


Kent State University Dept. of Computer Science	
CS 4/55231 Internet Engineering	→ <u>LECT-14</u>

Web Security

2

A Framework of Web Security


- Web System is composed of:
 - The Client
 - Client's Operating System
 - Client's Local Area Network
 - The Internet
 - The Server's LAN
 - The Server's Host Operating System
 - The Web Server Program
- The security of Web System can be compromised by holes in any of these components.


INTERNET ENGINEERING

LECT-14, S-3
IN2004S, javed@kent.edu
Javed I. Khan@2004

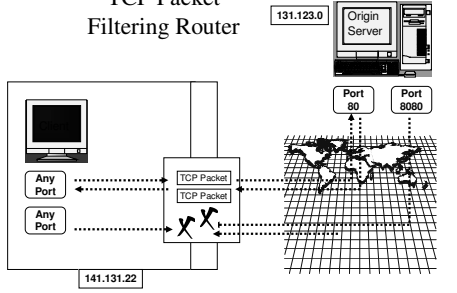
Firewalls & The Web


- A Firewall is a security mechanism which protects the computer and data on a private local area network from the uncontrolled activities of untrusted users and software on another network.
- Security Enhancement Devices:
 - Packet Filters
 - Circuit Gateway
 - Application Proxy


INTERNET ENGINEERING

LECT-14, S-4
IN2004S, javed@kent.edu
Javed I. Khan@2004

TCP Packet Filtering Router




INTERNET ENGINEERING


LECT-14, S-5
IN2004S, javed@kent.edu
Javed I. Khan@2004

TCP Header

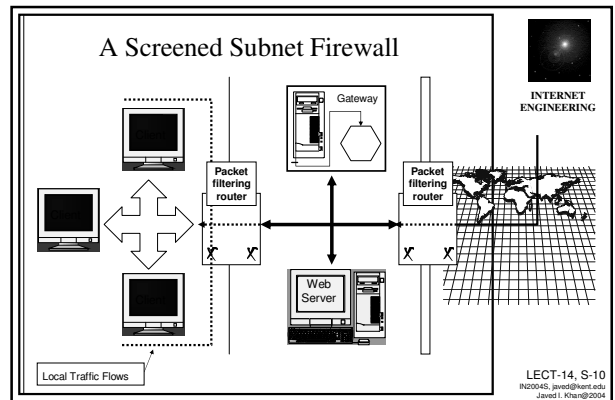
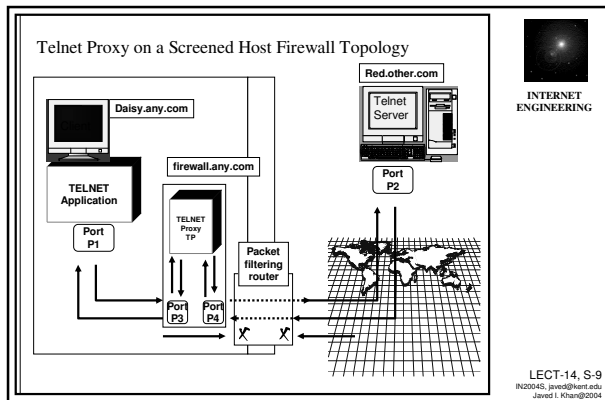
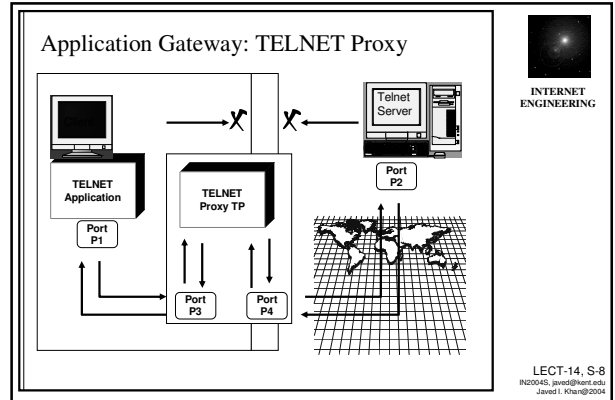
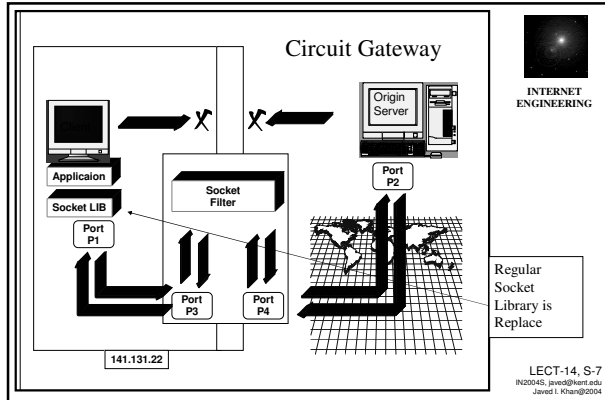
0	4	8	12	16	20	24	28	32
SOURCE PORT				DESTINATION PORT				
SEQUENCE NUMBER								
ACKNOWLEDGEMENT NUMBER								
HLEN		NOT USED		CODE BITS		WINDOW		
CHECKSUM				URGENT POINTER				
BEGINNING OF DATA								
⋮								

IP Header

0	4	8	12	16	20	24	28	32
VERSION		H. LEN		SERVICE TYPE		TOTAL LENGTH		
IDENTIFICATION		FLAGS		FRAGMENT OFFSET				
TIME TO LIVE		TYPE		HEADER CHECKSUM				
SOURCE IP ADDRESS								
DESTINATION IP ADDRESS								
IP OPTIONS (MAY BE OMITTED)				PADDING				
BEGINNING OF DATA								
⋮								


INTERNET ENGINEERING

LECT-14, S-6
IN2004S, javed@kent.edu
Javed I. Khan@2004



Security over Public Network

INTERNET ENGINEERING

LECT-14, S-12
IN2004S_javed@hert.edu
Javed I. Khan@2004

- ## Tools
- Cryptography
 - Private Key
 - Private/Public Key
 - Message Digest
 - Digital Certificates
 - Certificates
- Can a response which lacks validator be cached? Can it be validated, when expired?
- INTERNET ENGINEERING
- LECT-14, S-12
IN2004S_javed@hert.edu
Javed I. Khan@2004

Secure HTTP

Developed by CommerceNet, Palo Alto, CA.
NCSA Mosaic Supports it.

INTERNET
ENGINEERING

LECT-14, S-13
IN2004S_javed@kent.edu
Javed I. Khan@2004

Can Server initiate a secured communication?

INTERNET
ENGINEERING

LECT-14, S-14
IN2004S_javed@kent.edu
Javed I. Khan@2004

Secure Socket Layer (SSL)

Netscape® uses SSL 2.0 and Microsoft® has a copy PCT (Private Communications Technology)

40-bit key RC4 Encryption can be broken in 1 year by a 128-bit MIPS. USA version allows 128 bit-key.

INTERNET
ENGINEERING

LECT-14, S-15
IN2004S_javed@kent.edu
Javed I. Khan@2004

INTERNET
ENGINEERING

LECT-14, S-16
IN2004S_javed@kent.edu
Javed I. Khan@2004

Security Toll Booth

- How do client know that a server's public key is valid? What keeps an imposter server from sending its public key instead?
 - The answer is "trusted" certificate authority that signs the public key.
 - Netscape Commerce Server requires a digital certificate. A Browser will only authenticate a server which has a key signed by Netscape® (not available to public), or VeriSign® (an RSA spinoff company).
 - It costs \$295 for first server, and \$75 additional servers for first year. \$75 thereafter each year to get a certificate.
 - Soon USPS will compete with VeriSign®.

INTERNET
ENGINEERING

LECT-14, S-17
IN2004S_javed@kent.edu
Javed I. Khan@2004

SSL or S-HTTP?

- Neither is complete, and both are still under development.
- S-HTTP provides ultimate control to user.
 - Each document can have separate certificate and authentication.
 - Difficult to manage.
- SSL easy to manage and transparent.
 - But the security stops at the SSL layer.
 - Can be used for FTP, Telnet.

INTERNET
ENGINEERING

LECT-14, S-18
IN2004S_javed@kent.edu
Javed I. Khan@2004

Battle Continues..

- Leading encryption company RSA which has styled itself the most trusted name in e-security has had its web site successfully compromised twice recently, and seems to have changed web server platform on each occasion.
- On Thursday 10th February www.rsa.com was running Solaris and Netscape-Enterprise, by Sunday 13th it had switched to Linux and Apache/1.3.6, while today [Monday 14th February] it is running NT4 and Microsoft-IIS/4.0. It would be interesting to know the reasons for this; sometimes companies change platforms as a knee jerk reaction to a security or reliability problem, but going through the three most common platforms in four days seems exceptional. Presumably at least one of the attacks was a redirection of the DNS entry for www.rsa.com. (checkout email from netcraft)



INTERNET
ENGINEERING

LECT-14, S-19
IN2004S_jpvod@hert.edu
Janet L. Khan@2004

Interested in Learning More?

- We will learn more on Internet Security on the advanced IAD class:
- Topics to cover:
 - Public Key cryptography
 - X.509 digital certificates.
 - Virus spreading models.
 - Virus detection & removal techniques.
 - Distributed denial of service
 - Intrusion detection



INTERNET
ENGINEERING

LECT-14, S-20
IN2004S_jpvod@hert.edu
Janet L. Khan@2004