PREFACE

Communication between people has changed with the invention of the telephone. The ability to communicate across continents in real-time has also helped our society in several dimensions including entertainment, trade, finance, and defense. But this new capability did not come without an investment. Building an international telephony infrastructure has required the cooperation of both commercial and government organizations to evolve into what it is today. It has also led to the formation of international standard bodies that both direct and support the industry towards an interoperable communication networks.

IP networks are the next step from the traditional telecommunications. For a while, IP family of protocols was only used in the Internet, and the main applications were file transfers and e-mail. With the World Wide Web, the Internet changed into a global and always open information distribution channel. And finally with the advent of VoIP, the Internet is becoming a real-time communication media that integrates with all the earlier multimedia capabilities.

Traditional telecommunication networks are critical to the survival of our society. The PSTN is a closed network and its operational intricacies are known to a few select individuals who have devoted much of their lives to building it. Although operations in PSTN are not entirely a secret, they were and still remain proprietary for several reasons such as competitive advantage and national defense. The PSTN was and remains a closed infrastructure that concentrated its intelligence in its core network elements and left the edge devices very simplistic. The equipment and resources to operate a TDM network require a substantial financial investment. This lack of direct access to core network elements from subscribers and the high price of connectivity alleviated the risk for attacks. Ergo, subscribers demonstrate greater trust for communications through the PSTN compared to the Internet. This is a misconceived trust once you start analyzing the PSTN components and protocols and realize the lack of protection mechanisms.

In the earlier days of the Internet, security was appalling. The Internet was an open network where anyone could attack anyone anonymously and many of the attack tools were, and still are, available. As such, security research became a standard practice in government, commercial, and academic worlds with globally known research groups in organizations such as DARPA, DISA, CERIAS, MIT CIS, Bellcore, Bell Labs, and many others. Things became a bit more complicated with the transition of critical services such as telephony on the Internet along with other multimedia applications such as video and gaming. And due to the performance, availability, and privacy requirements of these applications, their security requires new approaches and methods compared to traditional IP security. Nevertheless the traditional security objectives apply such as confidentiality, integrity, and availability of services.

Before gaining the interest of the academia, the topic of Internet security has been a secret science, or not even a science. The security field was a competition between hackers and system administrators, in a constant race of "patch and penetrate." Very few people knew what they actually were fixing in the systems when they applied new security updates or patches. And very few hackers understood what the attack tools actually did when they penetrated the services they wanted access to. People spoke of threats, attacks, and security measures that needed to be applied to protect from these attacks. The actual core reasons that enabled the existence of the attacks were not understood. For most of the users of communication systems, these weaknesses were hidden in complex, hard-to-understand protocols and components used in the implementations.

VoIP has been discussed at length in many textbooks and thus we avoid long discussions of its origins and details on introductory concepts. Instead the book focuses on the details associated with the security of multimedia communications including VoIP. Our purpose is to extend your knowledge of vulnerabilities, attacks, and protection mechanisms of VoIP and generally Internet multimedia applications. We deviate from listing a series of security tools and products and instead provide detailed discussions on actual attacks and vulnerabilities in the network design, implementation, and configuration and protection mechanisms for signaling and media streams, architectural recommendations, and organizational strategy—thus enabling you to understand and implement the best countermeasures that are applicable to your environment.

The book is structured so that we start by briefly explaining VoIP networks, and then go through the threats, attacks, and vulnerabilities to

enable you to understand how VoIP attacks are made possible and their impact. The book discusses in great detail various attacks (published and unpublished) for eavesdropping, unauthorized access, impersonation, and service disruption. These attacks are used as proof of concept, but at the same time they also expose the reader to real-life weaknesses and serve as a mechanism to promote comprehension. In addition, this book discusses VoIP vulnerabilities, their structure, and their categorization as they have been investigated in enterprise and carrier environments.

Following VoIP vulnerabilities and attacks, the book discusses in great detail a number of protection mechanisms. In order to protect against current and emerging threats, there a number of areas that need to be considered when deploying VoIP. The book provides extensive coverage on the intricacies, strengths, and limitations of the protection mechanisms including SIPS, H.235, SRTP, MIKEY, ZTP, and others. Furthermore, the book focuses on identifying a VoIP security framework as a starting point for enterprise networks and provides several recommendations. Security architectures in enterprise and carrier environments are also discussed.

This first edition of the book aims in establishing the landscape of the current state of VoIP security and provides an insight to administrators, architects, security professionals, management personnel, and students who are interested in understanding VoIP security in detail.