NETWORKING APPROACH TO HOST-BASED INTRUSION DETECTION

DAVID FORMBY
INTERNET2 CINC UP CALL
OCTOBER 13, 2017

CREATING THE NEXT®

CURRENT EVENTS

Georgia Tech

KIM ZETTER SECURITY 11.29.10 04:18 PM

IRAN: COMPUTER MALWARE SABOTAGED URANIUM CENTRIFUGES

ANDY GREENBERG SECURITY 06.12.17 08:00 AM

'CRASH OVERRIDE': THE MALWARE THAT TOOK DOWN A POWER GRID

#CYBER RISK SEPTEMBER 6, 2017 / 6:05 AM / 14 DAYS AGO

Hackers gain entry into U.S., European energy sector, Symantec warns

WannaCry ransomware ca plant to shut down

It's still making the rounds.

OVERVIEW

- **Background**
  - **What is critical infrastructure and why is securing it so hard?**
  - **Why haven't there been more attacks on them?**
- Ransomware for industrial control systems
  - Ransomware business model
  - Demo ransomware attack against a water utility
- What to do about it?
  - Standard defenses and their shortcomings
  - Program change detection
- Conclusions and discussion

BACKGROUND: CRITICAL INFRASTRUCTURE

DHS – 16 Critical Infrastructure Sectors

9 rely on industrial control systems (ICS)

Chemical

Factories

Dams

Energy

Defense

Food

Nuclear

Transportation

Water

BACKGROUND: ICS (IN)SECURITY

Standard security practices

- Regular, timely patching
- SSH, SFTP, HTTPS
- Required, long, complex passwords
- Confidentiality, integrity, availability
- Firmware signing
- ASLR, DEP, stack canary

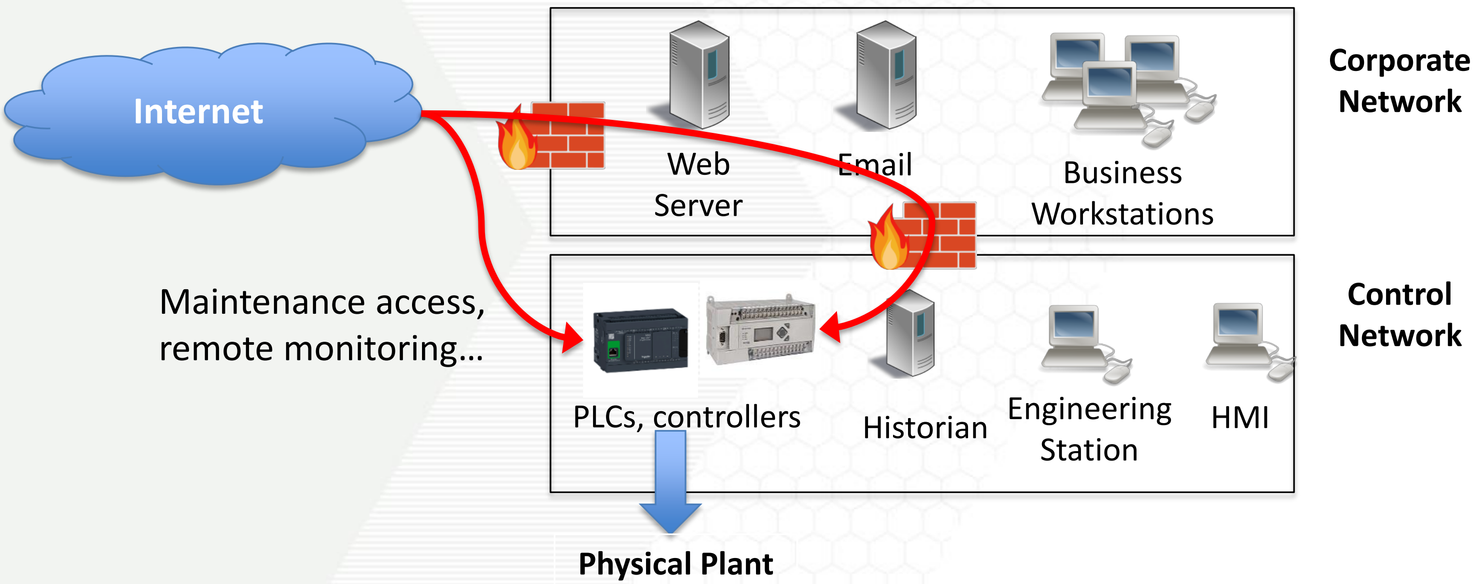
Standard ICS practices

- Patches – yearly, if ever
- Telnet, FTP, cleartext ICS protocols
- NO passwords, default, weak, clear
- Availability, availability, availability
- Starting to sign firmware
- Nope

Case study – Power grid

- Vulnerability – predictable TCP initial sequence numbers (*1985*)
  - Discovered from passive observations
  - Allows blind hijacking
- Power Distribution Substation Network
  - 196 Nodes – 68% vulnerable
  - 3 out of 8 device vendors vulnerable
    - VxWorks – the “Windows” of RTOS
    - GE – “no method available to update this device”

BACKGROUND: ICS (IN)SECURITY



WHY IS ICS SECURITY SO HARD?

- Downtime
  - Lost revenue every minute
  - Always on power grid, water distribution…
- Legacy devices
  - Designed for 20 year lifecycles, not the IT standard of 3-5 years
  - Originally made for dedicated serial links, the only access control was physical
  - Misconceptions in industry

MISCONCEPTION - AIRGAP

Claim

"Our control network is airgapped, so we don't have to worry about security."

Reality

- Vendor maintenance access
- Remote monitoring
- Laptops, USB sticks
  - Stuxnet
- Insiders

MISCONCEPTION - BACKUPS

Georgia Tech

Claim

“If a PLC gets infected, we’ll just switch it out with another.”

Reality

- Likely ALL of your PLCs
  - $10k x 100 PLCs > $1million of PLC inventory
- Engineering software likely infected
- Manpower rewiring, reprogramming
- Original vulnerability STILL there

MISCONCEPTION - MOTIVATION

Claim

"Why would anyone want to attack us?"

Reality

- Small to medium sized businesses hit hardest by cyberattacks
- Havex, BlackEnergy, DragonFly already widespread
- Motivation
  - Monetary in the form of ransomware

OUTLINE

- Background
  - What is critical infrastructure and why is securing it so hard?
  - Why haven't there been more attacks on them?
- **Ransomware for industrial control systems**
  - **Ransomware business model**
  - **Demo ransomware attack against a water utility**
- What to do about it?
  - Standard defenses and their shortcomings
  - Program change detection
- Conclusions and discussion

NEWS

Georgia Tech

Move over Healthcare, Ransomware Has Manufacturing In Its Sights

by Bill McGee | Jun 06, 2016 | Filed in: Industry Trends & News

Holding the HMI Hostage—The Growing Threat of Ransomware

as
works

The New York Times | https://nyti.ms/2jO7vbZ

EUROPE

Hackers Use New Tactic at Austri
Hotel: Locking the Doors

By DAN BILEFSKY JAN. 30, 2017

Ransomware locks up San Francisco public transportation ticket machines

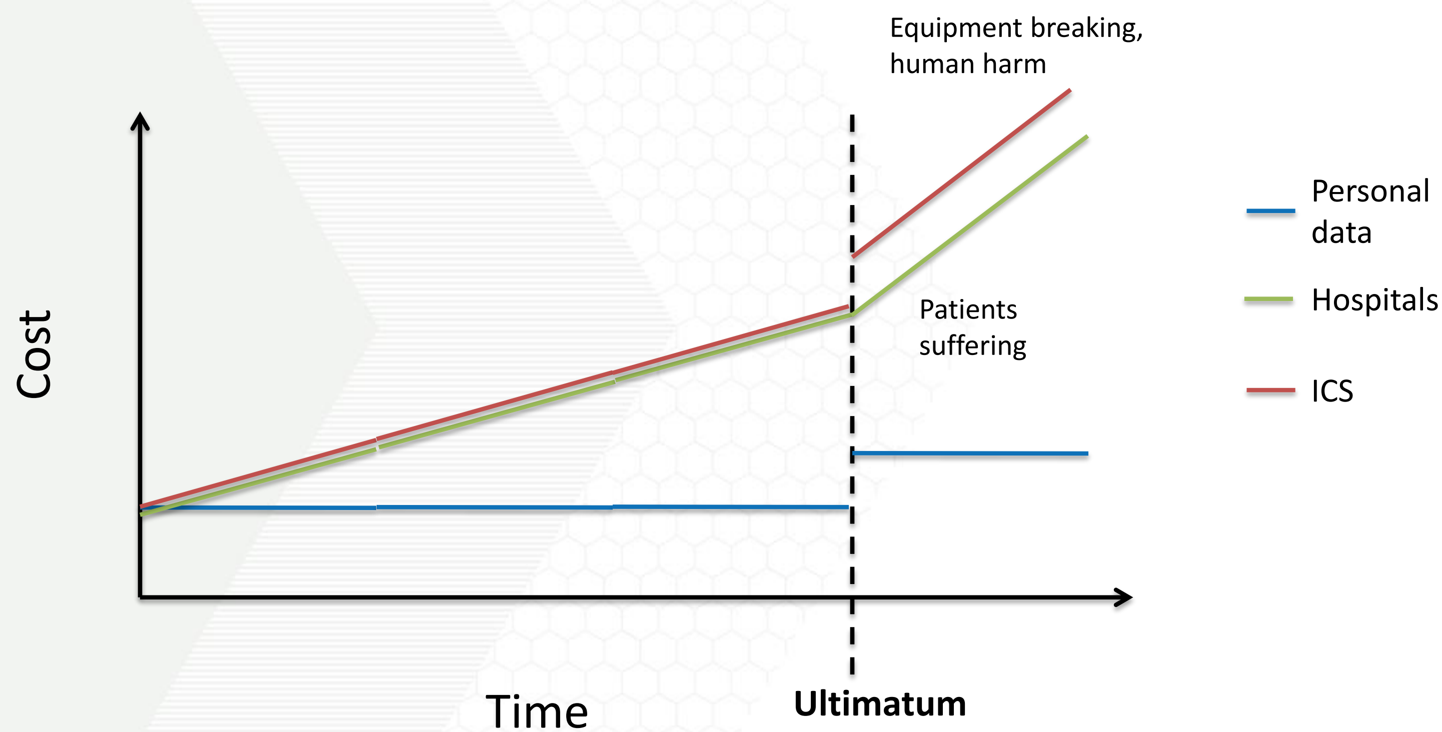
Some systems now restored; attacker demanded $73,000.

SEAN GALLAGHER - 11/28/2016, 11:51 AM

NotPetya Ransomware Attack C
Maersk Over $200 Million

FedEx estimates ransomware attack cost $300 million

ICS RANSOMWARE: IMPACT



WHAT MAKES A RANSOMWARE ATTACK SUCCESSFUL?

Hospitals

- Easier targets
  - Old equipment
  - Traditionally weak security posture
- Increasing time pressure
- Lives at stake
- Crown jewels = patient data

ICS Networks

- Easier targets
  - Old equipment
  - Traditionally weak security posture
- Increasing time pressure
- Lives at stake
- Crown jewels = safe operation

ICS RANSOMWARE: MARKET SIZE ANALYSIS

Businesses Hit by Ransomware

- 70% paid the ransom
- Median payout approx. $10k
- Small, medium sized businesses less prepared

Source: IBM, “Ransomware: How consumers and businesses value their data”

PLCs on the Internet

MicroLogix 1400

- 1,300

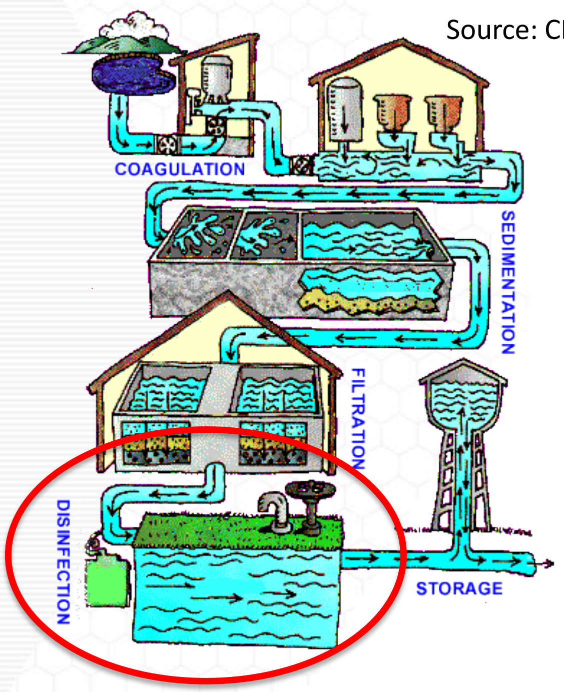
Schneider Modicon M221

- 200

1,500	x	**$10,000**	x	**50%**	=	**$7.5 Million**
Trivial PLCs		Expected payout		Conservative success rate		

DEMO: WATER TREATMENT FACILITY

Source: CDC, “Water Treatment”

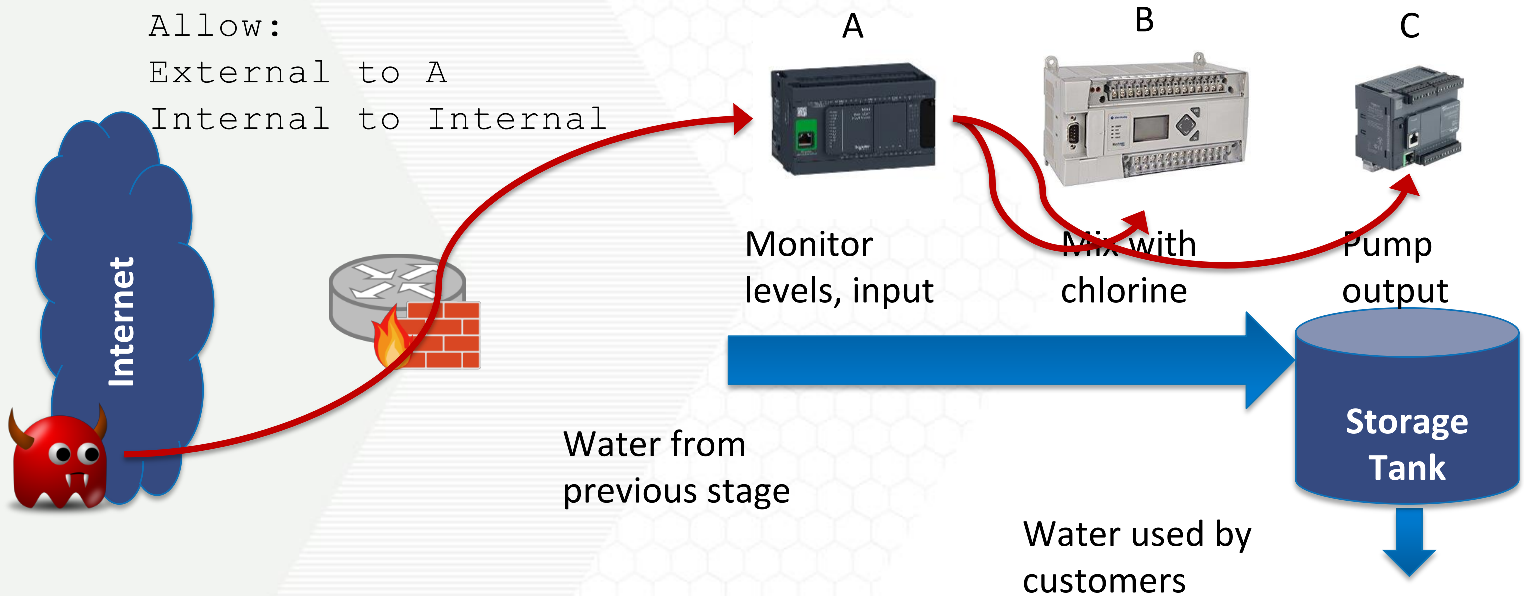


Testbed simulates the Disinfection and Storage stages

Typically mixed with chlorine to kill bacteria

We use iodine because it’s safer to handle and cooler looking

DEMO: NETWORK



DEMO: INITIAL FOOTHOLD

Georgia Tech

Schneider Modicon M241

- Running CODESYS V3
    - Third party PLC runtime environment used by over 200 vendors
- Password
    - No brute force checks
    - No strength policy
- Controlling the water input and monitoring the storage levels

DEMO: NETWORK SCAN

Reprogram the M241 to scan the internal network and grab model numbers

Allen Bradley MicroLogix 1400

Modicon M221

```
david@dell-xps: ~/Documents/rsa_pres
david@dell-xps:~/Documents/rsa_pres$ sudo nmap 192.168.1.241

Starting Nmap 6.40 ( http://nmap.org ) at 2017-02-03 15:17 EST
Nmap scan report for 192.168.1.241
Host is up (0.012s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
1105/tcp open  ftranhc
MAC Address: 00:80:F4:0A:9D:C7 (Telemecanique Electrique)

Nmap done: 1 IP address (1 host up) scanned in 159.76 seconds
david@dell-xps:~/Documents/rsa_pres$ python internal_recon.py
Devices found:

        192.168.1.140
        1766-LEC

        192.168.1.221
        TM221CE24T
david@dell-xps:~/Documents/rsa_pres$
```

DEMO: NETWORK SCAN

Allen Bradley MicroLogix 1400

- Password only checked in engineering software, **NOT** the PLC
- SMTP mail client
- Controlling the addition of chlorine (iodine)

Schneider Modicon M221

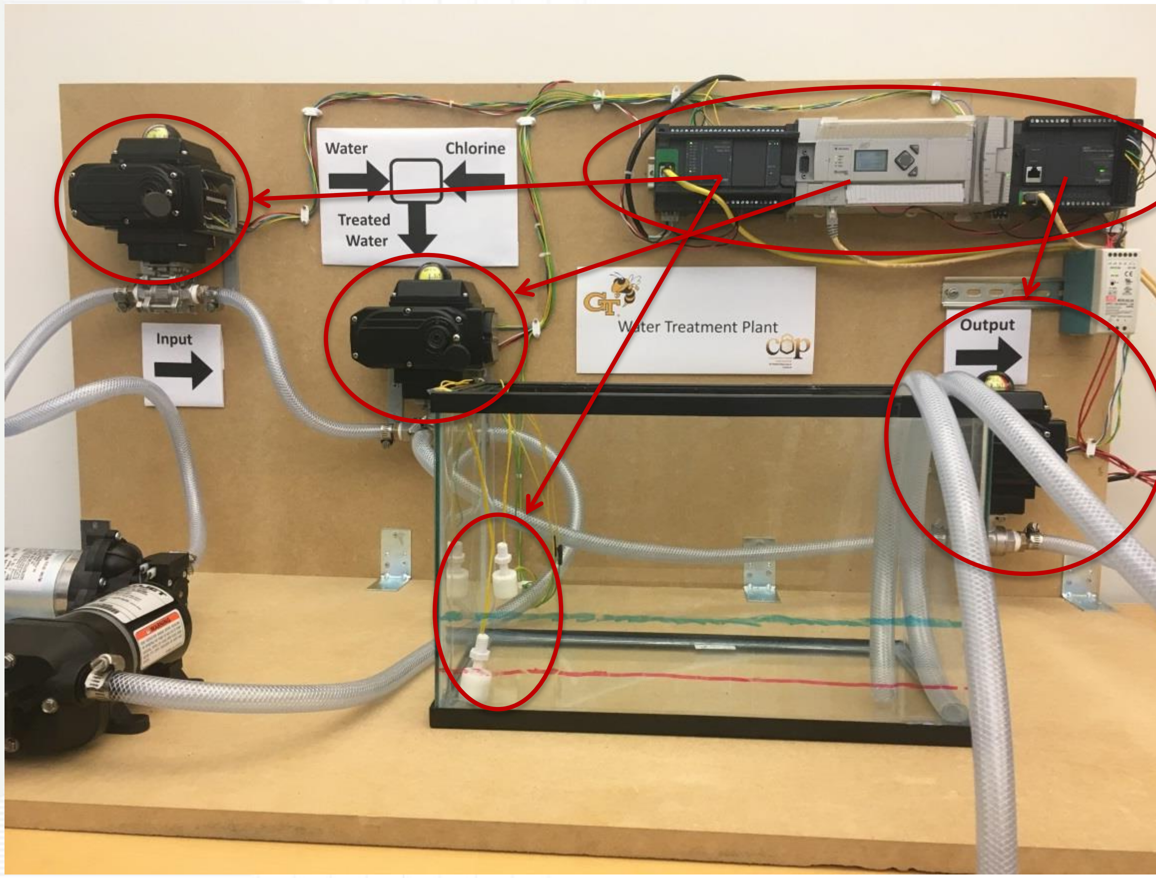
- Password only checked in engineering software, **NOT** the PLC
- Controlling the final output of treated water

DEMO: NETWORK

Input water valve

Mixing valve to control ratio of water/iodine

Level sensors



Programmable logic controllers

Output water valve

MAXIMIZE SUCCESS

- Pick targets with high downtime costs
- Understand the process behind the PLCs
- Threaten to screw things up if they don’t meet deadline
  - What if they just unplug everything?
- Covertly move system into critical state **before** notifying them
  - Allow reserve storage tank to get low first, blinding operators
  - Make continued operation by attacker more attractive than shutting everything down

DEMO

https://youtu.be/t4u3nJDXwes

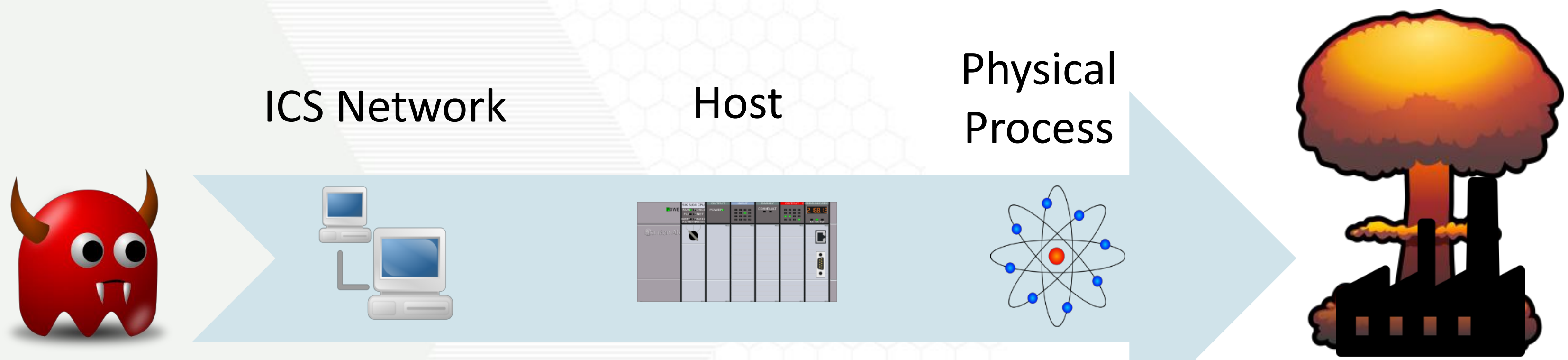
DEFENSES

- Proper password authentication
  - Requires vendors, not happening anytime soon
- Network segmentation, secure remote access
  - Insiders
- Monitor the network
  - Misses attacks launched from local access

OUTLINE

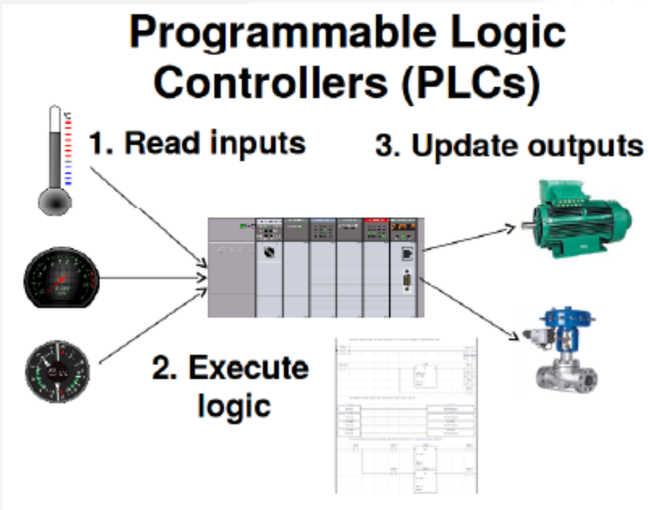
- Background
  - What is critical infrastructure and why is securing it so hard?
  - Why haven't there been more attacks on them?
- Ransomware for industrial control systems
  - Ransomware business model
  - Demo ransomware attack against a water utility
- **What to do about it?**
  - **Standard defenses and their shortcomings**
  - **Program change detection**
- Conclusions and discussion

MOTIVATION

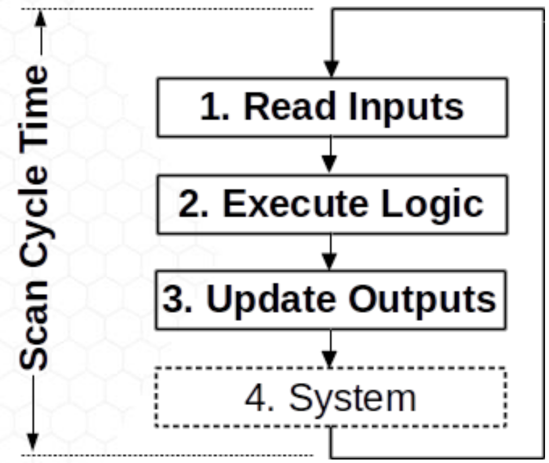


Problem: Need intrusion detection of hosts for defense-in-depth
Solution: Program execution time signatures

BACKGROUND



Used everywhere from oil & gas to rollercoasters and elevators



Determined by hardware and complexity of program

THEORY

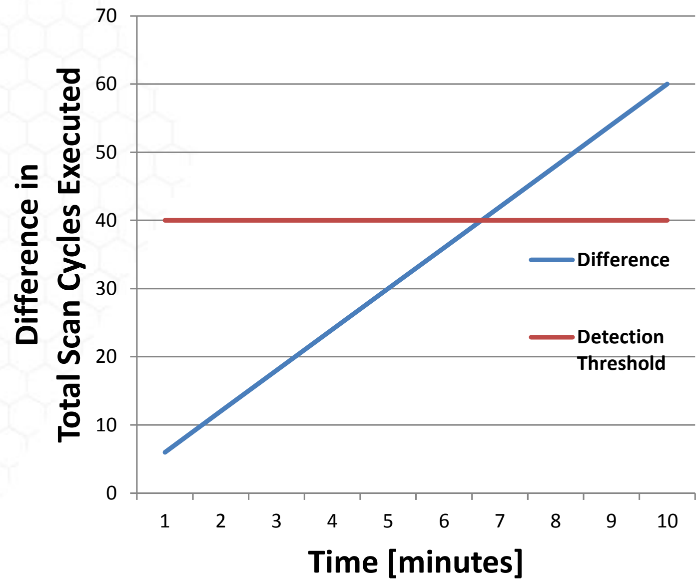
Any <u>consistent</u> change, no matter how small, will eventually build up to observable differences

Example

Original Scan Cycle Time = 1ms
+ single bit comparison (0.1µs)

Modified Scan Cycle Time = 1.0001ms

After 10 minutes, the original program has executed 60 cycles more than the modified one



DEFENSES: EXPERIMENTAL SETUP

Georgia Tech

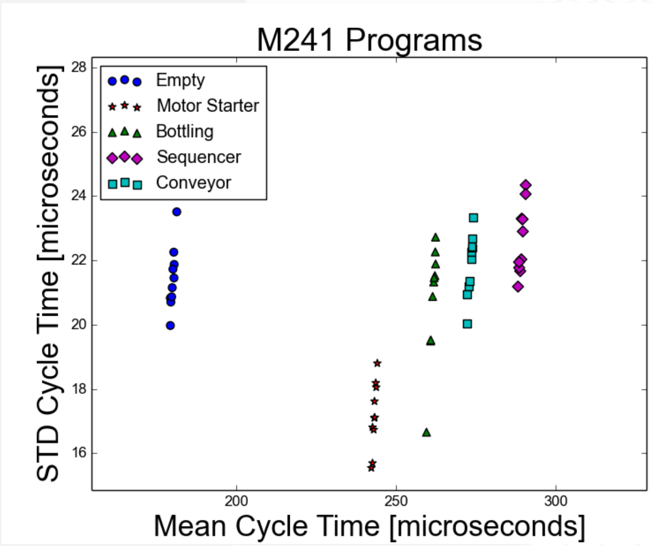
PLCs used

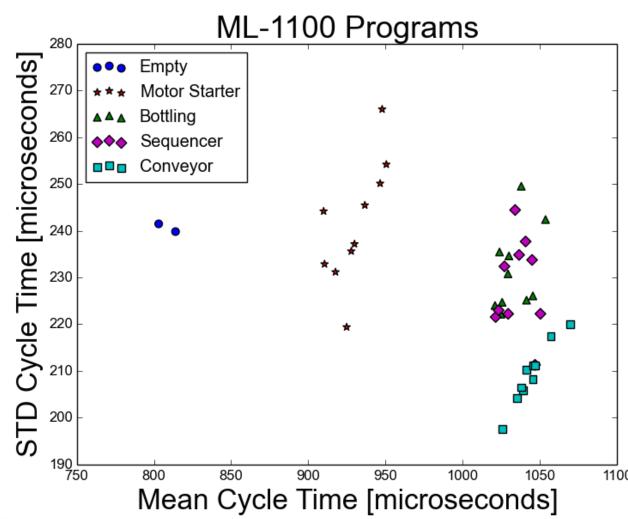
PLC Model	Application Memory	Cycle Resolution
MicroLogix 1100	8 KB	100 µs
Siemens S7-1200	75 KB	1 ms
Schneider M221	256 KB	1 µs
Schneider M241	8 MB	1 µs

Example programs used

Program	Description	Instructions	Data Words
P1	Motor Starter	553	1068
P2	Sequencer Example	365	160
P3	Bottling Plant	419	433
P4	Conveyor Belt	615	425

Fingerprints using system diagnostics





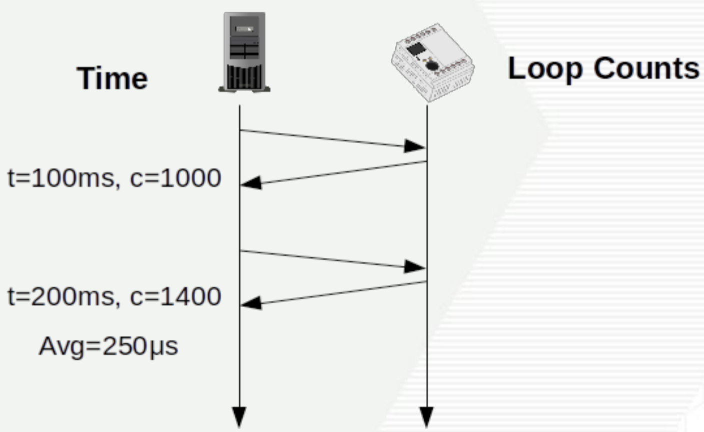
Faster processor and high resolution, clear differences

Slower, low resolution
Significant overlap

DEFENSES: REFINED SCAN CYCLE MEASUREMENT

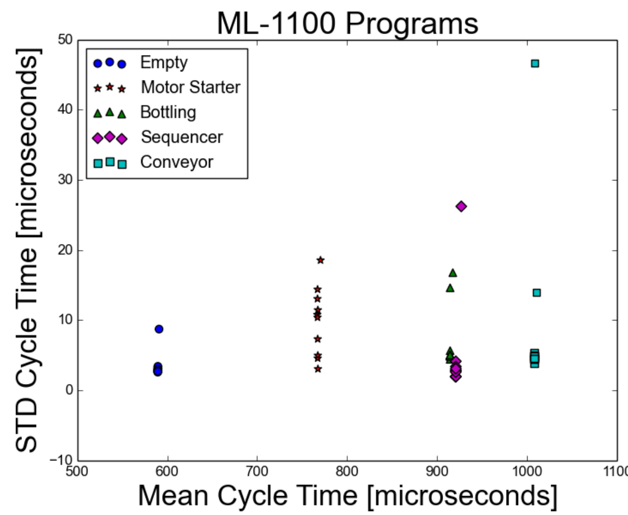
Improved accuracy

using cumulative scan cycle count



Clear distinctions

between programs

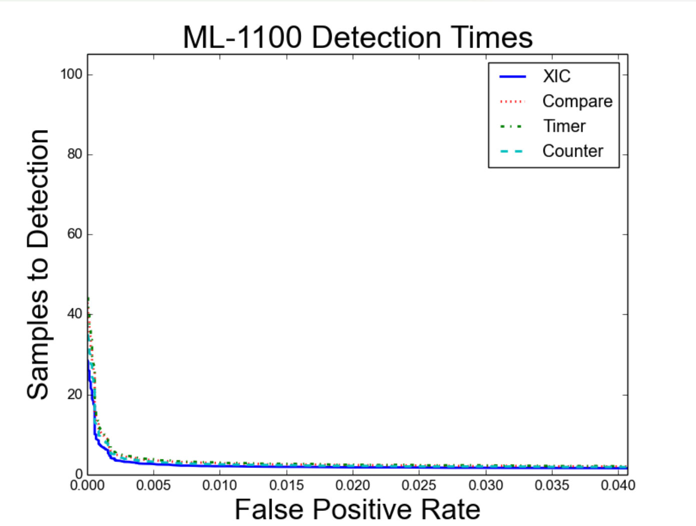


DEFENSES: ATTACKER MODEL

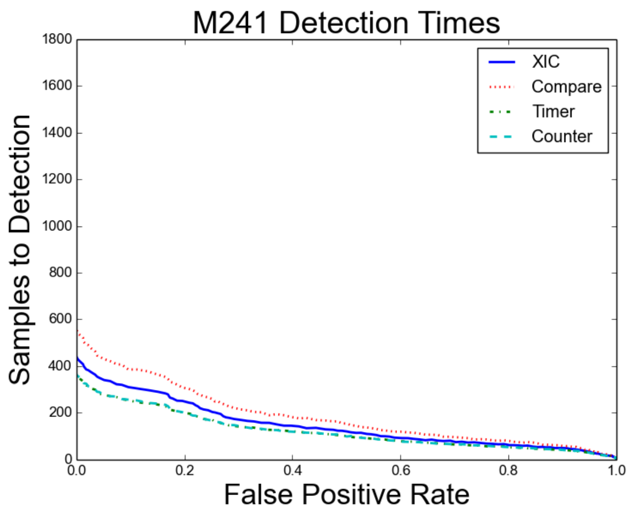
- Attacker Goals
  - No immediate impact on process to hide from operators
  - Insert logic bomb to cause damage over time
  - Stuxnet, e.g.
- Logic bomb triggers Inserted in Main Control Loop
  - Examine if closed (XIC)
  - Compare
  - Timer
  - Counter

DEFENSES: CHANGE DETECTION RESULTS

Detection time < 5 seconds, 0% FPR



Detection time < 1 minute, 0% FPR

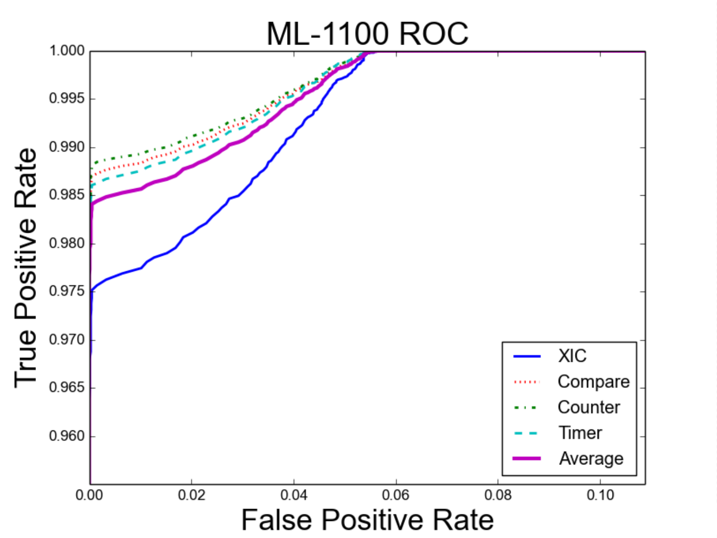


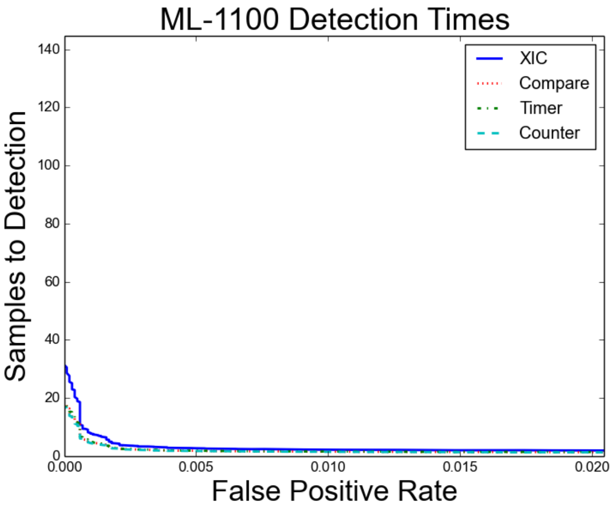
DEFENSES: INTELLIGENT ADVERSARY

- Intelligent adversary can replay and mimic
- Use proof of work functions to give PLCs “alibis”
  - Prove they were not executing additional instructions
  - More robust way of measuring program execution time
- Proof-of-work (POW) function
  - Computationally expensive to solve, but easy to verify
  - Typically used as defense against denial of service
  - Ex. Discrete Log Problem: Solve for k in $g^k \bmod p = b$

DEFENSES: PROOF OF WORK

98.5% TPR at 0% FPR





Detection time < 4 seconds, 0% FPR

DISCUSSION

- Branching
  - PLC programs mostly operate in states (startup, running, shutdown…)
  - Different fingerprints for different states
  - Little branching within state
    - Averages out quickly over thousands of cycles per second
- Overhead
  - Approximately 10 lines of code (2% increase)
  - Worst case, 1ms extra time

CONCLUSIONS

- Critical infrastructure is STILL insecure
- Lack of attacks not a sign of security, but of motivation
  - Ransomware could change this
- Current defenses fail to detect skilled adversaries
  - Need to go beyond simple network anomalies
  - Proof-of-work functions can give controllers provable “alibis”

THANK YOU!

DAVID FORMBY
DJFORMBY@GATECH.EDU

Georgia Tech

CREATING THE NEXT®