Why (Control System) Cyber-Security sucks...

Stephane Armanet (ESS), Kathryn Baker (STFC), Lisa Belk (LLNL), Mark Heron (STFC), James Jamilkowski (BNL), Stefan Lüders (CERN), Maurizio Montis (INFN), Remy Mudingay (ESS), Igor Oya (CTA), and Karen White (ORNL)
A big "THANK YOU" to all presenters, the participants and the ICALPECS program committee & staff!

Summary

On August 14, attackers published a series of rest-client versions from 1.6.10 to 1.6.13 using the credentials of a rest-client maintainer whose RubyGems.org account was compromised. The affected versions were downloaded a small number of times (~1000).

On August 19, @juskoljo observed the malicious gem version and created this issue. Later that day, the RubyGems security team yanked the offending gem version and locked the affected maintainer's account.
The Consequences

- Vulnerabilities in our control software could create safety risks
  - E.g. point the mirrors to burn the bushes

Super Computers Under Siege!

- Bamboo-zled in March 2017

RAW Paste Data

```xml
<MLT> i've had my IP blacklisted by an intrusion prevention system. Other than that, it's fine :P
<sc0rp> so what kind of sites will be vulnerable to this exploit?
<MLT> many - i've noticed a lot of high-profile sites with .gov, .mil, and .int TLD's are running MS SharePoint
<MLT> here are a few large sites which are currently vulnerable:
<MLT> http://cubai.en/Lists/Articles/DispForm.aspx?ID=127198
<MLT> http://calshare.berkeley.edu/Lists/KB/DispForm.aspx?ID=1276
<MLT> http://marines.mil/unit/mcscg/Pages/Forms/DispForm.aspx?ID=12761
<MLT> http://www.shipping.nato.int/Lists/AlertsReplace/DispForm.aspx?ID=127217
<sc0rp> nice
<MLT> using the exploit on CERN would be win, hacking the people who created the internet :P
<sc0rp> hahah
```
Main action items

- Set-up cyber governance
  - Planning
- Establish assets
- Build an assessment
  - Consolidate
  - Patch management
  - Malware
  - System hardening
- Architecture
  - Network
- Prepare an Action Plan
  - Aim for more
- Set up logging
- IT/OT Dependencies
- Organizer vulnerabilities
- Awareness training

Findings (from the report)

- DOE sites reviewed had not always implemented security controls over selected systems as in accordance with requirements
- Some facilities did not have complete inventories of their ICS’
- Some facilities did not properly categorize the impact of their ICS’ on external systems
- Some had weaknesses in:
  - documentation of security controls
  - vulnerability management (e.g. systems not patched)
  - physical or logical access control
Patch Management

- Patches applied quickly

  - All devices go through a vetting process in a controlled environment to mitigate the risk
    - Sniff for undesirable traffic
    - Scan for unacceptable vulnerabilities
    - Explicit operating procedure reinforces the vetting requirement, backed up by network monitoring

- Removed from devices not supported (still receiving)

- Vulnerability Management
Procedures for Production Deployment
• We don’t often make use of public repos for acquiring software, though code in the Open Source domain seems less of a concern

...and for Importing Remote Code
Remote Monitoring vs. Control

- We’ve converted from using RSA tokens to a competing Two-Factor Authentication service.
- No significant issues were encountered during or after the transition process.
Why (CS)² really sucks!