Advanced Network Security

Introduction

Dr. Yaeghoobi

PhD. Computer Science & Engineering, Networking, India

dr.yaeghoobi@gmail.com

00 Lesson Plan

01 Introduction

02 Network Security

03 Objectives

04 Security Risk

Lesson Plan

00

Course Goals

- Introduction to Network Security
- Threats and Attaks
- Firewalls
- IDS
- DoS
- Worms
- Botnets
- Honey-pots
- Spyware
- Phishing
- Routing Security
- Network Forensics
- Wireless Sensor Network Security
- VoIP

References

- Micro-Firewalls for Dynamic Network Security Framework, by Omid Mahdi Ebadati E., Harleen Kaur, M. Afshar Alam, Kaebeh Yaeghoobi, 2012
- CompTIA Security+ Guide to Network Security Fundamentals – Standalone, by Mark Ciampa, 2017
- Computer & Internet Security: A Hands-on Approach, by Wenliang Du, 2019

- Network Security Software:
  - OPNET
  - NS
  - AVG Internet Security Business Edition
  - EventTracker

Evaluation

1st Midterm Exam	5	5
2nd Midterm Exam	5	
Project + Assignments	5	
Final Exam	10	
Total	20	

Introduction

01

Introduction

- Networks are telecommunication highways over which information travels
- Networks and their associated information technology resources are exposed to potential points of attack (e.g. spoofing, traffic flow analysis, trap doors, Trojan horses, viruses, worms, etc.)
  - شبکه‌ها و منابع فناوری اطلاعات مرتبط با آنها در معرض حمله قرار می‌گیرند

(به عنوان مثال کلاهبرداری، تجزیه و تحلیل جریان ترافیک، درب‌های تله، تروجان، ویروس‌ها، کرم‌ها و غیره)

Introduction …

- Centralized network management authority does not exist so layered security measures are needed to protect data as it traverses the network
- These layered security measures include
  - Firewalls
  - Routers
  - Intrusion Detection Systems
  - Other components (VPNs, encryption, etc.)

Objectives for Connectivity

- Before the mid-1990s, there was little connectivity between computer systems.
  - Networks were primarily used to connect terminals to a mainframe, or to connect workstations to shared resources (e.g., for file sharing, printing, etc.) within an organization’s internal network
  - If an organization’s networks were connected to someone else, usually only a few key business partners were connected, and that was through private lines
- The Internet and the coming of “open” connectivity through TCP/IP changed this .

Objectives for Connectivity …

- **Efficiency –** Only key data is sent across the entire supply chain کارايي - فقط داده‌های کلیدی در کل زنجیره تأمین ارسال شود
- **Speed –** Transactions need to be processed “real time” سرعت - معاملات باید در "زمان واقعی" پردازش شوند
- **Ease –** Customers demand a “universal” solution that will interface with multiple technologies سهولت - مشتریان خواستار یک راه حل "جهانی" هستند که با چندین فناوری ارتباط برقرار کند
- **Information sharing –** Information leads to competitive edge اشتراک اطلاعات - اطلاعات منجر به رقابت می شود

Network Security

02

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.
- امنیت شبکه شامل مقررات و خط مشی های اتخاذ شده توسط مدیر شبکه برای جلوگیری و نظارت بر دسترسی غیرمجاز، سوءاستفاده، اصلاح یا انکار شبکه و منابع قابل دسترسی به شبکه است.
- Network security involves the **authorization of access to data** in a network, which is controlled by the network administrator.
- امنیت شبکه شامل مجوز دسترسی به داده ها در یک شبکه است که توسط سرپرست شبکه کنترل می شود.

Network Security …

- 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.

- امنیت شبکه انواع شبکه‌ها را پوشش می‌دهد، اعم از دولتی و خصوصی، که در مشاغل روزمره، انجام معاملات و ارتباطات بین مشاغل، سازمان های دولتی و افراد مورد استفاده قرار می گیرد.

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
- Guarantee availability of resources

- از اطلاعات حیاتی محافظت کنید در حالی که هنوز امکان دسترسی برای کسانی که به آن احتیاج دارند وجود دارد
- اسرار تجاری ، سوابق پزشکی و غیره
- تأیید اعتبار و کنترل دسترسی برای منابع
- تضمین در دسترس بودن منابع

Objectives

03

Objectives of Network Security

- **Objective 1:** To **provide control** at all points along the network perimeter in order to block network traffic that is malicious, unauthorized, or that otherwise presents risk to the internal network
- **Objective 2:** To **detect and respond** to attempted and actual intrusions through the network
- **Objective 3:** To **prevent** network messages that are sent across networks from being intercepted or modified in flight

- هدف ١ : فراهم آوردن کنترل در تمام نقاط شبکه به منظور مسدود کردن ترافيك مخرب، شبکه غیرمجاز، یا اینکه خطري را براي شبکه داخلي ایجاد می‌کند.
- هدف ٢: شناسايي و پاسخ به حمله های تلاش شده و واقعی از طریق شبکه
- هدف ٣: برای جلوگیری از پیگیری یا تغییر پیام‌ها در سراسر شبکه ها

Objectives of Network Security …

- Network security controls cannot completely eliminate risk. The goal is to minimize risk as much as possible and to avoid unnecessary or excessive risk.
- The goal of network security is really to “enable” network connectivity. Without network security, the risks/costs of network connectivity would be prohibitive.

- کنترل های امنیتی شبکه نمیتوانند ریسک را به طور کامل از بین ببرند. هدف این است که در حد ممکن ریسک را به حداقل برسانید و از خطر غیرضروری یا بیش از حد جلوگیری کنید
- هدف از امنیت شبکه فعال کردن اتصال شبکه است. بدون امنیت شبکه، خطرات / هزینه های اتصال به شبکه گران خواهد بود

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

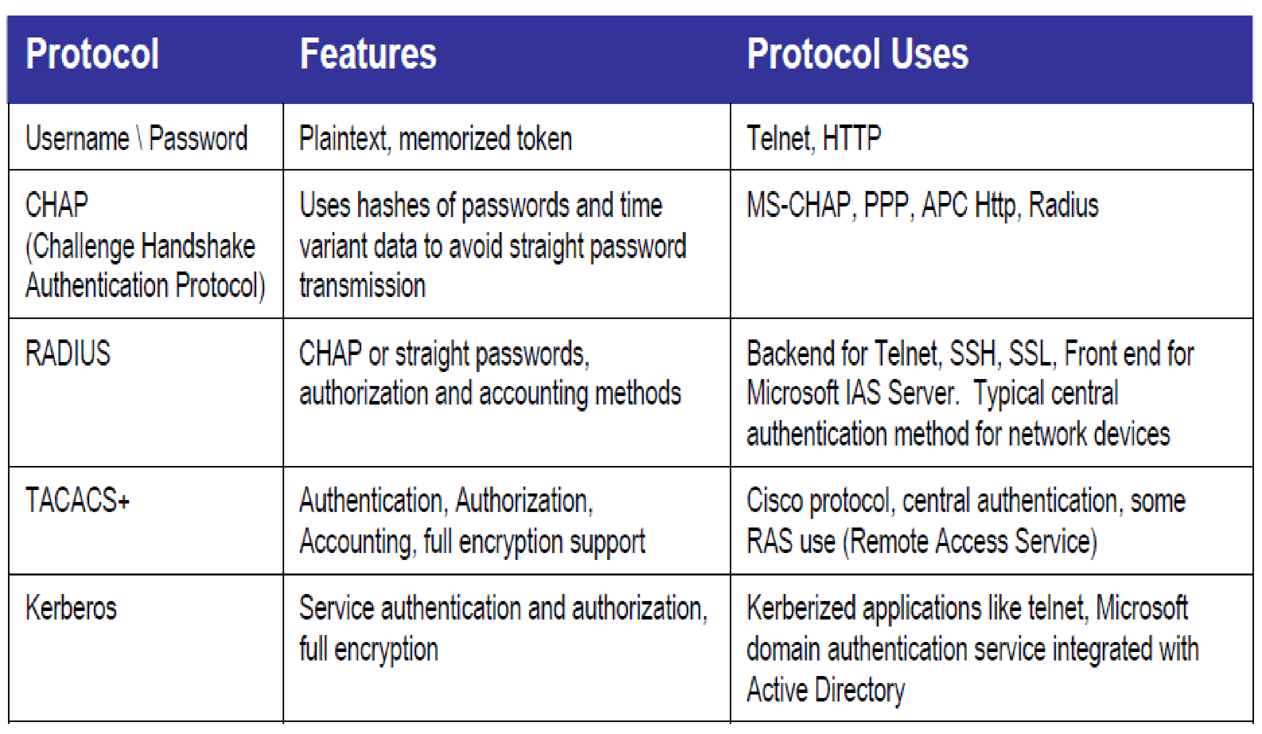
Authentication

- 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 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)

- 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.

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.

Security Risk

04

Internetworking Increases Security Risk

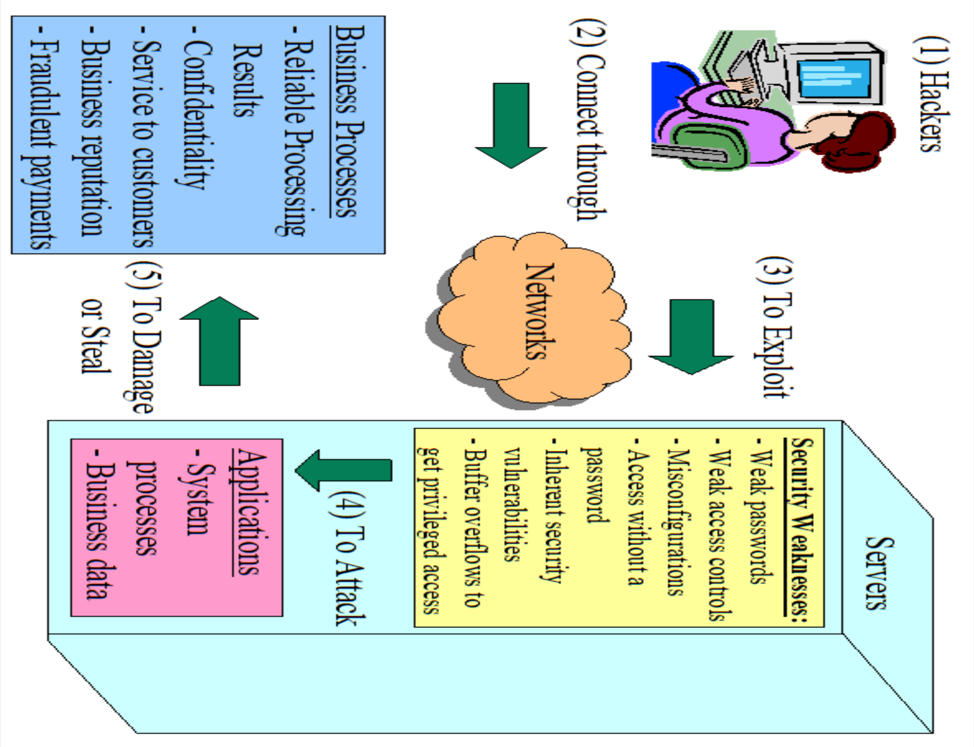
- Network connectivity dramatically changes the risk profile for systems security

- مشخصات اتصال شبکه، خطر را برای امنیت سیستم تغییر می دهد

Security Risk

- **Question:** Who can exploit security weaknesses (e.g., password weaknesses, backdoors, poor access controls, etc.) on internal systems?
- سوال: چه کسی می تواند در داخل سیستم از نقاط ضعف امنیتی (به عنوان مثال، ضعف رمز عبور، درب‌های پشتی، کنترل دسترسی ضعیف و غیره) سوءاستفاده کند؟
  - **Answer without connectivity:** Only people who can first access my bricks and mortar
  - **Answer with connectivity:** Anyone who is connected to my network and anyone who is connected to them and anyone who is connected to them and anyone who is connected to them, etc.

Network Security Risk



(1) Hackers

(2) Connect through

Networks

(3) To Exploit

Servers

Security Weaknesses:
- Weak passwords
- Weak access controls
- Misconfigurations
- Access without a password
- Inherent security vulnerabilities
- Buffer overflows to get privileged access

(4) To Attack

Applications
- System processes
- Business data

(5) To Damage or Steal

Business Processes
- Reliable Processing Results
- Confidentiality
- Service to customers
- Business reputation
- Fraudulent payments

Network Security Risk

- ***Denial of Service*** – Attacks on the **availability of networks** or **computer systems**
  - **Network packets** that violate protocol compliance or that are **malformed** can cause some systems to crash
  - Some network attacks **flood** a network with **more packets than the network can handle**
  - Other network attacks create **half-open connections** to utilize system **resources until none are left**

Network Security Risk …

- ***Information Theft*** – Attacks on **confidential information** (e.g., customer private information, credit card information, etc.)
  - Network services can be abused by **malicious users** to logon to (or otherwise access) **hosts and other devices** on the network
  - Confidential information may be easily accessible through network services due to **misconfigurations, poor access controls, etc.**
  - Confidential **information/messages are intercepted** while packets are being sent across publicly accessible network lines

Network Security Risk …

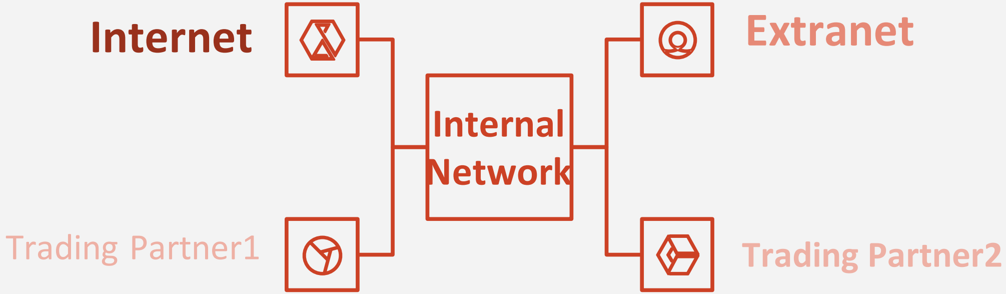
- ***Intrusion* – Unauthorized access** (usually with privileged access rights) to a network or computer system that could **compromise** the **integrity** and/or **availability** of critical systems and data
  - Some network services allow access to the host without any password required ➔ results in easy access
  - Some network services allow a user to sign-on across the network to access the host ➔ used for attacks on default or easily guessed passwords
  - Some network services use trusted access based on host IP addresses that can be spoofed ➔ used to obtain unauthorized access without a password
  - Some network services and malformed packets can be used for surveillance ➔ helps hackers focus their attacks
  - Some network services have buffer overflow vulnerabilities that provide attackers with privileged access ➔ game over

Network Security Risk …

- ***Reputation* –** Confidence of customers, business partners, etc. is lost.
- This is perhaps the biggest (but often unthought-of) risk that eBusinesses face

Internal Network Risks

- **Every connection to external networks** introduces risk.
- The internal network could be attacked from the **Internet (highly likely)**, from the **Extranet (moderately likely)**, or from a **Trading Partner (less likely)**



Internal Network Risks …

- An attacker from the Internet could also use our internal network connection as a launching point to initiate an attack against the Extranet or one of the Trading Partners
- The Trading Partners could attack each other through us
- If the Trading Partners are connected to the Internet, an attacker could use them as a launching point to attack us
- یک مهاجم از اینترنت می تواند از اتصال شبکه داخلی ما به عنوان نقطه شروع استفاده کند تا بتواند حمله‌ای را به Extranet یا یکی از شرکای تجاری انجام دهد.
- شرکا می توانند از طریق ما به یکدیگر حمله کنند.
- اگر شرکابه اینترنت متصل باشند، یک مهاجم می تواند از آنها به عنوان نقطه راه اندازی برای حمله به ما استفاده کند.

Causes of Network Security Risk

- The Computer Emergency Response Team Coordination Center (CERT/CC) believes that the answer is “chronic system administration problems” and inherent “flaws” in the protocols and network services due to poor design.
- The SANS Institute publishes “The Twenty Most Critical Internet Security Vulnerabilities”.

Most Critical Internet Security Vulnerabilities

- Default installations that run extraneous network services
- Accounts with no passwords or weak (default) passwords
- Unnecessary network service ports left open
- Packets with spoofed source addresses (packets from outside networks that masquerade as if they originated from the internal network)

- نصب های پیش فرض که سرویس های شبکه را اجرا می کنند
- حسابهای بدون رمز عبور یا گذرواژه‌های ضعیف (پیش فرض)
- پورت‌های سرویس غیر ضروری شبکه باز است
- بسته هایی با آدرس منبع خراب (بسته هایی از شبکه های خارجی که ظاهراً از شبکه داخلی منشا می شوند).

Most Critical Internet Security Vulnerabilities ...

- No logging or incomplete logging
- Programming flaws and buffer overflows that cause services to crash or execute arbitrary commands with privileged access
- Unprotected sharing of files and directories over the network
- Trust relationships that allow access without a password

- عدم ورود به سیستم یا ورود ناقص
- نقص برنامه نویسی و سرریز بافر که باعث خراب شدن سرویس‌ها یا اجرای دستورات دلخواه با دسترسی سطح بالا می شوند
- اشتراک گذاری محافظت نشده از پرونده‌ها و دایرکتوری‌ها از طریق شبکه
- به روابطی اعتماد کنید که امکان دسترسی بدون رمز عبور را دارند

Network security consists of the **technologies** and processes that are deployed to **protect internal networks from external threats**

Network security controls **cannot** completely eliminate risk. The goal is to **minimize risk** as much as possible and to **avoid** unnecessary or excessive risk

The primary goal of network security is to **provide controls** at all points along the network perimeter which allow access to the internal network and **only let traffic pass if that traffic is authorized, valid, and of acceptable risk**

Without network security, the **risks of connectivity would be too high**

Thanks for your Attention.