DRAGOS

Why You Need OT-Specific Threat Intelligence

INTRODUCTION

SELENA LARSON

- Cyber threat intelligence analyst at Dragos
- Specializes in ICS cybersecurity
- Identifies and reports on threats, trends, ICS-specific TTPs

REID WIGHTMAN

- Senior Vulnerability Researcher
- Validates and corrects publicly reported vulnerabilities
- Performs in-house research and vulnerability assessments on industrial hardware and software
- Sets things on fire (occasionally)

AGENDA

1. Defining Cyber Threat Intelligence
2. ICS Threat Intelligence Differentiators
3. Defining the ICS Threat Landscape
4. Vulnerability Intelligence
5. IT vs ICS Architectural Differences
6. Vulnerability Case Study
7. Generating OT Threat Intelligence
8. Operationalizing OT Threat Intelligence

WHAT IS CYBER THREAT INTELLIGENCE?

- Obtaining actionable information on adversaries, TTPs, and vulnerabilities so defenders and organizations can reduce harm through better security decision making

THE ADVERSARIES

Financially-motivated hacker who executes ransomware attack

- **Adversary:** Cybercriminal
- **Target:** IT-focused business ops
- **TTPs:** Spearphishing, RobinHood ransomware, network propagation via PsExec

Adversary interested in disrupting electric distribution

- **Adversary:** Sufficiently resourced, sponsored by entity who wants to further political means
- **Target:** Initial IT access to facilitate OT access
- **TTPs:** Spearphishing, customized malware, use of OT-specific devices and protocols

DEFINING THE THREAT LANDSCAPE

- Operational Technology (OT): OT should be thought of as mission critical IT in an ICS. It is the hardware and software that controls and monitors operations in an ICS environment, like domain controllers and Windows PCs.
- Industrial Control Systems (ICS): An umbrella term for software and hardware that controls and automates industrial processes. ICS environments can include electric utilities, oil & gas, and manufacturing.

CYBER THREAT INTELLIGENCE IT/OT DIFFERENTIATORS

- Adversaries, threat behaviors, and consequences of cyberattacks are different.
- Successful attacks can cause catastrophic human and environmental harm. ICS threat intelligence can help keep major disasters from happening.
- Vulnerability impacts and actions taken vary greatly.

ICS THREAT INTELLIGENCE CATEGORIES

Interested Adversaries	Intelligence on activities of adversaries known to have an interest in control systems, operation networks, and ICS organizations Example: ALLANITE targets electric utility and energy firms. It has the capability to infiltrate OT environments for reconnaissance purposes.
Direct ICS Impact	Intelligence on threats directly affecting the operation of industrial control systems Example: TRISIS is a malware framework designed and deployed to disrupt oil and gas operations, targeting SIS
Indirect ICS Impact	Intelligence on threats not associated with industrial control systems but have a high likelihood of disrupting their operation Example: Sodinokibi ransomware does not specifically target industrial control systems but can be debilitating to organizations if it accesses operational networks

Source: https://dragos.com/wp-content/uploads/Industrial-Control-Threat-Intelligence-Whitepaper.pdf

IT vs OT THREAT INTELLIGENCE

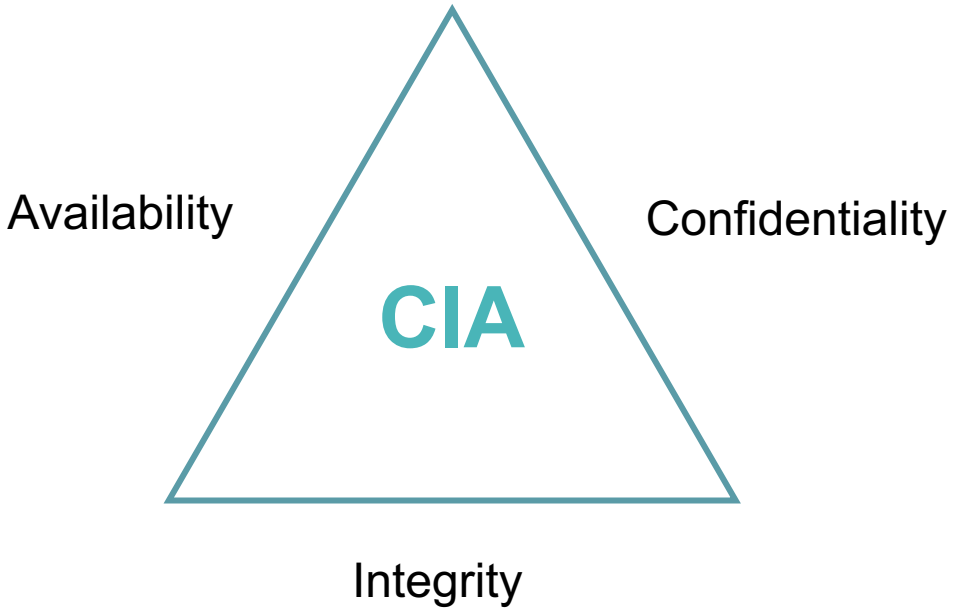
- Threat landscape is different
- OT has enterprise technology, but a lot of it requires specialized knowledge
- An adversary must maintain access and learn two different networks with specialized technology requiring specialized capabilities
- Components of threat intelligence might be the same (i.e. using IOCs and threat behaviors), however the behaviors themselves are much different
- Decision-making calculus is different

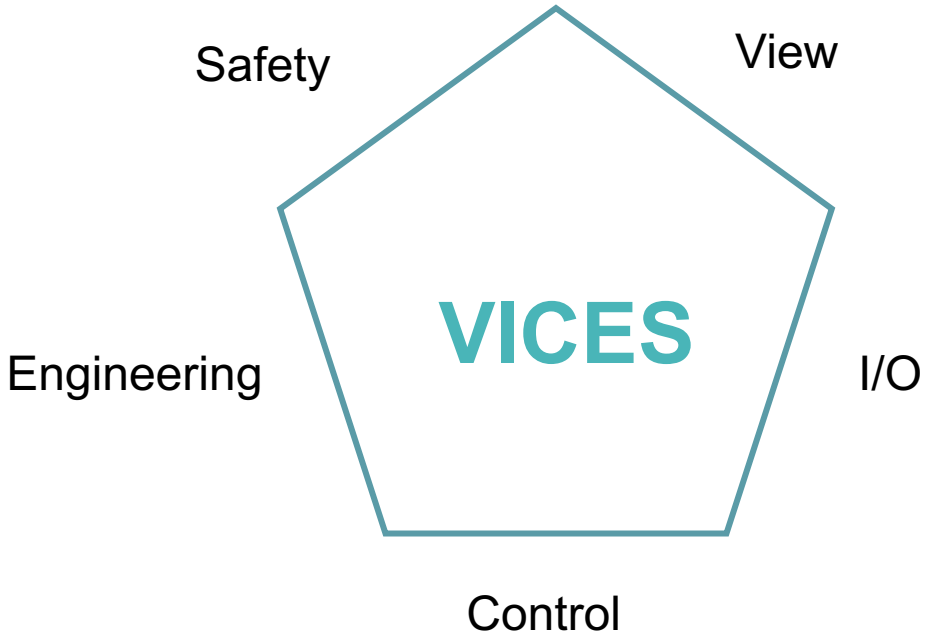
THREAT LANDSCAPE & THREAT SURFACE

- 11 public activity groups targeting ICS
- ICS-specific malware
- Supply chain and third-party access

  - Original Equipment Manufacturer (OEMs), telecommunications
- Remote access, vendor access
- Systematic and input/output threats
- Vulnerability exploitation to enable process disruption

CYBERSECURITY PRINCIPLES





VULNERABILITIES

Dragos validated – and in many cases, corrected – **212** advisories with **438** vulnerabilities

- **26% of advisories** had no patch available when the initial advisory was published, presenting a challenge for users trying to take action on the published vulnerability.

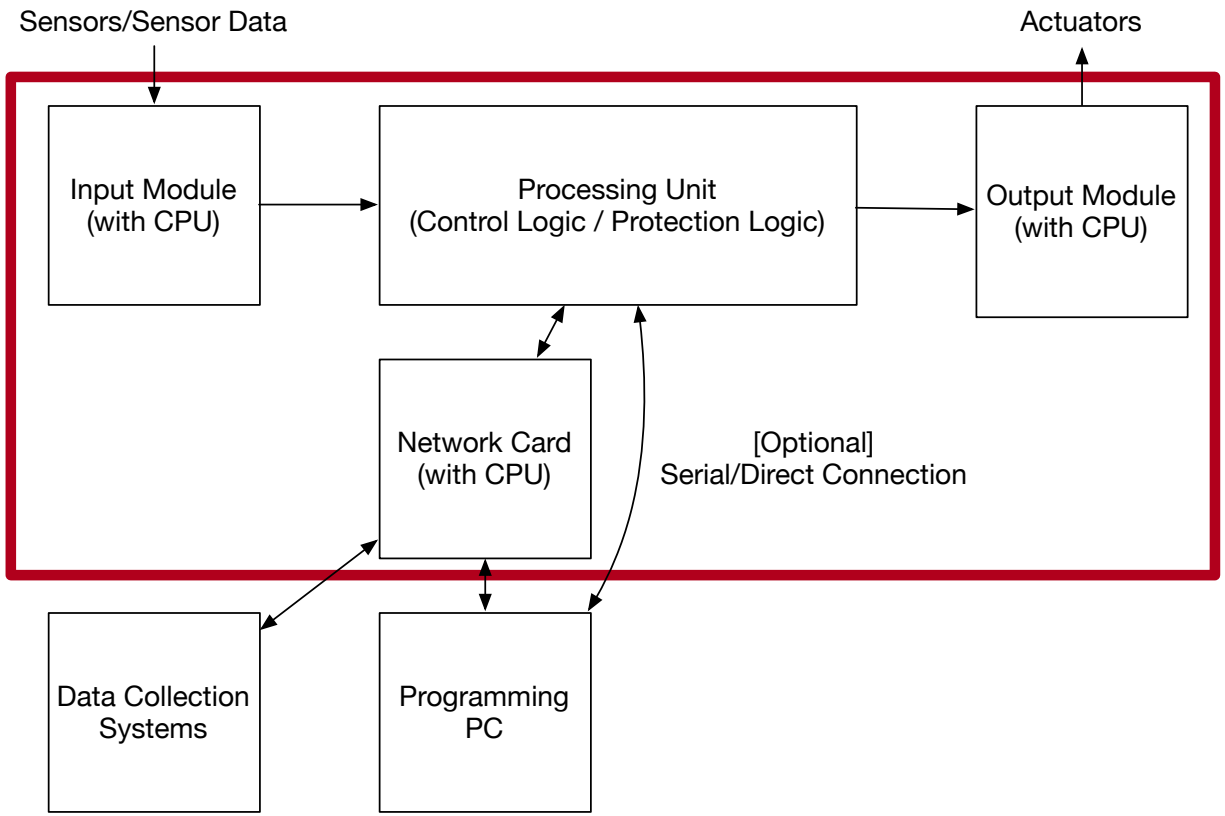
- **30% of advisories** published incorrect data preventing operators from accurately prioritizing patch management.

PROBLEMS WITH PATCHING

Patching vulnerabilities is limited by:

- Support contracts, outage windows, legacy software and hardware integration support, people relationships
- Causing more issues than mitigating the vulnerability in other ways
- Relying on vendors to release patches for vulnerabilities in software/hardware stacks, which can take longer than IT software and services

ARCHITECTURAL DIFFERENCES



- "A PLC" is really a network:
  - CPU
  - Input modules
  - Output modules
  - Network Card(s)
- The 'Network Card' is really a gateway/protocol converter

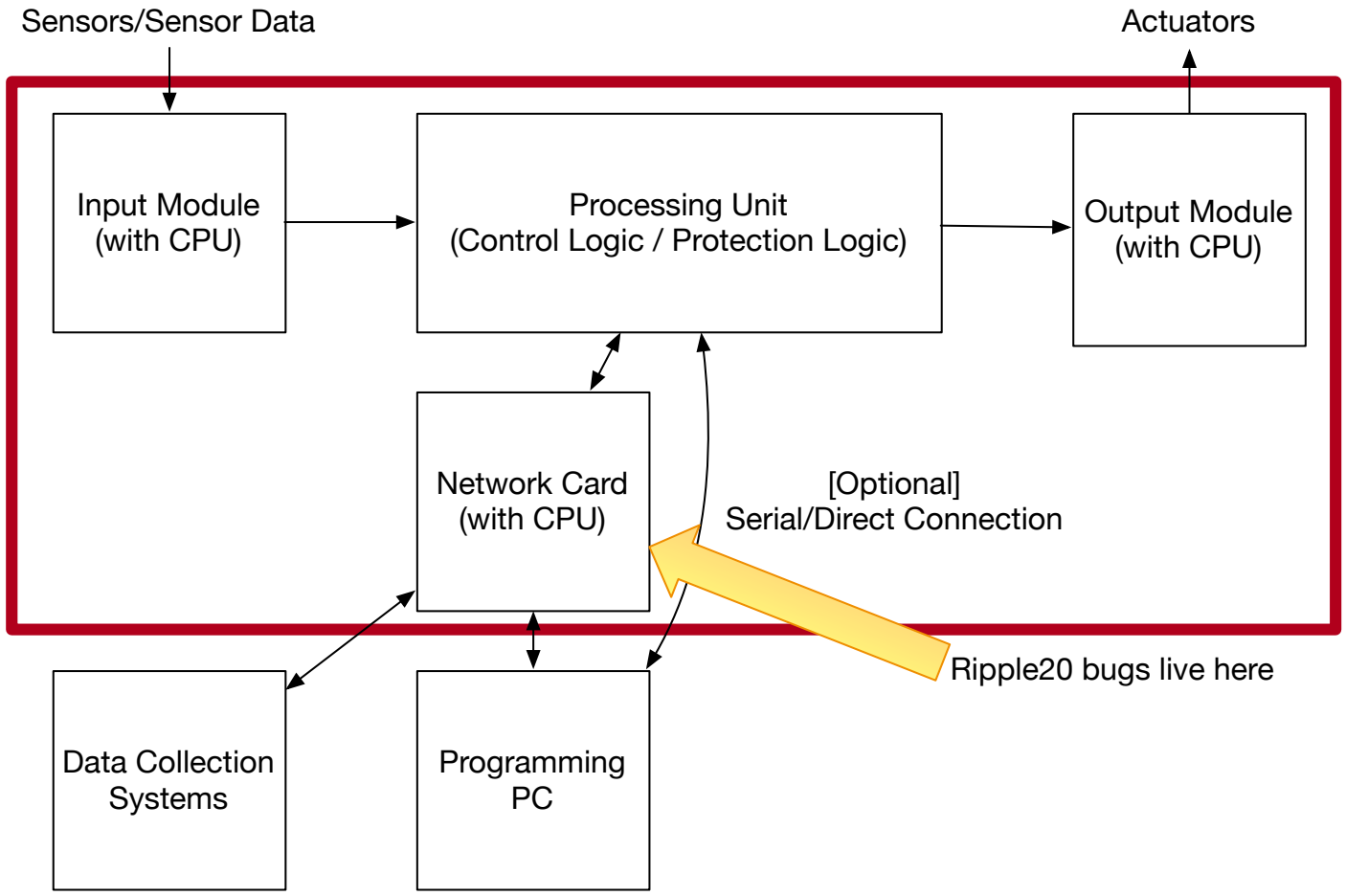
CASE STUDY: RIPPLE20

- Ripple20 is a set of 19 vulnerabilities that impact hundreds of millions of devices, including enterprise devices and co-embedded systems found in industrial control systems and Internet of Things (IoT) devices.
- Example impacted devices include Programmable Logic Controllers (PLCs), serial to ethernet converters, protocol converters, Remote Terminal Units (RTUs), digital protective relays, and some managed network switches and routers.
- Industrial operators must wait for vendors to create and apply fixes to products and software before making updates available to customers.

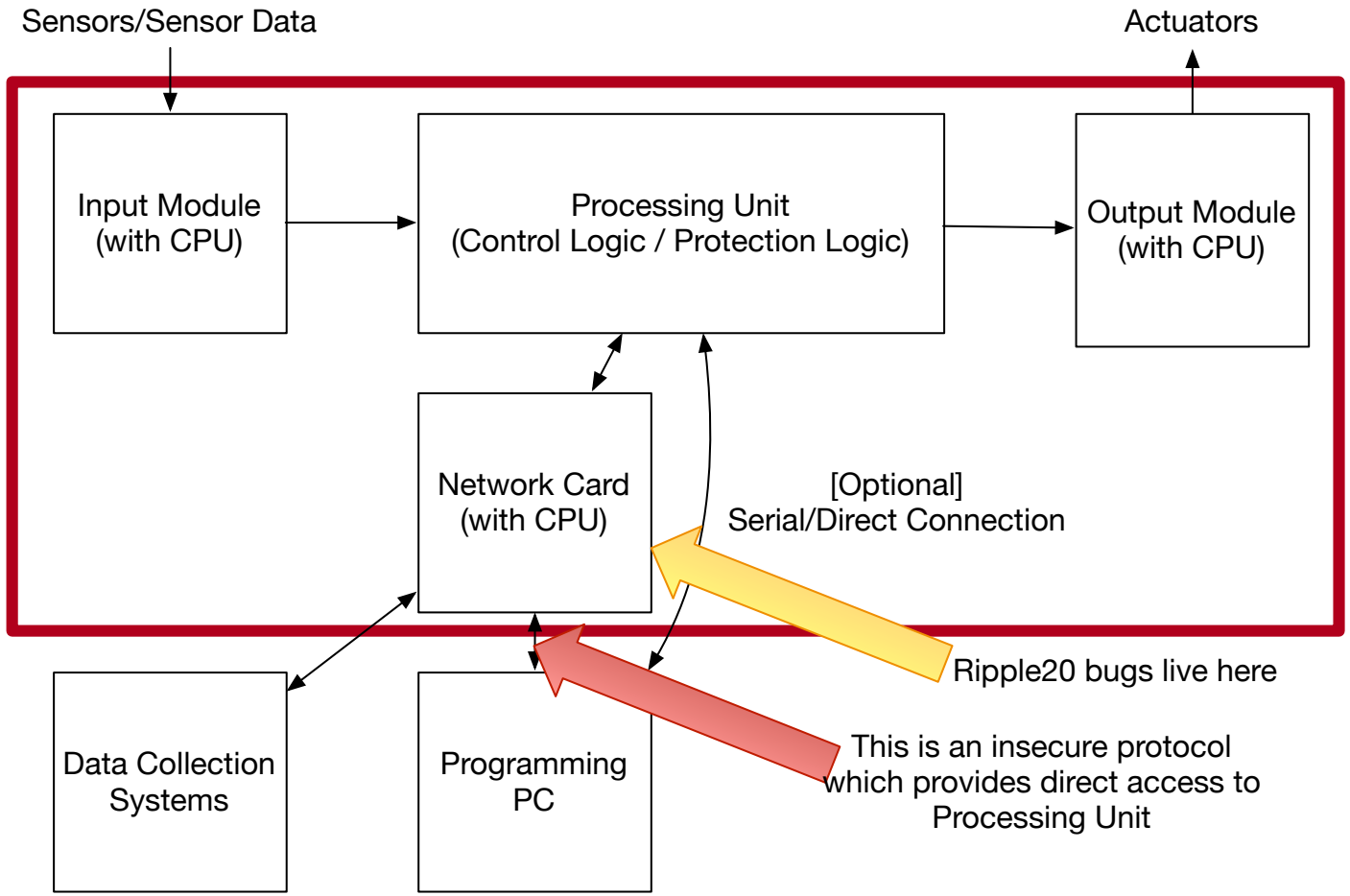
CASE STUDY: RIPPLE20

- Bugs impact *deeply embedded systems*
- For full control of the victim component, attacker has to do a LOT of stuff
  - Attack payload specific to processor
  - Knowledge of underlying operating system/memory layout/etc
  - Write exploit for underlying OS
- Unlikely we'll see widespread "RCE" attacks
- More likely we'll see DoS-style attacks
- DoS is ordinarily the *worst* thing that can happen in a control environment
- …but…

CASE STUDY: RIPPLE20



CASE STUDY: RIPPLE20



CASE STUDY: RIPPLE20

- In ICS, *a portion* of a PLC may be crashed
- Exploiting Ripple20 in an industrial environment will take more work than a traditional IT vulnerability due to differences in ICS device architectures
- The ‘data stealing’ bits of Ripple20 are mostly irrelevant to ICS, due to insecure protocols

CASE STUDY: RIPPLE20

- In addition to just the *device* architecture, consider overall *network architecture*
- Generally, crown jewels SHOULD NOT be exposed upstream
- Vulnerable PLCs, RTUs, protocol converters, etc: not likely exposed upstream
- Vulnerable Routers: MIGHT be exposed

CASE STUDY: RIPPLE20

- Take a measured approach:
  - Do not freak out
  - Step back and think about system and network architecture of the actual impacted device
  - Think through impacts an attacker can have using the vulnerability
  - Think through what ”just having access” to the controller gives an attacker
  - Decide if it is prudent to patch

ICS VULNERABILITY IMPACTS

- Industrial controllers are often insecure-by-design, so these vulnerabilities will be moot on some devices.
- True impact to operations:

  - 9% of advisories covered products that would be deemed high-likelihood initial targets in the ICS space.

  - 40% of advisories covered engineering workstation and operator station software.

  - 37% of advisories covered field equipment: industrial controllers, sensors, and the network equipment responsible for connecting controllers and sensors to the broader control systems network.

GENERATING OT THREAT INTELLIGENCE

- High-value assets (Crown Jewels) vary by industry and company, and so do the motivations for attacking them.
  - Data historians, chemical processing, safety controls
- Develop a hunt hypothesis based on an understanding of adversary's behavior.
  - If I increase the number of third-party service providers with access to my OT network, then this will provide adversaries additional avenues of access to my sensitive processes.
  - Identify third-party service provider and vendor relationship connections as a starting point for detecting potentially malicious activity.

GENERATING OT THREAT INTELLIGENCE

- Develop sufficient data sources and visibility into your OT network
- Understand the audience and be aware of context to make threat intelligence relevant
  - OT threat intelligence should help IT understand threat impact, context, and triage
  - Promote understanding outside factors: Attacks on ICS entities like oil and gas or electric utilities can be used to further political, economic, and national security goals
- Understand impediments to response
  - Vulnerability scanning can break the OT – sampling approach
  - Endpoint detection does not exist or is not supported – investigative playbooks
  - The next outage window to apply patches is in six months – mitigations/detections

OPERATIONALIZING OT THREAT INTELLIGENCE

- Develop an organizational program around threat intelligence, including vulnerability management
- Recognize that threat intelligence is a major function of risk management
- Threat intelligence must not only report activity, but advise countermeasures and/or mitigations for the defended environment
- Threat intelligence that can be shared up and down the organization, including executives, HR, and the SOC

CONCLUSION

- Goals of threat intelligence are largely similar for IT and OT
- Attacker capabilities, motivations, and attack surface vary between IT and OT targeting adversaries
- Security and vulnerability decisions within the IT and OT will be made differently, even if based on the same intelligence
- It takes everyone working together to make ICS entities – and the communities they operate in and support – safer and more secure

THANK YOU