Security Events
RISC

Marius Scurtescu, Google

IETF97 Seoul

November 2016

What is RISC

Risk and Incident Sharing and Coordination

Share information about important security events in order to thwart attackers from leveraging compromised accounts from one Service Provider to gain access to accounts on other Service Providers (mobile or web application developers and owners).

Enable users and providers to coordinate in order to securely restore accounts following a compromise.

http://openid.net/wg/risc/

The Problem

accounts are interconnected

- explicitly through federation
- implicitly through email address and recovery flows

owned on one service leads to owned on other services

RP sessions are disconnected from IdP

Events - Account Status Changes

Account Secured due to suspected compromise

Suspended - by owner

Suspended - by provider

Reactivated - by owner

Reactivated - by provider

Deleted - by owner

Deleted - by provider

Reissued

Events - Account Auth Changes

Password Changed

Session(s) Revoked

Recovery Email Changed

Recovery Phone Changed

Public Identifier Changed

2nd Factor Added

Token(s) Revoked

Event Recipient

Only the user's "Apps"!

1. Explicit

   based on OAuth grants

2. Implicit

   based on email recovery

   contractual relationships and background registration

Privacy

1. User Notification and transparency.

2. Settings and opt-out.

Google's Implementation

Current events:

SESSIONS_REVOKED

TOKENS_REVOKED

Near future:

ACCOUNT_LOCKED

ACCOUNT_RECOVERED

Using Google Cloud Pub/Sub for distribution. Publisher only.

Open Issues

Meaningful UX

Hijacking vs abuse

User registration for implicit case

- RISC publisher discovery

Distribution standardization

Critical mass

Event standardization