Communication Networks
The University of Kansas EECS 780
Network Security and Resilience

James P.G. Sterbenz

Department of Electrical Engineering & Computer Science
Information Technology & Telecommunications Research Center
The University of Kansas

jgs@eecs.ku.edu

http://www.ittc.ku.edu/~jgs/courses/nets
Network Security
Outline

SR.1  Security functions and services
SR.2  End system protection
SR.3  Internet security
SR.4  Survivability and resilience
Security and Resilience

Introductory Disclaimer

- This is a very brief overview of the area...
  ...ought to be subject of a full course, and \textit{is}:
  - EECS 565 Intro. to Information and Computer Security
Network Security

SR.1  Security Functions and Services

SR.1  Security functions and services
SR.2  End system protection
SR.3  Internet security
SR.4  Survivability and resilience
Network Security
Basic Functions and Mechanisms

• Confidentiality
  – message contents only visible to sender & intended receiver

• Authentication
  – confirm identity of entity

• Message integrity
  – guarantee that message not altered without detection

• Nonrepudiation
  – sender of message can’t deny sending

• Access control and availability of resources
  – access to resources and services limited to legitimate and authorised users
Network Security
Communication and Threat Model

- Good guys communicate through a *secure channel*
- Bad guys attempt to attack or subvert
Network Security
Communication and Threat Model

• Good guys (commonly denoted Alice, Bob, Carol, Dave, ...)
  – human user “Alice”, “Bob”, “Carol”, “Dave”, ...

other examples?
Network Security
Communication and Threat Model

• Good guys (commonly denoted Alice, Bob, Carol, Dave, ...)
  – human user “Alice”, “Bob”, “Carol”, “Dave”, ...
  – web browser and server for electronic commerce & banking
  – DNS servers
  – router signalling (BGP, OSPF, ISIS, etc.)
  – ...

• Bad guys
Network Security
Communication and Threat Model

• Good guys (commonly denoted Alice, Bob, Carol, Dave, …)
  – human user “Alice”, “Bob”, “Carol”, “Dave”, …
  – web browser and server for electronic commerce & banking
  – DNS servers
  – router signalling (BGP, OSPF, ISIS, etc.)
  – …

• Bad guys (human or bot)
  – eavesdropper (commonly called Eve)
  – malicious attacker (commonly called Mallory)
  – intruder (K&R call Trudy)
Network Security
Communication and Threat Model

- Threat to confidentiality by bad guys
  - eavesdropping on sensitive communication

- Threat to authenticity
  - impersonation, spoofing, identity theft, forgery of messages
  - hijacking connection or association by impersonation

- Threat to message integrity
  - altering messages

- Threat to authentication and resource availability
  - denial of service attacks
Network Security
Communication and Threat Model

• It is *essential* that security measures ...
  ... address an *actual* threat model
  – otherwise it is a waste of resources, time, and money
  – that could instead actually make things better

• *Security theatre* [Schneier]
  – security models *don’t* address a threat
  – e.g. random search at airports
    • assumes terrorist that care about getting arrested
    • there isn’t a long line waiting to try again
  – why? perhaps an attempt to:
    • convince people that they are safe
    • convince people that government doing something
Information Security
Confidentiality Service

- Service: confidentiality
  - message contents only visible to sender & intended receiver

Threat and mechanism?
Information Security
Confidentiality Mechanism

• Service: confidentiality
  – message contents only visible to sender & intended receiver
• Threat
  – eavesdropping
• Security mechanism: cryptography
  – information encrypted in secure channel

scope?
Information Security
Confidentiality Mechanism

• **Service:** confidentiality
  – message contents only visible to sender & *intended* receiver

• **Threat**
  – eavesdropping

• **Security mechanism:** cryptography
  – information encrypted in secure channel
  – scope: *must* be E2E by End-to-End Arguments

*what about multiuser systems?*
Information Security
Confidentiality Mechanism

• Service: confidentiality
  – message contents only visible to sender & intended receiver

• Threat
  – eavesdropping

• Security mechanism: cryptography
  – information encrypted in secure channel
  – scope: must be E2E by End-to-End Arguments
    • more precisely A2A: app-to-app on shared-use systems
Information Security
Confidentiality and Cryptography

• Service: confidentiality
  – message contents only visible to sender & \textit{intended} receiver

• Threat
  – eavesdropping

• Security mechanism: cryptography
  – information encrypted in secure channel
  – scope: \textit{must} be E2E by End-to-End Arguments

• Cryptanalysis
  – recovery of plaintext without access to key
  – if possible deduce key
  – more and longer messages increase probability of success
Confidentiality
Cryptography Overview

- Plaintext message $M$ needs to be confidential
  - transformed to ciphertext by encryption using key $k_1$
  - ciphertext $C = E_{k_1}(M)$ transferred through secure channel
  - plaintext $M = D_{k_2}(C)$ recovered by decryption using key $k_2$
- Eavesdropper cannot recover $M$ from $C$ without $k_2$
Information Security

Cryptanalysis Attacks

- Ciphertext-only attack
  - recover plaintext from ciphertext
- Known plaintext attack
  - deduce key from (plaintext / ciphertext) pairs
- Chosen plaintext attack
  - deduce key from (chosen-plaintext / ciphertext)
- Adaptive chosen plaintext attack
  - adapt subsequent plaintext choices based on previous results
Information Security

Cryptanalysis Attacks

- Chosen ciphertext attack
  - choose ciphertext to be decrypted
  - use resulting plaintext to recover key
- Chosen key attack
  - exploit knowledge of relationship between different keys
- Rubber hose attack
  - threaten, blackmail, or torture to obtain key
- Purchase key attack
  - bribe to obtain key
Confidentiality
Substitution Ciphers

- Substitution cipher
  - substitute plaintext string with cipher string
- Monoalphabetic substitution cipher
  - one character-by-character single substitution
- Caesar or shift cipher
  - monoalphabetic substitution cipher
  - rotate $n$ positions through the alphabet and substitute
Confidentiality
Substitution Ciphers

- Caesar or shift cipher
  - monoalphabetic substitution cipher
  - rotate \( n \) positions through the alphabet and substitute
  - example: rot-13
  - plaintext: \( \text{abcdefghijklmnopqrstuvwxyz} \)
  - ciphertext: \( \text{mnbvcxzasdfghjklpoiuytrewq} \)
  - bob. i love you. alice
  - nkn. s gktc wky. music

*Strength of code?
Confidentiality
Substitution Ciphers

• Caesar or shift cipher
  – monoalphabetic substitution cipher
  – rotate $n$ positions through the alphabet and substitute
  – example: rot-13
  – plaintext: $abcdefghijklmnopqrstuvwxyz$
  – ciphertext: $mnbvcxzasdfghjklpoiuytrewq$
    
    bob. i love you. alice
    nkn. s gktc wky. music

• Brute force attack
  – try all possible substitutions
    
    is this necessary?
Confidentiality
Substitution Ciphers

• Caesar or shift cipher
  – monoalphabetic substitution cipher
  – rotate $n$ positions through the alphabet and substitute
  – example: rot-13
  – plaintext: $abcdefghijklmnopqrstuvwxyz$
  – ciphertext: $mnbvcxzasdfghjklpoiuytrewq$

  bob. i love you. alice
  nkn. s gktc wky. music

• Exploit known characteristics of plaintext
  – frequency analysis of letters and words
    • example: $s$ must be either $a$ or $i$
Confidentiality
Symmetric Key Cryptography

- Sending and receiving keys identical: \( k = k_1 = k_2 \)
  \[ M = E_k(D_k(M)) \]

*Problem?*
Confidentiality

Symmetric Key Cryptography

- Sending and receiving keys identical: \( k = k_1 = k_2 \)
  
  \[
  M = E_k(D_k(M))
  \]

- Key must be \textit{secret} shared only by sender & receiver
  
  - how to distribute key?
Confidentiality
Symmetric Key Cryptography

- Sending and receiving keys identical: \( k = k_1 = k_2 \)
  \[ M = E_k(D_k(M)) \]
- Key must be **secret** shared only by sender & receiver
  - keys must be exchanged by out-of-band secure mechanism
    - e.g. pre-existing secure channel or face-to-face secret meeting
Symmetric Key Cryptography
Example: DES Overview

- DES (data encryption standard) 1975 [NIST FIPS 46-2]

- Characteristics
  - 56-bit symmetric key
  - block mode cipher using 64-bit plaintext blocks

- Strength
  - “Strong cryptography makes the world a safer place”
    first decrypted (brute force) in 1997
  - now can be done in minutes or less
  - too weak to use
Symmetric Key Cryptography

Example: 3DES Overview

- Weaknesses in DES
  - Moore’s law caught up with DES

- Triple DES
  - short term response to DES weakness
  - apply DES encryption three times on plaintext
Symmetric Key Cryptography
Example: AES Overview

• AES (advanced encryption standard) [NIST FIPS-197]
  - 2001 replacement for DES for commercial & consumer apps
  - NSA and DOD continues to use classified crypto algorithms

• Key design goals
  - significantly stronger than DES or 3DES
  - simple fast hardware implementation
    • pipelineable and parallelisable

• Public design competition sponsored by NIST
  - Rijndael selected (Vincent Rijmen and Joan Daemen)
    • pronounced as rine-dal

todo: pipeline diagram
Symmetric Key Cryptography

Example: AES Operation

- Encryption functions $f$
  - $n$ pipeline stage delays over $b$ blocks (parallel speedup)
Symmetric Key Cryptography
Example: AES Operation

- S: substitute bytes (table)
- \( \oplus \): shift rows (permute)
- Ж: mix columns (matrix \( \times \))
- \( \Theta \): add (xor) round key \( w \)
Symmetric Key Cryptography

Example: AES Operation

- 128b blocks
- 128/192/256b key $k$
  expanded to 1408/1664/1920b
  round key $w$;
  128b/round
- 10/12/14 reversible
  encryption rounds
- fully pipelineable
  (no feedback)
Confidentiality
Public Key Cryptography Overview

- Symmetric key cryptography has serious problem
  - how to negotiate shared secret?

*Alternative?*
Confidentiality

Public Key Cryptography Overview

- Symmetric key cryptography has serious problem
  - how to negotiate shared secret?

- Public key cryptography changed everything
  - 1973: Clifford Cocks in British Intelligence
    - classified until 1997
  - 1976: Diffie and Hellman
  - 1977: RSA (Ron Rivest, Adi Shamir and Len Adleman)
  - NSA claims to have discovered it previously
    - we’ll never know for sure
Confidentiality
Public Key Cryptography Overview

- Asymmetric key pair
  - solution to out-of-band key distribution problem
  - encryption using key $k_p$ is Bob’s public key, known to all
  - decryption using key $k_s$ is Bob’s private key (Bob’s secret)

- Remarkable advance
  - no need out of band secret key distribution
Confidentiality
Public Key Cryptography Properties

• Need public and secret keys

\[ M = D_{k_s}(E_{k_p}(M)) \]

secret key \( k_s \) must not be computable from public key \( k_p \)
Confidentiality
RSA Key Selection

- Choose two large prime numbers $p, q$
- Compute $n = pq$, $z = (p-1)(q-1)$
  - strength: factoring numbers is computationally expensive
  - measured in number of bits in $n$ e.g. 1024
    - $2^{1024} - 1 \approx 1.79769 \times 10^{308}$
- Choose $e$ such that $e < n$ no common factors with $z$
  - $e, z$ are relatively prime
- Choose $d$ such that $ed - 1$ is exactly divisible by $z$
  - $ed \mod z = 1$
- Keys: public key $k_p = (n,e)$ private key $k_s = (n,d)$
Information Security
Message Integrity Service

- Service: message integrity
  - guarantee that message not altered without detection
    - when confidentiality not needed or desired
  - associate message with identity of creator

**Threat?**
Information Security
Message Integrity Mechanism

• Service: message integrity
  – guarantee that message not altered without detection
    • when confidentiality not needed or *desired*
  – associate message with identity of creator

• Threat
  – altering messages

• Security mechanism: message digests
  – strong hash of contents
  – computationally less complex than encryption
    • perhaps only done when alteration is suspect
Message Integrity
Message Digests

- Compute “fingerprint” of message

*why not use Internet checksum?*
Message Integrity

Message Digests

• Compute “fingerprint” of message
  – checksum permits undetectably swapping characters
    • e.g. IOU $19 to IOU $91
  – hash function $H(M)$

• Properties required
  – computationally infeasible to alter message with same hash
Message Integrity
Message Digest Standards

- **MD5** (message digest 5) [RFC 1321]
  - computes 128-bit message digest in four steps
- **SHS** (secure hash standard) [FIPS 180-2]
  - former SHA-1 now part of SHS
Information Security
Digital Signatures Service

• Service: digital signatures
  – associate message with identity of creator

Threat?
Information Security
Digital Signatures Mechanism

- **Service:** digital signatures
  - associate message with identity of creator

- **Threat**
  - forging messages

- **Security mechanism:** digital signatures
  - sender digitally signs message using cryptography
  - verifiable and non-forgable
Digital Signature Operation

• Verification of sender by encryption
  – only receiver can decrypt
  – computational complexity of encrypting large messages
    • when confidentiality is needed

• Encrypt only the message digest
  – sender encrypts MD with secret key
  – receiver decrypts MD with public key
  – required property: $D_{ks}(E_{kp}(M)) = E_{kp}(D_{ks}(M))$
    • RSA has this property
Information Security
Authentication Service

• Service: authentication
  – confirm identity of entity

Threat?
Information Security
Authentication Mechanism

- **Service**: authentication
  - confirm identity of entity
- **Threat**
  - impersonation and spoofing
  - phishing
- **Security mechanism**
  - verification of sender identity
Authentication Overview

- Verify *identity* of sender of message $M$
  - without visual cues in face-to-face meeting
- Prevent impersonator pretending to be someone else
Authentication
Source Address

- Authentication by source address
  - e.g. verify IP address of sender

*problem?
Authentication
Source Address

• Authentication by source address
  – e.g. verify IP address of sender
  – IP address spoofing by sender relatively easy
    • forge source address in IP packet
  – network may check subnet match of sender

• Only feasible if source address unforgeable
  – not the case in the current Internet
Authentication

Password

- Authentication by password of sender
  - if password sent in the clear, eavesdropper can intercept
  - encrypted password prevents eavesdropping

*problem?
Authentication
Password

• Authentication by password of sender
  – if password sent in the clear, eavesdropper can intercept
  – encrypted password prevents eavesdropping
    • susceptible to playback attack
    • eavesdropper simply repeats encrypted password

Alternative?
Authentication
Nonce Challenge with Shared Secret Key

- Goal: avoid playback attack
- Solution: \textit{nonce} is number used only once

Choose \textit{random} nonce (\textit{why?})

- return encrypted nonce with shared secret key
- impersonator can’t properly encrypt nonce
- playback attack won’t work

\textit{Can we avoid need for prearranged shared secret?}
Authentication
Nonce Challenge with Public Key

• Goal: avoid need for shared secret
  – very awkward for general authentication scenarios

• Solution: use public key cryptography
  – sender encrypts nonce with secret key
  – receiver decrypts with public key
    • depends on secure distribution of public key
    • still subject to “man in the middle” attack
Network Security
Key Distribution

- Cryptography depends on key distribution
- Bilateral negotiation
  - may be difficult for private key exchange
  - defeats the purpose of public key encryption

*Alternative?*
Network Security
Key Distribution

- Cryptography depends on key distribution
- Symmetric cryptography
  - trusted intermediary: KDC key distribution center
  - prevents need for out-of-band key exchange for every pair
Network Security
Key Distribution

- Cryptography depends on key distribution
- Symmetric cryptography
  - KDC key distribution center
- Public key cryptography:
  - PKI (public key infrastructure)
Network Security

Key Distribution

- Cryptography depends on key distribution
- Symmetric cryptography
  - KDC key distribution center
- Public key cryptography:
  - need mechanism to authenticate public key holder
  - PKI (public key infrastructure)
  - need mechanism to authenticate public key holder
    - CA: certificate authority
    - X.509 certificate standard
Network Security
Key Distribution

- Cryptography depends on key distribution
- Symmetric cryptography
  - KDC key distribution center
- Public key cryptography:
  - need mechanism to authenticate public key holder
  - PKI (public key infrastructure)
  - web of trust
    - self-signed certificates propagate among trusted acquaintances
    - example: PGP (pretty good privacy)
Network Security
Certificate Revocation

- Certificates may need to be *revoked*

*Why?*
Network Security
Certificate Revocation

- Certificates may need to be *revoked*
- Reasons to revoke certificates
  - compromised key
  - compromise of CA
  - ...
Network Security

SR.2  End System Protection

SR.1  Security functions and services
SR.2  End system protection
SR.3  Internet security
SR.4  Survivability and resilience
End System Protection

Motivation

*How to prevent malicious software from running?*
Virus Scanners
Mechanisms

- **Virus scanner** looks for viruses and worms
  - periodic scan of hard drives; *be careful of USB sticks*
  - does not protect from downloaded or emailed code
    - until the next scan
    - was generally adequate before widespread use of Internet
  - scan code as it comes from networks
    - file downloads: HTTP, FTP, and other downloads
    - email attachments

*Problem?*
Virus Scanners

Mechanisms

- **Virus scanner** looks for viruses and worms
  - periodic scan of hard drives
  - scan code as it comes from networks
    - file downloads: HTTP, FTP, and other downloads
    - email attachments

- **Problem:** *zero-day attack*
  - some exploits discovered and fixed during development
    - open-source (e.g. Linux) far better for this
  - but many unleashed without prior warning
    - whitehats: inform developer before publication
    - blackhats: unleash malware
End System Security

Motivation

How to prevent attacks from the network?
Firewalls
Enterprise

- **Firewall** isolates network or host
  - filters and blocks selected packets

- Location
  - enterprise: located between organisation and public Internet

*advantages and disadvantages?*
Firewalls

Enterprise

- **Firewall** isolates network or host
  - filters and blocks selected packets

- Enterprise firewall
  - advantages
    - managed by enterprise IT
  - disadvantages
    - doesn’t protect against inside attacks
      - increasingly inadvertent with laptops and mobile devices
    - doesn’t protect users at home and when travelling
Firewalls

Enterprise

• *Firewall* isolates network or host
  – filters and blocks selected packets

• Enterprise firewall
  *alternative*?
Firewalls

Personal

- **Firewall** isolates network or host
  - filters and blocks selected packets
- Enterprise firewall
- Personal firewall
  - filtering software should be used on *every* machine
    - even MacOs and Linux *(why?)*
Firewalls

Combined Use

- **Firewall** isolates network or host
  - filters and blocks selected packets
- Enterprise/home + personal firewalls
  - combines the advantage of both
  - NAT provides added benefit of blocking inbound traffic
Firewalls

Stateless

- Stateless firewalls
  - individual per packet decision

- Filtering criteria
  - source, destination IP address
  - sourced, destination port numbers
    - may only allow certain protocols such as SMTP, IMAP, HTTP
  - ICMP message type
    - e.g. prohibit ping
  - TCP SYN and ACK bits
Firewalls
Stateless Example

• Block incoming and outgoing datagrams with
  – IP protocol field = 17 and with
  – either source or dest port = 23
  – all incoming, outgoing UDP flows blocked
  – all telnet connections are blocked

• Block outgoing packets with dest port = 80
  – (mostly) prevent outside Web access
Firewalls

Stateful

- Stateless firewalls make dumb decisions
  - permit incoming packets that do not correspond to flows
- Stateful filtering criteria
  - track status of every TCP connection
    - only permit incoming packets sensible for given connection
  - timeout inactive connections
Intrusion Detection Systems

Motivation

• Firewalls
  – generally only operate on TCP/UDP/IP headers
  – no correlation among session
  – no traffic monitoring

Solution?
Intrusion Detection Systems

Functions

- **IDS**: intrusion detection system
  - DPI: deep packet inspection
    - examine TCP/UDP payloads
    - filter for known attacks and unlikely protocol behaviour
  - correlate over multiple packets
    - port scanning, network mapping
  - monitor traffic characteristics
    - DoS attack detection
Intrusion Detection Systems

Introduction

- **IDS**: *intrusion detection system*
- Location
  - enterprise
  - personal
- Frequently part of firewall+IDS system
End System Security

Poll

*How many of you protect your systems?*
End System Security

Poll

How many of you protect your systems? 
all of your systems?
End System Security
Recommendations

• *All* (end) systems should be protected
  – and kept up-to-date

• Personal computers
  – Windows  *how?*
  – MacOS   *how?*
  – Linux   *how?*

• Mobile phones and slates (tablets)
  – Android  *how?*
  – iOS      *how?*
End System Security
Recommendations

• *All* (end) systems should be protected
  – and kept up-to-date

• Personal computers
  – Windows   FW in XP SP2+; AV opt in XP, built-in Win8+
  – MacOS     FW not on by default; 3rd party AV needed
  – Linux     FW: iptables ; 3rd party AV needed

• Mobile phones and slates (tablets)
  – Android   3rd party protection needed, e.g. Kaspersky
  – iOS       don’t worry; be happy!
    • built-in security; walled garden iTunes store (Apple tells you)
    • unless jailbroken / rooted
End System Security
Auto-Update Poll

How many of you auto-update your systems?
End System Security
Recommendations for Auto-Updating

- Systems should be regularly updated
  - automatic update notifications help
    - if user pays attention to them

- Auto-update risks
  - malware inserted into system software by *blackhats*
  - update domain hijacked, e.g. update.microsoft.com

- Result could be catastrophic
  - e.g. brick all Windows systems

- Best to get automatic notification
  - but regularly manual update after checking news
  - Microsoft makes this difficult (but not impossible) in Win10
Security and Resilience

SR.3  Internet Security

SR.1  Security functions and services
SR.2  End system protection
SR.3  Internet security
  SR.3.1 Application security
  SR.3.2 Transport layer security
  SR.3.3 IP security
  SR.3.4 Wireless access security
  SR.3.5 Network infrastructure protocol security
SR.4  Survivability and resilience
Internet Security

Overview

Where should Internet security be located?
Internet Security Overview

- Internet security mechanisms location
  - E2E for user and app communication by *E2E Arguments*
    - authentication, integrity, and confidentiality

*is that all?*
Internet Security Overview

- Internet security mechanisms location
  - E2E for user and app communication by *E2E Arguments*
    - authentication, integrity, and confidentiality
  - network infrastructure protocols
    - authentication for DNS, BGP, etc.
    - endpoints are source and destination of signalling messages

*Problem?*
Internet Security Overview

• Internet security mechanisms location
  – E2E for user and app communication by *E2E Arguments*
    • authentication, integrity, and confidentiality
  – network infrastructure protocols
    • authentication for DNS, BGP, etc.
    • endpoints are source and destination of signalling messages

• Security not designed into Internet architecture
  – deploying a series of hacks to existing protocols
Internet Security
Overview

• Internet security mechanisms location
  – applications
    • addons to email
    • SSH for remote login
    • HTTPS for Web browsing
  – E2E transport
    • SSL/TLS (secure sockets layer / transport layer security)
  – network layer
    • IPsec for authentication, integrity, non-replay, confidentiality
  – network infrastructure protocols
    • DNSSEC and sBGP
  – Wireless LANs: WPA (Wi-Fi protected access)
Security and Resilience

SR.3.1 Application Security

SR.1 Security functions and services
SR.2 End system protection
SR.3 Internet security
  SR.3.1 Application security
  SR.3.2 Transport layer security
  SR.3.3 IP security
  SR.3.4 Wireless access security
  SR.3.5 Network infrastructure protocol security
SR.4 Survivability and resilience
Application Security
Overview

• Application security
  – security mechanisms coded into or invoked by applications
  – may use standard transport-layer security services (e.g. SSL)

• Common applications
  – HTTPS for Web browsing (HTTP over SSL)
  – SSH for secure login
  – email
Application Security

HTTPS Motivation

- Secure Web browsing

Motivation?
Application Security

HTTPS Motivation

- Secure Web browsing
- Motivation
  - browsing involving private information
    - e.g. shopping and banking with credit card numbers
  - privacy in Web search queries
  - privacy in Web sites browsed
    - you employer is likely tracking your Web browsing activity
Application Security

HTTPS Overview

• HTTPS: HTTP over SSL / TLS
  – standardised in [RFC 2818]
  – HTTPS uses SSL/TLS instead of conventional TCP sockets
    SSL/TLS described later
  – supported by modern Web browsers

• Encrypted
  – HTTP headers
    • including get request and URL
  – returned Web page
  – cookies
Application Security

HTTPS URLs Browser UI

- HTTPS URLs
  - protocol type https://
  - increasingly Web sites will use HTTPS by default
    - e.g. DuckDuckGo, Google, Facebook, Twitter
    - financial and shopping sites, e.g. banks and Amazon

- Most Web browsers indicate secure connection
  - commonly padlock symbol
  - check to confirm when exchanging private information
Application Security

SSH Motivation

- Secure remote login

Motivation?
Application Security

SSH Motivation

- Secure remote login
  - replacing insecure telnet
- Motivation
  - prevent password sniffing
  - confidentiality in information exchanged in login session
Application Security
SSH Services and Protocols

• SSH (secure shell) [Ylönen HUT 1995] [RFC 4251]
  – authentication of user to server or remote machine
    • should be separate secure machine, e.g. ssh.ittc.ku.edu
  – encrypted tunnel for confidential login session

• Protocols
  – SSH authentication protocol [RFC 4252]
  – SSH connection protocol [RFC 4254]
    • multiplexes and port maps other protocols in session
  – SSH transport layer protocol [RFC 4253]
    • runs over conventional TCP
    • note: does not use SSL/TLS
Application Security
Secure Email Motivation

- Secure email

Motivation?
Secure email motivation

- prevent unauthorised access to emails on server
  - necessary with IMAP/POP or Web-based accounts
- authentication of email senders
  - reduce phishing attacks
- confidentiality in email contents
  - email text
  - attachments

**Problem?**
Application Security

Secure Email Issues

- Secure email motivation
  - prevent unauthorised access to emails on server
    - necessary with IMAP/POP or Web-based accounts
  - authentication of email senders
    - reduce phishing attacks
  - confidentiality in email contents
    - email text
    - attachments
    - *your employer may be looking at your email contents*
      - separation of work and personal email accounts recommended

- Problem
  - diversity in email clients and protocols used
Application Security
Secure Email Services

- Secure login to server
  - prevent unauthorised access to account
- Mechanism
  - SSL/TLS for SMTP and IMAP or POP access
    - passwords encrypted
    - email encrypted between user and server
  - HTTPS for Web-based email (e.g. Google, Hotmail)
    - passwords encrypted
    - email browsing encrypted

problem?
Application Security
Secure Email Services

- Secure login to server
  - prevent unauthorised access to account

- Mechanism
  - SSL/TLS or HTTPS for email server access
  - problems
    - does not provide confidentiality via Internet between servers
    - does not provide authentication of sender of email
      - simple to spoof email From: and Sent-by: headers
Application Security
Secure Email Services

- Secure login to server
  - prevent unauthorised access to account

- Mechanism
  - SSL/TLS or HTTPS for email server access
  - alternative solutions for authentication and confidentiality
    - PGP: pretty good privacy based on a web of trust
    - S/MIME: secure multipurpose Internet mail extension [RFC 3850–3852]

- Client alternatives
  - plugins for existing clients, e.g. GPGMail for MacOS mail
  - separate secure email clients, e.g. Mailmate
Security and Resilience

SR.3.2 Transport Layer Security

SR.1 Security functions and services
SR.2 End system protection
SR.3 Internet security
  SR.3.1 Application security
  SR.3.2 Transport layer security
  SR.3.3 IP security
  SR.3.4 Wireless access security
  SR.3.5 Network infrastructure protocol security
SR.4 Survivability and resilience
Transport Layer Security
Overview

• SSL: secure sockets layer [Netscape 1996 v3.0]
  – standardised as TLS (transport layer security) [RFC 5246]
    • TLS similar but not identical to SSL
  – end-to-end transport-layer security shim above TCP

• Motivation
  – provide security to socket-based applications

• Implementation
  – use by application designers
  – packaged with common applications
    • Web browsers running HTTPS
    • email clients for secure access SMTP and IMAP servers
• SSL associations: split for efficiency
  – session: security association between systems
    • established by SSL handshake
  – connection: secure transfer using record protocol
    • may be multiple connections per session

• SSL protocols
  – handshake protocol
  – change cipher spec protocol
  – alert protocol
  – record protocol
SSL / TLS
Handshake Protocol

- Handshake protocol
  - authentication
  - negotiate
- encryption
- MAC message auth code
- keys

Figure 17.6 Handshake Protocol Action [Stallings C&NS]
SSL / TLS
Record Protocol

- Record protocol
  - fragment
  - compress
  - add msg auth code
  - encrypt
  - add record header

Figure 17.3 SSL Record Protocol Operation [Stallings C&NS]
Security and Resilience

SR.3.3  IP Security

SR.1  Security functions and services
SR.2  End system protection
SR.3  Internet security
  SR.3.1  Application security
  SR.3.2  Transport layer security
  SR.3.3  IP security
  SR.3.4  Wireless access security
  SR.3.5  Network infrastructure protocol security
SR.4  Survivability and resilience
IPsec
Overview

- IPsec: crypto-based security for IPv4 and IPv6
  - [RFC 4301] and many more
- Motivation
  - no universal end-to-end security mechanism
    - SSL/TLS available only for TCP socket apps
  - not all applications have secure variants
  - provides a VPN (virtual private network) e2e service
- Implementation
  - BITS: (bump in the stack) in end systems
  - BITW: (bump in the wire) inline security gateway system
IPsec Services and Protocols

- **IPsec Services**
  - access control
  - connectionless integrity
  - data origin authentication
  - detection and rejection of replays
  - data confidentiality
  - limited traffic flow confidentiality

- **Protocols**
  - AH: authentication header (optional)
  - ESP: encapsulating security payload (mandatory)
  - IKE: internet key exchange for key management
IPsec
ESP Overview

• IPsec ESP
  – mandatory component of IPsec
  – most widely used
  – (mostly) superset of AH providing full set of IPsec services

• SA (security association)
  – unidirectional (connection) created for each direction
  – SAs stored in SAD (SA database) in each IPSec endpoint
  – payload (and optionally IP header) encrypted
  – ESP header and trailer added
  – authentication trailer added

• Many combinations of services and options
IPsec
ESP Transport Mode

• Modes
  – transport mode: between end systems (or to single server)
  – tunnel mode

• Transport mode encapsulation
  – IP header (needed in the clear) to destination ES
  – IPsec ESP (shim) header to provide security services
  – MAC (message authentication code) appended (in cleartext)
IPsec

ESP Tunnel Mode

• Modes
  – transport mode
  – tunnel mode: between security gateways for VPN

• Tunnel mode encapsulation
  – entire IP packet encapsulate and encrypted
  – new IP header to security gateway
  – IPsec ESP header and MAC to provide security services
IPsec ESP

IPsec Header

- **ESP header** [RFC 4303]
  - **SPI** [32 b]
    (security parameters index)
    arbitrary SA identifier
    generated by receiver
  - **sequence number** [32 b]
    per SA packet seq #
    to prevent replay

- **IPsec trailer**
  - **ICV** [variable]
    (integrity check value)
    ESP hdr + payload
Security and Resilience

SR.3.4 Wireless Access Security

SR.1 Security functions and services
SR.2 End system protection
SR.3 Internet security
  SR.3.1 Application security
  SR.3.2 Transport layer security
  SR.3.3 IP security
  SR.3.4 Wireless access security
  SR.3.5 Network infrastructure protocol security
SR.4 Survivability and resilience
Wireless Access Security

Motivation

- Wireless (LAN) access an open channel problem?
Wireless Access Security

Motivation

- Wireless (LAN) access an open channel
  - problem: others can eavesdrop by packet sniffing

Does the wireless link need encryption?
Wireless Access Security

Motivation

- Wireless (LAN) access an open channel
  - problem: others can eavesdrop by packet sniffing

*Does the wireless link need encryption?*

*What do the End-to-End Arguments say?*
Wireless Access Security

Motivation

• Wireless (LAN) access an open channel
  – problem: others can eavesdrop by packet sniffing

• Wireless link encryption
  – shouldn’t be necessary if all E2E communication encrypted

reality?
Wireless Access Security

Motivation

- Wireless (LAN) access an open channel
  - problem: others can eavesdrop by packet sniffing
- Wireless link encryption
  - shouldn’t be necessary if all E2E communication encrypted
  - reality is that Internet security is piecemeal
    - HTTPS for some Web sites
    - SSL/TLS for email password protection
    - VPNs using IPSec for many enterprise network users
      - but not most individuals’ personal use

solution?
Wireless Access Security

Motivation

- Wireless (LAN) access an open channel
  - problem: others can eavesdrop by packet sniffing
- Wireless link encryption
  - shouldn’t be necessary if all E2E communication encrypted
  - reality is that Internet security is piecemeal
  - solution: secure wireless access
    - significant improvement equivalent to wired access link
Wireless Access Security

802.11 Security

- 802.11 WEP: wired equivalent privacy [802.11-1997]
  - in original 1997 802.11 spec
  - serious security flaws (short key and reused IV)
    - crackable in several minutes in mid-2000s
    - should no longer be used
Wireless Access Security

802.11 Security

- **802.11 WEP**: wired equivalent privacy [802.11-1997]
  - insecure and should no longer be used

- **802.11i WPA**: Wi-Fi protected access [802.11-2007]
  - originally supplement [802.11i-2004]
  - significantly stronger
    - but still crackable, particularly if weak password used
    - downloadable cracking software exists

- **E2E security should still be used whenever possible**
  - especially SSL/TLS email connections and VPNs
  - especially using open or public 802.11 hotspots
Security and Resilience

SR.3.4  Wireless Access Security

SR.1  Security functions and services
SR.2  End system protection
SR.3  Internet security
  SR.3.1  Application security
  SR.3.2  Transport layer security
  SR.3.3  IP security
  SR.3.4  Wireless access security
  SR.3.5  Network infrastructure protocol security
SR.4  Survivability and resilience
Network Infrastructure Security

Motivation

- Network infrastructure protocols

  examples?
Network Infrastructure Security

Motivation

- Network infrastructure protocols
  - BGP
  - DNS

Motivation and need for security mechanisms?
Network Infrastructure Security

Motivation

- Network infrastructure protocols
  - BGP
  - DNS

- Motivation and need for security mechanisms
  - Critical to operations of the Internet
  - Need to insure that crackers can’t disrupt

Threat?
Network Infrastructure Security

Threat

- Network infrastructure protocols
  - BGP
  - DNS

- Motivation and need for security mechanisms
  - critical to operations of the Internet
  - need to insure that crackers can’t disrupt

- Threats
  - injecting signalling messages to alter operations
  - DNS hijacking and BGP advertisements to redirect traffic
  - black-holing to divert and discard traffic
DNS Security
Overview

• DNSSEC [RFC4033]
  – security extensions to DNS

• DNS services
  – origin authentication
  – data integrity

• Deployment increasing
BGP Security
Overview

• BGP security
  – several proposals and sets of standards
    • e.g. S-BGP, BGPsec
  – none adopted
    • concerns about overhead of key management
    • difficulty of incremental deployment

• Current state
  – policy-based filtering
Security and Resilience

SR.5 Resilience, Survivability, and DTNs

SR.1 Overview and threat models
SR.2 Cryptography and security services
SR.3 Internet and wireless LAN security
SR.4 End system protection
SR.5 Resilience, survivability, and DTNs
Resilient Networks

Definition

• Resilience
  – provide and maintain acceptable service
  – in the face of faults and challenges to normal operation

• Challenges
  – faults
  – unintentional misconfiguration or operational mistakes
  – large scale disasters (natural and human-caused)
  – malicious attacks from intelligent adversaries
  – environmental challenges
  – unusual but legitimate traffic
  – service failure at a lower level

[ComNet 2010]
Resilience Disciplines

Overview

- **Challenge Tolerance**
  - fault-tolerance: single or few random failures
  - survivability: many or correlated failures
    - attack or disaster
  - disruption tolerance and traffic tolerance

- **Trustworthiness**

- **Robustness**
Resilience Disciplines
Overview

- **Challenge Tolerance**
- **Trustworthiness:** measurable quantities
  - security
  - dependability (binary)
    - reliability
      \( \text{Pr[remains up for specified time]} \)
    - availability
      \( \text{Pr[up]} \)
    - maintainability
  - performability
    - degraded performance (non-binary)

- **Robustness**
Reliability and Availability

Mean Time to Failure

- **MTTF** (mean time to failure)
  - expected value of failure density function $f(t)$
- **MTTR** (mean time to repair)
  - expected value of repair density function
- **MTBF** (mean time between failures)
- $MTBF = MTTF + MTTR$
# Reliability and Availability

## Availability Level

<table>
<thead>
<tr>
<th>Availability</th>
<th>Downtime</th>
<th>Downtime</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A$</td>
<td>$9_i$</td>
<td>%</td>
</tr>
<tr>
<td>0.9</td>
<td>0.91</td>
<td>90</td>
</tr>
<tr>
<td>0.99</td>
<td>0.92</td>
<td>99</td>
</tr>
<tr>
<td>0.999</td>
<td>0.93</td>
<td>99.9</td>
</tr>
<tr>
<td>0.9999</td>
<td>0.94</td>
<td>99.99</td>
</tr>
<tr>
<td>0.99999</td>
<td>0.95</td>
<td>99.999</td>
</tr>
<tr>
<td>0.999999</td>
<td>0.96</td>
<td>99.9999</td>
</tr>
</tbody>
</table>

- Downtime / year relationship with availability
  - 1 nine unacceptable for most systems
  - 5 nines is a common (but aggressive) specification
  - 6 or more nines difficult to achieve without extreme FT
  - but may be necessary in some mission-critical systems
Reliability and Availability

Relative Importance

- High availability but low reliability
  - MTTR very low but MTTF also low

- High reliability but low availability
  - MTTF large but MTTR also large
Resilience Disciplines
Overview

- Challenge Tolerance
- Trustworthiness: measurable quantities
- Robustness:
  - control theoretic notion
  - $\Delta$ trustworthiness under challenge
Scope of Resilience

Relationship to Other Disciplines

- **Challenge Tolerance**
  - **Survivability**: many vs. targeted failures
  - **Fault Tolerance**: few & random
  - **Traffic Tolerance**: legitimate & flash crowd

- **Disruption Tolerance**
  - environmental delay, mobility, connectivity, energy

- **Trustworthiness**
  - **Dependability**: reliability, maintainability, safety
  - **Availability**: availability, integrity
  - **Security**: confidentiality, nonrepudiability
  - **AAA**: auditability, authorisability, authenticity
  - **Performability**: QoS measures

- **Robustness Complexity**
  - **Challenge Tolerance**
  - **Traffic Tolerance**
  - **Disruption Tolerance**
  - **Survivability**
  - **Fault Tolerance**

- **Survivability**
  - legitimate & flash crowd
  - electricity & DDoS

- **Disruption Tolerance**
  - energy & delay
  - mobility & connectivity

- **Trustworthiness**
  - confidentiality & nonrepudiability
  - integrity & availability
  - reliability & maintainability

- **Fault Tolerance**
  - many vs. targeted failures
  - few & random

- **Traffic Tolerance**
  - legitimate & flash crowd
  - attack & DDoS
ResiliNets Strategy

$D^2R^2 + DR$

- Two phase strategy for resilience
- Real time control loop: $D^2R^2$
  - defend
    - passive
    - active
  - detect
  - remediate
  - recover
- Background loop: DR
  - diagnose
  - refine

[Wiki 2005, ComNet 2010]
ResiliNets Principles

High Level Grouping

- Prerequisites: to understand and define resilience
- Tradeoffs: recognise and organise complexity
- Enablers: architecture and mechanisms for resilience
- Behaviour: require significant complexity to operate
Resilience Principles
Redundancy, Diversity, Heterogeneity

- **Diversity**
  - mechanism (wired & wireless), provider, **geographic path**
- **Multipath transport**
  - spreading (eraser code) or as hot-standby
Security and Resilience

Further Reading and Additional References

- William Stalling,
  *Cryptography and Network Security: Principles and Practice*,
  Pearson, 2014.
Security and Resilience

Acknowledgements

Some material in these foils comes from the textbook supplementary materials:

- Kurose & Ross, *Computer Networking: A Top-Down Approach Featuring the Internet*