Network Cyber Security

Presented by:
Motty Anavi
RFL Electronics

Agenda

- Cyber Security Threats
- Defense Strategy & Consequences
- Next Generation Networking
- ICS Vulnerabilities
- Liabilities
- Next Gen Networking – Contrasted
- Summary

“Secure” Private industrial network – The Smart Grid

- MV/LV transformers on poles now enhanced with Smart-Grid equipment
  - → Distributed automation in Secondary sub-stations
- Inter-connected by regional Ethernet networks with overlaying application communication using simple automation control protocols (IEC60870 , DNP3)

→ An attacker gaining access to 1 site can manipulate the operation of the devices in other sites

Vulnerability: Distributed large-scale open internal networks

“smart grid cyber-security guidelines did not address an important element… risk of attacks that use both cyber and physical means”

Electricity Grid Modernization; Report to Congressional requesters, US GAO, January 2011

Continuing And Growing Threats

Schoolboy hacks into city's tram system

By Graeme Baker
Last Updated: 2:48am GMT 11/01/2008

A teenage boy who hacked into a Polish tram system used it like "a giant train set", causing chaos and derailing four vehicles.

VIRUS INFECTION AT AN ELECTRIC UTILITY (Source: ICS CERT Jan. 2013)
In early October 2012, a power company contacted ICS-CERT to report a virus infection in a turbine control system which impacted approximately ten computers on its control system network. Discussion and analysis of the incident revealed that a

Symantec Official Blog

+6
6 Votes

Was S

Robert McMil

Septembe

A highly so

Dragonfly: Western Energy Companies Under Sabotage Threat

Cyberespionage campaign stole information from targets and had the capability to launch sabotage operations.

By: **Symantec Security Response** SYMANTEC EMPLOYEE

Created 30 Jun 2014

This campaign follows in the footsteps of Stuxnet, which was the first known major malware campaign to target ICS systems. While Stuxnet was narrowly targeted at the Iranian nuclear program and had sabotage as its primary goal, Dragonfly appears to have a much broader focus with espionage and persistent access as its current objective with sabotage as an optional capability if required.

In addition to compromising ICS software, Dragonfly has used spam email campaigns and watering hole attacks to infect targeted organizations. The group has used two main malware tools: Backdoor.Oldrea and Trojan.Karagany. The former appears to be a custom piece of malware, either written by or for the attackers.

Origin of Defense-in-Depth – in IT

"A military strategy sometimes called elastic defense. Defense in depth seeks to delay rather than prevent the advance of an attacker, buying time and causing additional causalities by yielding space."

http://en.wikipedia.org/wiki/Defense_in_depth

"…the practice of layering defenses to provide added protection. Defense in depth increases security by raising the cost of an attack. This system places multiple barriers between an attacker and your business critical information resources: the deeper an attacker tries to go, the harder it gets."

Brooke Paul, Jul 01,
Security Workshop at
Network Computing

Consequences of Loss of Network

- Teleprotection communications failure
  - Islanding
  - Degradation in grid security
- No SCADA connectivity
  - No control of RTUs and IED
  - No information on issues/outages
- Possible loss of auditing/video surveillance

Migrating From Circuits to Packets

- Telecom vendors have stopped development on all TDM platforms
- Many products obsoleted and not supported
- All US carriers have begun decommissioning and disconnecting legacy circuits at 2013
- Most active are AT&T and Verizon
- Expected decommissioning of all 4W circuits by 2019

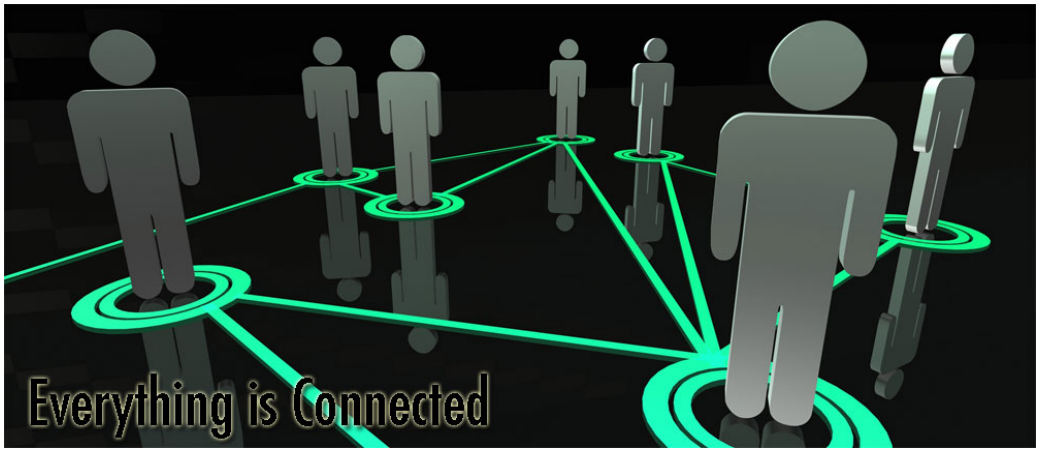
Table 1: Packet Switch & Circuit Switch Percentage of Installed Lines, North America & Western Europe

Year End	2011	2015
North America % CS	68.21%	33.49%
North America % PS	31.79%	66.51%
Western Europe % CS	63.82%	44.78%
Western Europe % PS	36.18%	55.22%
Source: Heavy Reading IP Network Transformation Market Tracker		

Historical Control Systems

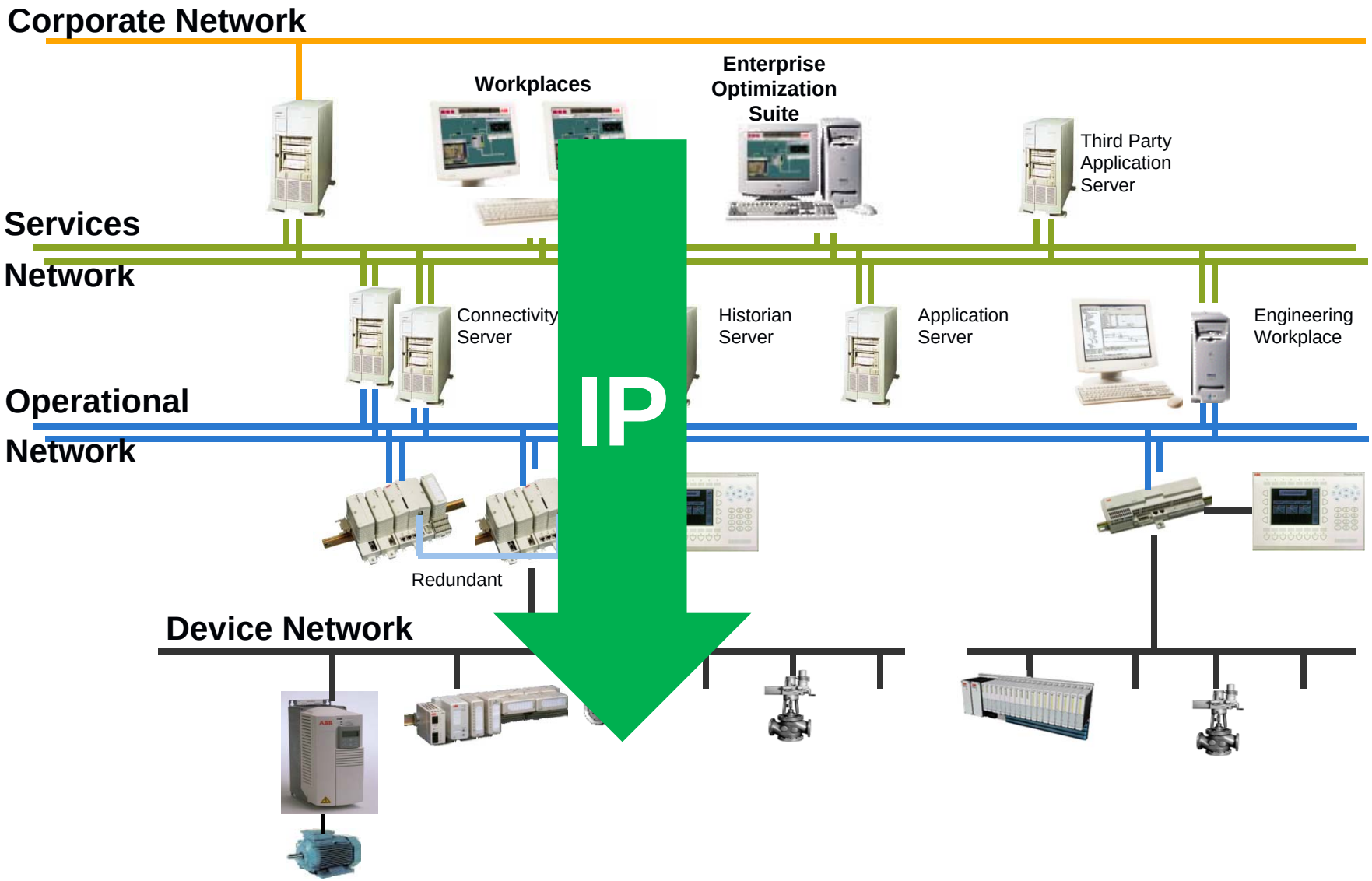
- Proprietary
- Complete
- Long service life
- Dedicated communications
- Security not designed into system
- No process for authentication
- Security by Obscurity

Progress in ICS



- Standardization of ICS
  - IP/Ethernet based
  - DNP3
  - Goose messaging
  - IEC 61850
  - AMI Protocols
- Use of off-the-shelf products
  - No more Security by Obscurity
- Everything could be interconnected

The Modern ICS



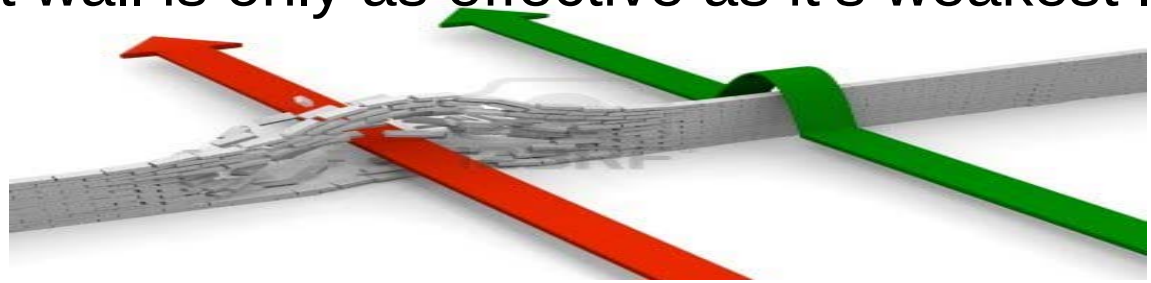
Landscape of ICS Threats*

Emerging Threat	Threat Trend
Drive-By Exploits	
Worms/Trojans	
Code Injection	
DoS	
Phishing	
Botnets	
Compromising Conf. Info	
Targeted Attacks	
Physical Theft/Damage	

*ENISA threat Landscape Dec. 2012

The Great Wall of China Defense

- Firewall are designed to keep intruders out
- Some provide impervious walls
- BUT: Once you break the physical constraint you can reach every point in the internal network
- Antivirus software is designed to identify known signatures and flag or block “suspicious activity”
- Antivirus software does not “know” what each application does
- These defenses – restrict access, but once overcome are ineffective
- The great wall is only as effective as it’s weakest link



Unmanned Field Sites

- Many unmanned field sites
- Many with dialup access
- Some with high-speed connectivity to control center
- Most with poor authentication and authorization

backdoor to the control center!

Examples of Attacks with MPLS

- Control plane attacks:
  - DoS attack on the control plane: could cause nodes to reboot and network reconvergence
  - Control Plane Corruption: Feeding erroneous/malicious information to control plane causing snooping, packets falling of the edge or network loops
  - RFC 4272
- Data plane attacks:
  - Plain vanilla DoS attacks
  - Snooping of network resources
  - Masquerading
  - RTU data insertion

What Do the Experts Say?

SDN/MPLS 2014

MPLS Data Vulnerabilities

- We are used to thinking of the network as being “safe” or “trusted”
  - Turns out that data can be extracted from the core
    - Subverted nodes
    - Tapped links
- *Pervasive monitoring is the widespread (often covert) surveillance through intrusive gathering of protocol artefacts* – RFC 7258
- This is an attack that can be performed by
  - Business interests
  - Organised crime
  - Foreign powers
- The end-user might protect their data through encryption
  - Although most do not
- Meta data is usually completely vulnerable
- Most of the data in the core traverses LSPs
  - Leads us to consider MPLS encryption

SDN MPLS

classroomclipart.com

JUNIPER NETWORKS

*SDN/MPLS conference Nov. 2014

MPLS Control Plane Attack?

- RFC 5920

Comparing Network Security

- Source Authentication:
  - MPLS – No source authentication, once entering an CE/PE – local id is erased
  - Ethernet – Universal address is maintained (MAC address), Standard for source authentication 802.1X
- Snooping / Scouting:
  - MPLS – LSPs used as transparent pipes from one location to another
  - Ethernet - Individual frames screened at global level (MAC) for validity
- Control Plane:
  - MPLS - BGP and other routing protocols very susceptible for attacks that can crash entire network
  - Ethernet - Control plane isolated and access controlled by corporate access control

Summary

- Threats to ICS networks are diverse and vary
- Threats are increasing in volume
- Attacks are more focused and targeted
- There are still holes in protection that are unplugged and represent major vulnerabilities
- Protection must be a multi layered process that’s integrated at all levels of design
- SCACA cyber security is a critical part of protecting industrial equipment

For Additional Information

www.rflelect.com

Motty Anavi

manavi@rflelect.com

(201) 787-3270

Network Selection Impact Security?

- Some packet protocols are easier than others to breach
- Attacks can be initiated on both the control and data planes
- Especially susceptible are packet protocols who do not provide source authentication, have the ability to provide dynamic routing and those removing source information – these include IP and MPLS
- More static “ridgid” networks that require NMS authentication for routing and provide a universal address space with source authentication are more resistant – these include SONET and Ethernet

MPLS Highlights

- Mature Technology
- Widely used
- Added deterministic routing to IP
- No Built-in Security (very susceptible for cyber attacks)
- Dynamic path establishment
- Well established resiliency mechanisms
- No built-in security (very susceptible for cyber attacks)
- Different in architecture than existing SONET/TDM
- Fairly unaffordable

Drawing Conclusions

- MPLS was designed for streamlining IP communications on carrier cores
- MPLS falls short on security and troubleshooting
- MPLS-TP has tried to address MPLS shortcomings, but is new and not widely deployed and tested
- Carrier Ethernet already answers all the requirement and had been finalized and widely deployed for more than 10 years
- Carrier Ethernet is the only technology that answers all of the Power Utility requirements