Tues 2pm Monterey

Scribing Template -Tues., Nov 12, 2013 at 2pm - Monterey Room

TOPIC: Federated Security Incident Response (FSIR)

CONVENER: Scott Koranda (UW-Milwaukee / LIGO) and Bob Cowles (Indiana University / CACR)

SCRIBE: Tom Scavo

# of ATTENDEES: unknown

MAIN ISSUES DISCUSSED:

ACTIVITIES GOING FORWARD / NEXT STEPS:

If slides are used in the session, please ask presenters to convert their slides to PDF and email them to acamp-info@incommon.org

Notes

- What are the barriers to IdPs participating in FSIR in an obligatory manner?
- In the grid community, here is the scenario:
    - A typical type of "incident" is a runaway process. Yes, account compromises occur but runaway processes are more common.
    - Systems are usually accessed (and compromised) via ssh.
    - Compromised systems contain X.509 credentials. Once compromised, the X.509 certificates must be revoked.
- *Use Case*: Suppose you are an IdP operator. A user account on your IdP is compromised. Would/could you contact affected SPs?
- Phishing leads to a compromised account, which is blacklisted for a time. Consider how this event might be communicated to the affected SP.
- Environments governed by the CISO and General Counsel are likely not able to participate in FSIR.
- Federated Security Incident Response is an InCommon recommended practice.
- Let's turn this around: if the RP accepts a weak assertion, the RP assumes the associated risk.
- Does FSIR include a compromised signing key at the IdP? No, since this is covered by the Silver IAP.
- At the end of the day, FSIR is about climbing the assurance ladder (Silver and above).
- Does the IdP have a "moral obligation" to participate in FSIR? Yes. Is there a legal and contractual obligation to participate? Probably not.
- Claim: The IdP is usually the first to know about a compromised account. An RP might observe "bad behavior" but an accompanying explanation of that behavior will probably not be known to the RP. In this case the RP will have to bring the bad behavior to the attention of the IdP.
- What if an IdP is contacted by an RP? Should the IdP report the incident to other RPs?
- Responding to a compromised account is just the tip of the iceberg since a compromised account is used by the Bad Guy as a stepping stone to further, perhaps escalated, compromise.
- The lack of FSIR is a barrier to the proliferation of Federation-wide services.
- Account compromise is hardly ever black and white. For example, an intentionally shared credential should be handled differently than a stolen credential.
- A compromised account doesn't necessarily imply a compromised service.
- How do we manage risk? It's not all-or-nothing.
- How many hoops must the compromised user jump through? This needs to be handled on a case-by-case basis.
- How hard can it be to run a script on a log file to produce a list of affected RPs?
- How will the conversation around FSIR change as a result of interfederation? EU privacy laws will certainly drive the conversation in certain directions.
- In one EU federation, only one SP has *ever* reported an incident.
- Should the SP notify the user rather than the idP?
- Real event: A user believes in freedom of information and published their username and password to the world.
- We know from experience that users often send their username and password to the help desk (which of course immediately invalidates the password credential).
- How does the IdP know that a compromised account was used to access an SP?
- The obligation to participate in FSIR is tied to level of assurance. The higher the asserted LoA, the stronger the requirement to report incidents.
- Does FSIR apply to all accounts and all services? If not, which ones?
- Begin by scoping FSIR to Silver.
- How do we properly scope the problem on the SP side? Do we tag SPs with an entity attribute that says "SP that wants to be notified if an account is compromised."
- FSIR is out of scope with respect to the Assurance Program (or is it?).
- What about some kind of entity attribute on the IdP side?
- A basic question: is there an entity attribute at the IdP or the SP (or both)?
- Is FSIR per-user (just-in-time) like Bronze or Silver?
- If FSIR is opt-in, who will subscribe to it?
- Right now, SPs chase IdPs for R&S, POPs, IAPs, and now FSIR. To the SP, the value of the Federation is questionable. No one wants to take on that responsibility.
- The question of per-user vs. per-IdP is a basic question that needs to be answered.
- Per-user is hard. This has to be an agreement between an IdP and an SP (like attribute release).
- FSIR and attribute release together grate at the value proposition of the Federation.
- When will InCommon step up to the plate?
- Why doesn't this issue come up while boarding *commercial* SPs? Of course the answer is the commercial SP wants your business.
- Perhaps the commercial SP assumes a hostile environment to begin with and takes steps to protect itself from abuse.
- Story: A user uploads porn to a commercial service. The service is subsequently brought down by DoS.
- Observation: The person who can search the logs (at the IdP) is *not* the person who can notify the SP.
- Litigation avoidance is a primary motivator in this space.
- A 100% reporting requirement is untenable.
- Compare FSIR with privacy, which is hard coded into the Participation Agreement.

- What happens when the SP contacts the IdP? Does the IdP contact a bunch of other SPs? This is the critical leg of the communication.
- Suggestion: Identify the SPs that need this particular IdP behavior.