Information Security in Internet2 Trust and Identity Services

Nick Roy, Nick Lewis - Internet2
Kim Milford - REN-ISAC
Internet2 Technology Exchange 2017

INTERNET2 2017 TECHNOLOGY exchange OCTOBER 15-18 SAN FRANCISCO CA

Introductions

Kim Milford, Executive Director, REN-ISAC
Nick Lewis, Security Services Program Manager, Internet2 NET+
Nick Roy, Director of Technology and Strategy, InCommon

Several Interconnected Stories

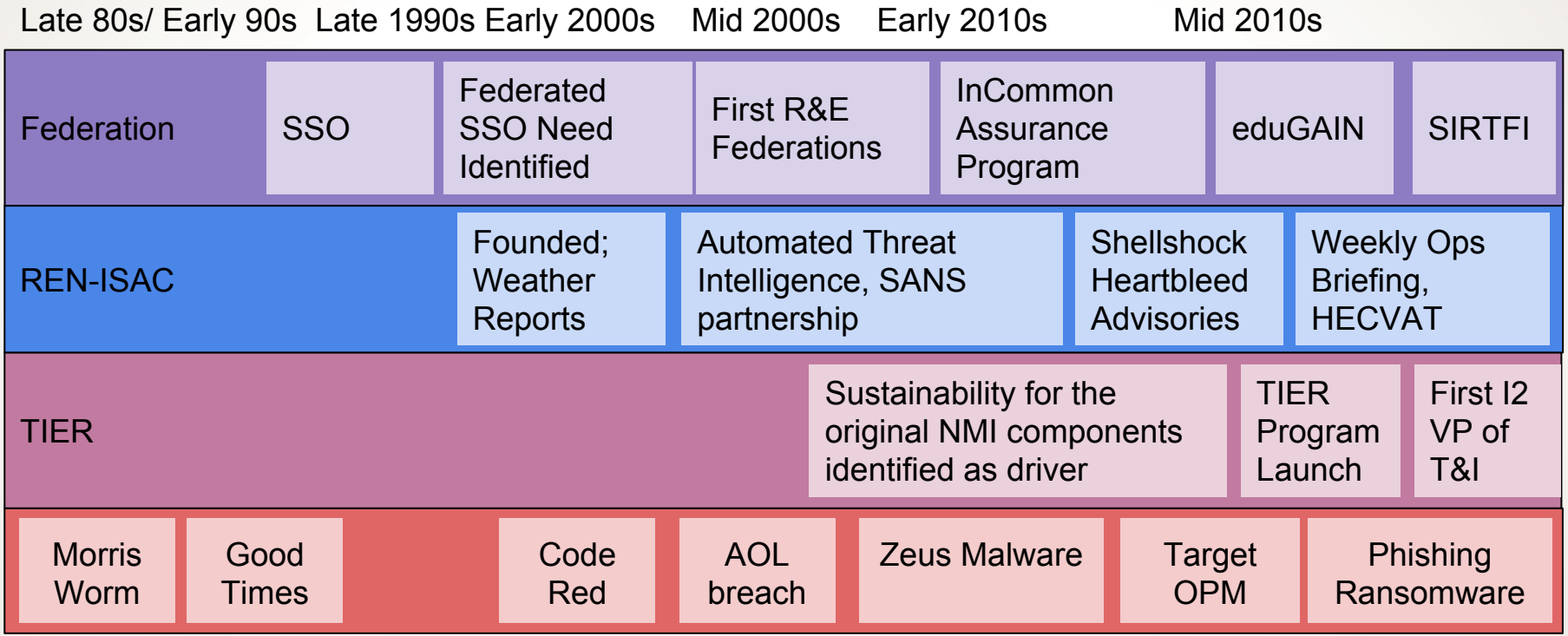
1. The rise of global trust federations based on open-development / community-sourced software and practices, and how we are addressing security in this environment
2. The sustaining model for securely developing and using that software now and into the future
3. The wider role of information security and identity practitioners in preserving and enhancing trust

The First Operational Internet2 Trust Service

InQueue - Summer, 2005 (“club Shib”)

- Very few IdPs, almost no SPs at first
- Operated as “best effort”
- Operational security was a focus from the start
  - Community working group created requirements for security, key handling, etc.

Timeline: Building Blocks for Scalable Trust



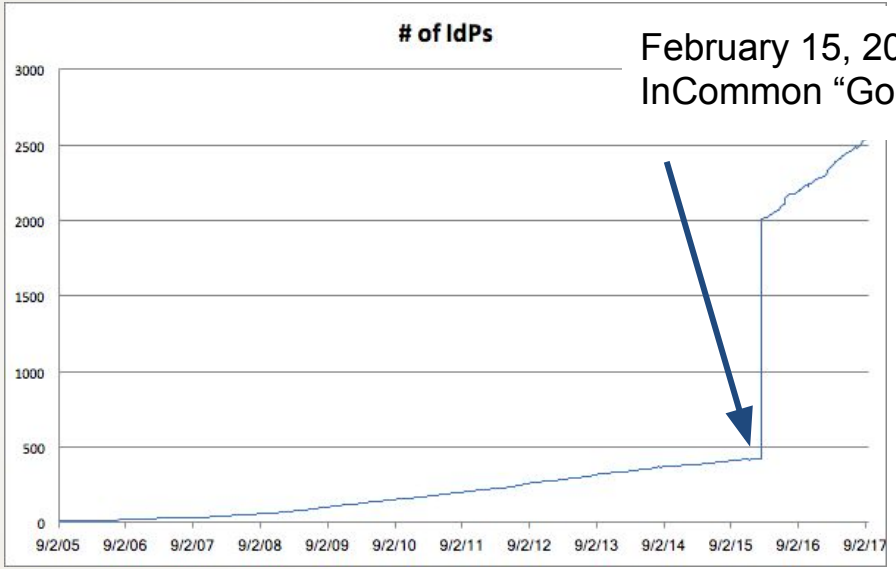
Maturation of the Federation Service: Mid-Late 2000s

- In the 2008-2010 time range, research computing groups within the federation identified a need for security incident response at federation scale
- InCommon introduced security contact information into the metadata
- Committee on Institutional Collaboration (now: Big Ten Academic Alliance) IAM working group proposed a federated incident response framework

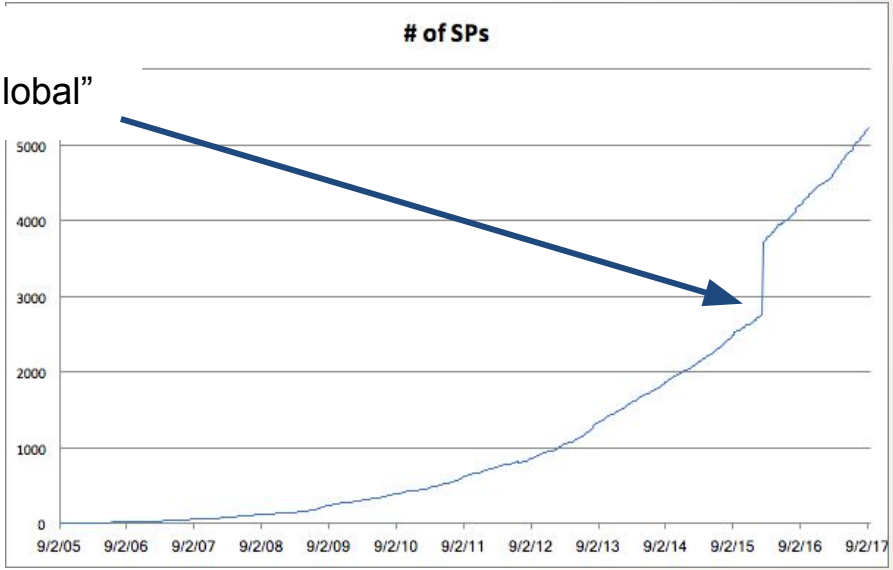
Federated Incident Response Takes Center Stage

- In 2015, InCommon conducts an operations review which highlights a need for a dedicated security function for the federation and related services
- InCommon integrates with eduGAIN, quadrupling the number of IdPs in metadata and doubling the size of metadata
- The FIM4R project and REFEDS standardize the Security Incident Response Trust Framework for Federated Identity (Sirtfi) framework, entity attribute and security contact in 2016

InCommon Growth Over Time



February 15, 2016:
InCommon "Goes Global"



2016: Internet2 Trust and Identity Services Is Formed

- Trust and Identity identified as a core focus of the Internet2 community and the Internet2 Trust and Identity Services unit is formed within Internet2. It takes over responsibility for InCommon and TIER
- Kevin Morooney is named Vice President, Internet2 Trust and Identity Services
  - Planning for increased staffing level within InCommon to support services such as SIRTFI begins
  - A Trust and Identity Security Lead position is identified as a need
  - InCommon Participation fees raised in November, 2016

Federated Incident Response Goes Into Production

InCommon publishes its production Incident Handling Framework in early 2017
Security incidents handled to date:

1. IdPs sending duplicate person identifiers
2. Delegated SP metadata administration credential spoofing attack

Incident 1: Duplicate NameIDs

- November 17, 2016
- InCommon's Incident Handling Plan is still in draft form
- We are notified that two InCommon IdPs are releasing duplicate SAML persistent nameIDs to the ORCID SP
- Coordinated incident response across two different US IdPs, one global SP based in the Dutch federation
- Both IdPs fully remediated within 24 hours from initial report of problems with each
- Both IdP problems were due to configuration errors during upgrade processes in completely unrelated federation software
- Lesson Learned: A draft incident response plan is better than none at all
- Lesson Learned: Even the simplest incident requires large amounts of coordination and staff time
- Lesson Learned: Deployment testing is critical when upgrading IdP software

Incident 2: Delegated Metadata Admin Spoofing

- August 1, 2017
- We have a production incident handling plan, but no security lead
- An InCommon Site Administrator reports the ability to access the delegated SP metadata administration interface with only a username, no password
- InCommon/Internet2 staff immediately identify the problem, apply a patch
- Root cause analysis as part of incident handling identifies multiple redundant controls in place that would prevent unauthorized SP metadata submissions
- Permanent software fix in place within 16 hours
- Lesson Learned: Mixed-mode local and federated authentication is risky and can cause security problems in a deployment
- Lesson Learned: Multiple controls around critical processes are incredibly valuable
- Lesson Learned: Log correlation capability is critical to the future of InCommon operations

Late 2017 Developments

Shannon Roddy hired as Internet2 Trust and Identity Services Security Lead
Initial Priorities:

1. Understanding existing service security and trust models
2. Conduct security reviews of T&I operational services
3. Lead security-related components of InCommon's Per-Entity Metadata project
    a. New metadata signing key generation, security, DR/BC
    b. Hardware security module requirements
    c. Secure signing environment requirements/design

Takeaways In Our First Year of Operation

1. It's still early in our experience running an information security program - we still have a lot to learn and to work towards. This will take time.
2. Even the simplest of incidents take large amounts of staff time to handle
3. Security incidents in a federated context are complex, require many people to participate in mitigation of threats - coordination is the primary time sink to date
4. We look forward to seeing the results of the security reviews and discussing them with our community-driven leadership including InCommon Steering and the Trust and Identity Services Program Advisory Group (PAG) to identify further steps in our evolution

Incident Handling Framework: Where to Learn More

Check out:

https://spaces.internet2.edu/display/InCFederation/Security+Incident+Handling

For info on the InCommon Federated Incident Handling Plan and Incident Response Reports

InCommon Community Security Activities

- Federated Multifactor Authentication
  - The ability to perform multifactor authentication in a federated context
- Baseline practices
  - Expectations for InCommon participants that all will be required to meet and the proposed processes for meeting them.
  - Focused on generally-accepted security practices and reasonably secure information and maintain user privacy
- Sirtfi
  - The Security Incident Response Trust Framework for Federated Identity (Sirtfi) aims to enable the coordination of incident response across federated organisations.
- TIER
  - TIER Security and Audit Working Group
  - Federation as a TIER component

TIER Security

- TIER Security and Audit Working Group
  - The TIER Security and Audit working group (SAWG) is charged with providing ongoing recommendations, oversight, and support of the TIER project through identification and review of security and audit standards and best practices for the TIER application suite
  - Scoping what is a campus or software development responsibility

- TIER SAWG recommendations:
  - Software Development Standards and Frameworks
  - IT Security Risk Assessment
  - Tier Product Security Testing
  - Threat Modeling

- Engagement with TIER Developers

Campus Information Security Engagement in Identity Management

- Where does the campus Infosec teams fit in this
  - IDM and federation are key components to enterprise information security programs
  - IDM and federation have many intersections with infosec, privacy, IT GRC, BCDRP, etc

- Core to managing access control across campuses and is one of the most visible aspects of information security to most of your campus.

- Auditors, Compliance, and Legal also seem to be interested in who has what access and how it's managed, which may pull information security teams into audits or other activities.

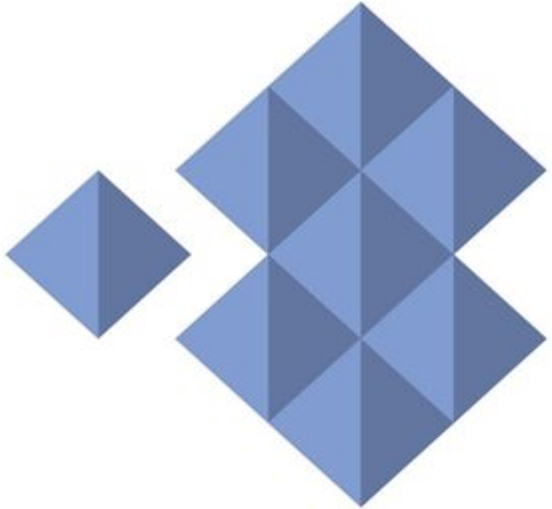
- Where can campus information security teams get involved?
  - Working groups on assurance and security

REN-ISAC, InCommon TAC and Sirtfi

- How Does REN-ISAC Fit Into All This?
- Role On The InCommon Technical Advisory Committee
- Support for the Security Incident Response Trust Framework for Federated Identity (Sirtfi)

REN-ISAC

Aid and promote cyber security operational protection and response within the higher education and research (R&E) communities.



REN-ISAC: What We See

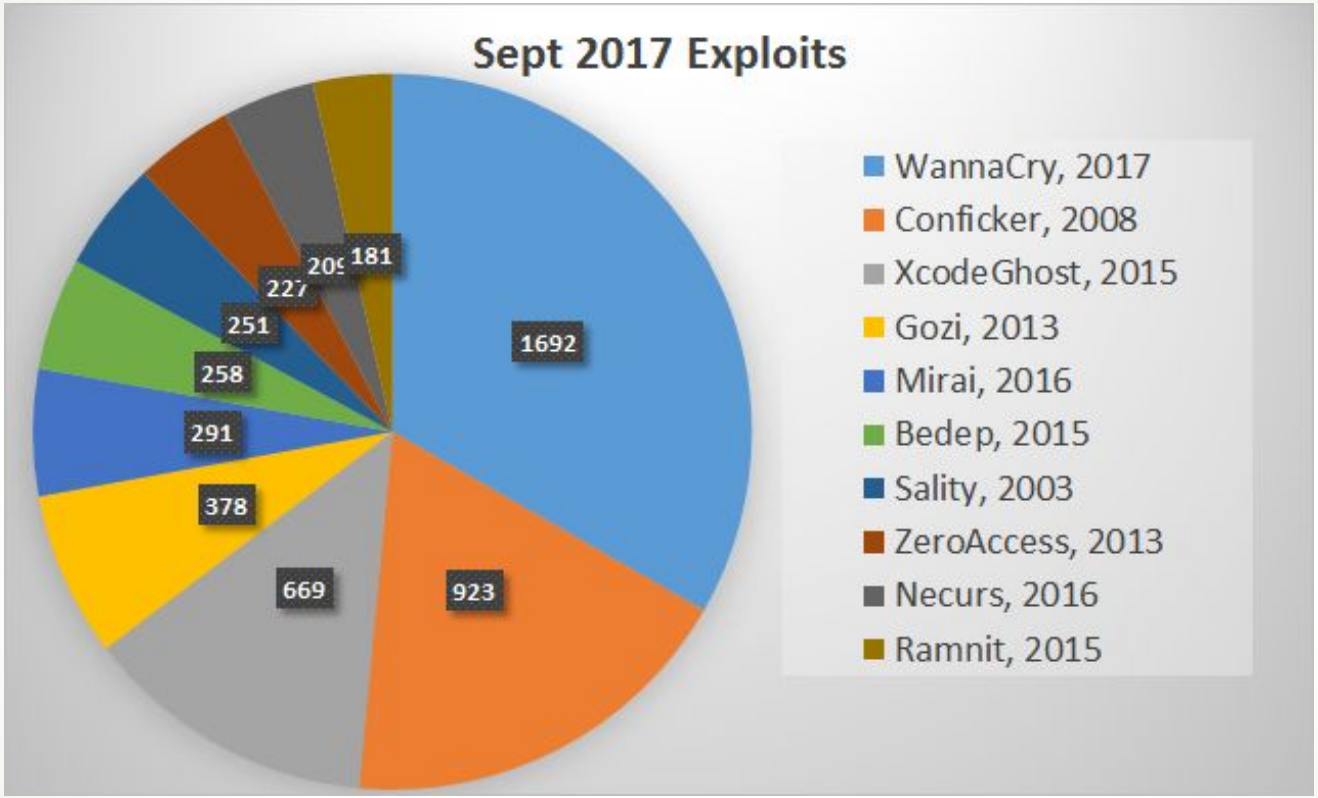
- 455 incidents with 73 confirmed data exposures
- 71% of breaches were external actors
- Motives: 45% financial; 43% espionage
- Compromised data: 56% personal; 27% secret; 8% credentials

2017 Verizon Data Breach Report

REN-ISAC: What We See

CSIRT Notifications	Q1	Q2	Q3	2017		2016 YTD Q3
Credentials	1,483	3,559	1,096	6,138		1,056,092
Compromised Machines	14,376	16,261	17,600	48,237		54,443
Open Recursive DNS Resolvers	707	357	565	1,629		2,113
Spam or Phish	118	92	93	303		314
Open Mail Relays	39	37	30	106		114
Other	70	28	14	112		51
Total	**16,793**	**20,334**	**19,398**	**56,525**		**1,113,127**

REN-ISAC: What We See



REN-ISAC: What We See

Trend1: Proliferation on successful attacks on the individual/account

Sharing is caring

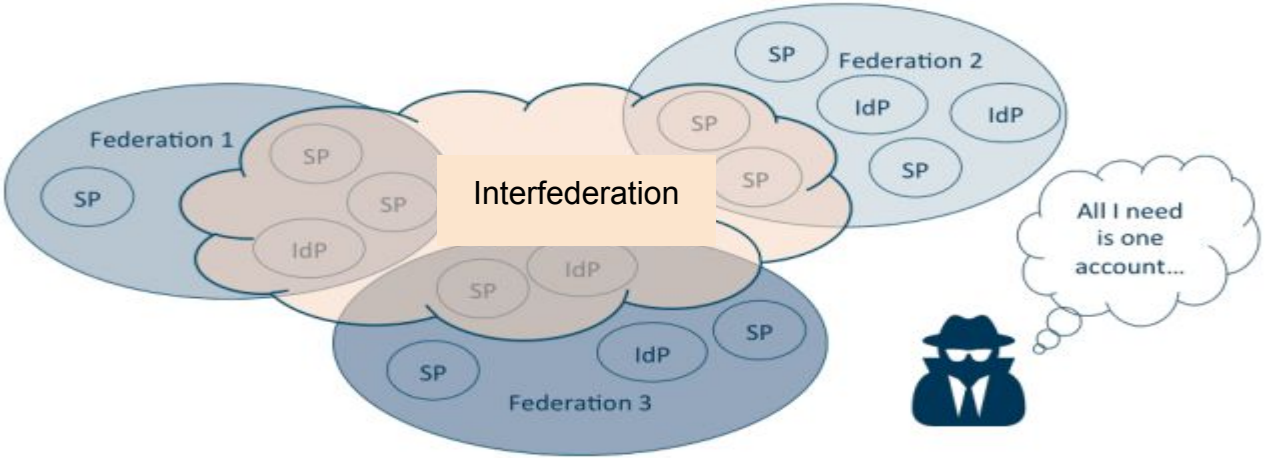
- Contact info (Sirtfi)
- Incident notifications and debrief

Enhanced and innovative identity and access management

Sirtfi

The Problem: Lack of Trust

The growth and inter-connection of federations has created a new vector of attack. One compromised account can provide access to a multitude of services across the inter-federation community.



Sirtfi

The credibility gained by asserting Sirtfi compliance opens doors within eduGAIN as organisations choose to enable authentication based on this enhanced trust.

IdPs	SPs
Gain **access** to useful services that only allow authentication from Sirtfi compliant IdPs	Gain **users** whose home organisations only allow authentication at Sirtfi compliant SPs

Guarantee an efficient and effective **response** from partner organisations during incident response

Raises the bar for operational security

REN-ISAC: What We See

Trend2: SecOps & IAM

- Originally often in same division
- Separated conceptually and organizationally
- Now coming back together

Discussion

Common Themes

1) We need a scalable combination of technology, policy and relationships to:
   a) Prevent security incidents
   b) Handle security incidents when they do happen
   c) Increase engagement with the community
2) The size and interconnectedness of the federated IAM space makes #1 even more critical
3) Identity and infosec practitioners need to have strong relationships and focus on building them even stronger - and focus on understanding each others' work and challenges

Thank You

Contact Info

Kim Milford: kmilford@ren-isac.net
Nick Lewis: nlewis@internet2.edu
Nick Roy: nroy@internet2.edu