Chapter 9

Dynamic Risk Assessment in IT Environments:

A Decision Guide

Omid Mirzaei
Universidad Carlos III de Madrid (UC3M), Spain

José Maria de Fuentes
Universidad Carlos III de Madrid (UC3M), Spain

Lorena González Manzano
Universidad Carlos III de Madrid (UC3M), Spain

ABSTRACT

Security and reliability of information technologies have emerged as major concerns nowadays. Risk assessment, an estimation of negative impacts that might be imposed to a network by a series of potential sources, is one of the main tasks to ensure the security and is performed either statically or dynamically. Static risk assessment cannot satisfy the requirements of real-time and ubiquitous computing networks as it is pre-planned and does not consider upcoming changes such as the creation of new attack strategies. However, dynamic risk assessment (DRA) considers real-time evidences, being capable of diagnosing abnormal events in changing environments. Several DRA approaches have been proposed recently, but it is unclear which technique fits best into IT scenarios with different requirements. Thus, this chapter introduces recent trends in DRA, by analyzing 27 works and proposes a decision guide to help IT managers in choosing the most suitable DRA technique considering three illustrative scenarios – regular computer networks, internet of things, and industrial control systems.

DOI: 10.4018/978-1-5225-4763-1.ch009

INTRODUCTION

Information Technology (IT) deals with the use of computers to store, manipulate and retrieve any kind of data, ranging from business to personal, and in most cases, sensitive data. This field is receiving more attention in recent years due to the emergence of computer networks, wireless networks, and interconnected smart devices also known as the Internet of Things (IoT). In particular, Industrial IoT (IIoT), known as 4th Industrial Revolution (4IR), has received significant attention. In 4IR, real and virtual capabilities are merged into Cyber-Physical Production Systems (CPPS) through extensive usage of cloud services and applications, and, also, big data analytics (Sadeghi, Wachsmann, & Waidner, 2015).

In order to make sure that 4IR helps in achieving both economic and social improvements, authorities must anticipate and cover all involved security risks. Particularly, security of information needs to be addressed in order to provide a satisfying degree of reliability, confidentiality, integrity, and availability (Gehling & Stankard, 2005). It must be noted that numerous threats may affect these four factors. Thus, passive attacks (e.g. eavesdropping) or active ones (e.g. packet injection) may harm this environment (Deka, Kalita, Bhattacharya, & Kalita, 2015), (Nadeem & Howarth, 2013).

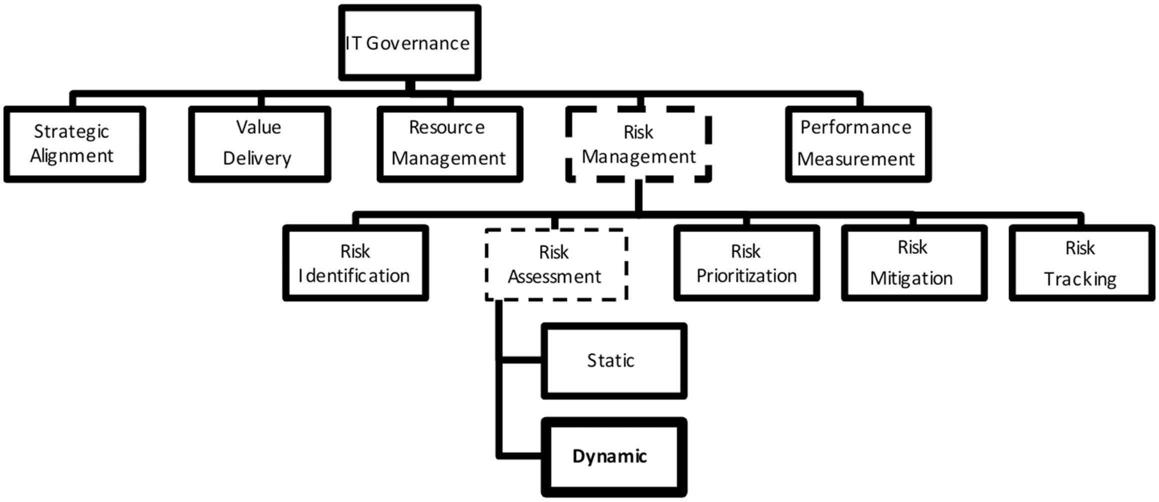
Regardless the type of threat or attack, they impose a magnitude of unreliability to information which is commonly known as “risk”. Speaking more precisely, the term “risk” is an estimation of the degree of exposure to a threat that may occur on one or more assets causing damage to an organization (Awan, Burnap, & Rana, 2016). In a computer network scenario, an asset may be any of its components (e.g. hardware devices or their software) as well as other related elements such as the network users.

Managing risks is critical to ensure the overall corporate security. For this reason, information security governance is already assumed to be an integral part of the corporate IT governance (Von Solms, 2005). In particular, Wilkin et al. highlight that risk management forms this process along with other corporate aspects such as strategic alignment, value delivery, resource management and performance measurement (Figure 1) (Wilkin & Chenhall, 2010). Thanks to risk management, it is possible to properly handle risks as it serves to identify, assess, prioritize, mitigate and track them (Garvey, 2008). Among these steps, risk assessment deserves special attention since it involves measuring an intangible factor – the degree of risk posed by an action (S. Fu & Zhou, 2011), (Benini & Sicari, 2008). This complex task is essential for responding to the threat (Shoemaker & Conklin, 2011).

Currently, there are two major risk assessment approaches, namely static and dynamic ones (Alireza Shameli-Sendi, Naser Ezzati-jivan, Masoume Jabbarifar, & Michel Dagenais, 2012). In a static system, risks are evaluated based on static values of factors related to risks, including assets, threats, and vulnerabilities. Today, with the dynamicity of threats, there is an urgent need for Dynamic Risk Assessment (DRA) processes. Particularly, choosing an appropriate risk assessment method in IIoT systems is challenging since they provide different attack surfaces at multiple abstraction layers ranging from electronic devices (e.g. processors and memories to process data and sensors and actuators to control physical processes) to software (e.g. operating systems and applications), humans, and, last but not least, network connections (e.g. WiFi). In such a context, adapting classic static risk assessment methods is not straightforward, and, thus, requires another method, at an additional cost, which allows systems to update the risk level at real-time, as well as dealing with the changing nature of security threats (Holgado, Perez, Perez, & Villagra, 2015) and various abstraction layers which are usually involved.

Due to the importance of risk assessment process, several surveys have been published dealing specifically with security risks in information systems and computer networks. For instance, information security risk assessment concepts are presented in (Zhiwei & Zhongyuan, 2012), (Behnia, Rashid, &

Figure 1. Risk assessment process as part of IT Governance areas



Chaudhry, 2012), and, moreover, various risk evaluation methodologies for information systems are analyzed based on the structures of these systems. A recent work also proposes a method to assess risks in such an environment (de Gusmão, e Silva, Silva, Poleto, & Costa, 2016).

Beside these, analyzing risks in Cyber-Physical Systems (CPS) (Lee, 2008), (Poovendran, 2010), like smart cities and smart grids, is discussed in (Kurosu, 2013), (Zhou & Chen, 2012). However, as a result of current incline of research community to DRAs, another work (López, Pastor, & Villalba, 2013) discusses dynamic risk management concepts for computer networks, and a short literature review of DRA approaches is presented therein.

Despite the abundance of DRA approaches in recent years, IT managers face the challenge of implementing DRA in very assorted scenarios. For the sake of illustration, we identify three representative settings – regular computer networks, Internet of Things (IoT) environments and Industrial Control Systems (ICS). These three settings are typically found in the underlying IIoT systems resulting from 4IR. Thus, ICSs usually govern computers and IoT devices to automatize the production process. These settings differ significantly in the degree of centralization and the resources of their nodes. Thus, regular computer networks are formed by potentially unconstrained devices which can be managed from a single manager system. On the contrary, IoT devices are resource-limited elements which usually operate in a decentralized manner. In-between these two, ICSs are formed by sensors with limited capacity, which are managed by regional devices with enough computational resources. Since each factory of the 4IR can be formed, to different extents, from these settings, we analyze them separately. This makes the analysis be suitable for any IIoT settings, as well as for any general IT environments in which these systems come into play.

In order to assist IT managers in choosing the most suitable DRA technique for their particular setting, in this paper we analyze 27 DRA works and provide an overview of how they deal with the three main issues in a DRA mechanism – assets, threats and risk calculations. Furthermore, we also study how these mechanisms have been applied into the aforementioned IT settings. Thus, our main contribution is a decision guide that is intended to provide IT managers (of IIoT systems, but not only) with enough background on DRA and the suitability of existing techniques for their concrete scenario.

The remainder of this paper is organized as follows: Section 2 provides a background on security and risk management in computer networks. Risk assessment is presented in Section 3. The analysis on dynamic risk assessment models and approaches is presented in Section 4. Section 5 points out open research directions and, finally, Section 6 concludes the paper.

BACKGROUND

In this Section, the main notions of IT security governance, and risk management are introduced. These issues form the context in which risk assessment is placed.

IT Security Governance

Due to extraordinary extension of computer networks and the Internet, there is an ever increasing need for security. Therefore, IT security governance is gaining attention from both academia and industry to improve the reliability of computer networks.

Several standards have addressed this issue. On the one hand, generic IT governance standards such as COBIT (De Haes, Van Grembergen, & Debreceny, 2013) and ITIL (Clinch, 2009) have covered security aspects as one of the areas in which controls have to be included. On the other hand, ISO 27001 (Calder & Watkins, 2010) specifically focuses on security management. Among the different steps involved in this process, ISO 27001 provides with a guideline for risk assessment and management.

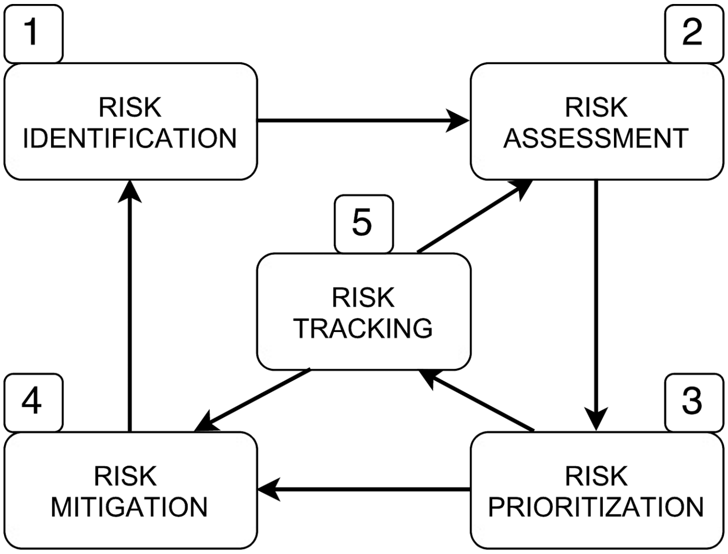
Risk Management

Risk management is a general process which consists of some important sub-processes. It usually includes risk identification, risk assessment, risk prioritization, risk mitigation and risk tracking (recall Figure 1) (Garvey, 2008). These procedures are not independent from each other, but related as shown on Figure 2.

According to the description by Garvey, risk identification (No. 1 in Figure 2) is the first step in the risk management process (Garvey, 2008). Its objective is the early identification of risks that can impact on the system's assets in particular, and on system's performance in general. In the second step (No. 2 in Figure 2), an assessment is made based on the impact that each risk event could have on the assets of system. Hardware devices such as routers, software applications, information, people, and also procedures can all be considered as critical assets.

After risk identification and assessment, security risks are assigned different priorities (No. 3 in Figure 2). A major purpose for prioritizing risks is to form a basis (link 3 → 5 in Figure 2) for allocating critical resources, including additional personnel or funding to resolve those risks (Garvey, 2008). Different risk mitigation plans (No. 4 in Figure 2) are designed to manage, eliminate, or reduce risks to an acceptable level (Garvey, 2008), (Chołda & Jaglarz, 2016). Apart from the previous sequential tasks, risk tracking (No. 5 in Figure 2) is also considered as a supervisory procedure (Garvey, 2008). The main goal of risk tracking is the exact monitoring of risk assessment (link 5 → 2 in Figure 2) and mitigation (link 5 → 4 in Figure 2) strategies based on the priorities of risks.

Figure 2. A general view of a risk management system



RISK ASSESSMENT

Among the risk management tasks described in Section 2.2, risk assessment is receiving attention for its relevance to determine the impact of risks (Dongmei, Changguang, & Jianfeng, 2007). For this purpose, several methodologies have been proposed (Ionita, Hartel, Pieters, & Wieringa, 2013). CRAMM (Yazar, 2002), OCTAVE (Caralli, Stevens, Young, & Wilson, 2007), NIST SP800-30 (Blank & Gallagher, 2012), and MAGERIT (Crespo, Amutio-Gómez, Candau, & Mañas, 2006) are among the most popular ones (Ionita et al., 2013), (Shedden, Scheepers, Smith, & Ahmad, 2011). All of these methods have three identifiable steps in common, namely (1) asset identification and analysis; (2) threat and vulnerability identification, and (3) countermeasure selection. In the first step, all the assets of an organization are specified. In the second step, vulnerabilities and threats are identified, and, finally, numerous security strategies and plans are set in the third step to mitigate or eliminate the risk posed by identified threats.

It is worth emphasizing that assets, vulnerabilities, and threats are considered as key factors in most risk assessment models. However, vulnerabilities are usually considered implicitly along with security threats since there would not exist any threat until there are some vulnerabilities within the system. For the sake of simplicity and without loss of generality, in what follows the process of risk assessment and its underlying concepts are explained taking MAGERIT methodology as the basis.

Basic Steps

Risk assessment involves some important steps and concepts which are shown in Figure 3 (Crespo et al., 2006). They are summarized as follows.

1. Determining the essential assets, their inter-relationships, and their importance (value) for the organization.
2. Determining the threats to which those assets are exposed.

3. Estimating the impact, defined as the damage to the asset arising from the appearance of the threat.
4. Estimating the risk degradation level, i.e. the level (the amount) of damage which is produced by threats.
5. Estimating the occurrence probability (frequency or likelihood) of degradations which is caused by threats.
6. Estimating the risk using the calculated probability and the impact from the aforementioned steps.

The assets of an organization have some values. These values are not initially limited to numeric magnitudes, but they can be observed from the "need to protect assets" perspective-- the more valuable an asset is, the higher protection it will need. In assigning values to assets, several dimensions, namely confidentiality, integrity, availability, authenticity, and accountability should be considered (Crespo et al., 2006).

Once it has been determined which security dimensions are of interest in each asset, they must be valued. Valuation is in fact the determination of the loss of value caused by an incident. For example, the integrity of data may have higher importance in contrast with other factors. Therefore, it should be assigned a higher weight in determining the value of this asset. After the valuation process, some administrators may consider priorities for their organization's assets according to their values (Boyer, Dain, & Cunningham, 2005). For instance, software assets could probably have more priority than physical assets since disruption of one or two devices would lead to fewer losses in comparison to a software incident. However, this is totally dependent to the application context and priorities that are considered by administrators.

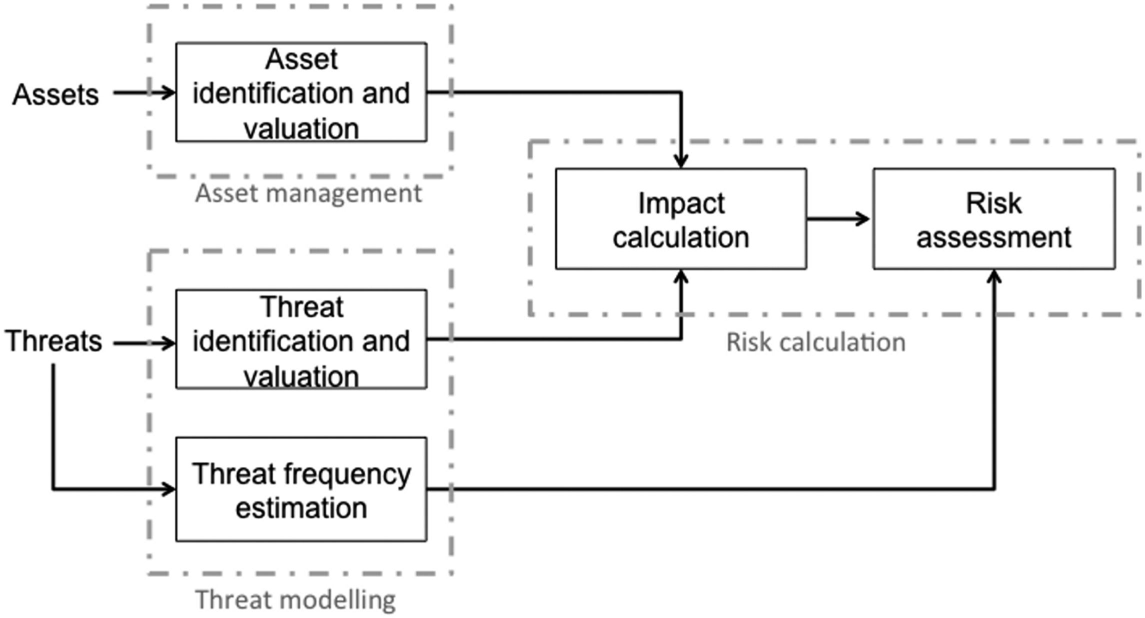
When assets are the victims of threats, not all of their dimensions are affected and not all to the same degree (Crespo et al., 2006). As an example, the integrity of information in the software database might be the target of attackers. Therefore, the exposure of assets must be estimated considering the degradation and the likelihood of threats. Degradation is the amount of damage which is produced by threats and will be imposed to the assets, and likelihood is the frequency or probability of threats' occurrences. Likelihood can be modeled either numerically (e.g., number of occurrences in a period) or descriptively (e.g., from "very frequent" to "rare"). Sometimes, likelihood of attacks can be expressed by numerical values, and, sometimes, it cannot be performed in that way and should be modeled by nominal scales.

By knowing the values of assets (in their different dimensions) and the degradation caused by attacks, the impacts of assets can be determined directly using Equation 1. Here, D .is the amount of degradation caused by a particular threat, and V .is the overall value of a particular asset. Thus, as it is clear, impact (I . is a function of threats' degradations and assets' values (Equation 1). Thus, the higher the degradation of threats and the higher the value of assets is, the more impact of threats.

$$I = f\left(D, V\right). \tag{1}$$

By knowing the impact of threats to assets, the risk can be derived directly taking into account the likelihood of threats' occurrences. Thus, the total risk of an IT environment formed by assets is calculated following Equation 2 (Kaplan & Garrick, 1981) similar to another formulation which has been proposed for Supervisory Control and Data Acquisition (SCADA) systems (Cherdantseva et al., 2016).

Figure 3. Main elements of a risk assessment system


Assets
Asset identification and valuation
Asset management
Impact calculation
Risk assessment
Risk calculation
Threats
Threat identification and valuation
Threat frequency estimation
Threat modelling

$$R_{Total}\left(t\right)=f\left(R_{ij}\left(t\right)\right)=f\left(P_{ij}\left(t\right),I_{ij}\left(t\right)\right),\qquad i=1,2,\ldots,M,\ j=1,2,\ldots,N\ . \tag{2}$$

Thus, the total risk is indeed a function of individual risks caused by various threats (i .in Equation 2) on each asset (j .in Equation 2), and an individual risk on each asset j .is a function of all threats' probabilities (P_{ij} .in Equation 2) and their impacts (I_{ij} .in Equation 2). As it is obvious from Equation 2, all these magnitudes may change over time

Types of Risk Assessment

Risk assessment can be discussed considering two criteria - first, how risk values are calculated and presented; second, how frequent they are evaluated and actually updated.

Regarding the first criterion, risk assessment methods can be implemented by following either a quantitative or a qualitative approach (Zhang, Jiang, Cui, Zhang, & Xia, 2010). Quantitative risk assessment systems use formulas and mathematical expressions to produce numeric estimates for risks. On the other hand, qualitative risk assessment methods estimate risks descriptively by using terms, such as "low", "medium", and "high". The latter approach is preferred for areas in which risk can hardly be estimated as an explicit value or in occasions where all the threats cannot be identified and registered technically.

Considering the second criterion, risk assessment systems can follow either a static or dynamic approach. Recalling Figure 3, in dynamic settings, several things may change over time. Initially, threats may be variable in three main areas (Holgado et al., 2015), (Crespo et al., 2006). First of all, new attack methods might devise in future (dynamicity of type), and, more importantly, the assessment of threats' capabilities would become inappropriate (Crespo et al., 2006). Secondly, the frequency of attacks (dynamicity of frequency) may also change over time, i.e. the probabilities of threats' occurrences are considered to be variable in dynamic risk assessment systems (López et al., 2013). Thirdly, the severity of threats (dynamicity of severity) may also change from time to time. Apart from threats, different aspects of assets may also change. This change would be the addition, modification, or suppression of assets within an organization, or even a change in their valuation (López et al., 2013). Finally, vulnerabilities of assets to attacks could also be variable at different points of time (Holgado et al., 2015).

Considering all these issues, static methodologies for risk assessment lack practical sense in changing scenarios, since they evaluate risks at discrete time intervals, thus being unable to adapt to new threats or changes in assets. On the contrary, Dynamic Risk Assessment (DRA) systems should be capable of estimating risks continuously considering the dynamic nature of environment.

DYNAMIC RISK ASSESSMENT

Once the basic concepts of risk assessment have been introduced, this Section focuses on the core of this paper – Dynamic Risk Assessment (DRA) techniques. For this purpose, each of the three main elements of a DRA mechanism (asset management, threat modeling and risk calculation, recall Figure 3) is described separately based on the information gathered in Table 3. The purpose of this Section is to illustrate the different DRA approaches taken in literature. Based on these alternatives, a decision guide will be presented in the following section to help the reader decide which ones best fit to his current environment.

Assets Management

Assets management deals with three main issues, including types of the assets which need to be considered, their behavior, and, also, their valuation. Regarding the types of assets, (Haslum, Abraham, & Knapskog, 2007) assumes that they can be both hardware and software, while (Haslum & Årnes, 2006) and (Årnes et al., 2005) have a more general view since the assets are considered to be within a computer network; however, they do not discuss exactly which components of a computer network have been considered as assets. Beside these, (Qi, Liu, Zhang, & Yuan, 2010) takes some extra options into account, including fame, reputation, public trust, and employees' confidence. Regarding the behavior of assets, (Holgado et al., 2015), (Qi et al., 2010), (W. Li & Guo, 2009), (G. Chen, 2010), and (Årnes, Valeur, Vigna, & Kemmerer, 2006) consider the change in assets although they do not discuss the aspects through which assets might change.

Speaking about the valuation of assets, several works such as (Haslum & Årnes, 2006), (Årnes et al., 2005), (Årnes et al., 2006), (Ma, Li, & Zhang, 2009), (Yu-Ting, Hai-Peng, & Xi-Long, 2014), (Liao, Li, & Song, 2010), (Poolsappasit, Dewri, & Ray, 2012), (Wu & Zhao, 2014), and (Cheng, Xu, Jia, & Zou, 2008) consider confidentiality, integrity, and availability dimensions in order to valuate assets, while (Wrona & Hallingstad, 2010) has a special focus on the availability. (Haslum et al., 2007) and (Haslum, Abraham, & Knapskog, 2008) concentrate on other factors, namely cost, criticality, sensitivity, and recovery, while (Qi et al., 2010) assumes that assets are valuated manually. Ultimately, a few number of works (Boyer et al., 2005), (W. Li & Guo, 2009) propose the dynamicity of assets' priorities. Within these models, assets are assigned different priorities that can change at various moments according to any modifications in the administrator's policies.

Threat Modeling

This section focuses on the threats' assumptions, and, also, the threat modeling technique adopted in different DRA works. Concerning threats, most of the systems consider Distributed Denial of Service (DDoS) attacks (W. Li & Guo, 2009), (Årnes et al., 2006), (Ma et al., 2009), (Wu & Zhao, 2014), (Wrona & Hallingstad, 2010), (Haslum, Abraham, et al., 2008), (Ahmed, Al-Shaer, Taibah, & Khan, 2011), (Rezvani, Ignjatovic, Bertino, & Jha, 2014). However, (Liao et al., 2010) and (Phillips & Swiler, 1998) have developed a program to simulate the behavior of an intruder. Several models also focus on the dynamicity of threats in different aspects. Security threats may change in type (i.e. new threats might emerge) (Ahmed et al., 2011), (Phillips & Swiler, 1998); the frequency of threats can be variable (Poolsappasit et al., 2012), (Wrona & Hallingstad, 2010), (Phillips & Swiler, 1998), (Volftrub & Polikarpov, 2007), (Hu, Ding, & Huang, 2008); and, also, their severity may change over time (Qi et al., 2010), (W. Li & Guo, 2009), (Haslum, Abraham, et al., 2008). From the analyzed collection, some works exist (Holgado et al., 2015), (Wu & Zhao, 2014), (Cheng et al., 2008) which do not have any assumptions on the changes of threats.

To model threats, researchers have used a variety of tools, including Hidden Markov Models (HMMs), attack graphs and threat clustering, to name a few. According to our observations, HMMs (taken in 10 works) and graph-based data structures (suggested in 7 works) are the most frequent techniques used for threat modeling. Threat modeling becomes critical as they influence how the likelihood (probability) of threats and their impacts on assets are measured. Therefore, each of these techniques is described in what follows.

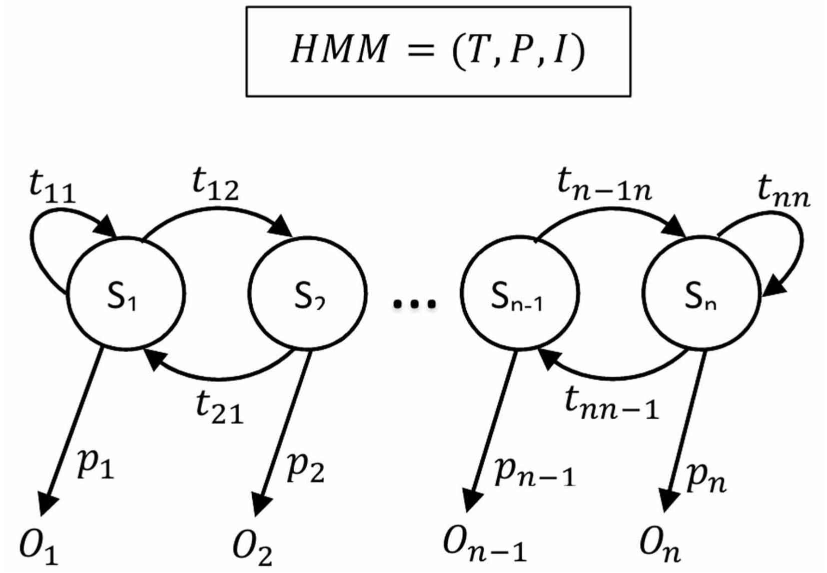
Hidden Markov Models (HMMs)

HMMs are statistical models, mainly based on state transitions (e.g. security states of assets), that are triggered by events (or threats) which happen randomly according to a probability distribution (Haslum, Moe, & Knapskog, 2008). Moreover, it can be used to predict future unobserved events based on previous records and witnesses (Gao, Sun, & We, 2003). Hidden Markov models have been used in a variety of works (Holgado et al., 2015), (Haslum et al., 2007), (Haslum & Årnes, 2006), (Årnes et al., 2005), (W. Li & Guo, 2009), (G. Chen, 2010), (Årnes et al., 2006), (Ma et al., 2009), (Yu-Ting et al., 2014), (Haslum, Abraham, et al., 2008) to model security threats.

In an HMM, the assets of interest are assumed to have different security states s_i .which are defined and set by administrators and are demonstrated in Figure 4. For instance, three security states, including "Safe", "Under Attack", and "Compromised" may be considered for each asset.

HMM includes a triple to model the state of the system (W. Li & Guo, 2009). These are "Initial Matrix", "Observation (Probability of Observation) Matrix" and "Transition Matrix" (I, P and T in Figure 4, respectively). Initial matrix demonstrates the initial security state of an asset. Observation matrix is our observation (O_i .in Figure 4) about the probability of an attack (p_i .in Figure 4) when an asset is in a particular state. Ultimately, Transition matrix includes the probabilities of transitions between the states of an asset (t_{ij} .in Figure 4). Transitions are due to different types of attacks over time. One of the key aspects of HMMs is the definition of these matrices. Thus, some approaches have applied techniques such as genetic algorithms to optimize the values of these matrices (W. Li & Guo, 2009).

Figure 4. A general view of a Hidden Markov Model (HMM)



Several HMMs can also be combined together for modeling threats. For instance, within the system proposed in (Haslum, Abraham, et al., 2008), the information of HMMs is combined to extract the probability of an attack, and, next, this parameter is mixed with other factors such as probability of threat success and its severity using fuzzy logic (explained later in this Section).

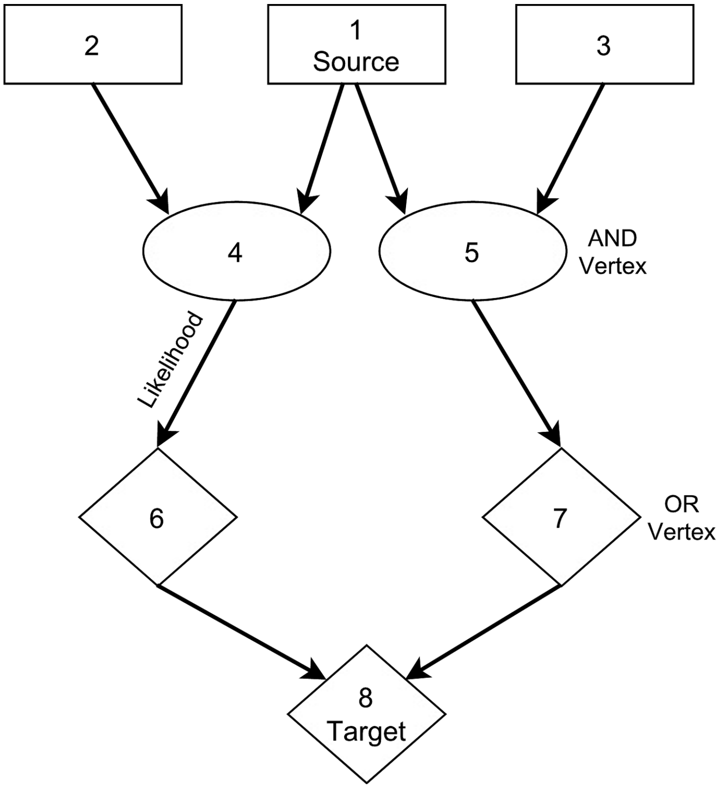
Graph-Based Modeling Techniques (GMs)

Graphs are also applied to several models of dynamic risk assessment. There is a slight difference between various graphs used here and HMM. Within these graph structures, nodes show the attacker states whereas in HMM nodes represent security states of assets and the probability of an attack to be exercised in each state. Thus, HMM can be considered as an asset-centric threat modeling technique while graph-based modeling techniques are attack-centric showing different attack steps an attacker can pass to reach the desired target. Three graph structures are used for this purpose, namely Attack Graphs (AGs), Bayesian Networks (BNs) and Petri nets (PT Nets) which are introduced briefly in what follows.

An attack graph demonstrates possible multi-step attacks (attack paths) by representing the causal relationships among different vulnerabilities (J. H. Li & Levy, 2010). In particular, an AG model our knowledge about how multiple vulnerabilities may be combined for an attack. Here, nodes represent attack states while edges show exploits. Also, nodes can be assigned a numerical value reflecting the likelihood of an exploit in a particular state or the expected impact. This technique is adopted in works such as (Phillips & Swiler, 1998) and (Alhomidi & Reed, 2013) in combination with quantitative metrics.

A small sample of an attack graph is illustrated in Figure 5 to provide a general imagination of this modeling technique. According to this figure, “vertex 8” shows the target of any possible attacker which depends upon some combination of the other vertices. Ellipse vertices, called “AND” (e.g. vertex 5), can be exploited only if both pre-conditions (vertices 1 and 3) are satisfied, while diamond vertices, called “OR” (e.g. vertex 8) can be exploited by either or both of the pre-conditions (e.g. vertices 6 and

Figure 5. A simple Attack Graph (AG)



7). Lastly, vertices 1, 2, and 3 are called “leaf” vertices representing either a network configuration (e.g. an open port) or an existing vulnerability.

A critical problem regarding attack graphs is that the attackers’ plans are not always completely known. In other words, there exists a degree of uncertainty in attackers’ behavior (J. H. Li & Levy, 2010), and, for this reason, the logical causality modeled by a deterministic attack graph is not sufficient to identify all security threats. Moreover, AGs cannot handle situations where the exploitation of a vulnerability affects the likelihood of exploiting another vulnerability. Thus, BNs are proposed in some papers (Poolsappasit et al., 2012), (Wu & Zhao, 2014), (Wrona & Hallingstad, 2010), (Dantu, Kolan, & Cangussu, 2009) as an alternative although their construction from an attack graph is not a trivial task (J. H. Li & Levy, 2010).

There are some differences between BNs and AGs in terms of modeling. In BNs, nodes represent random variables (e.g. attack state, hypotheses) while edges show conditional dependencies which do exist between these variables. BNs make use of a Conditional Probability Table (CPT) to demonstrate the probability of a single variable (node) with respect to other nodes (its parents). Using this modeling technique resolves some issues which arise in AG modeling for instance when the order in which vulnerabilities are exploited is important. This technique determines quantitative values representing the overall system security by considering the combined effect of all known vulnerabilities. Another major difference which exists between BNs and AGs is in the risk calculation process which will be discussed later. One important application of BNs is to represent the uncertainty of an unavailable period – it may be due to misconfiguration or the result of a DoS attack.

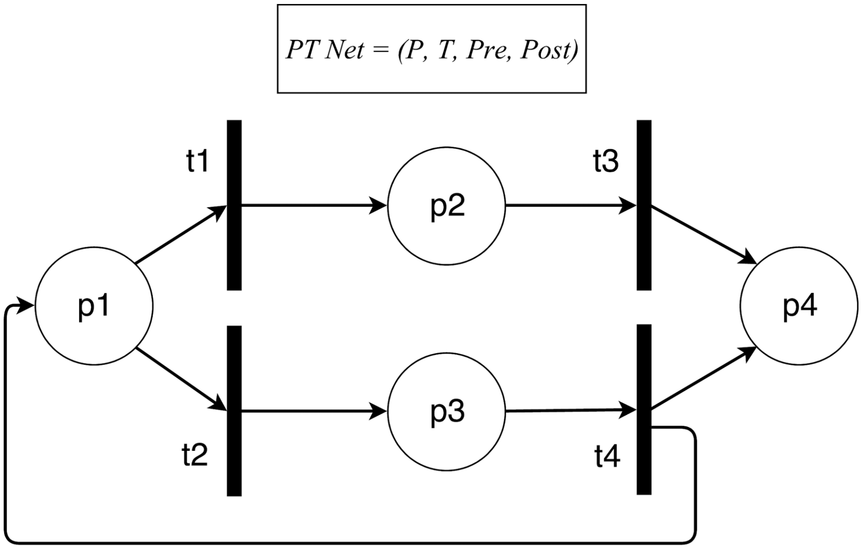
As a third graph-based structure, PT Nets (Place-Transition Nets) are appropriate to model discrete event systems and represent dynamic processes, specifically when few events may occur concurrently (Tabak & Levis, 1985). Therefore, in what comes to security threats, they can provide a model for estimating risks continuously (Liao et al., 2010). As shown in Figure 6, a basic PT Net is a directed bigraph with two disjoint set of nodes such that no two graph vertices from the same set are adjacent. The first set of nodes are Places (i.e. conditions, represented by cycles), and the second set of nodes are Transitions (i.e. events that may occur, represented by bars). The directed arcs describe which places are pre-conditions and/or post-conditions for which transitions (signified by arrows). The other advantage of using PT Nets is that they are well described by an algebraic formalism as a quadruple which include the set of Places (P .in Figure 6), Transitions (T .in Figure 6), Pre-(and Post-) conditions (Pre and Post in Figure 6) as shown in Figure 6.

Another variant of graph-based modeling can be observed in the work by Alhomidi and Reed (Alhomidi & Reed, 2013). They propose an epidemiological-based technique which base on the very behavior of the nature while addressing infections (Alhomidi & Reed, 2013). Within this model, a set of cells are considered that can send "danger" or "alarm" signals to some aggregators. These aggregators can further inform other group of cells, which decide whether the signals are enough to declare infection. In such a case, a set of countermeasures (e.g. killer cells) are deployed. By using such signals and communications and by imitating the immune response system of human body, this system is capable of modeling security threats in an efficient way.

Hierarchical Modeling Techniques (HMs)

Hierarchical threat models assume that any system can be structured in such a way that several hierarchical levels can be identified within it. Components can belong to different levels, and a higher component can include others of lower hierarchical level. They can also be united into sub-systems in a specific

Figure 6. A basic PT Net



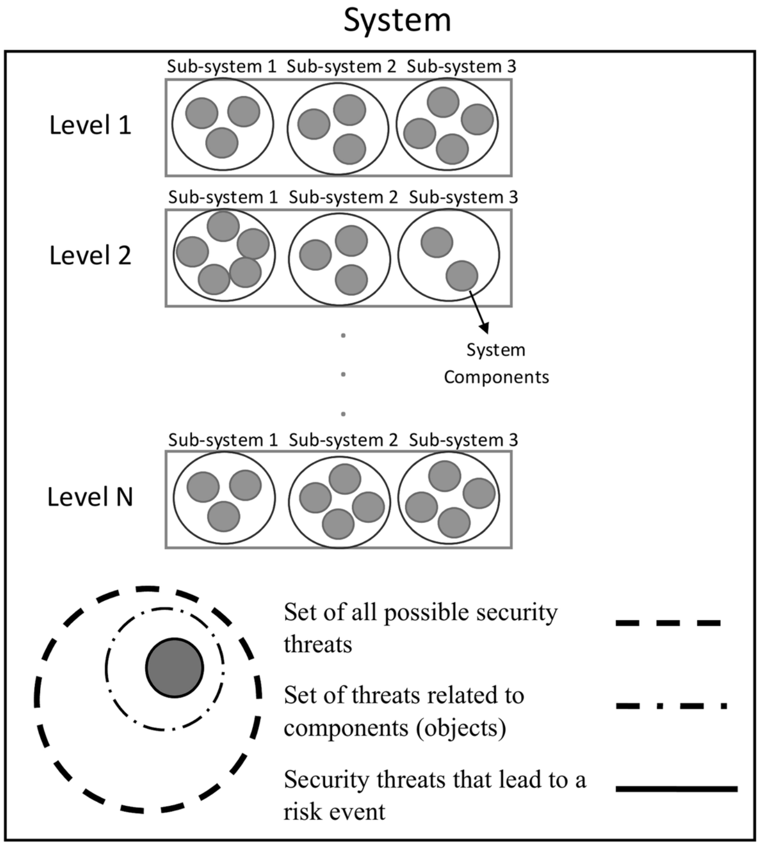
hierarchical level (Volftrub & Polikarpov, 2007). Each of these components are assumed to be vulnerable to a sub-set of threats from the set of all possible security threats which may appear. Also, not all of the threats would be of interest, but only those which may have negative impacts on the components and may lead to risk events.

Additionally, particular sets of threats can be determined for each sub-system (Volftrub & Polikarpov, 2007). These threats are not related to any object included in a sub-system, but only to the sub-system as a whole. Sub-systems can also be united into larger groups for which the same rule exists. This process is continued until the level of the whole system is reached (Figure 7).

Threats Clustering (TC)

Clustering of security threats is another modeling technique presented in a number of works (Liu, Chen, Dai, Wang, & Cai, 2005), (Y. Chen, Jensen, Gray, Cahill, & Seigneur, 2003). Within this model, each interaction (of mobile and autonomous entities in a ubiquitous computing environment as in (Y. Chen, Jensen, Gray, Cahill, & Seigneur, 2003)) with the environment is considered as a feature vector which consists of some elements that specify the context of the interaction, the participants, and other relevant historical or current information.

Figure 7. The hierarchical threat modeling technique in (Volftrub & Polikarpov, 2007)


System
Sub-system 1
Sub-system 2
Sub-system 3
Level 1
Level 2
System Components
Level N
Set of all possible security threats
Set of threats related to components (objects)
Security threats that lead to a risk event

A clustering procedure is used to group different feature vectors which have been derived from the historical data. When clusters are produced and confirmed, the number of unexpected points in clusters are easy to collect for historical data, from which the risk value is easy to calculate. More details for the process of risk calculation are presented in Risk Calculation section.

Fuzzy Logic (FL)

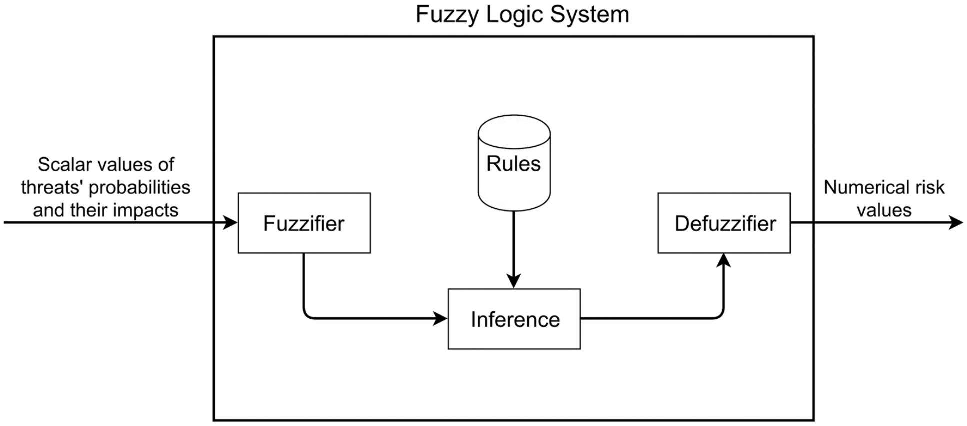
Fuzzy logic is another threat modeling technique proposed in (Michalopoulos, Mavridis, & Jankovic, 2014) due to the complexity and uncertainty which exist in ubiquitous computing environments (Liu et al., 2005). Fuzzy logic has become increasingly popular in addressing imprecision, uncertainty and vagueness (Liu et al., 2005). A fuzzy logic system can be defined as the nonlinear mapping of an input data to a scalar output data (Mendel, 1995). It consists of four main parts, namely fuzzifier, rules, inference engine, and defuzzifier (Rutkowski & Cpalka, 2003) (Figure 8).

In this modeling technique, initial numerical (or scalar) values of threats (and their impacts) are first converted to fuzzy sets using fuzzy membership functions. Fuzzy sets usually carry names that conform to adjectives we usually use in our daily linguistic usage such as “low”, “medium” and “high” which may demonstrate the severity of threats and help in dealing with uncertainties. This process is known as fuzzification. In the second step, an inference is made based on a set of rules (also known as fuzzy IF-THEN rules) which is important in the process of risk calculation and will be discussed later. Finally, membership degrees of the fuzzy sets are interpreted into a real value of risk through deffuzification process.

Other Models

Other works are not based on any of the discussed models (Boyer et al., 2005), (Qi et al., 2010), (Ahmed et al., 2011), (Rezvani et al., 2014), (C. Fu, Ye, Zhang, Zhang, & LanSheng, 2010). For instance, (Boyer et al., 2005) models and security threats by a set of rules written in Security Assessment Declarative Language (SADL). This language can combine knowledge of the IT environment, including critical

Figure 8. A general view of a fuzzy logic system



assets and vulnerabilities. Additionally, it separates information about the local network configuration from information about common attack patterns.

Risk Calculation

Once security threats are modeled, risk can be estimated considering the probability (frequency) and the impact of all possible threats as demonstrated earlier in Figure 3. In what follows, risk calculation will be discussed separately for each of the threat modeling techniques presented in Threat Modeling section. Before entering into this discussion, two dimensions need to be considered precisely regarding the risk calculation process. First, it must be analyzed whether risks are evaluated using quantitative or qualitative metrics (recall Section 3.2). In considered works, quantitative metrics are adopted in the majority of contributions (24 works). The second issue to consider is whether DRA approaches re-estimate and update risk values continuously or by intervals, due to the changes that may occur at different periods of time. Approaches which capture risk values continuously (11 works) can provide with a real-time evaluation of risks. Nevertheless, it comes at a cost of using a flexible threat modeling technique capable of timely adapting to these changes. On the other side, models which capture risk values at short intervals (suggested in 7 works) are less complex as they are based on simpler threat modeling techniques. However, they are prone to miss new security threats which might happen between these intervals.

In HMM modeling, the risk at each security state can be estimated by having the probability of threats (in Figure 4), and the impact of those threats on asset in a specific security state (recall Eq. 3). Finally, the overall risk is calculated by adding up these risks as the asset moves from one state to the other.

Among models proposed based on HMMs, 6 systems (Haslum et al., 2007), (W. Li & Guo, 2009), (Årnes et al., 2006), (Ma et al., 2009), (Yu-Ting et al., 2014), (Haslum, Abraham, et al., 2008) re-estimate risk values in considerably short time intervals using Discrete Time HMM (DTHMMs) in order not to miss any new changes in the environment, and 4 models (Holgado et al., 2015), (Haslum & Årnes, 2006), (Årnes et al., 2005), (G. Chen, 2010) evaluate risks using Continuous Time HMM (CTHMMs). In DTHMM, observations are updated at specific and regular points of time, while in CTHMM, observations are made at irregular (continuous) time points as the security states of assets evolve in continuous time (Elliott, Aggoun, & Moore, 2008). Transition probabilities in CTHMMs are a function of time and of transition intensities (Elliott et al., 2008). Briefly speaking, another matrix is also constructed in this type of HMM except the three aforementioned ones called "Transition Rate/Intensity Matrix".

Qualitative risk assessment based on HMMs measures risks using linguistic terms such as low, medium, or high (Haslum et al., 2007), while other works (Holgado et al., 2015), (Haslum & Årnes, 2006), (Årnes et al., 2005), (W. Li & Guo, 2009), (G. Chen, 2010), (Årnes et al., 2006), (Ma et al., 2009), (Yu-Ting et al., 2014) measure the overall risk in a quantitative way.

In graph-based modeling, the risk calculation is straightforward. The attack path is traced from the root to the target, and, at each state, the likelihood of a vulnerability to be exploited is multiplied by its negative impact. Thus, the overall risk is measured by adding all these values at different states from the source to the target. In Bayesian networks, Bayesian inference methods are used for the same purpose (Frigault & Wang, 2008).

Among graph-based modeling techniques, all of them (Liao et al., 2010), (Poolsappasit et al., 2012), (Wu & Zhao, 2014), (Wrona & Hallingstad, 2010), (Phillips & Swiler, 1998), (Alhomidi & Reed, 2013) evaluate risks in a quantitative manner. Moreover, the systems proposed in (Liao et al., 2010) and (Wrona

& Hallingstad, 2010) update risk values continuously, while other systems are not clear in terms of how frequent they update risk values.

In epidemiological-based models, risk is calculated similar to graph-based modeling techniques. In particular, different cells percept security threats from the environment and send appropriate alarms to some aggregators based on the frequencies and the impacts of threats. Then, these aggregators sum up the total risk values received from all the cells and can also trigger other cells if this value exceeds a predefined threshold. Systems that are based on this model (Alhomidi & Reed, 2013) can estimate risk values continuously or in real-time.

Models based on clustering divide security threats into different groups or clusters based on some features. When clusters are produced, risk probabilities of all inner feature vectors are calculated typically using a parameter called Average Loss Rate (ALR). ALR is actually a proportion which shows the number of unexpected interactions (between mobile and autonomous entities in a ubiquitous computing environment as in (Y. Chen, Jensen, Gray, Cahill, & Seigneur, 2003)) to the total number of interactions. An intuitive idea is to see how each feature vector is close to the average vector within any clusters. Therefore, the risk probability associated with each feature vector depends on its similarity to the average vector and the ALR.

When the framework or architecture is trained using the historical data, it can be used to have a prediction of risks in future by following a similar process. In particular, a new vector is produced by extracting all features from the current information. Then, the clustering procedure is applied to this new vector after which it should belong to one of the previous constructed clusters. Finally, the risk value of this feature vector is calculated through multiplying its similarity rate to the average vector by the ALR parameter. It must be noted that history information usually involves a significant amount of risk-related information. Thus, some methods are suggested in (C. Fu et al., 2010) to reduce the data dimension.

Both of the works that use clustering for modeling security threats (Liu et al., 2005), (Y. Chen et al., 2003) evaluate risks quantitatively. Furthermore, regarding how frequent they update risk magnitudes, (Y. Chen et al., 2003) uses a continuous mechanism, while (Liu et al., 2005) does not present any information about this criterion.

In a fuzzy based model, a fuzzy set is constructed based on several linguistic input parameters (such as threats and their corresponding impact). Then, a system is used to make an inference using some predefined (if-then) rules (e.g. "*if the threat has a high probability and its impact is very high, then the risk value is very high*"). Finally, the resulting fuzzy output is mapped to a crisp value (numerical value) using the membership functions (through the defuzzification process). This output represents the risk according to the input values. As an example, the work by Michalopoulos et al. measures risks qualitatively using this modeling technique and re-estimates (updates) risk values continuously (Michalopoulos et al., 2014).

Other methods calculate risk values in a different way and are not based on any of the aforementioned threat modeling techniques. The framework introduced in (Ahmed et al., 2011) quantifies objectively the most significant security factors, which include existing vulnerabilities, historical trend of vulnerabilities of the remotely accessible services, prediction of potential vulnerabilities for these services and their estimated severity, unused address space, and, finally, propagation of attacks. The first five factors are used to calculate the threats likelihood, while the last parameter, propagation of attacks, is used to estimate the impact of threats on the assets. Doing so, the overall risk is evaluated considering the likelihood of threats and their impacts on assets. The framework proposed here is in fact based on this hypothesis that if a service has a highly vulnerability prone history, then there is higher probability that the service will become vulnerable again in the near future. However, as mentioned earlier, history information usually includes an extra amount of risk-related information. Thus, (C. Fu et al., 2010) proposes a method to reduce the data dimension. Different from (Ahmed et al., 2011), economical loss derived from security risks is taken into account in (Qi et al., 2010).

Finally, in another model (Rezvani et al., 2014), the risks for both hosts (as an asset) and information flows are assessed, different from other systems that only rely on the risks of flows. The mentioned system is based on this idea that the risk score of a flow influences that of its source and destination hosts, and also the risk score of a host is evaluated by taking into account the scores of flows initiated by or terminated at the host.

From these contributions, all of them evaluate risks quantitatively. Furthermore, (Boyer et al., 2005) and (Ahmed et al., 2011) update risk values continuously different from (Rezvani et al., 2014) that re-estimates risk magnitudes at short time intervals. Other works (Qi et al., 2010), (C. Fu et al., 2010) do not include any information regarding this criterion.

DECISION GUIDE ON DRA FOR DIFFERENT SETTINGS

After a brief introduction of DRA main elements, including assets management, threat modeling, and risk calculation, an appropriate decision guide is presented in this section for three important application contexts related to the 4IR and its underlying IIoT -- Computer Networks (CNs), the Internet of Things (IoT) and Industrial Control Systems (ICSs). In particular, we do address three main issues in what follows. First, how to select the best threat modeling technique based on the identified assets and threats and the characteristics of the application context. Second, what specific architecture to adopt in calculating risk values of a DRA process for each context. Finally, what type of risk calculation to choose based on the assets and threats.

An efficient and reliable DRA is challenging without having a precise modeling of threats. Identifying the type and amount of critical assets, the behavior of threats, and, also, specific characteristics of the application context to which DRA is going to be applied are all some crucial factors which need to be considered in threat modeling. Table 1 shows the suitability of threat modeling techniques based on different assumptions for assets and threats. DRA is particularly useful when threats do change over time (Figure 9). So, once threats are known to be variable, critical assets need to be identified and valued. Then, if threats are found to be categorizable as well, hierarchical modeling techniques can be applied to model threats. Here, a threat on one component in a specific level of system hierarchy would not have the same impact as another threat on a different component in the higher level. If variable threats are not categorizable, the amount of assets and the uncertainty in threats should be considered in adopting other modeling techniques. Therefore, when the amount of assets is big and a high uncertainty exists in threats, using graph structures to model threats (GMs), fuzzy logic (FL) or threats clustering (TC) are the most appropriate techniques. However, when the amount of assets is limited and a high uncertainty exists in threats, HMM modeling is applied. This technique is particularly useful when assets of interest have different security states. Moreover, when assorted types of threats are expected, any modeling techniques can be used except the hierarchical ones in the case we are sure threats are not categorizable.

Due to the uncertain nature of threats appearing in CNs and IoT, HMMs and GM are widely used to model security threats in these application contexts. However, as mentioned earlier, HMMs are suitable when the amount of assets is limited. Furthermore, both of these modeling techniques do not scale well when the number of assets grows excessively. On the other hand, due to the limited number of assets which usually exist in an ICS, HMMs and GM have been used widely to model security threats. Nevertheless, other threat modeling techniques can also be applied as there is less uncertainty in the upcoming threats in this context. Risk assessment systems proposed for ICSs may need to be complemented with some additional considerations that do not exist when doing the same process for traditional IT systems since the impact of threats in an ICS may include both physical and digital effects. As for the goal of this study, decision guides proposed for DRA systems are focused on the risks which are related to information not physical devices.

Risk calculation architecture is the second import issue in DRA which have to be chosen based on the key characteristics of CNs, IoT and ICSs. Some of these characteristics include but not limited to scale, geographical distribution, constraints in power, the Internet usage, need for human interaction, and, finally, the possibility of facing physical impacts as a result of threats.

CNs are the first important area in which security threats may appear, and, thus, the reliability of information needs to be addressed accurately as organizations and enterprises usually own a local network of interconnected computers. However, the scale of computer networks is not limited to small business corporations, and, in most cases, it expands to a vast area. For this reason, computer networks are commonly highly distributed in terms of geographical position. In such a context, computers have direct interactions with users, and, commonly, are not constrained in resources (e.g. processing units and memory). Moreover, they have access to the Internet which may pose considerable amount of potential threats. Last but not least, most of the threats in computer networks may not impose direct physical impacts.

IoT is the second emerging area in which security and privacy is of great concern. It involves a huge amount of connected devices highly distributed in different geographical positions and ranging from smart objects to physical devices, buildings, and also vehicles to name a few. Suitable IoT frameworks should allow the interaction between all these devices and help in the development of distributed applications. These devices do have continuous interactions with users regularly and are commonly resource-constrained. Furthermore, they may not connect to the Internet constantly. Security threats in IoT context would impose both physical and non-physical impacts. Here, threats do appear with uncertainty as well. Also, they may have different levels. So, any of threat modeling techniques capable of dealing with uncertainty such as HMMs, GM, HM or FL are applicable. Nevertheless, HMMs and GM scalability issues should not be neglected.

ICSs are the third area in which security has turned to be a major global concern in recent years. Therefore, ensuring the security of information in such context is critically important. In particular, threats that may lead to loss of information or service in other environments may result in real and

Table 1. Suitability of threat modeling techniques based on assets and threats

Threat Modeling Technique	Assets	Threats
HMMs	• Limited to average number of assets • Assets with different security states	• Threats with uncertainty
GM	• Limited to average number of assets	• Threats with uncertainty
HM	• Large number of assets	• Threats with different levels
TC	• Large number of assets	• Limited known threats
FL	• Large number of assets	• Threats with uncertainty

physical impacts on connected network of industrial control systems. As an example, the Stuxnet worm was mainly developed to target Programmable Logic Controllers (PLCs) that lay at the heart of the centrifuges used by the Iranian government (Campbell, 2016). Another important issue is that ICSs may include devices or components which may or may not be resource-constrained with the ability to be connected to the Internet continuously. They have less human interaction comparing with computer networks and IoT devices. Finally, they are not highly distributed geographically in contrast with IoT devices and computer networks.

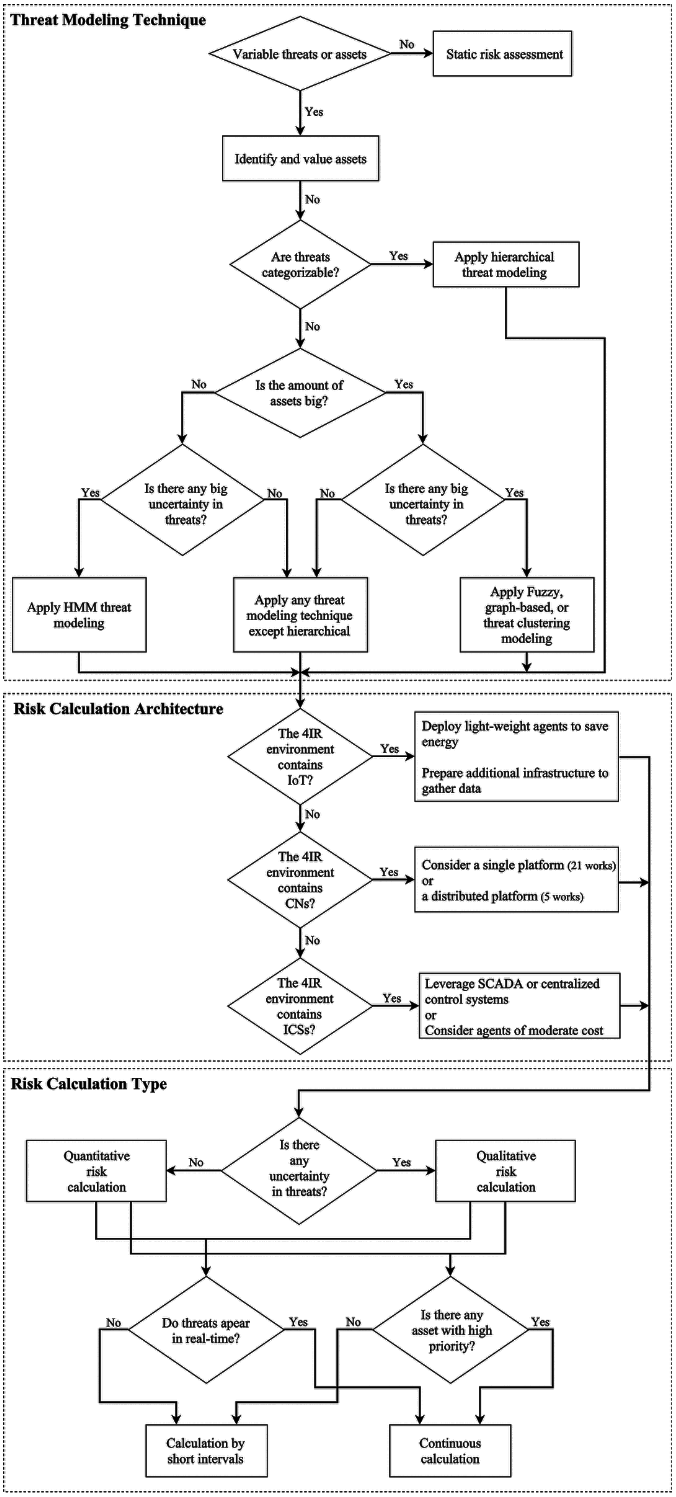
Risk assessment systems for computer networks tend to calculate the associated risk of each computer separately and in a centralized manner as it will show the degree of exposure of each of these devices to security threats. Nevertheless, a decentralized risk assessment system would also work for such an application context. Centralized models (proposed in 21 works) assess the risk using a single platform, i.e. they collect the information of different security threats (i.e. their likelihood and impact) in one place in order to evaluate the overall risk of a computer network. On the other side, decentralized models (proposed in 5 works) consider a distributed or a multi-agent framework for this purpose. A decentralized architecture can decrease the computational burden by breaking the task of risk assessment between distributed agents. Furthermore, it provides mechanisms for agents' communications, and, as a result, can lead to better dynamic risk estimation. However, the agents need to be implemented very simple; otherwise, a decentralized model would have a low performance in large complicated networks.

In an IoT context, risk assessment systems need to be designed based on a distributed (decentralized) architecture in order to address the reliability of information in an efficient way. One important aspect is that decentralization involves having several data sources. This issue is beneficial for learning mechanisms such as HMMs, which are well-prepared to combine and mix information elements with different degrees of certainty. However, decentralization needs an additional infrastructure to gather data from different sources (Figure 9). Thus, given a system with a set of agents (in (Haslum et al., 2007), each one being a sensor), each one is equipped with an HMM. In an IoT context, these agents can be assigned to different devices (assets) which are involved. Agents are usually lightweight in order to avoid battery drain in IoT devices (Figure 9). Based on the received information, the goal is to model and predict the next step of attackers considering all the threats and the calculated risks. 4 works (Holgado et al., 2015), (Haslum et al., 2007), (Haslum & Årnes, 2006), (Haslum, Abraham, et al., 2008) present a decentralized architecture for risk assessment based on HMM threat modeling technique (Table 3).

Another decentralized system which can be applied to IoT context is the Epidemiological-based threat modeling technique (Alhomidi & Reed, 2013). Here, a number of cells are employed and assigned to assets, with the capability of communicating with each other through sending and receiving signals. Doing so, the overall risk can be calculated by integrating all the estimations from different cells. More importantly, these signals impose a low computational burden as they do not carry huge amount of information. Thus, this approach has the potential to be applied to large IoT environments for the evaluation of risks due to the constraints in resources.

A dynamic risk assessment system for ICSs may either hold a centralized architecture when it is designed for one particular component (or a number of components), or a decentralized architecture when it is intended to break down the risk assessment process into several agents assigned to the components of an industrial control system. From centralized architectures, (Boyer et al., 2005), (Ahmed et al., 2011), (Rezvani et al., 2014), (Qi et al., 2010), (C. Fu et al., 2010), and, also, all the systems investigated in (Cherdantseva et al., 2016) can be applied to ICS application context. From decentralized architectures,

Figure 9. An overall decision guide for threat modeling, and risk calculation architecture and risk calculation type


Threat Modeling Technique
Variable threats or assets
No
Static risk assessment
Yes
Identify and value assets
No
Are threats categorizable?
Yes
Apply hierarchical threat modeling
No
Is the amount of assets big?
No
Yes
Is there any big uncertainty in threats?
Yes
No
Is there any big uncertainty in threats?
No
Yes
Apply HMM threat modeling
Apply any threat modeling technique except hierarchical
Apply Fuzzy, graph-based, or threat clustering modeling
Risk Calculation Architecture
The 4IR environment contains IoT?
Yes
Deploy light-weight agents to save energy
Prepare additional infrastructure to gather data
No
The 4IR environment contains CNs?
Yes
Consider a single platform (21 works) or a distributed platform (5 works)
No
The 4IR environment contains ICSs?
Yes
Leverage SCADA or centralized control systems or Consider agents of moderate cost
Risk Calculation Type
Quantitative risk calculation
No
Is there any uncertainty in threats?
Yes
Qualitative risk calculation
No
Do threats apear in real-time?
Yes
No
Is there any asset with high priority?
Yes
Calculation by short intervals
Continuous calculation

DRA systems proposed for IoT can be adopted for ICSs as well; however, those proposed for ICSs cannot be applied to IoT necessarily as they are constrained in terms of resources.

Finally, risk calculation type (i.e. quantitative/qualitative and continuous/by short intervals) is the third critical issue in DRA which is commonly chosen based on the identified assets and expected appearing threats. Qualitative risk calculation is usually applied when there is an uncertainty in the upcoming threats. As neither the probability of threats nor their impact is known, human linguistic terms are used to help modeling the uncertain threats and measure risk values. Moreover, continuous risk calculation is used when either assets have a high priority (i.e. a minor impact on any of them would impose a huge amount of risk to the overall system) or threats are expected to appear in real-time. In cases where threats do not appear in real-time, risk values are calculated by short intervals though there is always a concern of missing some threats which may appear in these intervals.

CONCLUSION

Security and reliability of information need to be addressed taking into account the current threats in IT environments. This task becomes a challenge taking into account that networks, systems and attacks evolve rapidly over time. In order to achieve the desired security level, it is critical to assess the risk level in a suitable way. For this purpose, different Dynamic Risk Assessment (DRA) approaches have been proposed in the past.

In this work, we have studied 27 different DRA systems and have analyzed them based on three important building blocks of risk assessment systems, including assets management, threat modeling technique, and risk calculation method. Moreover, we have summarized key characteristics of three main application areas which are of great concern nowadays and have suggested decision guides to the security experts in order to choose the best threat modeling and risk calculation techniques for their contexts which are Computer Networks (CNs), Internet of Things (IoT) and Industrial Control Systems (ICSs).

CNs and IoT do contain lots of assets both from hardware and software, and, thus, are considerably larger in terms of scale in comparison with ICSs. Moreover, threats are quite more uncertain and variable in the two former contexts than the latter. Therefore, due to the uncertain nature of threats appearing in computer networks, HMMs and GM can be used to model security threats. In particular, HMMs are suitable when assets of interest have different security states. However, these modeling techniques do not scale well when the number of assets is significantly high. On the other hand, due to the limited number of assets which exists in ICSs and the assorted type of threats appearing, any of the modeling techniques are applicable here. Specific characteristics of ICS should also be considered. For instance, due to the limited human interaction which may exist in ICS, threats which are coming from these interactions should not be neglected in modeling.

There are commonly two risk calculation architectures which are applied based on the characteristics of the application context. In CNs, both architectures can be used potentially. However, the majority of works studied (21 works) have adopted a centralized architecture in contrast with a few ones which have adopted a decentralized architecture (5 works). A decentralized architecture can decrease the computational burden by breaking the task of risk assessment between distributed agents. Furthermore, it provides mechanisms for agents' communications, and, as a result, can lead to better dynamic risk estimation. However, some extra considerations are taken into account based on the application area. For instance, in an IoT context, lightweight agents are assigned to different IoT devices to save energy and avoid battery drain, and, in an ICS context, agents are expected to be of moderate cost. Furthermore, there is always a need to an additional infrastructure to gather data in a distributed architecture.

Rather than considering an architecture for risk calculation process, two main decisions have to be made regarding the type of risk calculation. First, it must be clarified whether risks should be evaluated using quantitative or qualitative metrics. Commonly, qualitative methods are used when there is an uncertainty in the upcoming threats. In considered works, quantitative metrics are adopted in the majority of contributions (24 works). The second issue is to decide whether DRA approaches need to re-estimate and update risk values continuously or by intervals, due to the changes that may occur at different periods of time. Approaches which capture risk values continuously (11 works) can provide with a real-time evaluation of risks. Nevertheless, it comes at a cost of using a flexible threat modeling technique capable of timely adapting to these changes. On the other side, models which capture risk values at short intervals (suggested in 7 works) are less complex as they are based on simpler threat modeling techniques. However, they are prone to miss new security threats which might happen between these intervals.

ACKNOWLEDGMENT

This work has been partially supported by MINECO grants TIN2016-79095-C2-2-R (SMOG-DEV), TIN2013-46469-R (SPINY: Security and Privacy in the Internet of You) and CAM grant S2013/ICE-3095 (CIBERDINE), co-funded with European FEDER funds.

REFERENCES

Ahmed, M. S., Al-Shaer, E., Taibah, M., & Khan, L. (2011). Objective risk evaluation for automated security management. *Journal of Network and Systems Management*, *19*(3), 343–366. doi:10.100710922-010-9177-6

Alhomidi, M., & Reed, M. (2013). Risk assessment and analysis through population-based attack graph modelling. In *Internet Security (WorldCIS), 2013 World Congress on* (pp. 19–24). Academic Press. 10.1109/WorldCIS.2013.6751011

Årnes, A., Sallhammar, K., Haslum, K., Brekne, T., Moe, M. E. G., & Knapskog, S. J. (2005). Real-time risk assessment with network sensors and intrusion detection systems. In *International Conference on Computational and Information Science* (pp. 388–397). Academic Press.

Årnes, A., Valeur, F., Vigna, G., & Kemmerer, R. (2006). Using Hidden Markov Models to Evaluate the Risks of Intrusions. *Recent Advances in Intrusion Detection*, 145–164. 10.1007/11856214_8

Awan, M. S. K., Burnap, P., & Rana, O. (2016). Identifying cyber risk hotspots: A framework for measuring temporal variance in computer network risk. *Computers & Security*, *57*, 31–46. doi:10.1016/j.cose.2015.11.003

Behnia, A., Rashid, R. A., & Chaudhry, J. A. (2012). A survey of information security risk analysis methods. *SmartCR*, *2*(1), 79–94.

Benini, M., & Sicari, S. (2008). Risk assessment in practice: A real case study. *Computer Communications*, *31*(15), 3691–3699. doi:10.1016/j.comcom.2008.07.001

Blank, R. M., & Gallagher, P. D. (2012). *Guide for Conducting Risk Assessments.* NIST Special Publication.

Boyer, S., Dain, O., & Cunningham, R. (2005). Stellar: A fusion system for scenario construction and security risk assessment. In *Information Assurance, 2005. Proceedings. Third IEEE International Workshop on* (pp. 105–116). IEEE. 10.1109/IWIA.2005.16

Calder, A., & Watkins, S. G. (2010). *Information Security Risk Management for ISO27001/ISO27002*. Retrieved from https://books.google.com/books?hl=es&lr=&id=8Ffa1dOFgO4C&pgis=1

Campbell, T. (2016). Information Security Implementation. In *Practical Information Security Management* (pp. 63–70). Springer. doi:10.1007/978-1-4842-1685-9_5

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). *Introducing octave allegro: Improving the information security risk assessment process*. Academic Press.

Chen, G. (2010). Research on network security real-time risk assessment model. In *Electronics and Information Engineering (ICEIE), 2010 International Conference On* (*Vol. 2*, pp. V2--548). ICEIE. 10.1109/ICEIE.2010.5559746

Chen, Y., Jensen, C. D., Gray, E., Cahill, V., & Seigneur, J.-M. (2003). *A general risk assessment of security in pervasive computing*. Retrieved from Https://www. Cs. Tcd. Ie/publications/techreports/reports, 3

Cheng, W., Xu, X., Jia, Y., & Zou, P. (2008). Network Dynamic Risk Assessment Based on the Threat Stream Analysis. In *The Ninth International Conference on Web-Age Information Management* (pp. 532–538). IEEE. 10.1109/WAIM.2008.65

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, *56*, 1–27. doi:10.1016/j.cose.2015.09.009

Chołda, P., & Jaglarz, P. (2016). Optimization/simulation-based risk mitigation in resilient green communication networks. *Journal of Network and Computer Applications*, *59*, 134–157. doi:10.1016/j.jnca.2015.07.009

Clinch, J. (2009, May). ITIL v3 and information security. *Clinch Consulting White Paper*, 1–40.

Crespo, F. L., Amutio-Gómez, M. A., Candau, J., & Mañas, J. A. (2006). Methodology for Information Systems Risk Analysis and Management (MAGERIT version 2). In Book II-Catalogue of Elements. Madrid: Ministerio de Administraciones Públicas.

Dantu, R., Kolan, P., & Cangussu, J. (2009). Network risk management using attacker profiling. *Security and Communication Networks*, *2*(1), 83–96. doi:10.1002ec.58

de Gusmão, A. P. H., Silva, L. C., Silva, M. M., Poleto, T., & Costa, A. P. C. S. (2016). Information security risk analysis model using fuzzy decision theory. *International Journal of Information Management*, *36*(1), 25–34. doi:10.1016/j.ijinfomgt.2015.09.003

De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. *Journal of Information Systems*, *27*(1), 307–324. doi:10.2308/isys-50422

Deka, R. K., Kalita, K. P., Bhattacharya, D. K., & Kalita, J. K. (2015). Network defense: Approaches, methods and techniques. *Journal of Network and Computer Applications*, *57*, 71–84. doi:10.1016/j.jnca.2015.07.011

Dongmei, Z., Changguang, W., & Jianfeng, M. (2007). A risk assessment method of the wireless network security. *Journal of Electronics (China)*, *24*(3), 428–432. doi:10.100711767-006-0247-6

Elliott, R. J., Aggoun, L., & Moore, J. B. (2008). *Hidden Markov models: estimation and control* (Vol. 29). Springer Science & Business Media.

Frigault, M., & Wang, L. (2008). *Measuring network security using bayesian network-based attack graphs*. IEEE. doi:10.1109/COMPSAC.2008.88

Fu, C., Ye, J., Zhang, L., Zhang, Y., & LanSheng, H. (2010). A Dynamic Risk Assessment Framework Using Principle Component Analysis with Projection Pursuit in Ad Hoc Networks. *Ubiquitous Intelligence & Computing and 7th International Conference on Autonomic & Trusted Computing (UIC/ATC), 2010 7th International Conference on*, 154–159. 10.1109/UIC-ATC.2010.42

Fu, S., & Zhou, H. (2011). The information security risk assessment based on AHP and fuzzy comprehensive evaluation. In *2011 IEEE 3rd International Conference on Communication Software and Networks* (pp. 124–128). IEEE. 10.1109/ICCSN.2011.6014018

Gao, F., Sun, J., & We, Z. (2003). The prediction role of hidden Markov model in intrusion detection. *CCECE 2003 - Canadian Conference on Electrical and Computer Engineering. Toward a Caring and Humane Technology (Cat. No.03CH37436), 2*, 893–896. 10.1109/CCECE.2003.1226038

Garvey, P. R. (2008). *Analytical methods for risk management: A systems engineering perspective*. CRC Press. doi:10.1201/9781420011395

Gehling, B., & Stankard, D. (2005). eCommerce security. In *Proceedings of the 2nd annual conference on Information security curriculum development - InfoSecCD '05* (p. 32). New York: ACM Press. 10.1145/1107622.1107631

Haslum, K., Abraham, A., & Knapskog, S. (2007). DIPS: A Framework for Distributed Intrusion Prediction and Prevention Using Hidden Markov Models and Online Fuzzy Risk Assessment. In *Third International Symposium on Information Assurance and Security* (pp. 183–190). IEEE. 10.1109/IAS.2007.67

Haslum, K., Abraham, A., & Knapskog, S. (2008). Fuzzy online risk assessment for distributed intrusion prediction and prevention systems. *Proceedings - UKSim 10th International Conference on Computer Modelling and Simulation, EUROSIM/UKSim2008*, 216–223. 10.1109/UKSIM.2008.30

Haslum, K., & Årnes, A. (2006). Multisensor real-time risk assessment using continuous-time hidden markov models. In *International Conference on Computational and Information Science* (pp. 694–703). Academic Press. 10.1109/ICCIAS.2006.295318

Haslum, K., Moe, M. E. G., & Knapskog, S. J. (2008). Real-time intrusion prevention and security analysis of networks using HMMs. *2008 33rd IEEE Conference on Local Computer Networks (LCN)*, 927–934. 10.1109/LCN.2008.4664305

Holgado, P., Perez, M. G., Perez, G. M., & Villagra, V. A. (n.d.). Evolving from a static toward a proactive and dynamic risk-based defense strategy. Jornadas Nacionales de Investigacion en Ciberseguridad (JNIC 2015).

Hu, Z.-H., Ding, Y.-S., & Huang, J.-W. (2008). Knowledge-based framework for real-time risk assessment of information security inspired by danger model. In *Intelligent Information Technology Application Workshops, 2008. IITAW'08. International Symposium on* (pp. 1053–1056). Academic Press.

Ionita, D., Hartel, P. H., Pieters, W., & Wieringa, R. J. (2013). *Current established risk assessment methodologies and tools.* Technical Report TR-CTIT-14-04, Centre for Telematics and Information Technology, University of Twente, Enschede. Retrieved from http://eprints.eemcs.utwente.nl/24541/01/%5Btech_report%5D_D_Ionita_-_Current_Established_Risk_Assessment_Methodologies_and_Tools.pdf

Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis*, *1*(1), 11–27. doi:10.1111/j.1539-6924.1981.tb01350.x PMID:11798118

Kurosu, M. (2013). Human-Computer Interaction: Towards Intelligent and Implicit Interaction. In *15th International Conference, HCI International 2013 Proceedings* (Vol. 8008). Springer.

Lee, E. A. (2008). Cyber Physical Systems: Design Challenges. *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, 363–369. 10.1109/ISORC.2008.25

Li, J. H., & Levy, R. (2010). Using Bayesian networks for cyber security analysis. *2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)*, 211–220. 10.1109/DSN.2010.5544924

Li, W., & Guo, Z. (2009). Hidden Markov Model Based Real Time Network Security Quantification Method. *2009 International Conference on Networks Security, Wireless Communications and Trusted Computing*, 94–100. 10.1109/NSWCTC.2009.375

Liao, N., Li, F., & Song, Y. (2010). Research on real-time network security risk assessment and forecast. In *Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on* (Vol. 3, pp. 84–87). Academic Press. 10.1109/ICICTA.2010.273

Liu, F., Chen, Y., Dai, K., Wang, Z., & Cai, Z. (2005). *Research on Risk Probability Estimating Using Fuzzy Clustering for Dynamic Security*. Academic Press.

López, D., Pastor, O., & Villalba, L. J. G. (2013). Dynamic risk assessment in information systems: State-of-the-art. *Proceedings of the 6th International Conference on Information Technology*, 8–10. Retrieved from http://sce.zuj.edu.jo/icit13/images/Camera Ready/Sorftware Engineering/772.pdf

Ma, J., Li, Z., & Zhang, H. (2009). A fusion model for network threat identification and risk assessment. In Artificial Intelligence and Computational Intelligence, 2009. AICI'09. International Conference on (Vol. 1, pp. 314–318). Academic Press. doi:10.1109/AICI.2009.487

Mendel, J. M. (1995). Fuzzy logic systems for engineering: A tutorial. *Proceedings of the IEEE*, *83*(3), 345–377. doi:10.1109/5.364485

Michalopoulos, D., Mavridis, I., & Jankovic, M. (2014). GARS: Real-time system for identification, assessment and control of cyber grooming attacks. *Computers & Security*, *42*, 177–190. doi:10.1016/j.cose.2013.12.004

Nadeem, A., & Howarth, M. P. (2013). A survey of manet intrusion detection & prevention approaches for network layer attacks. *IEEE Communications Surveys and Tutorials*, *15*(4), 2027–2045. doi:10.1109/SURV.2013.030713.00201

Phillips, C., & Swiler, L. P. (1998). A graph-based system for network-vulnerability analysis. In *Proceedings of the 1998 workshop on New security paradigms* (pp. 71–79). Academic Press. 10.1145/310889.310919

Poolsappasit, N., Dewri, R., & Ray, I. (2012). Dynamic security risk management using bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*, *9*(1), 61–74. doi:10.1109/TDSC.2011.34

Poovendran, R. (2010). Cyber-physical systems: Close encounters between two parallel worlds. *Proceedings of the IEEE*, *98*(8), 1363–1366. doi:10.1109/JPROC.2010.2050377

Qi, W., Liu, X., Zhang, J., & Yuan, W. (2010). *Dynamic Assessment and VaR-Based Quantification of Information Security Risk. In 2010 2nd International Conference on E-business and Information System Security* (pp. 1–4). IEEE; doi:10.1109/EBISS.2010.5473537.

Rezvani, M., Ignjatovic, A., Bertino, E., & Jha, S. (2014). Provenance-aware security risk analysis for hosts and network flows. In Network Operations and Management Symposium (NOMS), 2014 IEEE (pp. 1–8). IEEE. doi:10.1109/NOMS.2014.6838250

Rutkowski, L., & Cpalka, K. (2003). Flexible neuro-fuzzy systems. *IEEE Transactions on Neural Networks*, *14*(3), 554–574. doi:10.1109/TNN.2003.811698 PubMed

Sadeghi, A.-R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial internet of things. In *Proceedings of the 52nd Annual Design Automation Conference on - DAC '15* (pp. 1–6). New York: ACM Press. 10.1145/2744769.2747942

Shameli-Sendi, A., Ezzati-jivan, N., Jabbarifar, M., & Dagenais, M. (2012). Intrusion Response Systems : Survey and Taxonomy. *International Journal of Computer Science and Network Security*, *12*(1), 1–14. Retrieved from http://paper.ijcsns.org/07_book/201201/20120101.pdf

Shedden, P., Scheepers, R., Smith, W., & Ahmad, A. (2011). Incorporating a knowledge perspective into security risk assessments. *Vine*, *41*(2), 152–166. doi:10.1108/03055721111134790

Shoemaker, D., & Conklin, W. A. (2011). *Cybersecurity: The Essential Body Of Knowledge*. Cengage Learning. Retrieved from https://books.google.com/books?id=TUUKAAAAQBAJ&pgis=1

Tabak, D., & Levis, A. H. (1985). Petri net representation of decision models. *IEEE Transactions on Systems, Man, and Cybernetics*. *SMC*, *15*(6), 812–818. doi:10.1109/TSMC.1985.6313468

Volftrub, A. B., & Polikarpov, A. K. (2007). Methods of multifactor damage risk management in automated information systems. *Automatic Documentation and Mathematical Linguistics*, *41*(1), 46–52. doi:10.3103/S0005105507010074

Von Solms, S. H. (2005). Information Security Governance - Compliance management vs operational management. *Computers & Security*, *24*(6), 443–447. doi:10.1016/j.cose.2005.07.003

Wilkin, C. L., & Chenhall, R. H. (2010). A Review of IT Governance: A Taxonomy to Inform Accounting Information Systems. *Journal of Information Systems*, *24*(2), 107–146. doi:10.2308/jis.2010.24.2.107

Wrona, K., & Hallingstad, G. (2010). Real-time automated risk assessment in protected core networking. *Telecommunication Systems*, *45*(January), 205–214. doi:10.100711235-009-9242-1

Wu, T., & Zhao, G. (2014). A novel risk assessment model for privacy security in Internet of Things. *Wuhan University Journal of Natural Sciences*, *19*(5), 398–404. doi:10.100711859-014-1031-3

Yazar, Z. (2002). *A qualitative risk analysis and management tool--CRAMM*. SANS InfoSec Reading Room White Paper.

Yu-Ting, D., Hai-Peng, Q., & Xi-Long, T. (2014). Real-time risk assessment based on hidden Markov model and security configuration. In *2014 International Conference on Information Science, Electronics and Electrical Engineering* (Vol. 3, pp. 1600–1603). IEEE. 10.1109/InfoSEEE.2014.6946191

Zhang, Y., Jiang, S., Cui, Y., Zhang, B., & Xia, H. (2010). A qualitative and quantitative risk assessment method in software security. In *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)* (Vol. 1, pp. V1-534-V1-539). IEEE. 10.1109/ICACTE.2010.5578960

Zhiwei, Y., & Zhongyuan, J. (2012). A survey on the evolution of risk evaluation for information systems security. *Energy Procedia*, *17*, 1288–1294. doi:10.1016/j.egypro.2012.02.240

Zhou, L., & Chen, S. (2012). A survey of research on smart grid security. In *Network Computing and Information Security* (pp. 395–405). Springer. doi:10.1007/978-3-642-35211-9_52

KEY TERMS AND DEFINITIONS

Assets Management: It deals with three main issues, including types of the assets which need to be considered, their behavior, and, also their valuation.

Risk: An estimation of the degree of exposure to a threat that may occur on one or more assets causing damage to an organization.

Risk Assessment: An assessment which is made based on the impact that each risk event could have on the assets of system.

Risk Identification: Early identification of risks that can impact on the system's assets in particular, and on system's performance in general.

Risk Management: A general process to handle risks as it serves to identify, assess, prioritize, mitigate, and track them.

Risk Mitigation: Plans which are designed to manage, eliminate, or reduce risks to an acceptable level.

Risk Prioritization: A major purpose for prioritizing risks is to form a basis for allocating critical resources, including additional personnel or funding to resolve those risks.

Risk Tracking: The main goal of risk tracking is the exact monitoring of risk assessment and mitigation strategies based on the priorities of risks.

Threat Modeling: It models security threats which may impose risks to assets of interest.

APPENDIX

Table 2. Dynamic Risk Assessment Models in IT environments

DRA Approach	Assets		Threats		Threat Modeling Technique						Risk Calculation				Setting		
	Type	Valuation	Type	Evolution	HMMs	GM	HM	TC	FL	Others	Quantitative	Qualitative	Continuously	In Short Intervals	CN	IoT	ICS
(Holgado et al., 2015)	NA	NA	NA	Dynamic	×						×			×		×	
(Haslum et al., 2007)	Data, Devices	Cost, Criticality, Sensitivity, Recovery	NA	NA	×						×		×			×	
(Haslum & Årnes, 2006)	Computer Network	Confidentiality, Integrity, Availability	NA	NA	×							×		×		×	
(Årnes et al., 2005)	Computer Network	Confidentiality, Integrity, Availability	NA	NA	×						×		×		×		
(W. Li & Guo, 2009)	NA	NA	Multi-step DDoS	Dynamic	×						×		×		×		
(G. Chen, 2010)	NA	NA	NA	NA	×						×			×	×		
(Årnes et al., 2006)	NA	Confidentiality, Integrity, Availability	DDoS	NA	×						×		×		×		
(Ma et al., 2009)	NA	Confidentiality, Integrity, Availability	Multi-step DDoS	Dynamic	×						×			×	×		
(Yu-Ting et al., 2014)	NA	Confidentiality, Integrity, Availability	Attacks that destruct confidentiality, integrity and availability	NA	×						×			×	×		
(Haslum, Abraham, et al., 2008)	NA	Cost, Criticality, Sensitivity, Recovery	DoS, User to Root, Remote to Local, Probing	Dynamic	×							×		×		×	
(Phillips & Swiler, 1998)	NA	NA	Simulated attacks	Dynamic		×					×				×		
(Alhomidi & Reed, 2013)	NA	NA	NA	NA		×					×					×	
(Poolsappasit et al., 2012)	NA	Confidentiality, Integrity, Availability	NA	Dynamic		×					×				×		
(Wu & Zhao, 2014)	NA	Confidentiality, Integrity, Availability	Various kinds of attacks including DoS	Dynamic		×					×				×		
(Wrona & Hallingstad, 2010)	NA	Main focus on Availability	DoS	Dynamic		×					×		×		×		
(Dantu et al., 2009)	NA	NA	NA	NA		×					×				×		
(Liao et al., 2010)	NA	Confidentiality, Integrity, Availability	A simulated intruder	NA		×					×		×		×		
(Hu et al., 2008)	NA	NA	NA	Dynamic		×					×		×		×		
(Volftrub & Polikarpov, 2007)	NA	NA	NA	Dynamic			×				×				×		
(Liu et al., 2005)	NA	NA	NA	NA				×			×				×		
(Y. Chen et al., 2003)	NA	NA	NA	NA				×			×		×		×		
(Michalopoulos et al., 2014)	NA	NA	Grooming attacks	NA					×			×	×		×		

continued on following page

Table 2. Continued

DRA Approach	Assets		Threats		Threat Modeling Technique						Risk Calculation				Setting		
	Type	Valuation	Type	Evolution	HMMs	GM	HM	TC	FL	Others	Quantitative	Qualitative	Continuously	In Short Intervals	CN	IoT	ICS
(Boyer et al., 2005)	NA	NA	NA	NA						×	×		×				×
(Qi et al., 2010)	Software, Hardware, Data, Fame, Reputation, Public trust, Employees' confidence	Assets are recognized and assigned a value manually	NA	Dynamic						×	×						×
(Ahmed et al., 2011)	NA	NA	DDoS	Dynamic						×	×		×				×
(Rezvani et al., 2014)	NA	NA	DDoS	NA						×	×			×			×
(C. Fu et al., 2010)	NA	NA	NA	NA						×	×						×

HMMs: Hidden Markov Models
GM: Graph-based Modeling
HM: Hierarchical Modeling
TC: Threats Clustering
FL: Fuzzy Logic
CN: Computer Networks
IoT: Internet of Things
ICS: Industrial Control Systems