Attack Trees for System Protection against Evolving Biometric Presentation Attacks

Conference Paper · April 2017

CITATIONS
0

READS
48

4 authors, including:

Emanuela Marasco
University of North Carolina at Charlotte
26 PUBLICATIONS **295** CITATIONS
SEE PROFILE

Mohamed Shehab
University of North Carolina at Charlotte
81 PUBLICATIONS **1,075** CITATIONS
SEE PROFILE

Usman Rauf
University of North Carolina at Charlotte
13 PUBLICATIONS **26** CITATIONS
SEE PROFILE

Attack Trees for Protecting Biometric Systems against Evolving Presentation Attacks

Emanuela Marasco, Bojan Cukic
Dept. of Computer Science
Univ. of North Carolina at Charlotte
28223 Charlotte, NC, USA.
Email: emarasco,bcukic@uncc.edu

Mohamed Shehab, Usman Rauf
Dept. of Software and Information Systems
Univ. of North Carolina at Charlotte
28223 Charlotte, NC, USA.
Email: mshehab,urauf@uncc.edu

***Abstract*—Several reports have highlighted that spoofing biometric traits represents a serious threat for active identity management systems. Applications of biometrics are critically important technologies for traveler, immigration and refugee management systems deployed or considered for deployment by the Department of Homeland Security. Due to motivations and consequences of identity misrepresentations at US borders, threats specific to these categories differ from generic biometric applications. Thus, there is a strong need to reduce the risk of spoof-based fraud mitigation strategies are needed. Biometric system attack vector analysis is growing but still not as fast as the general level of security threats. Therefore, in this paper we analyze feasibility of biometric presentation attacks behind identity misrepresentation and discuss a practical methodology for classifying biometric identity attack vectors based on their risks. The classification will lead towards practical vulnerability assessment methods and countermeasures, technical as well as managerial. Our findings aim to enable identification of biometric presentation attack risks and severities, leading towards a well-defined defense strategy.**

I. Introduction

Biometric recognition is playing a strong role as technology for traveler, immigrant and refugee management. Due to wide use in homeland security, biometric systems are a key target for presentation attacks (PAs). PAs refer to techniques which inhibit the intended operation of a biometric capture system, interfering with the acquisition of the actual biometric sample pertaining to the authorized individual [1], [2], [3], [4]. Typical PAs utilize a prosthetic to conceal the biometric signature or present an alternative biometric signature [5], [6], [7]. Biometric systems in use at national points of entry or those that support immigration are now acknowledged as potential points of identity concealment attacks, carrying a risk of failure. Biometrics for automated border control and other high-security applications needs robust integrated anti-spoofing capability. System defense concerns are factors that should be taken into consideration while developing countermeasures to thwart attacks. Among these are financial cost, risk, image and customer confidence. Assuring system integrity is not a static task. A system can be kept secure whether it is defended against a growing number of attacks. This interplay of system protection in light of evolving biometric presentation attacks is the problem that we want to address. In this regard, it is important to systematically document newly discovered attacks and implemented countermeasures. Attack patterns, motivations and resources can vary; thus, *dynamic* countermeasures are expected to be more efficient. The complexity of potential biometric presentation attack scenarios regard motivations, technical expertise, access to resources.

- Personal motivations are generally related to quick need for cash due to feeding addictions (e.g., drug habits, gambling debts) or loss of the job, work permits (e.g., to obtain goods and services), concealment of other crimes (i.e., the stolen identity is implicated in crimes) and political reasons (e.g., terrorism).
- Technical expertise consists of social skills (e.g., ability to manipulate social situations) and technical skills (e.g., technical knowledge needed to produce fake samples).
- Access to resources describes available know-how (e.g., employees of various business or state agencies), association with criminal or political organizations with substantial financial means or using the employment for access (banks, universities, government).

Higher risks are generally present for those who have already committed a crime. Police in Japan found that a woman paid a plastic surgeon to surgically alter her fingerprints to evade detection. She did pass through the checkpoint using fake fingerprints. Furthermore, a woman who was originally arrested for faking a marriage license, passed the screening system by placing special tape over her fingerprints[1]. She had actually succeeded at the airport in a real-time scenario, high-stress environment such as the one of an immigration line. Attackers do not have defeat just the technology, but they need to defeat the social system around it such as the officers who supervise the fingerprint acquisition. Thus, also social skills play an important role.

In this paper, we expand the existing efforts in biometric liveness detection by considering the attacker perspective and her motivations. We develop a practical methodology for classifying identity attack vectors related to biometric systems based on their complexity, cost, feasibility and risks to homeland security. The paper is organized as follows. In Section 2, we describe attack trees for biometric presentation

[1] http://abcnews.go.com/Technology/GadgetGuide/surgically-altered-fingerprints-woman-evadeimmigration/story?id=9302505

attacks scenarios. Section 3 illustrates the security cards framework that captures relevant information. Section 4 discusses risk analysis based on attack trees. In Section 5 we draw conclusions.

II. Attack Trees for Biometric Presentation Attacks

The deployment of presentation attack detection methods based on the characteristics of acquired images is only one aspect of PAD defense. This section discusses methodologies for system-level risk understanding and analysis. System-level focus opens the opportunities for improved and broader defense measures, which may include human factors and process constraints. System engineers are often reluctant to publicize data related to system design flaws or vulnerabilities. Thus, owners and operators of biometric identification systems may be unaware of the existence of opportunities for presentation attacks. To some extent, this situation is similar to the early days of cybersecurity. When a vulnerability of a biometric system is exploited and thus an attack occurs, the owners and commercial providers may fear that revealing details about the attack will provoke similar attacks, ruin their reputation, and subsequently affect customer confidence. Given the right vulnerability analysis methodology and tools, it should become easier for system engineers to identify and analyze potential points of attack and implement the appropriate countermeasures for each before the attacks occur.

It is vital that extensive vulnerability analysis is performed during system design and later in deployment. The methods used should greatly simplify the task of analyzing vulnerabilities and identifying possible means of exploitation. The designer can then implement appropriate countermeasures to prioritize and mitigate the vulnerabilities, resolve some and document or possibly ignore the others. Attack tree is a methodology for analyzing the security of systems and subsystems. It was introduced by Bruce Schneier in 1999.

Attack Tree is a tool to decompose complex events (attacks) into components, allowing a large universe of attacks to be divided into a structured set. Attack Trees aid with probabilistic risk analysis, by decomposing the scenarios related to attacks [8]. Specifically, it can be used to map out the various components of a threat scenario (the vulnerabilities and the threat sources) and organize them into a more easily understood structure through which threat sources can be systematically compared to vulnerabilities. Attack trees are a useful baseline for the assessment of attack risk[2], which is challenged by intelligent adversaries who may adapt to the defensive measures.

The security of systems can be methodically described and analyzed using attack trees. The analysis of biometric systems using attack trees represent a general approach to vulnerability identification and it is a relatively new area [9], [10], [11], [12]. This formal representation of attacks also enables ways to create and examine the vulnerabilities for a particular system

[2]http://ishandbook.bsewall.com/risk/Assess/Risk/components.html

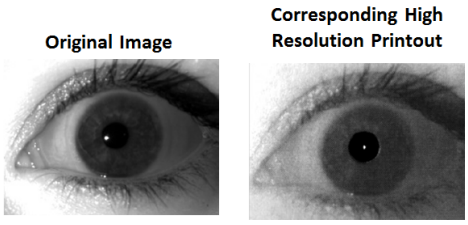

Fig. 1: Examples of biometric presentation attacks: (a) Original image of an iris (on the left) and the corresponding high resolution printout (on the right). These sample images belong to the Warsaw subset [17].

Fig. 2: Human finger (on the left) versus a high resolution printout of the corresponding fingerprint (on the right). Images collected at MSU [18].

[13], [14], [15]. After vulnerabilities are identified, they must be analyzed to determine potential means of exploitation and develop countermeasures to thwart attacks. This methodology allows attacks on a system to be represented in a Boolean-logical tree structure, with the root node as the goal of the attack and its children as elementary activities performed by the attacker to accomplish that goal. For the same attack goal, different attackers may take different attack paths [16]. In case of multiple threat scenarios connected to an elementary exploit, an OR-relation can be used which means that any threat is sufficient to execute the feat. This allows the analyst to represent complex attack scenarios while maintaining a holistic view. Attack trees help the analyst understand ways in which a system may be attacked and, subsequently, determine which countermeasures are necessary. Furthermore, an attack tree can include special knowledge such as risks assumed by the attacker.

We illustrate the attack tree methodology for biometric presentation attack analysis with specific examples related to iris and fingerprint spoofing. Among possible ways to perform a presentation attack against an iris recognition system, the easiest way consists of presenting a printed image of an iris pertaining to an authorized user to the system, see Figure 1. If undetected, the attack allows an impostor's access under presumed identity. Figure 3 shows the attack tree relate to a 2D printout attack in which a high quality printout is displayed to the sensor. The higher the quality of the photo prints, the higher the probability of success of this attack

[19], [20]. Figure 4 shows the attack tree when using a 2D printed fingerprint in place of the corresponding finger, to deceive a fingerprint collection device [18]. The fingerprint of the authorized individual is photographed and printed on a transparent sheet. The spoof is manually fabricated using a material such as white wood glue and presented to the sensor embedded in the mobile phone, see Figure 2. In this method, the quality of spoof fingerprint and the accuracy of spoof attack may be affected by the attacker's experience[3] or access to know-how resources.

We can look at the attributes of the attack tree as being either related to attacker's actions or capabilities, or may signify the opportunities for defensive countermeasures. Attack attributes provide an understanding of the attacker and help determine the likelihood of a particular path of exploitation. Motivation represents the attacker's reasoning and justification to perform the attack. In some cases motivation may be easy to determine, but in others there may be a plethora of motives. Many attackers are motivated by financial gain. Some are motivated by achieving a status and recognition. Others gain neither money nor status and are motivated by revenge or anger towards an organization (state). Gain may fall under the category of motivation, but risk is a different category altogether. The risk an attacker takes in performing an attack refers to the consequences she may face, if caught. These may include fines, jail time, etc. The risk one is willing to take is directly related to the motivation and the likelihood of getting caught. No one in their right mind would risk serious consequences for a low gain, unless the likelihood of getting caught is low. On the other hand, if the probability of getting caught is medium but the gains are substantial, it may be worth the risk. Gain can in some cases be ideological and to a large extent misunderstood by defenders. Motivational calculus is primarily the attacker's concern. Public knowledge of the vulnerability is a factor typically controlled by research and development organizations, commercial entities or law enforcement community. Media (in a broad sense, including online actors) may inadvertently help making the vulnerability more exposed. For example, attacks often occur to systems immediately following the vendor‘s (or adversary's) disclosure of vulnerability and the release / deployment of a patch to fix it. Systems, especially those of large scale, cannot be patched instantaneously. It takes time for the system owners to install the patch to all vulnerable systems under their control. These aspects of attack vectors are not adequately represented in attack trees. Therefore, we searched for a related methodology that could help us understand and represent them. One such methodology - security cards - is presented below.

III. The Identification Security Cards Methodology

For defenders, quantifying the attack probabilities requires knowledge, data or modeling about the motivations, intent and capabilities of attackers in addition to the known attacks and their relevance to the current risk. Thus, in this section we propose an assessment of activities, motivations, intent and capabilities of attackers. Generally, attack patterns, motivations and resources are expected to change. Thus, there is a strong need for designing dynamic countermeasures.

Proposed by T. Denning, B. Friedman and T. Kohno, the Security Cards is a security threat brainstorming toolkit which consists of 42 cards divided in four dimensions: Human Impact, Adversarys Motivations, Adversarys Resources, and Adversarys Methods [21]. This methodology offers a practical way to categorize and evaluate potential vulnerabilities of identity collection and management systems. It offers a practical way to collect and organize the information. The goal of this methodology is to understand attack techniques and patterns already used and postulate those that may be tried in the future. The methodology has to be able to stimulate thinking broadly and creatively about biometric system security. It is often the case that developers and system maintainers assume they understand all common attack patterns but fail to explore specific attack vectors and employ accepted security procedures. The ways a deployed system is used or misused can introduce unanticipated threats.

Cards pertaining to different dimensions are typically solicited from stakeholders.

- *Human Impact* explores how security breaches may affect humans. In case of border security, identity fraud is clearly related to consequences that may not be clear at the time of security breach. Examples include privacy violations (damage to identity owners), avoiding legal repercussions for past actions, or threat for the loss of life in case of terrorist activities.
- *Adversary Motivations* describe why someone might want to attack a system. The Security Card methodology helps us represent possible motivations more concisely, and express them with more clarity. The methodology elicits possible attack motivation that range from ideological, religious and political factors to convenience and self-promotion.
- *Adversarys Resources* analysis explores assets that might be widely available and used to launch an identity attack. These resources correspond to hardware and software tools, the access to technical or social impersonation expertise and the ability to influence the actions of people. For instance, Technical Expertise refers to the potential technical skills of the attacker.
- *Adversarys Methods* explore the high-level approaches that might be used to perform an attack. Mmanipulation of people, the adherence to burdensome bureaucratic processes or specific exception handling rules (the person does not have distinguishable fingerprints, for example) may, in fact, play a role insome of the identity attack vectors.

[3]https://www.theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked

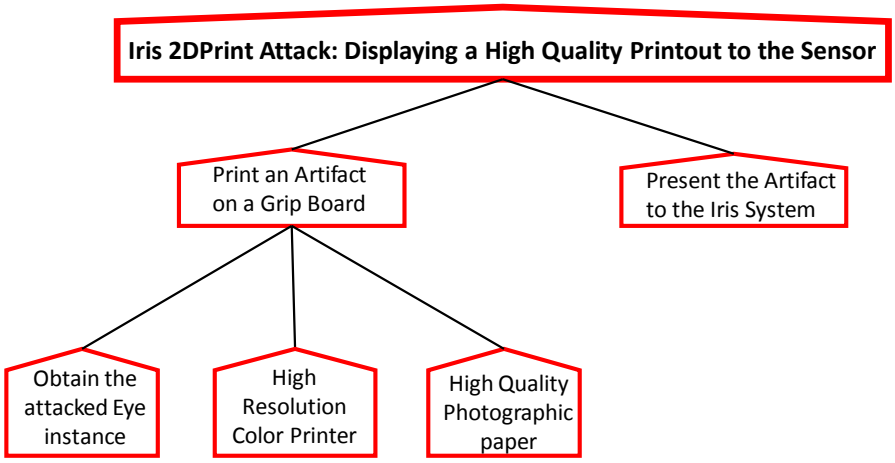

Fig. 3: Iris 2D Print Attack

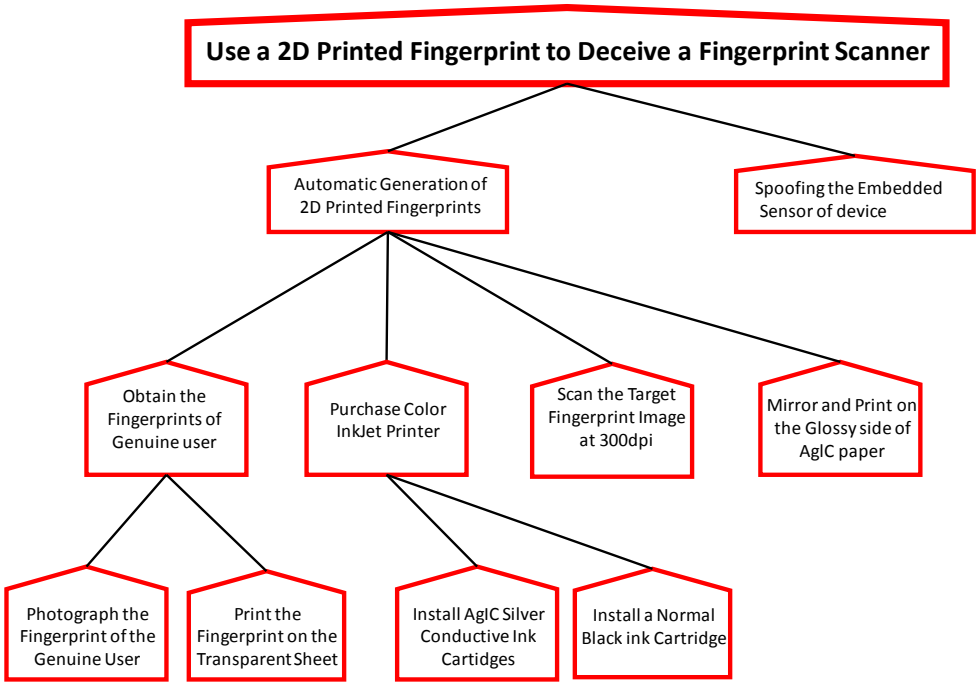

Fig. 4: Use of a 2D Printed Fingerprint to Deceive a Fingerprint Locked Mobile Phone

IV. Risk Analysis Based on Attack Trees

A. Risk Model for Attack Prediction

Accurate quantitative model that measures security risk can be achieved by a probabilistic approach [22]. A simple risk model includes two primary components:

- The *Probability* that an attack will occur, which is a function of vulnerabilities (i.e., lack / weaknesses in controls) and threats (i.e., people / external events exploiting vulnerabilities).
- The *Cost* intended as the amount of losses (i.e., impact or financial exposure) that would result from the success of an attack. The cost is computed as the product between the losses results from an attack and the number of times that such an attack will occur in a certain period.

The risk is a combination of the probability that an attack will occur with the damages that it would cause. Higher risk is associated with attacks that are highly likely to occur and / or have a high impact. The risk can be computed as the product between the estimated losses associated to the occurrence of an attack and the probability that the attack will occur, see Eqn. 1.

$$Risk = Cost \times Probability \tag{1}$$

The occurrence of an attack depends on both the adversary and the system. An attack will succeed if the following conditions are met:

- There are motivated adversaries who want to harm the system.
- The adversaries possess the necessary capability to carry out the attack [4].

The motivation, in combination with the capability, determines the threat of an attack, see Eqn. 2.

$$Threat = Capability \times Motivation \tag{2}$$

Combining expressions 1 and 2,

$$Risk = (Capability \times Motivation \times Vulnerability) \times Cost \tag{3}$$

Translating these expressions into identity domain, capability corresponds to the resources available immigrants / refugees / travelers. Assuming reasonably constant level of motivation within immigrant, refugee and traveler population, the probability of an attack scenario can be estimated by combining the attackers capabilities with systems vulnerabilities. Attack trees offer direct link between the two.

Generally, the integration of risk assessment with attack trees is based on fusing the attacker's goals and the defender's feared events, but also on fusing the elementary activities performed by the attacker (i.e., the exploits) and the threat scenarios [12]. When fusing the attacker's goals with the defender's feared events, security and safety studies are combined. An attack tree can be initiated only if a safety hazard has been identified. The decomposition stops when it is possible to execute an attacker's exploit by one or more threat scenarios.

B. Risk Analysis Formulation as Constraint Satisfaction Problem

One way to analyze an Attack Tree (AT) is to represent it as Constraint Satisfaction Problem (CSP), and then perform risk or vulnerability analysis, depending on the requirements [23]. CSP offers a deeper understanding of the problem structure and complexity. There are two different conventions for representing such problems as CSP:

- enlist the possible actions that can be conducted by an attacker as a top layer of the tree containing root elements. Each root element is an action which can lead to a certain or multiple outcomes. Thus a sequence of actions leading towards a certain leaf node (with no more child nodes), can be referred to an attack sequence, according to the first convention.
- list the goals as root nodes and enlist the actions downward as a sequence.

In this paper, we adopt first type of convention and provide an overview to the readers by formally representing the problem as CSP. Formally an attack tree can be represented as a 5-tuple $AT =< O, G, I, C_i, Lab >$, where:

- O is a set of possible originating actions (root nodes)
- G is a set of possible goals (for attacker)
- I is a set of possible intermediate (sequence of) actions that attacker must perform to reach a certain goal $O \cap I : \emptyset$ and $G \cap I : \emptyset$ to avoid the cycles
- C_i is a set of additional constraints if there are any
- Lab is a labeling function such that $Lab(O_i, G_i, I_i, C_i) : (O_i, G_i) \longrightarrow I_i$ where $I_i \subseteq I$

An attack corresponds to a carefully selected sequence of actions / exploits, but there can be multiple ways to breach for a certain goal. Therefore, it can be formally represented as indicated in Eqn. 4.

$$G_i = \bigvee_{j:1\to n} \left(\bigwedge_{k:1\to m} \left(a_k \right) \right) \tag{4}$$

where $\bigwedge_{k:1\to m} \left(a_k \right) = (a_1 \wedge a_2 \wedge a_3 ... \wedge a_m)$

The assignment of values to some or all the variables can define the state of the problem which is consistent when the assignment does not violate any constraint. A complete assignment that satisfies all the constraints represents a solution to the CSP under study. After formulating the problem as CSP, by mapping the possible attack scenarios as action sequences, we can conduct vulnerability analysis. In the context of biometric systems, vulnerability analysis can help identifying the minimum number of exploits / vulnerabilities that can be eliminated or patched in order to guarantee that no goals are achieved. Identifying a set of minimum number of vulnerabilities is an NP-Hard problem, but can be solved in reasonable amount of time, once it is converted into satisfiability problem [24].

Another type of analysis can be conducted by introducing the risk parameter in the formalization as a constraint. From attackers perspective, not all actions have same associated risk; specifically, attackers prefer considering *high benefit - low cost* strategies. For biometric system designers, eliminating all the vulnerabilities might be difficult and costly. Using additional constraints for risk and cost designers and defenders can set a certain bearable threshold and then find a satisfiable solution for the mentioned model.

For this purpose, it is important to quantify the risk associated to each action that can be carried out by an attacker. Potentially, risk can be defined as function of the likelihood of a certain activity $Prob_i$ (i.e., likelihood of being exposed if a certain action is taken by an attacker) and the corresponding impact Imp_i (i.e., amount or duration of penalty), see Eqn. 5.

$$Risk_i = Prob_i \times Imp_i \tag{5}$$

where $Prob_i \in Prob$ and $Imp_i \in Imp$

Carefully mapping the values of likelihood of actions to the corresponding impact can help in formalizing the risk constraint as indicated in Eqn. 9.

$$Prob = w_1, w_2, ...w_n \tag{6}$$

$$Imp = Imp_1, Imp_2, ...Imp_n \tag{7}$$

[4]http://ishandbook.bsewall.com/risk/Assess/attack_trees.html

$$Risk_i = w_i \times Imp_i \tag{8}$$

$$\textbf{Risk Constraint} : \sum_i \Big(Prob_i \times Imp_i \Big) \geq \theta \tag{9}$$

By incorporating the above-mentioned constraint, different strategy profiles can be synthesized, for eliminating the vulnerabilities according the user defined threshold. As we mentioned already not all the vulnerabilities can be patched due to the high cost or for technical reasons. Due to budget limitations, usually all the identified vulnerabilities cannot be addressed; thus, defenders reasonably patch vulnerabilities with cost below a certain threshold and leave those with high cost but risk, for the attacker to be penalized or be caught, above a certain threshold. Similarly, constraints related to the cost / benefit, can also be incorporated in the model.

V. Conclusion and Future Work

The science behind biometric system attack vector analysis is emerging, but not nearly as fast as the general level of security threats. In Attack Trees (AT), attacks against a system are represented in a tree structure that helps the designer understand different ways in which the system may be attacked as well as who the attackers may be, including their abilities, motivation, and goals. Security analysts may use attack trees to identify attack patterns, which in turn can serve system designers to implement more effective defense mechanisms. However, for defenders, quantifying the attack probabilities requires knowledge, data or modeling about the motivations, intent and capabilities of attackers in addition to the known attacks and their relevance to the current risk. We aim to develop a process which supports continual improvement of defensive capabilities related to identity concealment attacks where it is important to systematically document identity attacks and implement countermeasures.

In this paper, we present Attack Trees as strategy to analyse potential ways to exploit biometric systems' weaknesses. We also describe the Identification Security Cards brainstorming toolkit as methodology for categorizing and evaluating potential vulnerabilities of identity collection and management systems. This methodology has to be able to stimulate thinking broadly and creatively about biometric system security. Finally, we discuss the attack trees-based model as Constraint Satisfaction Problem (CSP) to perform risk and vulnerability analysis.

Acknowledgment

This work has been supported by the Border Trade Immigration (BTI) Institute, a Department of Homeland Security (DHS) Center of Excellence.

References

[1] S. Schuckers, "Spoofing and Anti-Spoofing Measures," *Information Security Technical Report*, vol. 7, no. 4, pp. 56–62, 2002.
[2] ——, "Presentations and Attacks, and Spoofs, Oh My," *Image and Vision Computing*, vol. 55, pp. 26–30, 2016.
[3] E. Marasco and A. Ross, "A Survey on Anti-Spoofing Schemes for Fingerprint Recognition Systems," *ACM Computing Surveys (CSUR)*, vol. 47, no. 2, p. 28, 2015.
[4] S. Marcel, M. Nixon, and S. Li, *Handbook of Biometric Anti-Spoofing*. Springer, 2014.
[5] J. Galbally, S. Marcel, and J. Fierrez, "Biometric Antispoofing Methods: A Survey in Face Recognition," *IEEE Access*, vol. 2, pp. 1530–1552, 2014.
[6] N. Erdogmus and S. Marcel, "Spoofing Face Recognition with 3D Masks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 7, pp. 1084–1097, 2014.
[7] K. Bowyer, K. Hollingsworth, and P. Flynn, "A Survey of Iris Biometrics Research: 2008–2010," in *Handbook of Iris Recognition*. Springer, 2013, pp. 15–54.
[8] B. Ezell, S. Bennett, D. Winterfeldt, J. Sokolowski, and A. Collins, "Probabilistic Risk Analysis and Terrorism Risk," *Risk Analysis*, vol. 30, no. 4, pp. 575–589, 2010.
[9] V. Saini, Q. Duan, and V. Paruchuri, "Threat Modeling Using Attack Trees," *Journal of Computing Sciences in Colleges*, vol. 23, no. 4, pp. 124–131, 2008.
[10] B. Kordy, S. Mauw, S. Radomirović, and P. Schweitzer, "Foundations of Attack–Defense Trees," *International Workshop on Formal Aspects in Security and Trust*, pp. 80–95, 2010.
[11] S. Mauw and M. Oostdijk, "Foundations of Attack Trees," *International Conference on Information Security and Cryptology*, pp. 186–198, 2005.
[12] S. Paul and R. Vignon-Davillier, "Unifying Traditional Risk Assessment Approaches with Attack Trees," *Journal of Information Security and Applications*, vol. 19, no. 3, pp. 165–181, 2014.
[13] E. Marasco, M. Shehab, and B. Cukic, "A Methodology for Prevention of Biometric Presentation Attacks," *IEEE Seventh Latin-American Symposium on Dependable Computing (LADC)*, pp. 9–14, 2016.
[14] D. Speicher, "Vulnerability Analysis of Biometric Systems Using Attack Trees," Ph.D. dissertation, West Virginia University, 2006.
[15] B. Schneier, "Attack Trees," *Dr. Dobb's Journal*, vol. 24, no. 12, pp. 21–29, 1999.
[16] S. Wang, Z. Zhang, and Y. Kadobayashi, "Exploring Attack Graph for Cost-Benefit Security Hardening: A Probabilistic Approach," *Computers & Security*, vol. 32, pp. 158–169, 2013.
[17] D. Yambay, J. Doyle, K. Bowyer, A. Czajka, and S. Schuckers, "Livdet-Iris 2013 - Iris Liveness Detection Competition 2013," *IEEE International Joint Conference on Biometrics (IJCB)*, pp. 1–8, 2014.
[18] K. Cao and A. Jain, "Hacking Mobile Phones using 2D Printed Fingerprints," *MSU Technical report, MSU-CSE-16-2*, 2016.
[19] R. Raghavendra and C. Busch, "Robust Scheme for Iris Presentation Attack Detection using Multiscale Binarized Statistical Image Features," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 703–715, 2015.
[20] P. Gupta, S. Behera, M. Vatsa, and R. Singh, "On Iris Spoofing Using Print Attack," *IEEE 22nd International Conference on Pattern Recognition (ICPR)*, pp. 1681–1686, 2014.
[21] T. Denning, B. Friedman, and T. Kohno, "The Security Cards: A Security Threat Brainstorming Toolkit," *Univ. of Washington, http://securitycards.cs.washington.edu*, 2013.
[22] M. Sahinoglu, "Security Meter: A Practical Decision-Tree Model to Quantify Risk," *IEEE Security & Privacy*, vol. 3, no. 3, pp. 18–24, 2005.
[23] R. Dechter, *Constraint Processing*. Morgan Kaufmann, 2003.
[24] M. Davis and H. Putnam, "A Computing Procedure for Quantification Theory," *Journal of the ACM (JACM)*, vol. 7, no. 3, pp. 201–215, 1960.