# Enterprise Level Security: Insider Threat Counter-Claims

William R. Simpson *Member, IAENG* and Kevin E. Foltz

***Abstract*— Enterprise Level security (ELS) has no accounts or passwords, and consequently identity is an important issue. All person and non-person entities in ELS are registered and known. PKI credentials are issued, and when necessary, multi-factor authentication is used to improve the assurance of the identity. Because the next step in ELS is claims-based access and privilege, many data owners are worried about the trustworthiness (sometimes called reputation) of the identified requesters (this applies to person and non-person entities within the enterprise). Individuals are vetted periodically, and a baseline is established by those instances; however, activities that occur between those vetting events may provide clues about the trustworthiness of the individuals. Similarly, pedigrees in software and hardware entities are established periodically. Because the terms trust and integrity are overloaded, we refer to these data as veracity. Further, when requested, the veracity that applies to certain categories will be provided as counter-claims along with the claims. These counter-claims may be used by the applications and services for increased levels of surveillance and logging and perhaps even limitation of privilege. This paper reviews the data categories, data requirements, and data resources that apply to entity veracity, as well as the counter-claim structures and issues associated with their tracking and usage. The paper then presents finding and recommendations, along with the future work necessary to complete this evolution.**

***Index Terms*—Behavior, Claims, Counter-Claims, Insider Threat, Integrity, Reputation, Motivation, Veracity**

## I. Introduction

Like it or not, the insider threat must be monitored and assessed, at least for those of us who must comply with executive orders. Since Edward Snowden [1], Bradley Manning [2], and others [3], we simply have no choice but to assess our own insider threat situation.

> "An **insider threat** is a malicious **threat** to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems." [4]

But the manifestation of the threat may come from any entity in the environment, person or non-person. The spate of insider activity has led to a U.S. executive order [5] that requires, in part, federal agencies and enterprises to:

> "…perform self-assessments of compliance with policies and standards issued pursuant to sections 3.3, 5.2, and 6.3 of this order, as well as other applicable policies and standards, the results of which shall be reported annually to the Senior Information Sharing and Safeguarding Steering Committee established in section 3 of this order…."

To For Enterprise Level Security (ELS) [6] federal applications, we must include these self-assessments. The requirement has led to the development of new products and an overwhelming volume of white papers and other research telling us how some vendors would do this assessment, and a number of patents pending [7-10]. All of this leads to a number of product offerings to perform the analysis of entity veracity within the enterprise. A summary of these techniques (through 2011) is provided in [11]. The basic idea is to gather information concerning the trustworthiness of an entity in our system, as shown in Fig. 1. This is an ELS adaption of the figure presented in patent application [8].

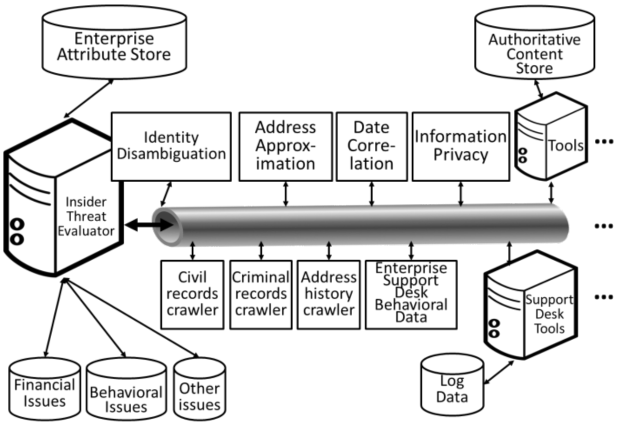

Fig. 1. Data Gathering for Insider Threat Analyses

This paper presents a form of self-assessment that evaluates veracity from the ELS perspective rather than from the perspective of the product's baseline. This paper also addresses the issues associated with the self-assessment, and

Manuscript received April 5, 2017; revised July 30, 2017. This work was supported in part by the U.S. Secretary of the Air Force and The Institute for Defense Analyses (IDA). The publication of this paper does not indicate endorsement by any organization in the Department of Defense or IDA, nor should the contents be construed as reflecting the official position of these organizations

Kevin E. Foltz is with the Institute for Defense Analyses. (email: kfoltz@ida.org).

William R. Simpson is with the Institute for Defense Analyses, 4850 Mark Center Drive, Alexandria, Virginia 22311 USA, and is the corresponding author phone: 703-845-6637, FAX: 703-845-6848 (e-mail: rsimpson@ida.org).

it provides a framework and a process for using veracity information within ELS. To do this, we examine integrity, reputation, and veracity as they apply to the problem of the insider threat.

## II. Integrity, Reputation, and Veracity

Generally, the determination of trustworthiness of an individual is based upon an assessment of the integrity of that individual. One definition of integrity is given below:

> "**Integrity** is the quality of being honest and having strong moral principles; moral uprightness. It is generally a personal choice to hold oneself to consistent moral and ethical standards. In ethics, integrity is regarded by many people as the honesty and truthfulness or accuracy of one's actions." [12]

Social media would define this as reputation, which is good because integrity is already over-used in the information technology (IT) literature. However, the literature defines reputation as a soft issue.

> "**Reputation** is the estimation in which a person or thing is held, especially by the community or the public generally." [13]

Microsoft has refined reputation by adding trust as in:

> "**Reputation** Trust represents a party's expectation that another party will behave as assumed, based upon past experience. Reputation Trust is bidirectional and can be split into Consumer Reputation Trust and Provider Reputation Trust." [14]

But trust is an overloaded term in information technology and requires a great deal of context. The dictionary description of veracity comes closer to the target, and it is not used in any of the IT contexts associated with ELS:

> "**Veracity** is the quality of being truthful or honest." [15]

From the IT standpoint, we have adopted the concept of veracity and tailored its definition to be more amenable to self-assessment in ELS environments:

> **Entity Veracity** is the degree to which an entity is worthy of trust as demonstrated by resistance to or avoidance of factors that denigrate trust or compromise reliability. Positive factors may enhance veracity, and negative ones may reduce veracity. Veracity is based upon recognized accomplishments and failures, along with the associated stress factors or other trust debilitating factors present. A history of actions in difficult circumstances provides strong evidence for or against veracity.

The next step is to determine which of the factors need to be measured. But first we need to understand how identity and access control are handled within ELS.

## III. Enterprise Level Security

The ELS design is a distributed security approach (see Fig. 2) that addresses five security principles derived from the basic design concepts. We address only two here, and the interested reader is directed to [6] for a more complete treatment:

- Know the Players – this is done by enforcing bi-lateral end-to-end authentication;
- Separate Access and Privilege from Identity – this is done by an authorization credential.

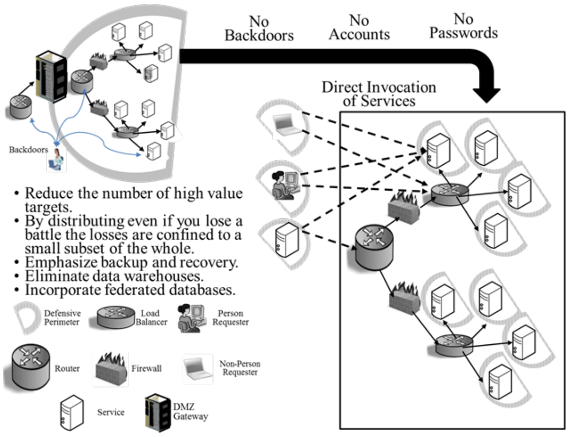
No Backdoors
No Accounts
No Passwords
Direct Invocation of Services
Backdoors
• Reduce the number of high value targets.
• By distributing even if you lose a battle the losses are confined to a small subset of the whole.
• Emphasize backup and recovery.
• Eliminate data warehouses.
• Incorporate federated databases.
Defensive Perimeter
Load Balancer
Person Requester
Router
Firewall
Non-Person Requester
Service
DMZ Gateway

Fig. 2. Distributed Security Architecture

### A. Know the Players

In ELS, the identity certificate is an X.509 Public Key Infrastructure (PKI) certificate [16]. This identity is required for all requesters and providers of services (active entities), both person and non-person, e.g., services, as shown in Fig. 3. PKI certificates are verified and validated. Ownership is verified by a holder-of-key check. Supplemental (in combination with PKI) authentication factors, such as identity-confirming information or biometric data, may be required from certain entities.

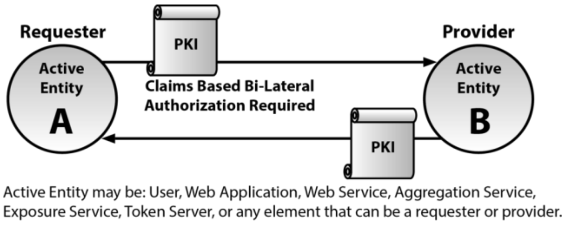
Requester
Provider
PKI
Active Entity A
Claims Based Bi-Lateral Authorization Required
Active Entity B
PKI
Active Entity may be: User, Web Application, Web Service, Aggregation Service, Exposure Service, Token Server, or any element that can be a requester or provider.

Fig. 3. Bi-lateral Authentication

### B. Separate Access and Privilege from Identity

ELS can accommodate changes in location, assignment, and other attributes by separating the use of associated attributes from the identity. Whenever changes to attributes occur, claims are recomputed based on the new associated attributes (see section III), allowing immediate access to required mission information. As shown in Fig. 4, access control credentials utilizing the Security Assertion Markup Language (SAML) (SAML authorization tokens differ from the more commonly used single-sign-on (SSO) tokens, and in ELS, they are not used for authentication.). [17] SAML tokens are signed, and the signatures are verified and validated before acceptance. The credentials of the signers also are verified and validated. The credential for access and privilege is bound to the requester by ensuring a match of the distinguished name used in both the authentication and the authorization credentials.

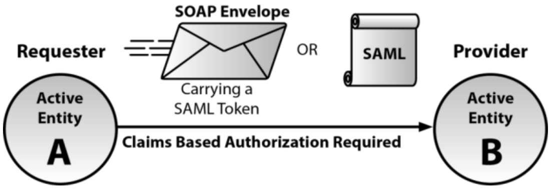

Fig. 4. Claims-Based Authorization

Veracity must be presented as a counter-claim, a claim that provides possible re-consideration of the claim's information.

## IV. Elements of Veracity

A list of indicative events may be formulated by category and data sources. [18–19] We start categorization with person entities because this is required in the self-assessment, but veracity extends to all entities within the enterprise because non-person entities may actually be under insider threat control. For all entities, we assume a default value of 1.0 for veracity before detailed veracity computations are made. This is the minimum value needed to pass periodic re-evaluations, so it is assumed that all entities in the enterprise possess this value unless veracity factors indicate otherwise.

### A. *Person Entities*

Person entity factors cover a variety of data about the person and his behaviors and may come from a variety of sources. These data cannot be considered unless they derive from designated (by the enterprise) authoritative sources. Entity veracity factors are assigned, initially, unit values and may be combined from a number of sources. Unit values may be positive or negative (either increasing or decreasing veracity), and they are applied to veracity measures in a later section. Any previously resolved issues (through vetting or supervisor administrative judgement) may be discarded. Five categories are delineated below:

1. Community information – characteristics or events that add to the veracity of a person. Each adds a fixed value to overall veracity.
   a. Ties within the community (positive or negative),
   b. Recent job title change (positive or negative),
   c. Recent relevant awards or job punishments (positive or negative),
   d. Direct support or doubt from notable entities (Trust transitivity) (positive or negative).
2. Financial information. Degree of debt or other financial burdens since last vetting. These may be age-and source-sensitive, and they may be attribution-sensitive, as discussed in the next section.
   a. Issues with credit cards (negative),
   b. Large number of credit reports (negative),
   c. Recent suspicious loan activity (negative),
   d. Sudden explained or unexplained wealth (negative),
   e. Debt exceeds ability to pay (negative).
3. Legal issues or other stress factors. These may be age- and source-sensitive, and they may be attribution-sensitive, as discussed in the next section.
   a. Recent death in family (negative),
   b. Poor job performance rating (negative),
   c. Divorce (negative),
   d. DUI (negative),
   e. Felony or misdemeanor charges (negative).
4. Discovered secrets. These may be age- and source-sensitive, and they may be attribution-sensitive, as discussed in the next section.
   a. Attempts to hide sexual issues (negative),
   b. Uncovered alternate identities (negative),
   c. Residential ambiguity or multiple residences in a locale (negative).
5. Unusual behavior. These will generally be from the Enterprise Support Desk Records and may be considered authoritative.
   a. Non-cleared travel (negative);
   b. Unusual and unexplained IT usage (negative),
      i. Unusual downloads (negative),
      ii. Unusual hours of usage (negative),
      iii. Many open applications at same time (negative);
   c. Sharing of credentials (negative);
   d. Frequent use of backup methods (negative);
   e. Unusual delegations (negative);
   f. Extended on-line absence followed by high activity (negative);
   g. Unusual hours or time on-line (negative).

### B. *Non-Person Entities.*

These will generally be from the Enterprise Support Desk Records and may be considered as authoritative. All are negative.

1. Recent attacks. These are considered unless complete teardown and rebuild has happened since the attacks.
2. Recognized misuse of privilege. This may be documented through the enterprise support desk.
3. The host server is physically moved outside (or into) a protected area. All enterprise assets are registered, and the registration must be updated when any changes occur.
4. Call-out to unknown URLs. This is a known sign of exploitation, and unless the device is being used in counter-cybersecurity, it should be considered for a complete teardown and rebuild.
5. Missing log records.
6. Lenient access and privilege requirements. Privileges granted to the device may be greater than the device uses for its own access.
7. Available software interfaces that are not authorized. One clear step with ELS is to close all interfaces not being used and remove the software behind those interfaces where possible.
8. Non-uniform identity requirements on interfaces. All interfaces in use should have the same identity assurance requirements.
9. Missing current patches that are authorized. One example is Industrial Control Systems (ICS) not being patched until they have to be taken off-line.

## V. Issues Based on Elements of Veracity

It is not easy to discern where an entity is facing issues that may lead to an insider problem. At the same time, acquisition of the data may have ethical and legal implications. We will briefly discuss some of the issues associated with computing veracity.

1. Data Sources:
   a. Public and private mix. Confirming sources is problematical, and public web sites readily trade information, which obscures the original source.
   b. Attribution. (Source www.whitepages.com (3 November 2016: 190 possible matches for Frank Jones in Virginia, 50 in Richmond area, 12 are 50–65 years old, 5 of these are Frank E. Jones.) Many public sources are subject to error and may or may not have enough confirming information to provide unimpeachable attribution.
   c. Few vetted sources or authoritative content stores.
   d. PII issues. Privacy affects not only the acquired data, but the confirming data. Use of social security or other private information may assist with attribution but cross privacy lines.
2. Veracity of the veracity data:
   a. In ELS, entity attributes are meticulously screened. Fig. 5 shows a portion of the enterprise attribute ecosystem used for the creation of claims. The attribute data is required to come from authoritative sources (meaning that an organization is tasked with maintaining the accuracy and currency of the data). Even then, the data is not completely trusted and must pass sanitization and mediation before it is accepted into the attribute store. Public sources may have little more than a data entry clerk and no checks for accuracy or completeness.
   b. In the public domain, sources feed one another and veracity checks may or may not be made. Old events may acquire new dates, and some of the details may get further confused.

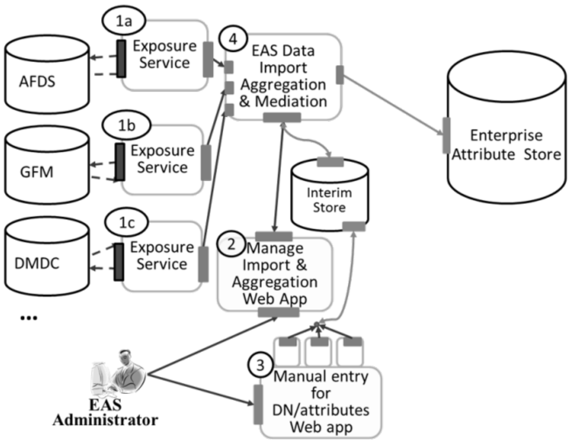
1a
Exposure Service
AFDS
1b
Exposure Service
GFM
1c
Exposure Service
DMDC
...
4
EAS Data Import Aggregation & Mediation
Enterprise Attribute Store
Interim Store
2
Manage Import & Aggregation Web App
3
Manual entry for DN/attributes Web app
EAS Administrator

Fig. 5. Creating an Attribute Store

   c. Errors in the public private data. Even when data correction paths are available,
   d. The data may get regenerated as in (b) above.
   e. Can reputations be rebuilt? This question is real, and we do not currently have the answer. ELS users are periodically re-vetted, and we can assume issues that happened before that vetting will be resolved during the vetting process. One finding is to limit (by configuration) how far back insider data is considered.
3. Veracity adjustments to access or privilege may affect getting the job done. This can lead quickly to unrecoverable situations.
4. Delegation is an issue. ELS claims that are discretionary in nature may be delegated. Delegation itself may be considered a veracity issue.

## VI. Creating a Veracity Model and Counter-Claims

A simplified model is developed as a start. While weightings may be applied to the various values of veracity factors, it is best to await some actual experience with the representation before beginning that modification. In section 4, we delineated five basic categories of veracity for person users and a single category for non-person users for evaluation, subject to data sources and correlation. Accordingly veracity is described as an n-tuple shown below:

For Persons:

Veracity = (Enhancing Characteristics = $V_1$, Financial = $V_2$, Legal = $V_3$, Other = $V_4$, and Behavior = $V_5$) (eq. 1)

For Non-Persons:

Veracity =$V_6$ (eq. 2)

Further, each value has a default value of 1.0 which is appreciated by $\Delta V$ in category 1 for each of the unique factors in that category.

$(\Delta V_1)_k$ = +/-0.1* source factor1*source factor 2 (eq.3)
for every k with a unique occurrence of a category in paragraph 4A1.

The default value of 1.0 is reduced by $\Delta V$ for each of the unique factors in categories 2–6 where applicable.

$(\Delta V_i)_k$=(+/-0.1)$_i$ *source factor1*source factor 2 (eq.4)

where i=2-6 and for every k with unique occurrence of a category in paragraph 4Ak.

Source factor1 is 0.5 for publicly derived data, and 0.25 for publicly derived data without source citation or date of item. Source factor1 is 1.0 for authoritative source data. Source factor2 is 0.5 where attribution is approximate and 1.0 where attribution is certain.

$V_i = V_i + \sum \Delta V_i$ (eq.5)

Counter claims will be provided when requested by the data owner in the registration of his/her service. The counter claims will be given as a vector of values:

Counter Claim for a person = $V_1$, $V_2$, $V_3$, $V_4$, $V_5$, none (eq.6)

Counter Claim for a non-person = none, none, none, none, none, $V_6$ (eq.7)

Supervisors and data owners will have claims for access to component data from the insider threat server for subordinates (in the case of supervisors) and for application and service users (in the case of data owners). Issues may be marked as resolved at the supervisor's discretion (subject to attribution and logging). An example would be at periodic vetting, the supervisor may mark some issues resolved.

Actions possible:

1. Threshold for denial of access to resources. Not recommended.
2. Threshold for notification to supervisors and data owners (Recommended).
3. Reduce privilege. Not recommended. This may affect performance reviews and cause the value of veracity to further decline in a self-generated spiral.
4. Upon notification, set up a counseling session with the individual or the owner of the asset to review the issues and seek corrections (Recommended).
5. After review, the data may be manually reset, if desirable, by providing rationale and obtaining appropriate authority.

In all cases, when requested by the data owner, the counter claim will be passed in the SAML.

## VII. Conclusions and Findings

The formulation is new and in response to a presidential directive. However, certain findings are appropriate at this point:

1. For persons, the data associated with information generated prior to the last formal vetting of the person may be marked as resolved at the supervisor's discretion.
2. For persons, it is not felt that automated responses are warranted at this time.
3. For persons, manual resolutions of unfavorable veracities should be implemented at this time.
4. For non-persons, automated responses may be appropriate.
5. Thresholds and responses should be worked out over time with experience.
6. Self-assessment – data as required by executive order 13587 should be summarized and reported.

The veracity measures can provide a management view into the insider threat and can be used to satisfy the requirement for self-assessment. This work is part of a body of work for high-assurance enterprise computing using web services. Elements of this work are described in [6, 20-33].

## References

[1] Bill Gertz, "The Cyber Threat: Snowden—Ultimate Insider Threat Missed by NSA Security," September 20, 2016. http://freebeacon.com/national-security/cyber-threat-snowden-insider-threat-at-nsa/?utm_source=Freedom+Mail&utm_campaign=1dd6da9f89-WFB_Morning_Beacon_09_20_169_19_2016&utm_medium=email&utm_term=0_b5e6e0e9ea-1dd6da9f89-40546409 accessed April 17, 2017.

[2] Steve Fishman, New York Magazine, "Bradley Manning's Army of One," July 3, 2011. http://nymag.com/news/features/bradley-manning-2011-7/, accessed April 17, 2017.

[3] Ryan Francis, CSO online, "9 employee insiders who breached security," October 6, 2014. http://www.csoonline.com/article/2692072/data-protection/data-protection-165097-disgruntled-employees-lash-out.html, accessed Apr 17, 2017.

[4] Wikipedia, "Insider threat," https://en.wikipedia.org/wiki/Insider_threat, October 2016.

[5] Barack Obama, "Executive Order 13587 – Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 7, 2011.

[6] Simpson, William R., CRC Press, "Enterprise Level Security – Securing Information Systems in an Uncertain World," by Auerbach Publications, ISBN 9781498764452, May 2016, 397 pp.

[7] Ann Margaret Strosaker, Michael Thomas Strosaker, Patent, "Determining veracity of data in a repository using a semantic network," US 8108410 B2, International Business Machines Corporation, January 31, 2012. https://www.google.com/patents/US8108410?dq=US+8108410+B2&hl=en&sa=X&ved=0ahUKEwjg6PyH-IzQAhVD2yYKHfOMCAwQ6AEIHTAA, accessed Apr 17, 2017

[8] Geoffrey Lee, Patent, "Candidate-initiated background check and verification," US 20050055231 A1, published March 10, 2005. http://www.google.com/patents/US20050055231

[9] Eileen Shapiro, Steven Mintz, Patent, "System and method for providing access to verified personal background data," US 20040168080 A1, August 26, 2004. http://www.google.com/patents/US20040168080

[10] Yu Zhao, Jianqiang Li, Patent, "Hierarchy extraction from the websites," US 20090327338 A1, Nec (China) Co., Limited, December 31, 2009. https://www.google.com/patents/US20090327338

[11] J. Hunker, C.W. Probst, "Insiders and insider threats – an overview of definitions and mitigation techniques," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* (JoWUA), 2 (2011), pp. 4–27.

[12] Wikipedia, "Integrity",https://en.wikipedia.org/wiki/Integrity, accessed November 2016.

[13] Dictionary.com, http://www.dictionary.com/browse/reputation, "reputation," accessed November 2016.

[14] Gerrit J. van der Geest and Carmen de Ruijter Korver, Microsoft, *The Architecture Journal*, "Managing Identity Trust for Access Control," July 2008. https://blogs.msdn.microsoft.com/nickmac/2009/05/21/the-architecture-journal/,.

[15] Merriam-Webster, "Veracity," http://www.merriam-webster.com/dictionary/veracity, accessed November 2016.

[16] X.509 Standards
   a. DoDI 8520.2, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 24 May 2011.
   b. JTF-GNO CTO 06-02, Tasks for Phase I of PKI Implementation, 17 January 2006.
   c. X.509 Certificate Policy for the United States Department of Defense, Version 9.0, 9 February 2005.
   d. FPKI-Prof Federal PKI X.509 Certificate and CRL Extensions Profile, Version 6, 12 October 2005.
   e. RFC Internet X.509 Public Key Infrastructure: Certification Path Building, 2005.
   f. Public Key Cryptography Standard, PKCS #1 v2.2: RSA Cryptography Standard, RSA Laboratories, Oct 27, 2012.
   g. PKCS#12 format PKCS #12 v1.0: Personal Information Exchange Syntax Standard, RSA Laboratories, June 1999; http://www.rsa.com/rsalabs/node.asp?id=2138 PKCS 12 Technical Corrigendum 1, RSA laboratories, Feb 2000.

[17] Organization for the Advancement of Structured Information Standards (OASIS) open set of Standards
   a. Ragouzis et al., Security Assertion Markup Language (SAML) V2.0 Technical Overview, OASIS Committee Draft, March 2008.
   b. P. Mishra et al. Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, March 2005.
   c. S. Cantor et al. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, March 2005.

[18] J. W. Butts, R. F. Mills, and R. O. Baldwin, "Developing an insider threat model using functional decomposition," in Computer Network Security, ser. Lecture Notes in Computer Science, V. Gorodetsky, I. Kotenko, and V. Skormin, Eds. Springer Berlin / Heidelberg, 2005,

vol. 3685, pp. 412–417. [Online]. Available: http://dx.doi.org/10.1007/11560326 32

[19] R. Chinchani, A. Iyer, H. Q. Ngo, and S. Upadhyaya, “Towards a theory of insider threat assessment,” in Proc. of the 2005 International Conference on Dependable Systems and Networks (DSN’05), Yokohama, Japan. IEEE, June–July 2005, pp. 108–117.

[20] William R. Simpson, Coimbatore Chandersekaran and Andrew Trice, “A Persona-Based Framework for Flexible Delegation and Least Privilege,” Electronic Digest of the 2008 System and Software Technology Conference, Las Vegas, Nevada, May 2008.

[21] William R. Simpson, Coimbatore Chandersekaran and Andrew Trice, “Cross-Domain Solutions in an Era of Information Sharing,” The 1st International Multi-Conference on Engineering and Technological Innovation: IMET2008, Volume I, Orlando, FL, June 2008, pp. 313–318.

[22] Coimbatore Chandersekaran and William R. Simpson, “The Case for Bi-lateral End-to-End Strong Authentication,” World Wide Web Consortium (W3C) Workshop on Security Models for Device APIs, 4 pp., London, England, December 2008.

[23] William R. Simpson and Coimbatore Chandersekaran, “Information Sharing and Federation,” The 2nd International Multi-Conf. on Engineering and Technological Innovation: IMETI2009, Volume I, Orlando, FL, July 2009, pp. 300–305.

[24] Coimbatore Chandersekaran and William R. Simpson, “A SAML Framework for Delegation, Attribution and Least Privilege,” The 3rd International Multi-Conf. on Engineering and Technological Innovation: IMETI2010, Volume 2, pp. 303–308, Orlando, FL, July 2010.

[25] William R. Simpson and Coimbatore Chandersekaran, “Use Case Based Access Control,” The 3rd International Multi-Conference on Engineering and Technological Innovation: IMETI2010, Volume 2, pp. 297–302, Orlando, FL, July 2010.

[26] Coimbatore Chandersekaran and William R. Simpson, “A Model for Delegation Based on Authentication and Authorization,” The First International Conference on Computer Science and Information Technology (CCSIT-2011), Springer Verlag Berlin-Heildleberg, Lecture Notes in Computer Science, 20 pp.

[27] William R. Simpson and Coimbatore Chandersekaran, “An Agent Based Monitoring System for Web Services,” The 16th International Command and Control Research and Technology Symposium: CCT2011, Volume II, Orlando, FL, April 2011, pp. 84–89.

[28] William R. Simpson and Coimbatore Chandersekaran, “An Agent-Based Web-Services Monitoring System,” International Journal of Computer Technology and Application (IJCTA), Vol. 2, No. 9, September 2011, pp. 675–685.

[29] William R. Simpson, Coimbatore Chandersekaran and Ryan Wagner, “High Assurance Challenges for Cloud Computing,” Lecture Notes in Engineering and Computer Science: Proceedings World Congress on Engineering and Computer Science 2011, WCECS 2011, San Francisco, USA, 19–21 October 2011, pp. 61–66.

[30] Coimbatore Chandersekaran and William R. Simpson, “Claims-Based Enterprise-Wide Access Control,” Lecture Notes in Engineering and Computer Science: Proceedings World Congress on Engineering 2012, WCE 2012, London, U. K., 4–6 July 2012, pp. 524–529.

[31] William R. Simpson and Coimbatore Chandersekaran, “Assured Content Delivery in the Enterprise,” Lecture Notes in Engineering and Computer Science: Proceedings World Congress on Engineering 2012, WCE 2012, London, U. K., 4–6 July 2012, pp. 555–560.

[32] William R. Simpson and Coimbatore Chandersekaran, “Enterprise High Assurance Scale-up,” Lecture Notes in Engineering and Computer Science: Proceedings World Congress on Engineering and Computer Science 2012, WCECS 2012, San Francisco, USA, 24–26 October 2012, pp. 54–59.

[33] Coimbatore Chandersekaran and William R. Simpson, “A Uniform Claims-Based Access Control for the Enterprise,” International Journal of Scientific Computing, Vol. 6, No. 2, December 2012, ISSN: 0973-578X, pp. 1–23.