CTSC

CENTER FOR TRUSTWORTHY
SCIENTIFIC CYBERINFRASTRUCTURE

The NSF Cybersecurity Center of Excellence

Cybersecurity for the Modern Science Gateway

Von Welch and Mark Krenz

SGCI Webinar

February 14th, 2018

Science Gateways Cybersecurity
Three Key Aspects

1. Secure Software Development and Engineering
2. Identity and Access Control Management
3. Operational Cybersecurity

Science Gateways Cybersecurity
Three Key Goals

1. Maintain the trust of your resource providers
2. Maintain the trust of your community
3. Protect, as appropriate, the confidentiality, integrity, and availability of your key assets.

A Quick Overview of Resources…

"Best practices for science gateway security include the standard recommendations for any online service, plus science gateway specific concerns"

Science Gateway Security Recommendations; Basney, Welch; 2013
http://www.ncsa.illinois.edu/People/jbasney/201309-gwsec.pdf

CIS Top 20

- **https://www.cisecurity.org/controls/**
- Eliminates majority of organizations vulnerabilities
- Overview of top 5
  - Inventory of Authorized and Unauthorized Devices
  - Inventory of Authorized and Unauthorized Software
  - Secure Configurations for Hardware and Software
  - Continuous Vulnerability Assessment and Remediation
  - Controlled Use of Administrative Privileges

CIS Top 20

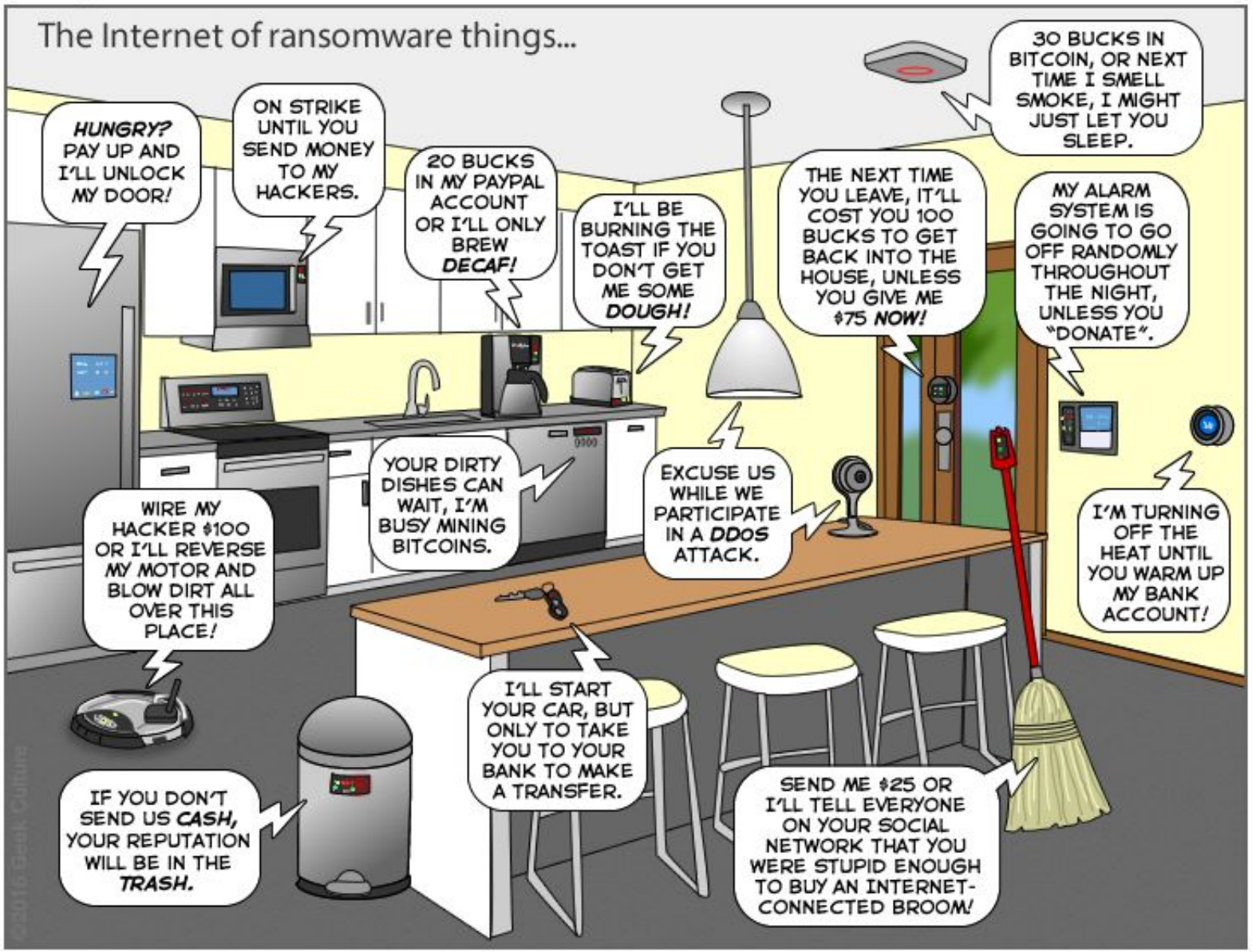
https://www.cisecurity.org/controls/

Inventory of Authorized and Unauthorized Devices

Source: Shutterstock

- Determine business needs for hardware
- Write/enforce policy
- DHCP Logs and Network scans to detect new hosts

CTSC



Source: http://www.geekculture.com/joyoftech/joyarchives/2340.html

CIS Top 20

https://www.cisecurity.org/controls/

Inventory of Authorized and Unauthorized Software

- Determine need for tasks
- Write/enforce policy
- Run a tight ship
- Use isolated system to evaluate new software
- Removed unneeded software from systems

CIS Top 20

https://www.cisecurity.org/controls/

Secure Configurations for Hardware and Software

- OS and software security hardening guide (How to secure *X*)
- Isolate functionality if possible

CIS Top 20

https://www.cisecurity.org/controls/

Continuous Vulnerability Assessment and Remediation

- Subscribe to notifications for software you use
- Subscribe to general security notification lists
  - Bugtraq
    http://seclists.org/bugtraq/
  - CTSC Cyberinfrastructure vulnerability list
    https://list.iu.edu/sympa/info/cv-announce-l
- Review system logs for attacks
- Scan your network for vulnerable software
  - OpenVAS
  - ssllabs.com

CIS Top 20

https://www.cisecurity.org/controls/

Controlled Use of Administrative Privileges

- More serious exploits possible
- Don't be admin all the time
- Use sudo on Unix/Linux
- Restrict access to administrative accounts
  - Very strong password or disable login
  - Different from other passwords
  - Limit people who can access
- Dedicated user for services
- Set up two-factor auth for admin access

Secure Software Development and Engineering

NSF “CI Framework for 21st century” (CIF21)

Software must be reliable, robust, and secure; able to produce trustable and reproducible scientific results;

…

https://www.nsf.gov/pubs/2012/nsf12113/nsf12113.pdf

Software Engineering
A Required Foundation

- Repositories/Hosting
- Testing
- Static Program Analysis
- Vulnerability Management
- Release & Delivery
- Coding/Project Tools
- Documentation

"Secure Software Engineering Best Practices"

Randy Heiland and Susan Sons

http://hdl.handle.net/2022/21322

Software Engineering
Repositories/Hosting

- Version Control
  - git
  - mercurial (hg)
- Hosting providers
  - Check permissions available for dev teams.
- Proper recovery from sensitive data leaks

Software Engineering
Testing

- Unit testing
- Functional testing
- Testing the process

"Secure Software Engineering Best Practices"

Randy Heiland and Susan Sons

http://hdl.handle.net/2022/21322

Software Engineering
Static Analysis

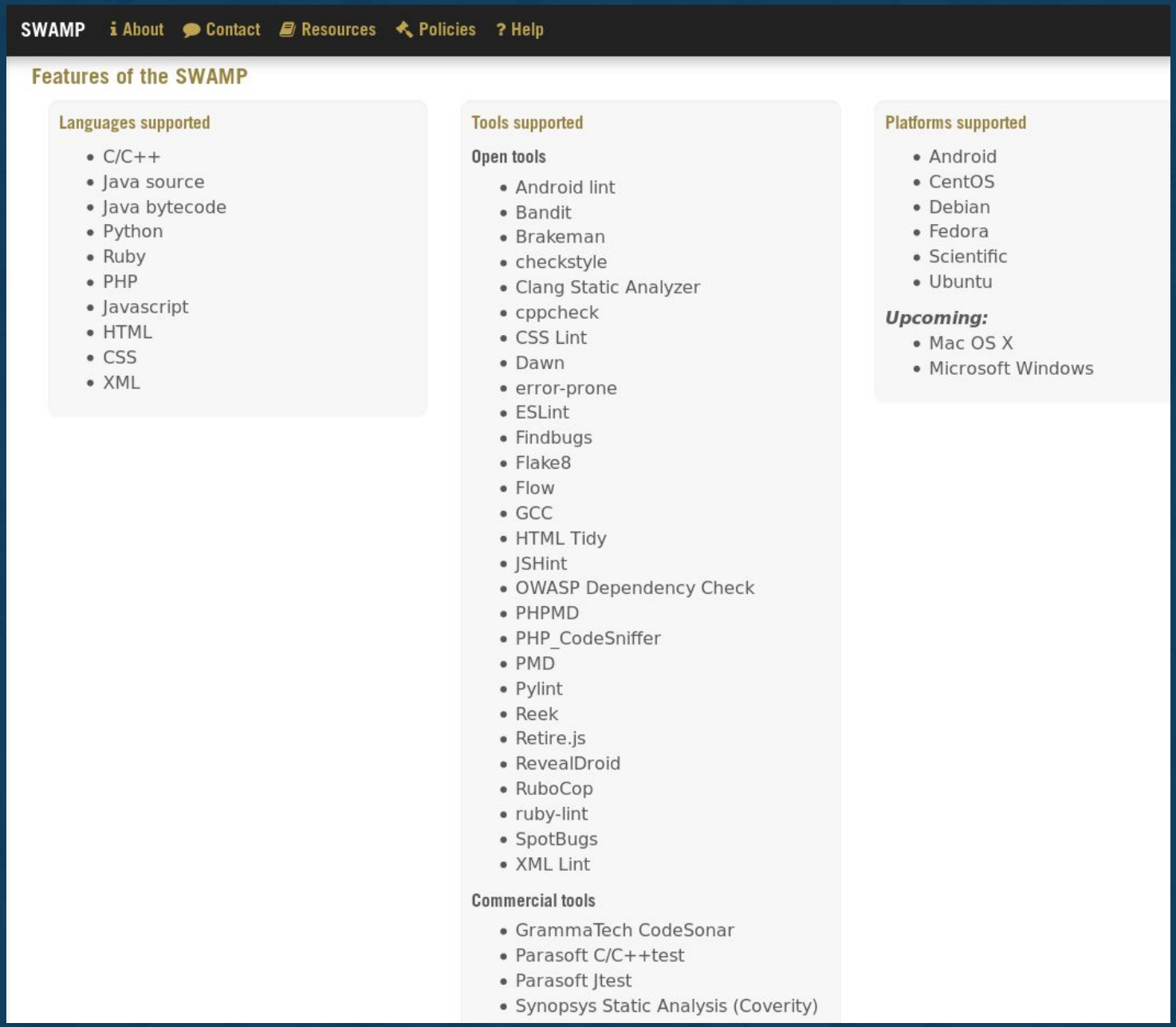
- Code analysis for weaknesses
- Automated tools
  - Tools vary by language
  - Cloud services that help

"Secure Software Engineering Best Practices"

Randy Heiland and Susan Sons

http://hdl.handle.net/2022/21322

SWAMP Features (continuousassurance.org)



CTSC

Software Engineering
Vulnerability Management

- Have a process for assessing and patching.
  - Notifying the appropriate people
  - Fixing / Patching
  - Testing the fix/patch
  - Communicating the fix
- What if you're software is open source?

"Secure Software Engineering Best Practices"

Randy Heiland and Susan Sons

http://hdl.handle.net/2022/21322

Software Engineering
Release & Delivery

- Checksums
- Cryptographic code signing

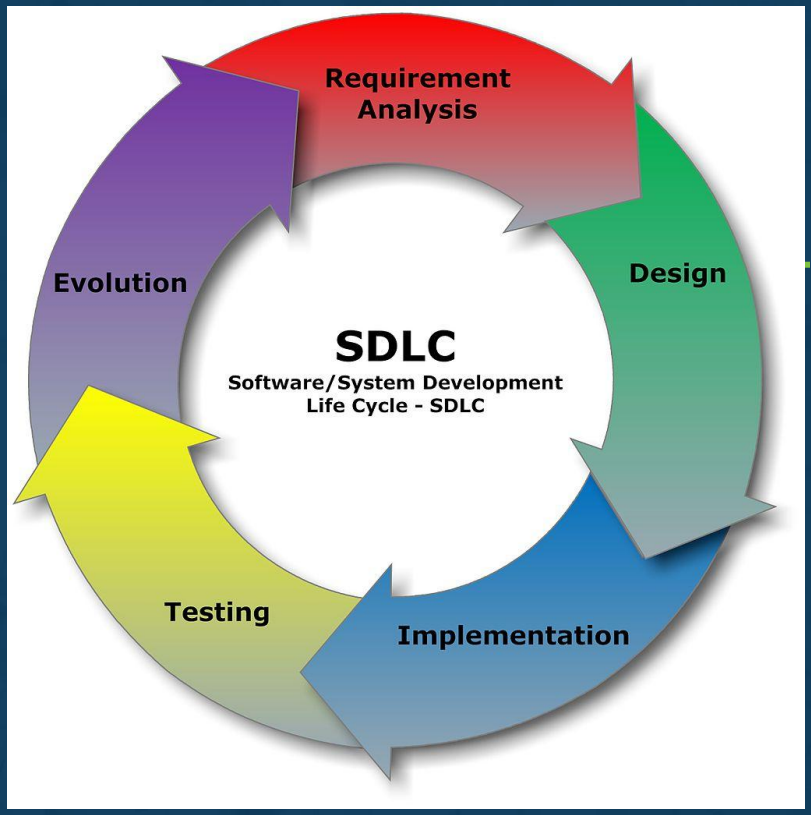
"Secure Software Engineering Best Practices"

Randy Heiland and Susan Sons

http://hdl.handle.net/2022/21322

Secure Coding

- Requirements
- Design
- Implementation
- Testing



Source: https://commons.wikimedia.org/wiki/File:SDLC_-_Software_Development_Life_Cycle.jpg

Secure Coding Practices and Automated Assessment Tools
Prof. Barton P. Miller & Prof. Elisa Heymann

http://hdl.handle.net/2022/21325

CTSC

Identity and Access Management (IAM)
Who can do what?

- Managing your community
- Different levels of access
- Who manages Groups/Communities/VOs?
- Local password or federated identity?
- User lifecycle

Federated Identity Management for Research Organizations
Jim Basney, Scott Koranda
http://hdl.handle.net/2022/21329

Facilitating Scientific Collaborations by Delegating Identity Management: Reducing Barriers & Roadmap for Incremental Implementation. Robert Cowles, Craig Jackson and Von Welch.
http://hdl.handle.net/2022/20357

Identity and Access Management (IAM)
Don't reinvent the wheel

IAM services/software serving research use cases:

- CILogon: IAM service supporting InCommon IDs
  https://cilogon.org/
- Globus Auth: OAuth-based IAM platform service
  https://docs.globus.org/api/auth/
- InCommon: trust fabric for US R&E
  https://incommon.org/
- ORCID: persistent researcher identities
  https://orcid.org/

IAM Best Practices, Training, and Resources
https://trustedci.org/iam

Full disclosure: CTSC team members have professional and personal ties to these projects.

CTSC

Cybersecurity Operations
Keeping Everything Going

- Ongoing program to manage risks
- Patching, incident detection, incident response
- Knowing your upstream software providers?
- Communications with your community and resource providers.

"Developing Cybersecurity Programs for NSF Projects"
Bob Cowles, Craig Jackson, Jim Marsteller, Susan Sons
http://hdl.handle.net/2022/21327

Other Resources

"Science Gateway Security Recommendations"
J. Basney, V. Welch
http://www.ncsa.illinois.edu/People/jbasney/201309-gwsec.pdf

"SciGaP-CTSC Engagement Summary"
Randy Heiland, Scott Koranda, Von Welch
http://hdl.handle.net/2022/20926

"CyberGIS-CTSC Engagement Final Report"
Randy Butler, Terry Fleury, Jim Marsteller, Von Welch
http://hdl.handle.net/2022/16816

"The Open Science Cyber Risk Profile (OSCRP)."
Rich LeDuc, Sean Peisert, Karen Stocks and Von Welch.
https://dx.doi.org/10.6084/m9.figshare.4584256

SGCI and CTSC are here to Help!

Email lists, webinars, training, engagements.

sciencegateways.org / trustedci.org