Shared Signals and Events Working Group Charter

1) Working Group Name

Shared Signals and Events

2) Purpose

The goal of the Shared Signals and Events Working Group is to enable the sharing of security events, state changes, and other signals between related and/or dependent systems in order to:

- Manage access to resources and enforce access control restrictions across distributed services operating in a dynamic environment, for instance through the continuous evaluation of session state and device posture.
- Prevent malicious actors from leveraging compromises of accounts, devices, services, endpoints, or other principals or resources to gain unauthorized access to additional systems or resources.
- Enable users, administrators, and service providers to coordinate in order to detect and respond to incidents.

3) Scope

The group will define:

- **Security events**
    - These are events – whether directly authentication or authorization-related or occurring at another time – that one party becomes aware of and that may have security implications for other parties.
- **State Updates**
    - These are updates that reflect state changes at one party that may have impact on the resource access decisions at other parties.

- **Taxonomy**
    - The group will develop a taxonomy of security events and state updates and a common set of semantics to express relevant information about a security event or state update, and recommended actions to take in response to an event or update.
- **Privacy implications**
    - Sharing security or state information amongst providers has potential privacy implications for both end users and service providers. These privacy implications must be considered against both (a) applicable regulations, policies, and the principles of user notice, choice and consent, and (b) the recognized benefits of protecting users' accounts and data from abuse. The group will consider ways to address such potential privacy implications when defining mechanisms to handle the various security events or state updates and recommend best practices for the industry.
- **Communications mechanisms**
    - The group will define bindings for the use of existing transport and event stream management protocols defined elsewhere, and define new protocols as needed to meet technical requirements identified by the group.
- **Trust frameworks**
    - The group will define at least one model for the conditions under which information would be shared.
- **Best practices**
    - Where specifications allow for a wide range of implementations, the group will provide recommended best practices on how to implement specifications safely and securely, and how to mitigate known threats.

Out of scope:

- Determining or issuing statements regarding the reputation or quality of a user.
- Definition of APIs and underlying mechanisms for connecting to, interacting with and operating centralized databases or intelligence clearinghouses when these are used to communicate security events between account providers.

4) Proposed Deliverables

The group proposes the following **Non-Specification** deliverables:

- **Security Event and Account Lifecycle Schema**
    - A taxonomy of security events and a common set of semantics to express relevant information about a security event and its relationships to other relevant data, events or indicators.
- **Security Event Privacy Guidelines**
    - A set of recommendations on how to minimize the privacy impact on users and service providers while improving security, and how to provide appropriate privacy disclosures, labeling and access control guidelines around information in the Security Event Schema.
- **State Change Schema and Guidelines**
    - A taxonomy of a set of state changes for a common set of use-cases to express the information conveyed in such a state change, its relationship to other relevant data and possible actions the receiver is expected or recommended to take.
- **Trust Framework**
    - A trust framework defining roles and responsibilities of parties sharing state changes and user security event information

The group proposes the following **Specification** deliverables:

- **Subscription Negotiation**
    - Defining the ways in which a publisher and subscriber can agree to sharing a set of events or updates and the properties thereof. Also defining the expected or recommended actions the subscriber needs to take in response to specific events or updates.
- **Communications Mechanisms**
    - Define bindings for the event messages to an already existing transport protocol to promote interoperability of sending event information to another Service Provider. This will allow a Service Provider to implement a single piece of infrastructure that would be able to send or receive event information to any other service provider.

- **RISC Event Schema**
    - Define an extensible set of security events related to state changes that can occur within the user account lifecycle.
- **CAEP Updates Schema**
    - Define an extensible set of security events related to state changes or other context changes that may impact the security posture of a user, device, app, client, session, or other context.

5) Anticipated audience or users

- Service providers who manage their own account systems which require an email address or phone number for registration.
- Account and email providers that understand key security events that happen to a user's account.
- Identity as a Service (IDaaS) vendors that manage account and authentication systems for their customers.
- Users seeking to regain control of a compromised account.
- Identity providers.
- Application and Software as a Service (SaaS) vendors that support identity federation.
- Software vendors operating in highly regulated verticals.
- VPN server and network hardware vendors.
- Administrators of systems operating under a zero-trust security model.
- Cloud Access Security Brokers.
- Device management services.
- Endpoint protection services.

6) Language

- English

7) Method of work:

- E-mail discussions on the working group mailing list, working group conference calls, and face-to-face meetings from time to time.

8) Basis for determining when the work is completed:

- Rough consensus and running code. The work will be completed once it is apparent that maximal consensus on the draft has been achieved, consistent with the purpose and scope.

Background information

Related work:

- RFC4120 (https://tools.ietf.org/html/rfc4120) – The Kerberos Network Authentication Service (V5)
- RFC6545 (https://tools.ietf.org/html/rfc6545) – Real-time Inter-network Defense (RID)
- RFC6546 (https://tools.ietf.org/html/rfc6546) – Transport of Real-time Inter-network Defense (RID) Messages over HTTP/TLS
- RFC6684 (https://tools.ietf.org/html/rfc6684) – Guidelines and Template for Defining Extensions to the Incident Object Description Exchange Format (IODEF)
- RFC6960 (https://tools.ietf.org/html/rfc6960) – Online Certificate Status Protocol (OCSP)
- RFC7642 (https://tools.ietf.org/html/rfc7642), 7643 (https://tools.ietf.org/html/rfc7643), 7644 (https://tools.ietf.org/html/rfc7644) – System for Cross-domain Identity Management (SCIM)
- RFC8322 (https://tools.ietf.org/html/rfc8322) – Resource-Oriented Lightweight Indicator Exchange
- RFC8417 (https://tools.ietf.org/html/rfc8417) – Security Event Token (SET)
- draft-hunt-scim-notify (https://tools.ietf.org/html/draft-hunt-scim-notify) – SCIM Notify
- draft-ietf-secevent-http-poll (https://tools.ietf.org/html/draft-ietf-secevent-http-poll) – Poll-based Security Event Token (SET) Delivery Using HTTP
- draft-ietf-secevent-http-push (https://tools.ietf.org/html/draft-ietf-secevent-http-push) – Push-based Security Event Token (SET) Delivery Using HTTP
- draft-ietf-secevent-subject-identifiers (https://tools.ietf.org/html/draft-ietf-secevent-subject-identifiers) – Subject Identifiers for Security Event Tokens
- ISO/IEC 27002:2013 (https://www.iso.org/standard/54533.html) – Information technology — Security techniques — Code of practice for information security controls

- ISO/IEC 27035:2011 (https://www.iso.org/standard/44379.html) – Information technology — Security techniques — Information security incident management
- sstc-saml-core-2.0-os (http://saml.xml.org/saml-specifications) - Security Assertion Markup Language (SAML) 2.0
- ws-trust-1.3-spec-os (http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.html) – WS-Trust
- XACML-v3.0-Errata01 (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml) – eXtensible Access Control Markup Language (XACML)

Proposers

2019 Re-charter as Shared Signals and Events Working Group

- Asad Ali, Thales
- Morteza Ansari, Cisco
- Annabelle Backman, Amazon
- Tim Cappalli, Aruba Security
- Pamela Dingle, Microsoft
- Erik Gustavson, Google
- Didier Hugot, Thales
- Rob Otto, Ping Identity
- Romain Lenglet, Google
- Marius Scurtescu, Coinbase
- Rich Smith, Cisco
- Atul Tulshibagwale, Google
- Jordan Wright, Cisco
- Reda Zerrad, Lookout

Original RISC Working Group

- Henrik Biering, Peercraft
- John Bradley, Ping Identity
- Adam Dawes, Google
- George Fletcher, AOL
- Andrew Nash, Confyrm
- Mark Risher, Google
- Nat Sakimura, Nomura Research Institute
- Vicente Silveira, LinkedIn

- Alex Weinert, Microsoft

Anticipated contributions:

- "CAEP Subscription Negotiation 1.0" under the Open ID Foundation's IPR Policy (http://openid.net/intellectual-property/).
- "CAEP Event Types 1.0" under the OpenID Foundation's IPR Policy (http://openid.net/intellectual-property/).
- "OAuth Event Types 1.0" under the OpenID Foundation's IPR Policy (http://openid.net/intellectual-property/).
- "OpenID RISC Event Types 1.0" under the OpenID Foundation's IPR Policy (http://openid.net/intellectual-property/).
- "OpenID RISC Profile of IETF Security Events 1.0" under the OpenID Foundation's IPR Policy (http://openid.net/intellectual-property/).
- "Security Event Token (SET) Stream Management API" under the OpenID Foundation's IPR Policy (http://openid.net/intellectual-property/).