



# Industrial Network Security

California Department of Transportation, District 2  
Jeremiah Pearce, P.E. – ITS Engineer  
[Jeremiah.Pearce@dot.ca.gov](mailto:Jeremiah.Pearce@dot.ca.gov)

2017 Western States Rural Transportation Technology  
Implementers Forum – Yreka, CA

# Industrial Network Security

- First What is an Industrial Network and what sets it apart from an administrative network?
  - Loosely defined an industrial network is a machine-to-machine, process control network environment
  - This is different from an administrative network which has many unique users running varying applications.
- Industrial Networking has been a growing market for years now
- Examples include, power plant, mining, rail, manufacturing, transportation management, etc.

# Industrial Network Security

- Why do we need to worry about Network Security?



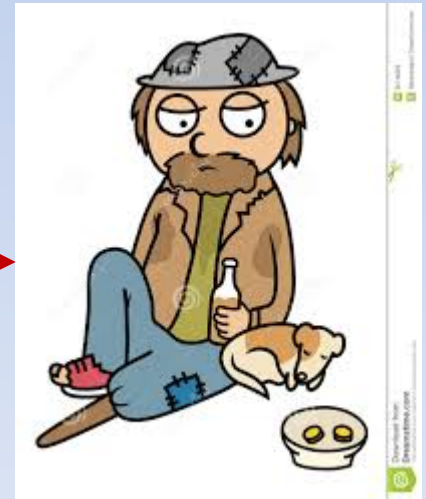
**Target**

**Interaction  
varies**



**Attacker**

**Compromised machine results in  
stolen sensitive information**



**Result**

# **Administrative Network Hack Example (Extreme)**

# Industrial Network Security

- Why do we need to worry about Network Security?
- What happens when an industrial network is not secure?



**Interaction  
varies**

**Attacker**

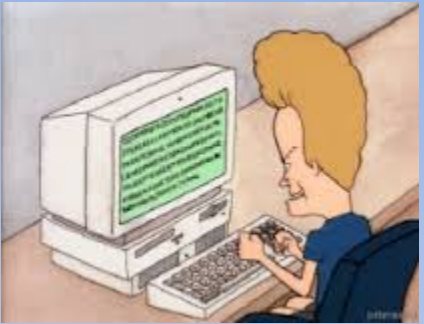
**Target**

**Compromised machine  
Results in loss of control**

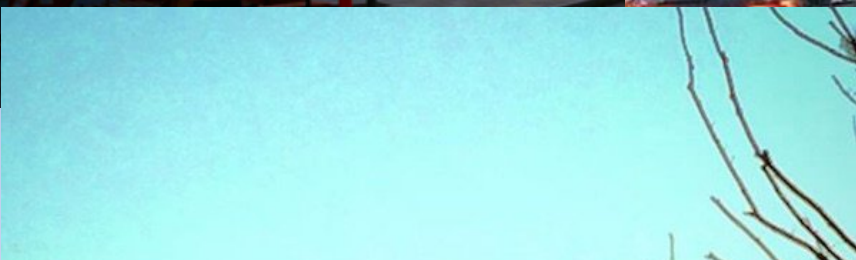


**Industrial Network Hack  
Example (Extreme)**

**Result**



**Attacker**



**TMS Network Hack  
Example Typical**



**Interaction  
varies**

**Attacker**

**Target**

**Compromised machine  
Results in loss of control**



**TMS Network Hack  
Example (Extreme)**

**Result**



# Industrial Network Security

- How do these networks get compromised?
  - Depends on a number of factors
    - Configuration
    - Physical security
    - Network topology
    - Or other methods
  - There's always a way in...

# Industrial Network Security

- Recent Industrial Networking security issues
  - RUGGEDCOM authentication bypass issue - 2013
  - RUGGEDCOM switch VLAN routing feature - 2015
  - Moxa multiple vulnerabilities - 2016
- Industrial Network security is unique in two ways,
  - Culture. Products are specialized and don't normally go through the same amount of scrutiny traditional IT hardware and software products experience
  - Industrial Network security objective prioritization
    - Availability
    - Integrity
    - Confidentiality

# Industrial Network Security

- What do we do about security, how do we implement it?
  - First, define and prioritize your security objectives
  - Second, define your known vulnerabilities
  - Third, define what steps are being taken to mitigate the vulnerabilities (sometimes the vulnerability is an acceptable risk)
- This is known as a Security Policy and is a formal written document maintained by the network manager

# Industrial Network Security

- Other issues to note...
- Balancing security with network availability and data integrity is the challenge with Industrial Networking
- Security feature availability is an issue with the industry
- After implementation there will likely be some risks, a tradeoff between implementation cost, the purpose of the network (what is it's function – our network doesn't have sensitive data so we don't encrypt links), etc.
- Embedded Linux device security - Shell Shock, etc.

# District 2 FEN Security

- Review of the District 2 Field Element Network (FEN)
  - “Field Element Network Design for a Rural Transportation Management Center, Parts One and Two” Ian Turnbull and Jeremiah Pearce, June 2012

[http://www.westernstatesforum.org/Documents/2012/presentations/CaltransD2\\_Turnbull\\_FINAL\\_FEN-TMCPrequel.pdf](http://www.westernstatesforum.org/Documents/2012/presentations/CaltransD2_Turnbull_FINAL_FEN-TMCPrequel.pdf)

[http://www.westernstatesforum.org/Documents/2012/presentations/CaltransD2\\_Pearce\\_Final2\\_FEN\\_TMC\\_Part2.pdf](http://www.westernstatesforum.org/Documents/2012/presentations/CaltransD2_Pearce_Final2_FEN_TMC_Part2.pdf)

# District 2 FEN Security

- Review of the District 2 Field Element Network (FEN)
  - “The Field Element Communications End Game - From POTS to Licensed Microwave” Jeremiah Pearce, June 2014

[http://www.westernstatesforum.org/Documents/2014/presentations/CaltransD2\\_Pearce\\_FINALb\\_FieldElementComm\\_min.pdf](http://www.westernstatesforum.org/Documents/2014/presentations/CaltransD2_Pearce_FINALb_FieldElementComm_min.pdf)

# References

- Common Cybersecurity Vulnerabilities in Industrial Control Systems. (2011, May). Retrieved from [https://ics-cert.us-cert.gov/sites/default/files/recommended\\_practices/DHS\\_Common\\_Cybersecurity\\_Vulnerabilities\\_ICS\\_2010.pdf](https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf)
- Moxa Nport Device Vulnerabilities. (2017, March 21). Retrieved from <https://ics-cert.us-cert.gov/advisories/ICSA-16-336-02>
- RuggedCom ROS Multiple Vulnerabilities. (2013, December 18). Retrieved from <https://ics-cert.us-cert.gov/advisories/ICSA-13-340-01>

# References

- Siemens RUGGEDCOM ROS IP Forwarding Vulnerability. (2015, September 01). Retrieved from <https://ics-cert.us-cert.gov/advisories/ICSA-15-244-01>
- Machenzie, H. (2012, October 31). SCADA Security Basics: Why Industrial Networks are Different than IT Networks. Retrieved from <https://www.tofinosecurity.com/blog/scada-security-basics-why-industrial-networks-are-different-it-networks>
- Bayuk, J. (2009, June 16). How to Write an Information Security Policy. Retrieved from <http://www.csoonline.com/article/2124114/it-strategy/strategic-planning-erm-how-to-write-an-information-security-policy.html>



# Questions

