Threat Centric Identity and Access Management

Rakesh Radhakrishnan, National Practice Lead - IAM Consulting

Mark Coderre, OpenSky National Practice Director – GRC & Security Services

September, 2015

OPENSKY
A TÜV Rheinland Company

Table of Contents

Table of Contents

Introduction – Emergence of Threat Centric Identity and Access Management 2
A Capability Model for Threat Centric IAM 3
Capability Level Definitions 4
Evolution of IAM Capability as an Enterprise Security Domain 6
Enterprise Benefits from Threat Centric IAM 7
Real World Vendor Examples of Threat Centric IAM 8
Conclusion 10
Glossary of Terms 11

Emergence of Threat Centric Identity and Access Management

Conventional security architecture took advantage of ingress and egress points on a fairly well defined set of enterprise perimeters. Various cloud patterns (IaaS, PaaS, and SaaS) have disrupted the perimeter and in some cases (such as native mobile to SaaS) totally bypassed it. Still, the need exists to enforce data-centric protection policies for both preventative and detective controls. If you can't hang these controls on the ingress and egress points, what's the new common denominator? What does everyone still want and need when they go about their daily business? The answer: Identity & Authentication. Whether your approach is single sign-on, centralized sign-on or simpler sign-on, there's a business benefit to investing heavily here. People want to get to information easily and information security wants to up the assurance levels as a key control in the ongoing cyber-resilience battle. Once you have hooked the request for information with authentication you have a new common-denominator for controls. Leveraging authentication as the new beachhead can replace classic perimeters in your cyber strategy.

In addition to weak authentication, passwords and cookie-based session hijacking, as well as privilege escalations are amongst the top vulnerabilities exploited in a high percentage of attacks. All of which point to the need for improved IAM maturity levels and impacts on cyber threats.

Hence, cyber-resilience requires a keen eye on threat means, motive and opportunity, and alignment with the evolution of security intelligence and sharing for a "Threat Centric IAM". Threat Centric IAM is a growing principle in IAM design and architecture.

Threat Centric IAM can be defined by the following elements:

- Next generation SIEM (security information and event management) tools have built-in big data technologies (Map Reduce, Hadoop, tuples, etc.) that are threat intelligence and risk / behavior aware making them threat intelligent systems (for example – Splunk with its acquisition of Caspedia and with support for Structured Threat Information Expression (STIX) interfaces).
- Threat analytics with big data technologies can feed this threat intelligence (STIX) to all security controls.
- Intelligence-driven architecture will involve real-time responses based on actionable intelligence. The response can be fine-grained in terms of a recommended set of actions.
- Threat intelligence will be integrated into the IAM stack for "design time", "provision time", "run time" and "access time" IAM control response.

- Threat intelligence will be integrated with network controls, application controls and data controls (pervasive integration).
- This Threat Centric IAM approach fulfills the full-loop integration required in intelligence driven security systems.
- Policy automation and dynamic policy generation (policy combinations) will mature the solution to respond real time with exception policies based on threats (Note - this makes a STIX profile for XACML an interesting technical committee initiative at OASIS for 2015 and 2016).

All industry verticals (healthcare, transportation, banking and more) will benefit from this Threat Centric IAM model in security architecture, IAM architecture, and the technology solutions deployed to mitigate risks from cyber threats. Threat centric models are a natural evolution from the earlier "network centric" or "identity centric" models, and builds on top of those approaches. Threat centric models actually leverage the earlier models for a better level of capability and maturity.

A Capability Model for Threat Centric IAM

In today's world of evolving IAM architectures and solutions, we can understand enterprise IAM maturity via a capability model with four levels. Visually the Threat Centric IAM cube below indicates the relationships between the four levels of IAM maturity, the threat intelligence dimension and the two major elements of identity and authentication (IDM), and access management (IAM).

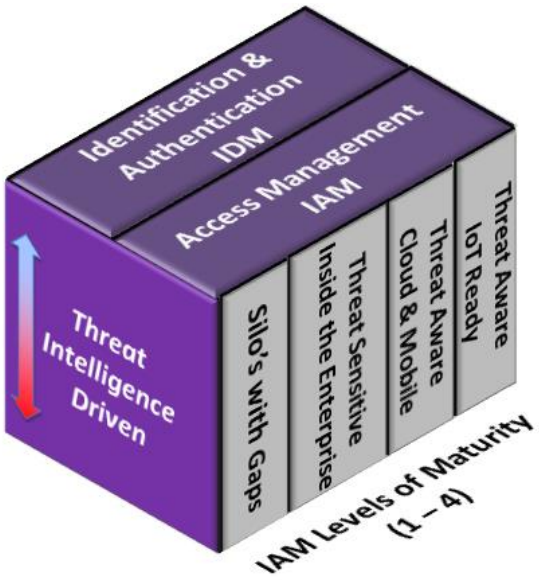

Figure 1 – The Threat Centric IAM Model

When compared to the overall Security Maturity Model as defined by Security Architects LLC, which takes into account people and process alongside security technologies, the IAM Maturity Model shown below is a technology centric viewpoint. The table and the subsequent section provide the specific capability definitions for the four levels of maturity in the Threat Centric IAM model.

Levels	Authentication (AuthN) User, device & Apps/Services	Federation – SAML and IA levels based on MFA	Role based Access Provisioning (privileged and non-privileged)	ABAC – access controls (XACML) for Applications and IaaS/PaaS/SaaS	Tag based Access Privileges (Documents, Tables, DB and DLP)	Token based Access Decisions (private and public STS)	IAM integrated Admission Controls (network) –& Identity in the Stack	STIX driven Policy exceptions and IoT
Level 1 – Siloed with gaps	Some authN exists non standard	Some enterprise federation exists	Partially implemented	Cover 20% or less apps	Not fully addressed	None	None	None
Level 2 – Threat sensitive inside the enterprise	Mature standards based authN (OATH, SIM, TPM, OTP, etc.) FIDO driven MFA	Mature deployments Enterprise SSO	90% there (intra enterprise)	For internal applications ONLY	For PCI and other high risk data and Files	None	None	None
Level 3 – Threat Aware Cloud and Mobile	Mature standards based authN (OATH, SIM, TPM, etc.) FIDO driven MFA Service Authentication	Mature deployments Mobile SSO (native via OAUTH) Cloud SSO	100% there (role based provisioning extended to cloud apps)	For internal applications and SaaS, PaaS, etc.	For PCI and other high risk data and Files (within compliant cloud offerings)	Yes (mature Token Service Implementations)	Yes (deployed extensive admission controls via a cloud connect model)	None
Level 4 – Threat Aware and IoT ready	Mature standards based authN (OATH, SIM, TPM, etc.) FIDO driven MFA IOT authentication	Mature deployments Mobile SSO (native via OAUTH) Cloud SSO	100% there (role based provisioning extended to cloud apps)	For internal applications, SaaS, PaaS, etc. FGES and ABAC for Object level Access as well	For PCI and other high risk data and Files (within compliant cloud offerings)	Yes (mature Token Service Implementations)	Yes (deployed extensive admission controls via a cloud connect model)	Yes (STIX XACML) Scalable Directory of IoT objects IoT LWM2M extensions to IAM

Table 1 – The Levels of Maturity in the Threat Centric IAM Model

Capability Level Definitions

Level 1 implies a lack of comprehensiveness, normalized IAM controls (duplicates yet not complete), lack of integration and consistent workflows.

Level 2 implies comprehensive (end to end), standard interface-based IAM controls that are cohesive. Privileged access is based on a role-based provisioning model and workflows. In general, access management is broken into 4 domains (access provisioning, access controls, privileged access and access decisions) with the following aspects:

- Roles are utilized for access provisioning
- Attributes apply for access controls

- Tags refer to access privilege designs
- Tokens are utilized for access decisions

Level 2 can also include some threat intelligence in the form of adaptive (risk based) authentication implementations.

Level 3 implies that the enterprise has a mature datacenter (private cloud) with an enterprise IAM system. This system would include related controls that act as the cloud connect (for IaaS, PaaS and SaaS public clouds and social networks) from end points that are controlled devices, and mobile end points. The datacenter has IAM integrated with admission controls (MDM, access network aware, device aware, VPN aware, VDT aware, etc.). The path of every connection to the clouds is controlled and the sessions can be recorded.

Level 3 also implies that IAM is integrated into network admissions control processes and data/application access controls (DB FW, DLP, Data Tokenization, Externalized Entitlement Service that are OWASP compliant and more).

At level 3 the threat intelligence goes beyond authentication and is leveraged for adaptive access controls or threat-based access exception rules, built into several application, data and network control products. This can also include threat intelligence of the enterprise network, end point and cloud offerings leveraged.

Level 4 requires that influx of STIX Indictors of Compromise (IOC)-based exception rules exists over and above distributed access decisioning – with STS, OAUTH, REST and other tokens. The threat intelligence expands to the Internet of Things (IoT) and SCADA-like networks beyond mobile end points and clouds.

Level 4 also indicates readiness for IoT adoption with identity in the stack and extending support to LWM2M like protocols (IoT to cloud connects as well).

This maturity model is relevant to the IAM domain alone, and in levels 2, 3 and 4 threat awareness also matures significantly. At level 2 enterprise threat tools are leveraged, at level 3 end point and cloud threat intelligence is taken into account, and at level 4 IoT threat intelligence is also taken into account.

Evolution of IAM Capability as an Enterprise Security Domain

Identity and Access Management as a significant domain within security has evolved rapidly since the first specifications of SAML (2001) from the Liberty Alliance and later OASIS. It is heavily standards driven today as shown below:

Category	Standard
Authentication	3GPP SIM authentication OATH protocol TPM authentication OpenID specification Kerberos Smartcard Alliance
Multi-factor Authentication	FIDO
Access Token	OAUTH
Federation and SSO	SAML 1 or 2 (carrying the authentication context)
Identity Assurance Levels	NIST IA Levels, Kantara and NSTIC
Access Control	XACML 1, 2 and 3.0
Identity Provisioning	NIST RBAC 1, 2 and 3, SCIM

Table 2 – IAM Standards

Enterprises at maturity level 2 moving towards maturity level 3 are focused on this standards based integration.

The majority of the compliance driven enterprises (50% or more) have embraced the maturity of these standards and are well integrated end-to-end via these standards specifications. IAM systems that are comprehensive and address identification, provisioning, authentication, authorization, administration end-to-end, will require extensive investments between 2015 and 2020 to achieve maturity levels 2 or 3. The investments in these initiatives are driven either by FFIEC, HIPAA, PCI-DSS, SOCS, ISO27002 and other compliance domains relevant for the enterprise.

Level 3 implies that the enterprise has an IAM strategy and architecture designed and working, not only within on-premise enterprise systems, but can also integrate with external cloud offerings – IaaS, PaaS, SAAS and social networks from mobile end points. This implies cloud security brokers are well integrated alongside their IAM implementation that allows for SAML-based access to SaaS - for example, integration of AWS public clouds with a private cloud implementation. A well designed solution allows for an enterprise IAM system integrated with private cloud datacenter's next generation, identity-aware, admission controls (NAC on steroids). This integrated IAM solution makes their private cloud implementation a "secure cloud connect" that handles user, device and service authentication, and admission controls to specific IaaS and PaaS platforms, based on RBAC/ABAC and XACML policies, propagated to

public cloud service access (like Box.com, DropBox.com, Amazon AWS) via cloud security brokers (like SkyHigh Networks, Netskope, and Pallera)

In 2015, the majority of enterprises are attempting to achieve maturity level 3, address shadow IT (clouds), and integrate their IAM strategy with a cloud connect model (context based admission controls), so adoption of cloud models and a varied mix of mobile end points is possible.

The next challenge is to take the IAM maturity level to level 4 that allows extensions to IoT (via protocols like LWM2M and object level access controls expressed in XACML) and fully leveraging threat intelligence (STIX IOC and STIX COA) for access control exception policies.

At maturity level 2 and 3, the policies are pre-defined and propagated with a life cycle (authentication rules, admission rules and resource access rules), such as RBAC (roles), ABAC (attributes) and TBAC (tag based). Level 4 capabilities, on the other hand, include the threat intelligence typically captured by a FireEye-like system (for IoT, SCADA, etc.) via:

- Indicators of Compromise in an XML format (like STIX IOC)
- Around an IoT, end point device, server device, IP address, identity credentials, a URL resource, or a piece of code
- With access exception rules that are allowed to kick in dynamically, based on the incident in question.
- Policy automation technologies (such as Oracle Policy Automation and Axiomatics ALFA policy automation languages) with run time threat intelligence makes access exception policies dynamic.

Enterprise Benefits from Threat Centric IAM

As an enterprise adopts this model and matures its IAM program from Level 1 to Level 2, the benefits reaped are a standards-based, threat-sensitive approach to internal, integrated IAM controls. For example, if you are threat aware based on internal threat detection, and a network device is detected to be vulnerable via a particular threat vector, integrated processes can quickly remove privileged credentials associated with that device, until the time it is restored to a high integrity state.

As organizations mature from level 2 to level 3, not only are they leveraging the enterprise threat intelligence tools, they also leverage the plethora of external threat intelligence services integrating that awareness and intelligence to cloud computing and mobile end points. Ultimately, this threat intelligence captured can also extend to SCADA networks and the internet of things so that the IAM controls can perform full-loop integration based on threat

intelligence on end points (mobile devices and IoT), enterprise networks and cloud-based partners.

This approach, therefore, expands an enterprise's threat detection capabilities and IAM capabilities to threat-based protection system, thus helping contain the impact of threats within an environment. As IAM is the key control to all other controls – network facing controls, application controls and data controls – a threat centric IAM model allows for the permeation of the threat centric approach to all other areas of controls. Over time as higher levels of maturity are achieved, a greater percentage of known threats are mitigated with automation, hence allowing for critical human resources to focus on more advanced tasks associated with threats that cannot be mitigated via automation.

Finally, this approach allows for business enterprises to expand to cloud computing and the economies of scale it has to offer (cost cutting), mobile devices and the business processes they allow (expanded markets) and IoT for consumer focused service delivery.

Real World Vendor Examples of Threat Centric IAM

We are seeing this type of Threat Centric IAM integration already taking shape in the Industry today. For large enterprises evaluating next generation threat intelligence (Indicators of Compromise detection tools - FireEye, Fidelis and SourceFire), one of the KEY evaluation criteria is how much of this threat intelligence can serve as actionable intelligence. This requires extensive integration of the Threat Centric IAM platform with several control systems in the network and end points. It may also include several recommended courses of action in the STIX XML attribute set, based on the malware detected. This approach paves the way for enterprises to mature their security architecture into one that is security intelligence oriented and adaptive to cybersecurity threats. The evolution to a Threat Centric IAM platform and a threat analytics platform can range from:

- Mobile end points and APT integration similar to FireEye and Airwatch or FireEye and Mobile Iron
- Identity provisioning workflow driven by data breach incident, and de-provisioning of credentials based on threat intelligence on a data breach incident (such as FireEye and ForgeRock integration)
- Authentication controls - similar to the integration of Norse with SecureAuth for example – where an authentication attempt is integrated with the threat intelligence of the IP address that is attempting such authentication. If the IP address is suspect, then authentication attempts fail.

- Admission controls - network admission controls - similar to FireEye +IBM NetSec or FireEye and Forescout – where the admission of a device to a network or network segment is driven by exception rules, based on device level threat intelligence.
- Access controls - web application firewalls (WAF) and application access control being threat aware, similar to FireEye and Imperva integration (for inbound payload inspection). In addition, all known threats are first mitigated by a Bluecoat or Websense, and then the payload is sent to FireEye (similar to FireEye and Bluecoat integration)
- Data access controls – database firewall and access control integration being threat aware similar to FireEye and Imperva integration - suspect SQL connections are terminated.

Kudos to FireEye for an amazing set of security controls integration and their support for STIX. Integrating security systems together for cross control co-ordination is an important strategic security initiative in cyber space. OpenSky recommends that enterprises consider their "Defense in Depth" strategy as more of an ecosystem than a random layering of controls.

Controls have relationships and there's an opportunity to capture the symbiotic nature of those relationships. This requires enterprises to think about how controls work (and fail) in coordination. Standard Defense in Depth mentality doesn't focus on that. One way to determine the end to end is to do a contextual architecture of the controls and then focus on key performance indicators (KPIs) for each control procedure. Those KPIs must be focused on inputs AND outputs as well as what they are supposed to be doing within their own function for generating risk intelligence indicators (KRIs). Process engineers/architects would use a SIPOC (Source, Inputs, Process, Outputs, and Consumers) approach to distill this. This is advanced security architecture, but if you think of it, other professions hint at the topic and may be more easily engaged in an exercise if you use their language too:

- Engineers: "fail open/close path"
- Security Operations: "control of next resort" (Lockheed Kill Chain context)
- Auditors: "compensating controls"

Conclusion

Why do we need such an integrated defense with a Threat Centric IAM model?

Simply having breach detection capabilities will not suffice, we need both prevention and tolerance as well, to defend against today's complex, multifactor attacks.

What is needed is a combination of:

- Advanced ***Threat Detection*** - threat intelligence and threat analytics
- Responsive/dynamic ***Threat Prevention*** systems - threat intelligence based access controls including format preserving encryption and fully homogenized encryption, that leverage policy automation technologies
- ***Threat Resilient*** systems which can include web containers and app containers, that are self- cleansing and intrusion tolerant.

This whitepaper is the first in a series on Threat Centric IAM. The following whitepapers will add more definition to the Threat Centric IAM model with an identity management framework and an access management framework, and then provide guidance for levels 2 through 4 of IAM maturity.

The primary benefit of this series is for Enterprise CIO, CTO, CISO and Chief Architects, who have invested heavily in IAM programs to gauge their maturity level of their IAM programs and to help align their thinking of IAM architectures and strategies based on business and industry movements towards cloud models, mobile or BYOD end point, and IoT.

Glossary of Terms

Acronym	Abbreviation
IDM	Identity Management
IAM	Identity Access Management
STIX	Structured Threat Information Exchange
IOC	Incident of Compromise
COA	Course of Action
XACML	Extensible Access Control Markup Language
SAML	Security Assertion Markup Language
OATH	Open Authentication
OAUTH	Open Authorization
SIM	Subscriber Identity Module
TPM	Trusted Platform Module
FIDO	Fast Identity Online
PCI	Payment Card Industry
PII	Personally Identifiable Data
LWM2M	Light Weight Machine to Machine
OMA	Open Mobile Alliance
IOT	Internet of Things
SCADA	Supervisory Control and Data Acquisition
DLP	Data Loss Prevention
OWASP	Open Web Application Security Project
REST	Representative State Transfer
RBAC	Role based Access Control
ABAC	Attribute based Access Control
NIST	National Institute of Standards Technology
HIPPA	Health Information Privacy Protection Act
FFIEC	Federal Financial Institution Examination Council
PCI DSS	Payment Card Industry – Data Security Standards
SOX	Sarbanes Oxley Act
ISO27002	International Standards Organization
NAC	Network Admissions Controls
SAAS	Software As A Service
PAAS	Platform As A Service
IAAS	Infrastructure As A Service
SecAAS	Security As A Service
KPI	Key Performance Indicators
KRI	Key Risk Indicators
BYOD	Bring your own device
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CTO	Chief Technology Officer
3GPP	3rd Generation Partnership Program
MDM	Mobile Device Management
OTP	One Time Password
VPN	Virtual Private Network
VDT	Virtual Desk Top