Top 10 Security Questions For Your Vendor

Jan 21 - 23 in Miami South Beach

Bryan Owen

Security Architect & PE - OSIsoft

s4xevents.com

We all know vendor questionnaires don’t really help you manage ICS security risk.

What if they could?

“It sort of makes you stop and think, doesn’t it.”

Third-party Questionnaires Are Security Theater

The most common vendor security control is also the most useless

By DANIEL MIESSLER in INFORMATION SECURITY

CREATED/UPDATED: DECEMBER 27, 2018

“So a dedicated team can be onsite for days, with full management and staff support and transparency, and still not find the dead bodies, but we think an outsider sending a form is going to somehow reveal the truth?

It’s fantasy, full stop.”

Perspective on vendor questionnaires at scale

Problematic examples…

- Assessment of all business risks
- Asks about all products and services
- Using service-oriented for COTS product
- Using non-standard frameworks

Source: RSAC 2018 Presentation - Mary Ann Davidson, CSO Oracle Corporation
https://www.rsaconference.com/industry-topics/presentation/monty-python-and-the-holy-rfp

Tom Alrich's Blog

Friday, October 11, 2019

You too can waste BIG money on CIP-013 compliance!

- Scatter resources on partially mitigating a lot of supply chain security threats
- Pour resources into over-mitigating a small number of threats, while barely addressing other threats at all
- Devote resources to mitigating risks that don’t even apply

No one has the resources to mitigate all supply chain cyber risk

Focus questions on products and services that matter most

Search online information about vendor security practices

Select other mechanisms to increase depth and confidence

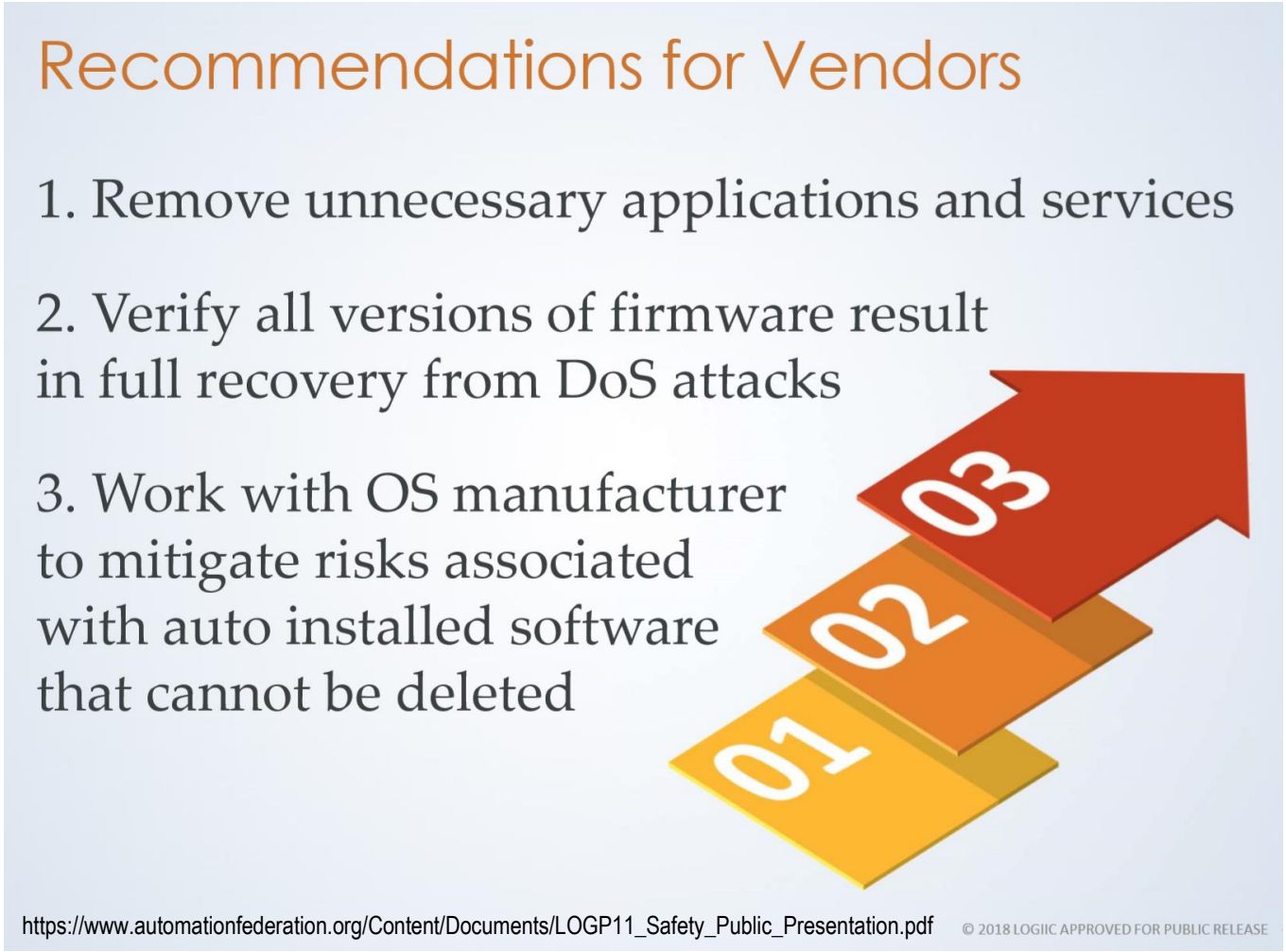
Organize vendor questionnaires by ICS impact classification

Safety and Protection

Control

View

4 topics for safety and protection system vendors



<u>4. Lock Functionality</u>
Third party research conducted in late 2017 showed that some of implementations could potentially be bypassed

Source: LOGIIC PROJECT 11 – Public Findings

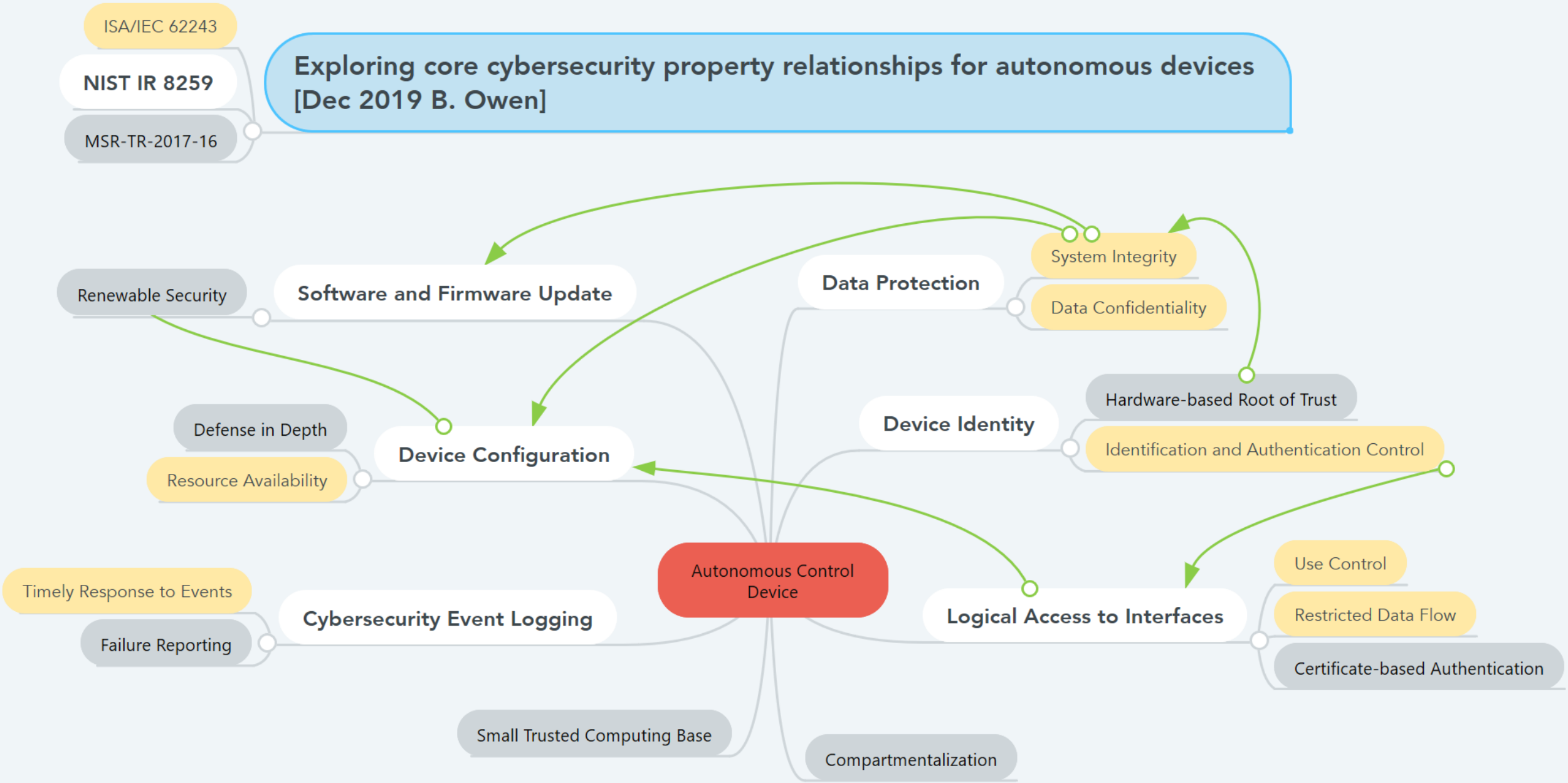
National Institute of Standards and Technology
U.S. Department of Commerce

Control Devices are Difficult to Secure

Is it feasible to identify 10 top questions?

- 7 Foundational Requirements (ISA/IEC 62443)
- 6 Core Baseline Capabilities (NISTIR 8259)
- 7 Properties of Highly Secure Devices (MSR-TR-2017-16)

Microsoft Research



https://mm.tt/1391634361?t=TUUAvmMnHQ

Questions 1-5 for control device vendors

1. Verification Testing
   - Is the device tested with a focus on discovering and exploiting vulnerabilities?
2. Device Identity
   - Does the device have a unique, unforgeable identity that is inseparable from the hardware?
3. Renewable Security
   - Are mechanisms available to support updates without impact to essential functions?
4. Logical Access to Interfaces
   - Does the device logically restrict access to each network interface by default?
5. Communication Integrity
   - Does communication integrity include authenticity of information received?

Questions 6-10 for control device vendors

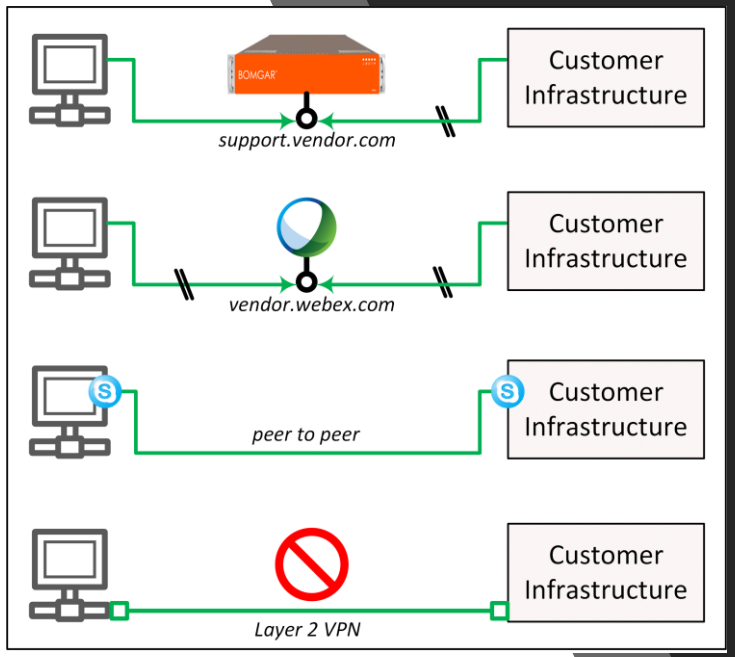
6. Software Integrity
   - Are software authenticity checks enabled by default?
7. Defense in Depth
   - Are exploit sequences documented and multiple mitigations applied?
8. Resource Availability
   - Does the device support a degraded mode for essential control functions in response to a network DoS attack?
9. Event Logging
   - Does the device log cybersecurity events and support transmission to authorized entities?
10. Software Bill of Materials
    - Is an inventory of supplier created and directly included third party software available?

Control Impact – Remote Service Vendors

<u>Ukraine 2015 event redux</u>

1. Spear phishing to gain access to the business networks
2. BlackEnergy 3 implants
3. Theft of credentials from the business networks
4. Use of VPNs to enter the ICS network
5. Use of existing remote access tools within the environment
6. Issuing commands directly from a remote station similar to an operator HMI

Questions for Remote Service Vendors



Common patterns for vendor interactive remote access

1. Is multifactor authentication enforced for remote access?
2. Can connections be initiated outbound from the asset owner to a vendor-authorized endpoint?
3. Do connections terminate at an intermediate system?
4. Will asset owner remote access credentials be stored by the vendor?
5. Is there an immutable audit trail of interactive remote service activity?
6. Is read-only access enough for typical remote service activity?
7. Are block or sever remote service connection procedures published?

Exploits with impact on ICS view

Project Robus

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned
Risks Posed by Firewall Firmware Vulnerabilities

It WISN't Me: Attacking Industrial Wireless Mesh Networks

Let's Get PHYsical

Link Layer Exhaustion Attacks Against Industrial Wireless Implementations

HART as an Attack Vector: from Current Loop to Application Layer

Could you hide…

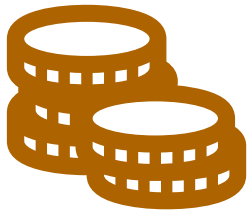
an entire attack in a pressure meter?

Questions for Integrators of ICS view components

1. Is the component tested for unauthenticated commands that alter data or stop data flow?
2. Does the component automatically detect loss of update from input data sources?
3. Are redundant sensors reconciled using a deterministic algorithm?
4. Is input data checked for timeliness and data quality before use?
5. Is indication provided for clamped and forced inputs?
6. Are data models used to check critical sensors? [1st principle, digital twin, soft sensor, …]
7. Do calibration tests check dynamic response of critical sensors?
8. Do threat models include compromise of maintenance and test equipment?

Other Ideas for Questionnaire Objectives

Assess Fit for Purpose



Reduce Cost to Defend

Identify Red Flags

General Suggestions

Do’s

- Focus on prioritized risk management concerns
- Scope the assessment to specific product and service lifecycle
- Provide rules of engagement and FAQ

Don’ts

- Don’t boil the ocean with comprehensive control catalogs
- Don’t fall for ‘everything is perfect’ responses
- Avoid excessive back and forth in follow ups

Closing Nugget: Verification testing will always be required!!!

- No questionnaire will adequately address the risk of ‘software backdoor’ implants in the ICS supply chain
- Simple tools should be used before formal testing [Mozilla observatory, Attack-surface Host Analyzer, etc]
- Avoid security theater. Stick to what matters most. Be efficient and cost-effective.


THANK YOU
OSIsoft®