Securing SCADA Systems Using Open Source Software

Engr. Prof. Dr. Athar Mahboob, TI
Professor and Dean
Faculty of Engineering & Applied Sciences
DHA Suffa University
Karachi, Pakistan
Email:athar.mahboob@dsu.edu.pk

2nd National Conference on Information Assurance
Military College of Signals, Rawalpindi
December 11-12, 2013

About Dr. Athar Mahboob, TI

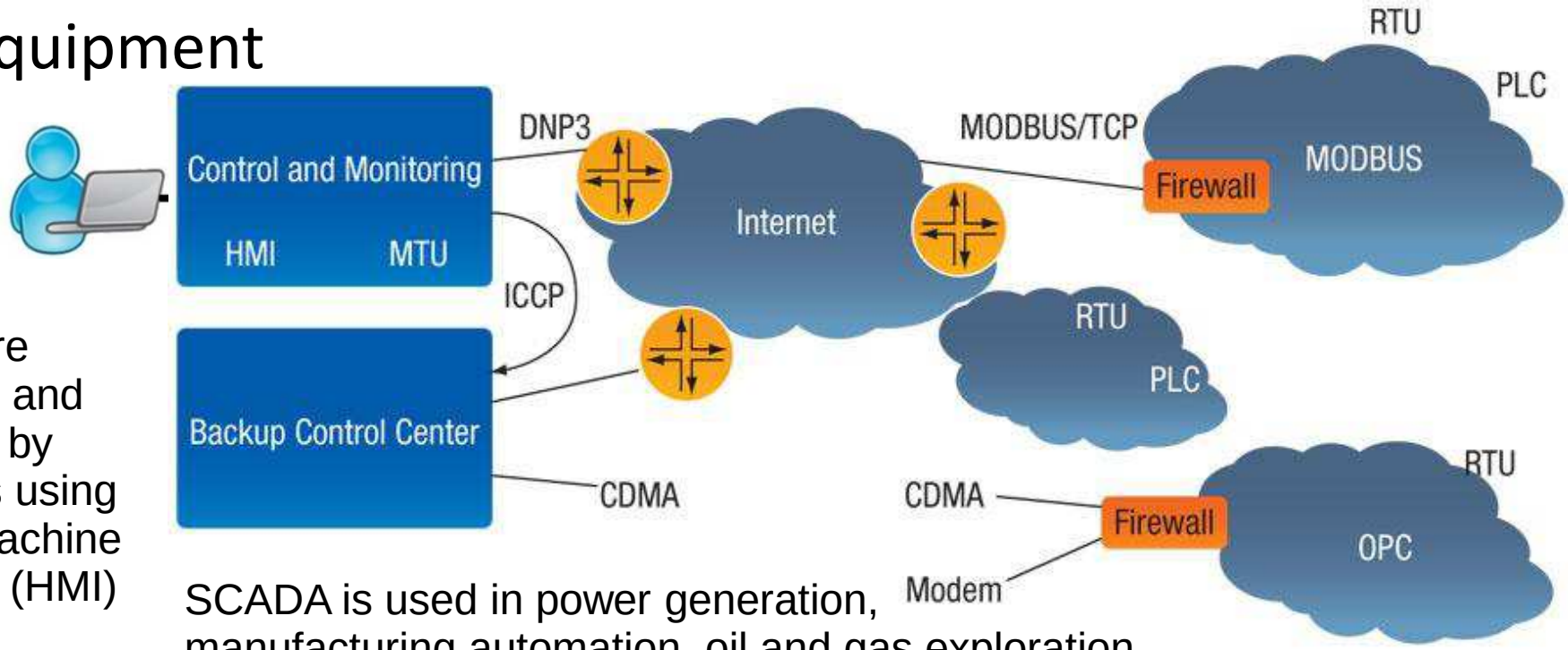
- Professor, Dean & Director IT, DHA Suffa University, Karachi 2012-2013
- PhD (Information Security & Cryptology), NUST, Pakistan, 2005
- MS & BS (Electrical Engineering), Florida State University, USA, 1995/1992
- Awarded Tamgha-e-Imtiaz (TI) by the President, Islamic Republic of Pakistan on account of valuable contributions to Engineering and Science & Technology Education in the country, 2012
- 25+ years of Teaching, Research, Industrial and Management Experience, 1988-2013
- President Ibn Khaldun Systems: successfully managed more than 50 industrial projects 2005-2012
- Former Head of Computer Science Department, PNEC-NUST, Karachi, 2011-2012
- Former Head of Computer Engineering Department, Sir Syed University of Engineering & Technology (SSUET), Karachi, 1996-2001
- Former Head of Linux Task Force for promotion of Linux and open source software, Ministry of Science & Technology (MoST), Government of Pakistan, 2001-2002
- HEC Approved PhD Supervisor
- Published a book on Cyber Security which is being used as a Textbook in advance universities of USA and Europe, 2011
- Invented: Bitwizard Secure Communication Device for VoIP Phones
- Trained large number of students and professionals in Linux, Cryptography, Information Security and Internet Technologies, 1996-2013
- Published more than 30 research papers in referred international journals and international conferences, 1998-2013

Presentation Outline

- What are SCADA Systems?
- Top issues and requirements of Industrial Cyber Security
- Addressing SCADA Security with Open Source Software
- Training testbed for SCADA Cyber Security
- Conclusion

What is SCADA?

- SCADA (**S**upervisory **C**ontrol **a**nd **D**ata **A**cquisition) automates industrial control and monitoring
- Field sensors, PLC (Programmable Logic Controllers) and RTU (Remote Telemetering Unit) are vital parts of SCADA
- These devices control and monitor industrial process equipment



Industrial devices are monitored and controlled by Engineers using Human Machine Interfaces (HMI)

SCADA is used in power generation, manufacturing automation, oil and gas exploration and utilities monitoring and control

What SCADA does?

- SCADA can:
  - Turn ON and OFF equipment automatically under the control of software OR remotely through human interface devices
  - Monitor parameters such as temperature, pressure, flow rate, pH etc.
  - Set off alarms based on collected historical and observed instantaneous data
  - Be operated through web based interface or specialized software on networked machines

Why is SCADA Security so Important?

- Networking allows sharing of data for maintenance and management thus improving process and industrial productivity.
- The control networks are typically organized with a star topology, with many sensors and actuators connected to a control center
- Protocols such as DNP and Modbus enable anyone who can communicate with a sensor to read it, while anyone who can send data to an actuator can give it instructions

Why is SCADA Security so Important?

- In March 2007, the Department of Energy's Idaho National Laboratory made a video demonstrating the 'Aurora vulnerability' in which a series of 'on' and 'off' commands are sent to a generator, timed in such a way as to bring it out of phase and thus destroy it.
- The video was released to the press in September 2007; in it, a large generating set shudders, emits smoke, and then stops.
- This helped make clear to legislators that the confluence of the private but internally open systems using in industrial control, with open networking standards such as TCP/IP, was creating systemic vulnerabilities.

Earlier Approach: Security through Obscurity, Air-Gap Principle – not feasible / 1

- Early industrial control systems used completely private networks – thus designers gave no thought to authentication or encryption.
- Private networks are expensive to maintain and difficult to access
- The prospect of orders-of- magnitude cost reductions led engineers to connect control systems to the Internet
- Such interconnected systems benefited from “security through obscurity” until recently

Earlier Approach: Security through Obscurity, Air-Gap Principle – not feasible / 2

- The SCADA command strings would be unknown even if a hacker gains access to the system
- For example“0F1AC980” ……the hacker needs to be a process engineer to know it means opening certain valves of boiler
- However, with the increasing use of COTS (Commercial off-the-shelf software) and IP connectivity, SCADA systems are no longer obscure for hackers

How Industrial Cyber Security is Different from Conventional IT Security

- Common IT platforms either get routinely patched every month (PCs) or else replaced frequently (mobile phones).
- Control systems may remain in use for decades, and many of their components were never designed for remote upgrade.
- The costs of taking down (say) a nuclear power plant to patch components may also be very substantial, while some systems require 99.999% availability – which translates into less than 6 minutes downtime per annum.
- The upshot is that control systems are patched late or not at all.
- Patch management has thus become contentious, with some firms believing that vulnerability information should not be published, and arguing in favor of a private CERT or even just reporting to the FBI/RCMP as mandated by NERC CIP

How Industrial Cyber Security is Different from Conventional IT Security

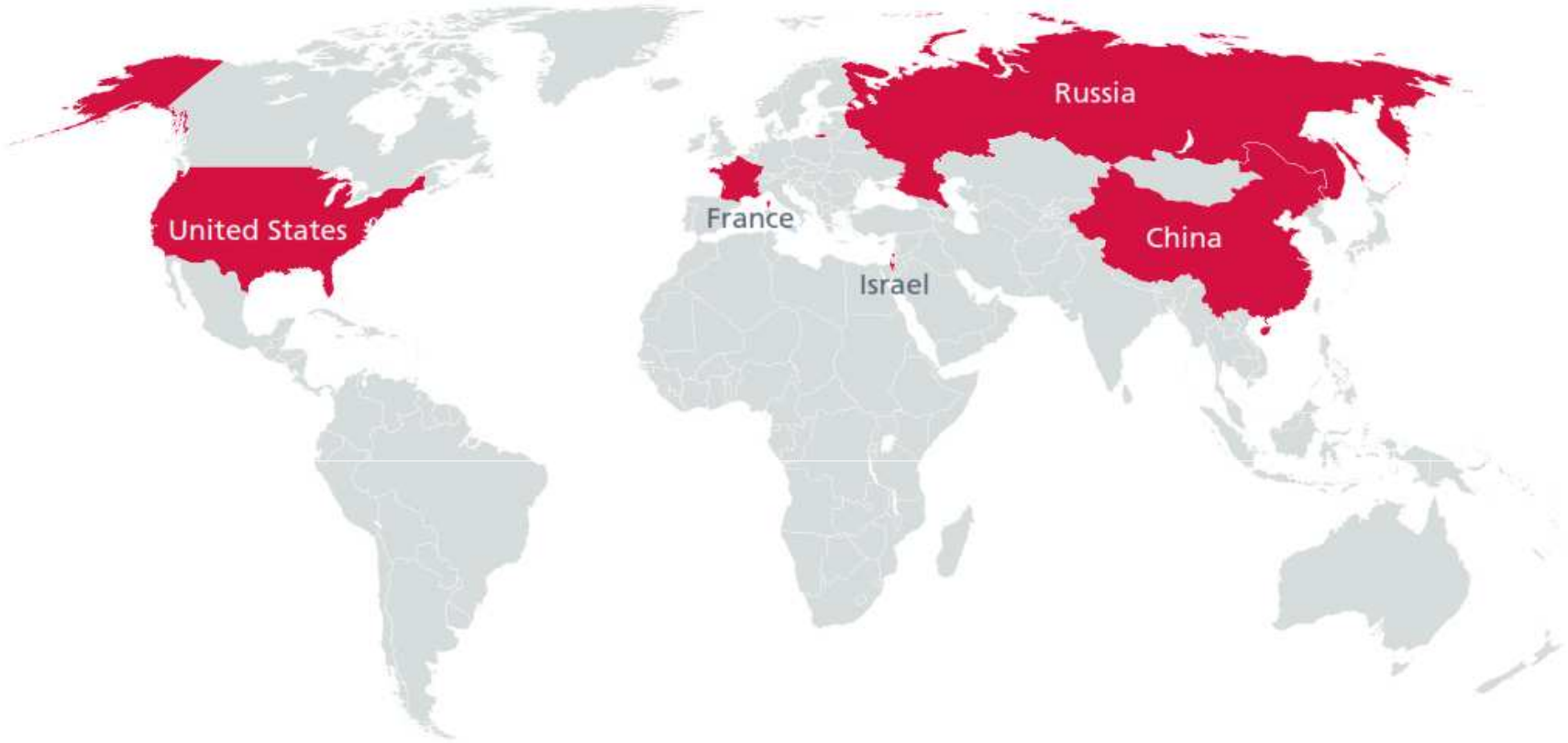
- Industrial environment is different from enterprise IT environment – intrusions in Industrial Environment can cause:
  - Environmental damage
  - Safety risk
  - Lost production
  - Power outages
- IT can tolerate delays and loss of data; IC cannot!! IC security must be proactive, not reactive

Emerging Threats to Cyber Industrial Systems - All is fair in love and war !!!

STATE ACTORS ARE PART OF THE THREAT ECONOMY TOO

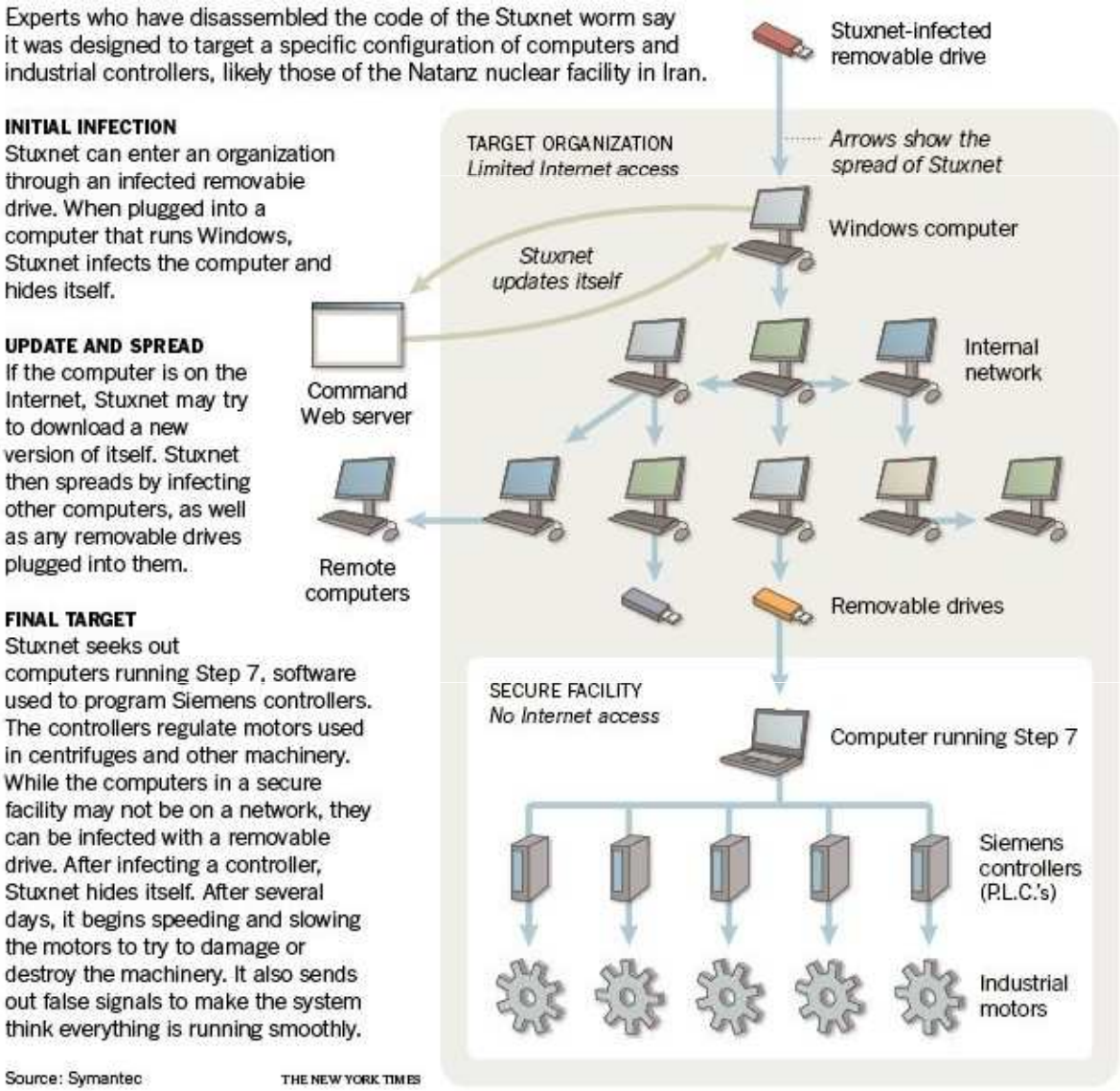
PUBLIC-PRIVATE PARTNERSHIP :-)

Countries Developing Advanced Offensive Cyber Capabilities



Advanced Persistent Threat - APT

- The attack techniques started from self replicating code evolved into Advanced Persistent Threat
  - Use 0-day
  - Be stealthy
  - Target users
  - Target indirectly
  - Exploit multi-attack vectors
  - Use “state-of-the-art” technique
  - **Be Persistent**
- Hacking is no more about fun
  - Corporate Espionage
  - State Secrets
  - Cyber “Sabotage”



Stuxnet – A Preview of Upcoming Threats: Advanced Persistent Threat (APT)

- June, 2010 – **StuxNet Worm**
- **Target:** Natanz Nuclear Facility
- **Motivation:** Cyber Sabotage?

Top SCADA Security Issues – According to Experts & Case Studies

- Inadequate security policy
- Lack of Layered Defense
- Remote access without controls
- Missing logs of access
- Internet based SCADA
- Lack of forensic and audit methods
- Gaming and non-related software on control pc
- Lack of detection tools
- Control software not scrutinized
- Control command and data not authenticated
- Advanced Persistent Threat

All of these imply need for better tools and training for industrial cyber security workers

Security Infrastructure for Defense in Depth of SCADA Systems

- Firewalls
- Intrusion Detection Systems/Intrusion Preventions Systems
- Deep-packet Inspection
- Antivirus
- Anti-malware
- Security Event Logs
- Access Control Systems
- Strong Password
- Multi-factor Authentication
- Public Key Infrastructure
- Network Security Protocols (IPSec, TLS, PPTP, etc.)
- Application level gateways
- VPN gateways

Defense in depth is an information assurance (IA) concept in which multiple layers of security controls (defense) are placed throughout an information technology (IT) system. Its intent is to provide redundancy in the event a security control fails or a vulnerability is exploited that can cover aspects of personnel, procedural, technical and physical for the duration of the system's life cycle. (Wikipedia)

Defense-in-Depth Defined

The synergistic integration of layered Information Assurance practices, providing resilient IT services while minimizing failures and intrusions.

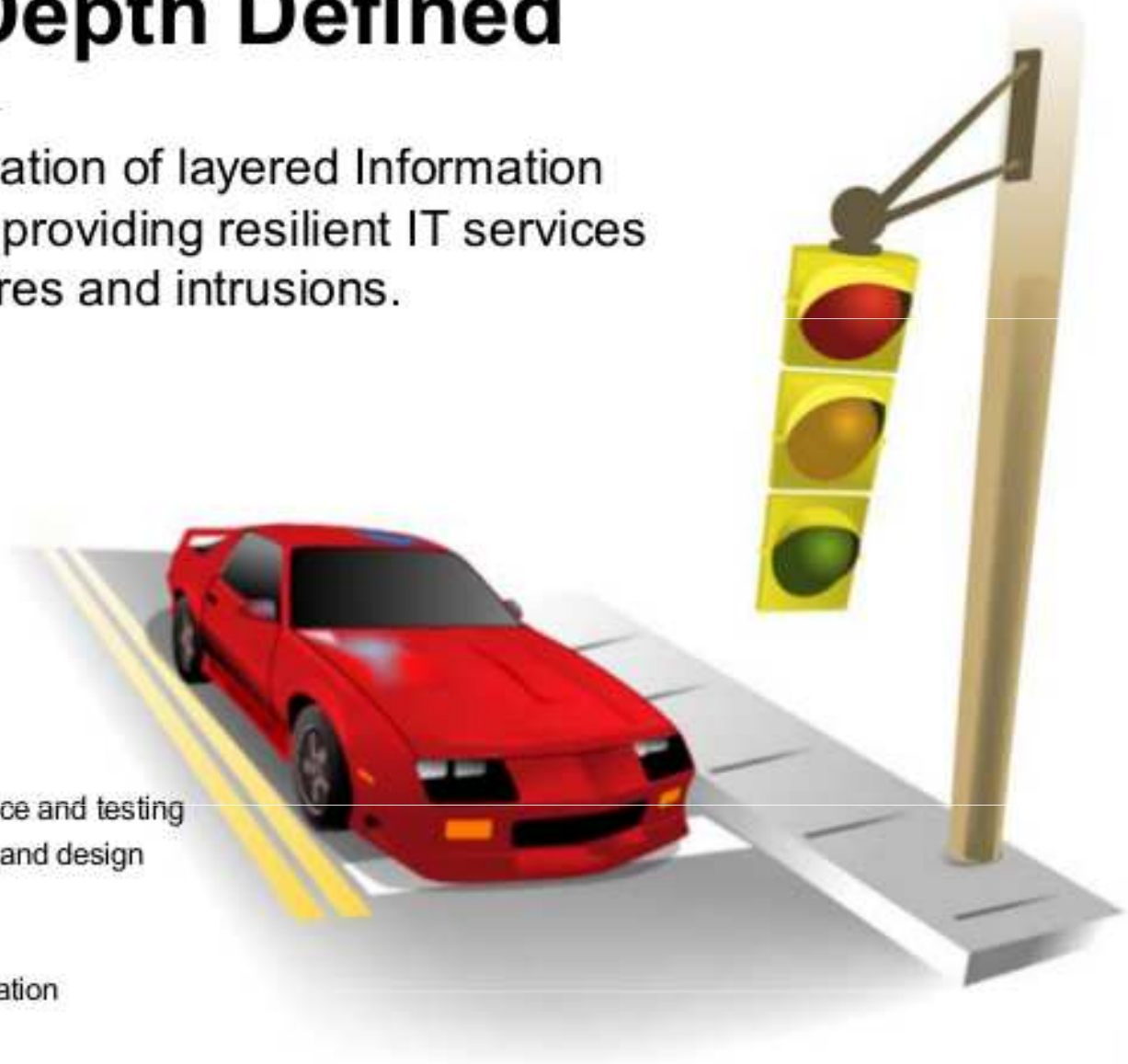
The Driving Analogy

Service

Safe, reliable transportation

Layered Controls

- Multiple airbags
- Seatbelts, bumpers
- Crush zones
- Extensive quality assurance and testing
- Time-proven engineering and design
- Reinforced cockpit
- Helmets
- Driver licensing and education
- Traffic laws, etc.



© 2006 Carnegie Mellon University

CERT

Defense-in-Depth Components

© 2006 Carnegie Mellon University

Deploy ing Defense in Depth Results in Massive Security Event Logs

What Security Event Logs?

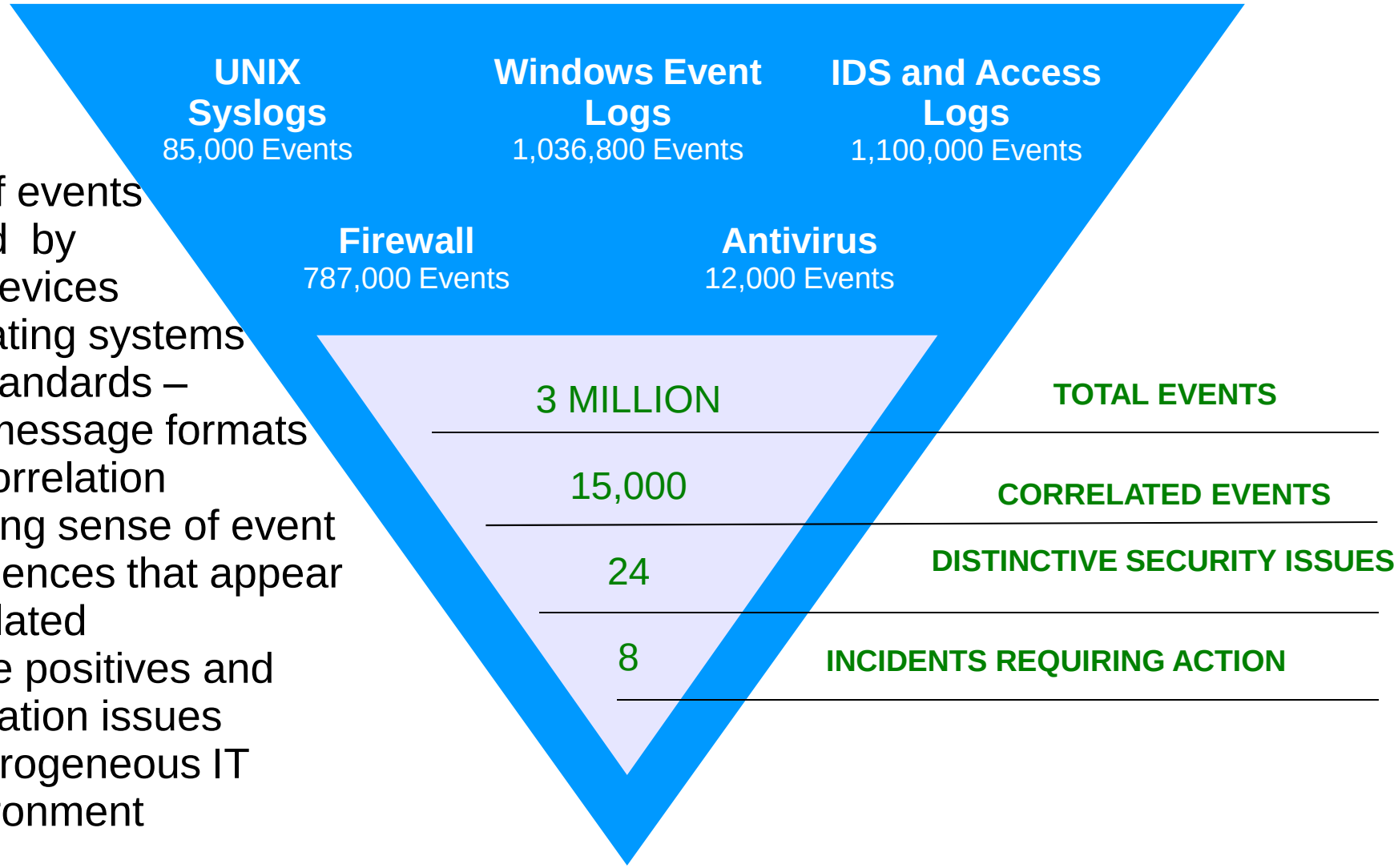
- Audit Logs
- Transaction Logs
- Intrusion Logs
- Connection Logs
- System Performance Records
- User Activity Logs
- Misc. alerts and other messages

From Where?

- Firewalls/Intrusion Prevention
- Routers/switches
- Intrusion Detection
- Servers, Desktops, Mainframes
- Business Applications
- Databases
- Anti-virus
- VPNs

The Challenge of Managing Security Information

Inverted Pyramid of Event Significance



- Millions of events generated by security devices and operating systems
- Lack of standards – different message formats
- Difficult correlation
  - Making sense of event sequences that appear unrelated
  - False positives and validation issues
  - Heterogeneous IT environment

Security Information & Event Management Systems (SIEM)

- "A SIEM or SIM is a computerized tool used on enterprise data networks to centralize the storage and interpretation of logs, or events, generated by other software [or hardware] running on the network"
- A new concept (About 10 Years old)
- A natural evolution of log management
- A SIEM enables organizations to achieve round-the-clock 'pro-active' security and compliance
- Increase overall security posture of an organization
- Turn chaos into order
- Aggregate log file data from disparate sources
- Create holistic security views for compliance reporting
- Identify and track causal relationships in the network in near real-time
- Build a historical forensic foundation

Why Open Source for SIEM?

- Commercial products have a high cost of entry barrier
- User can become confused with the:
    - Marketing terms
    - Feature bloat
- Open source SIEM has matured – can compete head-on with commercial offerings
- Open Source SIEM can even be used as a learning tool – requirements analysis tool for a commercial SIEM specifications
- Open Source can be used to create simulated industrial cyber security training environment

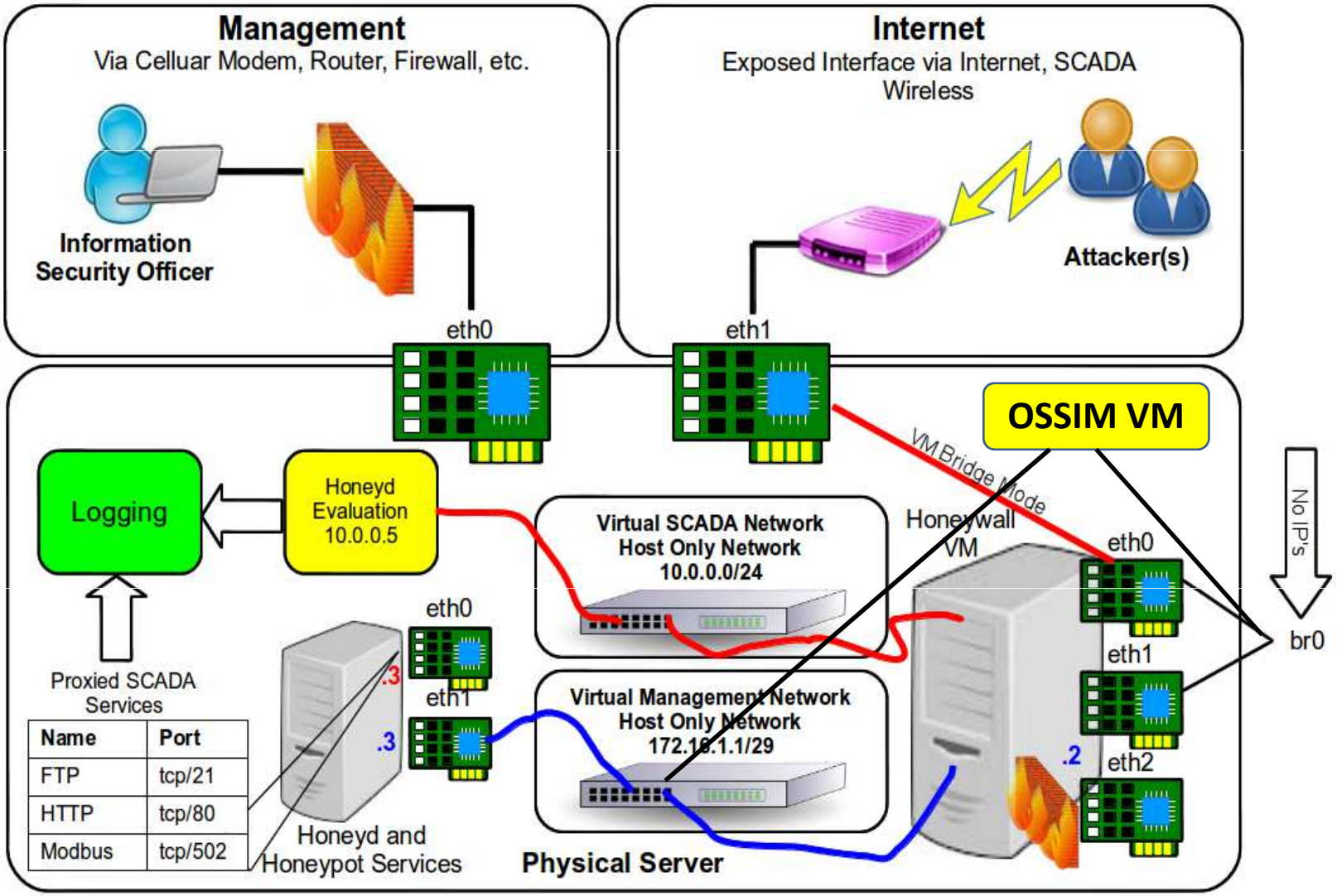
Why a Training Testbed for SCADA Security?

- Live /production industrial systems cannot be used for such training – because of critical nature
- IT Security experts need to know the workings of industrial systems – most industrial protocols developed outside of IT
- Simulation is a powerful teaching/learning aid – very cost effective
- Multicore CPUs (8 cores) in medium/high-end laptops make possible to run 4 or more VMs concurrently – sufficiently real-world training scenarios can be created
- All components planned to be upgradeable

SCADA Security Training Testbed

Virtualbox on high-end laptop runs 4 VMs

1. SCADA PLC
2. Honeyd
3. OSSIM
4. Management



Industrial Cyber Security Training Testbed Components

- Based on the ideas in [7] – however, a modern and more maintainable implementation
- All devices running as Virtual Machines using **Virtualbox Hypervisor** – user-friendly and high performance
- A **Modicon Quantum PLC** is simulated - exposes the **Modbus TCP** protocol and provides data points list from an electric substation
- A honeypot is created using **honeyd**
- **OSSIM** 4.3 SIEM is running on a VM as ALL IN ONE (sensor, collector, framework, database) with large number of integrated security tools
- Other components include: **Walleye, Sebekd, MySQL, Argus, Snort, rsyslog**

OSSIM - Integrated Cyber Security Tools

- Snort
- Ntop
- Fprobe
- NFDump
- NFSen
- OCS
- Nagios

- OpenVAS
- Nikto
- OSVDB
- OSSEC
- KISMET
- NMAP
- P0f
- ArpWatch

Active Versus Passive Tools

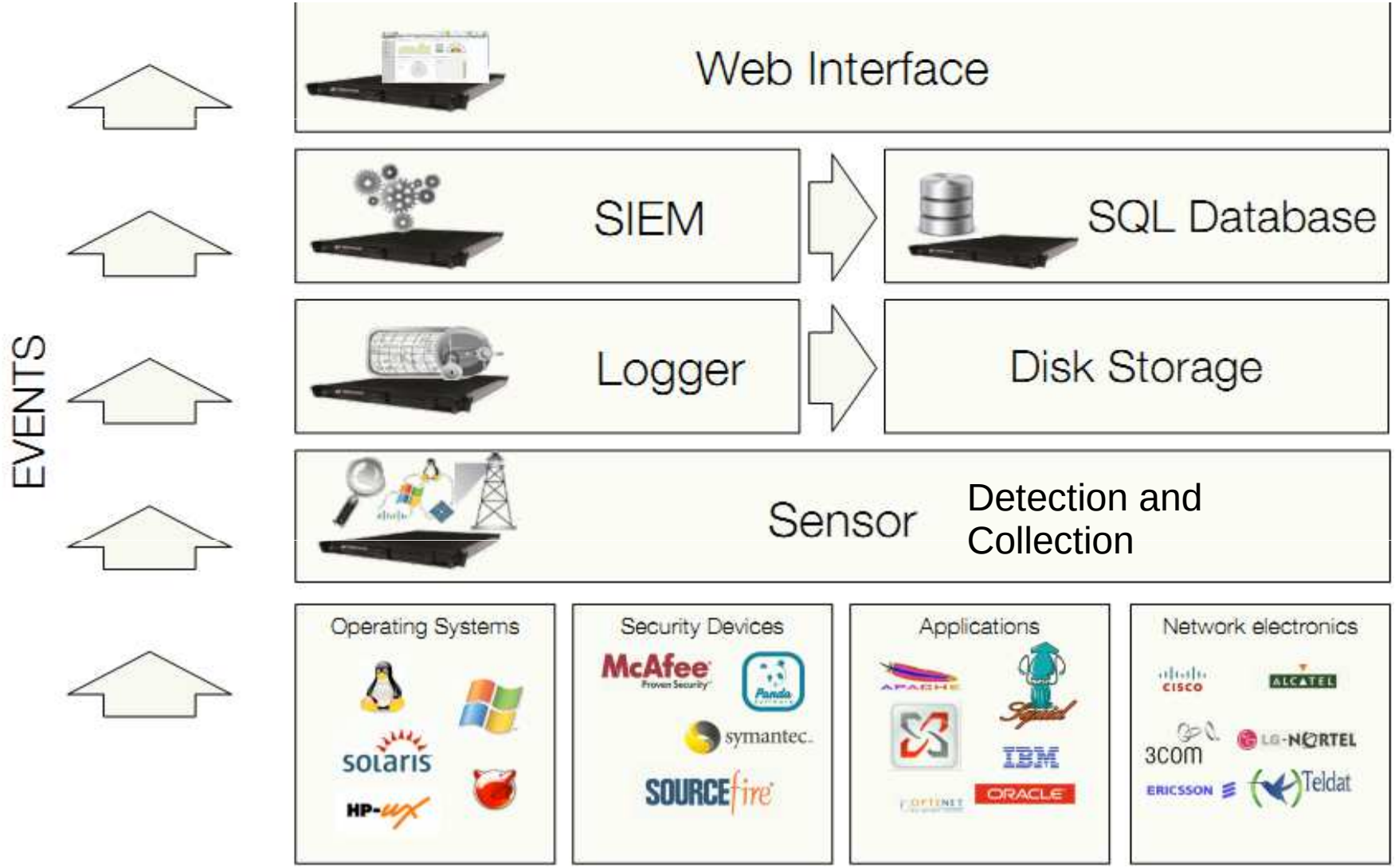
- The different tools integrated in OSSIM can be classified into two categories:
  - **Active:** They generate traffic within the network which is being monitored.
  - **Passive:** They analyze network traffic without generating any traffic within the network being monitored.

The passive tools require a port mirroring /port span configured in the network equipment.

OSSIM - The SIEM

- The SIEM component provides the system with Sec Intelligence and Data Mining capacities, featuring:
  - Real-time Event processing
  - Risk metrics
  - Risk assessment
  - Correlation
  - Policies Management
  - Active Response
  - Incident Management
  - Reporting

SIEM Concepts



Further work – we are not done yet

- Software on Honeywall needs to be updated so that it can integrate easily with the SIEM. This may require the creation of an entirely new VM on a more recent Linux distribution using more recent versions of all the software components of the Honeywall. An updated honeyd somewhat on the lines of HoneyDrive project [12] appears a feasible option. Furthermore, use of the OSSIM plugin honeyd to process events on the SIEM needs to be explored.
- Enhancing OSSIM to accept MODBUS events using a plugin to create a taxonomy of SCADA related events so that these could be used to generate alarms in OSSIM and also be used in correlation directives within OSSIM. In this connection we are exploring the use of Digital Bond's PortalEdge SCADA/ICS event classification and normalization project [13] for integration with OSSIM.
- A modbus client to generate malicious requests for the virtual PLC needs to be integrated in the testbed. We are currently working with MOD_RSSIM [14] to achieve this objective.

Conclusion & Summary

- Industrial SCADA systems deployed across the globe for refineries, water treatment, nuclear power plants, oil fields and process plants.
- SCADA systems vulnerable to attacks by hackers
  - Can damage expensive equipment and jeopardize human health and safety in large areas
- Configuring SCADA security using open source security software tools available under Linux technologically and economically feasible
- Systematic approach for securing SCADA systems using open source software developed

References

1. R. Krutz, “Securing SCADA Systems”, John Wiley Publishers 2006, ISBN 978-0-7645-9787-9.
2. A. Mahboob and J. Zubairi, “Intrusion Avoidance for SCADA Security in Industrial Plants”, Proc. CTS 2010, Pages 447-452, IEEE Digital Library.
3. J. Heinanen et. al. “A Two rate Three Color Marker”, RFC2698, Internet Engineering Task Force, http://tools.ietf.org/html/rfc2698, last accessed Oct 14 2013.
4. Wikipedia online “Modbus” http://en.wikipedia.org/wiki/Modbus last accessed Oct 7th 2013.
5. DNP Users Group, “Overview of the DNP3 Protocol”, http://www.dnp.org/pages/aboutdefault.aspx last accessed Oct 7th 2013.
6. W. Shaw, “Cybersecurity for SCADA Systems”, Pennwell Publishers 2006, ISBN 978-1-59370-068-3.
7. SCADA Honeynet, http://www.digitalbond.com/tools/scada-honeynet last accessed on October 10, 2013.
8. Wade, Susan Marie, "SCADA Honeynets: The attractiveness of honeypots as critical infrastructure security tools for the detection and analysis of advanced threats" (2011).Graduate Theses and Dissertations. Paper 12138.
9. Oracle VM VirtualBox, https://www.virtualbox.org/
10. Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security, NIST Special Publication 800-82 (INITIAL PUBLIC DRAFT)
11. AlientVault Press Release, ALIENVAULT RELEASES SCADA SIEM FOR CRITICAL INFRASTRUCTURE PROTECTION, available at http://www.reuters.com/article/2011/05/26/idUS183336+26-May-2011+BW20110526
12. HoneyDrive Virtual Appliance (OVA) with Xubuntu Desktop 12.04, http://bruteforce.gr/honeydrive
13. Digital Bond, PortalEdge SEM Integration, http://www.digitalbond.com/tools/portaledge/portaledge-sem-integration/
14. MOD_RSSIM, Modbus PLC Simulator, http://www.plcsimulator.org/