Cisco Systems

Intrusion Prevention Fundamentals

An introduction to network attack mitigation with IPS

ciscopress.com

Earl Carter • Jonathan Hogue

Intrusion Prevention Fundamentals

Earl Carter
Jonathan Hogue

Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Intrusion Prevention Fundamentals

Earl Carter and Jonathan Hogue

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

First Printing January 2006

Library of Congress Cataloging-in-Publication Number: 2005922371

ISBN: 1-58705-239-3

Warning and Disclaimer

This book is designed to provide an overview of intrusion prevention by examining Host-based Intrusion Prevention capabilities and Network-based Intrusion Prevention functionality. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc., shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Corporate and Government Sales

Cisco Press offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact: **International Sales** 1-317-581-3793 international@pearsontechgroup.com

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments about how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher	John Wait
Editor-in-Chief	John Kane
Executive Editor	Brett Bartow
Cisco Representative	Anthony Wolfenden
Cisco Press Program Manager	Jeff Brady
Production Manager	Patrick Kanouse
Development Editor	Deadline Driven Publishing
Senior Project Editor	San Dee Phillips
Copy Editor	Kevin Kent
Technical Editors	Greg Abelar, Gary Halleen, Shawn Merdinger
Editorial Assistant	Raina Han
Book and Cover Designer	Louisa Adair
Composition	Mark Shirar
Indexer	Tim Wright

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA

About the Authors

Earl Carter, CCNA, is a consulting engineer and member of the Security Technologies Assessment Team (STAT) for Cisco Systems, Inc. He performs security evaluations on numerous Cisco products, including everything from the PIX Firewall and VPN solutions to Cisco CallManager and other VoIP products. He started with Cisco doing research for Cisco Secure Intrusion Detection System (formerly NetRanger) and Cisco Secure Scanner (formerly NetSonar).

Jonathan Hogue, CISSP, is a technical marketing engineer in Cisco Security Business Unit, where his primary focus is the Cisco Security Agent. He has been involved with host-based security products since 1999 when he joined Trend Micro. In 2001, he began working with one of the first host intrusion prevention products, StormWatch by Okena, Inc. Okena was subsequently acquired by Cisco Systems.

About the Technical Reviewers

Greg Abelar has been an employee of Cisco Systems since December 1996. He was an original member of the Cisco Technical Assistance Security team, helping to hire and train many of the engineers. He has held various positions in both the Security Architecture and Security Technical Marketing Engineering teams at Cisco. Greg is the primary founder and project manager of the Cisco written CCIE Security exam.

Gary Halleen has been an employee of Cisco Systems, Inc., since 2000, and is a consulting systems engineer for security products. Gary works closely with Cisco security product teams and has presented at Networkers and other security conferences. Before he worked at Cisco, Gary held security positions at a college and an Internet service provider. Working with local law enforcement, Gary helped to prosecute the first successful computer crimes conviction in his state.

Shawn Merdinger is a security researcher based in Austin, Texas, with seven years of experience in the network security industry. He currently works with TippingPoint (a security division of 3Com), analyzing VoIP security. Before Shawn joined TippingPoint, he worked as a Security Research Engineer with the Cisco Systems Security Technologies Assessment Team (STAT) and Security Evaluation Office (SEO), where he performed vulnerability assessments on a variety of devices, technologies, and implementations. Shawn holds a master's degree from the University of Texas at Austin. Shawn is also an avid supporter of the local non-profit group AustinFreeNet, which helps to bridge the Digital Divide.

Dedications

Earl's dedication: Without my loving family, I would not be where I am today. They always support all the projects that I undertake. Therefore, I dedicate this book to my wife Chris, my daughter Ariel, and my son Aidan.

Jonathan's dedication: To my wife Liz, for believing in me.

Acknowledgments

First, we want to say that many people helped us during the writing of this book (too many to be listed here). Everyone that we have dealt with has been very supportive and cooperative. The technical editors, Greg Abelar, Shawn Merdinger, and Gary Halleen, supplied us with their excellent insight and greatly improved the accuracy and clarity of the text.

This Book Is Safari Enabled

The Safari® Enabled icon on the cover of your favorite technology book means the book is available through Safari Bookshelf. When you buy this book, you get free access to the online edition for 45 days.

Safari Bookshelf is an electronic reference library that lets you easily search thousands of technical books, find code samples, download chapters, and access technical information whenever and wherever you need it.

To gain 45-day Safari Enabled access to this book:

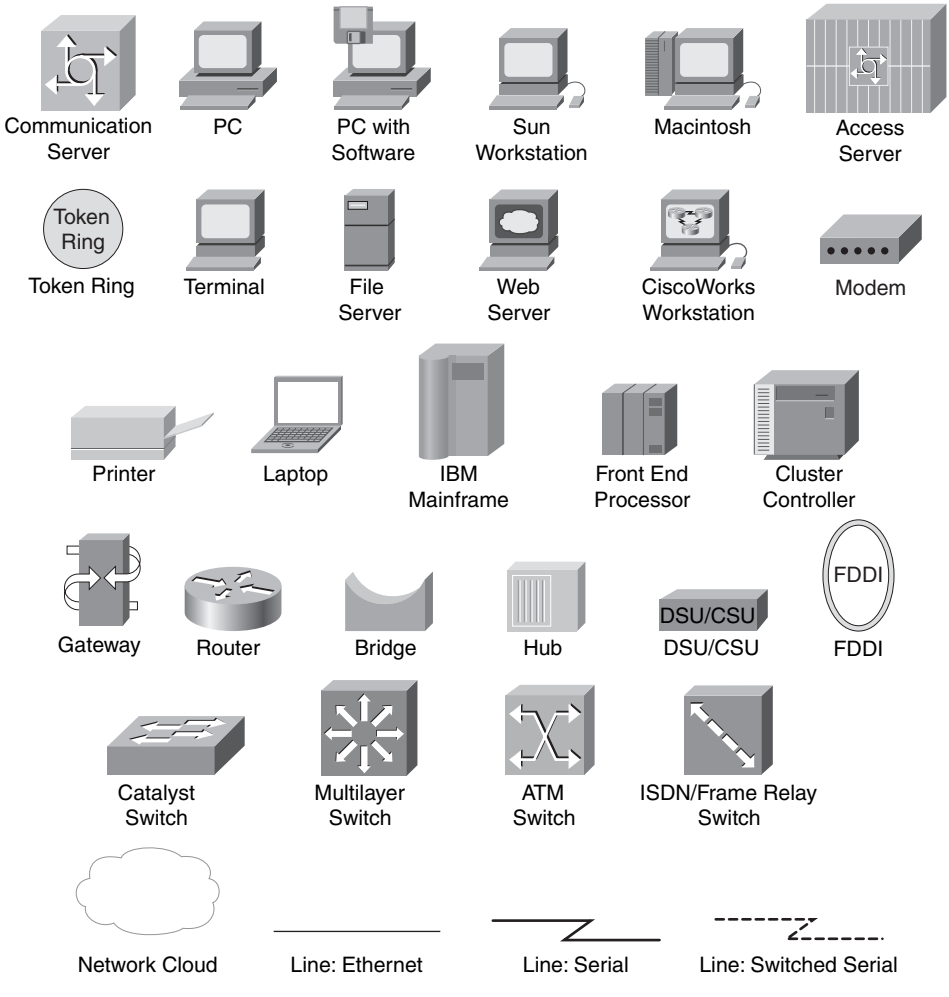
- Go to http://www.ciscopress.com/safarienabled
- Enter the ISBN of this book (shown on the back cover, above the bar code)
- Log in or Sign up (site membership is required to register your book)
- Enter the coupon code 4NF1-NPSG-QN6H-3TGF-DYJP

If you have difficulty registering on Safari Bookshelf or accessing the online edition, please e-mail customer-service@safaribooksonline.com.

Contents at a Glance

Contents

Icons Used in This Book



Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italics* indicate arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets [ ] indicate optional elements.
- Braces { } indicate a required choice.
- Braces within brackets [{ }] indicate a required choice within an optional element.

Introduction

Intrusion Prevention is a fairly new technology that you can deploy to protect your network from attack and help enforce your security policy guidelines. Understanding this technology is vital to successfully deploying this technology on your network. This book is designed to provide an overview of Intrusion Prevention that enables technology analysts and architects, especially those in charge of corporate security, to determine how Intrusion Prevention can be deployed on their networks. Furthermore, the information provided assists the reader to assess the benefits of Intrusion Prevention.

Goals and Methods

The goal of this book is to provide an introduction and in-depth overview of Intrusion Prevention as a technology, rather than a technical configuration guide. It uses real-world scenarios and fictitious case studies to walk readers through the lifecycle of an IPS project from needs definition to deployment considerations. Cisco IPS products are used as examples to help readers learn how IPS works, make decisions about how and when to use the technology, and what "flavors" of IPS are available. However, the intent of the material is to provide information on Intrusion Prevention as a technology, not just Cisco Intrusion Prevention products. The book answers questions such as the following:

- Where did IPS come from? How has it evolved?
- How does IPS work? What components does it have?
- What security needs can IPS address? How?
- Does IPS work with other security products? What is the "big picture?"
- Are there best practices related to IPS? What are they?
- How is IPS deployed, and what should be considered before a deployment?

Intrusion Prevention can be applied to your network at both the host level and at the network level. Each of these levels has specific capabilities that complement each other to provide a stronger overall level of security protection. This book explains the benefits of each of these areas of protection, and it walks the reader through detailed deployment examples to help you understand the steps you need to perform to deploy Intrusion Prevention on your network.

This Book's Audience

The primary audience for this book comprises information technology analysts and architects, especially those in charge of corporate security, networks, and business needs. These people should have an intermediate level of experience. The secondary audience includes network and security engineers with advanced experience as well as general technology analysts and journalists with experience at a beginner's level.

This book assumes that the reader has a basic understanding of common security technologies such as antivirus, Intrusion Detection Systems, and firewalls. Readers should also have a basic understanding of security threat and security regulations.

How This Book Is Organized

This book is organized into five major parts with subsections for each part. Part I introduces Intrusion Prevention technology as a whole, with subsections that detail the history and evolution of Intrusion Prevention System (IPS), the reason for its evolution, and continuing technology trends. Part II focuses on Host Intrusion Prevention specifically, how it works technically, an in-depth technical look at its components, what problems it can solve, purchase decisions, and so on. Part III examines Network Intrusion Prevention in a similar manner. Part IV delves into deployment of both technologies. Part V provides a sample Request for Information (RFI) document as well as a glossary of some key terms associated with Intrusion Prevention.

- **Part I: Intrusion Prevention Overview**

  The initial part provides a high-level overview of intrusion prevention. This overview provides the reader with a strong background understanding of Intrusion Prevention that is expanded in the Host Intrusion Prevention and Network Intrusion Prevention parts.

  — **Chapter 1, "Intrusion Prevention Overview"**—This chapter examines the factors that led to the existence of IPS, the evolution of security threats, the evolution of attack mitigation, and basic IPS capabilities.

  — **Chapter 2, "Signature and Actions"**—This chapter discusses the types, triggers, and actions of IPS signatures.

  — **Chapter 3, "Operational Tasks"**—This chapter reviews the high-level tasks related to using IPS. These include deployment, configuration, monitor IPS activities, and secure IPS communications.

  — **Chapter 4, "Security in Depth"**—This chapter demonstrates the importance of security in depth. It gives examples, explains the role of the security policy, and describes future IPS developments that re-enforce the concept.

- **Part II: Host Intrusion Prevention**

  This part provides detailed information about Host Intrusion Prevention and uses Cisco Security Agent (CSA) as a realistic example. The information provided, however, is not detailed step-by-step configuration examples. Instead, it explains in detail how the products can be used to provide Intrusion Prevention. Throughout each chapter, specific information is provided as to how CSA handles specific Host Intrusion Prevention problems that you might experience on your network.

  — **Chapter 5, "Host Intrusion Prevention Overview"**—This chapter looks at the capabilities, benefits, and limitations of HIPS.

  — **Chapter 6, "HIPS Components"**—This chapter examines the inner workings of HIPS agents and management infrastructures.

- **Part III: Network Intrusion Prevention**

  This part provides detailed information about Network Intrusion Prevention, along with realistic information to use Cisco Network Intrusion Prevention products. The information provided, however, is not detailed step-by-step configuration examples. Instead, it explains in detail how the products can be used to provide Intrusion Prevention. Each chapter provides detailed information on Cisco Network Intrusion product capabilities and how those capabilities can protect your network.

  - **Chapter 7, "Network Intrusion Prevention Overview"**—This chapter explains the capabilities that Network Intrusion Prevention Systems (NIPS) can add to a network to enhance its security posture.
  - **Chapter 8, "NIPS Components"**—This chapter analyzes and explains the various components that comprise a NIPS, including various sensor types and management options.

- **Part IV: Deployment Solutions**

  This section walks you through the deployment of Intrusion Prevention in different network configurations.

  - **Chapter 9, "Cisco Security Agent Deployment"**—This chapter describes the tasks and decisions you need to make during the implementation of a real-world HIPS product, the Cisco Security Agent (CSA).
  - **Chapter 10, "Deploying Cisco Network IPS"**—This chapter describes the tasks and decisions you need to make during the implementation of a real-world NIPS deployment, using the Cisco Network Intrusion Prevention System products as an example.
  - **Chapter 11, "Deployment Scenarios"**—This chapter covers an assortment of IPS deployment scenarios where each scenario uses a different type of company as an example.

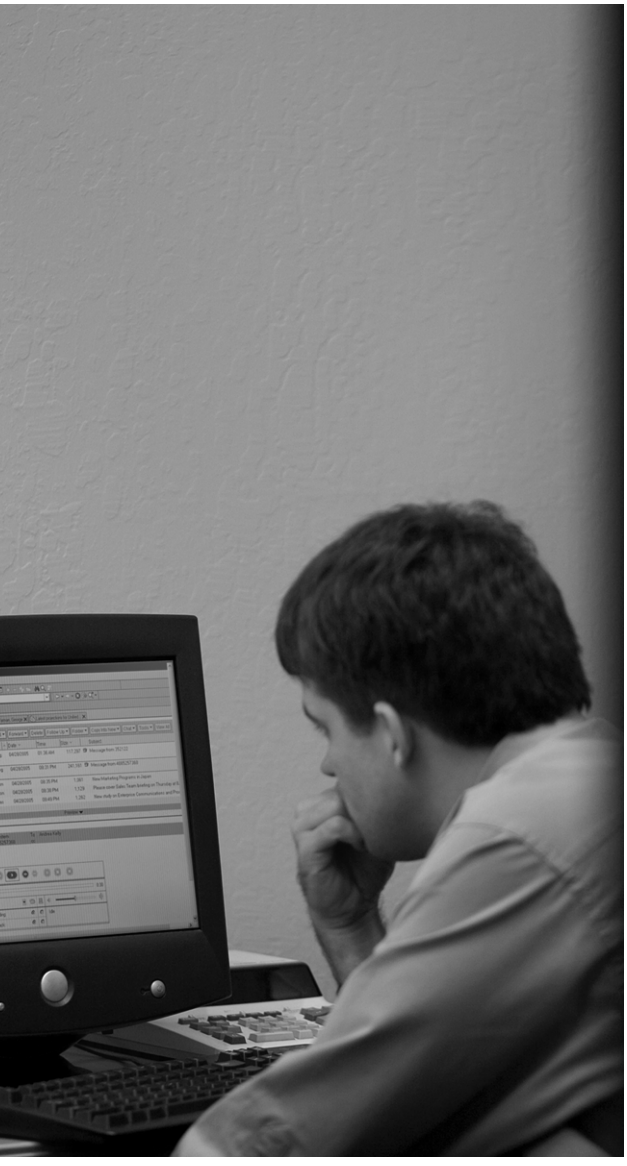
- **Part V: Appendix**

  - **Appendix A, "Sample Request for Information (RFI) Questions"**—This appendix provides a sample RFI to help the reader understand some of the issues that need to be considered when defining your IPS deployment requirements.

- **Glossary**—The glossary provides the definitions for various terms related to Intrusion Prevention along with definitions of other terms related to the book that the reader might need to understand.

This page intentionally left blank

Part I: Intrusion Prevention Overview



CHAPTER 1

Intrusion Prevention Overview

Computer and network security products evolve. Like living things, they change, grow, and adapt to reflect the conditions around them. Specifically, new threats to security force conditions in which security products adapt by implementing countermeasures that can handle the new threats. Examining the birth of a product and its evolution helps you understand why the product exists, what it can do, and how it might change in the future.

Intrusion Prevention Systems (IPS) are security protection devices or applications that can prevent attacks against your network devices. These systems began life as an adjunct feature of contemporary products, such as firewalls and antivirus products, and evolved into an independent and full-featured set of products in their own right. You find two types of IPSs: Network and Host. This chapter examines the factors that led to the existence of IPSs. It describes the evolution of computer security threats, the evolution of attack mitigation, and some of the IPSs' capabilities.

Evolution of Computer Security Threats

Security threats have always been around. Anything of value makes a viable target for a thief. Traditionally, theft required physical access to the object being stolen, limiting the number of attackers and increasing the chances of the perpetrator's being caught. This model applied to initial personal computer systems in which the computer was treated like another piece of expensive electronic equipment worth stealing.

Initially, mainframes and minicomputers allowed access to a limited number of directly connected dumb terminals. Gradually, the need for extended connectivity became more important. This need for connectivity led to dialup access to mainframes and minicomputers. Adding dialup connectivity increased the scope of attackers by enabling anyone across the world (with access to a telephone and a computer with a modem) to attempt to access the systems. This access, however, was still fairly limited in that attackers had to determine the phone number to use to connect to the computer system and pay the long distance charges if they were not in the same physical vicinity as the system being accessed. Furthermore, because mainframes and minicomputers were very expensive, attackers had difficulty gaining access to a system to try to find security vulnerabilities (except on the limited number of operational systems).

The development of the Internet has created an environment in which millions of computers across the world are all connected to each other. Furthermore, access to this network is fairly ubiquitous and cheap, enabling any thieves in the world to target your computer, regardless of their physical location. Personal computers are now also cheap. Attackers can easily (and cost effectively) set up various computers with different operating systems and search for exploitable vulnerabilities. Searching for vulnerabilities on systems that they control enables attackers to refine their exploit code before using it on actual systems. After they find a new vulnerability and develop an exploit, they can attack similar systems across the world. Therefore, the way you protect your computer assets has to change to match this new threat landscape. In addition, the international and distributed nature of the Internet makes it very difficult to regulate and control attacks against computer systems.

To protect access to internal networks, most companies deploy a firewall at their network perimeter to limit external access. The development of wireless network access (another technological enhancement) has enabled attackers to bypass these perimeter protection mechanisms. With wireless access, users do not need to be physically connected to gain access to the network. The problem is that wireless connectivity does not stop at the walls of your building. In many deployments, attackers can sit in the parking lot in front of your business and potentially gain access to your wireless network. Without proper protection, this wireless access gives attackers direct connectivity to your internal network.

FIREWALL

A *firewall* is a software or hardware application that limits network access to a private network from external networks. By limiting access, a firewall protects computer resources on the private (or internal) network. Firewalls can control which external systems can access which private systems, as well as limit the systems and applications to which private systems are allowed to connect.

The threats computer security professionals faced two-and-a-half decades ago are comparatively rudimentary and trivial by today's standards. They had no need for IPSs at that time. Unfortunately, threats have matured rapidly since then and are now sophisticated enough to warrant an advanced countermeasure like an IPS.

Many factors impact the security threats to which a computer system is vulnerable. Naturally, some threats are more severe than others, so when trying to understand why an IPS is necessary in today's networks, you need to consider the following factors:

- Technology adoption
- Target value
- Attack characteristics

Technology Adoption

It is sometimes easy to forget that, at 75 years of age, the digital computer industry as a whole is fairly young. You still find plenty of room for innovation, and new innovations in computing occur regularly. Inventions such as the personal computer and the Internet force businesses to change the way they operate.

The operational change might take some time because businesses don't usually adopt new technologies quickly. New technology comes with a set of risks, such as poor return on investment, security concerns, training costs, and so on. However, most technologies reach a point at which the rewards for adoption outweigh the risks. At that point, the technology is widely adopted, and the potential security risks become a reality. Even when these technologies are adopted, however, the objective many times is to simply get the technology working, with security being left as a future add on.

Four widely adopted technologies stand out as having had a tremendous impact on the evolution of security threats and thus the evolution of IPSs:

- Client-server computing
- The Internet
- Wireless connectivity
- Mobile computing

Client-Server Computing

Before the client-server architecture became commonplace in the 1990s, most businesses relied solely on mainframes for their computing needs. Users gained access to the mainframe using dumb terminals that were physically connected to the mainframe (but not each other), had a computer screen and a keyboard, but had almost no processing capability. All processing occurred on the mainframe.

MAINFRAMES

Mainframes are large and powerful computers that support thousands of simultaneous users. Early mainframes operated in timesharing mode, where all users shared processor time, or batch mode, where user programs were sequentially executed on the computer.

Client-server is a computing architecture that has largely replaced mainframes because of its lower cost of ownership. In client-server processing, power is not centralized. Instead, it is distributed across many networked computers, each acting as either a client or server. Clients are expected to provide a great deal of processing power so that the servers can be free to handle intensive computational operations.

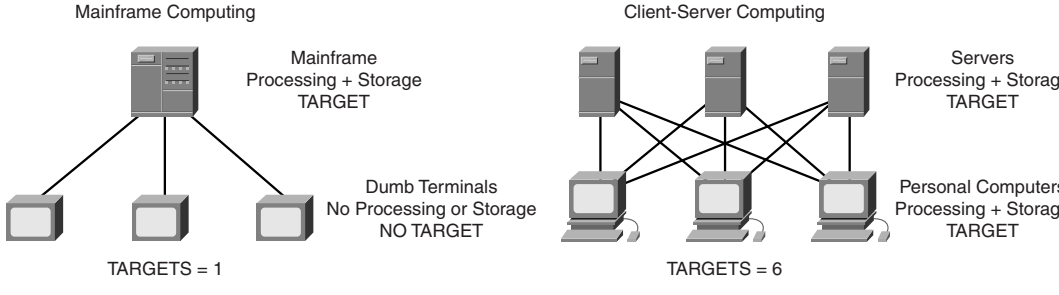
CLIENT-SERVER ARCHITECTURE

Servers are passive because they wait for a request from a client, fulfill the request, and send it back. Clients actively send requests and wait for a reply from the server. In either case, both computers must be networked together and have processing capability.

Attacks against dumb terminals were limited because the attacker needed physical access to the system. One common attack against these systems was for one user to use the dumb terminal and then run a program that mimicked the normal login program in an attempt to steal login credentials from other users who tried to use the dumb terminal. A terminal, however, that cannot store data and has no processor is usually not an attractive target. Furthermore, dumb terminals cannot be used as a client or a server because they have no processing capability and are not connected together.

Dumb terminals were replaced by personal computers or workstations that could meet the requirements of the client-server architecture. This resulted in a dramatic increase in the number of target hosts and networks available to an attacker. Figure 1-1 illustrates this increase. Large businesses can have hundreds of thousands of networked computers, all of which are potential targets for an attack.

Figure 1-1 *Mainframe Versus Client-Server*



A client-server architecture not only has more targets for an attacker, but it is also all networked together. If an attacker is able to compromise one computer, any computer connected to the compromised system is now a secondary target. Peer-to-peer networking contributed greatly to this problem by increasing the number of potential pathways between the systems. Furthermore, because the networked computers have high-speed connections and fast processors, they are very valuable and powerful targets.