SECURITYWEEK NETWORK:

- Information Security News
- Infosec Island
- Virtual Events

Security Experts:

WRITE FOR US

SECURITY WEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

- Subscribe
- 2020 CISO Forum
- ICS Cyber Security Conference
- Contact
- Malware & Threats
  - Vulnerabilities
  - Email Security
  - Virus & Malware
  - IoT Security
  - Threat Intelligence
  - Endpoint Security
- Cybercrime
  - Cyberwarfare
  - Fraud & Identity Theft
  - Phishing
  - Malware
  - Tracking & Law Enforcement
- Mobile & Wireless
  - Mobile Security
  - Wireless Security
- Risk & Compliance
  - Risk Management
  - Compliance
  - Privacy
- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - Network Security

Addressing SCADA Endpoint Protection Concerns

By Eric Knapp on May 21, 2012

Securing SCADA Endpoints Using the 3x3 Security Model

In my previous column, I wrote about a new model for control system cyber security. This model highlights the disparity of industrial control environments by presenting nine unique areas, each with unique cyber security challenges. This week, I'll be focusing on one of the more interesting areas of this model: SCADA endpoints.

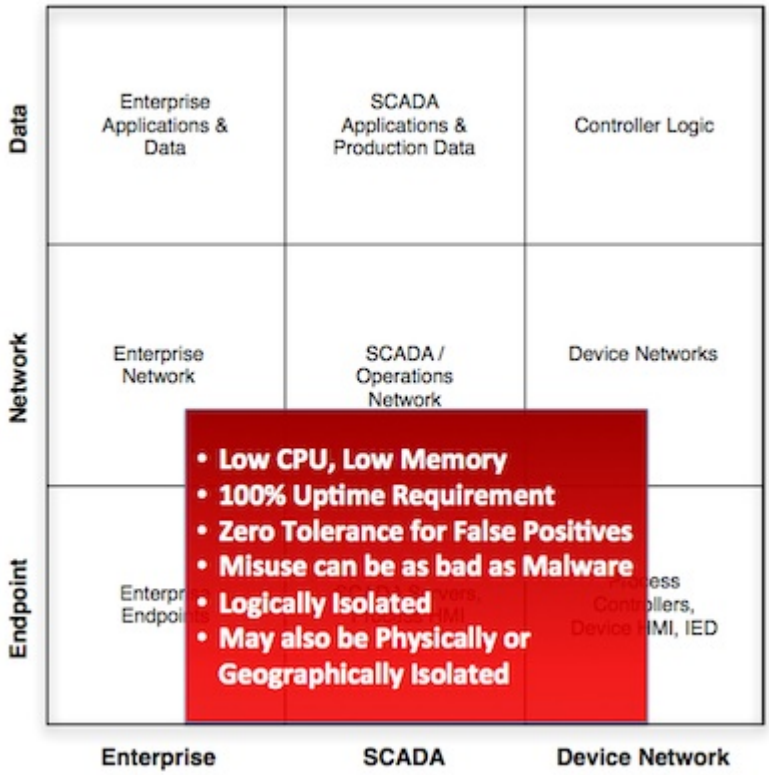
First, a primer for those who aren't familiar with the architecture of Supervisory Control And Data Acquisition: SCADA isn't a thing so much as it's a system. A SCADA system will typically consist of one or more servers, and several key applications. A SCADA system might perform several important functions: it could be a software development environment (SDE), an industrial protocol gateway, a Human Machine Interface (HMI), a business intelligence console, or combinations thereof. It is also, typically, the central management repository of the control system: it is an asset or inventory manager, an alarm manager and a data historian. In short, it's a fairly complex system that is closely tied to the real-time nature of the industrial control process that it supervises, controls and acquires data from.

You'd think that this would warrant building SCADA architectures using the latest and greatest network and server technology available, but unfortunately that's not the case. SCADA systems and the automated processes that they manage are built on reliability and precision, and for this reason most SCADA systems are still running on Windows 2000 or 2003. Quite simply, once these systems are up and running, nothing can change without risking the reliability and continued operation of the automated process(es). If a change is needed it must first be tested, and once tested the change can be applied only during the next available maintenance window. In other words: if it 'aint broke, it 'aint gettin' fixed.

This ensures reliability, but also results in technology lifecycles that are much longer than you might expect—often measured in decades. So while SCADA systems are reliable, they're also the textbook definition of 'legacy.' Older computing systems, with no horsepower to speak of, and no memory to spare.

SCADA servers are also (or at least they *should* be) isolated from the Internet, and even from the corporate IT network. This makes endpoint security much more challenging: on the one hand you have an older and likely unsupported (or less supported) operating system, and therefore you're at risk from unpatched OS vulnerabilities; on the other hand, the isolation of these systems makes your traditional endpoint security tools such as Anti-Virus systems notoriously difficult to maintain. Simply obtaining updated virus definitions can be

difficult. New virus definitions need to be downloaded elsewhere, tested, and then walked into the control room and applied via a removable media. The removable media, of course, is an attack vector of its own: Stuxnet was propagated via a zero-day USB-based exploit (as well as several other zero day exploits—some network based). With the rate of new malware increasing day by day, a manual process of updating virus definitions becomes increasingly ineffective. Even worse, as virus libraries increase in size, the processing overhead for a scan can be too much for devices with less memory, fewer CPU cycles to spare and less tolerance for latency or delay.



In a nutshell, endpoint protection in SCADA environments can pose some interesting cyber security challenges. Luckily, SCADA servers are also highly controlled devices, running only essential services. Because of this, a more rigid approach to security can be adopted in the control room. Application Whitelisting, for example, can be used. Anti-Virus is a blacklist technology: it knows what is bad, and when it detects something bad within a file it eliminates that threat. Whitelists take the opposite approach: they know which application files are good, and stop everything else. The assumption is: if it's not a known and authorized application, it could be malicious and therefore should be blocked. The "blocking" in this case occurs as the malicious application attempts to execute, preventing the malware from actually doing any harm—or anything at all, for that matter.

While sounds like a silver bullet, remember that there are other vectors to consider. A buffer overflow can inject malware directly into memory, so there is no file to validate. To truly "whitelist" a system, executables must be examined in both the filesystem and in memory. Otherwise, an already-established rootkit might bypass security software—including whitelisting—to operate persistently and secretly. And, of course, there's the worst malware of all: the human operator. An authorized user can do a lot of harm, intentionally or accidently.

So, while application whitelisting—with it's deliciously low CPU load and small memory footprint—has been making a name for itself over the past few years, it's only part of the solution. At the 2011 ACS Cyber Security Conference, Ralph Lagner demonstrated that a simple 14 byte change to a Siemens Step 7 program file could brick a PLC. While this change could be made as the result of "malware," it's still ultimately a change event: a malicious modification of the controller's configuration. Because SCADA systems are used to establish and implement controller logic, misuse can be as dangerous as malware. For this reason, whitelisting is best used in conjunction with change control mechanisms, in order to ensure that a PLC's logic files are not being maliciously manipulated by the SCADA system.

As we move closer to the automated devices in the ICS, of course, there's a need to protect the programmable logic of PLCs from direct manipulation, and that means securing embedded devices, real time operating systems, and the communications buses of the control system device network. In the next installment, we'll take a look at the lower-right sector of the 3x3 security model, and examine some of the new and emerging security technologies that can be used to help protect the most challenging area of industrial control cyber security: the Device Network.

Read more of Eric's columns on SCADA and Industrial Controls Systems Security here.

Eric D. Knapp (@ericdknapp) is a recognized expert in industrial control systems cyber security, and continues to drive the adoption of new security technology in order to promote safer and more reliable automation infrastructures. Eric is currently the Director of Cyber Security Solutions and Technology for Honeywell, and is the Chief Technical Advisor, North America for the Industrial Cybersecurity Center. He is also the author of "Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA and Other Industrial Control Systems." His new book, "Applied Cyber Security for Smart Grids" was co-authored with Raj Samani, McAfee CTO EMEA. The opinions expressed here represent Eric's own and are not those of his employer.

Previous Columns by Eric Knapp:

Critical Vulnerability Discovered in Waste Automation, Results in Global Ecological Disaster
Shall We Play a Game?
Tech Debate: Is The Cloud Critical Infrastructure?
ISA Automation Week Conference Wrap Up
ISA Automation Week Day One Wrap Up: Building an ROI for Industrial Cyber Security

Tags:

INDUSTRY INSIGHTS Management & Strategy

Most Recent Most Read

- EclecticIQ Closes $24 Million Series C Funding Round
- Flaws in Rockwell Automation Product Expose Engineering Workstations to Attacks
- Webinar Today: Advanced Tips for Securing Large AWS Environments
- Cybercriminals Already Targeting, Selling Leaked GO SMS Pro Data
- Baltimore County Schools Still Closed Following Cyber Attack
- Brazilian Plane Maker Embraer Targeted in Cyberattack
- Nation-State Cyberspy Group Drops Coin Miners as Distraction Technique
- Hacker Gets 8 Years in Prison for Threats to Schools, Airlines
- Online Learning Company K12 Paying Ransom Following Ransomware Attack

- Theoretical Attack on Synthetic DNA Orders Highlights Need for Better Cyber-Biosecurity

Popular Topics

Information Security News
IT Security News
Risk Management
Cybercrime
Cloud Security
Application Security
Smart Device Security

Security Community

IT Security Newsletters
ICS Cyber Security Conference
CISO Forum, Presented by Intel
InfosecIsland.Com

Stay Intouch

Twitter
Facebook
LinkedIn Group
Cyber Weapon Discussion Group
RSS Feed
Submit Tip
Security Intelligence Group

About SecurityWeek

Team
Advertising
Event Sponsorships
Writing Opportunities
Feedback
Contact Us