This book addresses three broad aspects of situational awareness in computer network defense: principles, methods, and applications, with six chapters devoted to each area.

PRINCIPLES

The principles section of the book is comprised as follows:

The in depth coverage of situational awareness rightly begins in chapter 2 by addressing the human factor component of situational awareness. The greatest threat to information security is generally considered to be the insider. This chapter gives an overview of business practices and how people and human relations influence situational awareness and information security in an organization. It highlights the need to train employees in information security with a view to improving their information security awareness. It shows the relevance of socio-technical theory and the general deterrence theory to investigations into the effectiveness of implemented organizational information security measures.

The effective conduct of warfare requires command and control systems for defensive and operational capabilities. Cyber-space is now considered to be the fifth domain of warfare after land, sea, air, and space. For national security it requires a Cyber Command and Control environment that is suitable for military and civilian use. Chapter 3 describes research undertaken to lay the foundations for the development of a Cyber Command and Control environment and identifies the challenges faced in realising that environment based on the body of knowledge in Command and Control and Situation Awareness Theory. The chapter presents a Cyber Command and Control reference architecture and a Collaborative Situational Awareness for Decision Making framework. It draws attention to the fact that the field of cyber security analytics requires extensive research in the interests of national security.

With the development of situational awareness in intrusion defense, the adoption a proactive defense strategy to combat a multi-stage attack is a realistic option. At its current stage, a multi-stage attack seeks to use intelligence gathered in previous stages of the attack to break the defense of the system. At a given stage of a multi-stage attack, a proactive defense strategy uses knowledge of the attack gained in previous stages of the attack to improve the defense of the system. The resulting situation can be modelled using classical game theory. In chapter 4 the best current move of the defender is modelled as a discrete-time stochastic control problem. An on-line scenario based proactive defense algorithm based on differential dynamic programming (DDP) is presented, which can solve the associated optimal control problem. The algorithm is validated through numerical experiment.
Chapter 5 proposes an alternative, more contextually-grounded framework for cyber-situational awareness that seeks to more fully account for the interaction of the human agent with the cyberspace environment. The framework is applicable to multiple levels of analysis by human agents. The knowledge dimension describes the internal cognitive processes and structures of the agent. The action component describes the interaction of the agent with the environment. and the environment dimension accounts for system, enterprise, and operational factors.

Chapter 6 describes the security needs of a Situational Awareness system, mentions the basic techniques that can be applied to achieve these goals, and discusses some of the issues. It discusses advantages and benefits of certain approaches and solutions, and weighs them against the cost of maintaining them, the difficulty of implementing them, or obtaining the desired degree of reliability. This chapter is not aimed at the IT manager or Network Security administrator, but at scientists seeking to expand the boundaries of the Computer Network Defense field and designers evaluating their options to decide on the acceptable set of compromises for the system they are working on.

Chapter 7 investigates task and system requirements that Computer Network Defense systems should meet to support enhanced operator situational awareness. Task requirements are human operator-specific tasks such as risk assessment, protective monitoring, and decision making. System requirements are automated system-specific tasks completed by computer systems and network appliances. There are two main categories of requirements: non-functional and functional. Non-functional requirements are concerned with the quality of the system. Functional requirements are functions the system performs such as processing, display, tasks, and analysis. The chapter provides a comprehensive assessment of pertinent factors to be considered when designing modern computer and network systems for situational awareness in a Computer Network Defense environment. It is highlighted that few contributions in the published literature discuss qualitative task and system requirements.

METHODS

The methods section of the book is comprised as follows:

Chapter 8 presents a cognitive Instance-Based Learning (IBL) model of a security analyst’s recognition and comprehension processes in a cyber-attack scenario. The IBL model recognizes network events based upon events’ situation attributes and their similarity to past experiences (instances) stored in the model’s memory. Then, the model comprehends a sequence of observed events as being a cyber-attack or not, based upon instances retrieved from its memory, the similarity mechanism used, and the model’s risk-tolerance. The model generates predictions about the recognition and comprehension processes of an analyst in a cyber-attack. It is proposed that computational models based on the IBL theory can be used to make predictions of a security analyst’s cyber-situational awareness in a cyber-attack scenario. Simulation results indicate that the cyber-situational awareness of an analyst is a function of their memory of threat and non-threat events, risk-tolerance, and the methods they use to compare network events to prior experiences of events. The predictions obtained indicate that it might be helpful to devise security analyst job training that makes analysts cautious about the possibility of cyber threats and less risk-tolerant, which enables them to look for features in attributes of network events that communicate the indication of potential threats.
Research into information fusion for multi-sensor data in support of military operations has led to the development of process models, creation of algorithms for signal and image processing, pattern recognition, state estimation, automated reasoning, and dynamic resource allocation. Chapter 9 adapts these models to the domain of cyber security and presents a novel means of situational awareness involving an auditory representation (sonification) of network traffic. The chapter suggests that effective information data fusion for computer network defense will require multi-disciplinary efforts and work on multiple areas including algorithms and techniques “inside the machine” and “outside the machine” to improve the ability of analysts to understand a) An evolving cyber situation, b) Identify and predict threats, and c) Develop collaborative decision making methods. It is asserted that success in this domain will require simultaneously addressing both areas, from both directions.

Chapter 10 reports work on quantitatively detecting threats and targeted intruder activity using sensor fusion Intrusion Detection Systems (IDSs), which are composed of several constituent IDSs. The more independent and distinct the attack space is for the constituent IDSs, the better the fusion IDS performs. A simple theoretical model is provided for the purpose of showing the improved performance of fusion IDSs. The detection rate and the false positive rate quantify the performance benefit obtained through the fixing of threshold bounds. The theoretical analysis is supplemented with experimental evaluation, and the detection rates, false positive rates, and F-score were measured. Preliminary experimental results support the correctness of the theoretical analysis. The chapter also demonstrates that sensor fusion based intrusion detection is more flexible and outperforms other existing fusion techniques using real-world network traffic embedded with attacks.

Chapter 11 presents the design of a dynamic collaborative defense infrastructure to detect and limit distributed denial of service attacks. The Collaborative Defense Architecture (CDA) introduces the design of a separate security plane to manage and pass information between the various network elements. The decision logic for the security mechanisms is distributed in a small set of active security guards (Active sentinels), each responsible for a set of core routers. The Active sentinels collaborate both by proactive and reactive mechanisms to mitigate attacks. The task of the Active sentinels is to actively probe packets sent probabilistically by routers in the network. Upon the detection of an attack, the Active sentinels send messages to the Edge firewall nodes to filter the attack traffic by changing their rule set. The design and evaluation study confirms that such a global and coordinated approach would be real-time and cost-effective with very minimal changes to the current network infrastructure.

The Domain Name System (DNS) is probably the most critical service in the Internet as it translates domain names into the numerical IP address of any network host. Any DNS security breach could cause severe problems to affected network domains, and in the worst case, to the Internet as a whole. However, the original DNS design was concentrated on availability, not security, and thus included no authentication. This security gap has been addressed by two cryptographic mechanisms: DNSSEC and DNSCurve. They both utilize public key cryptography and extend the core DNS protocol. Although the second mechanism is still in its infancy, while the first is well-standardized, they are both promising and quite likely to compete with each other in the near future. Chapter 12 provides a comprehensive and constructive comparison of DNSSEC and DNSCurve and concludes that a mechanism that combines the advantages of both methods; namely the high speed Elliptic Curve Cryptography of DNSCurve and the end-to-end security of DNSSEC would be highly appreciated.

For situational awareness, authentication of all users of the network is an absolute requirement. For users accessing company provided resources out of the office on a Next Generation Network (NGN), there will be two steps to authenticating users. First the user must be authenticated by the NGN, and
then, the corporate network must authenticate users of resources it provides who are accessing those resources over a NGN. In NGNs, the use of real-time applications in mobility will be critically dependent on stringent Quality of Service requirements being met. Roaming often implies a temporary service disruption due to handover from one Point of Attachment to another. Authentication, Access, and Accounting (AAA) based authentication mechanisms like Extensible Authentication Protocol (EAP) incur signalling overheads due to large Round Trip Times, and as a result, overall handover latency also increases. Such disruption is unacceptable for potentially business-critical applications such as Voice over IP (VoIP), video conferencing, streaming media, etc. In chapter 13, a fast re-authentication scheme is presented, which utilizes IEEE802.21 Media Independent Handover (MIH) services to minimize the EAP authentication process delays, and as a result, reduce the overall handover latency. Therefore, it is shown that the demands mobility places on availability can be broadly met, leaving only the generic issues of Internet availability.

**APPLICATIONS**

The applications section of the book is comprised as follows:

Chapter 14 describes work on modelling situational awareness information and system requirements for the mission based on Goal-Oriented Task Analysis using an Agent Oriented Software Engineering methodology called Secure Tropos. The security enhanced actor diagram used to model the mission’s security operational capability requirements represents each stakeholder’s objectives and demonstrates how these objectives can be modelled to achieve enhanced situational awareness for each stakeholder in the Computer Network Defense environment. This work provides valuable insight on how to effectively achieve the mission’s goal-orientated (high-level) and task-orientated (low-level) requirements. Model validation is done using security attack scenario testing. It is shown how a simulated attack can be assessed using the proposed model. The outcome of the security scenario testing is a security test case, which shows that the model has the capability to detect and dispel the type of attack launched.

Cyber-physical systems (CPS) are systems with a tight coupling of the cyber aspects of computing and communications with the physical aspects of dynamics and engineering. Real-time monitoring provided by wireless sensor networks (WSNs) is essential for CPS, as it provides information on the condition of physical systems. In WSNs, the attackers could inject false measurements through compromised sensor nodes, which not only threaten the security of the system, but also consume significant network resources, reducing the lifetime of sensor networks. To mitigate this type of attack, a number of situation aware en-route filtering schemes to filter false data inside the networks have been developed. However, there is lack of a systematic strategy to evaluate these schemes and establish a foundation for designing en-route filtering techniques. In chapter 15, a taxonomy of en-route filters is developed by categorizing the existing en-route filtering schemes and comparing their advantages and disadvantages. To fairly compare the schemes, a theoretical analysis is conducted, from which, a set of closed formulae for each of the schemes is derived. Extensive simulations validate the reported findings.

Chapter 16 describes how to use attack graphs to evaluate the security vulnerabilities of embedded systems and provides examples of the use of this technique. The systems investigated in this chapter are embedded systems that span hardware, software, and network communication. The example cases studied are (1) radio frequency identification (RFID), (2) vehicle networks, and (3) the Smart Grid (the next generation power and distribution network in the USA). Attack graphs describe the steps an
adversary could take to reach a desired goal and can be analyzed to quantify risk. Attack graphs enable
the discovery of new and unknown vulnerabilities. Armed with this, Information System designers can
redesign the system to address and remove these vulnerabilities. System administrators can use this
information to apply patches and other defensive measures to secure existing or deployed systems. Cur-
cently, most work in attack graphs focuses on development of the attack graph and not on the analysis
of the resulting attack graph. The chapter concludes that methods for the analysis of attack graphs that
are both accurate and computationally efficient must be developed and formalized.

Chapter 17 proposes a new machine learning method for intrusion detection. The method improves
the performance of multiple Intrusion Detection Systems (IDSs) using Data-dependent Decision fusion.
The Data-dependent Decision fusion approach gathers an in-depth understanding about the input traffic,
and also the behavior of the individual IDS by means of a neural network learner unit. The method
adapts and extends notions from the field of multi-sensor data fusion for the Data-dependent Decision
Fusion. The extensions are principally in the area of generalizing feature similarity functions to compre-
hend observances in the intrusion detection domain. The approach has the ability to fuse decisions from
multiple, heterogeneous, and sub-optimal IDSs. The test results reported using of the Data-dependent
Decision Fusion method are better than those predicted by the Lincoln Laboratory after the DARPA
IDS evaluation.

Chapter 18 focuses on the design of architecture and algorithms for optimization of network defense
systems, specifically firewalls, to aid not only adaptive and real-time packet filtering but also fast content
based routing (differentiated services) for today’s data driven networks. It presents various algorithmic
and architectural techniques that seek to overcome shortcomings in terms of adaptation, speed of opera-
tion (under attack or heavily loaded conditions), and overall operational cost-effectiveness of current
network defense systems. Approaches for Tier-I Internet Service Provider networks, and filtering rout-
ers are presented to correlate the dynamic metrics and achieve situational awareness required to protect
critical network infrastructure and data driven operations over the Internet. The tools proposed also aim
to offer the flexibility to include new approaches, and provide the ability to migrate or deploy additional
entities for attack detection and defense. The design aspects presented in the proposed automated tool
PITWALL assist network administrators in gaining real-time network dynamic information and hence
in enhancing the overall security of any typical enterprise network system.

As a starting point for the development of a common visualization of the forensics process by the
members of an investigating team, chapter 19 provides algorithms that provide guidance and step by
step instructions on how to deal with computer forensics and the investigations they carry out. A general
introductory overview of computer forensics is provided, and then the framework of a forensic inves-
tigation is summarized. On the basis of this framework, three algorithms are provided, one for each
phase of a forensic investigation, which cover the different aspects of computer forensics and address
key elements to be considered when attacked systems are investigated. Algorithms that provide a com-
plete model of the forensics process are unlikely to be created, but they are a starting point, from which
additional guidance can be provided to analysts on the basis of their particular expertise that leverages
their existing understanding of the workspace.