Continuous and Transparent User Authentication for Secure Internet Services

T.L.Priyadarsini[1], M.Swathi[2], M.Prakash[3]

Asst.Prof, Dept.of Computer Science and Engineering, VNRVJIET, Telangana, India

4th B.Tech, Dept.of Computer Science and Engineering, VNRVJIET, Telangana, India

4th B.Tech, Dept.of Computer Science and Engineering, VNRVJIET, Telangana, India

---***---

Abstract - *Session management in distributed Internet services is traditionally based on username and password, explicit logouts and mechanisms of user session expiration using classic timeouts. Emerging biometric solutions allow substituting username and password with biometric data during session establishment, but in such an approach still a single verification is deemed sufficient, and the identity of a user is considered immutable during the entire session. Additionally, the length of the session timeout may impact on the usability of the service and consequent client satisfaction. This paper explores promising alternatives offered by applying biometrics in the management of sessions. A secure protocol is defined for perpetual authentication through continuous user verification. The protocol determines adaptive timeouts based on the quality, frequency and type of biometric data transparently acquired from the user. The functional behavior of the protocol is illustrated through Mat lab simulations, while model-based quantitative analysis is carried out to assess the ability of the protocol to contrast security attacks exercised by different kinds of attackers. Finally, the current prototype for PCs and Android smartphones is discussed.*

Key Words: **functional behaviour, attackers, session expiration, biometric data, Session management, etc.…**

1. INTRODUCTION

What is Secure Computing?

Computer security (Also known as cyber security or IT Security) is information security as applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters. Otherwise, in the computer industry, the term security -- or the phrase computer security -- refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

Fig 1 the Secure Computing

Working conditions and basic needs in the secure computing: If you don't take basic steps to protect your work computer, you put it and all the information on it at risk. You can potentially compromise the operation of other computers on your organization's network, or even the functioning of the network as a whole.

1.1. Physical Security:

Technical measures like login passwords, anti-virus are essential. (More about those below) However, a secure physical space is the first and more important line of defense. Is the place you keep your workplace computer secure enough to prevent theft or access to it while you are away? While the Security Department provides coverage across the Medical center, it only takes seconds to steal a computer, particularly a portable device like a laptop or a PDA. A computer should be secured like any other valuable possession when you are not present.

Human threats are not the only concern. Computers can be compromised by environmental mishaps (e.g., water, coffee) or physical trauma. Make sure the physical location of your computer takes account of those risks as well.

1.1.1. Access Passwords:

The University's networks and shared information systems are protected in part by login credentials (user-IDs and passwords). Access passwords are also an essential protection for personal computers in most circumstances. Offices are usually open and shared spaces, so physical access to computers cannot be completely controlled.

To protect your computer, you should consider setting passwords for particularly sensitive applications resident on the computer (e.g., data analysis software), if the software provides that capability.

1.2. Prying Eye Protection:

Because we deal with all facets of clinical, research, educational and administrative data here on the medical campus, it is important to do everything possible to minimize exposure of data to unauthorized individuals.

1.2.1. Anti-virus Software:

Up-to-date, properly configured anti-virus software is essential. While we have server-side anti-virus software on our network computers, you still need it on the client side (your computer).

1.2.2. Firewalls:

Anti-virus products inspect files on your computer and in email. Firewall software and hardware monitor communications between your computer and the outside world. That is essential for any networked computer.

1.2.3. Software updates:

It is critical to keep software up to date, especially the operating system, anti-virus and anti-spyware, email and browser software. The newest versions will contain fixes for discovered vulnerabilities.

Almost all anti-virus have automatic update features (including SAV). Keeping the "signatures" (digital patterns) of malicious software detectors up-to-date is essential for these products to be effective.

1.2.4. Keep Secure Backups:

Even if you take all these security steps, bad things can still happen. Be prepared for the worst by making backup copies of critical data, and keeping those backup copies in a separate, secure location. For example, use supplemental hard drives, CDs/DVDs, or flash drives to store critical, hard-to-replace data.

1.2.5. Report problems:

If you believe that your computer or any data on it has been compromised, you should make an information security incident report. That is required by University policy for all data on our systems, and legally required for health, education, financial and any other kind of record containing identifiable personal information.

1.3. Benefits of Secure Computing:

a. Protect Yourself—Civil Liability:

You may be held legally liable to compensate a third party should they experience financial damage or distress as a result of their personal data being stolen from you or leaked by you.

b. Protect your credibility--Compliance:

You may require compliancy with the Data Protection Act, the FSA, SOX or other regulatory standards. Each of these bodies stipulates that certain measures be taken to protect the data on your network.

c. Protect your Reputation–Spam:

A common use for infected systems is to join them to a botnet (a collection of infected machines which takes orders from a command server) and use them to send out spam. This spam can be traced back to you, your server could be blacklisted and you could be unable to send email.

d. Protect your income—Competitive Advantage:

There are a number of "hackers-for-hire" advertising their services on the internet selling their skills in breaking into company's servers to steal client databases, proprietary software, merger and acquisition information, personnel detail set.

e. Protect your Business–Blackmail:

A seldom-reported source of income for "hackers" is to break into your server, change all your passwords and lock you out of it. The password is then sold back to you. Note: the "hackers" may implant a backdoor program on your server so that they can repeat the exercise at will.

f. Protect your Investment—Free Storage:

Your server's hard drive space is used (or sold on) to house the hacker's video clips, music collections, pirated software or worse. Your server or computer then becomes continuously slow and your internet connection speeds deteriorate due to the number of people connecting to your server in order to download the offered wares.

2. SYSTEM ANALYSIS:

2.1 Existing System:

Once the user's identity has been verified, the system resources are available for a fixed period of time or until explicit logout from the user. This approach assumes that a single verification (at the beginning of the session) is sufficient, and that the identity of the user is constant during the whole session.

In existing, a multi-modal biometric verification system is designed and developed to detect the physical presence of the user logged in a computer.

The work in another existing paper, proposes a multi-modal biometric continuous authentication solution for local access to high-security systems as ATMs, where the raw data acquired are weighted in the user verification process, based on i) type of the biometric traits and ii) time, since different sensors are able to provide raw data with different timings. Point ii) introduces the need of a temporal integration method which depends on the availability of past observations: based on the assumption that as time passes, the confidence in the acquired (aging) values decreases. The paper applies a degeneracy function that measures the uncertainty of the score computed by the verification function.

2.1.1. Limitations of Existing System:

a. None of existing approaches supports continuous authentication.
b. Emerging biometric solutions allow substituting username and password with biometric data during session establishment, but in such an approach still a single verification is deemed sufficient, and the identity of a user is considered immutable during the entire session.

2.2. Proposed System:

This paper presents a new approach for user verification and session management that is applied in the context aware security by hierarchical multilevel architectures (CASHMA) system for secure biometric authentication on the Internet.

CASHMA is able to operate securely with any kind of web service, including services with high security demands as online banking services, and it is intended to be used from different client devices, e.g., smartphones, Desktop PCs or even biometric kiosks placed at the entrance of secure areas. Depending on the preferences and requirements of the owner of the web service, the CASHMA authentication service can complement a traditional authentication service, or can replace it.

Our continuous authentication approach is grounded on transparent acquisition of biometric data and on adaptive timeout management on the basis of the trust posed in the user and in the different subsystems used for authentication. The user session is open and secure despite possible idle activity of the user, while potential misuses are detected by continuously confirming the presence of the proper user.

2.2.1. Advantages of Proposed System:

a. Our approach does not require that the reaction to a user verification mismatch is executed by the user device (e.g., the logout procedure), but it is transparently handled by the CASHMA authentication service and the web services, which apply their own reaction procedures.
b. Provides a tradeoff between usability and security.

3. LITERATURE SURVEY:

3.1. Quantitative Security Evaluation of a Multi-Biometric Authentication System:

Authors: L. Montecchi, P. Lollini, A. Bondavalli, and E. La Mattina,
Biometric authentication systems verify the identity of users by relying on their distinctive traits, like fingerprint, face, iris, signature, voice, etc. Biometrics is commonly perceived as a strong authentication method; in practice several well-known vulnerabilities exist, and security aspects should be carefully considered, especially when it is adopted to secure the access to applications controlling critical systems and infrastructures. In this paper we perform a quantitative security evaluation of the CASHMA multi-biometric authentication system, assessing the security provided by different system configurations against attackers with different capabilities. The analysis is performed using the ADVISE modeling formalism, a formalism for security evaluation that extends attack graphs; it allows to combine information on the system, the attacker, and the metrics of interest to produce quantitative results. The obtained results provide useful insight on the security offered by the different system configurations, and demonstrate the feasibility of the approach to model security threats and countermeasures in real scenarios.

3.2. Model-Based Evaluation of Scalability and Security Tradeoffs:

Authors: L. Montecchi, N. Nostro, A. Ceccarelli, G. Vella, A. Caruso, and A. Bondavalli
Current ICT infrastructures are characterized by increasing requirements of reliability, security, performance, availability, adaptability. A relevant issue is represented by the scalability of the system with respect to the increasing number of users and applications, thus requiring a careful dimensioning of resources. Furthermore, new security issues to be faced arise from exposing applications and data to the Internet, thus requiring an attentive analysis of potential threats and the identification of stronger security mechanisms to be implemented, which may produce a negative impact on system performance and scalability properties. The paper presents a model-based evaluation of scalability and security tradeoffs of a multi-service web-based platform, by evaluating how the introduction of security mechanisms may lead to a degradation of performance properties. The evaluation focuses on the

OPENNESS platform, a web-based platform providing different kind of services, to different categories of users. The evaluation aims at identifying the bottlenecks of the system, under different configurations, and assess the impact of security countermeasures which were identified by a thorough threat analysis activity previously carried out on the target system. The modeling activity has been carried out using the Stochastic Activity Networks (SANs) formalism, making full use of its characteristics of modularity and reusability. The analysis model is realized through the composition of a set of predefined template models, which facilitates the construction of the overall system model, and the evaluation of different configuration by composing them in different ways.

3.3. Attacks on Biometric Systems: A Case Study on Fingerprints:

Authors: U. Uludag and A.K. Jain
In spite of numerous advantages of biometrics-based personal authentication systems over traditional security systems based on token or knowledge, they are vulnerable to attacks that can decrease their security considerably. In this paper, we analyze these attacks in the realm of a fingerprint biometric system. We propose an attack system that uses a hill climbing procedure to synthesize the target minutia templates and evaluate its feasibility with extensive experimental results conducted on a large fingerprint database. Several measures that can be utilized to decrease the probability of such attacks and their ramifications are also presented.

3.4. Automated Generation and Analysis of Attack Graphs:

Authors: O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing .
An integral part of modeling the global view of network security is constructing attack graphs. Manual attack graph construction is tedious, error-prone, and impractical for attack graphs larger than a hundred nodes. In this paper we present an automated technique for generating and analyzing attack graphs. We base our technique on symbolic model checking algorithms, letting us construct attack graphs automatically and efficiently. We also describe two analyses to help decide which attacks would be most cost-effective to guard against. We implemented our technique in a tool suite and tested it on a small network example, which includes models of a firewall and an intrusion detection system.

3.5. Risk-Based Security Engineering through the Eyes of the Adversary:

Authors: S. Evans and J. Wallner

Today, security engineering for complex systems is typically done as an ad hoc process. Taking a risk-based security engineering approach replaces today's ad hoc methods with a more rigorous and disciplined approach that uses a multi-criterion decision model. This approach builds on existing techniques for integrating risk analysis with classical systems engineering. A resulting security metric can be compared with cost and performance metrics in making engineering trade-off decisions.

4. SYSTEM MODEL:

In this module, we create the System model to evaluate and implement our proposed system. CASHMA can authenticate to web services, ranging from services with strict security requirements as online banking services to services with reduced security requirements as forums or social networks. Additionally, it can grant access to physical secure areas as a restricted zone in an airport, or a military zone (in such cases the authentication system can be supported by biometric kiosk placed at the entrance of the secure area). We explain the usage of the CASHMA authentication service by discussing the sample application scenario, where a user wants to log into an online banking service.

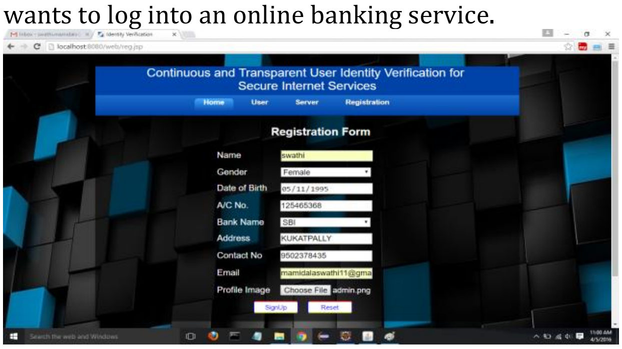

Fig 2 New User Registration Form

"**User Name**" refers to the identity of the user obtained from the Bank for the purpose of logging into the Internet Banking facility provided by the Bank.
"**Login Password**" is a unique and randomly generated password known only to the customer, which can be changed by the user to his/her convenience. This is a means of authenticating the user ID for logging into Internet Banking."

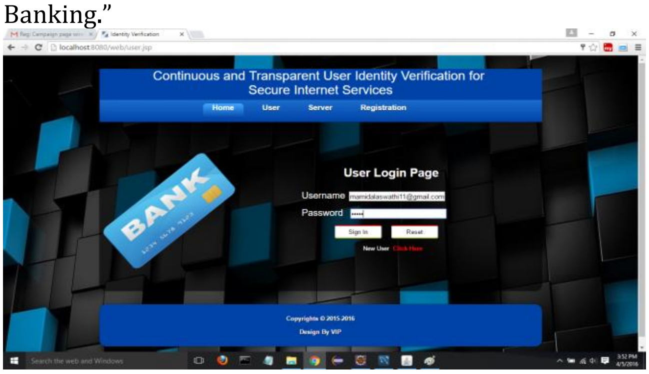

Fig 3 Login Page to authenticate the user

Transaction Password" is a unique and randomly generated password known only to the customer, which can be changed to his/her convenience. This is a means of authentication required to be provided by the customer for putting through the transaction in his/her/their/its accounts with Bank through Internet Banking. While User ID and Password are for valid access into the internet application, giving valid Transaction Password is for authentication of transaction/requests made through internet.

5. AUTHENTICATION SERVER:

In Internet banking as with traditional banking methods, security is a primary concern. Server will take every precaution necessary to be sure your information is transmitted safely and securely. The latest methods in Internet banking system security are used to increase and monitor the integrity and security of the system.

The Server maintains the functionality:

b. Customer Details
c. Activation of Beneficiary
d. Transaction Details
e. Activate Blocked Account

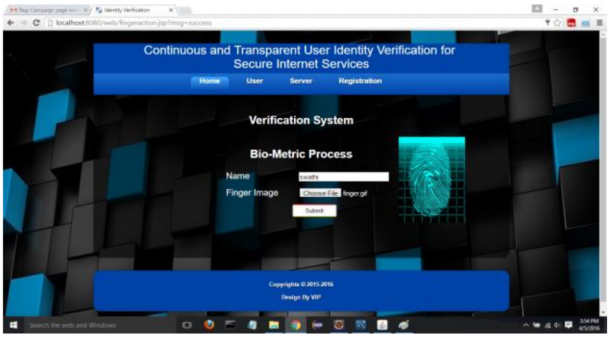

Fig 4 Biometric Verification for Authentication

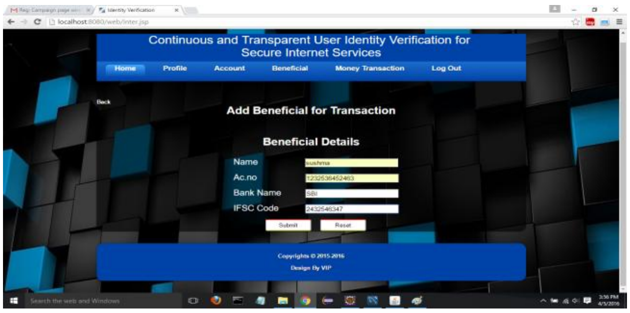

Fig 5 Adding Beneficial Data for Transaction

6. CASHMA CERTIFICATE:

In this module, we present the information contained in the body of the CASHMA certificate transmitted to the client by the CASHMA authentication server, necessary to understand details of the protocol. Time stamp and sequence number univocally identify each certificate, and protect from replay attacks. ID is the user ID, e.g., a number.

Decision represents the outcome of the verification procedure carried out on the server side. It includes the expiration time of the session, dynamically assigned by the CASHMA authentication server. In fact, the global trust level and the session timeout are always computed considering the time instant in which the CASHMA application acquires the biometric data, to avoid potential problems related to unknown delays in communication and computation.

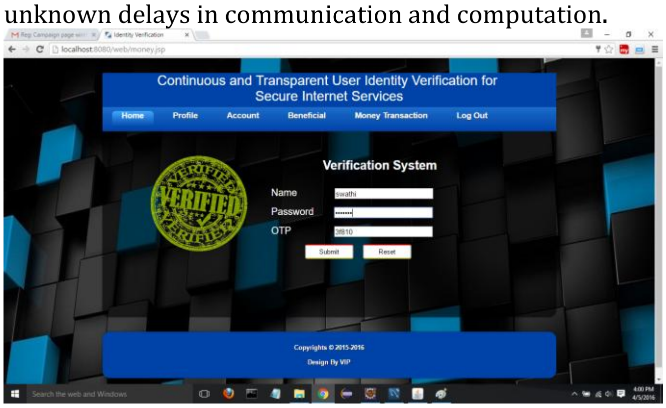

Fig 6 Verification through One Time Password

7. CONTINUOUS AUTHENTICATION:

A secure protocol is defined for perpetual authentication through continuous user verification. The protocol determines adaptive timeouts based on the quality, frequency and type of biometric data transparently acquired from the user. The use of biometric authentication allows credentials to be acquired transparently, i.e., without explicitly notifying the user or requiring his/her interaction, which is essential to guarantee better service usability.

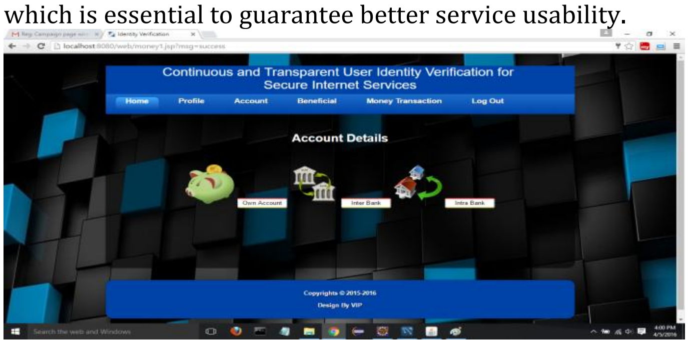

Fig 7 Type of Account Details that can be considered

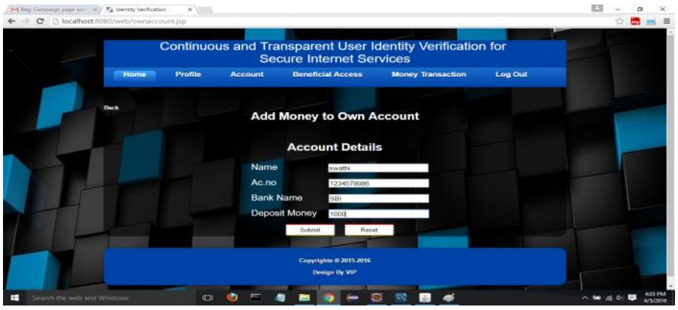

Fig 8 Adding Money to Own Account

The idea behind the execution of the protocol is that the client continuously and transparently acquires and transmits evidence of the user identity to maintain access to a web service. The main task of the proposed protocol is to create and then maintain the user session adjusting the session timeout on the basis of the confidence that the identity of the user in the system is genuine.

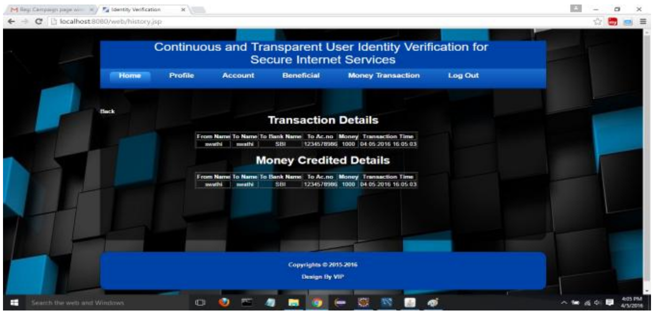

Fig 9 Transaction Details of Credited Account

8. CONCLUSION:

We exploited the novel possibility introduced by biometrics to define a protocol for continuous authentication that improves security and usability of user session. The protocol computes adaptive timeouts on the basis of the trust posed in the user activity and in the quality and kind of biometric data acquired transparently through monitoring in background the user's actions. Some architectural design decisions of CASHMA are here discussed. First, the system exchanges raw data and not the features extracted from them or templates, while crypto-token approaches are not considered; this is due to architectural decisions where the client is kept very simple. We remark that our proposed protocol works with no changes using features, templates or raw data. Second, privacy concerns should be addressed considering National legislations.

9. ACKNOWLEDGEMENT:

We are thankful to the Management and Principal of VNR Vignana Jyothi Institute of Engineering and Technology for providing their support and facilities such as labs, soft wares etc. needed to carry out this work.

10. REFERENCES:

[1] CASHMA-Context Aware Security by Hierarchical Multilevel Architectures, MIUR FIRB, 2005.

[2] L. Hong, A. Jain, and S. Pankanti, "Can Multibiometrics Improve Performance?" Proc. Workshop on Automatic Identification Advances Technologies (AutoID '99) Summit, pp. 59-64, 1999.

[3] S. Ojala, J. Keinanen, and J. Skytta, "Wearable Authentication Device for Transparent Login in Nomadic Applications Environment," Proc. Second Int'l Conf. Signals, Circuits and Systems (SCS '08), pp. 1-6, Nov. 2008.

[4] BioID "Biometric Authentication as a Service (BaaS)," BioID Press Release, https://www.bioid.com, Mar. 2011.

[5] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous Verification Using Multimodal Biometrics," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 687-700, Apr. 2007.

[6] L. Montecchi, P. Lollini, A. Bondavalli, and E. La Mattina, "Quantitative Security Evaluation of a Multi-Biometric Authentication System," Proc. Int'l Conf. Computer Safety, Reliability and Security, pp. 209-221, 2012.

[7] S. Kumar, T. Sim, R. Janakiraman, and S. Zhang, "Using Continuous Biometric Verification to Protect Interactive Login Sessions," Proc. 21st Ann. Computer Security Applications Conf. (ACSAC '05), pp. 441-450, 2005.

[8] A. Altinok and M. Turk, "Temporal Integration for Continuous Multimodal Biometrics," Proc. Workshop Multimodal User Authentication, pp. 11-12, 2003.

[9] C. Roberts, "Biometric Attack Vectors and Defences," Computers & Security, vol. 26, no. 1, pp. 14-25, 2007.

[10] S.Z. Li and A.K. Jain, Encyclopedia of Biometrics. first ed., Springer, 2009.

[11] U. Uludag and A.K. Jain, "Attacks on Biometric Systems: A Case Study in Fingerprints," Proc. SPIE-EI 2004, Security, Steganography and Watermarking of Multimedia Contents VI, vol. 5306, pp. 622-633, 2004.

[12] E. LeMay, W. Unkenholz, D. Parks, C. Muehrcke, K. Keefe, and W.H. Sanders, "Adversary-Driven State-Based System Security Evaluation," Proc. the Sixth Int'l Workshop Security Measurements and Metrics (MetriSec '10), pp. 5:1-5:9, 2010.

[13] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing, "Automated Generation and Analysis of Attack Graphs," Proc. IEEE Symp. Security and Privacy, pp. 273-284, 2002.

[14] D.M. Nicol, W.H. Sanders, and K.S. Trivedi, "Model-Based Evaluation: From Dependability to Security," IEEE Trans. Dependable and Secure Computing, vol. 1, no. 1, pp. 48-65, Jan.-Mar. 2004.

[15] T. Courtney, S. Gaonkar, L. Keefe, E.W.D. Rozier, and W.H. Sanders, "M€obius 2.3: An Extensible Tool for Dependability, Security, and Performance Evaluation of Large and Complex System Models," Proc. IEEE/IFIP Int'l Conf. Dependable Systems & Networks (DSN '09), pp. 353-358, 2009.

[16] W.H. Sanders and J.F. Meyer, "Stochastic Activity Networks: Formal Definitions and Concepts," Lectures on Formal Methods and Performance Analysis, pp. 315-343, Springer-Verlag, 2002.

[17] T. Casey, "Threat Agent Library Helps Identify Information Security Risks,," White Paper, Intel Corporation, Sept. 2007.

[18] A. Ceccarelli, A. Bondavalli, F. Brancati, and E. La Mattina, "Improving Security of Internet Services through Continuous and Transparent User Identity Verification," Proc. Int'l Symp. Reliable Distributed Systems (SRDS), pp. 201-206, Oct. 2012.

[19] Adobe Products List, http://www.adobe.com/products, 2014.

[20] T.F. Dapp, "Growing Need for Security in Online Banking: Biometrics Enjoy Remarkable Degree of Acceptance,," Banking & Technology Snapshot, DB Research, Feb. 2012.

[21] A.K. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Trans. Information Forensics and Security, vol. 1, no. 2, pp. 125-143, June 2006.

[22] L. Allano, B. Dorizzi, and S. Garcia-Salicetti, "Tuning Cost and Performance in Multi-Biometric Systems: A Novel and Consistent View of Fusion Strategies Based on the Sequential Probability Ratio Test (SPRT)," Pattern Recognition Letters, vol. 31, no. 9, pp. 884-890, 2010.

[23] S. Evans and J. Wallner, "Risk-Based Security Engineering through the Eyes of the Adversary," Proc. the IEEE Workshop Information Assurance, pp. 158-165, June 2005.

[24] M. Afzaal, C. Di Sarno, L. Coppolino, S. D'Antonio, and L. Romano, "A Resilient Architecture for Forensic Storage of Events in Critical Infrastructures," Proc. Int'l Symp. High-Assurance Systems Eng. (HASE), pp. 48-55, 2012.

[25] M. Cinque, D. Cotroneo, R. Natella, and A. Pecchia, "Assessing and Improving the Effectiveness of Logs for the Analysis of Software faults," Proc. Int'l Conf. Dependable Systems and Networks (DSN), pp. 457-466, 2010.

[26] N. Mendes, A.A. Neto, J. Duraes, M. Vieira, and H. Madeira, "Assessing and Comparing Security of Web Servers," Proc. IEEE Int'l Symp. Dependable Computing (PRDC), pp. 313-322, 2008.

[27] L. Montecchi, N. Nostro, A. Ceccarelli, G. Vella, A. Caruso, and A. Bondavalli, "Model-based evaluation of scalability and security tradeoffs: A case study on a multi-service platform," Electronic.