Sirtfi for Security Incidents in a Federated Context

InCommon Assurance Webinar
Wednesday, May 4, 2016

Tom Barton, University of Chicago and Internet2

The Whole Elephant

- Recall why compromises on campus should be reported to the campus IT security team
- They determine the nature and footprint of the overall intrusion and manage a response to it
- If not reported, more damage is done before a coordinated response can be mounted

- We're now part of a global interfederation
- How can the overall intrusion be determined and a coordinated response mounted?

What, When, Who, How

- Suppose campus IT security has an incident
- When should it be reported beyond the campus?
- To whom, what details should be shared, and how?

- Not always – some threats each campus must handle alone
- No national or global security response team to escalate to
- So what *can* and *should* we do, what barriers to that?

Sirtfi's Role in Sharing Beyond Campus

- Several ways campus IT security can share now (US)
  - REN-ISAC
  - FBI, other Feds
  - Peers in some consortia, e.g., CIC
  - Each with their own protocols – when, what, how
- Sirtfi: focus on threats that pivot through federation
  - Compromised accounts, in particular
  - How and when to contact which federated peers
  - What to expect when you do
  - Maintaining accurate contact information

Sirtfi Working Group

- Supported by REFEDS and AARC
  - Security people from EU & US research cyber infrastructures
  - R&E Federation and campus representatives
  - AARC-funded staff support at CERN
- Roots in research CI community
  - Need for federated incident response since unauthorized use can be very bad!
  - Integrity of research data: careers, science, public policy
  - Availability of specialized resources for intended purpose
  - Research CI makes amazing DoS canons

What Sirtfi WG is Shooting For

- Almost all entities in R&E Fed metadata have security contact info
- As many entities in R&E Fed metadata as possible meet Sirtfi v1 Trust Framework
  - Trusted to do their part in managing an incident and handle shared info properly
- Method for SPs to register need to know about compromises to accounts that access them
- Tool to let IdP orgs notify registered SPs of compromised accounts that recently accessed them

Sirtfi Elements

- Done
  - Trust framework specification (Sirtfi v1.0)
  - Registration of Sirtfi with IANA as an assurance profile (like Bronze & Silver)
  - Specification of SAML metadata extension for security contact information
- To Do
  - Specification of registration and maintenance practices for Sirtfi assurance metadata entity attribute
  - Guidance and promotional materials for R&E Fed Ops and Federation Members
  - Tools

Sirtfi v1 Assurance Profile

- Practices and attributes of organizations to coordinate security incident response across federations
- Low bar statements about
  - Operational Security (patching, vulnerability management, intrusion detection, user access management)
  - Incident Response (contact info, willing to respond, Traffic Light Protocol)
  - Traceability (logs available to aid Incident Response)
  - Participant Responsibilities (AUP exists)
- Queued for v2: IdP obligation to notify compromised accounts to “registered” SPs

Metadata Specs & Implementation

- Specs are done. Next up …
- Normative, guidance and promotional documentation
  - How R&E Fed Ops register & maintain Sirtfi assurance tag
  - Guidance on maintaining and testing security contact info
  - Guidance to Federation Members
- Partner with early adopters & promote!
  - R&E Feds (SurfNET & InCommon are stepping up)
  - Initial Federation Members (Your Name Here!!)

SPs That Need to Know

- Registration DB to enable automation of authorized IdP notifications
  - Perhaps with another metadata entity attribute
- What requirements or obligations should pertain?
- Start out with Research & Scholarship SPs?

Tooling to Support IdP Notification

- Premise: campus IT security becomes aware of compromise of some of its accounts
- Dump account list into an interface, get back which registered SPs each account accessed in last interval
- Press button to authorize notification of security contact at each registered SP of compromised accounts that accessed them during last interval
- Key design choices
  - Parse IdP logs vs maintain an out-board IdP activity DB
  - Interval length

Questions & Comments?

- What do you think the biggest barriers will be?
- Does your org already have security contact info in InCommon metadata?
- Will your org likely attest to Sirtfi v1?
- Would your org's security team be ok with using that IdP notification tool?
- What else might IT security, or any other party, want to know before being ok to authorize directed notification of access by compromised accounts?

Appendix: Sirtfi v1 Operational Security

[OS1] Security patches in operating system and application software are applied in a timely manner.

[OS2] A process is used to manage vulnerabilities in software operated by the organisation.

[OS3] Mechanisms are deployed to detect possible intrusions and protect information systems from significant and immediate threats

[OS4] A user's access rights can be suspended, modified or terminated in a timely manner.

[OS5] Users and Service Owners (as defined by ITIL [ITIL]) within the organisation can be contacted.

[OS6] A security incident response capability exists within the organisation with sufficient authority to mitigate, contain the spread of, and remediate the effects of a security incident.

Appendix: Sirtfi v1 Incident Response

[IR1] Provide security incident response contact information as may be requested by an R&E federation to which your organization belongs.

[IR2] Respond to requests for assistance with a security incident from other organisations participating in the Sirtfi trust framework in a timely manner.

[IR3] Be able and willing to collaborate in the management of a security incident with affected organisations that participate in the Sirtfi trust framework.

[IR4] Follow security incident response procedures established for the organisation.

[IR5] Respect user privacy as determined by the organization's policies or legal counsel.

[IR6] Respect and use the Traffic Light Protocol [TLP] information disclosure policy.

Appendix: Sirtfi v1 Traceability

[TR1] Relevant system generated information, including accurate timestamps and identifiers of system components and actors, are retained and available for use in security incident response procedures.

[TR2] Information attested to in [TR1] is retained in conformance with the organisation's security incident response policy or practices.

Appendix: Sirtfi v1 Participant Responsibilities

[PR1] The participant has an Acceptable Use Policy (AUP).

[PR2] There is a process to ensure that all users are aware of and accept the requirement to abide by the AUP, for example during a registration or renewal process.

2016 Internet2 Global Summit in Chicago

InCommon Baseline Practices BoF

Wednesday, May 18, 2016 – 7:30 – 8:30 am

Please join us!

InCommon Assurance Wiki

https://spaces.internet2.edu/display/InCAssurance/InCommon+Assurance+Program