Introduction to Network Security

Douglas W. Jacobson
Iowa State University

Table of contents

Part 4 Network-Based Mitigation

Preface

Approach

This book focuses on network security from the view point of a network's vulnerabilities, protocols, and security solutions. Unlike other books that focus on security and security paradigms where networks are viewed as a mechanism for communication, this book focuses on the network as a source of both insecurity and security. The book will examine various network protocols looking at vulnerabilities, exploits, attacks, and methods to mitigate an attack. Networks as communication systems have been around since the dawn of human history and rely on trust between communicating parties in order to function. Early communications systems relied on visual verification of the communicating parties involved and often used simple codes to protect the data. For example couriers were known by both parties and messages were sealed with wax to help ensure privacy. As technology improved, methods used to transmit data also improved and so did the methods to steal and to protect data. However, even as late as the end of the 20th century data was still being transmitted directly between two parties with no concept of a network. These parties relied on additional knowledge to verify the authenticity of the data. The issues we face today are more complex than those of the past. Today we have interconnected computers using a network not controlled by any one entity or organization. Unlike data communications of the past, today's networks consist of numerous devices that handle the data as it passes from the sender to the receiver. These networks are designed to facilitate communication and are intended for a small group of trusted and knowledgeable individuals. Security is not part of the design process.

Organization

Part 1 of this book is a brief discussion of network architectures and the functions of layers in a typical network along with a taxonomy of network-based vulnerabilities and attacks. This taxonomy is the framework for presenting the vulnerabilities and attacks at each layer of interest. The taxonomy divides the vulnerabilities and attack space into four categories.

- Header-based vulnerabilities and attacks: the protocol headers have been modified or are not valid.
- Protocol-based vulnerabilities and attacks: the packets are valid but are not used correctly.
- Authentication-based vulnerabilities and attacks: where the identity of the sender or receiver is modified.
- Traffic-based vulnerabilities and attacks: the volume of traffic creates the attack.

The remainder of the book is divided into three parts. Part 2 covers the different layers of the network (Physical, Network, and Transport) looking at the security for each layer. Using a bottom-up approach to network security allows the reader to understand the vulnerabilities and the security mechanisms provided by each layer of the network. For example, by understanding which vulnerabilities are introduced by the physical layer and what level of security can be provided, the reader can understand which vulnerabilities may exist in the network layer and which security mechanisms could be used to overcome the vulnerabilities. Part 3 looks at the security of several common network applications. On the Internet, applications treat the lower layers of the network as a simple pipe that sends data to another application and it arrives without error. This book views vulnerabilities as network functions provided by the layer below thus giving the reader insight into understanding the security needed to overcome the vulnerabilities. Part 4 provides an overview of several network-based security solutions that are often deployed and relates them back to the taxonomy.

This book describes a define-attack-defend methodology for network security. The relevant protocols are briefly introduced followed by detailed descriptions of known vulnerabilities and possible attack methods. The book then focuses on the attack methodology rather than on particular tools, though tools are introduced as possible homework problems and lab Experiments. Once the reader understands the threats against the protocol, possible solutions will be presented. Each chapter has homework problems that are based on the concepts introduced in the chapter and will have lab Experiments that will allow the reader to try some of the attacks and to look at the effectiveness of the solutions. An appendix provides details to develop and deploy a low-cost lab environment that can be used to support the classroom or used as a small corporate test bed. Another appendix provides an overview to cryptology.

Target Audience:

This book is targeted at two compatible audiences. The primary focus of the book is as a text for a senior or first year graduate course in network security for students in computer science or computer engineering. The book can be used for a network security course that is part of a security curriculum or for a course that is part of a networking curriculum. The book is also intended as a reference book for network and security professionals.

Differences between this book and other books:

- **Network focused**: This book looks at network security by looking at network protocols, their weaknesses, and countermeasures. Several books also have a network focus but primarily deal with a few application-level protocols (Kerberos, PGP, PEM, etc.) and are not concerned about the lower layers. (Physical, network, transport) Many of the difficult problems arise from the vulnerabilities in these layers.

- **Network view of security**: This book looks at network security using the approaches found in most network books, by looking at the layers and what services and functions are provided. We will look at vulnerabilities and security as services and functions provided by the layer. By using a network view, the book could be used in either a networking curriculum to add security or in a security curriculum to add network security.
- **Lab Experiments**: This book contains lab experiments to support the material. The experiments will look at both attacks and defenses. The book also provides a low-cost lab configuration that can be used as a model.
- **Web Site**: A web site is provided to support the book. The web site contains lecture materials, tutorials on UNIX, C, and socket programming, and detailed information to establish and maintain the test laboratory.
- **Practical view of network security**: This book has a practical view of network security. We will look at actual protocols and provide the reader with the details and information they need to understand the vulnerabilities and to develop appropriate countermeasures. This is reinforced through the lab Experiments.
- **Attack and defend approach**: This book looks at network security from an attack and defend approach. The book looks at the vulnerabilities in the current protocols and then looks at defense systems that could mitigate the attacks. While the book will not focus on attack tools, it will look at attack methods and through the lab Experiments students will be able to study the effects of certain attacks on the network and study the effectiveness of the security system.

- **Terms defined**: So much of networking and security involves the use of terms, many of which are specific to the field that the author feels that it is important that after each section of a chapter any new terms that were defined in the section will be enumerated with a short definition. Before we begin the text there are a few terms that should be defined so the reader has a common frame of reference.

Definitions:

Host: A term used to describe a computer connected to the Internet.

User: The individual using a computer application that utilizes the network, or a general computer user.

Application: A computer program that allows a user to connect to the network and perform a task.

Hacker: A person or persons that use the network to attack computer systems, networks, or other devices connected to the Internet.

Attacker: Same as a hacker

Target: The device, host, user, or object that the hacker is trying to attack.

Network: A group of interconnected devices that can communicate with each other.

Network Device: A device connected to the network. This is more generic than a host or computer in that it can be any network-enabled device.

Internet: A global collection of networks of interconnected network devices.

Acknowledgements

I would like to thank my wife Gwenna and my children (Sarah, Jordan, and Jessica) for all of their support and patience. I would also like to thank Sharon Sparks for her editing help.