

Network Security in Practice (cont.)

Kai Shen

12/10/2014 CSC 257/457 - Fall 2014 1

Practices of Network Security

- Access control: firewalls
- Attacks and counter measures
 - mapping, sniffing, spoofing, cross-site scripting, DOS attack
- Security protocol case studies
 - Application-layer PGP: **secure email**
 - Transport-layer SSL: **secure sockets**
 - Network-layer IPsec: **secure networking**
 - Anonymity networks

12/10/2014 CSC 257/457 - Fall 2014 2

Secure Email: Confidentiality

Alice wants to send confidential e-mail, m , to Bob.

□ encrypts message with Bob's public key, all problems solved?

12/10/2014 CSC 257/457 - Fall 2014 3

Secure Email: Confidentiality

Alice:

- generates *symmetric* key, K_S
- encrypts message with K_S
- encrypts K_S with Bob's public key
- sends both $K_S(m)$ and $K_B^+(K_S)$ to Bob

Bob:

- uses his private key to decrypt and recover K_S
- uses K_S to decrypt $K_S(m)$ to recover m

12/10/2014 CSC 257/457 - Fall 2014 4

Secure Email: Sender Authentication and Message Integrity

- Sender authentication and message integrity:
 - generates a digital signature of the message digest using his/her private key
- Put everything together
 - uses one-time session key and the receiver's public key to encrypt a digitally signed message
 - supports confidentiality, sender authentication, and message integrity
 - PGP (pretty good privacy) for Internet email

12/10/2014 CSC 257/457 - Fall 2014 5

Secure Sockets Layer (SSL)/ Transport Layer Security (TLS)

- SSL/TLS: transport layer security service to any TCP-based applications
 - used for remote terminal access (SSH).
 - used between Web browsers, servers for e-commerce (https).
 - used between IMAP clients and servers.
- Security services:
 - CA-certified public keys.
 - data confidentiality by encryption using a symmetric session key, key encrypted with server's public key.
 - source authentication & data integrity by signed message digests.

12/10/2014 CSC 257/457 - Fall 2014 6

Network Layer Security Protocol IPsec

- Two goals that secure socket layer cannot accomplish
 - secure everything (not just TCP traffic) on Internet
 - enable segmented protection – protect a segment of the Internet path (e.g., public internet but not internal company network)
- Like before:
 - data confidentiality by encryption using a symmetric session key
 - source authentication & data integrity by signed message digests
- Done in a way that is compatible with basic IP
 - IPsec packet is recognized as a supported protocol in IP
 - routers who don't support it can ignore it ⇒ allow incremental deployment with incremental benefits

IP header	IPsec header	Payload (potentially encrypted)
-----------	--------------	---------------------------------

12/10/2014 CSC 257/457 - Fall 2014 7

More on IPsec

- Transport mode (only host-to-host protection):


IP header	IPsec header	Payload is data (TCP/UDP)
-----------	--------------	---------------------------
- Tunnel mode (allow segmented protection):

IP header	IPsec header	Payload is a full IP packet
-----------	--------------	-----------------------------
- Tunnel mode allows intermediate segment of secure conn between two routers.
- (Virtual Private Network) VPN:


```

            graph LR
            A(IBM US) --- R1(( ))
            R1 --- B(Internet)
            B --- R2(( ))
            R2 --- C(IBM India)
            style R1 fill:none,stroke:none
            style R2 fill:none,stroke:none
            
```
- A rare example of success on enhancing the Internet!


12/10/2014 CSC 257/457 - Fall 2014 8



Tor Anonymity Network

- Standard encryption mechanisms protect the content of communication, but not the identities of the comm. parties
- Tor, The Onion Router, anonymity network
 - "Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than four thousand relays to conceal a user's location or usage from anyone conducting network surveillance or traffic analysis." --Wikipedia
 - "Edward Snowden used the Tor Network to send information about PRISM to the Washington Post and The Guardian in June 2013." --Wikipedia
 - <http://en.wikipedia.org/wiki/File:Tor-onion-network.png>


12/10/2014 CSC 257/457 - Fall 2014 9



Tor Anonymity Network

- NSA and GCHQ are interested in it
 - <http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption>
 - Compromise the source
 - **Quotes from Guardian:** But the documents [NSA leaks] suggest that the fundamental security of the Tor service remains intact. One top-secret presentation, titled 'Tor Stinks', states: "We will never be able to de-anonymize all Tor users all the time." It continues: "With manual analysis we can de-anonymize a very small fraction of Tor users," and says the agency has had "no success de-anonymizing a user in response" to a specific request.

12/10/2014 CSC 257/457 - Fall 2014 10



Network Security (summary)


Basic techniques.....

- cryptography (symmetric and public)
- authentication
- message integrity
- key distribution

.... network security in practice

- firewall
- attacks and countermeasures
- secure application (PGP for email)
- secure transport (SSL/TLS)
- secure network (IPsec)
- Tor anonymity network

12/10/2014 CSC 257/457 - Fall 2014 11



Disclaimer

- Parts of the lecture slides contain original work of James Kurose, Larry Peterson, and Keith Ross. The slides are intended for the sole purpose of instruction of computer networks at the University of Rochester. All copyrighted materials belong to their original owner(s).

12/10/2014 CSC 257/457 - Fall 2014 12