Applied Networks & Security

Introduction – with Critical Analysis

http://condor.depaul.edu/~jkrystof/it263/

John Kristoff
jtk@depaul.edu
Critical analysis disclaimer

Following this disclaimer are slides used in other versions of the course. We *mark up* some slides using strikethroughs and *underlined red in comic sans ms 20pt font*. This is not meant to slight other teachers or their material. Much of the material is good and helpful so we use it.

We do this to explore complex issues, refresh dated material, correct inaccuracies and stimulate critical thinking. In some cases we are pedantic where it seems useful, but we are not exhaustive and try to avoid being overly tedious when it is unnecessary.
IT 263
Applied Networks and Security
Introduction
Overview

- Course Goals and Overview
- Types of Networks
- Protocols and Packet Sniffing
- Typical SOHO Network Layouts
Course Topics

- Introduce networking and security technologies that everyone should know about, using small office home office (SOHO) networks as our main example
  - Networking Topics:
    - Network applications
    - Network connectivity (Ethernet cabling, switching, routers)
    - IP addressing, network address translation
    - Internet access services
  - Security Topics:
    - Typical threats and responses
    - Data Integrity and Encryption
    - Firewalls
    - Virtual private network (VPNs)
We will **not** study enterprise networking topics in this course, such as:

- Structured cabling systems (rack-based systems)
- Server operating systems and management
- User/resource Directory trees
- Network user administration
- Server arrays

These topics are covered in **TDC 363**
Network Types

- **Personal Area Networks (PANs)**
  - Interconnect personal devices (PDA, cell phone, portable game module, PC) within 30 feet or so.
  - Example: Bluetooth, docking cable

- **Local Area Networks (LANs)**
  - Interconnect devices within single business/building
  - Example: Ethernet - *often spans buildings/cities, PAN/LAN/MAN/WAN geographic delineation not always clear*
Network Types

- **Metropolitan Area Networks (MANs)**
  - Interconnect customer sites controlled by a single telecommunications carrier within a metropolitan geographic region.
  - Example: Hong Kong Broadband Network

- **Wide Area Networks (WANs)**
  - Interconnect customer sites around the world
  - Example: The Internet, Frame Relay
Network Interconnections
Network Applications

- What are networks used for?
  - Sharing resources
    - Printers, Disks, Folders
  - Communicating Information
    - 2-way: E-mail, Text Chat / Instant Messaging, Videoconferencing, Voice over IP.
    - 1-way: Web sites, IP-TV, music download
  - Distributed Applications
    - Collaborative work, Gaming
  - Internet Connectivity
SOHO LAN Applications

- Disk sharing

<table>
<thead>
<tr>
<th>Hard Disk Drives</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Disk (C:)</td>
<td>Local Disk</td>
</tr>
<tr>
<td>E STOR (E:)</td>
<td>Local Disk</td>
</tr>
<tr>
<td>DISK2PART02 (F:)</td>
<td>Local Disk</td>
</tr>
</tbody>
</table>
SOHO LAN Applications

- Folder Sharing
SOHO LAN Applications

- Printer Sharing

Samsung ML-1740 Series
Applications use Packets!

- All network services are provided via packet-based client-Server communications
  - Client machine sends a request packet to a server.
  - Server accepts request, processes it, and transmits back a response packet(s).
- Packets are strings of bytes and have size restrictions
  - For example, Ethernet packets frames can only be between 64 bytes and 1528 1518, in length, containing no more than 1500 bytes of user data.
Packet basics

- Clients and servers must follow a set of rules called a **protocol** which determines
  - Packet format
    - Permissible requests and responses
    - Format of header information and data
  - Packet ordering and timing
- **Protocol standards** are documents that define protocols.
  - For Internet applications, protocol standards are called **Request for Comments (RFCs)**.
Packet Flow

- To access a particular network application based on a particular protocol, the sequence of packets exchanged between a client and server form a packet flow for that application.

- In this course, we will study the following packet flows:
  - Establishing a TCP connection (3-way TCP handshake)
  - Retrieving files from a web server (HTTP)
  - Reading e-mail (IMAP)
  - Sending e-mail (SMTP)
Example: File Download Packet Flow

- Open File
- Read Data
- Close File

File Server → File Opened → Data (multiple pkts) → File Closed

Client

File Server
Protocols: a set of rules governing the format (syntax), meaning (semantics) and timing of the information that are exchanged between client and server.

Protocol Data Unit (PDU):

<table>
<thead>
<tr>
<th>Header</th>
<th>Data</th>
</tr>
</thead>
</table>

Prof: "John, where's your homework?"

Prof: "Class, the homework is due next week."
Protocol Layering

Layered Protocols:
- Client-Server communications processes are broken into simpler functions
- Each function implemented by its own hardware/software module
- Each module adds its own control information ("header") to the outgoing message
Windows Networking Model

Microsoft refers to these 3 protocol layers as:

- Services Layer
- Protocol Layer
- Hardware Layer
Example: HTTP Service
3-Layer Protocol Stack
Layering Example

WinXP PC running FireFox

User clicks “http://www.depaul.edu”

WinXP OS

FireFox Software (Client App)
TCP Software
IP Software
Ethernet Driver
Ethernet Card

WinXP PC running FireFox

Create GET Request in HTTP format

TCP Software
IP Software
Ethernet Driver

Receive and Process GET Request

Apache Software (Server App)
TCP Software
IP Software
Ethernet Driver

Ethernet Card

LINUX OS

Apache Software (Server App)
TCP Software
IP Software
Ethernet Driver
Ethernet Card
Packets inside Frames

- IP packet carried inside Ethernet frame
To view and understand data packets on the network, we will use a free packet analyzer tool called Ethereal.


What can Ethereal do?

- Captures a copy of every data packet going in and out of a computer (acts as a Sniffer).
- Displays the contents of each packet in an easy-to-read format.
Ethereal Example

- I access http://reed.cs.depaul.edu/lperkovic/it263/test while running Ethereal...
Ethereal Example

- This web page has the following underlying HTML source

```html
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
  <meta name="GENERATOR" content="Microsoft FrontPage 5.0">
  <meta name="ProgId" content="FrontPage.Editor.Document">
  <meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
  <meta http-equiv="Content-Language" content="en-us">
  <title>IT 263</title>
</head>
<body>
  <p align="center"><b><font size="5">IT 263 Course Test Page</font></b></p>
  <p align="center">Applied Networks and Security</p>
  <p align="left">This page will be used throughout the quarter for exercises and examples.</p>
  <p align="left">Course material is available at: <a href="http://reed.cs.depaul.edu/lperkovic/it263">http://reed.cs.depaul.edu/lperkovic/it263</a></p>
</body>
</html>
```
The Packet Flow

- Let’s look at the packet flow from Ethereal. Note: capture file is posted.
<table>
<thead>
<tr>
<th>No</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.000000</td>
<td>Cisco_55:b2:c6</td>
<td>Spanning-tree-(for STP)</td>
<td>Conf. Root = 8192/00:14:f1:ab:60:a9 Cost = 4 Port = 0x8012</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0.152086</td>
<td>Cisco_ab:60:00</td>
<td>CGMP</td>
<td>CCMP</td>
<td>Cisco Group Management Protocol</td>
</tr>
<tr>
<td>3</td>
<td>0.153174</td>
<td>140.192.34.248</td>
<td>224.0.0.1</td>
<td>IGMP</td>
<td>V2 Membership Query</td>
</tr>
<tr>
<td>5</td>
<td>2.657937</td>
<td>140.192.34.162</td>
<td>140.192.34.105</td>
<td>TCP</td>
<td>3294 &gt; http [SYN] Seq=0 Len=0 MSS=1460</td>
</tr>
<tr>
<td>6</td>
<td>2.658615</td>
<td>140.192.34.162</td>
<td>140.192.34.162</td>
<td>TCP</td>
<td>http &gt; 3294 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460</td>
</tr>
<tr>
<td>7</td>
<td>2.658642</td>
<td>140.192.34.162</td>
<td>140.192.34.105</td>
<td>TCP</td>
<td>3294 &gt; http [ACK] Seq=1 Ack=1 Win=17520 Len=0</td>
</tr>
<tr>
<td>8</td>
<td>2.658869</td>
<td>140.192.34.162</td>
<td>140.192.34.105</td>
<td>HTTP</td>
<td>GET /Iperkovic/it263/test/index.html HTTP/1.1</td>
</tr>
<tr>
<td>9</td>
<td>2.660964</td>
<td>140.192.34.162</td>
<td>140.192.34.162</td>
<td>TCP</td>
<td>http &gt; 3294 [ACK] Seq=1 Ack=724 Win=8676 Len=0</td>
</tr>
<tr>
<td>10</td>
<td>2.664563</td>
<td>140.192.34.162</td>
<td>140.192.34.105</td>
<td>TCP</td>
<td>http &gt; 3294 [ACK] Seq=724 Ack=1213 Win=16308 Len=0</td>
</tr>
<tr>
<td>11</td>
<td>2.882372</td>
<td>140.192.34.162</td>
<td>140.192.34.105</td>
<td>HTTP</td>
<td>HTTP/1.1 200 OK (text/html)</td>
</tr>
</tbody>
</table>

Frame 1 (60 bytes on wire, 60 bytes captured)
Why Learn Ethereal?

- It’s not just for network gurus! Ethereal is useful for ordinary PC users:
  - Find the cause of application errors
  - Check the health of your network
  - Figure out why “the network is slow”
  - Determine whether your PC is infected with a virus
Why Learn Ethereal?

- **Find the cause of application errors**
  - For example: JP was using Outlook Express to read his e-mail. He could read e-mail, but he couldn’t send any e-mail (got a “server not accessible” message).
    - Was it a problem in his PC?
    - Was it a problem in his network?
    - Was it a problem with his firewall?
    - Was it a problem with the Exchange server?
Why Learn Ethereal?

- Check the health of your network
  - When the network is slow or not working, running Ethereal can tell you:
    - Are packets getting through?
    - Is the network overloaded?
    - Are there error conditions that are creating lots of extraneous packets across the network?
Why Learn Ethereal?

.. Because you will use that tool extensively in your career:

- If you work in telecom/networking
- If you work in security
- If you work in computer forensics
Why Learn Ethereal?

**Determine whether your PC is infected:**

- If infected by a virus or bot, chances are: you PC is talking to something/someone.

- You really want to know ... especially if your PC is been running “slow” with lots of hard disk access....
SOHO Network Configurations

- Networks are composed of many devices, including:
  - workstations (computers and telephones)
  - servers
  - Ethernet hubs and switches
  - routers
  - firewalls
  - wireless access points (APs)
Home Network
Single PC
Home Network
Wired LAN

- CATV or DSL Line
- SOHO Router
- Hub
- PC
- Living Room
- Den
- Kitchen
- PC
- Dining Room
Home Network
Wireless LAN
Small Office Network
Wired LAN

- Client PC
- Ethernet Hub/Switch
- SOHO Router
- CATV or DSL Line
- Server
Small Office Network
Wired LAN - Logical Layout

- Client PC
- Client PC
- Client PC
- Server
- Ethernet Hub/Switch
- SOHO Router
- CATV or DSL Line
Small Office Network
Multiple Subnets

Subnet #1
- Client PC
- Client PC
- Client PC
- Server
- Ethernet Hub/Switch

Subnet #2
- Client PC
- Client PC
- Client PC
- Server
- Ethernet Hub/Switch

Router / Firewall
- Modem / CSU
- CATV or DSL or T-1 Line
Small Office Network
Public/Private Subnets

Subnet #1
- Client PC
- Client PC
- Client PC
- Server
- Ethernet Hub/Switch

Subnet #2
- Client PC
- Client PC
- Client PC
- Server
- Ethernet Hub/Switch

DMZ / Public Subnet
- Web Server
- E-mail Server

DMZ / Public Subnet
- Web Server
- E-mail Server

Router / Firewall
- Ethernet Hub/Switch

Modem / CSU
- CATV or DSL or T-1 Line

Router