Quantitative Security Evaluation of a Multi-biometric Authentication System

Leonardo Montecchi[1], Paolo Lollini[1], Andrea Bondavalli[1], and Ernesto La Mattina[2]

[1] University of Florence, 50134 Firenze, Italy
{lmontecchi,lollini,bondavalli}@unifi.it
[2] Engineering Ingegneria Informatica S.p.A., 90146 Palermo, Italy
ernesto.lamattina@eng.it

Abstract. 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.

Keywords: quantitative security evaluation, multimodal biometric authentication, modeling, ADVISE, CASHMA.

1 Introduction

Biometric authentication systems verify the identity of users by relying on their distinctivetraits like fingerprint, face, iris, signature, voice, etc. Even though biometrics is commonly perceived as a strong authentication technique, several well-known vulnerabilities exist in practice, potentially allowing attackers to substitute themselves to legitimate users of the system. As the adoption of biometric systems is spreading in real world applications, multi-biometric systems are starting to receive considerable attention. Such kind of systems combine multiple biometric traits to verify user identities, trying to overcome some of the limitations of unimodal systems, such as noisy data, intraclass variation, non-universality, and susceptibility to spoofing attacks [1]. Security aspects are of major importance in such systems, especially when biometric authentication is adopted to secure the access to applications controlling critical systems or infrastructures. The recent "Stuxnet" worm attack [2] shows that facing modern attackers requires to take into

F. Ortmeier and P. Daniel (Eds.): SAFECOMP 2012 Workshops, LNCS 7613, pp. 209–221, 2012.

account several aspects during security analysis, including skills and motivation of attackers, system knowledge, and human factors.

In this paper we perform a quantitative security evaluation of the multi-biometric authentication system defined within the CASHMA project [3], assessing the security provided by different system configurations against different attackers. The analysis is performed using the recently introduced ADVISE modeling formalism [4], which is especially tailored to quantitative security evaluation. The contribution of this work is twofold: on one hand we evaluate quantitative metrics that allow to compare different security configurations of the target system; on the other hand we describe one of the first applications of ADVISE for the analysis of a more comprehensive system, with the aim to assess its capabilities to represent security aspects in a real scenario.

The paper is organized as follows. Section 2 reviews related work, while Section 3 describes the CASHMA system and the scenario under analysis, discussing some of the major security threats. Section 4 provides a brief description of the ADVISE formalism, and then describes the model that will be used for evaluations. Evaluations and results are discussed in Section 5. Finally, conclusions are drawn in Section 6.

2 Related Work

Many works on the evaluation of biometric systems focus on the performance of the matching process, which compares the data acquired from sensors with reference samples associated with enrolled users. Two main quantities are usually considered: the rate of wrongly accepted matches (False Accept Rate, FAR), and the rate of wrongly rejected matches (False Reject Rate, FRR) [1,5]. Since the first measure provides a quantification of potentially unauthorized accesses, it is often used to quantify the security of the overall system. It is however believed that such simple indicators are no longer appropriate, and that more comprehensive evaluation frameworks taking into account the security of the system as a whole are needed [6].

Our approach uses model-based analysis to evaluate security measures of an overall biometric system. Model-based analysis has been extensively used for dependability analysis, and it has been later adopted in security analysis as well [7]. An abstraction of the system is created and then used to evaluate measures, verify properties, or identify possible issues on the system. One of the first formal models introduced for security analysis is the Dolev-Yao model [8], which is commonly used to verify properties of cryptographic protocols through semi-automatic tools like CASPER [9]. Attack trees [10] allow to describe the possible ways in which an attacker can compromise the system, and they are extensively used to model the security of the system as a whole; however they do not have the notion of time, and cannot be used to express complex dependencies between events. Attack graphs [11] extend attack trees by introducing the notion of state, thus allowing to describe more complex interactions between events and attacks. Other approaches use classic formalism borrowed from reliability analysis such as Stochastic Petri Nets and their extensions [12].

The ADVISE formalism, which has been recently introduced in [4,13], extends the attack graph concept, taking into account the attack behavior and capabilities of

different kind of attackers. Support for the formalism is going to be provided by future versions of the Möbius multi-formalism modeling framework [14]; currently, support is provided by an "alpha" (i.e., in development) version of the tool. To the best of our knowledge, the only case study that applies the ADVISE method is described in [4,13], where a SCADA system is analyzed.

3 Targeted System and Scenario

The purpose of the CASHMA system is to provide an authentication service, which operates as a bridge between users that need to access to a given application, and applications that require secure access control. The core elements of the CASHMA architecture are the authentication server and the template database, in which samples of biometric data ("templates") are stored. Different kind of biometric sensors, located on the client, are used to acquire user biometric data. When users need to access to a certain application, their biometric traits are acquired and transmitted to the authentication service, which compares them with the templates stored in the database. If authentication is successful, the user is provided with a certificate that can be used to access the application(s). The CASHMA authentication service supports very different kind of applications, including those with high security constraints (e.g., kiosks securing the access to critical infrastructures management facilities), but also entertainment and informational applications. The main assumption on client devices is that they have the only role of acquiring biometric data, while all the processing and comparison tasks are performed server-side.

3.1 Security Threats to Biometric Authentication Systems

Although common sense would suggest that biometrics provides a very high degree of security, there are actually several means for attackers to compromise a biometric system. For example, data acquired from biometric sensors during the authentication of a legitimate user can be logged and later reused by the attacker, in a similar way as logging keystrokes allows to obtain passwords typed at a terminal. Another option is to create an artificial biometric sample, which is actually feasible with common materials even for those considered strong biometric traits, like fingerprint [15] or even iris [16]. In the following we list some of the vulnerabilities that have been identified for the CASHMA authentication service, briefly discussing how they could be exploited by an attacker and which are the possible countermeasures. Such list has been used as a basis in the construction of the analysis model.

Denial of service (DoS) attacks are designed to corrupt or incapacitate the biometric sensors, and can consist in physical damage, power loss, or introducing adverse environmental conditions to degrade the quality of the acquired data. Using *fake physical biometric*, also known as *sensor spoofing*, consists in using counterfeit physical biometrics to circumvent the biometric system. This is one of the most convenient attacks to this kind of systems: little system knowledge is required, involved materials are usually common and cheap, and most digital countermeasures (e.g., data

encryption) are bypassed. Copies of legitimate biometrics can be obtained with relatively low effort: fingerprints are left on many things we touch; face and voice are easily recorded. Countermeasures to this kind of attack are "liveness detection" mechanisms [1], i.e., mechanisms looking for life indicators, like heartbeat or eye movement.

Reuse of residuals exploits the fact that some biometric devices may hold the last few acquired samples in some kind of local memory. If an attacker gains access to this data, he may be able to reuse it to provide a valid biometric sample. Countermeasures to this attack include clearing memory and forbidding perfectly identical biometric samples. *Replay attacks* involve the communication between the sensor and the processing resource that performs the comparison. A replay attack is composed of at least two stages: first an authentic communication is intercepted (*eavesdropping*), then it is replayed when needed, possibly modifying its content in accordance with the objectives of the attacker. Data encryption and digital signatures offer significant protection against this kind of attack. Finally, *template modification* consists in directly altering the template database, and it is one of the most serious threats to biometric systems: it potentially allows an attacker to obtain unauthorized access by simply presenting its real biometrics, and substituting to any of the legitimate users of the system. Countermeasures to this kind of attack include strict access policies to the template database, as well as encryption and digital signature for database content.

The attacks that an adversary may attempt obviously depend on the system architecture; a more comprehensive list of threats to biometric systems can be found in [1] and [17]. Finally, it should be noted that one of the most valuable resources for an attacker is the collaboration, or the coercion, of a legitimate user of the system.

3.2 Scenario Description and Analysis Objectives

The scenario that we consider in our analysis is an instance of the CASHMA system, supporting three biometric traits: voice, face, and fingerprint. The authentication server and the template database reside on a private network, protected from the Internet by a firewall. Communication between the client and the authentication server uses an encrypted logical channel (e.g., the SSL/TLS protocol [18]).

No assumptions are made on the kind of application(s) to which the authentication service provides access. Consequences of unauthorized access depend on the actual application, and potentially include catastrophic events in case of critical infrastructures control systems. Therefore, we focus on security attributes of the authentication service, and consider the time that it takes for an attacker to obtain unauthorized access as the main indicator of system security. In particular, we evaluate:

- $P_E(t)$: Probability that, at time t, the attacker has been successfully authenticated.
- T_E: Mean time required to the attacker to obtain authentication.

In our analysis we will compare three different system configurations, which have been identified as representative alternatives within the project:

1. User authentication requires only two of the three supported biometric traits. This configuration allows to trade security for broader client support: the absence of one sensor (e.g., fingerprint reader on mobile phones) or bad environment conditions (e.g., low light or noise) will still allow authentication by using the remaining sensors. The acquired biometric data is transmitted using a single encryption key.
2. User authentication requires all the supported biometric traits. The acquired biometric data is transmitted using a single encryption key.
3. User authentication requires all the supported biometric traits, and the biometric data is transmitted using three separate encryption keys.

The three above configuration variants are intended for systems having different security requirements, and aim to provide an increasing level of security, with #1 being the least secure configuration, and #3 being the most secure. It is assumed that the system is subject to different kind of attackers, distinguished by the knowledge they have of the system, the elements they can access, and their skills. Our objective is to assess the ability of above configuration to contrast the different attackers.

A realistic characterization of attackers is a challenging task for system-level security analysis; a common technique for network-based systems is the use of "honeypots", i.e. intentionally low protected machines exposed on public networks to attract attackers and analyze their actions (e.g., see [19]). This approach is however less practical when non-network-based attacks are considered. In our analysis we consider a representative set of attackers, covering different abilities, knowledge, and accesses. The detailed definition of the different attacker profiles is provided in Section 4.2.

4 Modeling Approach

This section describes how the system has been modeled using ADVISE. Section 4.1 briefly introduces the formalism, while Section 4.2 describes the model itself.

4.1 The ADVISE Formalism

The analysis method supported by the ADVISE [4,13] formalism relies on creating executable security models that can be solved using discrete-event simulation to provide quantitative metrics. One of the most significant features introduced by this formalism is the precise characterization of the attacker (the "adversary") and the influence of its decisions on the final measures of interest. In fact, the overall security of a system is influenced not only by its actual strength in contrasting intrusion attempts, but also by its strength as *perceived* by attackers.

The specification of an ADVISE model is composed of two parts: an Attack Execution Graph (AEG), describing how the adversary can attack the system, and an adversary profile, describing the characteristics of the attacker. The AEG is a particular kind of attack graph comprising different kinds of nodes: *attack steps*, *access domains*, *knowledge items*, *attack skills*, and *attack goals*. Similarly as in attack graphs, attack steps describe the possible attacks that the adversary may attempt. Access domains describe what the attacker needs to possess (e.g., intranet access), while

knowledge items describe what it needs to know (e.g., admin passwords); attack skills describe the proficiency of the adversary in certain abilities; attack goals describe its objectives. Each attack step requires a certain combination of items to be held by the adversary. The set of what has been achieved by the adversary defines the current state of the model. Differently from other attach graphs, ADVISE attack steps have also additional properties, which allow creating executable models for quantitative analysis. Each attack step has an associated stochastic duration, a cost, and a set of different outcomes, each one modifying the state of the model in a different way. A probability of occurrence and a probability of being detected (as perceived by the adversary) are associated with each outcome.

The adversary profile defines the set of access items and knowledge items that are initially owned by the adversary (i.e., the initial state of the model), as well as his proficiency in attack skills. The adversary starts without having reached any goal, and works towards them. To each attack goal it is assigned a *payoff* value, which specifies the value that the adversary assigns to reaching that goal. Three weights define the relative preference of the adversary in: i) maximizing the payoff, ii) minimizing costs, or iii) minimizing the probability of being detected. Finally, the *planning horizon* defines the number of steps in the future that the adversary is able to take into account for his decisions; this value can be thought to model the "smartness" of the adversary.

The ADVISE execution algorithm [4] evaluates the reachable states based on enabled attack steps, and selects the most appealing to the adversary based on the above described weights. The execution of the attack is then simulated, leading the model to a new state. Metrics of interest are defined using reward structures [7].

4.2 ADVISE Model

Due to space limitations, in this section we only provide a high-level description of the model. The full details of the model can be found as a technical report in [20].

Attack Execution Graph. The AEG for configurations variant #2 (see Section 3.2) consists of 1 attack goal, 10 access domains, 5 knowledge items, 5 attack skills, and 18 attack steps; the AEGs for the other two variants have only slight differences. Its graphical representation is shown in Fig. 1, using the graphical notation introduced in [4]: attack goals are represented by ovals, access domains by squares, knowledge items by circles, attack skills by triangles, and attack steps by rectangles.

The description of the AEG in Fig. 1 is carried out in the following, in a bottom-up fashion. The model has only one attack goal, "Open Session", representing the objective of obtaining authentication. In configuration #2, to accomplish its goal the attacker should be authenticated by each unimodal biometric subsystems. Successful authentication with each of the three biometric traits is represented by the three access domains "VoiceAuth_Ok", "FaceAuth_OK", and "FingerprintAuth_OK", which enable the "WaitResponse" attack step. In this step the attacker simply waits the response from the authentication service. The adversary has basically two ways to reach the three access domains: he can perform a combined spoofing attack on biometric sensors, or he can compromise the template database.

Fig. 1. The structure of the ADVISE attack execution graph for variant #2

The modification of the template database is represented by the "InsertFakeTemplate" attack step. However, to successfully accomplish that, he needs a high score in the "HackSkill" attack skill, access to the template database ("TemplateDatabaseAccess" access domain) and knowledge of previously transmitted feature sets ("TransmittedFeatureSet" knowledge item). If this attack is successful he can then use his real biometrics to obtain authentication ("PresentVoice", "PresentFace", "PresentFingerPrint" attack steps). Access to the template database can be obtained by knowing its location and credentials ("DBLocation" and "DBPassword" knowledge items) and having access to the private network ("CASHMA_Network_Access"), which enables the "TemplateDatabaseLogin" attack step. Another way to access the database is performing the "TemplateDatabaseHack" attack step, which requires knowing the location of the database, having access to the CASHMA internal network, and a high proficiency in the "HackSkill" attack skill. If the location of the database is not known to the attacker, he can obtain it with the "Eavesdropping" attack step, i.e., observing network communication on the CASHMA internal network. The same attack may also provide information on transmitted biometric data ("TransmittedFeatureSet"); however it requires access to the internal network, and the "HackSkill" attack skill.

Obtaining the three access domains through sensor spoofing techniquesis represented by the "SensorSpoofing_Voice", "SensorSpoofing_Face", and "SensorSpoofing_Fingerprint" attack steps, each one requiring a specific attack skill and access

domain. For example, "SensorSpoofing_Fingerprint" requires a high proficiency in the "SkillSpoofing_Fingerprint" attack skill, and the "FakeFingerprint" access domain. Moreover, the success probability of this attack step is directly proportional to the score in the related attack skill. Fake biometric samples can be either owned by the attacker at the beginning of the scenario, or can be obtained in a sneaky way from legitimate users, but it is required to have knowledge of registered users of the system ("UsersKnowledge"). Such knowledge can be obtained by performing the "GetInformationAboutUsers" attack step, which has no particular prerequisites. Obtaining fake samples for voice and face biometric traits ("CreateFakeVoice" and "CreateFakeFace" attack steps) does not require additional items, since it may be as simple as taking a picture or recording a conversation; however, a high probability of detection is associated with such attack steps. For the fingerprint biometry, instead, it is necessary to have the fingerprint of an authorized user ("UserFingerprint" knowledge item), which can be either found on the biometric device ("FindLatentPrint"), or obtained from the user by fraud, e.g., having him touch some particular item or material. The latter option however requires proficiency in the "FraudMastery" attack skill".

To evaluate the other two configuration variants, little modifications are required to the AEG. Considering only two biometric traits for user authentication simply requires to modify the prerequisites for the "WaitResponse" attack step, in order to enable it even when only two out of three biometric traits are provided. Having three different encryption keys is represented by replicating the "Eavesdropping" attack step and the "TransmittedFeatureSet" knowledge item, to represent that the tree communications using different keys needs to be intercepted by the attacker.

Adversary Profiles. A summary of parameters used for the definition of the four adversary profiles is shown in Table 1. The table is divided in five blocks which describe, from top to bottom: the proficiency in attack skills, access domains, knowledge items, preference weights, and planning horizon of the four adversaries. Access domains and knowledge items that are not mentioned in the table are not owned by any adversary at the beginning of the scenario.

Table 1. Definition of the four adversary profiles

	Malicious user (voice)	Malicious user (voice+face)	Hacker	Terrorist organization
SkillSpoofing_Voice	1000	1000	200	600
SkillSpoofing_Face	200	900	200	600
SkillSpoofing_Fingerprint	200	200	200	600
FraudMastery	200	200	200	600
HackSkill	200	200	800	600
FakeVoice	Y	Y	N	N
FakeFace	N	Y	N	N
FakeFingerprint	N	N	N	N
DatabaseLocation	N	N	Y	N
WeightCost	0.3	0.3	0.25	0.05
WeightDetection	0.3	0.3	0.25	0.05
WeightPayoff	0.4	0.4	0.5	0.9
PlanningHorizon	7	7	7	7

The *malicious user (voice)* attacker represents a malicious user of the system trying to authenticate on behalf of someone else. He owns a fake biometric sample of the victim's voice, which could have been obtained for example by simply recording a conversation, but he does not have other particular skills. The *mailicious user (voice+face)* is also able to provide a fake sample of the victims' face biometry, e.g. a high resolution picture. The *hacker* attacker has an high skill in the "HackSkill" ability, allowing him to perform advanced cyber-attacks to the system, and he has some additional knowledge on system configuration. Finally, the *terrorist organization* attacker is characterized by a high motivation in reaching the intended goal ("WeightPayoff") and pays little attention to needed costs and to the possibility of being detected. It has average proficiency in several skills, but he does not have fake biometric samples to use for sensor spoofing.

The planning horizon parameter has been set to 7 for all the adversaries, as a good compromise between solution time and accuracy of results: by further increasing it we experienced a great increase in computation time, without significant differences in the evaluated measures of interest. For all the adversaries a payoff of 1000 has been set for the "SessionOpen" attack goal; measures of interest are however not affected by this value, since it is the only attack goal available to attackers.

5 Evaluation and Results

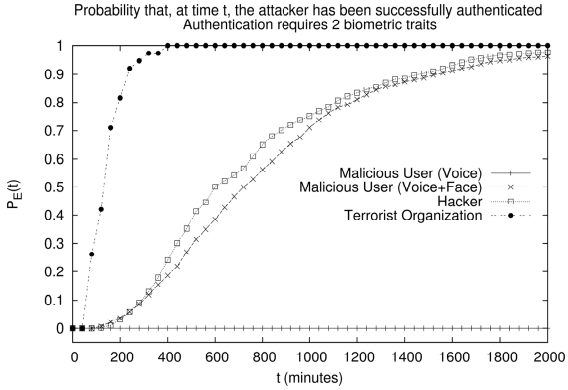
In this section we describe the results obtained by evaluating the model defined in Section 4.1. The model has been solved using the simulator included in the Möbius framework. The probability that the attacker has been successfully authenticated at time t, $P_E(t)$, is obtained by evaluating the probability that, at time t, the adversary owns the "SessionOpen" attack goal. All the measures have been evaluated using a relative confidence interval of 0.1, a confidence level of 99%, and collecting at least 100 and at most 10000 samples.

5.1 Variant #1: Two Biometric Traits, Single Encryption Key

Fig. 2 shows the results obtained for the default system configuration, for each of the four attackers. In this configuration three of the four considered attackers are able to reach the goal. The "terrorist organization" attacker is the fastest to compromise the system, since it is able to obtain authentication in 1/5 the time required to the other two successful attackers. This is due to the great ability of this attacker to perform sensor spoofing attacks on the system [20]; moreover, since only two of them are required for authentication, he is allowed to select the ones that require less effort for him (both in time and costs). The "malicious user (voice+face)" and "hacker" attackers are both able to obtain authentication, with the former spending on the average 25% additional time (about 150 minutes) with respect to the latter.

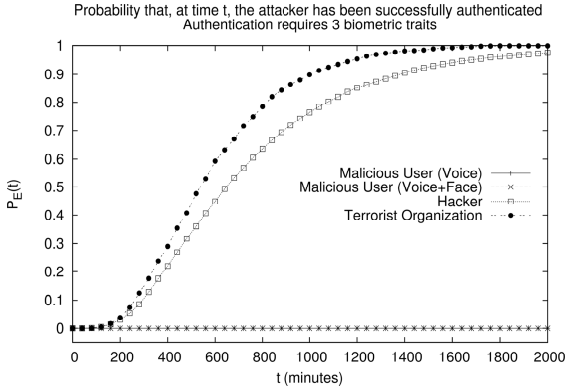
5.2 Variant #2: Three Biometric Traits, Single Encryption Key

In this section we evaluate the impact of using three biometric traits for authentication; results are shown in Fig. 3. This configuration variant has two main effects on system security. The first is a considerable increasing of the time required to the "terrorist organization" attacker to obtain authentication, which has increased by 4 times with respect to variant #1. The second effect is that only two of the four adversaries are able to obtain authentication: the "malicious user (voice+face)", which was able to obtain authentication in Variant #1, is now unable to compromise the system, since he has no means to bypass fingerprint authentication. Finally, this modification has little effect on the "hacker" adversary, which is still able to compromise the system using the same amount of time as in variant #1. This attacker spends the greatest part of the time in accessing the database and eavesdropping the communications [20], steps that



	T_E (minutes)
Mal. user (v)	∞
Mal. user (v+f)	841
Hacker	757
Terr. org.	139

Fig. 2. Results obtained for variant #1, for the different adversaries



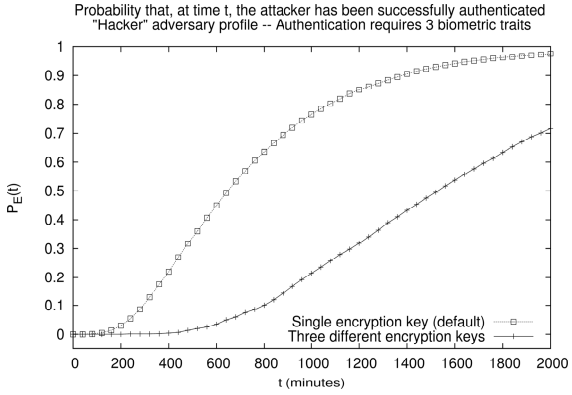
	T_E (minutes)
Mal. user (v)	∞
Mal. user (v+f)	∞
Hacker	761
Terr. org	595

Fig. 3. Results obtained for variant #2, for the different adversaries

require the same amount of timein this configuration as well. As expected, using additional biometric traits results in a considerable increase of security against certain kind of attackers. However, it is also highlighted that such solution provides a security improvement only if the template database is well-protected: against the "hacker" attacker this configuration is no more secure than variant #1.

5.3 Variant #3: Three Biometric Traits, Three Encryption Keys

In the third configuration variant, biometric data acquired from sensors is transmitted to the server using three different encryption keys, one for each biometric trait. This modification only affects the "hacker" attacker, which is the only one able to obtain authentication by compromising the template database [20]. Fig. 4 compares how $P_E(t)$ and T_E change for the "hacker" adversary when introducing this modification. Introducing different encryption keys does not prevent the "hacker" adversary to obtain authentication from the system; however he will need more time to succeed, since he will have to perform additional attack steps to obtain all the data required to modify the template database. Moreover, results show that security is not simply improved by a factor of 3: the mean time required to obtain authentication is in fact only doubled with respect to variants #1 and #2.



	T_E (minutes)
Hacker – Variant #2	757
Hacker – Variant #3	1683

Fig. 4. Results obtained for the "hacker" adversary in variant #3

6 Conclusions

In this paper we have performed a quantitative security evaluation of the CASHMA multi-biometric authentication system, using the recently introduced ADVISE formalism. We successfully modeled the threats to biometric authentication systems, taking into accountaspects related to human factors (e.g., cheat on users to obtain biometric samples), system knowledge, and skills of attackers. Taking into account these aspects in assessing the security of critical infrastructures control systems is of primary importance in understanding and contrasting modern cyberattacks. However, some aspects need to be further investigated; in particular, setting model parameters is

challenging; for example, defining the duration and cost of each attack step introduces several assumptions that are hard to verify. Another interesting aspect concerns model solution, which is currently carried out by discrete-event simulation; analytical solution techniques, when applicable, could improve the accuracy of results.

Acknowledgments. This work has been partially supported by the Italian Ministry for Education, University, and Research (MIUR) through the FIRB project CASHMA: Context Aware Security by Hierarchical Multilevel Architectures [3].

References

1. Li, S.Z. (ed.): Encyclopedia of Biometrics, 1st edn. Springer Reference (2009)
2. Chen, T., Abu-Nimeh, S.: Lessons from Stuxnet. IEEE Computer 44(4), 91–93 (2011)
3. FIRB – Fondo per gli Investimenti della Ricerca di Base, CASHMA: Context Aware Security by Hierarchical Multilevel Architectures (2008)
4. LeMay, E., Ford, M., Keefe, K., Sanders, W., Muehrcke, C.: Model-based Security Metrics Using ADversary VIew Security Evaluation (ADVISE). In: 8th International Conference on Quantitative Evaluation of Systems (QEST 2011), pp. 191–200 (2011)
5. Phillips, P.J., Martin, A., Wilson, C.L., Przybocki, M.: An introduction evaluating biometric systems. IEEE Computer 33(2), 56–63 (2000)
6. Henniger, O., Scheuermann, D., Kniess, T.: On security evaluation of fingerprint recognition systems. In: International Biometric Performance Conference (IBPC 2010), March 1-5. National Institute of Standards and Technology, NIST (2010)
7. Nicol, D.M., Sanders, W.H., Trivedi, K.S.: Model-based evaluation: from dependability to security. IEEE Trans. on Dependable and Secure Computing 1(1), 48–65 (2004)
8. Dolev, D., Yao, A.C.: On the security of public-key protocols. IEEE Transactions on Information Theory 29(8), 198–208 (1983)
9. Lowe, G.: Casper: a compiler for the analysis of security protocols. In: Proc. 10th Computer Security Foundations Workshop, June 10-12, pp. 18–30 (1997)
10. Ten, C.-W., Liu, C.-C., Govindarasu, M.: Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees. In: IEEE Power Engineering Society General Meeting, June 24-28, pp. 1–8 (2007)
11. Sheyner, O., Haines, J., Jha, S., Lippmann, R., Wing, J.M.: Automated generation and analysis of attack graphs. In: IEEE Symposium on Security and Privacy, pp. 273–284 (2002)
12. Beccuti, M., et al.: Quantification of dependencies in electrical and information infrastructures: The CRUTIAL approach. In: 4th International Conference on Critical Infrastructures (CRIS 2009), pp. 1–8 (2009)
13. LeMay, E., Unkenholz, W., Parks, D., Muehrcke, C., Keefe, K., Sanders, W.H.: Adversary-Driven State-Based System Security Evaluation. In: Proceedings of the 6th International Workshop on Security Measurements and Metrics, MetriSec 2010 (2010)
14. Courtney, T., Gaonkar, S., Keefe, K., Rozier, E.W.D., Sanders, W.H.: Möbius 2.3: An Extensible Tool for Dependability, Security, and Performance Evaluation of Large and Complex System Models. In: DSN 2009, Estoril, Lisbon, Portugal, pp. 353–358 (2009)
15. Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S.: Impact of artificial ‘gummy’ fingers on fingerprint systems. In: Proc. SPIE, vol. 4677, pp. 275–289 (2002)
16. Pacut, A., Czajka, A.: A liveness Detection for IRIS Biometrics. In: Proc. of the 40th Int. Carnahan Conference on Security Technology (ICCST 2006), pp. 122–129 (October 2006)

17. Roberts, C.: Biometric attack vectors and defences. Computers & Security 26(1), 14–25 (2007)
18. Dierks, T., Rescorla, E.: The Transport Layer Security (TLS) Protocol – Version 1.2, RFC 5246, IETF Network Working Group (August 2008)
19. Salles-Loustau, G., Berthier, R., Collange, E., Sobesto, B., Cukier, M.: Characterizing Attackers and Attacks: An Empirical Study. In: IEEE 17th Pacific Rim International Symposium on Dependable Computing (PRDC), pp. 174–183 (2011)
20. Montecchi, L., Lollini, P., Bondavalli, A.: ADVISE model for the security evaluation of the CASHMA multi-biometric authentication system, University of Florence, RCL Group, Technical Report RCL120301 (2012), http://rcl.dsi.unifi.it/publications