Security Events 101

Phil Hunt, Oracle

Marius Scurtescu, Google

October 2016

Agenda

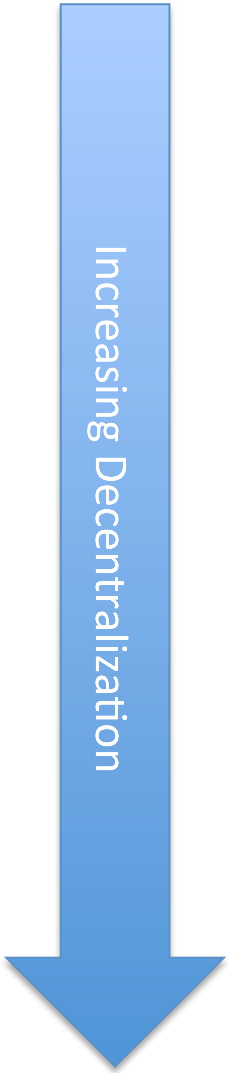
- Introduction
- Decentralization
- What is the problem?
- Events Community
- Security Event Token Standard

Introduction

- Security Events are a new technology to address common problems in distributed Identity Systems
  - Logout
  - Token Revocation
  - Session Management
  - Account Suspensions
  - Suspicious Activity
  - Provisioning
  - Consent
- Why is this needed? Lets look at history…

Historical Introduction

- Identity evolution over the years
  - RFC2617 Basic Authentication Was the Original Authentication Mechanism
    - Applications each with separate users and passwords
  - Applications integrating with LDAP and checking passwords centrally
  - Adoption of form based login
  - Applications integrating with SSO systems
  - Introduction of Federation
  - RFC6749 OAuth2 Delegation
  - OpenID Connect
  - IoT related Identities (ACE)



Increasing Decentralization

Decentralization / Parallelism

- Early apps in the 80s maintained passwords & profiles
  - Eventually they got centralized in LDAP
  - identities pulled out of App SILOs into directory silos
- SSO "sessioning" in the form of cookies
  - Multiple applications share one session
    - Ideally, apps validate self-asserting cookies rather then perform complex per request look-ups
  - SSO systems made LDAP calls and not the apps (except for profile information)
    - Increase in scale

Emergence of Federation

- Federation brought about cross-organizational portability
  - Verifiable tokens (SAML and JWT) that can be wielded by bearers
  - No need to check back with providers
  - Can be quickly and independently validated
- Stateless authentication - Web service providers no longer need to keep checking with a central data store for each request
  - tokens and cookies store state at the user-agent end.

Why is "stateless" important?

- Gives the user-agent control
- Consistent login ceremony & experience
- Speed – no calling back to a central authority
- Per request won't work as web pages and APIs infinitely more complex – a web page involves hundreds of HTTP requests
    - Checking each request centrally won't scale
- Polling Costs $$$ and Performance!
    - Centralized state servers have to be at least 10-100x bigger than the biggest web site served.
        - Has to support worst case loading of all of its clients polling at once
    - Combinatorial effect can cause IDM "brownouts"

What is the problem?
Isn't stateless great?

Initiation Good / Clean-up Bad

- Many systems depend on the browser to "set-up" a session
  - User's leave a lot of profile and session "footprints"
  - We have log-in but not log-out
- Independence of action means
  - Hard to tell where login assertions have actually been used
- Provisioning is now collaborative
  - Systems have similar but unequal information/state
  - Identity crosses boundaries
- Tokens and Cookies are valuable attack vectors

Profile Promiscuity

- This isn't just protocol exploits…
- People will consume services from multiple providers
  - They share their profile data directly and indirectly across many providers
- Attackers can exploit weakness in one provider to use against another
  - Account recovery using 3rd party email
  - Common profile / knowledge factors
- More Info
  - Wired Magazine Matt Honan Story
  - Andy Nash's "Shared Signals" at CIS
  - …

Events Community

A Year Ago

- A number of initiatives were starting to appear to address
  - Logout, Sessions Control, RISC, SCIM, HEART, Token Revocation
- At IIW and at IETF Yokohama (Fall 2015) we observed a lot of similarities in requirements
- Proposal to begin work on defining a common Identity Event format.
  - this has evolved into Security Event Tokens…

Security Events

- Event messages that can be delivered to subscribers in a pub/sub relationship
  - A special use of JSON Web Token (JWT) tokens
  - Can by signed and/or encrypted
  - Often delivered asynchronously or out-of-band to some originating action or state change
- Contain a simple statement about a state change
  - Token <id> is revoked, session <id> is revoked
  - Subject <id> has reset their password
  - Subject <id> modified
  - Subject <id> is suspended
  - Note that the <id> used can have very different impacts (user id, vs token id, vs device id)
    - What is it a provider is actually logging out?

Events Enable Independent Action

- Events are NOT commands – they are statements
  - No error signalling
  - A statement of fact by an asserting party
    - That may or may not be true elsewhere
  - Events do not transfer state, they co-ordinate state
- Events allow independent action
  - A relying party may not have a session for a user
  - A user modified in service A, may not even exist in B.
    - A command to modify a user, presumes the user exists
    - A informing B it changed a user, is more useful
  - A session cancellation says the IDP has cancelled the session. The relying party is not obliged to cancel local session

Closing The Gaps in Identity Systems

- Implementing Logout and Revocation
- Alerting providers to protect identity
- Co-ordinating profiles on a need-to-know basis (co-operative provisioning)

Security Event Token Specs

The SET Token

- Just a JWT token
  - Reuses key attributes: jti, iat, iss, aud, nbf, sub
  - New attributes
    - events – a list of URIs declaring the type of event
    - txn – a unique identifier for the originating transaction
    - event objects – a JSON attribute whose name is the event URI and whose value is a JSON object containing one or more event specific attributes

Example Password Reset

```
 {
     "jti": "3d0c3cf797584bd193bd0fb1bd4e7d30",
     "events":[
       "urn:ietf:params:scim:event:passwordReset",
       "https://example.com/scim/event/passwordResetExt"
     ],
     "iat": 1458496025,
     "iss": "https://scim.example.com",
     "aud":[
       "https://jhub.example.com/Feeds/98d52461fa5bbc879593b7754",
       "https://jhub.example.com/Feeds/5d7604516b1d08641d7676ee7"
     ],
     "sub":"https://scim.example.com/Users/
44f6142df96bd6ab61e7521d9",
     "urn:ietf:params:scim:event:passwordReset":{
       "id":"44f6142df96bd6ab61e7521d9"
     },
     "https://example.com/scim/event/passwordResetExt":{
        "resetAttempts":5
     }
   }
```

Event Type

Event Payload

Example OpenID Logout

```
{
   "iss": "https://server.example.com",
   "aud": "https://rp.example.com",
   "jti": "3d0c3cf797584bd193bd0fb1bd4e7d30",
   "iat": 1458668180,
   "exp": 1458668580,
   "sub": "248289761001",
   "events": [
     "https://specs.openid.net/logout"
   ],
   "https://specs.openid.net/logout": {
     "iss": "https://token.example.com",
     "sid": "08a5019c-17e1-4977-8f42-65a12843ea02"
   }
 }
```

User – Subject identifier

Additional Data
Session id, subject issuer

Example Consent

```
{
    "jti": "fb4e75b5411e4e19b6c0fe87950f7749",
    "events":[
      "https://openid.net/heart/consent.html"
    ],
    "sub": "248289761001",
    "iat": 1458496025,
    "iss": "https://my.examplemed.com",
    "aud":[
      "https://rp.example.com"
    ],
    "https://openid.net/heart/consent":{
      "consentUri":[
        "https://terms.examplemed.com/labdisclosure.html#Agree"
      ]
    }
   }
```

User – Subject identifier

What was agreed to

Security And Confidentiality

- As with normal JWTs,
  - SETs can be encrypted (JWE) for confidentiality
  - SETs can be signed (JWS) to provide verifiability

Standards Status

- The IETF is forming a new working group: Sec Events
  - https://datatracker.ietf.org/wg/secevent/charter/
- Deliverables:
  - SET Token Format profiling JWT
  - A secure method for assured event delivery using HTTP POST
  - PubSub Management
    - Feed Metadata
    - Subscription management and verification
- Maturity
  - Profiling mature standards JWT and SCIM
  - HTTP POST is relatively simple
  - Id-Events in discussion for a year (Nov 2015)
- Proposed Drafts:
  - https://datatracker.ietf.org/doc/draft-hunt-idevent-distribution/
    - Initial draft adjusted to match charter
  - https://datatracker.ietf.org/doc/draft-hunt-idevent-token/
    - Fairly mature, expect fast progress to WGLC (6 revisions)

Discussion / Thanks!