WHAT EVERY PEN TESTER NEEDS TO KNOW ABOUT ICS

LESLEY CARHART, SANS HACKFEST SUMMIT 2019
Introductions

Lesley Carhart
Principal Industrial Responder
Dragos, Inc

- GCIH, GCFA, GPEN, GREM
- Specialist in Hunt and DFIR on industrial systems
- 12 years in InfoSec
- Speaker, blogger, volunteer
What We Think We Know about ICS

COMMON MISCONCEPTIONS

• ICS is an edge case...
  and
• ...has to be out of scope for scans, pen tests, and assessments
• ...is arcane and requires specialized training to learn
• ...is protected by air gapping, data diodes, and segmentation
• ...is purposefully neglected in security
• ...could easily be secured using modern security tools
• ...is tremendously vulnerable due to being on Shodan
ICS ARE EVERYWHERE

In fact, they are imperative to the function of our civilization.

ALL OF THOSE ASSUMPTIONS ARE (MOSTLY) WRONG

Our assumptions about what protects and does not protect ICS are wrong.

ICS MUST BE SECURED AND TESTED

There are necessary reasons some ICS are legacy, and modern cybersecurity tools, tactics, and procedures require adaptation.
First, Some Terminology

- **Industrial Control System:** A mechanical, analog, or digital device which directs and controls all or part of an industrial **process**.
- **ICS != interchangeable with SCADA**
- **OT:** Operational Technology – a broad term for environments in which industrial processes occur
- **Operator:** A skilled technician who utilizes an industrial control system.
What’s a “Process”?  

INDUSTRIAL BASICS

• A series of discrete kinetic actions which accomplish a physical task  
• **Examples:**  
  • Hydrocracking Oil  
  • Electrical Generation and Transmission  
  • Canning Tuna  
  • Pumping Well Water  
  • Packaging Warehoused Goods...  
• Processes can be component parts of processes
Process Loops

SENSOR

TEMPERATURE
PRESSURE
MOTION
LIGHT...

MECHANICAL
RTUs
PLCs
IoT DEVICES

CONTROLLER

ACTUATOR

MOTOR
PUMP
SWITCH
VALVE...
A Very Simple Process
AUTOMATIC REVOLVING DOOR

- SENSOR
  - MOTION
  - OBSTRUCTION

- CONTROLLER
- ACTUATOR
  - MOTOR (Rotation)

- Is someone in the door?
- Is the door obstructed?
- What is the motor state?

- When am I supposed to rotate?
- When am I supposed to stop rotating?
1. Actuator **fails to start** when it’s supposed to
2. Actuator **fails to stop** when it’s supposed to
3. Actuator **starts too early** or **too late**
4. Actuator goes on for the **wrong period of time**

- Consider implications in the door example, and other processes
Industrial Processes (and ICS) are Facing Increased “Cyber” Threats

• Sabotage, espionage are as old as civilization
• **Kinetic impacts are highly visible**
• Technology has made tampering easier from a distance
• ICS are increasingly interconnected and digitized for cost savings and convenience
1. **Maroochy Sewage Spill**: 2001. Disgruntled employee uses knowledge to reverse the flow of sewage and release 800,000 liters of sewage, causing physical impact and environmental damage.

2. **Stuxnet**. Iranian centrifuge failure. Adversary understood the physical process and the engineering controls in place.

3. **CRASHOVERRIDE**: Ukraine 2015, 2016: Effective attacks against Ukraine’s electrical grid. Extensive system knowledge and reconnaissance...
• Adversaries are **building footholds** and conducting reconnaissance
• **Commodity malware** may have the same ultimate **consequences**
  • **Insiders** pose a very real threat
The Reality of Industrial Processes
• Many devices work in synchronization
• Several protocols will be used in even simple environments
• Different vendors and devices exist in different verticals
Levels of Purdue Reference Model:

- **Level 4**: Corporate Network
- **Level 3.5**: DMZ
- **Level 3**: Operations
- **Level 2**: Supervisory
- **Level 1**: Control
- **Level 0**: Instrumentation

Generally accepted structure, there will be variations.
Understanding an ICS

- Overarching process
- **Which protocols** exist at each level
- Protocol **limitations** and **security**
- **Device** make, model, and function
- Mechanical / physical / non-networked **controls**
- Human controls
- **Interactions** and dependencies between processes
1. ICS are often based around legacy hardware and protocols
2. Familiar IT tech is becoming common
3. Networking increasingly common
4. Air-gapping is pretty much a fairy tale
5. ICS protocols rarely have authentication or encryption
6. ICS technology can be sensitive to scanning / exploitation, but there are ways to test it
7. Operators have different (and usually correct) priorities
8. ICS is learnable, and we must learn and secure it
Yes, we see XP embedded (and older) frequently
But why?

• Systems purchased as interdependent package
• System support contracts don’t allow modification
• Hardware lifecycles are very long
• Maintenance windows are rare, and tricky to arrange

This requires adaptation to legacy hardware and software!
• IT hardware and software is cheap and accessible
• Reinventing the wheel causes problems
• Engineers are often familiar with IT software & hardware
• Parts are easier to replace
Why is this stuff being plugged into the LAN / Internet?

• Operator / technician convenience
• Remote process control (SCADA)
• Historian monitoring (telemetry and statistics)
• System efficiency
So why not air-gap all these sensitive systems?!

- Air-gapping is expensive
- Some connectivity is almost always required
- “Air-gapping” usually isn’t
- Data diodes are expensive and rarely seen
• Encapsulated legacy protocols
• The “A” of C.I.A. is king in ICS
• Newer ICS devices may have some improved security
• Devices must function in operational environments
• Expectation of redundancy, physical and human controls
Yes, Scanning *can* Break Stuff...

- Some protocol stacks lack features
- Legacy may not fully implement modern standards
- Embedded systems with minimal resources

**Do not scan or exploit ICS without permission and an expectation of outage.** However...

- Digital twin systems
- Outage windows
- Passive traffic, configuration, and protocol analysis...
- **Don Weber will discuss this further!**
Operators have a Different Point of View

• Operators care about **consequences** and **risk**
  
  *Loss of life, injury, contamination, process failure…*

Your finding **may not result** in a consequence they care about

- **Infection** won’t necessarily cause a consequence
- **Exposure** won’t necessarily cause a consequence

• Understanding process and key consequences is **critical**
• What **systems** and **conditions** can cause those consequences
  • How are consequences **mitigated**?
1. ICS are integral to our society and to you
2. Pick a starting point; don’t get overwhelmed
3. Lots of OSINT!
   - Scribd, Shodan, Google, eBay...
4. Build relationships and dialogues with OT!
   - Operators do care about security
5. Learn about processes, consequences, and operations
6. Formal training is available, but limited in scope
QUESTIONS?

@hacks4pancakes

hacks4pancakes@gmail.com