HOW DID WE GET HERE?

The History and Future of Cyberattacks against Industrial Control Networks
Greetings

- Lesley Carhart, Director of Incident Response, Dragos Inc
- 15 years in industrial cybersecurity, previously Motorola
- USAF Retired
- Lecturer, Blogger, Mentor, Conference Organizer
@hacks4pancakes on the things
Why I’m Here

Industrial Control Systems (ICS) make our modern world function, and they are under attack.

Today’s Primer:
• ICS Concepts, Architecture, and Theory
• Failure Points and Consequences
• A Brief History of ICS
• 25 Years of ICS Cyberattacks
• Current State and Challenges
• What’s Next?
ICS Concepts and Theory

First, let’s understand a “process”

- “Industrial processes are procedures involving chemical, physical, electrical or mechanical steps to aid in the manufacturing of an item or items, usually carried out on a very large scale” – Wikipedia

Processes must be **controlled** in a defined way by **something**

**Industrial Control Systems** provide some level of automation for the control of industrial processes
What is an Industrial Control System?
Process Control Loops

- Every Industrial Control System is made up of at least one Process control loop
- Control loops must have 3 components
Process Control Loops

SENSOR

TEMPERATURE
PRESSURE
MOTION
LIGHT...

CONTROLLER

MECHANICAL
RTUs
PLCs
IoT DEVICES

ACTUATOR

MOTOR
PUMP
SWITCH
VALVE...

35th ANNUAL FIRST CONFERENCE | EMPOWERING COMMUNITIES
Process Control Loops

When am I supposed to rotate?
When am I supposed to stop rotating?

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

Obligatory hotel example

SENSOR

• MOTION
• OBSTRUCTION

CONTROLLER

ACTUATOR

• MOTOR
(Rotation)
What Can Go Wrong?

The Actuator…

1. Fails to start when it’s supposed to
2. Fails to stop when it’s supposed to
3. Starts too early or too late
4. Goes on for the wrong period of time

This Photo by Unknown Author is licensed under CC BY-NC-ND
Why is this Important?

- December, 1984 - Bhopal, India Plant Disaster
- Union Carbide India Limited (UCIL) pesticide plant
- Triggered by refrigeration system failure
- Safety system malfunction and bypass compounded degradation and poor system maintenance
- Over half a million people exposed to toxic methyl isocyanate (MIC), thousands dead
- **Industrial systems operating in incorrect ways have real, kinetic impacts**
We Rely on Industrial Control Systems, Today

- Essential utilities at scale
- Manual controls are limited and no longer universal
- Just in time logistics
- Transportation
- Not just electrical power...
- Essential quality of life and safety
- Real Consequences
A Brief History of ICS
The Beginning

- Industrial Control Systems can be **mechanical**, **analog**, or **digital**
- Earliest ICS were mechanical
- Ktesibios’s water clock in Egypt ~270 B.C.
- Cornelis Drebbel - first furnace thermostat in 1620
- Early industrial control was heavily focused on maritime, time, and trains
- Gears and weights provide control, instead of humans

Photo by Unknown Author is licensed under CC BY-ND
ICS Through the 20\textsuperscript{th} Century

- Mass-production manufacturing
- Urbanization
- Aviation
- Migration to analog electronic control devices
- Electronic circuits, instead of gears and weights, provide control
Digitization of ICS

- First industrial computer – Louisiana Power & Light, 1958
- First digital ICS – Texaco, 1959
- Development of the transistor and small, cheap computing machines
- By 1971, there were 41 manufacturers of ICS computers
- Ladder logic, and serial protocols instead of simple circuits, provide control

Let’s Understand ICS A Little Better

- A single control loop is limited
- A complex process is made up of many control loops
- Require human or automated synchronization
Distributed Control and SCADA

- Modern computers can provide granular efficiency and telemetry
- **Distributed Control Systems** – Limited Geography
- **SCADA** – Wide scale, deeper analytics
IT/OT Convergence

- Commercial computing equipment is **cheap** and **readily available**
- Shift from custom software and hardware to **enterprise vendors**
- Networks increase **efficiency** and **remote capability**
- **Cost savings** drive business choices

Unfortunately, the threat landscape is much larger against networked, popular operating systems and protocols...
More Presence and Power, More of a Target...
Early Attacks against ICS

- 2000 - Maroochy Shire Sewage Spill
- 2007 - Idaho National Labs Aurora Generator Test
Stuxnet: Pandora’s Box

- Worm discovered in 2010
- Suspected development as early as 2005
- Disrupted Iranian nuclear program through centrifuge tampering
- First known cyberweapon targeting ICS
- Highly complex, required deep knowledge of specific process and control systems

Most of us are familiar with the story of Stuxnet, but it remains a key point in history, and likely inspired future attacks / capabilities
German Steel Mill

- 2014 – “under the radar” report of cyberattack against steel mill
- German government’s *Bundesamt fur Sicherheit in der Informationstechnik* (BSI) annual findings report
- Knowledgeable attackers
- Caused control system failures resulting in “massive damage”
Ukraine Power Grid Cyberattacks

- Ukraine is a long-term test bed for kinetic cyberattacks
- December 2015 – cyber attack cuts power to quarter million Ukrainians for ~six hours
  - BlackEnergy 3 malware as vector
- December 2016 – second attack on Ukrainian power grid, with additional disruptive elements, more sophisticated and repeatable tactics
  - CRASHOVERRIDE / Industroyer malware specifically targets power
  - Disruption to restoration efforts – holistic process
- Cyberattacks reportedly continue against Ukraine during war
Safety is a key consideration in processes for a reason.

Safety Instrumentation Systems supplement analog and human safety controls.

2017 - TRISIS/TRITON targeted Triconex safety systems.

Deep implications for human safety and process operation.
Recent History – Ransomware and PIPEDREAM

- ICS cyberattacks are evolving and becoming more efficient
- Ransomware, Colonial Pipeline, and commodity malware impacts
- 2022 - PIPEDREAM toolkit lowering the barrier to entry...
The Bottom Line

- **Criminals** will always try to make money
- States will always **spy**
- **Sabotage** will always be an element of warfare and geopolitics
- Computers **make this more accessible**
ICS Cybersecurity in 2023
Daily DFIR Casework in 2023

Commodity Malware

Insider Threats

State Adversaries
The State of Modern Industrial Networks

- There is **awareness** of cyber threats
- Organizations are **under-resourced**
- Regulation is limited and haphazard
- Verticals vary vastly in maturity
- Many **faulty assumptions** by executives and practitioners
- Tool and **research** landscape is relatively immature
Challenges in Industrial Security and Response

- Process consequences
- System sensitivity and safety
- Legacy technology and lifecycles
- Proprietary infrastructure and warranties
- Low-level devices
- Legacy security tooling
- Growing divergence between cybersecurity training and ICS cybersecurity
- Focus on bugs, when process is the real concern
Real Solutions are Holistic

- Understanding **Environment** and **Assets**
- Secure Architecture and Vulnerability Management
- Interpersonal **Relationships**
- Preparation (Incident Response, Business Continuity, Disaster...)
- Passive Monitoring and Detection
- Consequence-Driven Planning and Evaluation
The Near Future...

- OT workforce reaching **retirement** age
- ICS DFIR **skill divergence**
- Immense spaces to cover in **research** and **tool** development
- PIPEDREAM socialized a concerning concept
- Barrier to entry continues to lower
- Global **financial conditions** drive efficiency for adversaries, too
We Need You!

**Leaders**: Executive buy-in, awareness of programs and process environments, bridge-building, resourcing

**Practitioners**: Attention to process environments, adaptability, consequence and process focus

**Researchers**: Tools, strategies, reverse engineering of industrial devices beyond simple bugs

**Voters and Citizens**: Concern for industrial systems that make our world work, even if they ‘always work’.
Questions? Comments?

lcarhart@dragos.com
@hacks4pancakes