NETWORK SECURITY

INTRODUCTION

- Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more and more people become ``wired'', an increasing number of people need to understand the basics of security in a networked world.

WHAT IS NETWORK SECURITY?

- Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.
- Network security involves the authorization of access to data in a network, which is controlled by the network administrator.
- Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals.

WHY DO WE NEED SECURITY?

- Protect vital information while still allowing access to those who need it
  - Trade secrets, medical records, etc.
- Provide authentication and access control for resources
  - Ex: AFS
- Guarantee availability of resources
  - Ex: 5 9's (99.999% reliability)

SECURITY OBJECTIVES

- IDENTIFICATION
- AUTHENTICATION
- ACCESS CONTROL

IDENTIFICATION

- Something which uniquely identifies a user and is called UserID.
- Sometimes users can select their ID as long as it is given too another user.
- UserID can be one or combination of the following:
  - User Name
  - User Student Number
  - User SSN

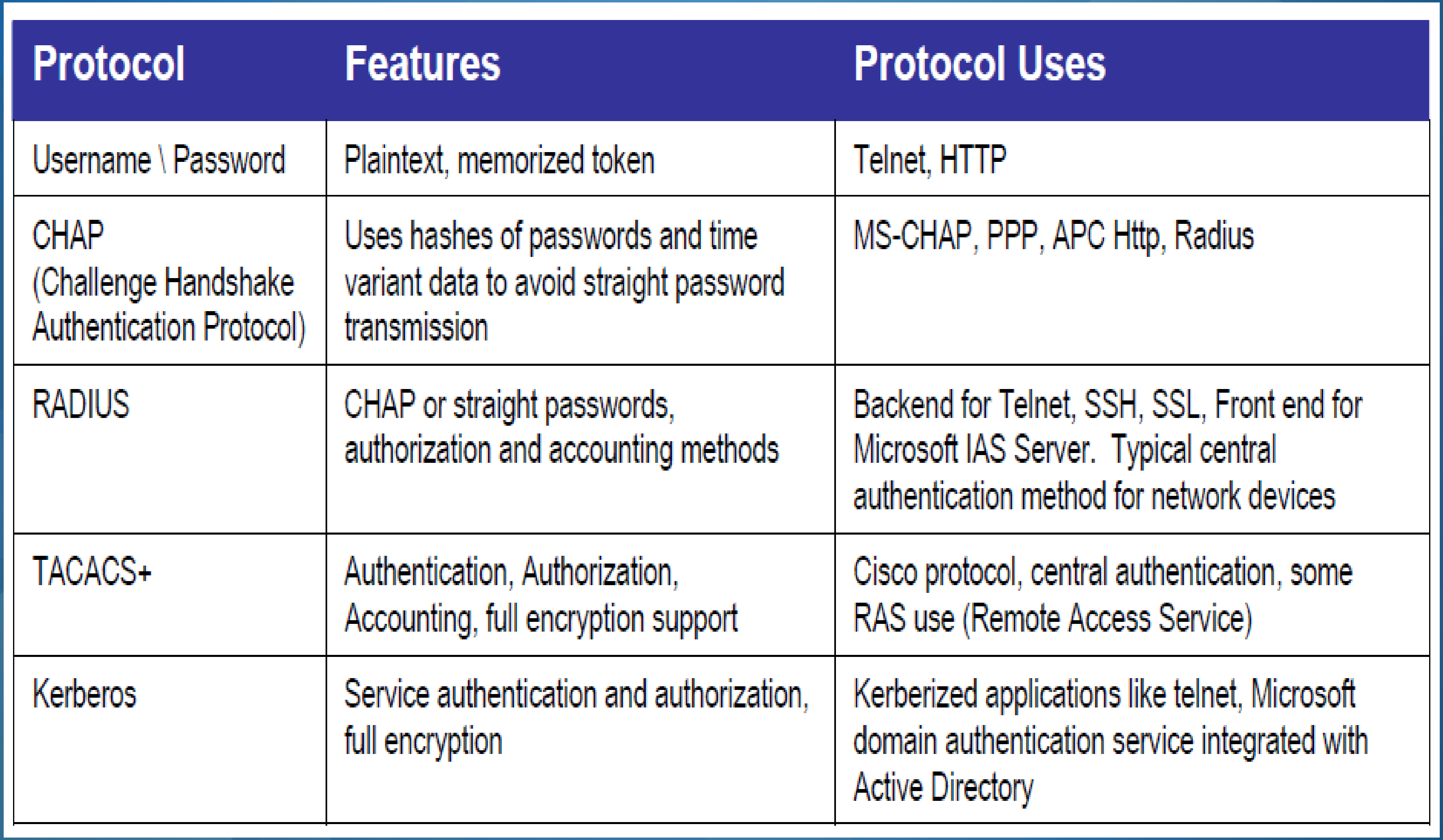
AUTHENTICATION

- The process of verifying the identity of a user
- Typically based on
  - Something user knows
    - Password
  - Something user have
    - Key, smart card, disk, or other device
  - Something user is
    - fingerprint, voice, or retinal scans

AUTHENTICATION: 2 SUB CONCERNS

- GENERAL ACCESS AUTHENTICATION
  - To control whether or not a particular user has ANY type of access right to the element in question. Usually we consider these in the form of a “User Account”.
- FUNCTIONAL AUTHORIZATION
  - Concern with individual user “rights”. What, for example, can a user do once authenticated? Can they figure the device or only see data.

AUTHENTICATION: MAJOR PROTOCOLS

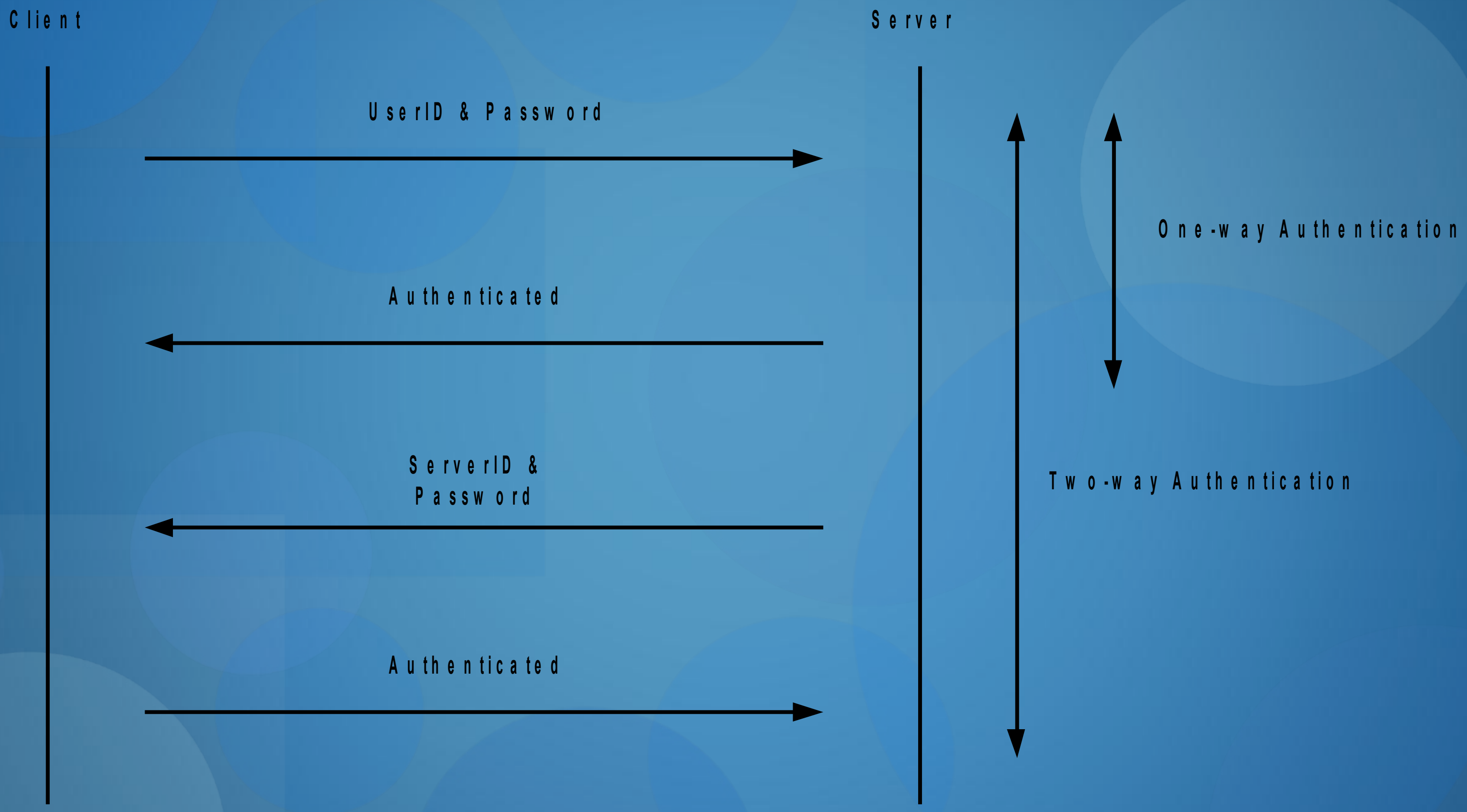


Protocol	Features	Protocol Uses
Username \ Password	Plaintext, memorized token	Telnet, HTTP
CHAP (Challenge Handshake Authentication Protocol)	Uses hashes of passwords and time variant data to avoid straight password transmission	MS-CHAP, PPP, APC Http, Radius
RADIUS	CHAP or straight passwords, authorization and accounting methods	Backend for Telnet, SSH, SSL, Front end for Microsoft IAS Server. Typical central authentication method for network devices
TACACS+	Authentication, Authorization, Accounting, full encryption support	Cisco protocol, central authentication, some RAS use (Remote Access Service)
Kerberos	Service authentication and authorization, full encryption	Kerberized applications like telnet, Microsoft domain authentication service integrated with Active Directory

AUTHENTICATION: PROCEDURE

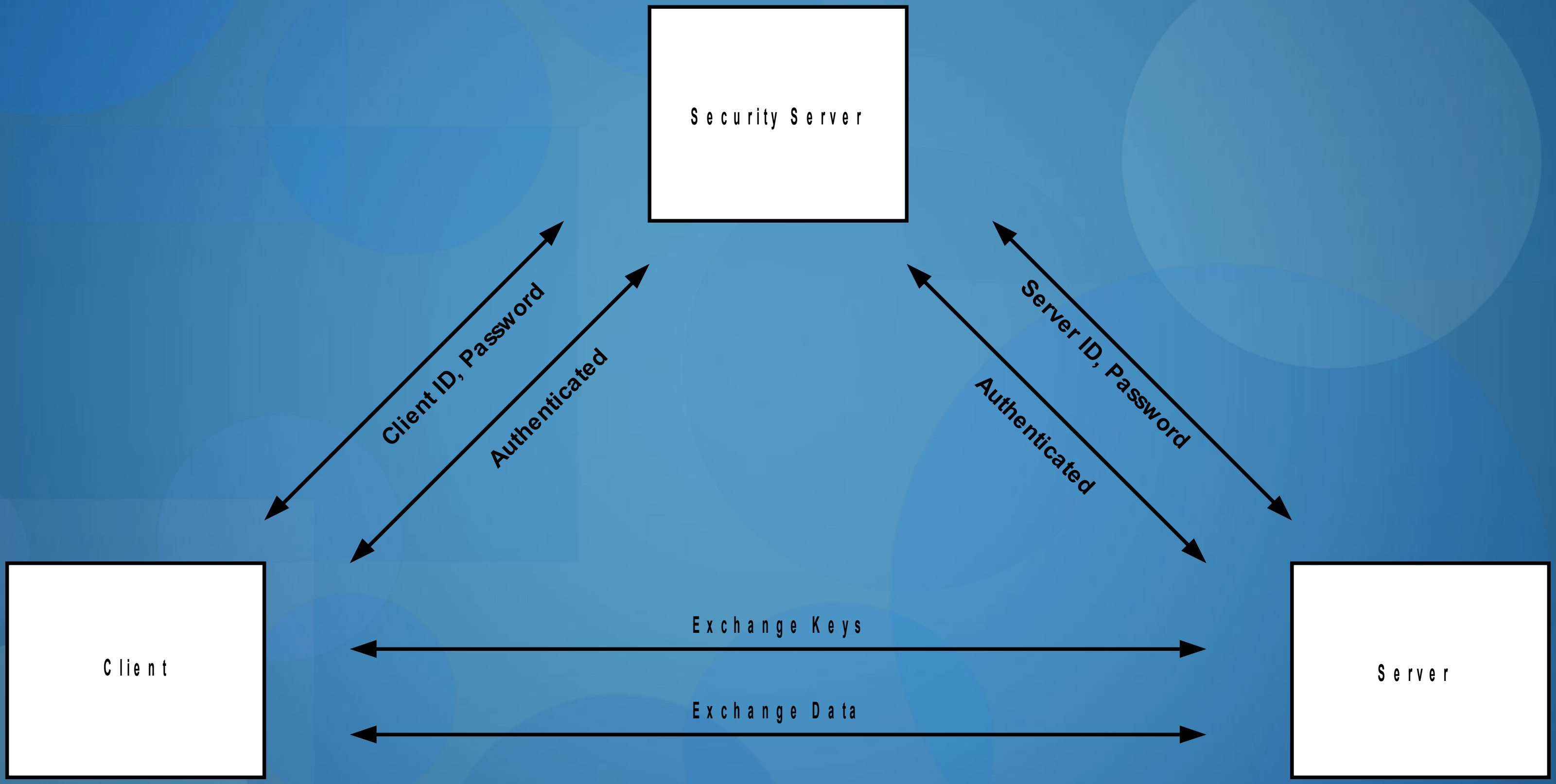
- Authentication procedure
  - Two-Party Authentication
    - One-Way Authentication
    - Two-Way Authentication
  - Third-Party Authentication
    - Kerberos
    - X.509
  - Single Sign ON
    - User can access several network resources by logging on once to a security system.

AUTHENTICATION: PROCEDURE



Two-Party Authentications

AUTHENTICATION: PROCEDURE



Third-Party Authentications

ACCESS CONTROL

- refers to security features that control who can access resources in the operating system. Applications call access control functions to set who can access specific resources or control access to resources provided by the application.

ENCRYPTION

ENCRYPTION

- In cryptography, encryption is the process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.
- The reverse process, i.e., to make the encrypted information readable again, is referred to as **DECRYPTION.**

ENCRYPTION: USES

- Encryption can be used to protect data "at rest", such as files on computers and storage devices (e.g. USB flash drives).
  - **Digital rights management systems** which prevent unauthorized use or reproduction of copyrighted material and protect software against reverse engineering
- Encryption is also used to protect data in transit
- Encryption, by itself, can protect the confidentiality of messages.

ENCRYPTION: APPLICATIONS

- Disk encryption software (also known as OTFE software)
- File/folder encryption
- Database encryption
- Communication encryption software

ENCRYPTION: APPLICATIONS

- NETWORK TRAFFIC ENCRYPTION TOOLS
  - Generic
  - IPSec based

WIRELESS SECURITY

WIRELESS SECURITY: INTRODUCTION

- Very convenient to have wireless connections
- Nightmare for security – the range for 802.11 is often a few hundred meters, so that one can spy on a company by leaving a laptop on in the parking lot
- Many problems arise from the vendors trying to make their products as friendly as possible – when you plug the device it starts working right away, usually with no security by default.
- Several ways wireless nets handle security
  - 802.11i
  - Bluetooth
  - WAP 2.0

WIRELESS SECURITY: 802.11 SECURITY

- IEEE 802.11i specifies security standards for IEEE 802.11 LANs
  - Interoperable implementations called Wi-Fi Protected Areas (WPA)
- **Wireless Application Protocol (WAP)** – standard to provide wireless phones and other wireless devices access to telephony and information services, including the internet.
- WAP security primarily provided by **Wireless Transport Layer Security (WTLS)** – provides security between the mobile device and the WAP gateway to the Internet

WIRELESS SECURITY: 802.11 SECURITY

- 802.11 standard prescribed a data link-level security protocol called WEP (Wired Equivalent Privacy) designed to make the security of a wireless LAN as good as that of a wired LAN.
  - WEP has been broken already in July 2001
- Solution
  - Replace WEP with WPA (Wi-fi Protected Access) or WPA2
  - Final proposal in 802.11i: Robust Security Network (RSN)
    - The Wi-Fi Alliance certifies vendors in compliance with the full 802.11i specification under the WPA2 program.

WIRELESS SECURITY: BLUETOOTH

- Considerably shorter range than 802.11 – cannot be attacked from the parking lot but feasible to attack it from next office.
  - An attacker next door can read the signals from one's keyboard or the data sent to the Bluetooth printer in the next office.
- Bluetooth has 3 security modes ranging from nothing to full data encryption and integrity control – many users have security turned off.
  - Two devices must share a secret key – perhaps the user types a PIN in both

WIRELESS SECURITY: BLUETOOTH

- They negotiate the channel to be used and establish a 128-bit session key (some bits made public due to government restrictions)
- Encryption uses a stream cipher called E0, integrity control uses SAFER+, both classical block-ciphers

WIRELESS SECURITY: WAP 2.0

- Introduced for handheld-devices connectivity (mobile phones)
- Uses standard protocols in all layers
- It is IP-based and it supports IPsec in the network layer
- TCP connections protected by TLS in the transport layer
- Uses HTTP client authentication
- Probably better than 802.11 and Bluetooth because it only relies on well-known security standards.

SECURITY PROCESSES

HOW TO SECURE DATA IN THE NETWORK?

SECURITY PROCESSES: INTRODUCTION

- Some data is also confidential; not only do you want to lose it, you don't want others to even view it without authorisation.
- Let's look at some ways to protect your all-important user data from loss and/or unauthorised access.
- http://www.zdnet.co.uk/news/networking/2006/04

SECURITY PROCESSES: 10 WAYS

E **Back up early or often-** you can use the backup utility built into Windows (ntbackup.exe) to perform basic backups. You can use Wizard Mode to simplify the process of creating and restoring backups.

i **Use file-level and share-level security-** to keep others out of data, the first step is to set permissions on data files and folders. If you have data in network shares, you can set share permissions to control which user accounts can and cannot access the files across the network. If you share the computer with someone else, you'll have to use file-level permissions (also called NTFS permissions, because they're available only for files/folders stored on NTFS-formatted partitions). File-level permissions are set using the Security tab on the properties sheet and are much more granular than share-level permissions.

SECURITY PROCESSES: 10WAYS

- **Password-Protect Documents**- Many productivity applications, such as Microsoft Office applications and Adobe Acrobat, will allow you to set passwords on individual documents. To open the document, you must enter the password. To password-protect a document in Microsoft Word 2003, go to Tools | Options and click the Security tab. You can require a password to open the file and/or to make changes to it. You can also set the type of encryption to be used. You can also use zipping software such as WinZip or PKZip to compress and encrypt documents.

  Use EFS Encryption- Windows 2000, XP Pro, and Server 2003 support the Encrypting File System (EFS). You can use this built-in certificate-based encryption method to protect individual files and folders stored on NTFS-formatted partitions. Encrypting a file or folder is as easy as selecting a check box; just click the Advanced button on the General tab of its properties sheet. Note that you can't use EFS encryption and NTFS compression at the same time.

SECURITY PROCESSES: 10 WAYS

e **Use Disk Encryption-** Disk encryption products can be used to encrypt removable USB drives, flash drives, etc. Some allow creation of a master password along with secondary passwords with lower rights you can give to other users. Examples include PGP Whole Disk Encryption and DriveCrypt, among many others.

r **Make use of a public key infrastructure-** A public key infrastructure is a system for managing public/private key pairs and digital certificates. Because keys and certificates are issued by a trusted third party (a certification authority, either an internal one installed on a certificate server on your network or a public one, such as Verisign), certificate-based security is stronger.

d **Protect data in transit with IP Security-** Your data can be captured while it's travelling over the network by a hacker with sniffer software (also called network monitoring or protocol analysis software). To protect your data when it's in transit, you can use IPsec — but both the sending and receiving systems have to support it.

SECURITY PROCESSES: 10 WAYS

- **Secure Wireless Transmissions-** Data that you send over a wireless network is even more subject to interception than that sent over an Ethernet network. Hackers don't need physical access to the network or its devices; anyone with a wireless-enabled portable computer and a high gain antenna can capture data and/or get into the network and access data stored there if the wireless access point isn't configured securely.

  You should send or store data only on wireless networks that use encryption, preferably WPA, which is stronger than WEP.

- **Use Rights Management to retain Control-** If you need to send data to others but are worried about protecting it once it leaves your own system, you can use Windows Rights Management Services (RMS) to control what the recipients are able to do with it.

ETHICAL HACKING

ETHICAL HACKING

- **HACKER-** A person who enjoys learning the details of computer systems and how to stretch their capabilities—as opposed to most users of computers, who prefer to learn only the minimum amount necessary.

  - One who programs enthusiastically or who enjoys programming rather than just theorizing about programming.

ETHICAL HACKING: Definition

- also called *Penetration testing* or *white-hat hacking*
- Evaluate the target systems' security and report back to the owners with the vulnerabilities they found and instructions for how to remedy them.
- This method has been in use from the early days of computers.

ETHICAL HACKING: Goals

- Hack your systems in a non destructive fashion
- Enumerate vulnerabilities and if, necessary, prove to upper management that vulnerabilities exists.
- Apply results to remove vulnerabilities & better secure your systems.

ETHICAL HACKING: History

- The United States Air Force conducted a "security evaluation" of the Multics operating systems for "potential use as a two-level (secret/top secret) system."
- With the growth of computer networking, and of the Internet in particular, computer and network vulnerability studies began to appear outside of the military establishment
    - One of these was the work by Farmer and Venema, which was originally posted to Usenet in December of 1993.
    - Idea: assess the security of the system
    - Security Analysis Tool for Auditing Networks (SATAN)- program created by Farmer and Venema for auditing capability

ETHICAL HACKING: Network-infrastructure Attacks

- Connecting into a network through a rogue modem attached to a computer behind a firewall
- Exploiting weaknesses in network transport mechanisms, such as TCP/IP and NetBIOS.
- Flooding a network with too many requests, creating a denial of service (DoS) for legitimate requests
- Installing a network analyzer on a network and capturing every packet that travels across it, revealing confidential information in clear text
- Piggybacking onto a network through an insecure 802.11b wireless configuration.

ETHICAL HACKING: What do ethical hackers do?

1. **FORMULATE A PLAN**

- 3 basic questions:
  - What can an intruder see on the target systems?
  - What can an intruder do with that information?
  - Does anyone at the target notice the intruder's attempts or successes?
- The "get out of jail free card"
  - A contractual agreement between the client and the ethical hackers, who typically write it together.
  - Protects the ethical hackers against prosecution
  - Provides a precise description, usually in the form of network addresses or modern telephone numbers, of the systems to be evaluated.

ETHICAL HACKING: What do ethical hackers do?

- "no-holds-barred" approach
  - The agreement must describe how they should be tested once the target systems are identified.
- Testing may begin as define in the agreement
  - Remote network- simulates the intruder launching an attack across the internet
  - Remote dial-up network- simulates the intruder launching an attack against the client's modem pools
  - Local network- simulates an employee or other authorized person who has legal connection to the organization's network

ETHICAL HACKING: What do ethical hackers do?

- Stolen Laptop computer- the laptop computer of a key employee, such as an upper-level manager or strategist, is taken by the client without warning and given to the ethical hackers
- Social Engineering- evaluates the target organization’s staff as to whether it would leak information to someone
- Physical Entry- acts out a physical penetration of the organization’s building.

The final report- collection of all of the ethical hacker’s discoveries made during the evaluation

ETHICAL HACKING: What do ethical hackers do?

1. **SELECTING TOOLS**

As with any project, if you don't have the right tools for ethical hacking, accomplishing the task effectively is difficult. Having said that, just because you see the right tools doesn't mean that you will discover all vulnerabilities

Many tools focus on specific tests, but no one tool can test for everything.

- to crack passwords, you need a cracking tool such as LC4, John the Ripper, or pwdump.
  - A general port scanner, such as Superscan, may not crack passwords

ETHICAL HACKING: What do ethical hackers do?

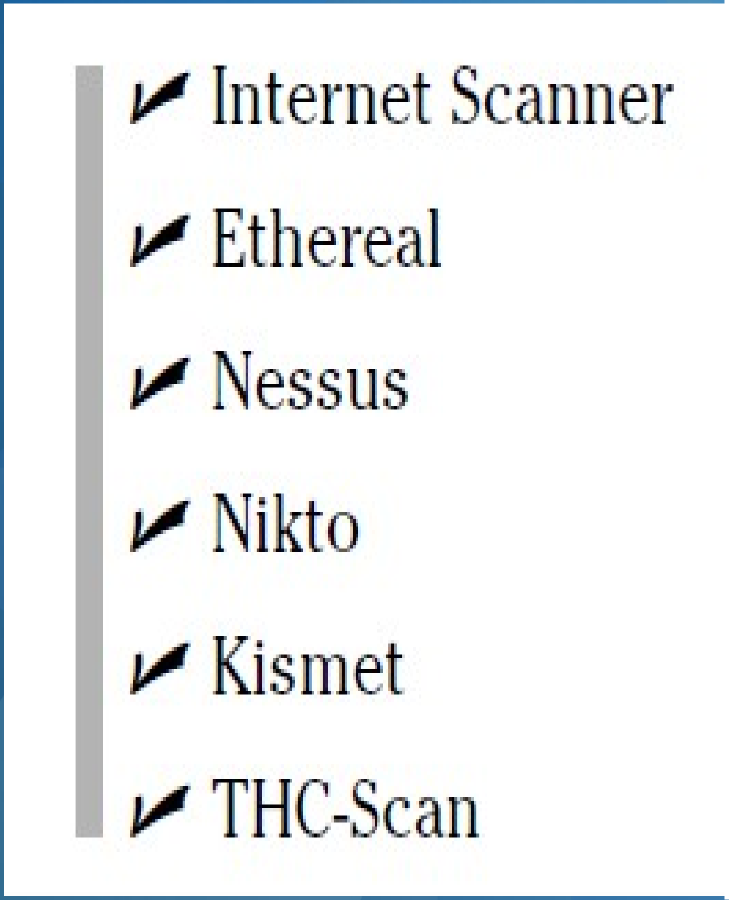
1. **SELECTING TOOLS**

As with any project, if you don't have the right tools for ethical hacking, accomplishing the task effectively is difficult. Having said that, just because you see the right tools doesn't mean that you will discover all vulnerabilities

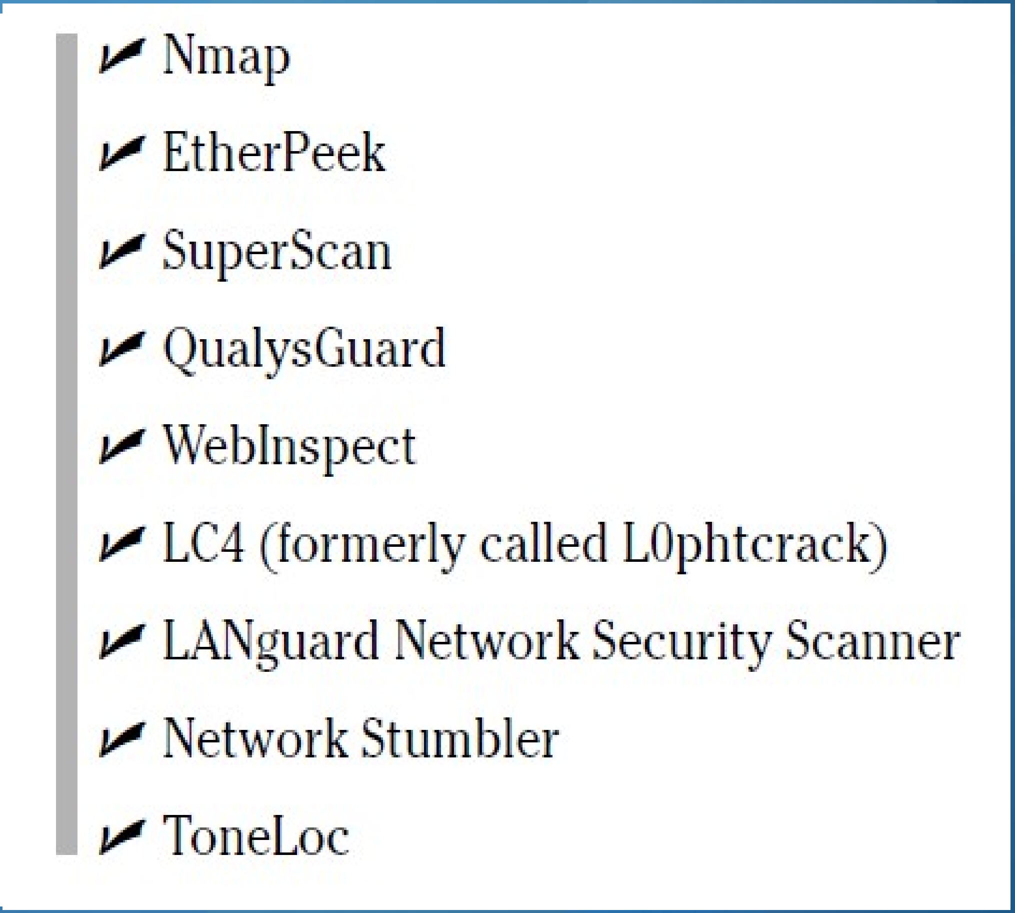
Many tools focus on specific tests, but no one tool can test for everything.

- to crack passwords, you need a cracking tool such as LC4, John the Ripper, or pwdump.
  - A general port scanner, such as Superscan, may not crack passwords

ETHICAL HACKING: What do ethical hackers do?



- ✓ Internet Scanner
- ✓ Ethereal
- ✓ Nessus
- ✓ Nikto
- ✓ Kismet
- ✓ THC-Scan



- ✓ Nmap
- ✓ EtherPeek
- ✓ SuperScan
- ✓ QualysGuard
- ✓ WebInspect
- ✓ LC4 (formerly called L0phtcrack)
- ✓ LANguard Network Security Scanner
- ✓ Network Stumbler
- ✓ ToneLoc

ETHICAL HACKING: What do ethical hackers do?

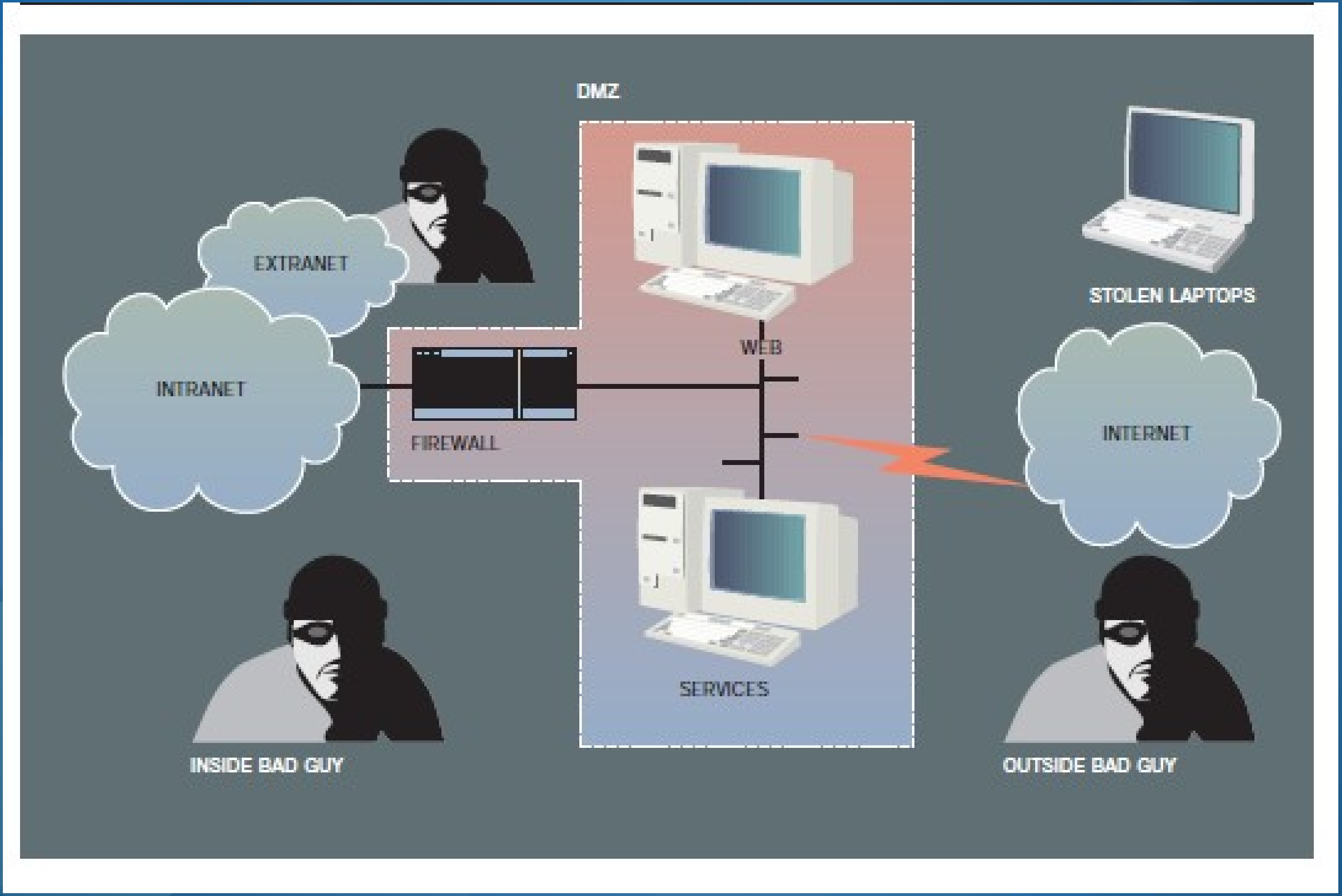
1. **EXECUTING THE PLAN**

- Ethical Hacking can take persistence. Time and patience are important. Be careful when you're performing your ethical hacking tests.
- Make sure you keep everything as quiet and private as possible. This is especially critical hen transmitting and soring your test results. If possible, encrypt these emails and files using Pretty Good Privacy (PGP) or something similar. At minimum, password-protect them.

ETHICAL HACKING: What do ethical hackers do?

1. **Evaluating Results**
   - Assess your results to see what you uncovered, assuming that the vulnerabilities haven’t been made obvious before now. Submit a formal report to upper management or to your customer, outlining your results.
3. **Moving On**
   - When you’ve finished your ethical hacking tests, you still need to implement your analysis and recommendations to make sure your systems are secure.

ETHICAL HACKING: What do ethical hackers do?



PRESENTED BY:

ABARE, DONNA

AMON, GICHELLE

MARTES, ELVIN JAN