2014 TECHNOLOGY exchange

OCTOBER 26-30

INTERNET2® ESnet

INDIANAPOLIS, IN

Federated Security Incident Response

Tom Barton, University of Chicago
Jim Basney, NCSA
Vincente Brillault, CERN
Scott Koranda, LIGO

SPARKINGEXT

Prologue – An Example

- Criminals target University Employee Self Service (ESS) applications
  1. Phish password credentials
  2. Change bank routing information in ESS
  3. Steal paychecks
- Institutional response
  - HR/Payroll procedure
    - Create and review reports to identify suspicious activity
    - Verify with rightful account owners
    - Report credential misuse to IT Security
  - IT Security
    - Check compromised accounts against ESS access
    - Notify HR/Payroll
  - Enable Multi-Factor Authentication opt-in

- Effective
- Specific

The Problem – Identity Provider (IdP) Perspective

- Incident: credential misuse detected
  - By a Relying Party (RP)
    - Internal, external
  - By IdP security operations
    - Phishing target
    - Intrusion detection
    - Magic carpet
  - By credential owner
- Incident Response
  - Disable credential
  - Notify credential owner
  - Gather incident details
  - Notify 0 or more relying parties
  - Respond to incident reporter

- How does your organization respond?
- *How can external relying parties notify us?*
  - *Should we act on that? Or are we being gamed?*
- *Which relying parties should we notify?*
  - *How do we know which ones?*
  - *How to contact them?*
  - *Why should they act on that?*
  - *Why should we be willing to tell them?*

The Problem – Relying Party (RP) Perspective

- Incident: credential misuse detected
  - By RP security operations
  - By RP resource operator
  - By peer RP operator (VO)
  - By credential IdP operator
  - By credential owner
- Incident Response
  - External credential?
    - Disable credential access
    - Notify IdP
  - Local credential?
    - Disable credential
  - Notify credential owner
  - Gather incident details
  - Notify 0 or more peer RPs
  - Respond to incident reporter

- *How can we notify external IdPs?*
- *How can external IdPs notify us?*
  - *How can they contact us?*
  - *Do they know that we want to know?*
  - *Which credentials should they notify us about?*
  - *Why should they trust us with that information?*
  - *Or maybe it's not that important to us, depending on our risk profile*

Dimensions of the Problem

- Scale: Incident Response Diameter
  - Same organization
  - Small group of affiliated organizations
  - Unaffiliated organizations
- Direction
  - Relying Party initiates incident response
  - Identity Provider initiates incident response
- Scope: Incident Types
- IdP Context: Ability and Accountability
  - Operated by and for a single organization
  - Service contracted by multiple organizations
  - Service provided to anyone

Roots in Research Cyberinfrastructure

- Need to enable access for increasing user populations makes federated identity approaches look attractive
- Except for what they still lack
  - 100% coverage of Universities & Colleges
  - Federated authentication for non-browser use cases
  - Authentication assurance and strong authentication credentials
  - Federated security incident response

- "A Roadmap for Using NSF Cyberinfrastructure with InCommon", Indiana University, 2011
  - NSF CI projects are frequently, due to their use of sensitive resources and/or data, more interested in computer security incident response than are typical service providers
  - Configure IdP auditing to support debugging, security incident response and gathering usage statistics

Roots in Research Cyberinfrastructure

- "Federated Identity Management for Research Collaborations", CERN, August 2013
  - **Traceability.** Identifying the cause of any security incident is essential for containment of its impact and to help prevent re-occurrence. The audit trail needs to include the federated IdPs. Appropriate **Security Incident Response** policies and procedures are required which need to include all IdPs and SPs.

- GRID-SEC
  - Hierarchical coordination of CSIRTs across EU grid infrastructures

- "Federated Security Incident Response Policy", CIC, 2011
  - Suggested Federated Security Incident Response Policy and implementation procedures for adoption by InCommon Federation
  - Fractional implementation

Lessons learned from the Grids

- EGI & WLCG:
  - Collaboration of a large number of site in many countries
  - Users from all around the world, split in VOs
  - Resource: CPU time, data storage
- Central CSIRT team coordinating incident response
- Most seen incidents (spreading across the grid):
  - Acceptable Use Policy violation
  - Unpatched & vulnerable servers
  - Compromised host stealing credentials

Typical community incident at EGI/WLCG

- Acceptable Use Policy violation (e.g. Bitcoin mining):
  - User (VO X) submit several mining jobs to different sites
  - Site A detects it:
    - User locally suspended
    - Jobs frozen/killed
    - Reports to central CSIRT
  - Central CSIRT (e.g. EGI):
    - Investigate incidents (enough proof?)
    - Suspend user centrally
    - Identify submission point and other sites potentially impacted
    - Broadcast to sites B/C/D and continue investigating
    - Coordination with VO X
  - Site B/C/D:
    - Freeze/Kill jobs
  - VO X:
    - Check submission systems
    - Accounting/user banning/legal actions …

Typical community incidents at EGI/WLCG II

- Outdated & Vulnerable servers:
  - CSIRT probes the grid
  - Vulnerable sites are notified, potentially excluded from the grid
- Compromised host stealing credentials
  - Most of the time close to the Grid, not inside
  - Stealing standard SSH credential:
    - Using known_hosts/history to try to spread
    - Spread to other sites/institutes (shared users)
    - Mostly automated script with (old) escalation attacks
  - (Stealing Grid credentials, x509: never used (too complex))
  - Compromise host or malicious connections detected
  - CSIRT: Broadcast compromised or malicious IP & username
  - Sites: check activity from IP & username, report back

Inter-federation incident simulation

- Policy (which one?) violation, e.g. copyright violation?:
  - User (**IdP X**) stores/distributes copyrighted material
  - **SP A** detects it/receive a DMCA notice:
    - User locally suspended?
    - Data removed?
    - Reports to **IdP X?**
  - **IdP X** (where the user came from):
    - Notified?
    - Can it get enough proof? Is it a real incident?
    - Forward to other **SPs**?
  - **SP B/C/D** (also abused):
    - Get notified by **IdP X** or DMCA or never?
- Can we contain it?

Lots of Technologies

- STIX, CYBOX, MAEC, TAXII @ Mitre
- Fordrop
- https://confyrm.com
- IODEF
- …

- That's not a problem

Latest Work: Sir-T-Fi

- Security Incident Response Trust for Federated Identity
- EU & US research CI security people, some R&E Federations
- < 6 months
- First problem: promote trust by IdP & RP organizations self-asserting level of maturity in each of several areas of practice
  - "A Trust Framework for Security Collaboration among Infrastructures", draft 0.6
- Second problem: process and tools for federated incident response

Latest work: Fir-US

- Federated Incident Response – US
  - Identity Management and Security leaders at several US Universities
  - Kim Milford @ REN-ISAC
  - Ann West @ InCommon
- Form consensus on federated incident response use cases and language to describe them
- Provide feedback on Sir-T-Fi draft trust framework
- < 1 month!

Latest work: ACAMP

- Advance CAMP: open space/unconference event
- Federated security incident response break-outs
- < 1 week
- Trust for incident response always builds on existing relationships
- Security incident response is another trust framework, orthogonal to other trust frameworks
- Scale
  - XMPP Operators have addressed this
  - REFEDS can devise and promote a common approach for ~50 R&E Federations to adopt
    - Sir-T-Fi document provides a model
  - REN-ISAC in US and TF-CSIRT in EU
- Direction
  - Start with Relying Party initiated incident response
- Scope
  - Start with credential misuse, including sharing of information needed to contain and remediate the overall incident

Next Steps

- Sir-T-Fi meeting Friday @ IU
  - Work on Trust Framework draft
  - Factor in ACAMP discussions
- Fir-US feedback on the above
- Tell us what you think
- Join us! Contact
  - Kim Milford <kmilford@ren-isac.net>
  - Ann West <awest@internet2.edu>
  - Tom Barton tbarton@uchicago.edu
  - Subscribe to Sir-T-Fi list: http://www.terena.org/mailinglists.php

Epilogue – Multi-Factor Authentication (MFA)

- Why not just do MFA so accounts won't be stolen any more? Then no need for federated incident response, right?
- ***Please implement MFA!*** It will help a lot!
- There have already been credential misuse incidents in research cyber infrastructure with MFA
- We still must figure out how to work together on incidents, even when we haven't already been introduced

2014 TECHNOLOGY exchange

OCTOBER 26-30

INDIANAPOLIS, IN

Federated Security Incident Response

Fir-US contact info:

Kim Milford <kmilford@ren-isac.net>
Ann West <awest@internet2.edu>
Tom Barton <tbarton@uchicago.edu>

Tom Barton

CISO, University of Chicago