Guest Editorial Preface

The Growing Importance of Identity Management

Abdullah Rashed, University of Minho, Portugal

Henrique Santos, University of Minho, Portugal

Ubiquity and mobility have laid to a new era of computer users (Higby & Bailey, 2008), that use Internet to do a significant part of their life's activities. Furthermore, a growing number of users are accessing the Internet through wireless devices, from everywhere (Yan, Abouzakhar, Xiao, & Qayyam, 2009). This Internet growth has made it an integral part of many businesses' daily operations (Taylor, 2001). Users need both flexibility and mobility (Keshariya & Hunt, 2008). Moreover, the growth in the popularity of "global" Internet services, added to the increasing demands of mobile users, demands integration and inter-working of these heterogeneous access networks (Keshariya & Hunt, 2008).

No surprise, the number of security incidents also raised, not only due to the technical vulnerabilities typically found in high complex devices, but also due to misuse. Securing wireless networks in an untrustworthy open environment is always a challenging problem (Boudriga, Baghdadi, & Obaidat, 2006). Even with good internal security practices, such as firewalls and virus protection, mobile devices are still vulnerable to malware, since wireless access allows the spread of computer viruses and worms once accessing less-protected networks (Yan, Abouzakhar, Xiao, & Qayyam, 2009). In this environment Access Control and Identity Management assume a very important role being the first barrier to protect devices and the information they carry. Within Access Control, Authentication is a process of two different actions: provision and verification (Sklavos, Denazis, & Koufopavlou, 2007). In a simple way, provision aims to generate some sort of shared secret (e-identity), which is stored on a device for later comparison with data provided by a subject that claims to be the same that have provided the secret. There are different techniques available to implement these operations. Efficiency is critical, as is acceptance, since even the most efficient technology fails if users do not accept it and find a way to misuse it.

Without a face to face interaction, stolen or lost credentials can be easily abused to hide many types of e-crimes. Besides, users can be fooled to provide personal digital identity to rogue sites, unless they are very well trained (Madsen, Koga, & Takahashi, 2005). To il-

lustrate that, we will use this example: when users visit a bookshop they do not need to show their unique numbers or any other personal information; in contrast, when they visit e-bookshop, they have to provide, at least, their IP address but normally, sites are able to capture more information (Sklavos, Denazis, & Koufopavlou, 2007), which altogether set up a digital identity. So, Identity Management (IDM) becomes a very import function (Ahn & Lam, 2005) and it seems essential to protect the privacy of users in the electronic society (Clauβ, Kesdogan, & Kólsch, 2005) and to make them feel safe.

In order to better understand the existing risks, it is useful to have a look in the typical attacks effecting individuals in the e-world. The typical attacker tries to capture information that is confidential about a target, to gain some kind of advantage. Some examples are:

- Blackmailing: To extort money by threatening to discredit or to personal injure revealing sensitive information (Clauβ, Kesdogan, & Kólsch, 2005).
- Impersonate: Stealing the identity of the victims and communicate with society with their digital identity (Rashed, 2004).
- Denying Access: When attackers obtain the identity of the victims they might change the credentials so the victims will not be able to access their information anymore (Rashed & Santos, 2012).
- Identity Attack by Phishing: The act of luring the victims to provide their digital identity to rogue websites (Rashed, 2004).
- Password Attack: Users have many accounts (may reach 40) and frequently use the same password or very simple passwords, like "12345" (Imperva, 2010); so users may be fooled by simple guessing the password, by brute force (Madsen, Koga, & Takahashi, 2005).
- Privacy Attack: Attack may aim to disclosing private information against user willing (Clauβ, Kesdogan, & Kólsch, 2005).
- Databases Attack: Attacking the database to obtain sensitive information about individuals or companies, e.g., personal records, statistical databases, transaction databases, and unstructured knowledge bases (Clauβ, Kesdogan, & Kólsch, 2005) and (Rashed, 2004).
- Disclose Network Anonymity: To gain some information about users, attackers could break the anonymity to attack sensitive information or disclose the secrets.

Digital identity can be defined as the digital representation of the known information about a specific individual or organization (Squicciarini & Czeskis Bhargav-Spantzel, 2008). Being so, IDM is a set of business processes and a supporting infrastructure for creation, maintenance and use of digital identity. Besides the identification and authentication operations, an IDM is supposed to support other functions like: manage the identity information workflows, provide services like Single Sign-on (SSO); implement federation of several identities of an entity, etc. (Yan, Abouzakhar, Xiao, & Qayyam, 2009). An IDM System (IDMS) is a system that provides the control tools for managing the identity information and the amount of it that should be available for each interaction in electronic society (Clauβ, Kesdogan, & Kólsch, 2005).

The context where an IDMS is implemented depends largely on the set of networks and Information Systems involved, which naturally imposes different requirements. It is frequent to identify at least the following contexts: isolated, centralized, federated and personal. The isolated and personal models are very simple, but do not scale to distributed environments like the ones we are addressing here. The centralized model uses a single service provider where all identity information belonging to each entity is stored and verified; this type of control is usually efficient, but considering large networks the service provider it is a single point of failure, which is a relevant drawback. Finally, the federated model allows for several service providers to store and manage application or service specific user's attributes, but maintaining them linked

through an Identity Provider, where users can keep and control personal information, giving access to just is needed by each service provider (Yan, Abouzakhar, Xiao, & Qayyam, 2009).

Currently there are many IDM protocols, systems, specifications and supporting languages. Among them it should be highlighted (Yan, Abouzakhar, Xiao, & Qayyam, 2009): SAML (Security Assertion Markup Language; Liberty Alliance Specification, split by several aspects of IDM application; XACML (Extensible Access Control Markup Language); Shibboleth (an implementation of SAML v1.1); WS-Federation; OpenID; LID (Light-Weight Identity; XRIs (Extensible Resource Identifiers; and Windows Cardspace.

Despite the benefits of each approach, there is no one-size-fits-all solution and it still remains difficult problems to solve. The first one is the lack of interoperability of the above platforms, which imposes serious limitations to large scale adoption. Secondly, most of the solution available performs well in a given context, but not so well on others. This is because the IDM functions are different in different contexts, e.g., at the network-level, or at the service-level. Related with this, another important issue is the inexistence of a common identity model, which can be used at different levels – for instances, we can easily envisage a SSO solution for the Internet, where a given set of system trust on a central Identity Provider, but this is almost impossible to deploy at the local network level, since there are a lot of local services that will never recognize that same mechanism for authentication. IDM systems also deal with a large set of issues concerning the privacy and other social values that are not equal for everyone in the e-world. To figure out the real extension of the IDM effect, it is useful to list the identity management issues by different dimensions (Madsen, Koga, & Takahashi, 2005) and (Rashed & Santos, 2012):

- Technical issues: Concerning the infrastructure to support an IDMS.
- Legal system: Especial legislation for data protection.
- Information police: For dealing with identity theft.
- Social and humanity: Dealing with issues such as privacy.
- Security components: Such as access control.
- Participating organizations.

But even with their limitations, IDM frameworks can help users to mitigate the risks associated with the attacks listed, or the awful effects they may cause. The advantage of this especial issue is that it covers different aspects of IDM problems starting with assessment and analysis. Thus the solutions come in parallel with problems and suggest frameworks protocols.

REFERENCES

Ahn, G., & Lam, J. (2005). Managing privacy preferences for federated identity management. In *Proceedings of the Workshop on Digital Identity Management*, Fairfax, VA (pp. 28-36).

Boudriga, N., Baghdadi, M., & Obaidat, M. (2006). A new scheme for mobility, sensing, and security management in wireless ad hoc sensor networks. In *Proceedings of the 39th Annual Simulation Symposium*.

Casassa Mont, M., & Thyne, R. (2006). Privacy policy enforcement in enterprises with identity management solutions. In *Proceedings of the International Conference on Privacy, Security and Trust: Bridge the Gap between PST Technologies and Business Services*, Markham, ON, Canada (Vol. 380).

Clauβ, S., Kesdogan, D., & Kólsch, T. (2005). Privacy enhancing identity management: Protection against re-identification and profiling. In *Proceedings of the Workshop on Digital Identity Management*, Fairfax, VA (pp. 84-93).

Dabrowski, M., & Pacyna, P. (2008). Overview of identity management. *China Communications*, *5*, 129-142.

Higby, C., & Bailey, M. (2008, October 28-30). Wireless security patch management system. In *Proceedings of the 5th Conference on Information Technology Education*, Salt Lake City, UT (pp. 165-168).

Imperva. (2010). *Consumer password worst practices*. Redwood Shores, CA: Author. Retrieved from_http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf

Keshariya, M., & Hunt, R. (2008, September 10-12). A new architecture for performance-based policy management in heterogeneous wireless networks. In *Proceedings of the International Conference on Mobile Technology, Applications & Systems*, Ilan, Taiwan (p. 97).

Madsen, P., Koga, Y., & Takahashi, K. (2005). Federated identity management for protecting users from ID theft. In *Proceedings of the Workshop on Digital Identity Management*, Fairfax, VA (pp. 77-83).

Rashed, A. (2004). *Intelligent encryption decryption systems using genetic algorithms* (Unpublished doctoral dissertation). Arab Academy, Amman, Jordan.

Rashed, A., & Santos, H. (2012). Wireless identity management: Multimodal biometrics and multi-layered ID. In H. Al-Bahadili (Ed.), *Simulation in computer network design and modeling: Use and analysis* (pp. 284-296). Hershey, PA: IGI Global.

Sklavos, N., Denazis, S., & Koufopavlou, O. (2007). AAA and mobile networks: Security aspects and architectural efficiency. In *Proceedings of the Third International Conference on Mobile Multimedia Communications*, Nafpaktos, Aitoloakarnania, Greece.

Squicciarini, A., & Czeskis Bhargav-Spantzel, A. (2008). Privacy policies compliance across digital identity management systems. In *Proceedings of the SIGSPATIAL ACM GIS International Workshop on Security and Privacy in GIS and LBS* (pp. 72-81).

Taylor, D. S. (2001). *Multi-layered approach to small office networking*. Retrieved from http://www.sans.org/.../hsoffice/multilayered_approach_to_small_office_networking_624

Yan, L., Abouzakhar, N., Xiao, H., & Qayyam, R. (2009, June 21-24). Multimodal security enforcement framework for wireless ad hoc networks. In *Proceedings of the International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, Leipzig, Germany (pp. 921-925).