SCADA Cybersecurity

Lawrence Kravets

Overview

What are we covering?

- Introduction and bio
- History
- State of Cybersecurity for SCADA
- Q&A

Lawrence Kravets

IT Director

My story:

- University of Illinois at Chicago, 94
- Certified Information Systems Security Professional (CISSP)
- Global Industrial Cyber Security Professional (GICSP)
- 25+ years in Information Technology
- 12 years in IT / OT @ Concentric Integration

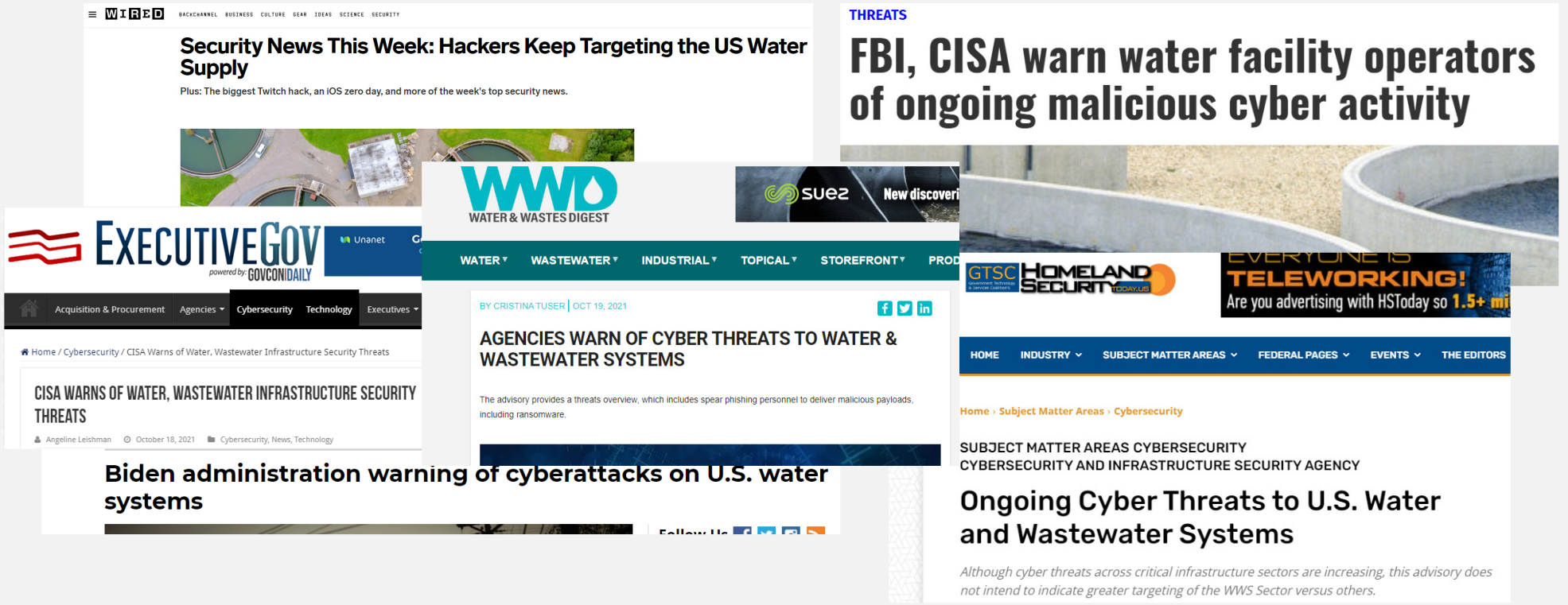
SCADA

Supervisory Control and Data Acquisition

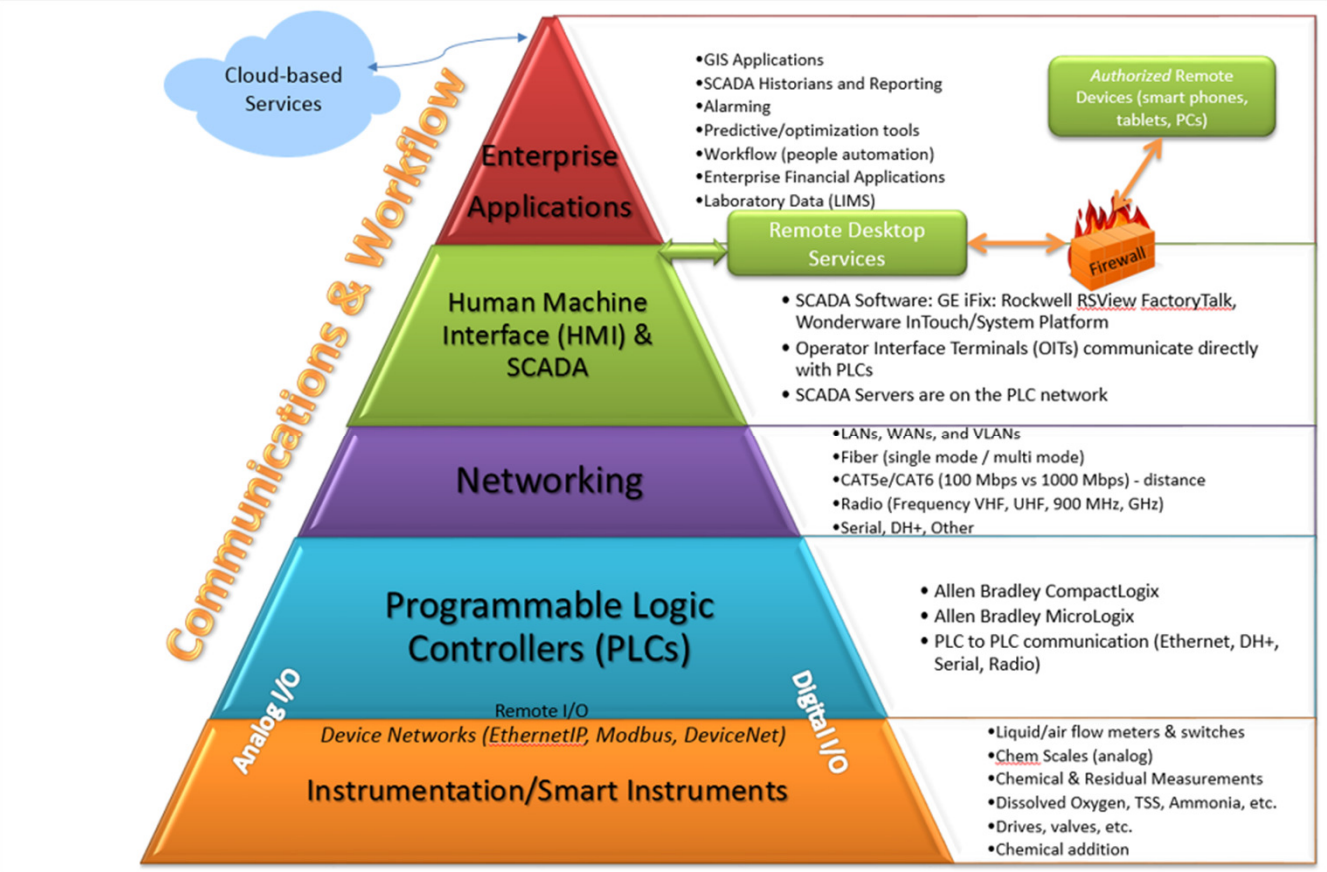
- "Humble Beginnings"
  - Started off as a single computer with SCADA
  - Not very complex
  - Analog / serial connected devices
  - No remote access
  - Limited exposure to malware

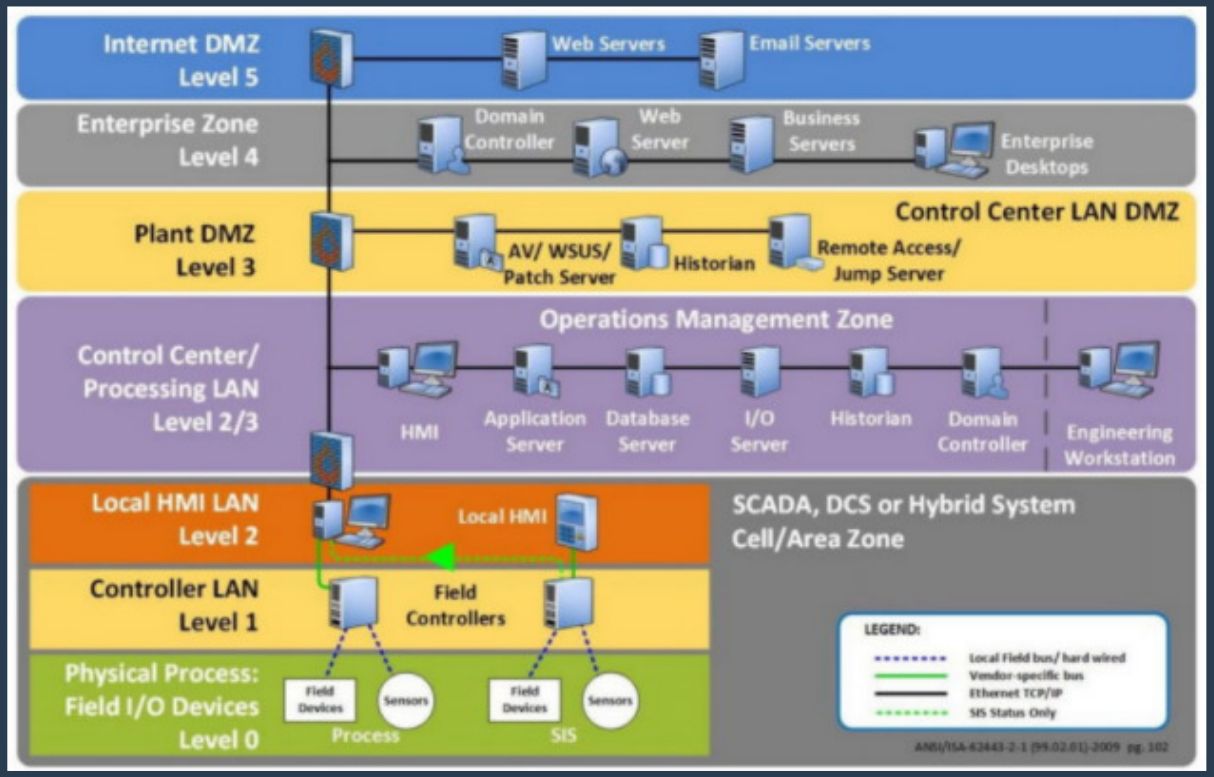

SCADA Now
Complexities!
• Internet connected
• Virtualization
• Remote access
• Reporting
• Smartphones and tablets
• Malware and Ransomware
• Disaster recovery
• Cloud
• Cellular
• Licensing
• Cyber-insurance

SCADA Now - In the news media…



What makes up a SCADA System?





Purdue Model ICS – how to defend SCADA

Now what?

- It may seem very overwhelming
- Find help, your IT department / Contractor / SCADA Integrator
  - Even Homeland Security
- Start making lists maybe performing SCADA master plan
- Having documentation is key
  - Network diagrams
  - Commented PLC code
- It's best when its not last minute or an emergency

What are some simple things you can do?

- Make sure you are running supported Operating Systems
  - No Windows 7 or XP
- Patch your Windows systems
  - Windows Updates
- SCADA software updates
- Install Antivirus or Endpoint Detection and Response (EDR)
  - Make sure it updates daily
- Backups
  - Keep a base system configuration off the network (thumb drive)
  - “dial tone”
- Proactive maintenance
  - Update firewalls, PLCs, HMIs, and other devices

What are some simple things you can do?

- Strong passwords
- No default passwords
- Network segmentation using a dedicated SCADA firewall
  - Protect the SCADA network from access outside the SCADA network
- No critical infrastructure should be available directly on the internet
  - Put things behind a security device like a firewall
- Secure any remote access using multifactor authentication
  - Username + password + time-based token = access

Best practices when using SCADA

- Do not check email on the same system that you use to access SCADA
  - Targeted spear-phishing attacks – how someone gets a "foothold" in your network"
- Limited or no internet access on SCADA computers
- Have accounts log off into guest mode when not using (view vs control)
- Make sure your people have the rights to do what they need but not more than they need

Advanced topics

- Virtualization
- Private cellular networks
- Unidirectional gateways
- PLC modes – run vs remote modes
- Disaster recovery and business continuity (plan for issues and test)
    - Incident response planning
- Penetration testing (validate your security controls)

Advanced topics

- Port security on network devices
  - Lock it until it’s needed
- Intrusion detection systems
  - Detect abnormal traffic
- Cameras
  - Physical security
- Monitoring service
  - Have a service actively monitor your network
- Individual usernames and passwords
- Password management
  - Passwordless?

Q&A

Questions and answers

- What's next?

Lawrence Kravets

8678 Ridgefield Rd, Crystal Lake IL 60012

815-788-3600

www.goconcentric.com

lkravets@goconcentric.com

CONCENTRIC INTEGRATION