secevent
Internet-Draft
Intended status: Informational
Expires: December 31, 2017

M. Scurtescu
Google

June 29, 2017

Security Events RISC Use Cases
draft-scurtescu-secevent-risc-use-cases-00

Abstract

This document describes the RISC use cases for security events and helps with defining the requirements for token format and event distribution.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 31, 2017.

Copyright Notice

Table of Contents

1. Introduction

2. Definitions

- Transmitter - the entity that sends security events
- Receiver - the entity that receives security events
- IdP - Identity Provider, in most cases but not always this is the transmitter
- RP - Relying Party, in most cases but not always this is the receiver
- RISC - Risk and Incident Sharing and Coordination, see http://openid.net/wg/risc/
- SCIM - System for Cross-domain Identity Management, see http://www.simplecloud.info/

3. Use Cases

3.1. Explicit IdP to RP

- Transmitter: IdP
- Receiver: RP

Simplest use case, IdPs send security events to relevant RPs.

RP can make control plane calls to the IdP and can authenticate with access tokens issued by IdP.

3.2. Explicit RP to IdP

- Transmitter: RP
- Receiver: IdP

The RP can also send RISC events back to IdP. We want to make it very easy for the RP to do that, no complicated registration steps and crypto of possible.

IdP can document well-known endpoint for data plane (where it receives events). RP can use access token when sending events on data plane and maybe does not need to sign SETs.

If RP is sophisticated and is exposing its own control plane then during RP stream registration with IdP (either manual or programmatic) it can advertise its own issuer and that issuer through .well-known can specify full transmitter functionality of RP.

3.3. Implicit IdP to RP

- Transmitter: implicit IdP
- Receiver: implicit RP

Example: Google and Amazon, Amazon account can be backed by gmail address. Amazon acts as implicit RP to Google in this case.

Google and Amazon need legal agreement, When Amazon account is created or updated with gmail address Amazon makes REST call to Google to enroll this new email address for RISC events. If enrollment succeeds then RISC events will flow bidirectionally (see next section, for simplicity only unidirectional is considered in this section).

Assumption: Amazon/RP is registered with Google/IdP as an OAuth 2 client and can use access tokens for control plane.

Open question: what are the implications of unverified email addresses?

Open question: discovery of hosted domains, how does Google know that example.com is managed by Oracle and that subject enrollment should be sent to them?

3.4. Implicit RP to IdP

- Transmitter: implicit RP
- Receiver: implicit IdP

No enrollent call is strictly necessary. The RP can start sending events to IdP as new identifiers show up.

3.5. Pseudo-implicit

Common email address or phone number used by two different RPs.

Example: Amazon and PayPal, both Amazon and PayPal each have an account with the same gmail address.

Mutual discovery by exchanging email address hashes.

Open question: legal and privacy implications

3.6. Identity as a Service

Example: Google Firebear, IdaaS manages large number of RPs and implements RP functionality on their behalf.

IdaaS should be able to manage SET distribution configuration for its RPs with a given IdP using the credentials already established between the RP and the IdP. Control plane operation to create/update stream allows that.

Assumption: IdaaS can impersonate RP at IdP (can obtain access token on behalf of RP)

3.7. Security as a Service

Similar to IdaaS described in previous estion, but the service provider has its own set of credentials different from the credentials and RP is using. The SP cannot impersonate the RP at IdP. The IdP must define delegation rules and allow the SP to make requests on behalf of the RP.

3.8. On-Premise RP

The RP (receiver) is behind a firewall and cannot be reached through HTTP. The only way to deliver events is if the RP periodically polls an endpoint provided by the transmitter.

Author’s Address

Marius Scurtescu
Google

Email: mscurtescu@google.com