End User Computing Environments for Improved Information Security

Pankaj Goyal
MicroMega Inc.
Denver, USA
e-mail: Pgoyal@micro-mega.biz

***Abstract*— Access control does not prevent an authorized "insider" inadvertently or deliberately leaking information to an unauthorized external or internal party. The "insider threat" is one of the greatest threats to enterprise security, and nearly 70% of recently surveyed organizations view Web 2.0 (and by extension cloud computing environments) as a serious data loss risk. The primary focus has been on Data Loss Prevention (DLP) methods to prevent "malicious" data leakage; data leakage includes data loss as well as inadvertent data sharing. In today's highly interconnected world, with a proliferation of camera equipped cell phones, preventing data loss by a determined insider, possibly in collusion with other insiders is impossible. However, if as multiple analyses of data breaches show, the majority of data breaches (as high as 80% of all data breaches) occur from end-user error then the incidence and resulting loss from data breaches can be significantly reduced. This paper presents a method for organizing the end-user computing (EUC) environment to prevent inadvertent data leakage and, thus, improve information security.**

Keywords- information security; data loss prevention; insider threats; end-user computing environment.

I. INTRODUCTION

Ubiquitous untethered anywhere anytime access to vast amounts of information, applications, services and computing resources is fast becoming a reality. Even today, companies and individuals store and provide access to their intellectual property, trade secrets, confidential private information and other assets over a network. Ensuring who gets access to and do what is the subject of both physical and logical security. The major objective of security is to deny, deter, delay and detect unauthorized access.

Crime Prevention Through Environment Design (CPTED) is a holistic multi-disciplinary approach to security. The objective of CPTED is to consider all aspects of the environment in deterring and denying opportunities, including impulsive, for crime. The factors include facilities, Heating, Ventilation, & Air Conditioning (HVAC), utilities (electric, water, waste), Fire, perimeter, physical access control, and intrusion detection.

In both physical and logical access control, the purpose of Identification is to establish the "who" the user is, Authentication is to confirm the veracity of that claim, and Authorization is to verify whether the user has access to the "object" (services, resources, information, documents and other assets). Similar to the physical world, presenting some credential from a trusted credential issuing authority may establish identification. In a highly distributed environment and with no central trusted authority this can be a major challenge; another issue is of preventing fraudulent credentials. Authorization establishes the "rights" of a user to perform some set of actions on an "object" and access control methods aim to protect the "object" from unauthorized access or actions. This is again a challenging problem with distributed and mobile "objects;" in a cloud computing environment (CCE) the objects may relocate to meet performance or other requirements.

In the physical world, perimeter security consists of fences, gates, rooms, doors, dogs and guards; guards, motion detectors and closed circuit television (CCTV) provide surveillance to detect intrusion. In the logical world, network perimeter security through endpoints, intrusion detection systems (IDS), access control and logs all help to delay and detect, and intrusion prevention systems (IPS) to prevent access to achieve security. Safes and secure rooms embedded deep within other rooms, with multiple levels of access control including physical guards, provide asset security. Securing servers and networks is not quite a match for this level of physical deep depth defense; even with hardened infrastructure, the user environment and its usage is not subject to rigorous control.

In the current and emerging ubiquitous computing environments, the "castle defense" mentality of trusting everyone within the organization is flawed. Access control does not prevent an authorized user inadvertently or deliberately leaking an object to an unauthorized party – data breach or data loss; the ubiquitous access to and ease of distribution (or leaking) of objects in a CCE vastly compounds this problem. This "insider threat" is one of the greatest threats to enterprise security. Almost 70% of all organizations view Web 2.0 as a serious concern for data loss prevention (DLP) [8]. Organizations around the world

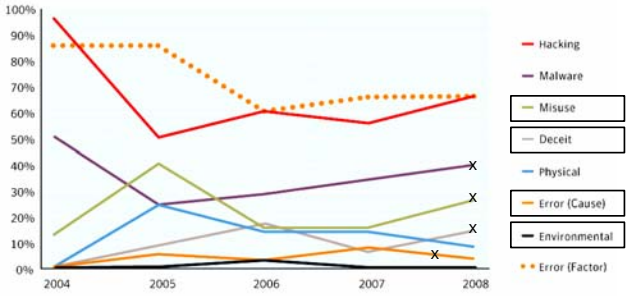

Figure 1. Threat categories over time by percent of breaches [34] (adapted to highlight insider threats).

 ISBN: 978-1-61208-010-9

are facing increased regulatory pressure to secure and safeguard at "rest" or "in flight" digital information; in the US, in addition to federal regulations such as Health Insurance Promotion and Accountability Act (HIPAA)[15], Sarbanes-Oxley[33], Gramm-Leach-Bliley[14], a number of states have imposed their own sometimes more stringent regulations and penalties for breach. However, in today's highly interconnected world preventing data loss by a determined insider, possibly in collusion with other insiders, is impossible; malicious person(s) with appropriate administrative system privileges or even camera equipped cell phones. Although intellectual property theft accounted for less than one percent of all cybercrimes against businesses, it resulted in more than 50 percent of the total monetary loss [31].

An analysis of insider data breaches continues to show that the majority of breaches, as high as 80%, are inadvertent and non-malicious [28, 34]. Fig. 1 shows data breaches by category with the insider breaches boxed; the malicious or "deceit" insider breaches are about half of the insider misuse breach and much less when combined with other breaches such as those due to error and environments. This Data Loss Prevention (DLP) from negligence and non-malicious human error is a major challenge and largely unaddressed, except for the creation of and training on policies. An aspect of DLP that remains unanalyzed is the affect of internal data leaks on performance, such as productivity.

Kulkarni et al [20] addressed the issue of the corporate risks due to uncontrolled storage of data associated with End User Computing Applications, such as spreadsheets, databases etc., with the potential risks posed to the confidentiality, integrity, and availability of this data due to its existence on EUC Applications. It is estimated that around 32% of financial data resides in EUC Applications [27].

The prevention of inadvertent data leakage – the predominant cause of all data leaks – will significantly reduce the incidence and resulting loss from data breaches. This paper presents a method for DLP applicable to the large percentage of such external and internal inadvertent data breaches. The paper examines some well known security mechanisms and shows their inapplicability for inadvertent data breaches.

II. BACKGROUND AND RELATED WORK

In a usage control policy, the object stakeholder defines the allowed accesses to a target object on a target platform. A stakeholder can be the owner of the object, or a provider delegated by the object owner to protect the object. An object can be services, tools, systems, resources, facilities, information, data, messages, or even a credential [37].

A. Identity Management

The special issue of Computer magazine [29] on identity management contains a number of papers that deal with the very important issue of digital identity management including interoperable trusted identity [26], federated identity management [7], challenges for federated assurance [23], multifactor identity verification [25] and an identity management framework [22]. The user-centric IDM approach [18] that allows users to control their digital identities and uses identifiers or attributes to define a user.

DLP methods do not require any special identity management and the end-user environment may be subject to multiple different identity management techniques. Access control, DRM and other usage control techniques do not prevent data leakage by authorized users.

B. Access Control

Access control technologies enforce or enable enforcement of usage control policies. Access control aims to protect objects from unauthorized access or use by "agents;" agents includes users and tools/systems. Or alternately, grant agents permissions to perform some set of actions on objects. Most popular method is role-based access control (RBAC) that employs the concept of "roles" assigned permissions or "rights" on an "object;" no assignment of individual rights [32]. RBAC is very efficient for large numbers of users, and can deal with a wide range of security policies. Role hierarchies, for example, reflecting some line of authority and responsibility are a common aspect of RBAC models. Role hierarchies support role inheritance a very useful feature when assigning common permissions to large groups. Inheritance also creates role hierarchies where a senior role has more permissions than a junior role; the senior role (r_s) inherits the permissions of the junior role (r_j) and may have additional permissions of its own [35]; the role inheritance satisfies the constraint: (Permissions (r_j) subset of Permissions (r_s)) and (Authorized-Agents (r_s) subset of Authorized-Agents (r_j)).

Attributes-based access control (ABAC) is useful in highly distributed heterogeneous environments [19, 36] and can also be used in conjunction with RBAC. Environment roles can capture the security-relevant context of the environment, as access decisions may depend on the context of the requests [10]; context-based RBAC provide fine-grained access control [16, 21]. Environment roles support the securing of context-aware applications and security policies that make use of environment roles to control access to resources. Constraints in RBAC [35] deal with static and dynamic separation of duty such that either no users are assigned to conflicting roles (static separation of duties), or users cannot be activated for conflicting roles simultaneously (dynamic separation of duty). Rule-based RBAC [1] provides mechanisms to assign roles based on rules defined by the security policy; the rules may establish seniority relationships and, thus, a roles hierarchy. Temporal Role Based Access Control (TRBAC) controls role activation time constraints [4, 17]; limits access to certain times. Temporal and other constraints are a subset of general conditions that control usage; access permitted only when user at specified premise and after a certain event occurring. Other extensions include generalization of roles to include subject, object and environmental roles [24], history [12] and privacy-preserving protocols using zero-knowledge proof-based techniques [3]; and assignment of user rights and permissions for web services based on the

 ISBN: 978-1-61208-010-9

strength of the identification mechanism in a context dependent RBAC can be a viable approach for access control in web-based services [35].

In very large organizations or in extended or virtual organizations, centralized RBAC administration is an issue and major challenge. In decentralized domain level RBAC, different administrated domains are independent [2]; the administrator in a domain manages a subset of all the roles and users, and can even define different roles. This however, is a problem for inter-domain role and user rights management.

Most of these access control methods do not address information flow restrictions; for example, usage control of an object released into an end-user environment.

C. Usage Control

Previous work on usage control enabling mechanisms mainly focuses on digital rights management (DRM). Usage control in distributed environments requires the enforcement of security policies on a remote client platform with high assurance and verifiable trust. However, in general, in use DRM mechanisms cannot support enforcement in an EUC Environment for an authorized user. Most importantly, DRM mechanisms are usually proprietary, work best in closed environments and do not interoperate with other DRM techniques. DRM techniques use encryption/decryption and some externally managed trust (key, certificate, rights) or content server; decryption may be restricted to a specific target environment and a particular application; the approaches do not support environment and application heterogeneity. The lack of interoperability (including standards), the need for a centralized external trust server or the need for continuous control hampers adoption in highly distributed environments.

Zhang et al. [37] present general security requirements for usage control and propose a general framework. Their approach requires a hardware-based trusted subsystem that includes a root-of-trust, trust chain, and a policy transformation and enforcement mechanism such that a policy stakeholder can deploy sensitive data and services on the subsystem.

Pretschner et al. [30] present a taxonomy of enforcement mechanisms for usage control and provide an overview of the existing usage control mechanisms. To plan for a future enforcement mechanism the team [30] elicited functional usage control, actions, conditions and obligations requirements from many different organizations and users. In their model, conditions constrain usage restrictions and action requirements, and specify circumstances under which usage restrictions or action conditions apply; conditions are concerned with time, cardinality, events that happened, purpose, and environment. Rare and limited support exists for action requirements and event-defined conditions in current usage control mechanisms.

D. Information Life Cycle and Security Supply Chain

Traditional security aims to protect the IT infrastructure and systems – the perimeter and the structures – that house, manipulate and transport the valuable information assets. Information Lifecycle Management (ILM) manages the flow of information from creation, storage, transport, use, to its deletion. One possible way to identify and address information security issues, over the information lifecycle, is to consider the information security supply chain (ISSC) over the information life cycle [5]. Boyson et al. [5] present a Cyber Supply Chain Assurance Reference Model that draws from supply chain risk and physical security management, and defines key actors, processes, vulnerabilities, and identifies strategic interdependencies at each node of the supply chain.

An ISSC, should make accessible all relevant security-related information to every relevant company in the supply chain to optimize and deliver the most effective security over the entire supply chain and life cycle rather than sub optimize for local the company; lacking this capability, information security is the weakest of the supply chain and life cycle participants. Effective security delivery over the supply chain and life cycle requires both transactional (raw) and analytical security information; analytical information that predicts future possibilities or future impacts of current and past events and decisions is critically important.

III. INSIDER THREATS

The exposure of confidential information is now the single greatest threat to enterprise security. According to one survey, Web email or Web posting (e.g., message board, blog) accounted for 37% of information leaks and that almost 70% of all organizations view Web 2.0 as a serious concern for DLP [8]. Company employees who inadvertently violate data security policies continue to represent a major factor in occurrence of data breaches – some 67% in one analysis and 88 percent in another [28]. Insider threats manifest in a number of ways [29]. Proliferation of information is the natural result of business activity and a productive workforce. As a result of data proliferation, most organizations do not know how much sensitive data exists on their systems and where.

The most common type of data breach occurs when confidential data has been stored, sent or copied by well-meaning insiders [34]. This type of DLP from negligence and non-malicious human error is a major challenge and largely unaddressed, except for creation of and training on policies.

Current mechanisms to thwart insider threats include: (a) content monitoring and filtering solutions; (b) gateway appliances that protect data in motion, such as that in e-mails, instant messages and general Web traffic; and (c) monitoring for suspicious usage patterns. Event and usage logs provide compliance related controls and audits, in addition to the ability to detect threats. Detecting policy violations involving nebulous concepts—such as the transfer of sensitive information and trade secrets—is more difficult and generates numerous false positives [6].

Insider adversaries continue to defeat the current individual and mostly non-integrated protection strategies, and, so a systems-based approach, considers all operational activities including the insider's characteristics, motives,

 ISBN: 978-1-61208-010-9

and capabilities [11]. A controlled double-blind experiment, however, with 50 participants randomly divided into benign and malicious users to detect insiders who misuse their privileges, did not identify any one behavior that distinguishes malicious users from benign ones [6]. The team also reviewed the current state of the art and reviewed publicly available information on malicious insider cases.

IV. END-USER COMPUTING WORKSPACES MODEL FOR INFORMATION SECURITY

Individually, we participate or operate in a number of social contexts: work, family, professional, etc. (Fig. 2). We possess an identity and perform some role in each of these contexts; our identities and roles may not be identical in these different contexts. In a given context, the identity determines the role but the role identifies a set, possibly null, of individuals (identities); please note that the identity and role cannot determine the context.

In the non-digital world, Identity Management (and analogously role management) is the natural human behavior of generating, managing and choosing roles according to a found social context; where these roles are often mandated by socio-cultural norms and possibly refined by each individual ("role making") [9]; sometimes we choose identities for specific contexts. In a particular context, people choose an appropriate role ("role taking") or perform the role assigned to them, and exhibit a natural capability of resolving any apparent role conflicts in their behavior. They have learned an intuitive understanding of what information to divulge and how to react to information received, in the context of the environment and their own as well as their communication partners' role.

Both in the real world (non-digital world) and the virtual world, these social compacts sometimes wittingly or unwittingly breakdown – "insider threat."

A. *End-User Computing Environment Workspaces*

The EUC environment, commonly referred to as the desktop environment, refers to all of the programs, applications, processes, and data used by an end-user; In this paper the term EUC environment is used as it does not denote any particular end-user hardware. EUC virtualization separates an EUC environment from a physical machine, with the EUC environment (the "virtualized" desktop) residing on a remote central server and running in a virtualized machine. This allows users to access their desktops from any capable device.

An EUC workspace, in the digital world, corresponds to the real world social context. The EUC workspace is a virtualized computing environment characterized by some features, for example, organization, team, role, user identity, applications and operational environment with the objective of, say, managing usage and access control governed by policies and event conditions. An EUC workspace provides a functional EUC environment and encapsulates everything above the operating system kernel – applications, data, and any non-privileged operating system subsystems; each EUC workspace also contains Gateway Services (see below).

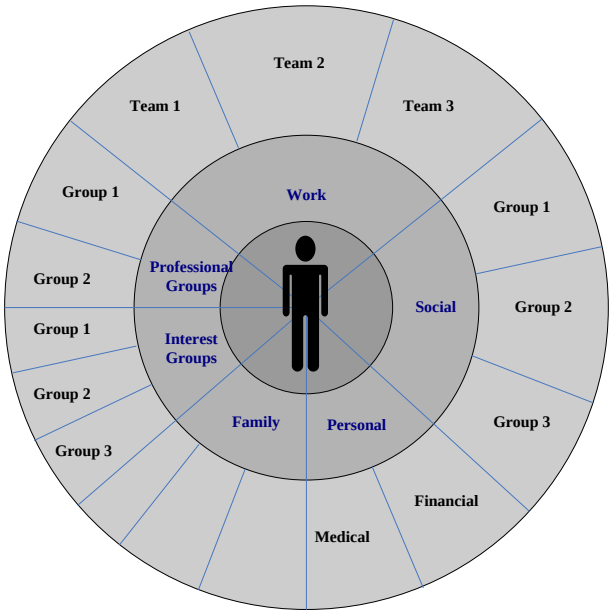

Figure 2. An Individual's social contexts; in the digital world, domains correspond to social contexts.

Please note that these workspaces are quite different from Linux workspaces; every Linux workspace contains the same desktop, the same panels and the same menus, but does not provide workspace isolation.

The EUC environment can, thus, be partitioned into isolated multiple EUC workspaces. Applications within a workspace can interact with each other but are isolated from those in the other workspaces. An application can exist in multiple workspaces but applications in different workspaces are distinct; for example, an email program in two workspaces may have different address books, where the address books contain only entries of authorized recipients, and, thus, only information within the workspace can be emailed to another authorized user. Additionally, an application in different workspaces may be configured differently; for example, some functionality may exist in a workspace but not in another. Thus, the isolation provided by EUC workspaces, the configuration of the applications, authorized user lists, etc. prevents even inadvertent sharing of information with non-authorized personnel. While multiple EUC workspaces may be operating simultaneously, the end-user can only manipulate one workspace at any given time i.e., focus can only be on one EUC workspace. To operate in another workspace, the user has to switch workspaces; switching workspaces does not terminate any running programs, applications, etc.

Secondly, the Gateway Services ensure not only proper logging for audit trail but also ensure that all information (and message exchanges) is automatically encrypted, abides to all policies that govern the workspace, such as information duplicated to the appropriate corporate store.

The EUC workspaces can be arranged in a hierarchy based on security levels (security hierarchy); this is particularly useful for enterprises that typically have an employee participate in multiple teams and where

 ISBN: 978-1-61208-010-9

hierarchies are natural. This hierarchical organization of EUC workspaces can be used for asset fragmentation, location distribution and customization and, hence, risk reduction. Promotion of assets, to a higher secure classification level for access in a more secure environment, only after asset security examination – virus scan, integrity checks, and required sign-offs. Demotion of assets, to a lower classification level for wider accessibility, only after asset meets reclassification conditions and organizational policies; thus, a document released for wider audience only after, say, all reviews completed and publication date met. When an asset is successfully reclassified it cannot be accessed from the previous workspace.

Object supply chain (usage, movement, etc.) creates an object use graph (OUG). The OUG for object O_i includes information on all usage (life cycle) and on "parent" objects – objects with superset of content or "simultaneously" accessed objects while O_i created or modified, where "simultaneously" is defined as within some time interval independent of the EUC workspace. The OUG for O_i (or $OUG(O_i)$) determines the set of objects on which O_i may have a content dependency. Our model is an extension of the dependency graph of [29]. An object O_i is demotable to a target EUC workspace (can be moved to the target workspace – parent hierarchy) if and only if (i) all objects in $OUG(O_i)$ already demoted (usable in target workspace), and (ii) the policy governing demotion of O_i is satisfied (for example, approval by a review committee).

Typically, workspaces exist on an EUC device but there are no technical obstacles for them to exist in a virtualized environment; the virtualized environment will have to support the underlying operating system.

1) Physical EUC devices

EUC devices are partitioned into virtual computing environments; can be either hardware level virtualization through the use of hypervisor or supported through the Operating System. An EUC workspace is associated with one and only one virtual computing environment. The current generation of EUC devices is quite capable of handling virtualization.

2) EUC on Cloud Computing Environment (CCE)

The same principle applies, except that in a CCE the virtual machines hosting the EUC workspaces may not be on the same server hardware or even the same CCE.

B. Gateway Services

Gateway Services control incoming and outgoing messages; only permissible messages are allowed. Ongoing analysis of the gateway logs of all events, messages, etc. and their correlation with other logs (other gateways, access controls, etc.) provides a mechanism for real-time surveillance. Each workspace gateway services serves as Message Intrusion Detection (MIDS) and Message Intrusion Prevention System (MIPS). The gateway/proxy architecture of [13] easily adopts to perform the MIPS and MIDS functions. Analysis of MIPS and MIDS logs, events and messages can take advantage of parallel computation and use of multiple analysis techniques, such as those used to identify behavioral patterns and statistical anomalies.

V. CONCLUSION AND FUTURE WORK

Our individual participation in different social (including work) environments in both our real and digital (virtual) world is a source of data/information loss. In the real world, we are trusted to intuitively safeguard information from unauthorized recipients. This also applies to the digital world. Given easy access and the possibility of errors, for example use of an incorrect email address (of another similarly named individual or a personal instead of official address), the problem of inadvertent, or malicious, data loss is magnified. In many ways, the term and challenges with data protection are being redefined with the advent of virtual and cloud computing environments. The existing problem of insider threats if not properly addressed would be magnified in these environments. Work to date, in the security field has concentrated on preventing unauthorized access to information, whether by internal users or external miscreants. This paper outlines our model for the prevention of non-malicious insider threats.

The model is an EUC focused solution that reduces the risk of inadvertent data leakage. The solution is easy to implement. For example, some capabilities of the model are easily simulated in a multi-user environment by the assignment of different user-ids for each domain; it has also been implemented on a desktop running virtualization software and multiple instances of Linux and even a MS Windows environment. Other capability implementations require changes to, for example, applications; again feasible with open-source applications.

It is impossible to design experiments that simulate actual behaviors in multiple organizations; the data [28, 34], with significant variations among reporting organizations, is of reported breaches and the human error rate ranges between 70 and 90% (Fig. 1). Thus, it is difficult to evaluate the efficacy of the proposed solution until it is adapted by a significant percentage of organizations; then their prior to and post-adaption results can be compared. Though, if the existing data surveys and analysis is correct, then the errors due to inadvertent written disclosure of information shall be minimized; it should be noted that there is no way to prevent verbal disclosure.

A major issue concerns software application licensing and how the major software vendors would treat multiple virtual environments in EUC devices. The solution presented here is also applicable to cloud computing environments. The issue of how Software as a Service (SaaS) providers would treat users that have multiple distinct environments is still open and beyond the scope of this paper; an equitable resolution may increase the appeal of using SaaS in large enterprises.

In the very near future, if not already today, environmental conditions such as "noisy" and "unsecure," and proximity to unauthorized would be easily detectable and, thus, incorporable in a insider threat risk mitigation plan.

 ISBN: 978-1-61208-010-9

REFERENCES

[1] M.A. Al-Kahtani and R. Sandhu. "Induced role hierarchies with attribute-based RBAC," Proceedings of the 8th ACM symposium on Access control models and technologies, 142-148, 2003.

[2] J. Bacon, K. Moody, and W. Yao, "A model of OASIS role-based access control and its support for active security," ACM Trans. Information Systems Security, vol. 5, 492-540, 2002.

[3] E. Bertino, F. Paci, and R. Ferrini, "Privacy-Preserving Digital Identity Management for Cloud Computing," IEEE Computer Society Data Engineering Bulletin, 1–4, Mar. 2009.

[4] E. Bertino, P.A. Bonatti, and E. Ferrari, "TRBAC: A temporal role-based access control," ACM Transactions on Information and System Security, 4(3), 191-223, 2001.

[5] S. Boyson, T. Corsi, and H. Rossman, "Building a Cyber Supply Chain Assurance Reference Model," Science to Solutions Magazine, SAIC, vol. 2, 2009.

[6] D. Caputo, M.A. Maloof, and G.D. Stephens, "Detecting Insider Threat of Trade Secrets," IEEE Security & Privacy, vol. 7, 14-21, 2009.

[7] D.W, Chadwick and G. Inman, "Attribute Aggregation in Federated Identity Management," IEEE Computer, Vol. 42, 33-40, 2009.

[8] C. .A. Christiansen, B. E. Burke, and G. Pintal, "Web Security SaaS: The Next Generation of Web Security," IDC White Paper, 2008.

[9] S. Clauss and M. Kohntopp, "Identity Management And Its Support Of Multilateral Security," Computer Networks, vol. 37, 205-219, 2001. http://dx.doi.org/10.1016/S1389-1286(01)00217-1.

[10] M.J. Covington, W Long, S. Srinivasan, A.K. Dev, M. Ahmad, and G.D. Abowd, "Securing context-aware applications using environment roles," Proceedings of the 6th ACM symposium on Access control models and technologies, 10-20, 2001.

[11] F.A. Duran, S.H. Conrad, G.N. Conrad, D.P. Duggan, and E.B. Held, "Building a System for Insider Security," IEEE Security & Privacy, vol. 7, 30-38, 2009.

[12] G. Edjlali, A. Acharya, and V. Chaudhary, "History-based access control for mobile code," ACM Conference on Computer and Communication Security, 38-48, Nov. 1998.

[13] P. Goyal, "An Interoperability Enabling Framework: Services, Processes and Clouds," 2009 IEEE Asia-Pacific Services Computing Conference (IEEE APSCC), 174-179, 2009.

[14] Gramm-Leach-Bliley Act, "Financial Services Modernization Act," 1999, http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/content-detail.html

[15] Health Insurance Portability and Accountability Act (HIPAA), 1996, http://www.hhs.gov/ocr/privacy/hipaa/administrative/statute/index.html

[16] J. Hu, A. Weaver, A Corradi, R Montanari, and D Tibaldi, "Context-based access control for ubiquitous service provisioning," 28th Annual International Computer Software and Applications Conference (COMPSAC 2004), 444-501, 2004.

[17] J.B. Joshi, R. Bhatti, E. Bertino, and A. Ghafoor, "Access Control Language for Multi-domain Environments," IEEE Internet Computing, 8(6), 40–50, 2004.

[18] M. Ko, G.-J. Ahn, and M. Shehab "Privacy-Enhanced User-Centric Identity Management," IEEE Int'l Conf. Communications, pp. 998–1002, 2009.

[19] D.R. Kuhn, E.J. Coyne, and T.R. Weil, "Adding Attributes to Role-based Access Control," IEEE Computer, Vol. 43, 79-81, June 2010.

[20] A. Kulkarni, E. Williams, and M.R. Grimaila, "Mitigating Security Risks for End User Computing Application (EUCA) Data," IEEE International Conference on Privacy, Security, Risk and Trust, 1171-1176, 2010.

[21] A. Kumar, N. Karnik, and G. Chafle, "Context sensitivity in role-based access control," ACM SIGOPS Operating Systems Review, 36(3), 53-66, 2002.

[22] G. Lopez, O. Canovas, A.F. Gomez-Skarmeta, and J. Girao, "A SWIFT Take on Identity Management," IEEE Computer, Vol. 42, 58-65, 2009.

[23] P. Madsen, H. Itoh, "Challenges to Supporting Federated Assurance," IEEE Computer, Vol. 42, 42-49, 2009.

[24] M. Moyer and M. Ahamad, "Generalized role-based access control," 21st international conference on distributed computing systems (ICDCS'01), 391-398, 2001.

[25] F. Paci, R. Ferrini, A. Musci, K. Steuer Jr., and E. Bertino, "An Interoperable Approach to Multifacotr Identity Verification," IEEE Computer, Vol. 42, 50-57, 2009.

[26] P. Pacyna, A. Rutkowski, A. Sarma, and K. Takahashi, "Trusted Identity for All: Toward Interoperable Trusted Identity Management, Systems," IEEE Computer, Vol. 42, 30-32, 2009.

[27] E. Perry and J. Jinnet, "Spreadsheet Chaos: Impact of Federal Bailout and Other Developments," Prodiance Corporation, April 2009.

[28] Ponemon Institute, Fourth Annual US Cost of Data Breach Study: Benchmark Study of Companies, Ponemon Institute, 2009, http://palisadesystems.com/common/files/Ponemon_CODB_2009.pdf

[29] S. Pramanik, V. Sankaranarayanan, and S. Upadhyaya, "Security Policies to Mitigate Insider Threat in the Document Control Domain," 20th Annual Computer Security Applications Conference (ACSAC'04), 304-313, 2004.

[30] A. Pretschner, M. Hilty, F. Schutz, C. Shaefer, and T. Walter, "Usage Control Enforcement: present and Future," IEEE Security & Privacy, vol. 6, 44-53, 2008.

[31] R.R. Rantala, "Cybercrime against Businesses, 2005," Bureau of Justice Statistics Special Report, Sept. 2008; www.ojp.usdoj.gov/bjs/pub/pdf/cb05.pdf.

[32] R.S. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E. Youman, "Role based access control models," IEEE Computer, 29(2), pp. 38-47, February 1996.

[33] Sarbanes–Oxley Act of 2002, "Public Company Accounting Reform and Investor Protection Act," 2002, http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/content-detail.html

[34] Symantec, "Anatomy of a Data Breach: Why Breaches Happen…and What to Do About It," Symantec, 2009.

[35] R. Wolf, T. Keinz, and M. Schneider, "A Model for Context dependent Access Control for Web-based Services with Role-based Approach," In the Proceedings of the 14th International Workshop on Database and Expert Systems Applications(DEXA'03), 2003, pp.209-214.

[36] E. Yuan and J. Tong, "Attributed Based Access Control (ABAC) for Web Services," IEEE International Conference on Web Services (ICWS'05), pp.561-569, July 2005.

[37] X. Zhang, J-P Seifert, and R. Sandhu, "Security Enforcement Model for Distributed Usage Control," 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2008, pp. 10-18.

 ISBN: 978-1-61208-010-9