

Applied Networks & Security

Applications

<http://condor.depaul.edu/~jkristof/it263/>

John Kristoff
jtk@depaul.edu

HTTP/HTTPS

- The language of the World Wide Web
- Text-based
- Actions defined using methods (e.g. GET, POST)
- Header identifies content
- HTTPS specifies crypto (usually TLS/SSL3)
- Commonly associated with transferring HTML/XML
- Some might call this the “new transport layer”, why?

SMTP/POP/IMAP

- Simple Mail Transfer Protocol (SMTP)
 - For sending mail, text based
- Post office protocol (POP)
 - For receiving mail, text based, primarily for disconnected use
- Internet Message Access Protocol (IMAP)
 - For receiving mail, text based, primarily for connected use
- MUAs (clients) and MTAs (servers)

FTP/TFTP

- File transfer protocol (FTP)
 - FTP server control channel is port 21
 - FTP server data transfer over port 20
 - Two modes possible, both use TCP:
 - Active: server connects to client from port 20
 - Passive: client connects to server on port 20
- Trivial file transfer protocol (TFTP)
 - One packet to server UDP port 69 for negotiation
 - The security concern is not what people think it is

VoIP/SIP/Skype

- Just another application? Why all the hype?
- For interactive multimedia, latency and delay matter
- Skype
 - Peer-to-peer with crypto
 - Public nodes may become supernodes
 - Supernodes help clients find each other
 - Directory/auth server(s) to help do updates and discovery
- <see other 263 slides for lots of details>

IRC/IM/Jabber

- Real-time inactive text messaging
- Crypto may be between server and client or from client to client in direct one-to-one chat
- Usually not encrypted, but probably should be
- Supports the notion of real-time availability/presence
- IRC widely used by botnets and the underground

File sharing (e.g. BitTorrent/KaZaA)

- The Internet always was peer-to-peer
- Newer apps make file sharing easy, maybe too easy
- You need to some way to “insert” into the p2p net
- Use other nodes to search for what you want
- Everyone may share or cache content
- Many copyright violation issues
- Numerous capacity congestion inducing issues
- <see SANS 2001 presentation>

Quality of Service

- The holy grail, let's just look at the Joint Techs presentation.

TELNET/SSH

- TELNET emulates an interactive terminal
 - Generally bytes sent as you hit the keys
 - Can have kerberized TELNET
 - But most people just use plain text
 - Still widely used for interacting with network gear
- Secure shell (SSH)
 - Key difference, crypto and pub key auth
 - Supports tunneling and file transfer
 - You want to be using this over TELNET

SNMP

- Simple network management protocol (SNMP)
 - You can SNMP poll or have agents and trap
- Information based on ASN.1 (very obtuse)
 - These are read-only and read/write parameters in agents, may be counters, config options, etc.
- Management information base
 - Definition of how to organize data ASN.1 formatted data
 - Hierarchy kind of like DNS, but not as friendly
 - e.g. 1.3.6.1.4.1.9.9.13.1.3.1.3

syslog

- Text-based limited log exportation mechanism
- Can be destined to local or remote host
- Use of facilities and severities to organize messages
- UDP, one-way protocol, simple, widely used
- Extensions to add TCP and other features

NetFlow

- One-way summary of packet stream of unique IP addresses, IP protocol and upper layer ports/types
- Generated by most larger, popular routers
- Widely used for traffic monitoring and analysis
- Often flows are sampled due to traffic and export limits

Tor

- Tor (and onion routing) <http://tor.eff.org>
- Directory server for client to build a multi-hop path
- Only client knows the full path
- TLS/SSL3, pub/symmetric key crypto used
- SOCKS interface for TCP apps
- DNS helper app so that queries do not leak

NTP

- Network time protocol
- Stratum of NTP devices syncing time
- Stratum-1 usually get time from GPS/modem
- Based on round trip time measurements/estimates
- NTP stabilizes over to over .1 ms accuracy
- SNTP can obtain 1 s accuracy
- UoWisc incident

RADIUS

- Remote authentication Dial-in User Services
- Authentication
- Authorization
- Accounting
- Involves a centralized RADIUS server and its clients
- Widely used for dial-up
- Also widely used for network management

Kerberos

- Method to authenticate over an untrusted net
- Secret key shared by client and KDC
- You are granted tickets by the KDC
- I like this:
 - <http://web.mit.edu/kerberos/dialogue.html>

nmap

- Handy tool to interrogate/probe a remote system
- Uses varying combinations of packets
- Interprets results to profile system and services

scappy

- Nmap on steroids
- You can create your own custom nmap in essence
- Send packets, take action based on the response

Various other tools

- dsniff
- Nessus
- Tcptraceroute
- Snort
- Netcat
- Metasploit framework
- Also some coding
 - For me, shell, Perl, simple C hacking, debugger

Research topics that come up

- Client puzzles
- Doing DDoS defense by offense
- Prefix hijacking monitoring
- Blacklists, whitelists, filtering
- Intrusion detection, prevention systems
- Log/data correlation
- Visualization
- peer-to-peer