Exploitable Vulnerabilities Hidden Deep in OT

Mark Carrigan
COO, PAS Global

Emerging Threat Landscape

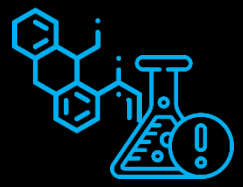
Traditional IT Hacker + OT Domain Expertise + Chemical Engineer = Havoc

OT Configuration: The Next Frontier

Top Vulnerabilities in OT Today

- Scope of Analysis
  - 10,000+ industrial endpoints
  - 380,000+ vulnerabilities
  - Variety of operating environments

Oil & Gas



Refining & Chemicals

Power Generation

Pulp & Paper

Metals, Mining & Minerals

Microsoft

OT Configuration (Programming) 101

Component	Description	Example
Control Function	Library of pre-programmed objects	Flow Controller: Model equation, data acquisition, error handling, alarms…..
Application	Embedded or third-party	Embedded: AMCL, SFC, HLBL….. Third Party: APC, Optimizers…
HMI	Graphical interface	

Exploitable Weaknesses Designed into OT

Ubiquitous Weaknesses = **They're Everywhere!!**

Unique Weaknesses = **Specific to OT Make & Model**

The Reverse

Ubiquitous

- Control Function Parameter – Output Characteristic
  - Name of parameter unique to each control system
- Binary Setting
  - Determines direct or indirect action based upon error (Setpoint-Process Value)

Flip the Setting, Watch the Fun!

- *Valve that was 20% open will now be 20% closed*
- *Fail safe valve will do the opposite of intended action*

Example

```
LOCAL t  : TIME      -- Time variable
….
SET t = now       -- Get current time in t

IF T > 86350 THEN GOTO SET_REVERSE
 ELSE GOTO LAST_ST


WAIT 15 Mins
GOTO SET_FORWARD
|
SET_REVERSE: SET FC_9290_23A.OPTDIR =REVERSE   'CTLACTN =REVERSE also work
SET FC_9290_23B.OPTDIR =REVERSE
SET FC_9290_23C.OPTDIR =REVERSE
…
GOTO LAST_ST
…
SET_FORWARD:SET FC_9290_23A.OPTDIR =FORWARD 'CTLACTN =FORWARD also works
SET FC_9290_23B.OPTDIR =FORWARD
SET FC_9290_23C.OPTDIR =FORWARD
…
GOTO LAST_ST
…

LAST_ST:
END OUTPUTDIR
```

Behold, I Am King!

Unique

X[illegible]_KEY([illegible])

- Inject this line into control system HMI
- Grants admin privileges on the entire network

Windows Account Privileges?
HA! Don't Care!

Code Invaders!

Ubiquitous

- Today's HMI – Most Use HTML
- Non–versioned, Free Format
- Implemented on Stations with Elevated Privileges
- Can Inject Code to Do Almost Anything You Want
  - Change Flow Controller Settings? Done!
  - SQL Injections into Configuration Database? Easy Peasy!
  - Hover Over a Page Corner, Be Directed to Porn Website? Sounds Fun!

Gonna Use Code Invaders to Run a Reverse Today…!

Come on Baby, Light My Fire!

Unique

Settings to Balance Computer Loading

Flow Indicator		Flow Controller
Tag 1	⟵	Tag 2
Sample Rate: 0.5 seconds	⟶	Sample Rate: 0.5 seconds
Calculation Period: 1 second		Calculation Period: 1 second

- Tags that talk better have the same settings
- Mix them up, control problems ensure (conflicting values in calculations)
- Line them up — see ya CPU!

Use that Code Invader to Change It Back…
Who's Gonna Know?

PAS

Default, Are You Kidding Me?

Unique

User Names, Profiles, & Password Hash
Stored in Configuration Database

user_profile_name	password_hash	user_full_name
SystemEngineer	-9**9	NULL
Admin	866167787	
Default	-1804721073	NULL
Engin	-115131539	Engineer
C******\sy***4_c	-805374805	*****, Da****
C******\d****1_c	-1340616663	Ty***, Jo****

1. Duplicate user name & password hash at every location

2. Changing either can create service disruptions

So, Waddya Gonna do?

You Can’t Lock It All Down

Owner Operators: Do the Basics

1. Implement Configuration Management on Crown Jewels
2. Routinely Audit for Unexpected Change

OT Security Community: Develop Best Practices

1. Leverage CIS (formerly SANS Top 20)
2. Develop Best Practices for OT Configuration Management (general & specific)

Improving Configuration Management
Improves Safety & Reliability
While Reducing Cyber Risk

Thank You

mcarrigan@pas.com