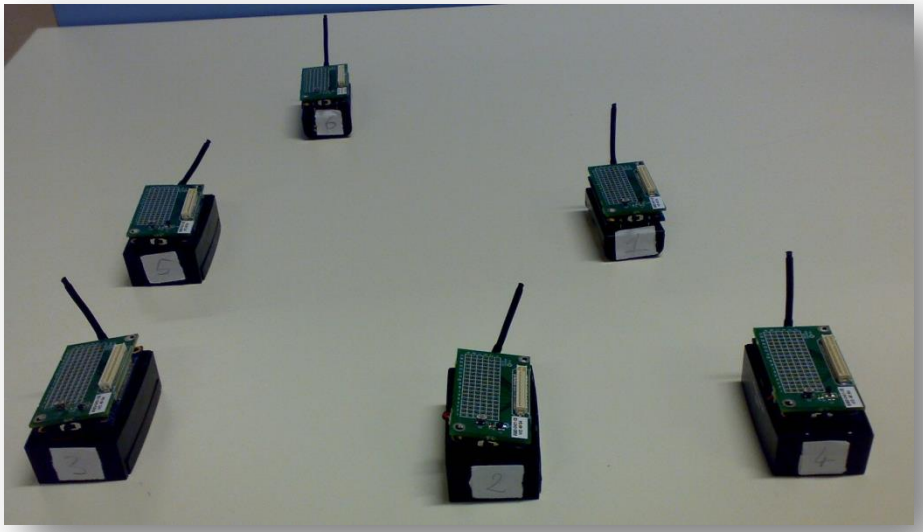
Performance - Correlated probes

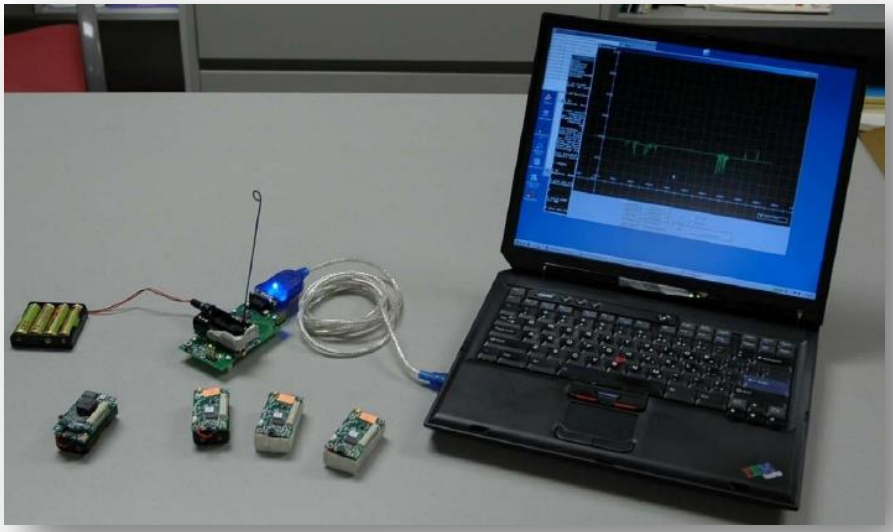


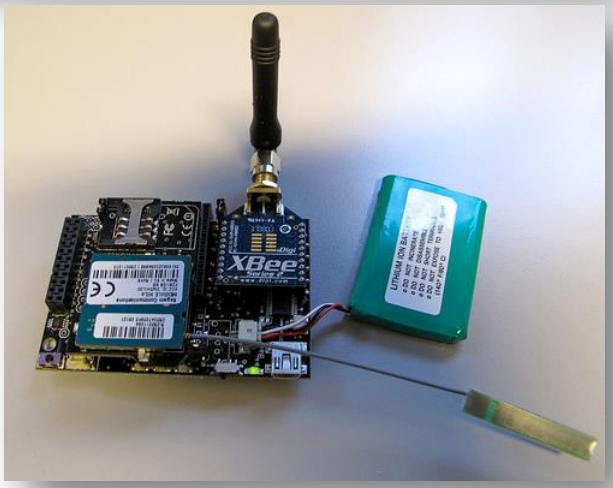
- False positives produced by the ACDM probe are drastically reduced: from 36% to 16% (5% SQLi, 11% XSS)
- The percentage of correctly diagnosed SQLi attacks rises from 73% (Scalp alone) to 91% (Scalp + ACDM + AQFM)
- Correct diagnosis of XSS attacks rises from 63% (Scalp alone) to 71% (Scalp + ACDM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

Taking SEC&DEP monitoring beyond SOTA: Protecting WSN zones

WSN technology







Claim

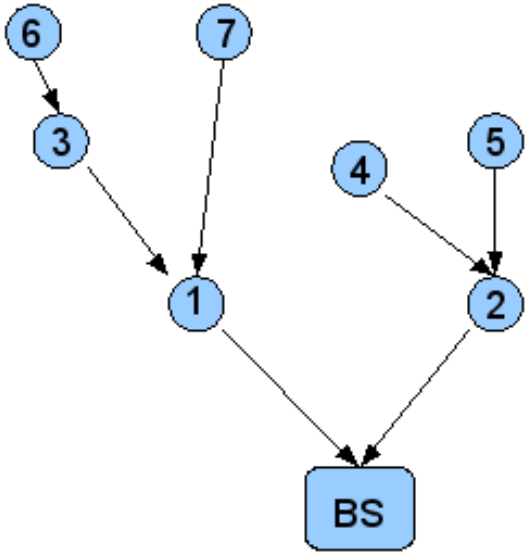
- WSNs will be an integral part of a wide variety of CIs, for a number of reasons, and in particular:
  - **Technical**
    - Potential of significantly improving the sensing capabilities of SCADA sub-systems
    - Potential of increasing the resilience of the overall SCADA architecture
  - **Political**
    - 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
  - 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

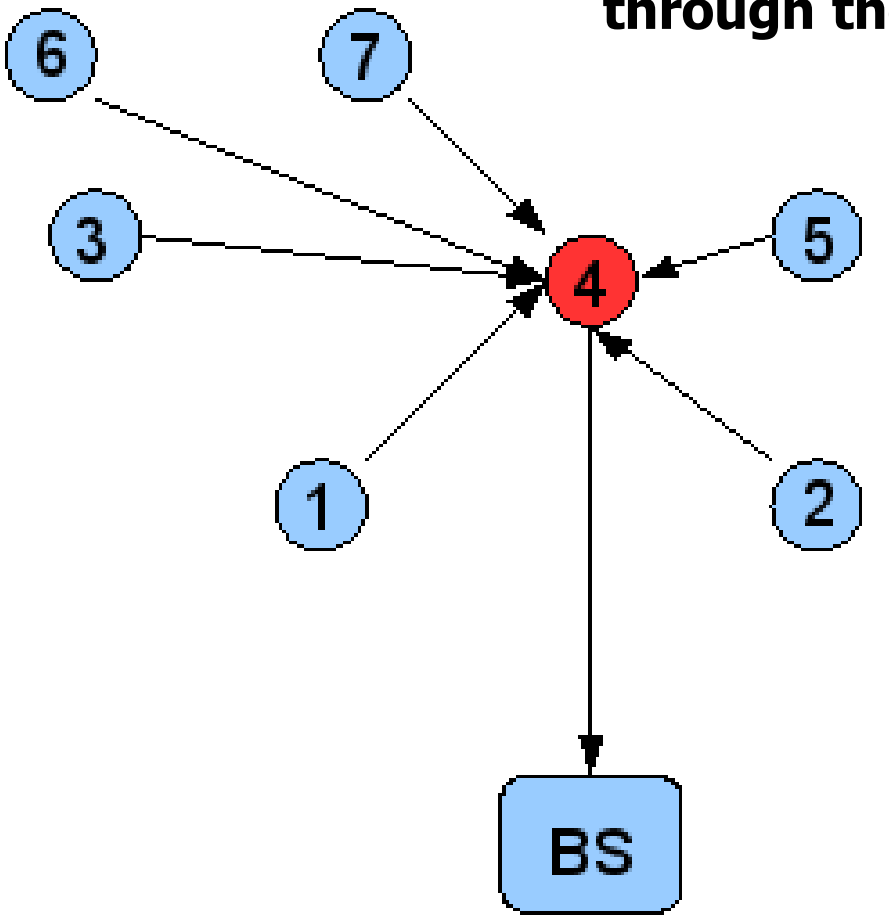
- The malicious node (node 4):
  - Advertises that it has a very low EXT (EXpected Transmission cost) value
  - Claims an high routing packets sending rate for its neighbours in order to force the routing changes



Assumption:

Somehow the node has been compromised

Sinkhole attack



The effect is that all traffic flows through the attacker node

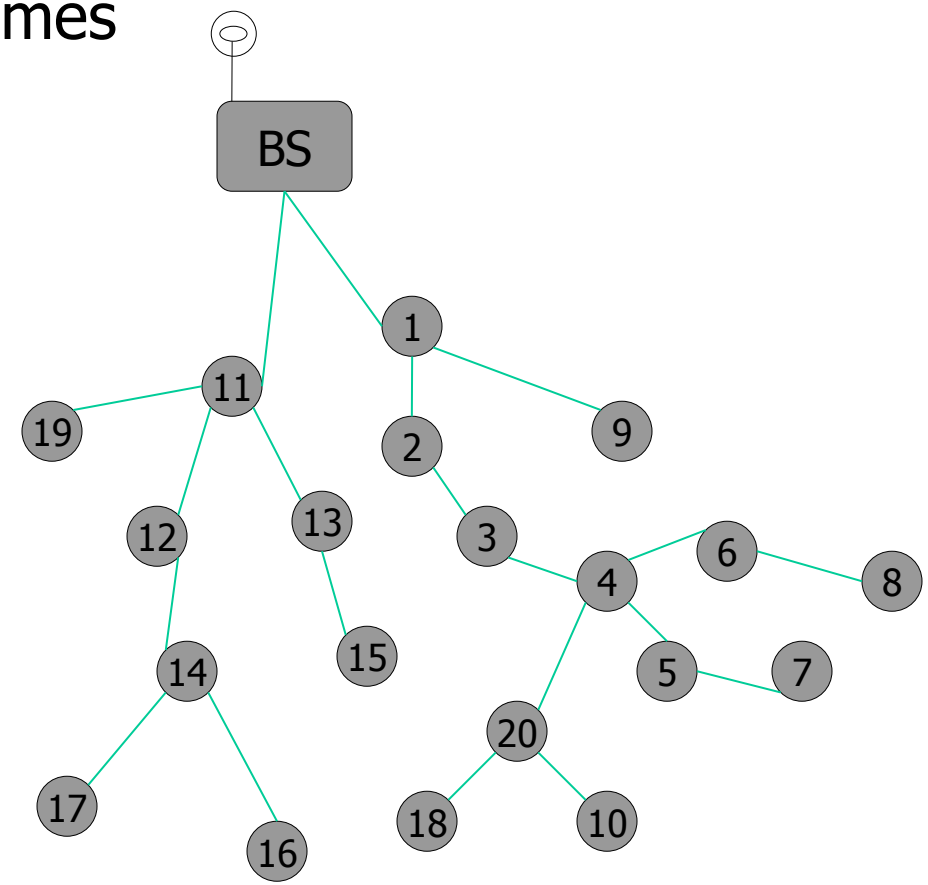
The attacker is thus able to:

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

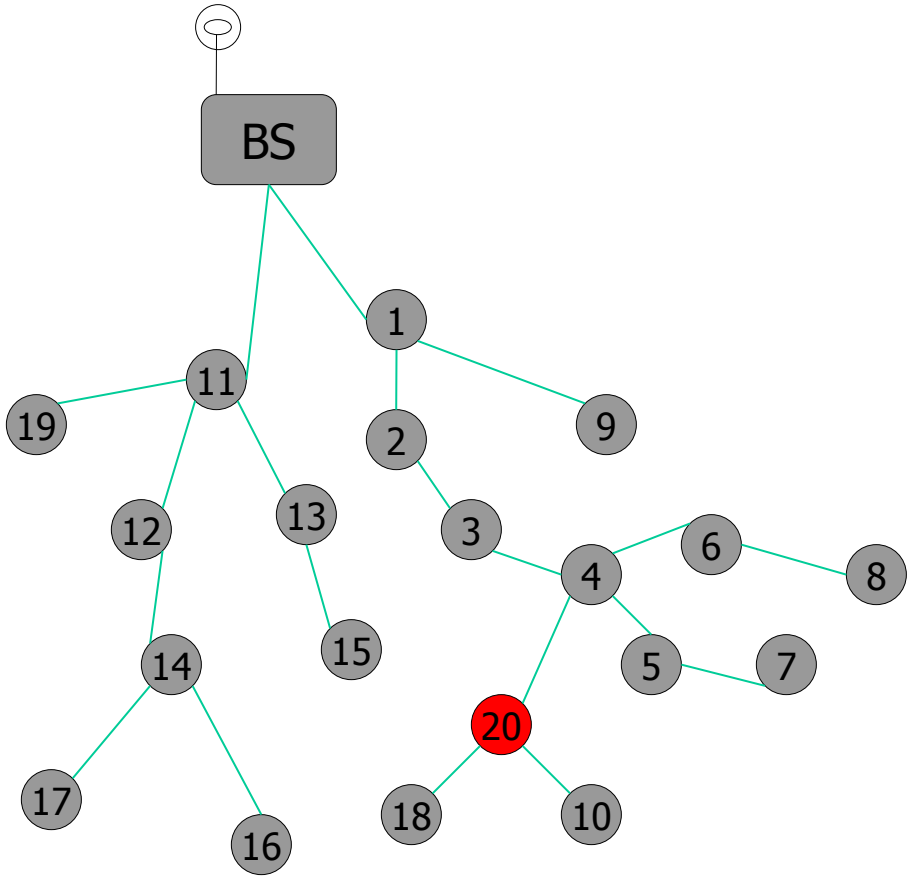
Sleep Deprivation attack

Two alternative tecniques (attacker is node 20)

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



Sleep Deprivation attack

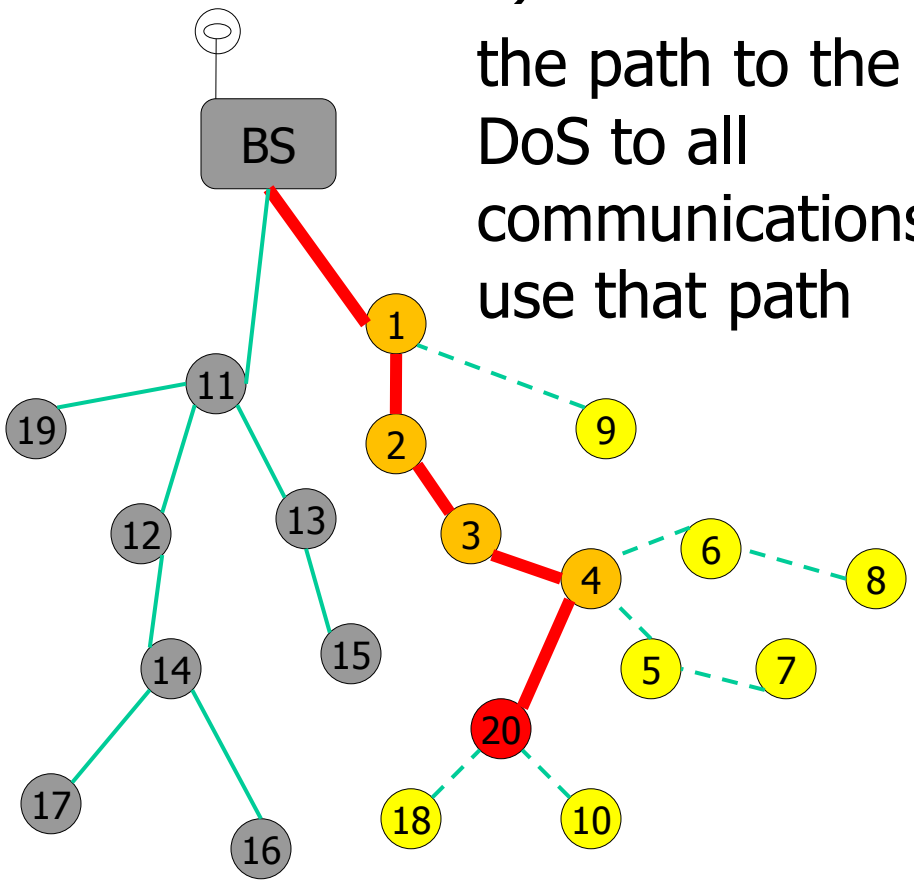


Two effects:

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

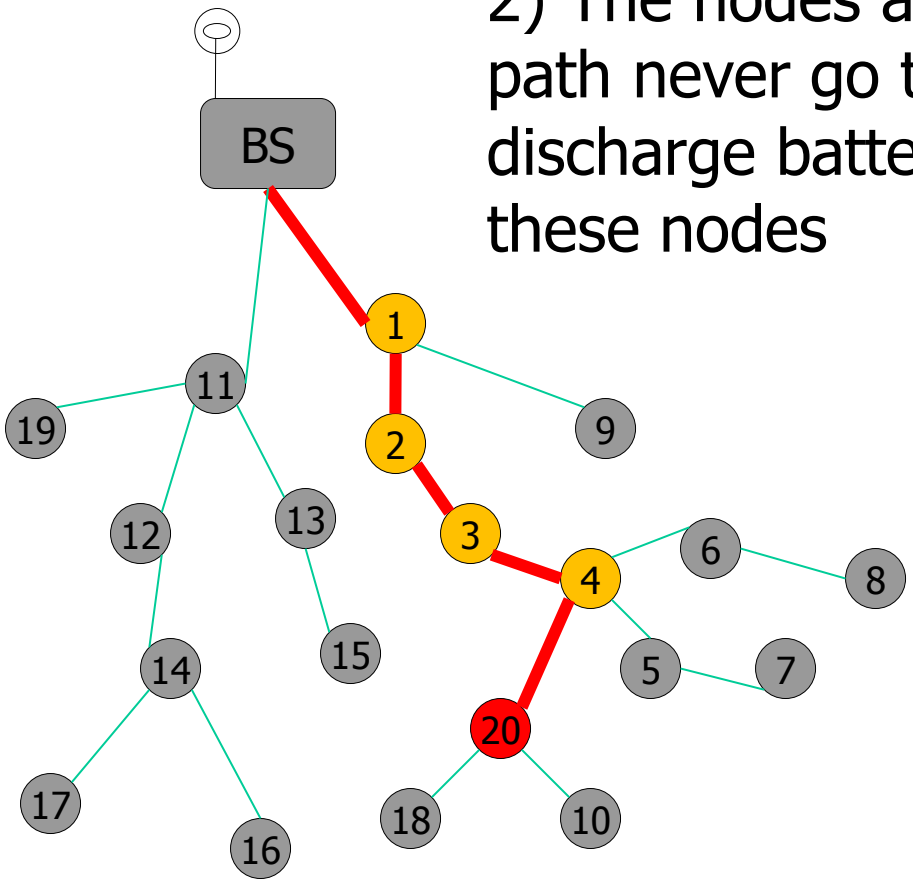
2) The nodes along the path never go to sleep → discharge batteries of these nodes

Victims of DoS



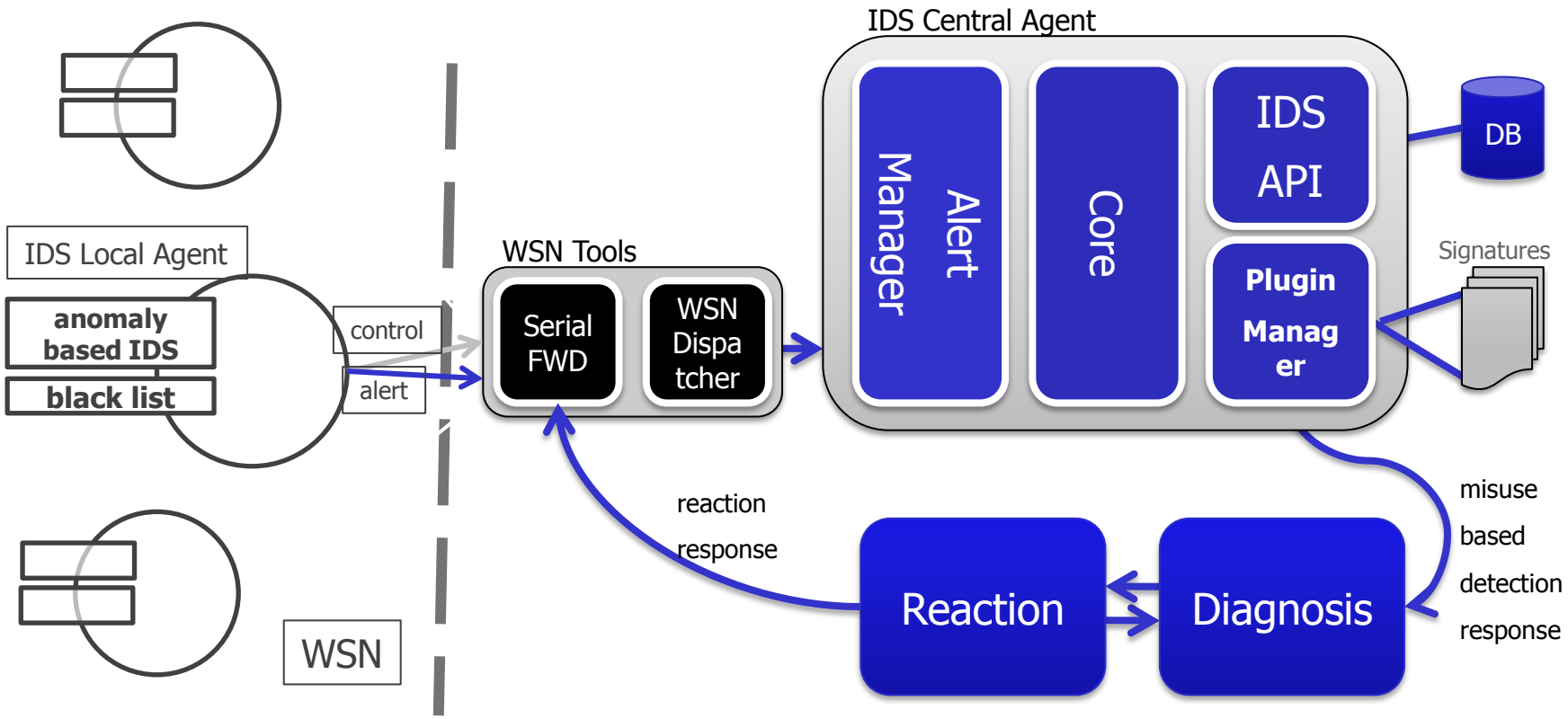
1) The attack overloads the path to the BS → DoS to all communications which use that path

Victims of Battery Discharge



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

Conceptual Architecture



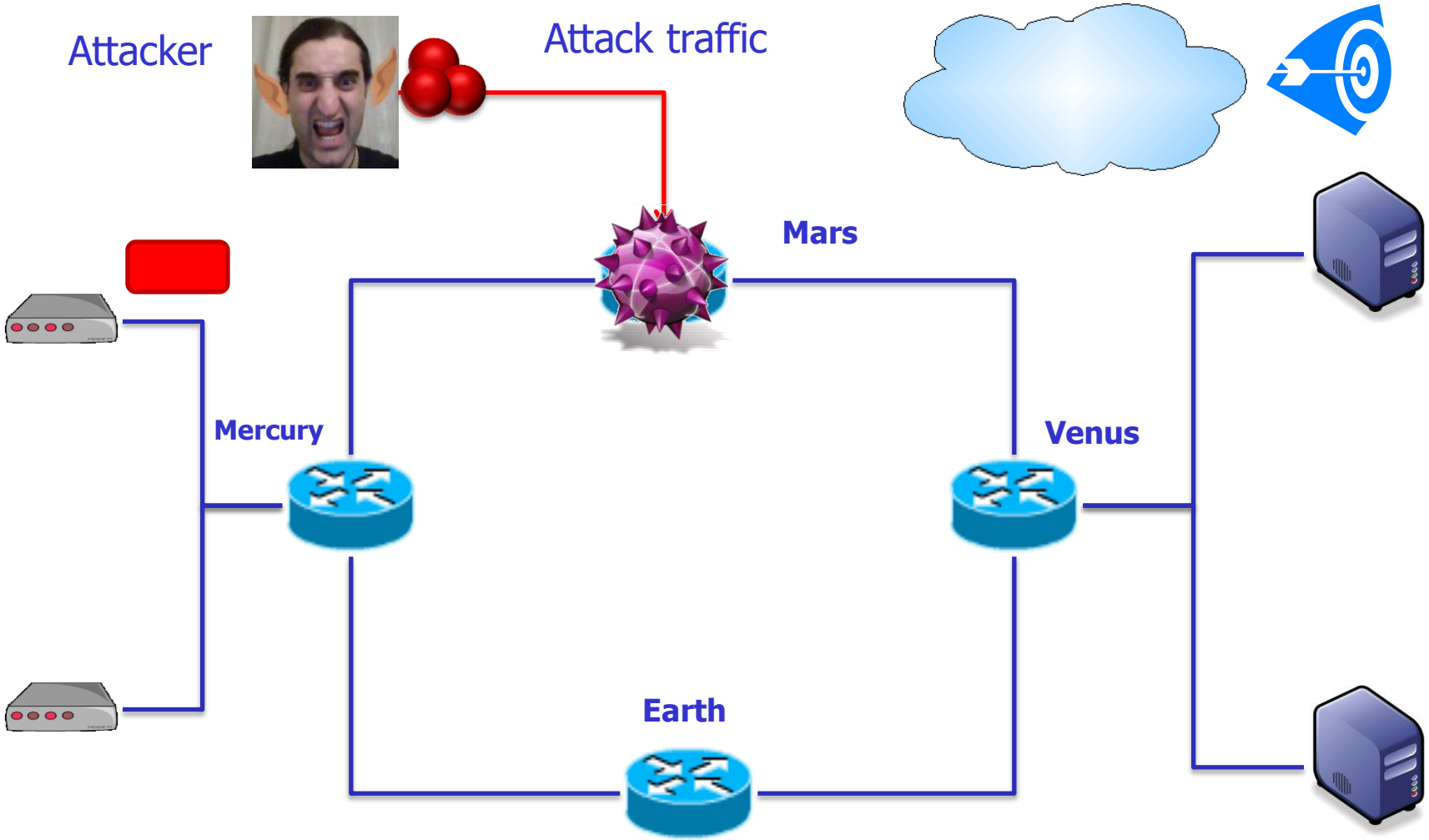
- *Twice* hybrid solution:
  - Distributed and Centralized architecture
  - Anomaly based and Misuse based detection

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

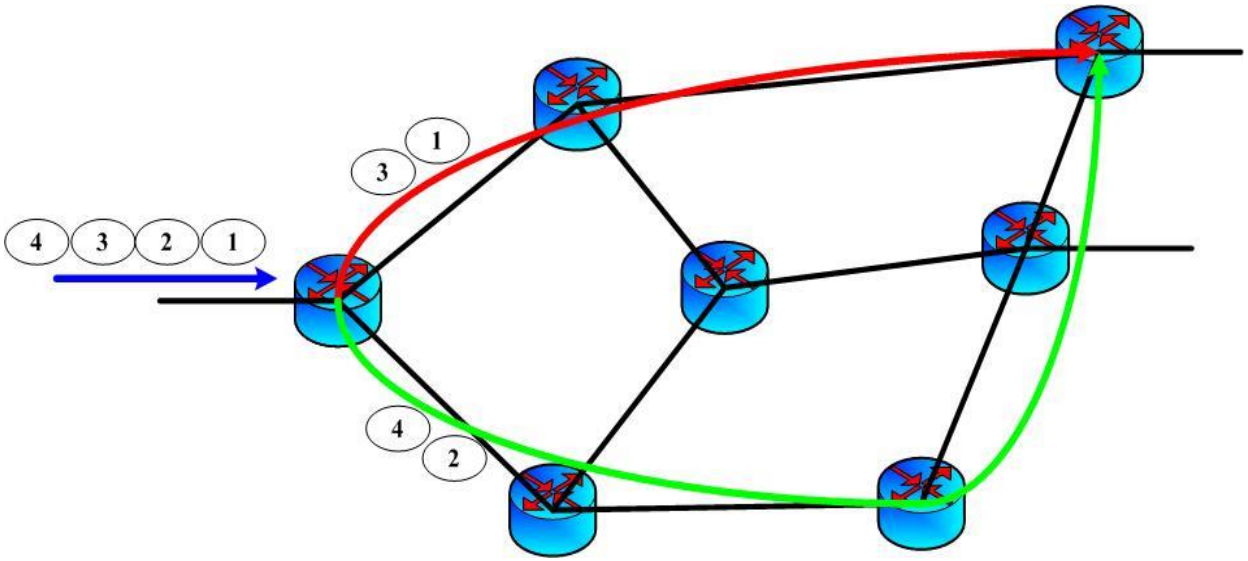
Protecting Critical Flows: an MPLS-based approach

Preserving SEC&DEP monitoring traffic in the face of Attacks

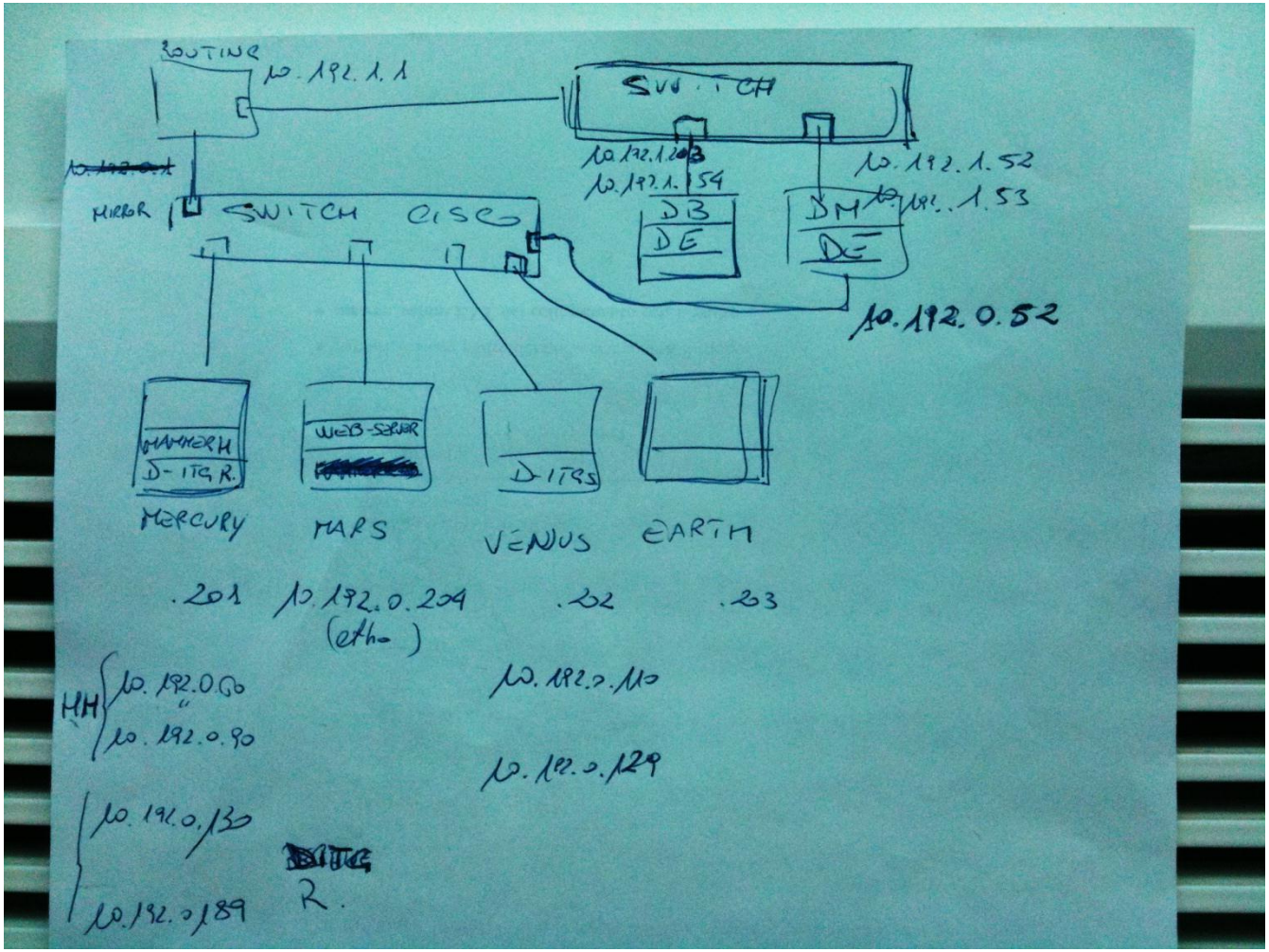


MPLS splitting

- Automatic reconfiguration of the backbone nodes of the monitoring 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



Testbed design ☺



...and the real thing!

Case Studies from the Critical Infrastructure Protection domain


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

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

→(False) belief: **Traditional** CIs were intrinsically secure systems

CI technology today

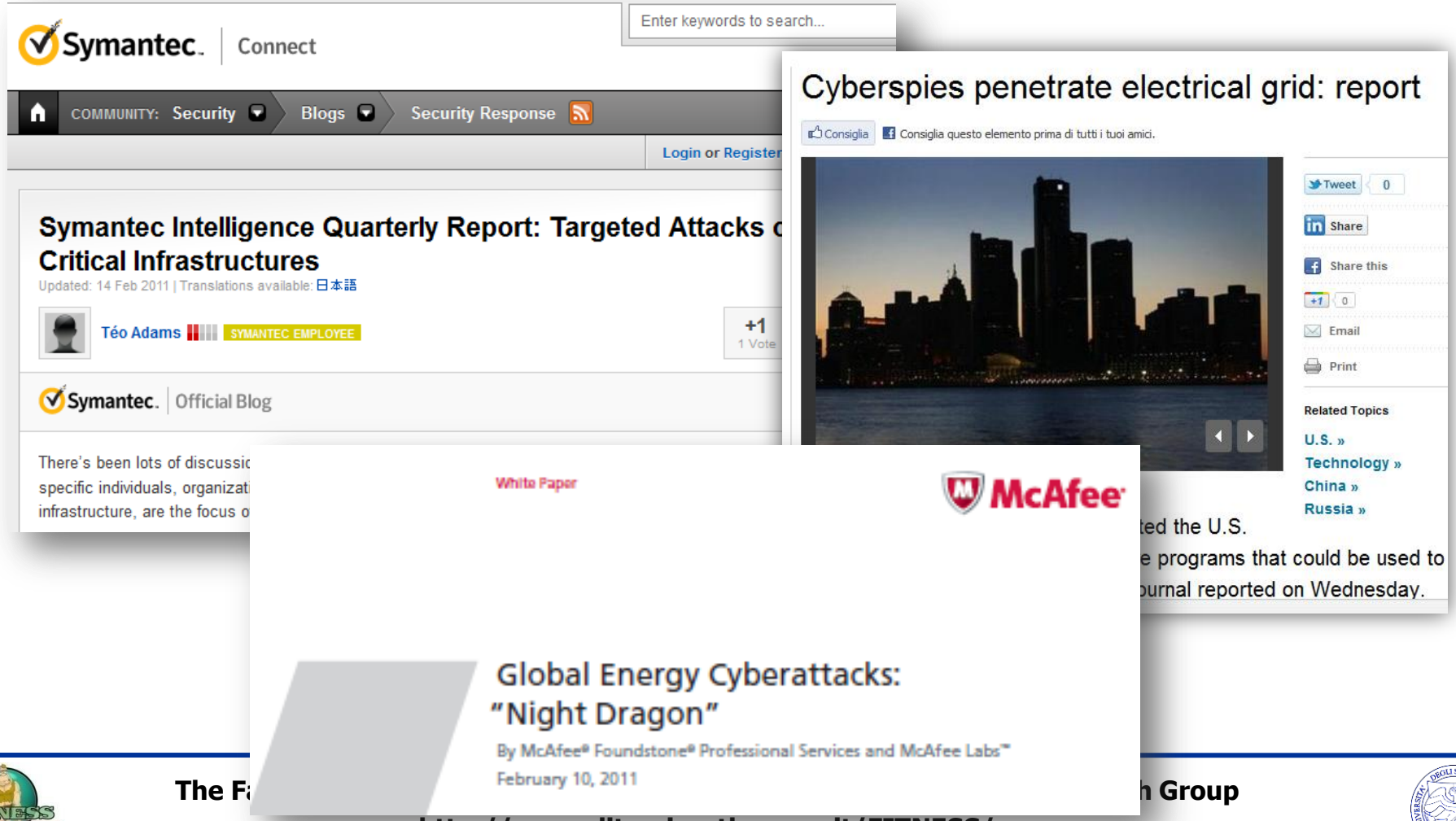
- Commercial-Off-The-Shelf (COTS) components are being massively used for implementing SCADA systems
- Subsystems are being connected using the infrastructure of the corporate LAN, or even WAN links, possibly including the public Internet, as well as wireless/satellite trunks
- Open communication protocols 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

Need for SEC & DEP monitoring in CIs

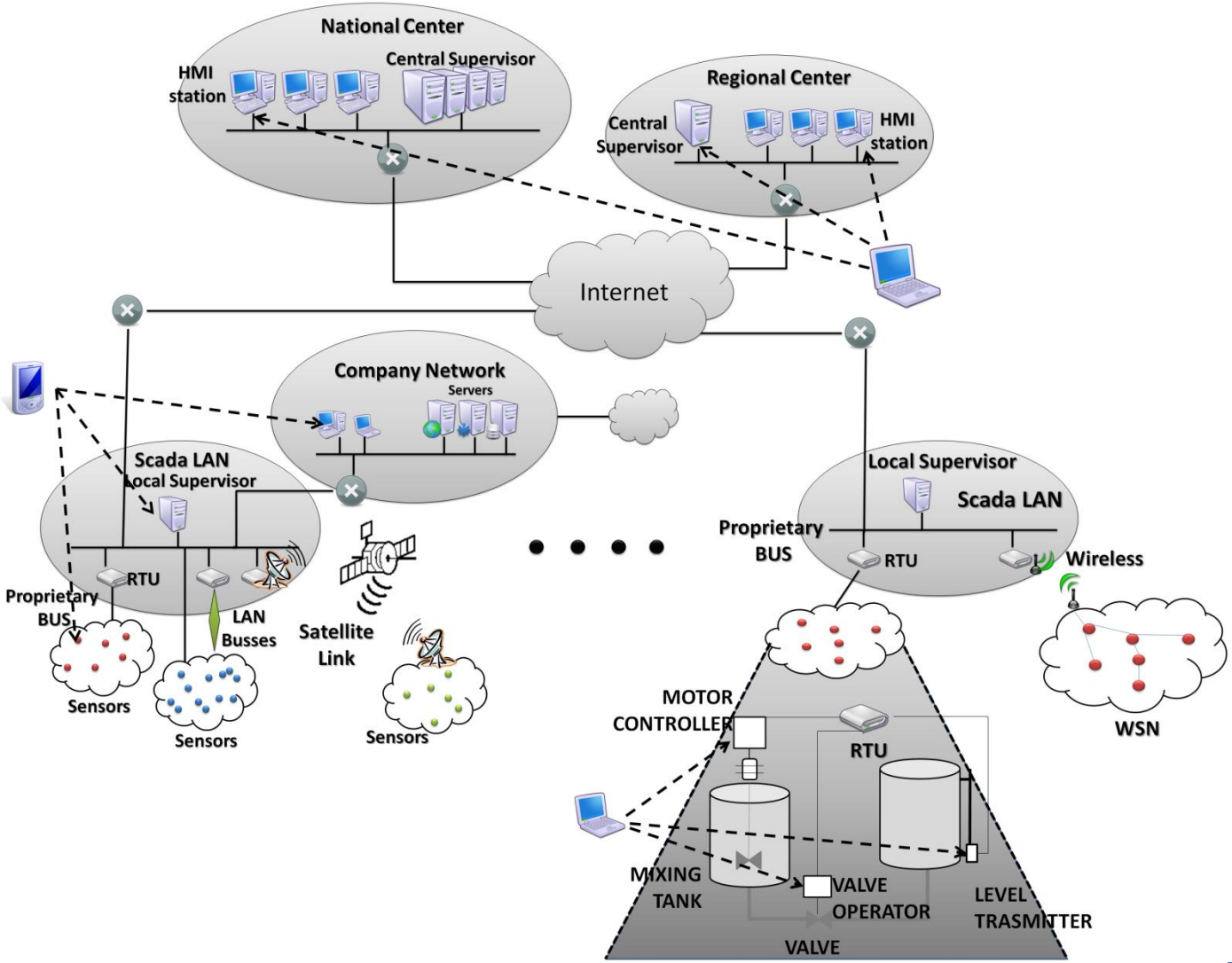
- Critical Infrastructures (CIs) are exposed to major security risks (will provide evidence)
- Trend of security incidents:
  - external borne → dramatic increase
  - internal borne → basically stable
  - accidental → increased only slightly
- The shared communication infrastructure has become an obvious 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

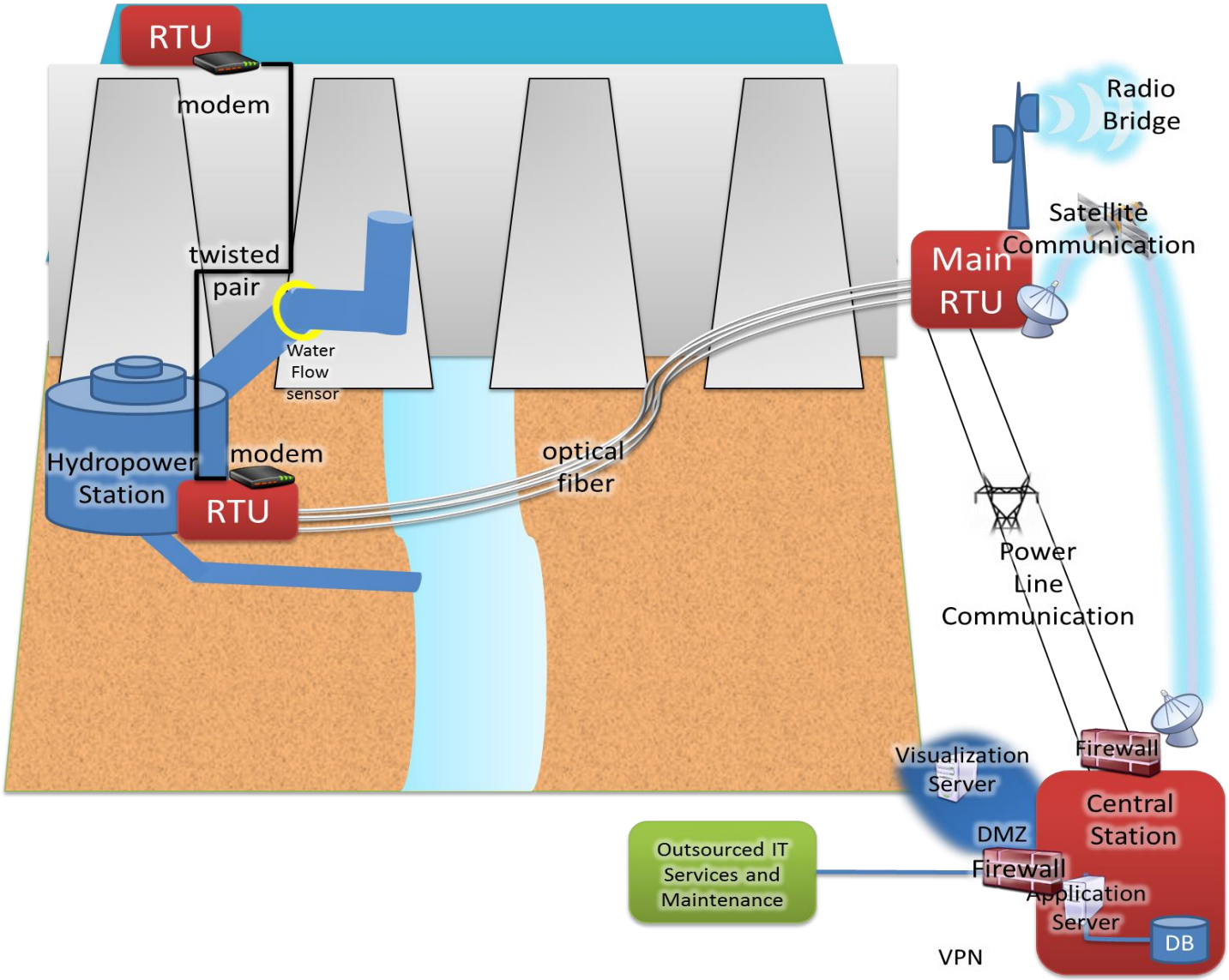
Evidence is showing that Critical Infrastructures (CIs) are already exposed to Cybersecurity attacks, and they will be even more so in the future



Typical architecure of a SCADA system



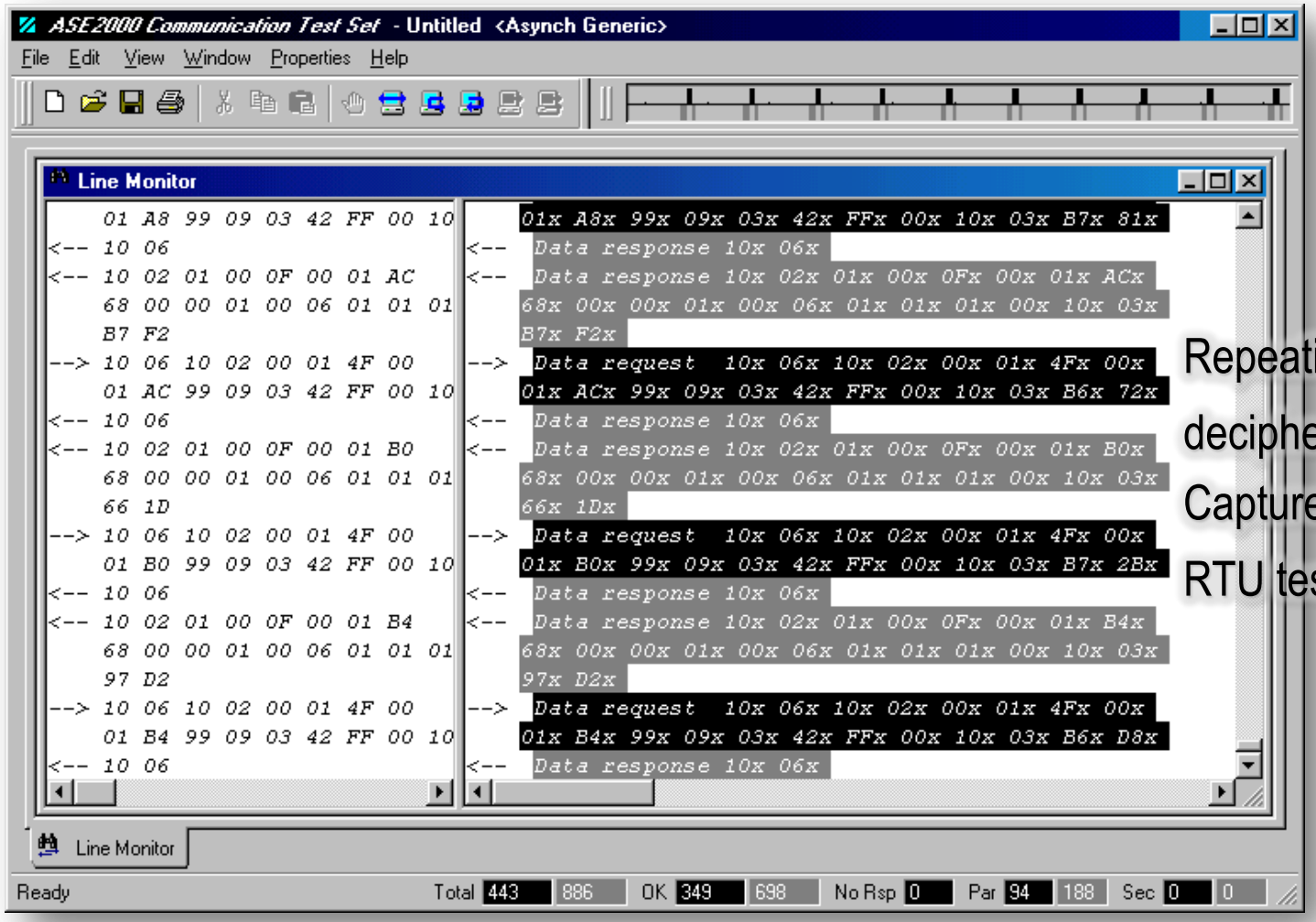
Protecting a dam



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



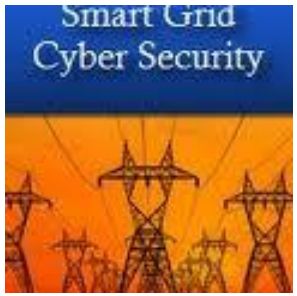
Repeating easily decipherable format Captured by RTU test set

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

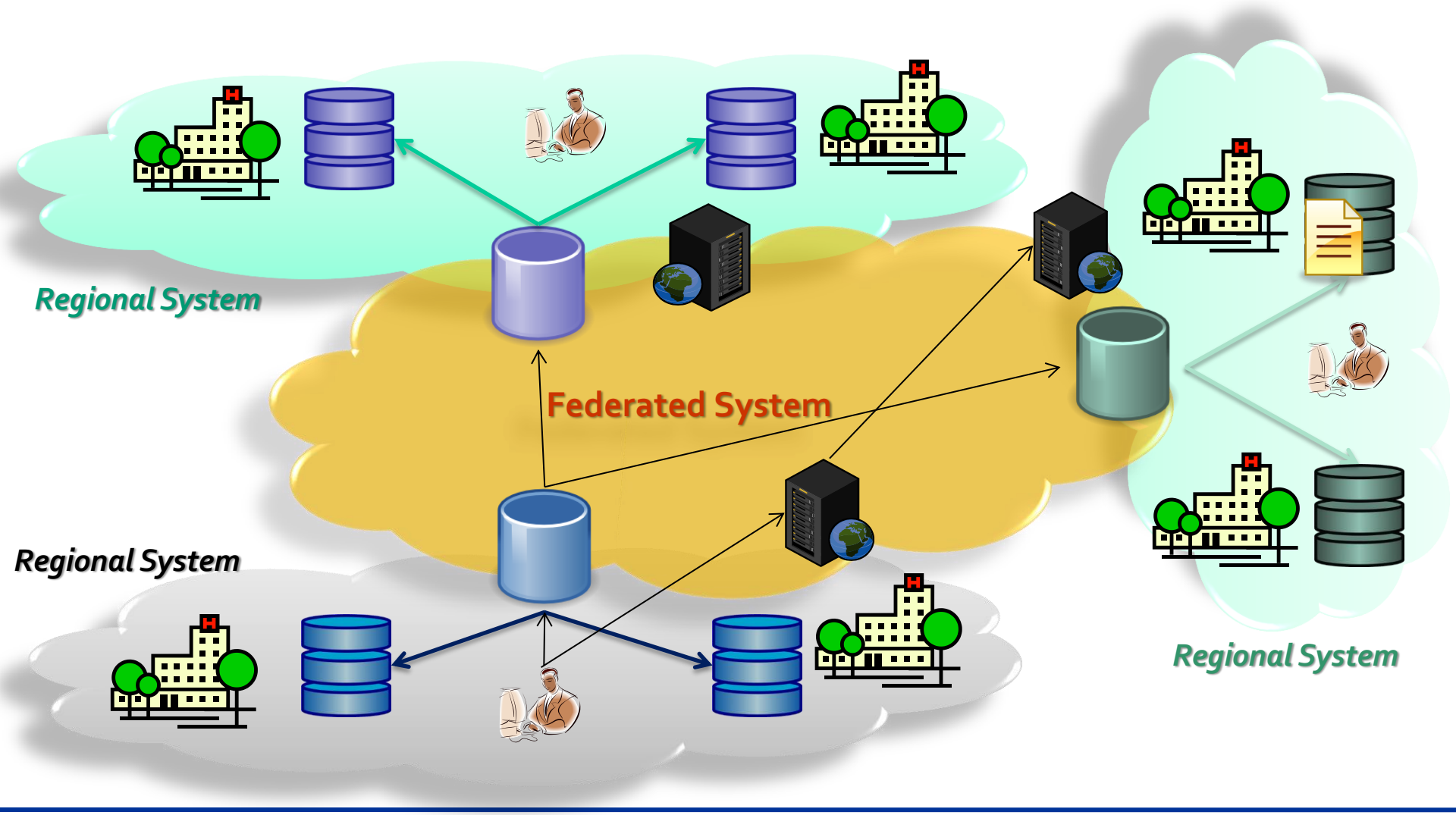


Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, National Institute of Standards and Technology Interagency Report 7628, vol. 1 289 pages (August 2010)

Summary of Main Findings

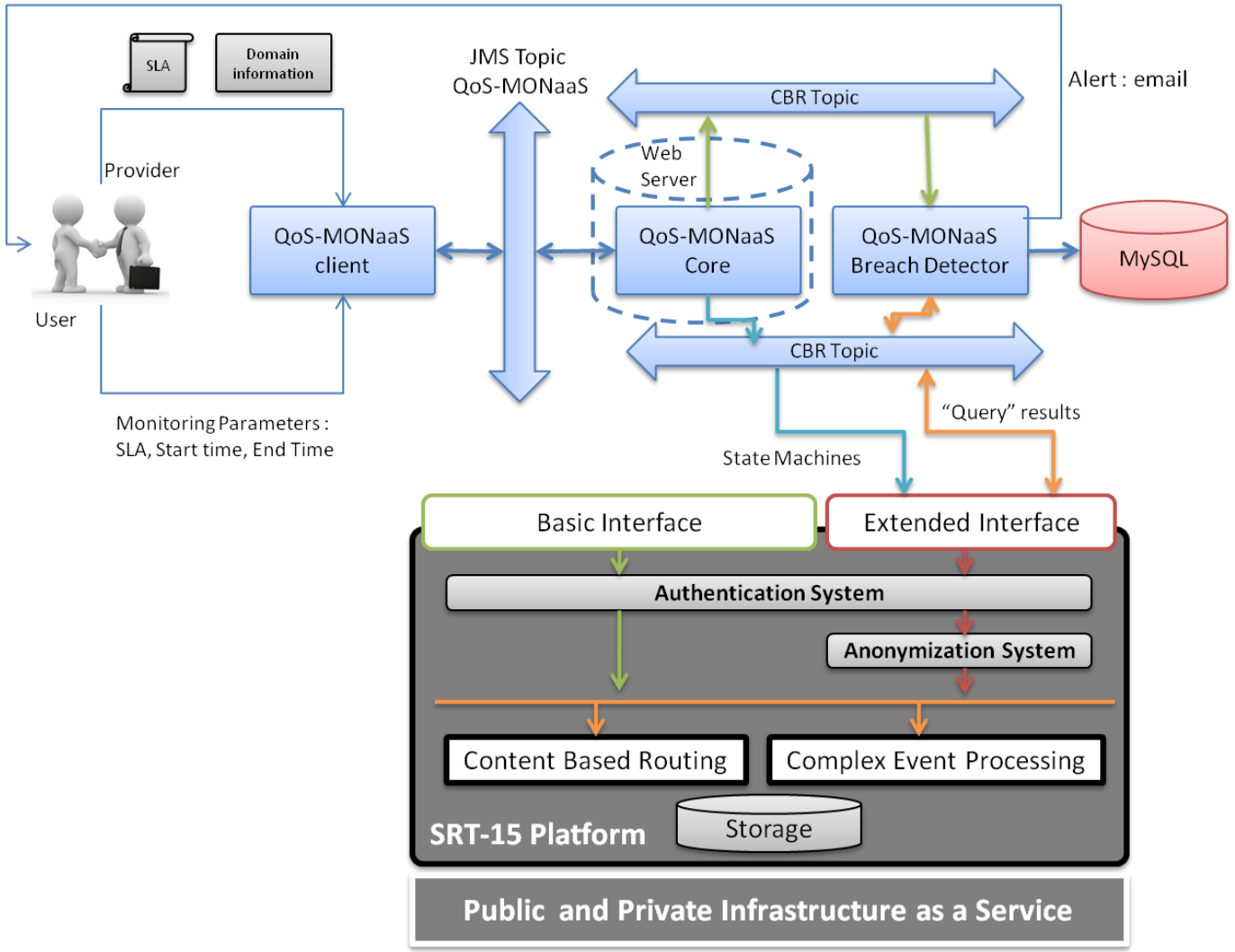
- We have conducted a security assessment of the key technologies enabling data collection in Power Grids
- The study has been conducted on commercial grade products (specifically, a mix of open source and proprietary ones)
- We have collected evidence proving that state of the art components for building 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

Electronic Health Record (EHR)



Case Study:
QoS monitoring in the cloud

QoS-MONaaS: QoS MONitoring as a Service



Acknowledgements & Contact Info

Acknowledgements – 1/2

- INTERSECTION
  - http://www.intersection-project.eu
- INSPIRE
  - http://www.inspire-strep.eu
- INSPIRE-INCO
  - http://www.inspire-inco.eu
- MASSIF
  - http://www.massif-project.eu

Acknowledgements – 2/2

- SRT-15
  - www.srt-15.eu
- SAWSOC
  - Coming soon…..

SAWSOC


Security Research
SAWSOC
Situation AWare Security Operations Center
(SAWSOC)
Topic SEC-2012.2.5-1 Convergence of physical and cyber security
Project Coordinator: Anna Maria Colla
annamaria.colla@selexelsag.com
Technical Coordinator: Luigi Romano
luigi.romano@uniparthenope.it
SELEX ELSAG
Secure Networking Solutions
A Finmeccanica Company

Contact Info

Luigi Romano

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

The Fault and Intrusion Tolerant NEtworked SystemS (FITNESS) Research Group
http://www.dit.uniparthenope.it/FITNESS/