BioEnergy: Take A Walk On The Wild Side

Matthew Carpenter

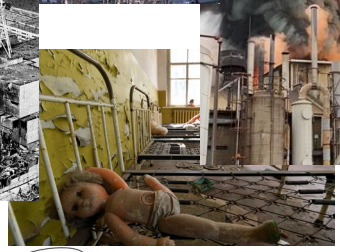
matt@grimm-co.com

GRIMM

Who am I?

- **Matthew Carpenter <matt@grimm-co.com> @Ma77Carpenter**
- **Father, Husband, Christian**
- **Exploitation Expert**
  - Involved in Software Exploitation since **2004**
  - Involved in Control Systems Exploitation since **2007**
  - Developing code analysis tools since **2005**
  - Created first Smart Meter Red Team in **2008**
- **Biker**

What happens when your Control Systems are out of control?

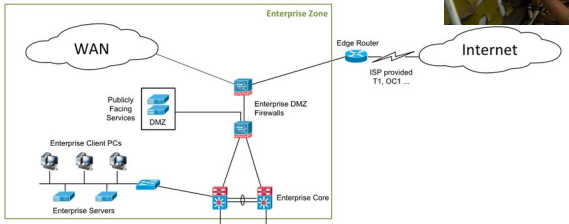


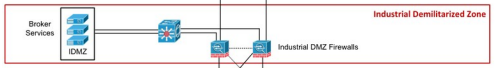
Concerns and Risks

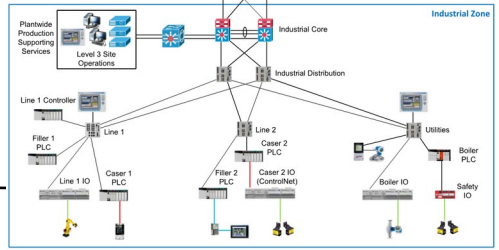
- What **blows** up?
- What goes **bad**?
- What **costs** money?
- What kills **people**?
- What kills **reputation**?

- Details matter.

What happens if someone else controls any 1-3 control systems in your facilities?







The State of OT Security

ICS represents the Tonsils of the Internet

Control Systems were Never intended to touch the Internet

- TCP/IP was “new kid on the block”
- Developers only considered natural threats
- Rugged and Costly
- Demand for Availability causes problems

Control Systems are expected to last 30-50 years

- Mfg’s didn’t budget for Security Support
- Some are already out of business

Protocols mostly created for low-latency/high availability

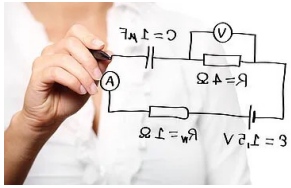
- “It just works” isn’t always secure

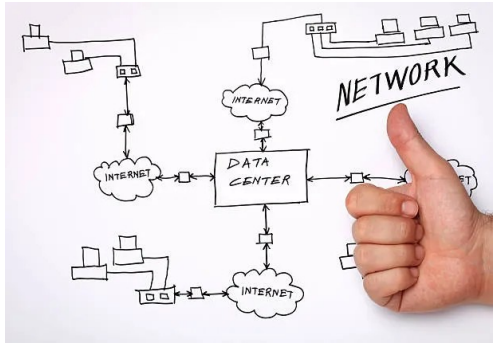
New Research

- National Labs continue to work towards securing OT
  - Sandia has been working on some interesting stuff

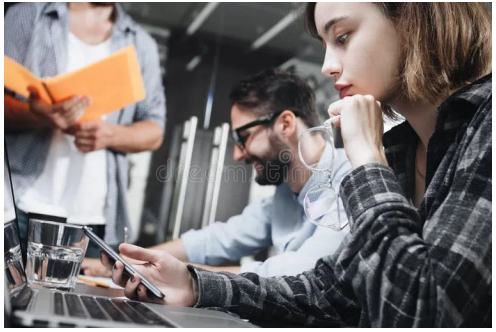
Sandia National Laboratories

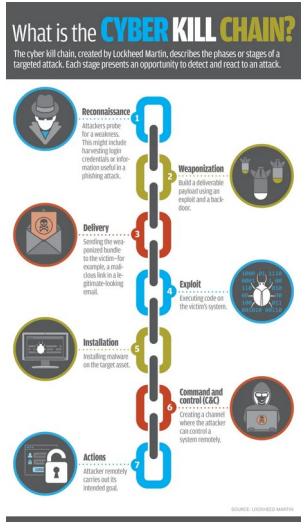
How to Think about Cybersecurity





- **All** Software has **Bugs**
- Compromised Systems
  - Can be **Pivot** Points
  - Can Do **anything** Physics Allows (with nuance)
- **People** can be **access-points**
  - Email / Text / Social Media
  - USB sticks
- **Copper** can't house viruses
- Computers **Will Be** Compromised
- **Visibility** and **Response** are **Critical**





Know Your Adversaries

- All sectors have different adversaries, but similar categories
  - Nation State
  - Organized Crime
  - Competitors
  - Detractors
  - Jim Bob with a ‘puter

- The adversaries **exploit** similar **weaknesses**
  - **People**
  - Connected **Technology**

- **Pivoting** to Maximize Success!

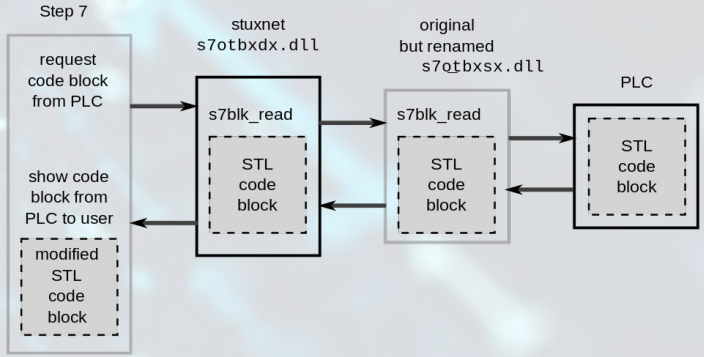
Some Context: StuxNet

For your consideration:

- **USB Thumb Drive** – via Russian Contractors? Iranian Mole?
- "**Airgapped**" Facility in Natanz
- Modded WinCC **`s7otbxdx.dll`** and **ICS Programming** Station
- Pushed "a **gift**" to the **PLCs**
- "the gift" (PLC code) **self-identifies** the right PLC
  - Only Siemens **S7-300** PLC's with **variable-frequency drives** from **Vacon** and **Fararo Paya** spinning between **807Hz** to **1,210Hz** !!!!!!
- First PLC Root Kit – **hiding and effects in rotational speed**
- Complex methods of getting **updates** (numerous versions)
- Developed in **2005**, **2007** launch, not widely known until July **2010**...

Costly:

- 4 zero-day vulns, 2 known vulns
- USB attacks
- Windows and PLC payloads
- DLL modification
- User / Kernel-mode Rootkits
- Digitally Signed Kernel Drivers (signed by two well-known public keys)



Know Yourself

What do I need to know?

- What is your **attack surface**?
- What "**stuff**" do I have? (aka "assets")
  - Computerized/**"Smart" things**
  - IT systems
  - Cell Phones
  - **Vehicles**
- Refinery / Magic Caldrons
- **Normal Network Activity**
- Product Storage
- **Transportation/Logistics**

ICS-CERT

Lab Equipment

Who Finds the Undetected?

Who's responsible for finding the unfound?

- If it's not someone's **responsibility**...
  - If the org doesn't **realize** it should be...
    - Persistent threats will only be discovered with a **catastrophe**.

Visibility / Threat Hunting

Without Visibility

– All is well! You never know otherwise
  - until it's too late

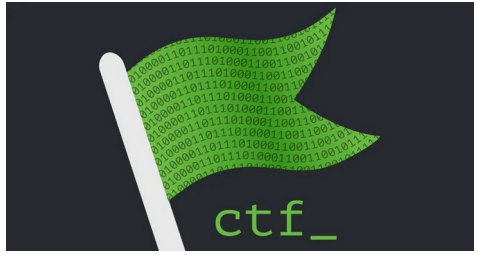
Network Monitoring
Intrusion Detection Tools
Knowledge Management Tools

Threat Hunting

– Looking for **Adversaries** on your networks
  - In **Response** to Activity / Alerts / Suspicion
  - **Preemptively** looking for problems
– Must **know** your network / devices
– Must **understand** what "**normal**" looks like
– Must **develop skills**
  - In **advance**
  - For the **long haul**
  - Never fully "ready," but possibly "**ready enough**"

How do you Train/Maintain Cyber-Minded Workforce?

- **Training**
  - SANS
  - BlackHat
  - others
- Participation in **Security/Hacking Organizations**
  - ISSA
  - HTCIA
  - InfraGard
  - hacking groups/conferences
  - City-Sec groups
- **CTFs** - Hands-On Makes it Real
  - Many Types of CTF
    - Binary Analysis/Exploitation
    - Web / Network-pen-testing
    - other focuses
  - ICS Village



How are you building community?

- "Friends"
- Other industries
- ISAC

bioisac

ICS-ISAC

Sample R&D Areas

- **Vulnerability Research** (can't exploit a bug that doesn't exist)
- **Protective Defenses**
- **Visibility**
- **Test** and **Lab** Development (economies)
- **Collaboration**
- **Physical Protections**
- **Design and Implementation Security REVIEW** (identify what is)

Conclusion

–**OT Security is hard**
- Diligence
- Knowledge / Experience
- Design / Implementation / Product Securability

–**BioE is unique**, but **shares** much context with other OT verticals

–IT/OT are **both important**, and many **lessons** can be learned **both ways**

–**Take care of your people**, help them **thrive** and **grow**
- HANDS ON MAKES IT REAL

–**Do not underestimate** the adversaries who:
- Want you to **fail**
- See you as a **lucrative** target

Thank You!

“Offensive Cyber for Fun and Safety”

Thank you

Matthew Carpenter
@Ma77Carpenter
GRIMM (SMFS, Inc)

matt@grimm-co.com
616-813-5103

info@grimm-co.com