The Threat of Ransomware in Energy Delivery Systems

David M. Nicol
Franklin W. Woeltge Professor of ECE
Director, Information Trust Institute
University of Illinois at Urbana-Champaign

The Threat

To:chief.executive.officer@gotham.city.power.com
From:chief.infosecurity.officer@gotham.city.power.com

Mr CEO---this message is not authored by your CISO. We are the Citizen's Alliance for Clean Energy, and we have control of your cyber systems, in particular, of your Moon River power plant. Ask your engineers, they've lost control of the plant.

Our software will cause destruction of its generators by midnight tonight, unless you publically announce the plant's immediate retirement. On seeing this announcement we will tell you how you can disable that timer. Be aware however that any subsequent actions not directly connected to a shutdown will trigger the destruction.

Happy Halloween!
Citizen's Alliance for Clean Energy

The big issue in energy delivery systems…the consequences

- Physical damage / harm to humans resulting from
    a. Loss of control
    b. Loss of situational awareness
- Loss of operational service
- Loss of administrative support service

A bit ‘o history

Ransomware found in utilities

- April 2016. Lansing Board of Water and Light
  - Interface to services interrupted for 1 week. **Service itself was not.**
- May 2017. Bengal power utility hit by WannaCry.
  - Only billing systems affected
- August 2017. Staunton County Public Power District (NE).
  - Admitted by customer service agent ‘updating Adobe Flash’.
  - **Files in business unit** were locked
  - Entity recovered, using backups, within a day.
- Private communications with ICS-CERT revealed that a number of electric utilities have reported ransomware on business systems
  - **But not to ICS**

Approach to problem…

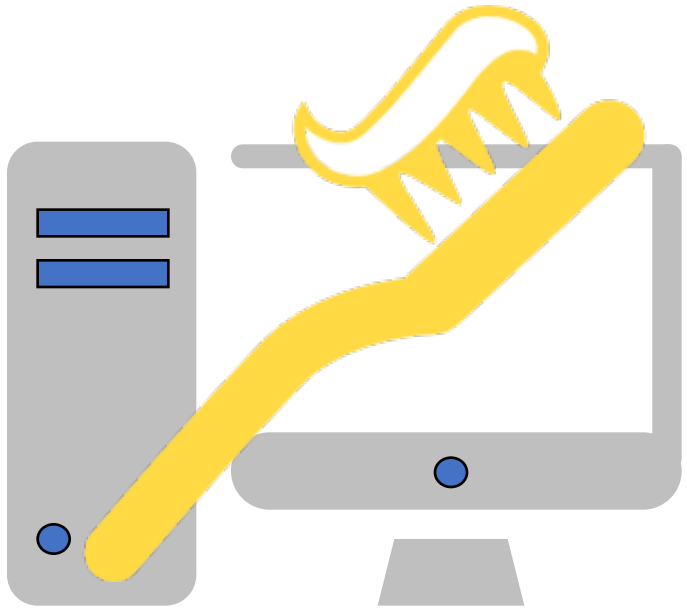
Today's threat…attack vector through email attachments, connecting infected machines to OT devices, malvertising

Best Approach:

Approach to problem…

Today's threat…attack vector through email attachments, connecting infected machines to OT devices, malvertising

Best Approach:



Approach to problem…

Today's threat…attack vector through email attachments, connecting infected machines to OT devices, malvertising

Approaches:

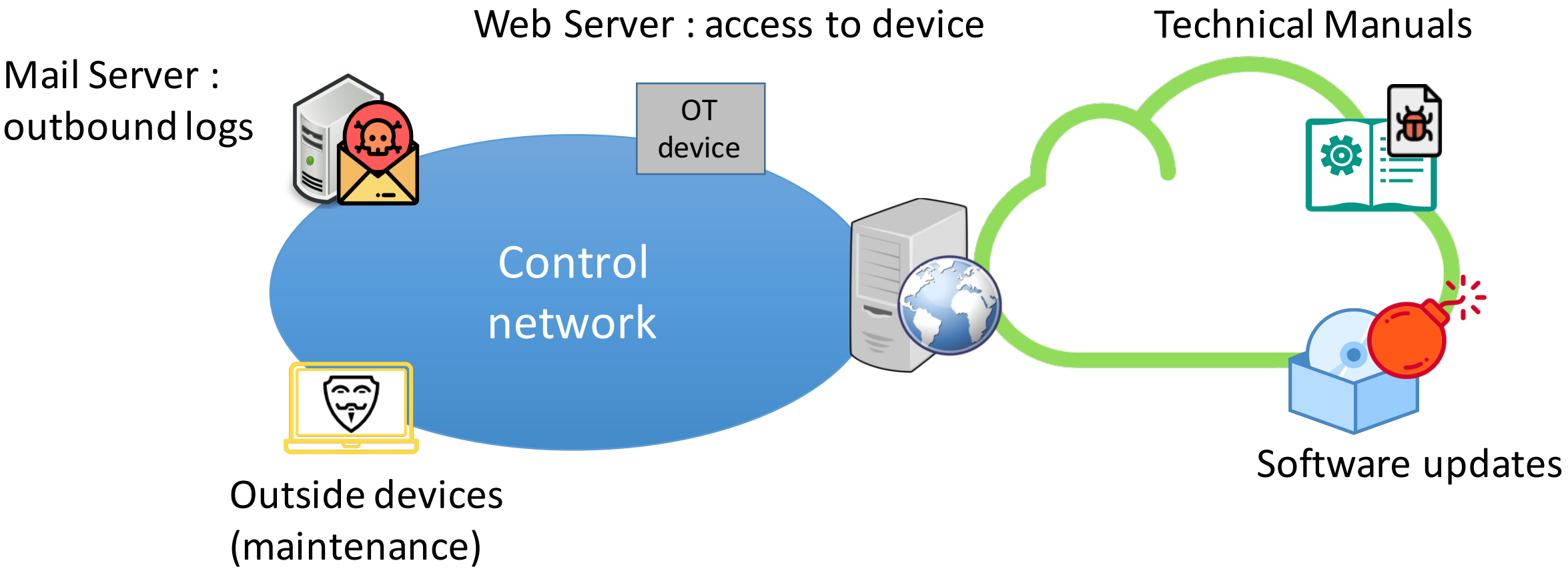
- Known best practices
- Develop "cut-out" between inbound documents/code and transfer/viewing by user
  - Example, mimecast "Targeted Threat Protection-Attach Protect" transforms Word attachments to pdf
  - "Sandboxie" brings up email inside of VM
    - Malware can't leave, but neither can anything else….
- White list applications.
  - E.g., Sophos, Carbon Block Cb
- White list outbound connections.
- Rigorous and enforced limitations on connecting to OT devices

Future threat---penetration to control and OT systems

- Assumption: Well funded adversary can engineer ways past defenses
- Assumption: “Ransom” will not be relatively small amounts of bitcoins
  - Political demands
  - Very large monetary demands
- Assumption: attacker will not have/need control, implying that threats with deadlines are likely real deadlines

Future threat---penetration to control and OT systems

- Ransomware Access to Operational Technology?



Future threat---penetration to control and OT systems

Attack Vectors

- “direct deposit” through purloined VPN access to vulnerable HMI inside ICS
- Email to host inside ICS
- Outbound Internet connection to outside unpleasantness
  - E.g., downloading software. Story about operators wanting to show images taken by drone, loading VLC
- Corrupted software update and/or corrupted configurations

Is the threat real? Yes…

Larger utilities do in fact have outbound internet access, and email servers, within the ICS

- Email typically only outbound, to transfer logs
- Outbound internet for access to reference materials

Mitigate through configuration control

Is there any good reason to have USB slots open inside ICS? SEL thinks not…

But what about

- stolen credentials bringing an attacker inside the ICS?
- Corrupted software updates or configurations?
- The threat of ransomware getting in anyway?

Raising the bar

Multifactor authentication designed to defeat key-logger theft of credentials

- Various technologies exist
- we're currently skewed in the convenience versus security tradeoff space

Verifiable provenance of digital artifacts (e.g., software, configurations)

- Signed updates/changes can verify all modifications
  - Multiple signers makes it harder for attacker to fool system with stolen private key

When ransomware strikes anyway….

- Research underway to virtualize control systems
- Core idea---if a VM *might be* compromised, wipe it and bring in copy of gold version
- Challenges
  - How can this be done without interrupting service?
  - How can you ensure that the gold version is not in fact pyrite?
  - How can one do on-line state data check-pointing that is
    - Cost effective
    - Safe from being locked by ransomware?
  - What's involved in virtualizing devices touching the physical system, e.g. PLCs?

Conclusions

The Good News

- Good computer hygiene and known technologies can lengthen the attack chain required to place ransomware inside of an ICS

The Bad News

- Increasing resiliency comes at a cost, and the incentive structure for doing that isn't clear

Open Questions and Future Work

- Where's the sweet spot for ruggedized authentication and provenance of digital artifacts?
- How can one approach virtualization of PLCs and other specialty devices without impacting real-time requirements?
- Can one quickly swap out potentially compromised systems with minimal impact on operations?