1 Information Assurance

CHAPTER

Yi Qian University of Puerto Rico at Mayaguez, Puerto Rico
James Joshi University of Pittsburgh, USA
David Tipper University of Pittsburgh, USA
Prashant Krishnamurthy University of Pittsburgh, USA

1.1 INTRODUCTION

Recent advances in computer networks and information technology (IT) and the advent and growth of the Internet have created unprecedented levels of opportunities for the connectivity and interaction of information systems at a global level. This has provided significant new possibilities for advancing knowledge and societal interactions across the spectrum of human endeavors, including fundamental scientific research, education, engineering design and manufacturing, environmental systems, health care, business, entertainment, and government operations. As a result, our society has already become intrinsically dependent on IT. In fact, networked information systems have been recognized as one of the basic critical infrastructures of society [1]. A consequence of the increasing dependence on networked information systems has been the significantly heightened concerns regarding their *security* and *dependability*. In particular, the interconnections, interactions, and dependencies among networked information systems and other critical infrastructure systems (e.g., electric power grids) can dramatically magnify the consequence of damages resulting from even simple security violations and/or faults. Hence, there is an urgent need to ensure that we have in place a solid foundation to help us justify the trust that we place on these information technologies and infrastructures.

Research and development activities focused on ensuring that a networked information system (a) functions correctly in various operational environments,

and (b) provides the protection of critical information and resources associated with them, have been pursued within both the security and dependability communities. Although the security and dependability communities appear to focus on significantly overlapping concerns (e.g., *availability*), the efforts to converge their approaches and accumulated knowledge to generate innovative solutions have not been forthcoming or has been very slow at best. At the same time, the threats to the emerging networks and infrastructures, as well as the sophistication level of automated attack tools and malicious agents to easily inflict serious damages, are growing rapidly. It is a common belief now that ensuring *absolute security* is an unachievable practical goal. Hence, a growing concern is that of ensuring that networks and systems provide an assured level of functionalities even in the presence of disruptive events that attempt to violate their security and dependability goals. The capability of a system has been described by various terms, such as, *survivability*, *resilience*, *disruption tolerance*, and so on. A plethora of solutions has also been generated within these communities to address their respective, albeit overlapping, concerns related to increasing the trustworthiness of the overall system. We believe that efforts should be directed toward exploiting the synergies that exist among various piecemeal solutions from both security and dependability areas to seek out integrated, holistic solutions that allow us to provide assurances about the trustworthiness of the networks and systems that we use. It is worth noting that similar sentiments have recently been expressed in the research community [2–5].

We have conceived of this book as an effort toward the key goal of exploring the issues related to the *integration of* and *interaction between* approaches, models, architectures, and so on, prevalent in the security and dependability areas. In particular, we view *information assurance* (IA) as a growing area that can form an umbrella to bring together the efforts in security and dependability areas, mainly because their primary goal is to provide an adequate level of assurance that the networked information systems and infrastructures can be relied upon and trusted. Furthermore, the interaction between dependability and security is only beginning to be addressed in the research literature but is a crucial topic for successfully building IA into IT systems.

To the best of our knowledge, there is currently no comprehensive book that focuses on such an integrated view of IA. This book is an initial attempt to fill this gap. The goal of this book is to present a sample of the state-of-the-art survey of *dependability* and *security* techniques followed by an in-depth look at how these two components interact in providing IA and what the challenges are for the assurance of emerging systems. Our hope here is that by bringing both areas together, we will make a start toward integrating the approaches.

1.2 INFORMATION ASSURANCE: DEPENDABILITY AND SECURITY OF NETWORKED INFORMATION SYSTEMS

As mentioned earlier, we view IA as encompassing both dependability and security areas. In this section, we briefly introduce key terminologies from these areas and present our view on the need for such an integrated view.

Information or computer security primarily focuses on the issues related to *confidentiality*, *integrity*, and *availability* (CIA) of information [7]. *Confidentiality* refers to ensuring that highly sensitive information remains unknown to certain users. *Integrity* refers to the authenticity of information or its source. *Availability* refers to ensuring that information or computer resources are available to authorized users in a timely manner. Other key security issues often added include *accountability*, *non-repudiation*, and *security assurance* [7]. *Accountability* ensures that an entity's action is traceable uniquely to that entity; *non-repudiation* refers to ensuring that an entity cannot deny its actions; and *security assurance* refers to the confidence that the security requirements are met by an information system. Policy models, mechanisms, and architectural solutions have been extensively investigated by the security community to address issues related to specification and enforcement of the security requirements of networked information systems. In addition to proactive, preventive techniques, reactive techniques that involve detection followed by response and recovery continue to be developed to address the overall protection issues. Cryptographic techniques are widely used as mechanisms to achieve the above mentioned security goals.

The *dependability* area, on the other hand, has primarily focused on how to quantitatively express the ability of a system to provide its specified services in the presence of failures, through the measures of *reliability*, *availability*, *safety*, and *performability* [6]. *Reliability* refers to the probability that a system provides its service throughout the specified period of time. *Availability*, a key goal of security also, more specifically refers to the fraction of time that a system can be used for its intended purpose within a specified period of time. *Safety* refers to the probability that a system does not fail in such a way as to cause a major damage. *Performability* quantitatively measures the performance level of a system in the presence of failures. An important observation that can be made here is that of the richness of the quantitative techniques within the dependability area in contrast to the scarcity of such techniques in the security area. One reason for this is the difficulty in applying quantitative techniques for *confidentiality* and *integrity* issues, as well as the cryptographic techniques. Confidentiality and integrity issues were the primary security concerns for the security community for a considerable period of time and several "formal" approaches focused on these were developed to

address the issues of verification and qualitative validation of security properties. Interestingly, both *confidentiality* and *integrity* issues are also sometimes considered as relevant dependability goals [8].

A related notion that attempts to capture both the security and dependability concerns is that of *survivability*. *Survivability* has been defined in various ways by different researchers and no consensus yet exists on its standard definition. One way to define survivability is as the capability of a system to fulfill its mission, in a timely manner, in presence of attacks, failures, or accidents [6]. A key goal here is to provide a quantitative basis for indicating that a system meets its security and dependability goals. A key motivation towards this direction is provided by the fact that absolute security is an unachievable goal, as indicated by the undecidability of the *safety problem* related to security shown by Harrison, Ruzzo, and Ullman in their seminal paper [9]. It is also virtually impossible to completely identify all the vulnerabilities in a networked information environment that is characterized by ever increasing heterogeneity of its components. In the face of such an insurmountable challenge, a key alternative is to set *provisioning of an acceptable level of services in presence of disruptive events* as a practical goal; in other words, a more realistic goal is that of ensuring a desired level of assurance that the required security and dependability goals are met by a system throughout its life cycle.

While there is an urgent need for solutions that integrate dependability and security, the two communities have largely remained separated, although efforts can be seen towards desirable interactions between them. A simple and often cited difference between the two areas is that dependability focuses primarily on faults and errors in the systems that are typically non-malicious in nature (primarily from the fault tolerance design area), while security focuses mainly on protection against malicious attempts to violate the security goals. However, such a difference is not accurate and can be seen in the various taxonomies developed within each community. For instance, the taxonomies for security vulnerabilities developed by Landwehr et al. [10] and later by Avizienis et al. [11] incorporate both *intentional* and *unintentional* sources of security vulnerabilities. The growing realization of the overlapping nature of the two areas can be seen among researchers in their efforts towards cross-pollinating the two areas in order to synthesize integrated frameworks.

This book first aims to highlight the overlapping aspect of the dependability and security areas (Figure 1.1), an understanding which we believe is fundamental to exploiting the synergies within the two communities. An integrated taxonomy that congregates the attributes of dependability and security is an important goal and some efforts towards this direction can be seen (e.g., Chapter 6). A natural outcome of the overlapping concerns of the two areas is that of using the well developed techniques in one area to address issues in the other or of

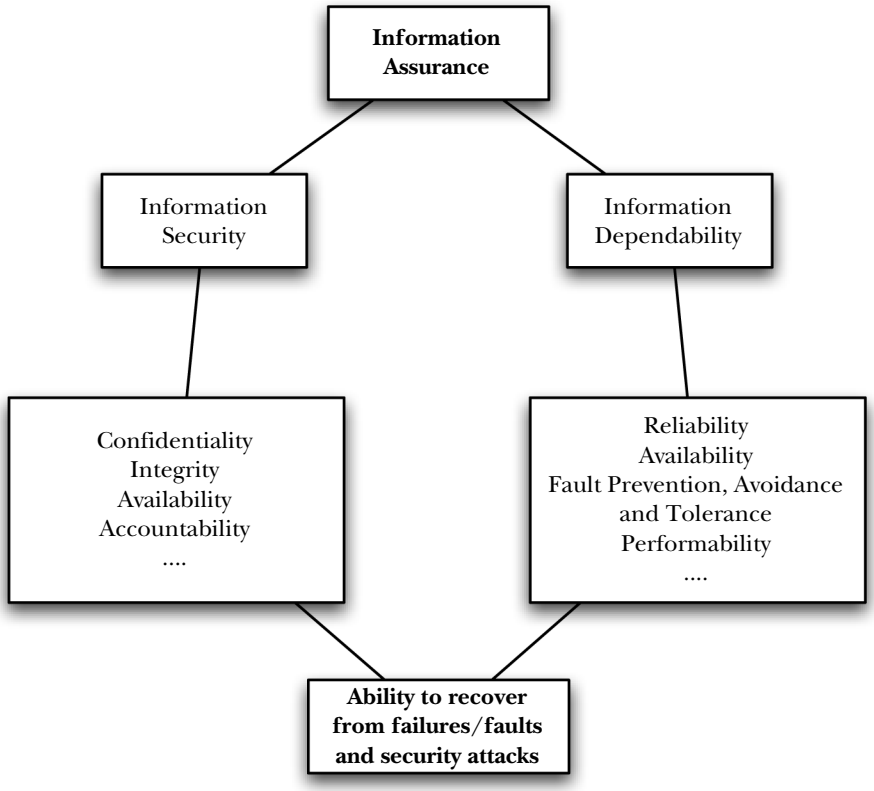

FIGURE 1.1 Information assurance: interaction between security and dependability.

synthesizing similar techniques from the two areas to create more effective, integrated solutions. One such area of cross-pollination can be seen in the use of fault-diagnosis techniques using fault trees in the fault tolerance community that parallels the use of attack trees/graphs to characterize security intrusions. Furthermore, correlating alerts and symptoms to more accurately identify the source of a problem and/or its consequences are important diagnostic activities related to both dependability and security. This commonality provides prospects for integrated diagnostic frameworks that can capture disruption scenarios related to malicious activities or non-malicious events. Such integrated fault and attack diagnosis and alert correlation approaches have already emerged as active research foci. An important observation related to security is the non-predictability of security threats and attacks; it makes modeling attackers significantly challenging. Furthermore, as mentioned earlier, the security area currently lacks viable quantitative

techniques. These deficiencies add newer research challenges to generating integrated, holistic solutions to modeling, analysis, and evaluation of security and dependability of a networked information system to establish assurance of its quality (e.g., lack of vulnerability, or appropriate measures against possible threats) and eventually its trustworthiness. Sophisticated stochastic techniques, such as Markov models, which have been widely used for dependability analysis, are currently being adopted and extended to additionally address security issues as discussed in Chapter 7. Such quantitative techniques, as well as newer game-theory based approaches (e.g., Chapter 8), are also currently being pursued to address the challenges related to the coincident effect of all types of disruptive events. Furthermore, it is important to note that the security and dependability concerns related to different system or architectural layers/components, such as operating systems, applications, networks, wireless infrastructures, and so on, bring forth their unique challenges. In addition to developing solutions for these different types of IT environments, there is also a crucial need to synthesize these solutions to ensure the survivability of huge infrastructures against large scale cyber attacks, which could become a catastrophe for a society that now relies so much on the technology.

In summary, we characterize IA to encompass dependability and security concerns and emphasize that combined IA approaches that address security and dependability together is the needed direction because:

- Many threats to dependability and security are common or similar. Combined modeling of failures and security threats will help provide more accurate understanding of the underlying problems.
- There is a need for both qualitative and quantitative base when establishing the overall assurance that a system maintains a desired level of trustworthiness. Quantitative and qualitative techniques that are abundant in dependability and security areas, respectively, complement each other and will help create more effective IA solutions.
- In reality, all types of disruptive events (faults and attacks) may coexist within a single networked information system. Hence, all types of disruptive events should be modeled together so that any coincident effect of different disruptive events and their emergent characteristics can be more accurately understood.
- Different techniques developed within each area may be useful in the other area. For instance, design diversity and redundancy, which were typically employed in fault-tolerance community, have been beneficial for security. At the same time, a combined approach will avoid duplication of effort.

1.3 BOOK ORGANIZATION

In this section, we briefly overview the organization of the book, which has been divided into three parts, each containing several chapters.

1.3.1 The Three Parts of the Book

One of our key goals for this edited book has been to emphasize the need to bring together the communities and rich research results from the areas of security and dependability to exploit the synergies that exist between them, so that the growing issue of survivable and resilient networked information systems can be addressed in a holistic manner. Toward this goal, our key efforts have been to focus on the interaction and integration of tools and techniques from the security and dependability areas. Figure 1.2 illustrates the generic organization of the book into three parts.

Part I focuses on the foundational concepts from both security and dependability areas and sets the stage for looking at the issues related to their integration and interaction. A key goal of these chapters is to provide the overview of the various concepts and terminologies needed to understand the later chapters so that the book is self-contained.

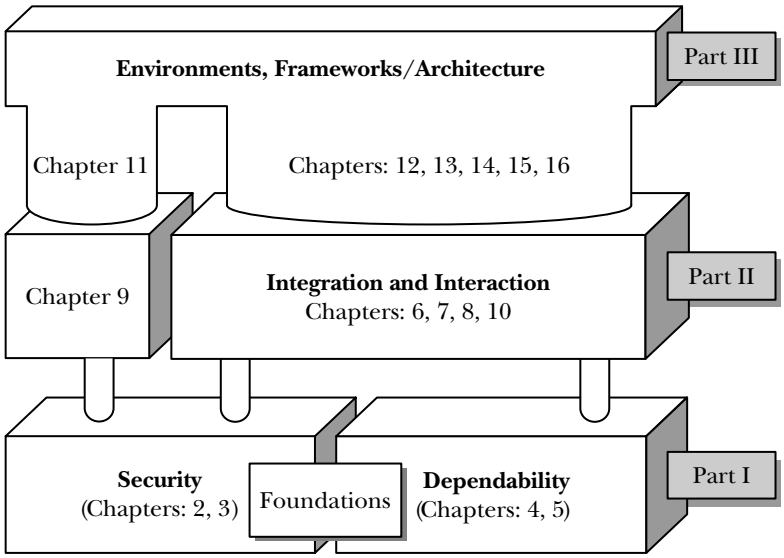

FIGURE 1.2 Organization of the book into three parts, each containing multiple chapters.

Part II focuses on the interaction and integration of mechanisms and approaches from the areas of security and dependability. Chapter 9, which stands separate from the other four chapters in this part, focuses more on security, although its approach is generically applicable to the integrated environment. Also, the content of Chapter 9, generating attack trees and capturing attack scenarios, is a crucial step in building a resilient system and can potentially be integrated with fault tree concepts from the dependability community.

In Part III, which further builds on interaction and integration of security and dependability approaches, we have grouped the chapters that address related issues in specific types of environments (e.g., operating systems in Chapter 12 and wireless systems in Chapter 15) or the design of frameworks/architecture (e.g., integrated fault and security management framework in Chapter 16). Chapter 13 focuses on intrusion response systems that we believe are crucial for building survivable systems. We have included Chapter 11 in Part III, although it primarily focuses on security vulnerabilities, because it addresses a specialized environment (i.e., optical network environments) and monitoring and detection issues that are key components for survivable systems.

An overview of each chapter is provided in the following sections.

1.3.2 Chapter 2: Network Security

This chapter introduces key concepts related to *network security*. In particular, the chapter focuses on issues related to the assessment of networks' current state of security, mechanisms to prevent and detect security violations, and policies, procedures, and techniques to respond to security intrusions. The chapter overviews various security services currently available and introduces cryptographic techniques and security protocols that are commonly used for securing a networked environment. The chapter also briefly overviews network security threats and attacks and how they can be addressed by using various security services and architectural configurations.

1.3.3 Chapter 3: Security for Distributed Systems: Foundations of Access Control

This chapter provides a comprehensive overview of key concepts underlying the foundations of access control and a discussion of key issues and trends in *access control for distributed systems*. The chapter introduces the notions of identification, authentication, and access control for distributed systems. It touches on various

access control models, such as the *role-based access control* (RBAC) and *Bell-LaPadula* models, and surveys the main techniques for their implementation. The chapter also presents newly emerging access control-related standards such as *Security Assertion Markup Language* (SAML) and *EXtensible Access Control Markup Language* (XACML). Newer security issues within the context of distributed systems, such as *trust negotiation*, *secure interoperation*, *location-based security*, and *federated digital identity management* are also discussed.

1.3.4 Chapter 4: Network Survivability

This chapter explores *network survivability* and dependability mechanisms used to construct fault-tolerant communication networks. Basic network survivable design and traffic restoration concepts are reviewed. Research issues in the current literature are discussed along with potential avenues for integration with security techniques.

1.3.5 Chapter 5: System Survivability

This chapter introduces several topics that are at the core of *systems survivability*. It first introduces the notion of survivability and discusses its relation to fault models to establish a bridge between survivability and fault tolerance. It analyzes the limitations of standard fault-tolerance techniques to environments subjected to malicious acts. The chapter introduces the concept of *design for survivability* and discusses various design approaches for survivability. The author introduces *decentralization* as a basic concept in overcoming the impact of faults and security compromises, and discusses it as a mechanism to achieve survivability. The chapter finally presents a transformation model that can be used to relate survivability problems to problems from other well-established theoretical fields, followed by a discussion on how this will enable us to find solutions to survivability issues in new solution spaces, and allow for complexity analysis and comparison of solutions.

1.3.6 Chapter 6: Taxonomy and Framework for Integrating Dependability and Security

This chapter surveys various taxonomies and frameworks for integrating *dependability* and *security*. It emphasizes that security issues have not been comprehensively

treated in existing taxonomies and frameworks. For instance, the security issues of authenticity and nonrepudiation have not been well integrated into the existing taxonomies and frameworks. In addition, many elements of existing taxonomies appear loosely integrated without generic relationships that capture interactions among different elements. Based on this observation, the authors present a novel integrated generic taxonomy and framework by using a feedback control system as a model to integrate concepts and attributes of both dependability and security. The chapter further expands the framework to cover lower-level techniques related to security and survivability.

1.3.7 Chapter 7: Stochastic Models/Techniques for Secure and Survivable Systems

This chapter focuses on the need for the quantitative analysis of dependability attributes, in particular, security and survivability. In this chapter, the authors explain *stochastic modeling techniques* based on Markovian and non-Markovian models for evaluating the system security and survivability. In particular, efforts toward capturing the details of real architectures for the systems often result in large stochastic models that are difficult to solve. The chapter emphasizes the use of higher-level formalisms based on stochastic Petri nets and their extensions for this purpose. The chapter presents these formalisms and illustrates them in the context of security and survivability modeling of the networked systems.

1.3.8 Chapter 8: Integrated Dependability and Security Evaluation Using Game Theory and Markov Models

This chapter attempts to interpret and assess the trustworthiness of networked information systems by combining security and dependability approaches. In particular, the chapter emphasizes the need for a combined approach in order to more accurately model reality. The chapter discusses the security of a system in a probabilistic manner with a goal to supplement assessment techniques from both security and dependability domains. The chapter extends a continuous-time Markov chain (CTMC) to include security attacks modeled using *game theory techniques* and categorized as intentional faults. It shows how dependability modeling and analysis can be further used to obtain quantitative metrics of system security as well as system trustworthiness.

1.3.9 Chapter 9: Scenario Graphs Applied to Network Security

This chapter deals with the complex problem of generating attack graphs. While the traditional model-checking approach produces one counterexample to illustrate a violation of a property by a model of a system, this chapter adopts the model-checking approach to generate all counterexamples that violate a given property. The chapter presents algorithms to create a set of *all* the counterexamples, called a *scenario graph*, for a networked system. The chapter explains how a scenario graph can be used to study what attacks are possible on a particular configuration of a networked system. Using a detailed example, the chapter illustrates how one can model a computer network and automatically generate and analyze attack graphs. The attack graph produced by the algorithms presented shows all ways in which an intruder can violate a given desired security property.

1.3.10 Chapter 10: Vulnerability-Centric Alert Correlation

This chapter discusses issues related to survivability of systems under multistep network intrusions. Defending a network against such intrusions is particularly challenging because experienced attackers can circumvent security controls and detections by gradually elevating their privileges on the intermediate hosts before reaching the final goal. This chapter describes recent advances in correlating intrusion alerts for the defense against such multistep network intrusions. Alert correlation techniques aim to reassemble correlated intrusion detection system (IDS) alerts into more meaningful attack scenarios. The chapter presents a *vulnerability-centric* approach to alert correlation that benefits from the advantages of topological vulnerability analysis and those of alert correlation. The chapter discusses how this method can effectively filter out irrelevant alerts, defeat the so-called *slow attacks*, and add to alert correlation the capabilities of hypothesizing missing alerts, predicting possible future alerts, and aggregating repetitive alerts. Empirical results presented show that these tasks can be fulfilled faster than the IDSs can report alerts under intensive attacks.

1.3.11 Chapter 11: Monitoring and Detecting Attacks in All-Optical Networks

This chapter focuses on the security attacks related to an all-optical network (AON). An AON is essentially a network in which data does not undergo optical-to-electrical (O-E) or electrical-to-optical (E-O) conversion within the network.

Although AONs are a viable technology for future telecommunication and data networks, little attention has been devoted to the intrinsic differences between AONs and existing electro-optic/electronic networks in issues of security management. AON features like transparency and nonregeneration make attack detection and localization difficult. However, it is important to detect and localize an attack quickly in a transparent AON. The chapter specifically focuses on the diagnosis of crosstalk attacks as crosstalk attacks have the potential to create the widespread damage in AONs. The chapter provides a crosstalk attack model and a monitoring model, and then shows that it is possible to effectively reduce the number of monitors while still retaining all diagnostic capabilities. In particular, the chapter presents necessary and sufficient conditions for diagnosis of both single as well as multiple (i.e., *k*-crosstalk) attacks. The key ideas used for this include employing the status of existing connections along with that of test connections for diagnosis. The chapter also develops efficient monitor placement policies, test connection setup policies, and routing policies for such a network.

1.3.12 Chapter 12: Robustness Evaluation of Operating Systems

This chapter focuses on the *robustness* of the operating system (OS). Because it is a key component in all computer systems, it is imperative that the OS has an ability to correctly support the applications running on it even in the presence of operational perturbations. The chapter introduces *OS robustness* as the degree to which an OS can handle the perturbations and maintain its correct functionality. Among various perturbations that an OS may have to withstand include hardware malfunction, buggy software, invalid inputs, and stress generated by applications running on it. In essence, OSs are highly complex functional entities with countless environment interaction scenarios that limit the use of static analytical approaches. This chapter emphasizes experimental evaluations of *OS robustness* as a preferred approach and discusses various experimental methods. The chapter places key emphasis on *target system definition*, *choice of evaluation strategy*, *the metrics to use*, and *interpretation of the results*. Using a case study, the chapter illustrates these various aspects of the robustness evaluation methods.

1.3.13 Chapter 13: Intrusion Response Systems: A Survey

Protecting networks from security attacks is an important concern. While the *intrusion prevention* and *intrusion detection* systems have been the subject of much study, the actions that need to follow the steps of prevention and detection, namely

response, have received less attention from researchers or practitioners. It was traditionally thought of as an offline process with humans in the loop, such as system administrators performing forensics by going through the system logs and determining which services or components need to be recovered. This chapter lays out the design challenges in building an autonomous intrusion response systems and provides a classification of existing work on the topic in four categories: *response through static decision tables*, *response through dynamic decision process*, *intrusion tolerance through diverse replicas*, and *intrusion response for specific classes of attacks*. The existing intrusion response systems are analyzed by using the classification schemes presented in this chapter. The chapter also presents methods for benchmarking the intrusion response systems.

1.3.14 Chapter 14: Secure and Resilient Routing: A Framework for Resilient Network Architectures

This chapter presents a generic framework for a secure and *resilient network routing architecture*. Such an architecture provides different services with different priorities to coexist in a virtualized environment. A key issue here is to provide robustness to the routing architecture to protect against network overloads and security attacks. The chapter discusses building blocks for the proposed framework, which is shown to be conducive to providing secure traffic engineering as well as network resiliency. The approach taken in this chapter starts with the identification of the need for the service requirement for security and resiliency in a prioritized environment and works backwards to identify the desirable architectural components to support this service paradigm.

1.3.15 Chapter 15: Security and Survivability of Wireless Systems

Information assurance techniques employed in wired networks have limited direct applicability in *wireless networks* because of the unique aspects of wireless networks (e.g., user mobility, wireless communication channel, power conservation, limited computational power in mobile nodes, security at the link layer, and so on). The interaction between the components of information assurance, namely availability and security, in a wireless network environment poses new challenges. In this chapter, recent research on understanding survivability and security in wireless networks and their interaction is presented.

1.3.16 Chapter 16: Integrated Fault and Security Management

This chapter focuses on an integrated framework for managing *faults* and *security intrusions*. The chapter emphasizes the need to be careful while identifying symptoms related to faults and security attacks, which may be similar, and classifying faults or security attacks based on such symptoms. Integration of fault and intrusion management is, however, a natural result of the similarity in the techniques used to analyze and identify them (i.e., based on symptom collection, correlation, and evaluation). The chapter presents an active problem diagnosis framework that analyzes faults and security alarms using the same engine. A key challenge is to ensure that incomplete symptom information is handled to properly identify faults and intrusions. The chapter then presents an architecture for network-based intrusion detection systems that analyzes traffic collected from different sensors, identifies faults and intrusions, and initiates actions to mitigate the intrusions/faults and their effects.

1.4 CONCLUSION

As noted above, the goal of the book is to provide the reader with an appreciation of the need for integrating security and dependability techniques to address information assurance problems. Note that the chapters included in this book represent some pressing issues and they are not in anyway exhaustive in considering the integration of the security and dependability areas; for example, discrete event simulation has been used for both security and dependability analysis [6], but currently we have no chapter addressing the discrete event simulation approach.

Lastly, the editors wish to thank the authors for their contributions to the book and help in its publication.

References

[1] T. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Wiley-Interscience, 2006).

[2] E. Jonsson, "An Integrated Framework for Security and Dependability," *Proceedings of 1998 ACM Workshop on New Security Paradigms*, Charlottesville, Virginia, United States 1998.

[3] J. McDermott, A. Kim, and J. Froscher, "Merging Paradigms of Survivability and Security: Stochastic Fault and Designed Faults," *Proceedings of ACM New Security Paradigms Workshop*, Ascona, Switzerland 2003.

[4] National Science and Technology Council, "Federal Plan for Cyber Security and Information Assurance Research and Development," April 2006, at http://www.nitrd.gov/.

[5] Secure IST Advisory Board, "Recommendations for a Security and Dependability Research Framework," Issue 3.0, January 2007, at http://ftp.cordis.europa.eu /pub/ist /docs/trust-security/securist-ab-recommendations-issue-v3-0_en.pdf.

[6] D. Nicol, W. Sanders, and K. Trivedi, "Model-Based Evaluation: From Dependability to Security," *IEEE Transcript on Dependable and Secure Computing* 1, No. 1 (January–March 2004). pp. 48–65

[7] M. Bishop, "Computer Security: Art and Science," Addison-Wesley (ISBN: 0-201-44099-7), 2002.

[8] B. E. Helvik, "Perspectives on the dependability of networks and services," Telektronikk (100th Anniversary Issue: Perspectives in telecommunications), Vol. 3, 2004, pp. 27–44.

[9] Michael A. Harrison, Walter L. Ruzzo and Jeffrey D. Ullman, "Protection in Operating Systems", Communications of the ACM, Vol. 19, No. 8, August 1976, pp. 461–471.

[10] Carl E. Landwehr, Alan R. Bull, John P. McDermott, William S. Choi, "A taxonomy of computer program security flaws" ACM Computing Surveys (CSUR), Vol. 26 , Issue 3 (September 1994) pp. 211–254.

[11] Avizienis, A., J. C. Laprie, B. Randell and C. Landwhehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 1, Jan–March 2004, pp. 11–33.