CS5285
Information Security for eCommerce

Lecture 9

Prof. Gerhard Hancke

CS Department

City University of Hong Kong

Reminder of previous lecture

- Computer security
  - Authentication (passwords)
    - Multi-factor (know, have, are)
    - Password files (dictionary attacks)
    - Phishing
  - Access control
  - Firewall
    - Four basic types
      (Packet filter, stateful, appplication proxy, personal)
  - Malware
    - Different types (e.g. bacteria, worm, virus, logic bomb..)

Today's Lecture

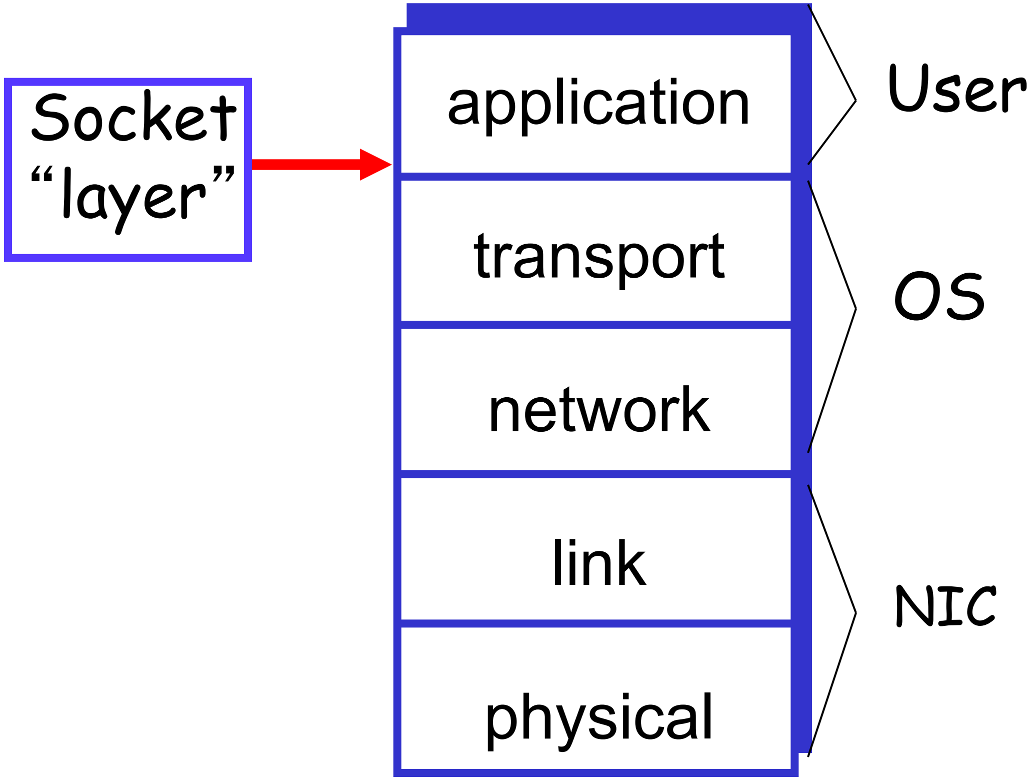
- For all e-commerce systems we need to securely communicate and exchange data
- Aspects of Network Security
  - Web (TLS/SSL)/IPSEC
  - WiFi/Mobile Networks
  - DoS
- CILO1,CILO2, CILO3 and CILO4

  (Data security, security requirements, security measures, security assessment)

Secure Socket Layer (Transport Layer Security)

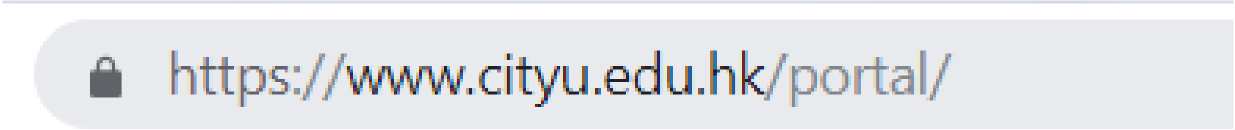
Socket layer

- "Socket layer" lives between application and transport layers
- SSL usually lies between HTTP and TCP



What is SSL?

- Secure Socket Layer (SSL) is the protocol used for most secure transactions over the Internet



https://www.cityu.edu.hk/portal/

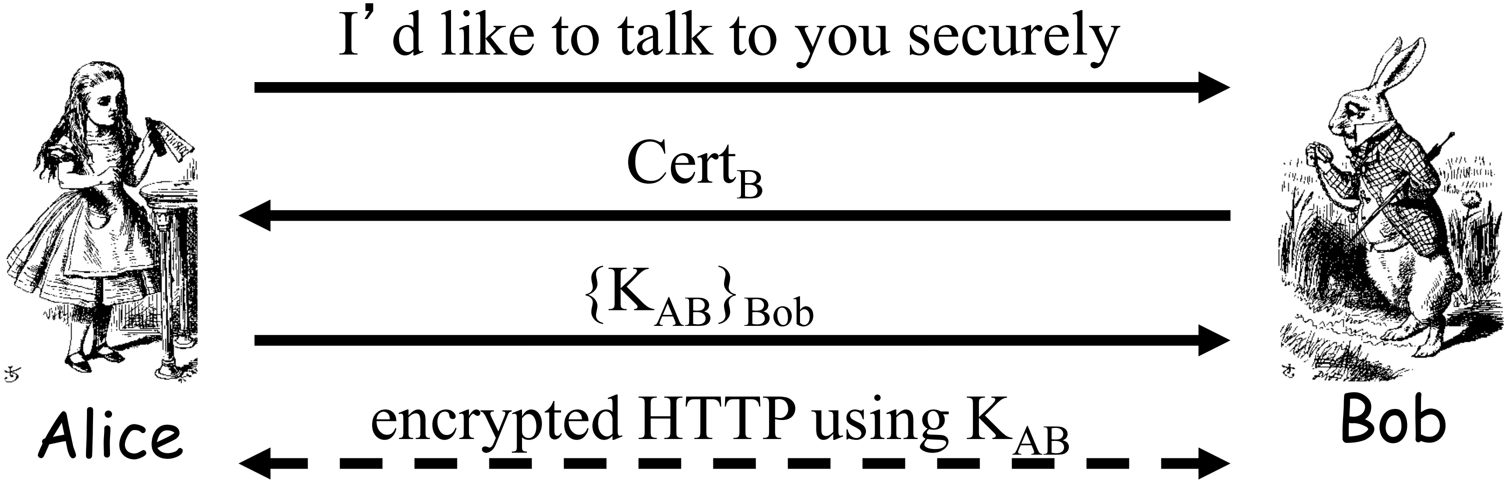
- For example, if you want to buy a book at amazon.com…
  - You want to be sure that you are dealing with Amazon (**one-way authentication**)
  - Your credit card information must be protected in transit (**data confidentiality**)
  - As long as you have money, Amazon doesn’t care who you are (**authentication need not to be mutual**)
    - Mutual version does exist (if client has certificate, server to server)

TLS and SSL

- TLS (SSL has evolved into Transport Socket Layer)
  - SSL 1.0, 2.0, 3.0 >> TLS 1.0, 1.1, 1.2, 1.3
  - DTLS is version for UDP (instead of TCP)
- Handshake and record protocols
  - Handshake: Authentication, key establishment, cipher options
  - Record: Confidentiality and integrity
- Ciphersuite
- See: www.openssl.org/docs/manmaster/man1/ciphers.html
- TLS 1.3 supports 5 cipher suites (all authenticated encryption)

TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_CCM_SHA256
TLS_AES_128_CCM_8_SHA256

Simple SSL-like Protocol



Alice

I’d like to talk to you securely

Cert_B

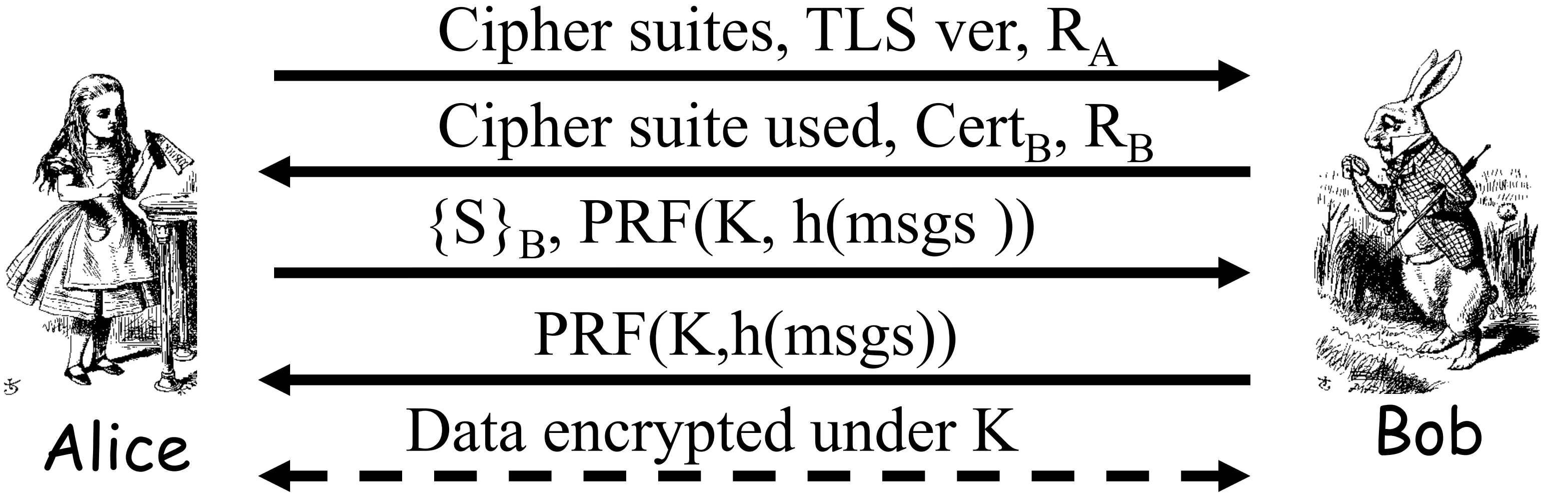
$\{K_{AB}\}_{Bob}$

encrypted HTTP using K_{AB}

Bob

- □ Is Alice sure she’s talking to Bob?
- □ Achieve Data Confentiality?

Simplified SSL Handshake Protocol



Cipher suites, TLS ver, R_A

Cipher suite used, Cert_B, R_B

$\{S\}_B$, PRF(K, h(msgs))

PRF(K,h(msgs))

Data encrypted under K

Alice

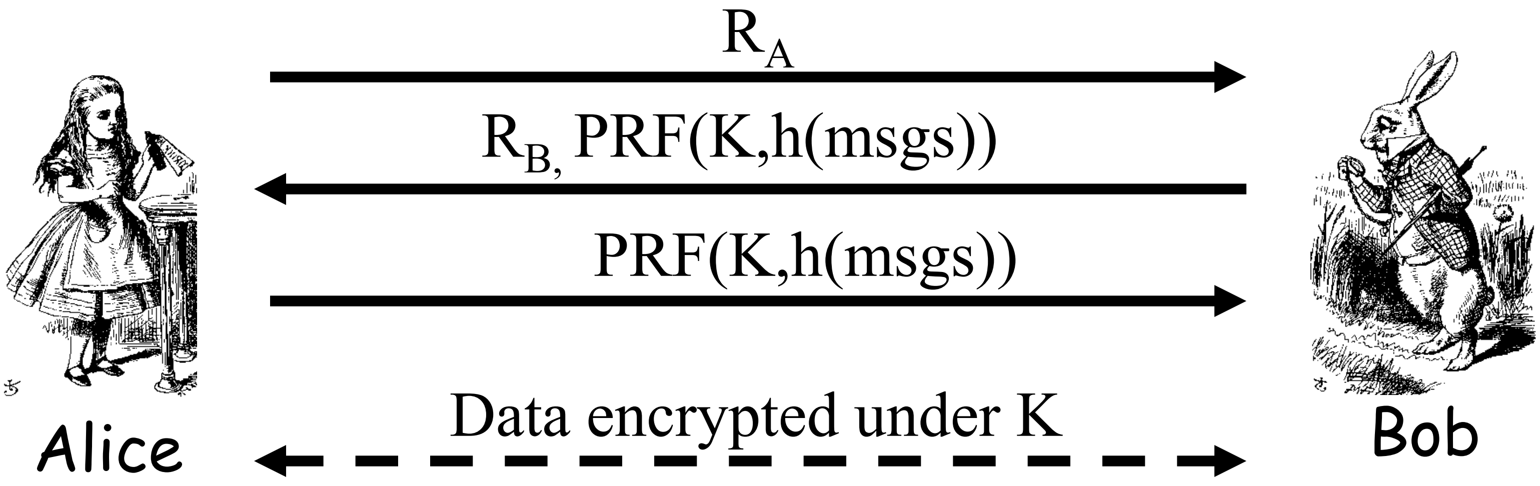
Bob

- S is **randomly chosen by Alice**
- $K = h(S,R_A,R_B)$
- msgs = all previous messages

SSL Sessions vs Connections

- SSL designed for use with HTTP 1.0
- HTTP 1.0 usually opens multiple simultaneous (parallel) **connections**
- SSL session establishment is costly
  - Due to public key operations
- SSL has an efficient protocol for opening new connections given an existing session

SSL Connection



R_A

R_B, PRF(K,h(msgs))

PRF(K,h(msgs))

Data encrypted under K

Alice

Bob

- Assuming SSL **session** exists
- So S is already known to Alice and Bob
- Again, $K = h(S,R_A,R_B)$
- **No public key operations!** (relies on known S)

Comment: SSL/TLS

SSLVerifySignedServerKeyExchange (iOS 7.0.6/OS X 10.9, TLS 1.1, Forward Secrecy)

```
. . .
hashOut.data = hashes + SSL_MD5_DIGEST_LEN;
hashOut.length = SSL_SHA1_DIGEST_LEN;
if ((err = SSLFreeBuffer(&hashCtx)) != 0)
    goto fail;
if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
    goto fail;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;
err = sslRawVerify(...);
. . .
```

Remember Signature verification

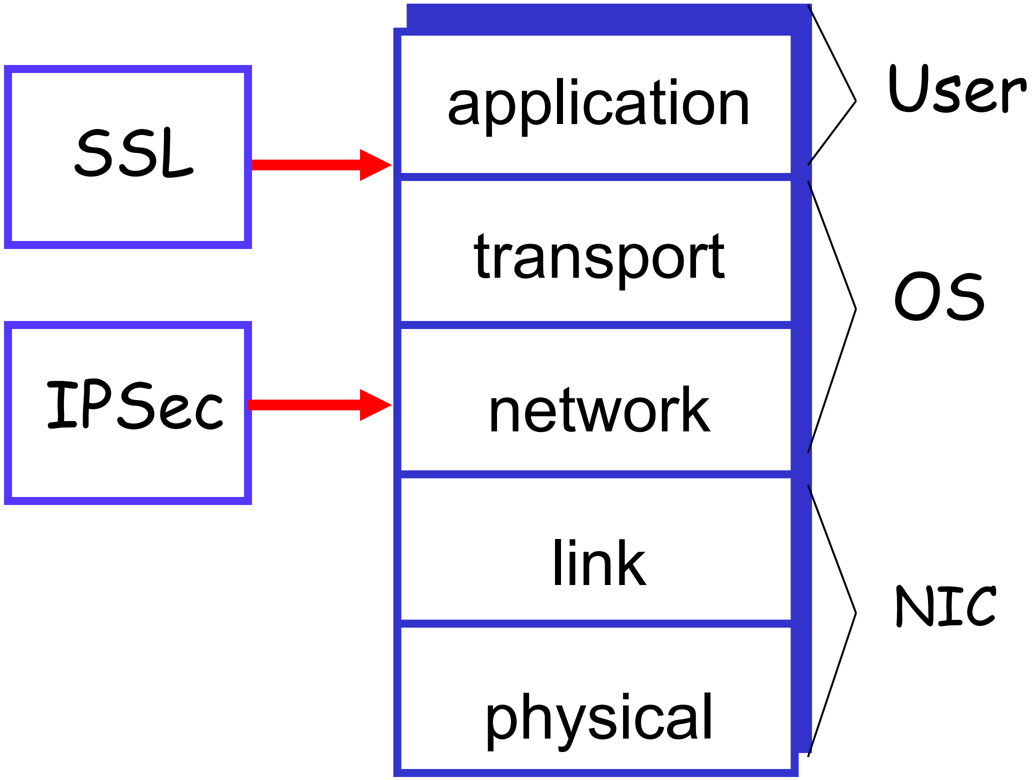
Do hash of data

- Verify signature
  - With hash and public key

IPSec
(Network Layer Security)

IPSec and SSL

- IPSec lives at the network layer
- IPSec is transparent to applications



IKE and ESP/AH

- Two parts to discuss
  1. Establish a session key - IKE
  2. How a secure channel works - ESP or AH

- In SSL, it also has these two parts
  - We have only discussed the first part - establishing a session key
  - We didn' t discuss how the secure channel works

IKE

- ❑ IKE has 2 phases
  - o Phase 1 — master session key setup
  - o Phase 2 — ESP and/or AH key setup
- ❑ Phase 1 is comparable to SSL session
- ❑ Phase 2 is comparable to SSL connection

- ❑ In this course, we don't cover Phase 2

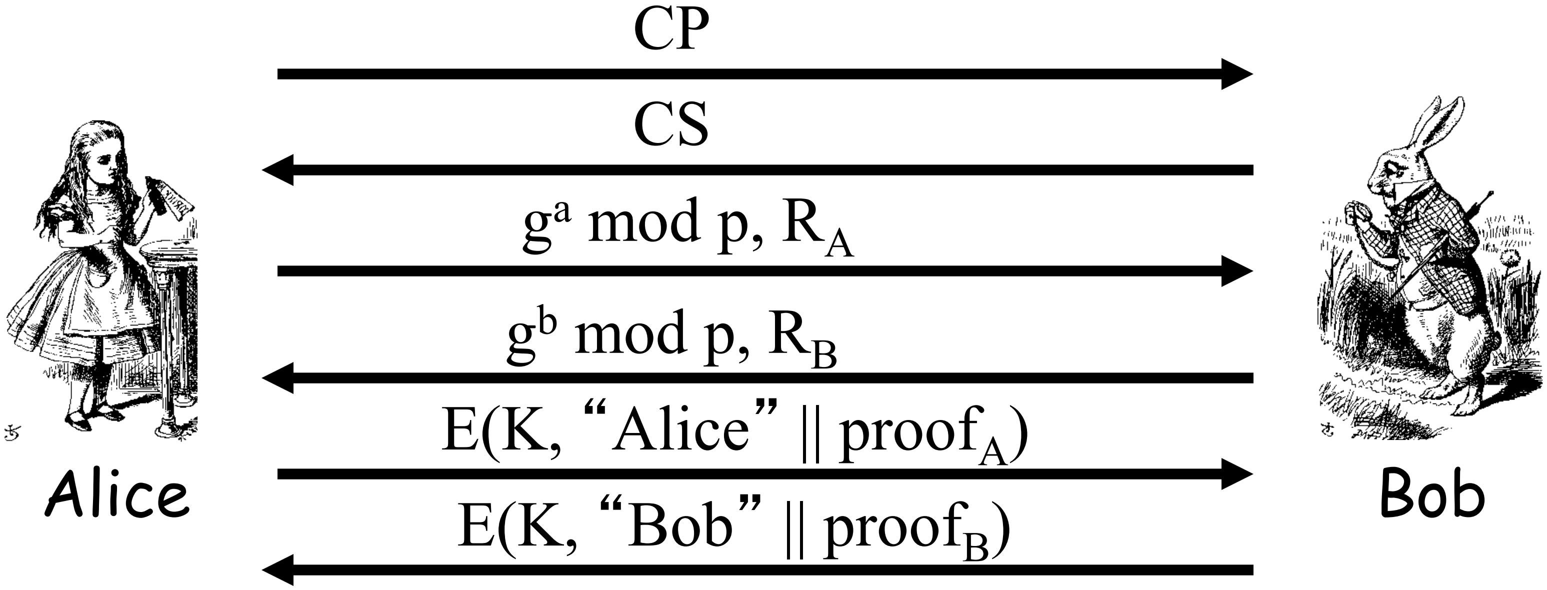
IKE Phase 1

- Three ways to run phase 1
  - Public key encryption based
  - Signature based
  - Symmetric key based
- For each of these, there are two different "modes" to choose from
  - Main mode
  - Aggressive mode
- **There are 6 variants of IKE Phase 1!**
- Evidence that IPSec is over-engineered?

IKE Phase 1

- According to the IKE specification,
  - Main mode **MUST** be implemented
  - Aggressive mode **SHOULD** be implemented
  - In other words, if aggressive mode is not implemented, "you should feel guilty about it"

IKE Phase 1: Signature Based (Main Mode)



CP

CS

$g^a \bmod p, R_A$

$g^b \bmod p, R_B$

E(K, “Alice” || proof_A)

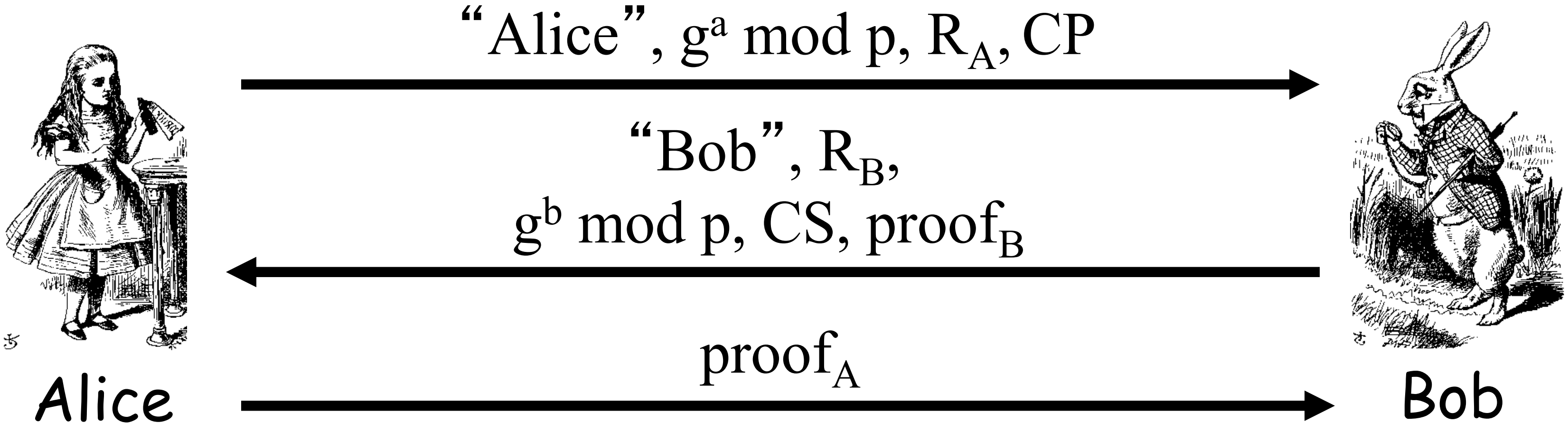
E(K, “Bob” || proof_B)

Alice

Bob

- CP = crypto proposed, CS = crypto selected
- $K = h(g^{ab} \bmod p, R_A, R_B)$
- $\text{SKEYID} = h(R_A, R_B, g^{ab} \bmod p)$
- $\text{proof}_A = [h(\text{SKEYID}, g^a \bmod p, g^b \bmod p, \text{CP}, \text{“Alice”})]_{\text{Alice}}$

IKE Phase 1: Signature Based (Aggressive Mode)



Alice

“Alice”, $g^a \bmod p$, R_A, CP

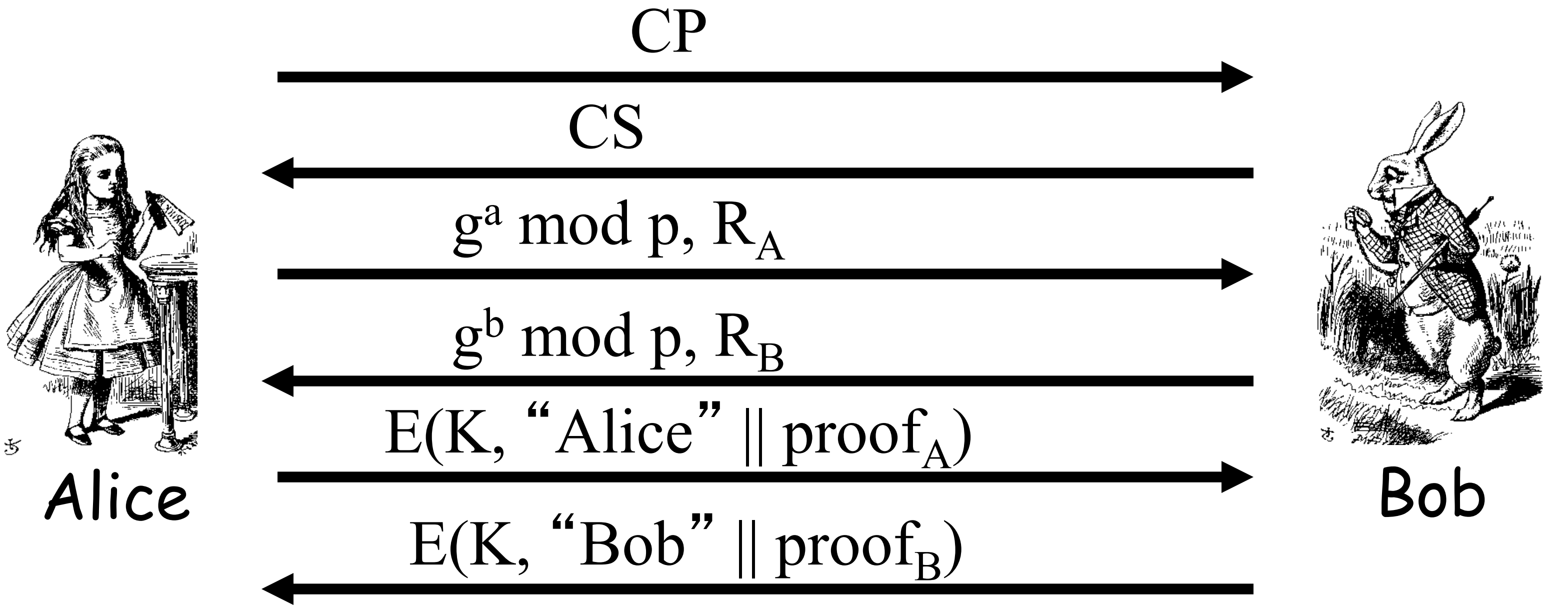
“Bob”, R_B,
$g^b \bmod p$, CS, proof_B

proof_A

Bob

- Main difference from main mode
  - Not trying to protect identities
  - Cannot negotiate g or p

IKE Phase 1: Symmetric Key Based (Main Mode)



Alice

Bob

CP

CS

$g^a \bmod p, R_A$

$g^b \bmod p, R_B$

E(K, "Alice" || proof_A)

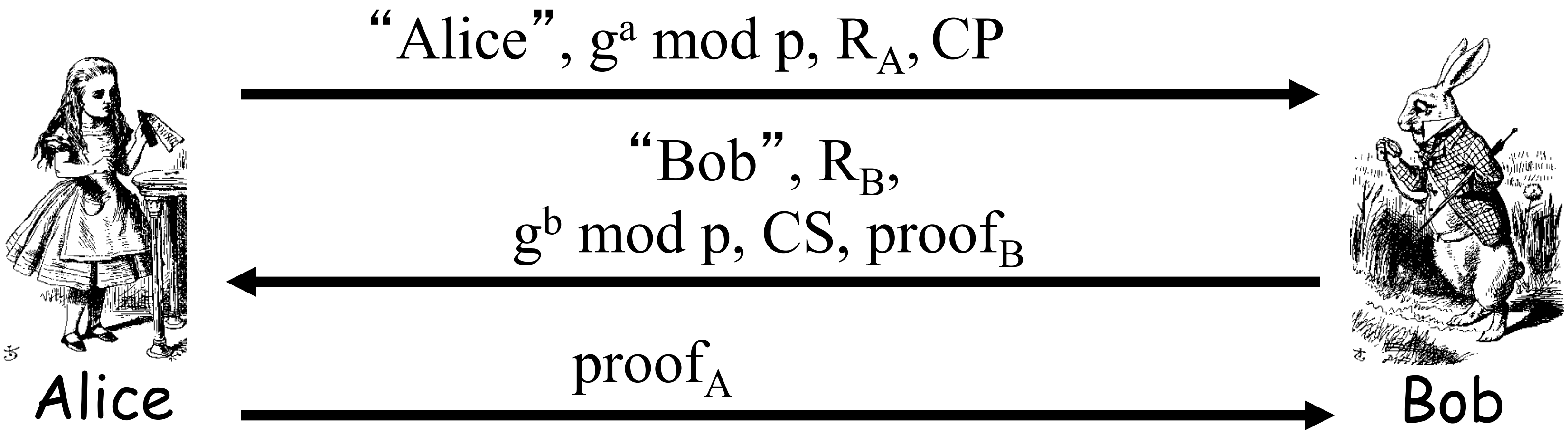
E(K, "Bob" || proof_B)

- K_{AB} = symmetric key shared in advance
- $K = h(g^{ab} \bmod p, R_A, R_B, K_{AB})$
- $\text{SKEYID} = h(K, g^{ab} \bmod p)$
- $\text{proof}_A = h(\text{SKEYID}, g^a \bmod p, g^b \bmod p, \text{CP}, \text{"Alice"})$

Problems with Symmetric Key Based (Main Mode)

- Catch
  - Alice sends her ID in message 5
  - Alice's ID encrypted with K
  - To find K Bob must know K_{AB}
  - To get K_{AB} Bob must know he's talking to Alice!
- Result: **Alice's ID must be IP address!**
- Useless mode for the "road warrior"

IKE Phase 1: Symmetric Key Based (Aggressive Mode)



"Alice", g^a mod p, R_A, CP

"Bob", R_B,
g^b mod p, CS, proof_B

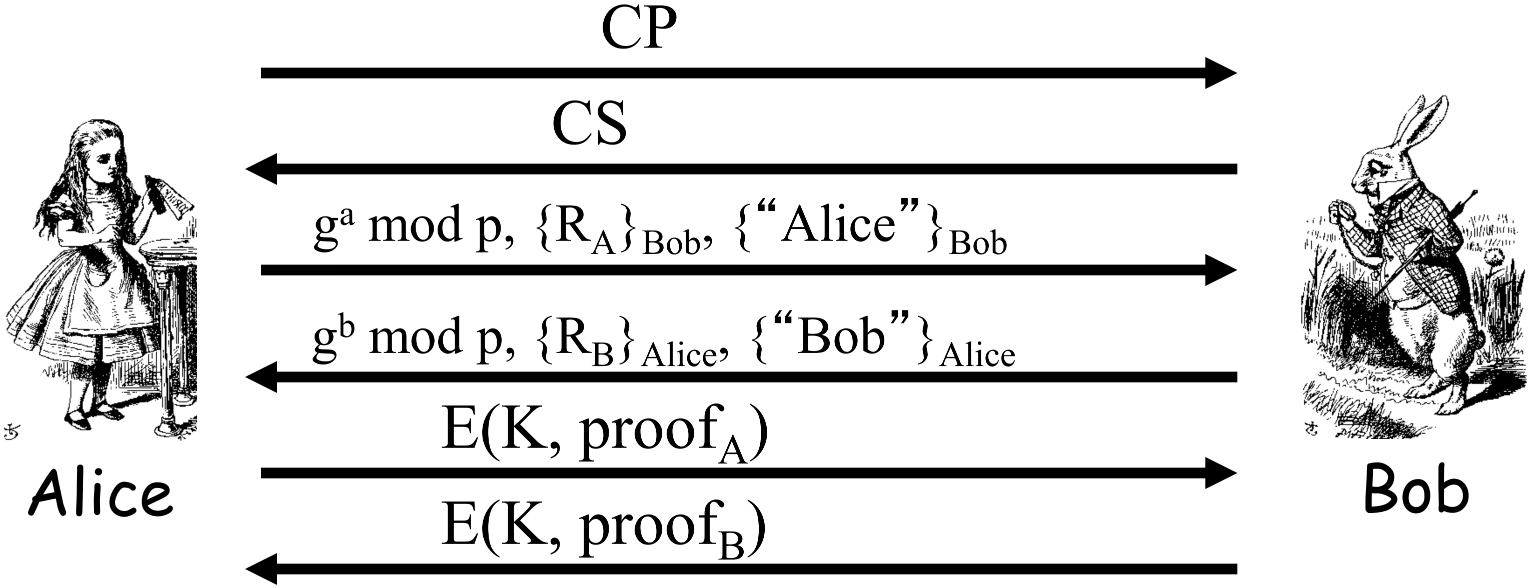
proof_A

Alice

Bob

- Same format as digital signature aggressive mode
- Not trying to hide identities…
- As a result, does **not** have problems of main mode

IKE Phase 1: Public Key Encryption Based (Main Mode)



CP

CS

g^a mod p, $\{R_A\}_{Bob}$, $\{$“Alice”$\}_{Bob}$

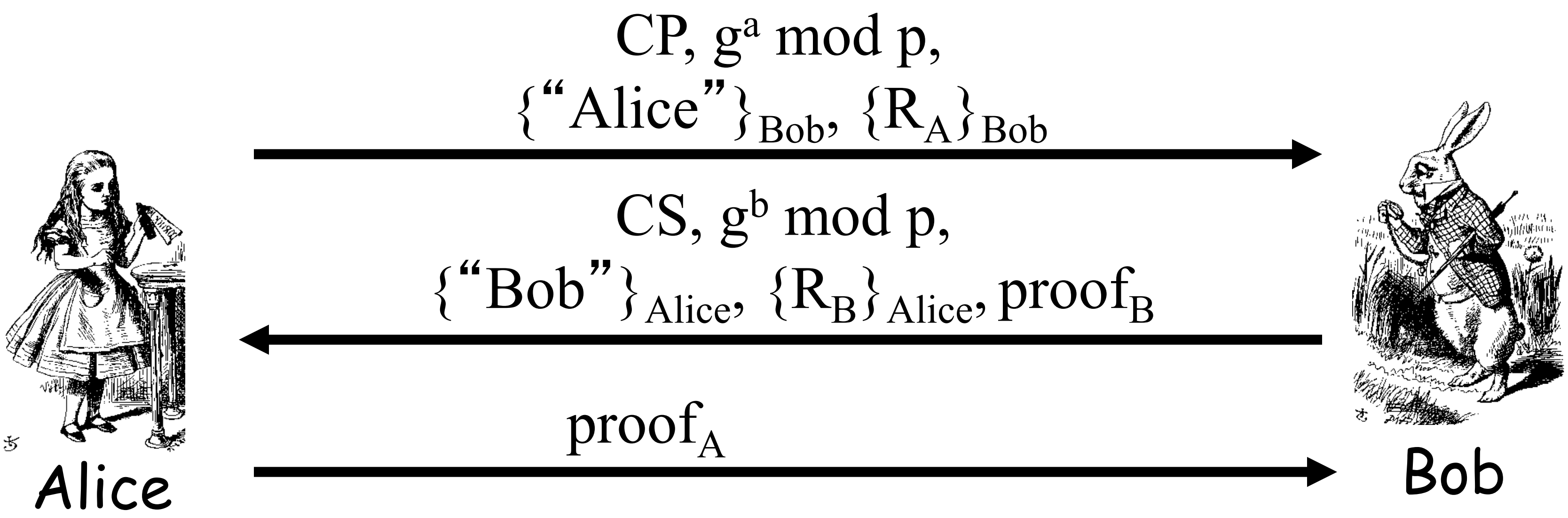
g^b mod p, $\{R_B\}_{Alice}$, $\{$“Bob”$\}_{Alice}$

E(K, proof_A)

E(K, proof_B)

- ❑ K = h(g^{ab} mod p, R_A, R_B)
- ❑ SKEYID = h(R_A, R_B, g^{ab} mod p)
- ❑ proof_A = h(SKEYID, g^a mod p, g^b mod p, CP, “Alice”)

IKE Phase 1: Public Key Encryption Based (Aggressive Mode)



CP, g^a mod p, $\{\text{“Alice”}\}_{\text{Bob}}$, $\{R_A\}_{\text{Bob}}$

CS, g^b mod p, $\{\text{“Bob”}\}_{\text{Alice}}$, $\{R_B\}_{\text{Alice}}$, proof_B

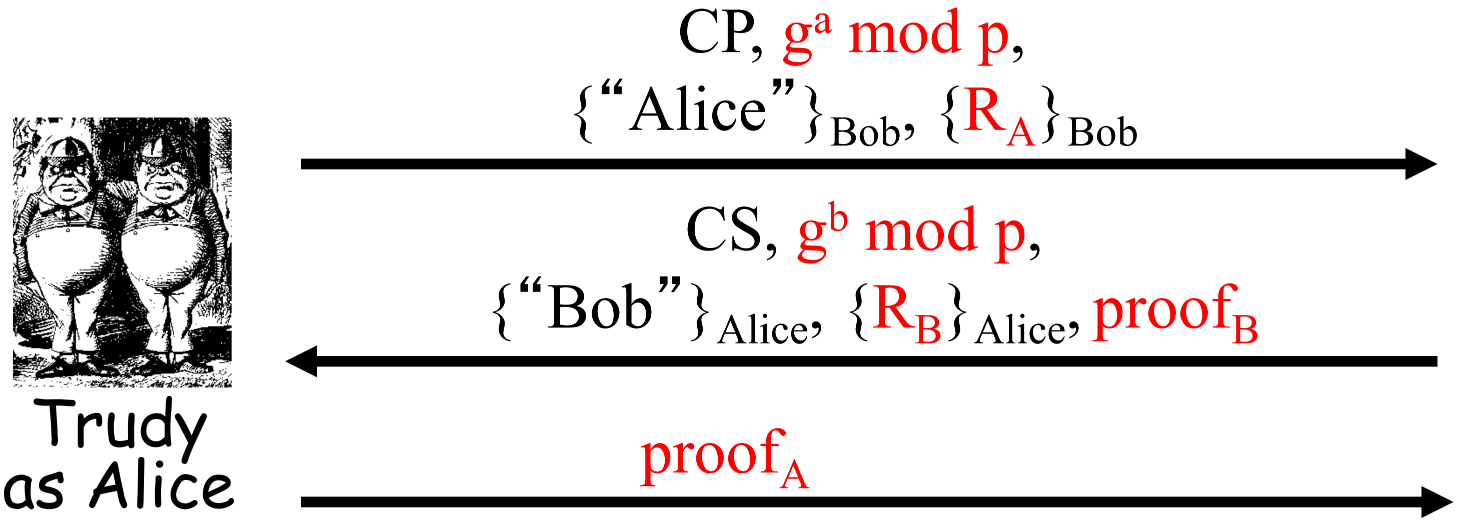
proof_A

- K, proof_A, proof_B computed as in main mode
- Note that identities are hidden
  - The only aggressive mode to hide identities
  - Then why have main mode?

Public Key Encryption Issue?

- Public key encryption, aggressive mode
- Suppose **Trudy** generates
  - Exponents **a** and **b**
  - Nonces $\mathbf{R_A}$ and $\mathbf{R_B}$
- Trudy can compute "valid" keys and proofs: $\mathbf{g^{ab} \bmod p}$, **K**, **SKEYID**, $\mathbf{proof_A}$ and $\mathbf{proof_B}$
- Also true of main mode

Public Key Encryption Issue?



CP, $g^a \bmod p$,
$\{\text{“Alice”}\}_{\text{Bob}}$, $\{R_A\}_{\text{Bob}}$

CS, $g^b \bmod p$,
$\{\text{“Bob”}\}_{\text{Alice}}$, $\{R_B\}_{\text{Alice}}$, proof_B

proof_A

Trudy as Alice

Trudy as Bob

- Trudy can create exchange that appears to be between Alice and Bob
- Appears valid to any observer, **including Alice and Bob!**

Plausible Deniability

- A security failure?
- In this mode of IPSec, it is a feature!
  - **Plausible deniability:** Alice and Bob can deny that any conversation has taken place!
- In some cases it might be a security failure
  - If Alice makes a purchase from Bob, she could later repudiate it (unless she had signed)

How IPSec Secure Channel Works

- After IKE Phase 1, we have a master session key
- After IKE Phase 2, we have keys for ESP and AH
- Now what?
  - We want to protect IP datagrams by giving them confidentiality and message authentication (a.k.a. integrity)

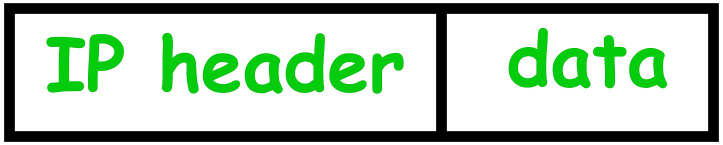
ESP and AH

- Two Encapsulation modes
  1. Transport mode
  2. Tunnel mode

- Two Protocols
  - AH – Authentication Header – support message authentication only
  - ESP – Encapsulating Security Payload
    1. Encryption only
    2. Encryption with message authentication

IP Review

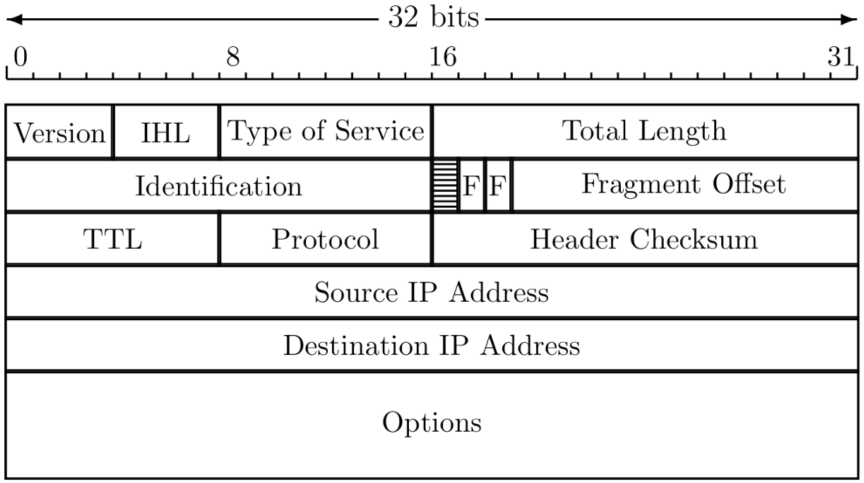
- IP datagram is of the form



IP header

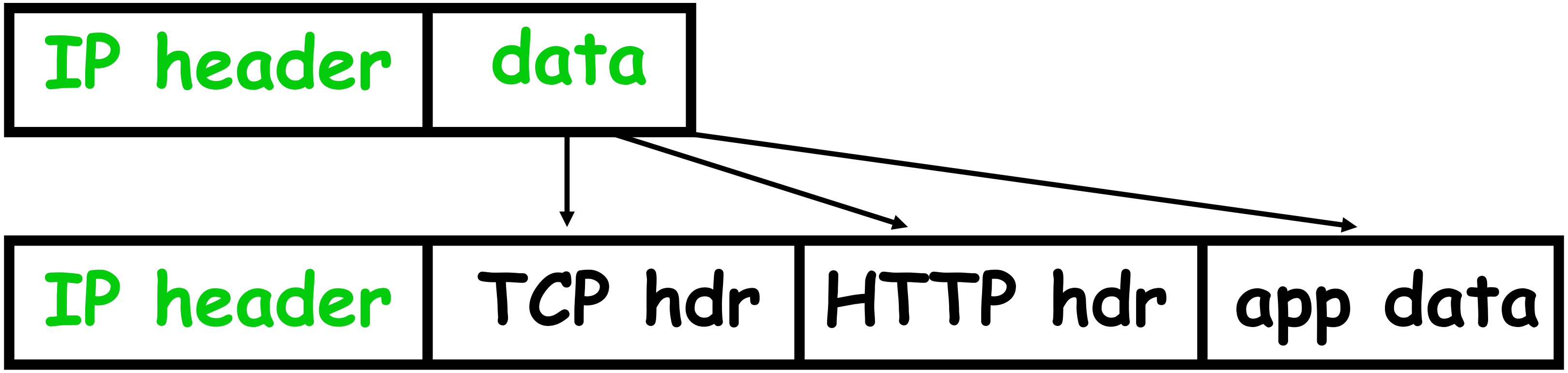
data

- Where IP header is



IP and TCP

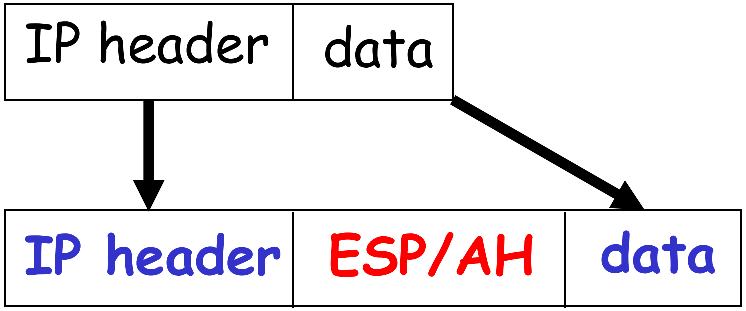
- Consider HTTP traffic (over TCP)
- IP encapsulates TCP
- TCP encapsulates HTTP

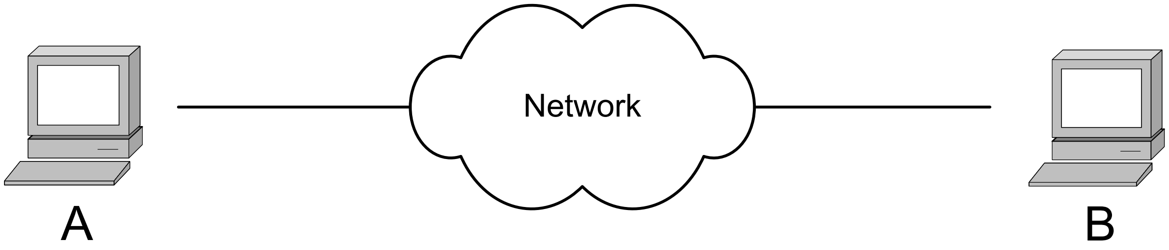


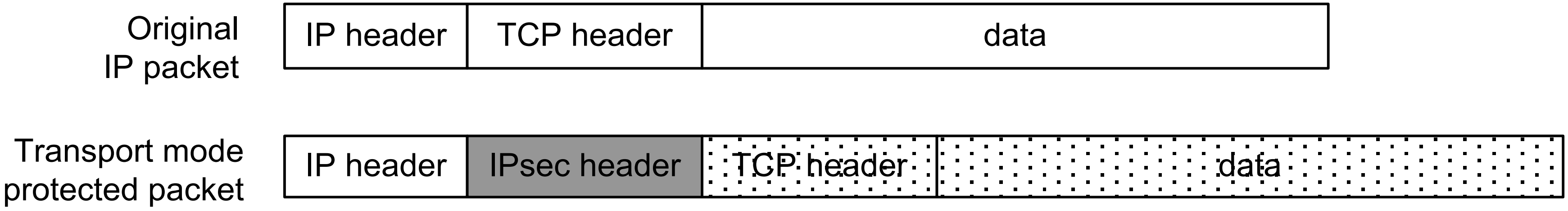
- IP **data** includes TCP header, etc.

IPSec Transport Mode

- Transport mode designed for host-to-host
- The original header remains
    - Passive attacker can see who is talking

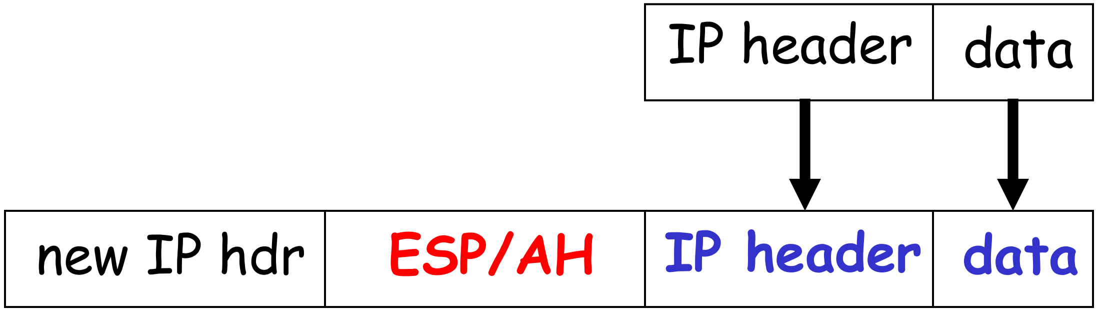






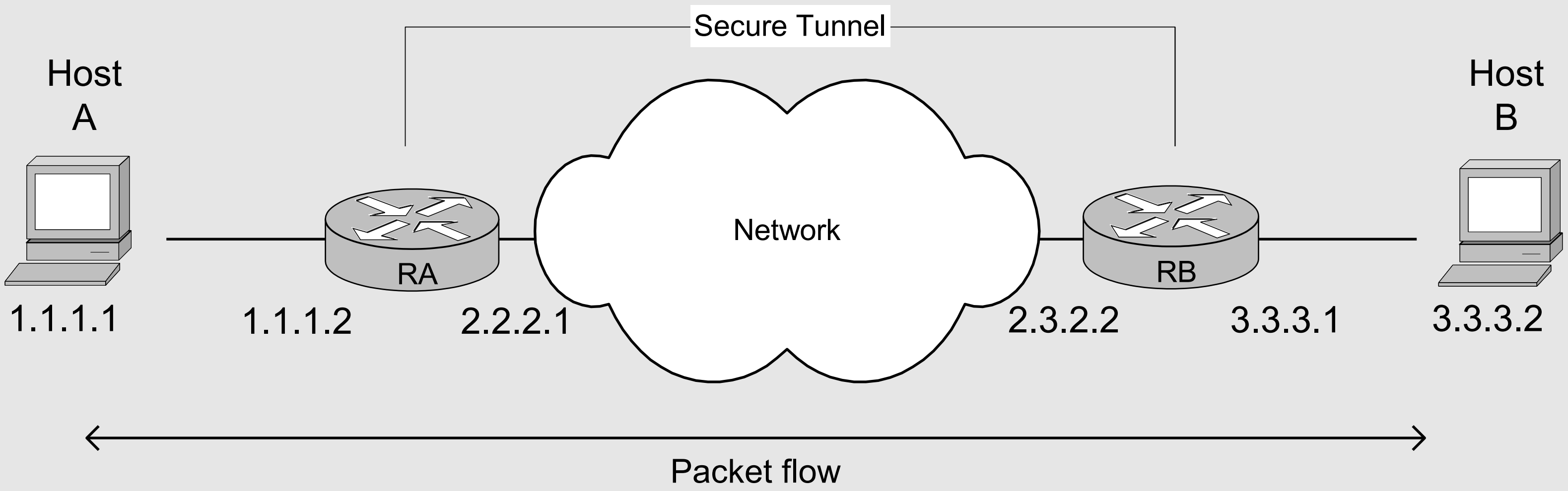
IPSec Tunnel Mode

- IPSec **Tunnel Mode**



- Tunnel mode for gateway to gateway VPN
- Original IP packet encapsulated in IPSec
- Original IP header not visible to attacker
  - New header from firewall to firewall
  - Attacker does not know which hosts are talking

Tunnel mode
(Router-to-router / Gateway-to-gateway)

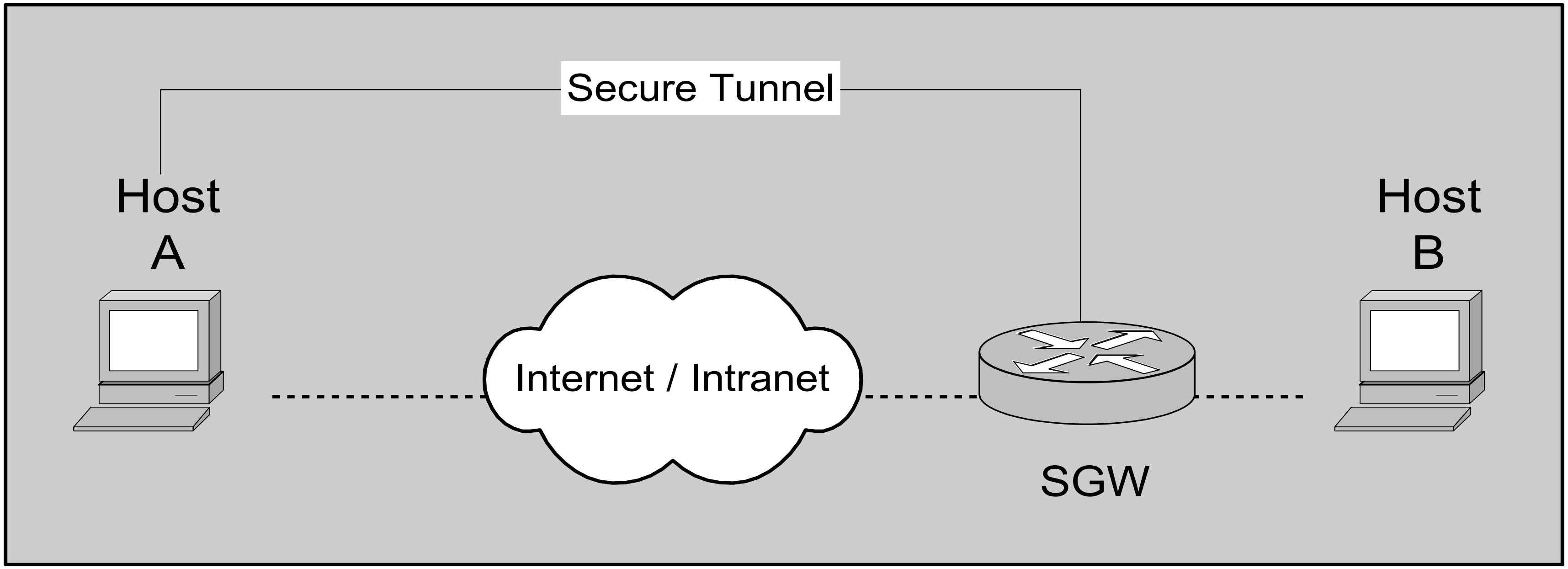


Nested packet format

IP header	IPsec header	IP header	TCP header	data

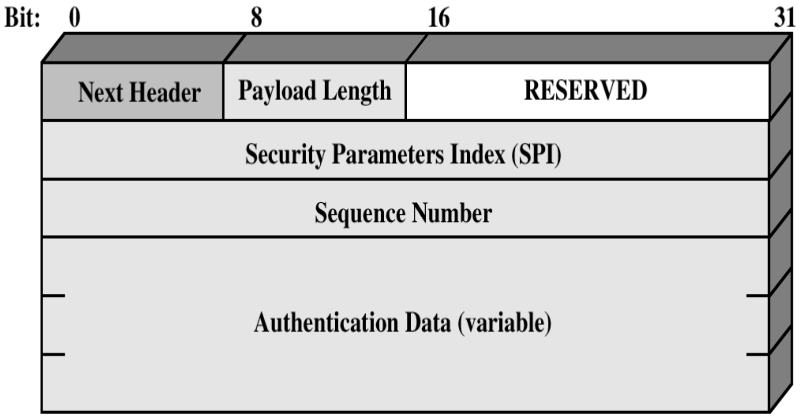
Src = 2.2.2.1
Dst = 2.3.2.2
		Src = 1.1.1.1
		Dst = 3.3.3.2		

Tunnel mode
(Host-to-Router / Remote Access)



AH and ESP

- Authentication Header (AH)
  - Provides message authentication.
  - Next header: TCP, UDP, etc.


Bit:
0
8
16
31
Next Header
Payload Length
RESERVED
Security Parameters Index (SPI)
Sequence Number
Authentication Data (variable)

IPSec Authentication Header

- Encapsulating Security Payload (ESP)
  - Provides confidentiality and authentication. Either is optional.
  - Either encryption or authentication (or both) must be enabled

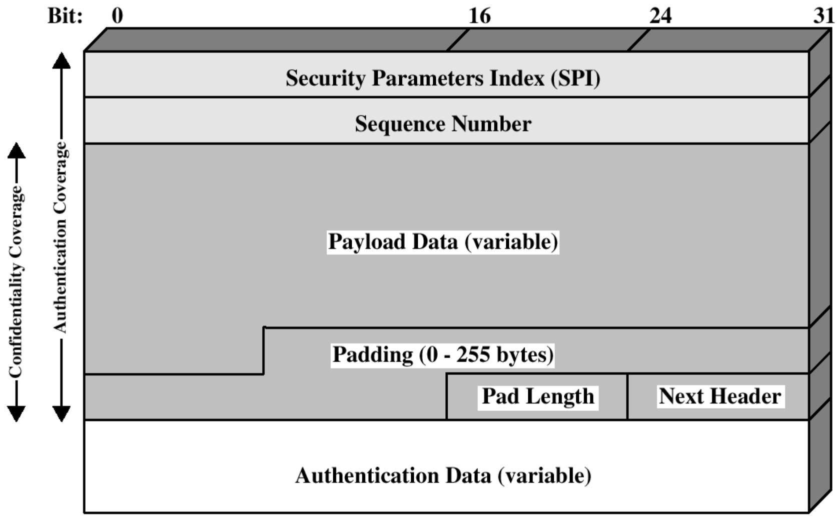
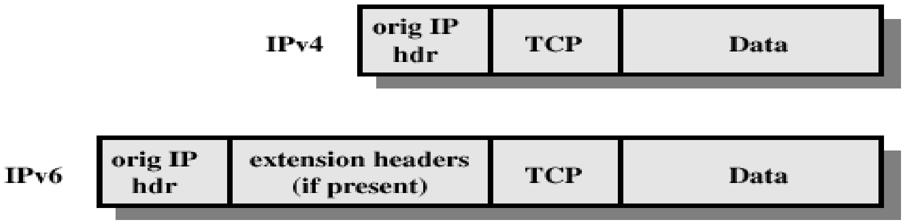


Figure 6.7 IPSec ESP Format

Authentication Header (AH) Protocol

- Original IP packets



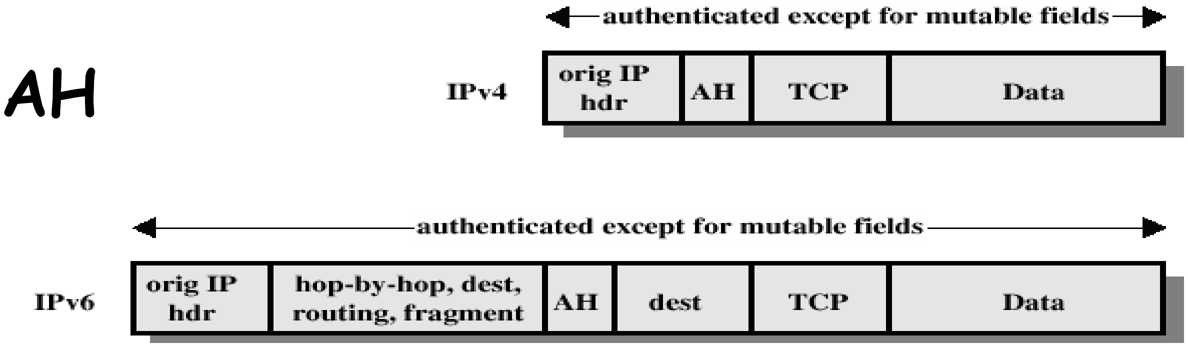
IPv4

orig IP hdr	TCP	Data

IPv6

orig IP hdr	extension headers (if present)	TCP	Data

- Transport Mode AH
  - Host-to-host authentication



authenticated except for mutable fields

IPv4

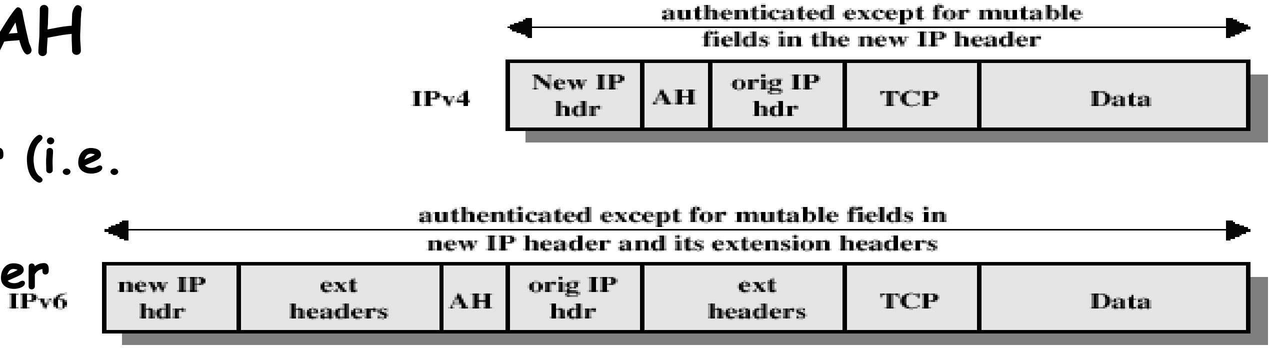
orig IP hdr	AH	TCP	Data

authenticated except for mutable fields

IPv6

orig IP hdr	hop-by-hop, dest, routing, fragment	AH	dest	TCP	Data

- Tunnel Mode AH
  - Host-to-host
  - Host-to-router (i.e. remote access)
  - Router-to-router



authenticated except for mutable fields in the new IP header

IPv4

New IP hdr	AH	orig IP hdr	TCP	Data

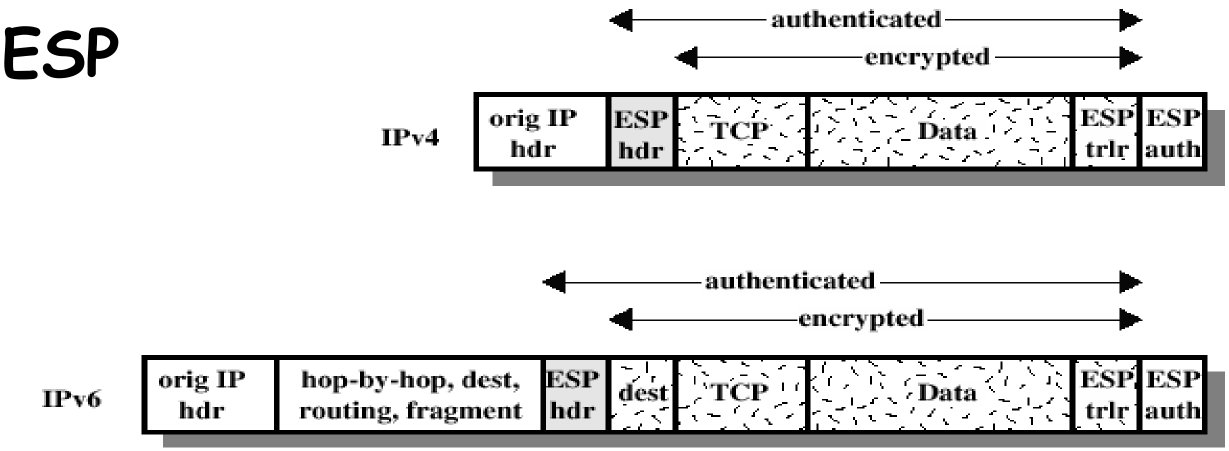
authenticated except for mutable fields in new IP header and its extension headers

IPv6

new IP hdr	ext headers	AH	orig IP hdr	ext headers	TCP	Data

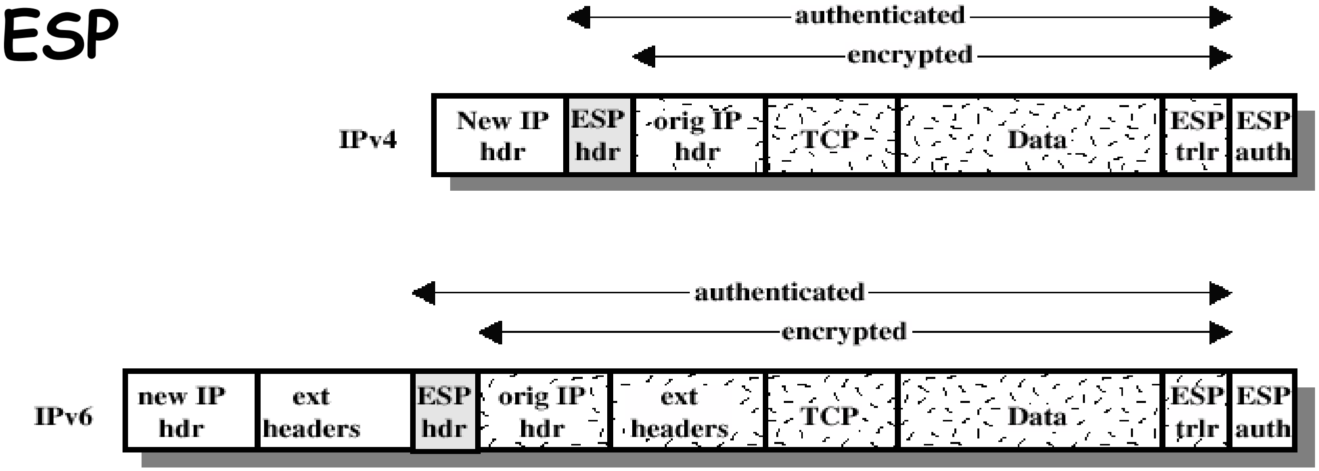
Encapsulating Security Payload (ESP) Protocol

- Transport Mode ESP



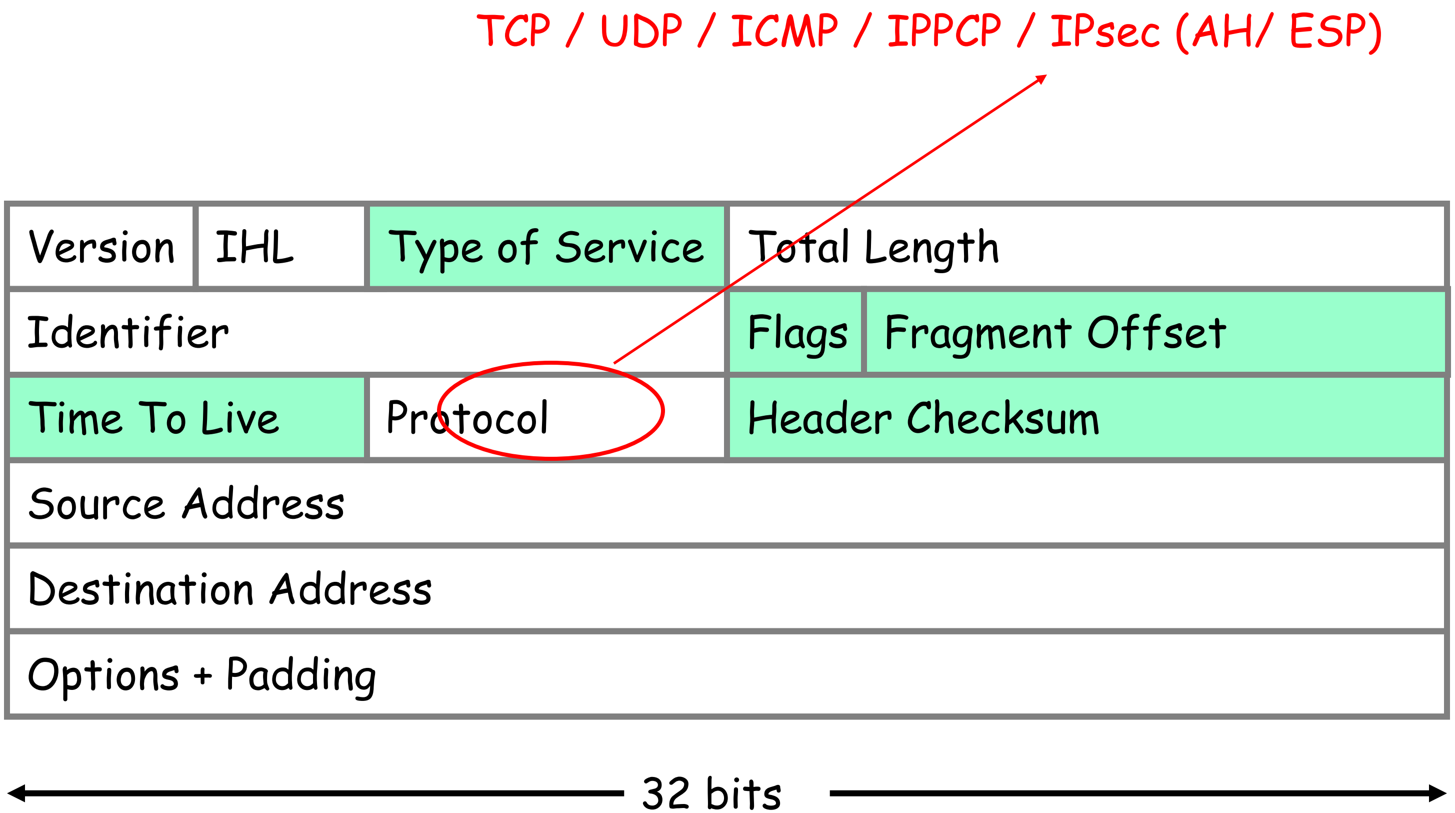
(a) Transport Mode

- Tunnel Mode ESP



(b) Tunnel Mode

IPv4 header



TCP / UDP / ICMP / IPPCP / IPsec (AH/ ESP)

Version | IHL | Type of Service | Total Length

Identifier | Flags | Fragment Offset

Time To Live | Protocol | Header Checksum

Source Address

Destination Address

Options + Padding

32 bits

- Note the mutable and immutable fields of an IPv4 header

Why Does AH Exist?

- No confidentiality
- AH authenticates **immutable fields** in IP header only
  - TTL, for example, must change
- ESP can provide both confidentiality and integrity (not of the IP header)

Mobile Network Security

Cell Phones

- First generation cell phones
  - Analog
  - Little or no security
  - Susceptible to **cloning**
- Second generation cell phones: **GSM**
  - Began in 1982 as Groupe Speciale Mobile
  - Now, Global System for Mobile Communications
- Third generation
  - 3rd Generation Partnership Project (3GPP)

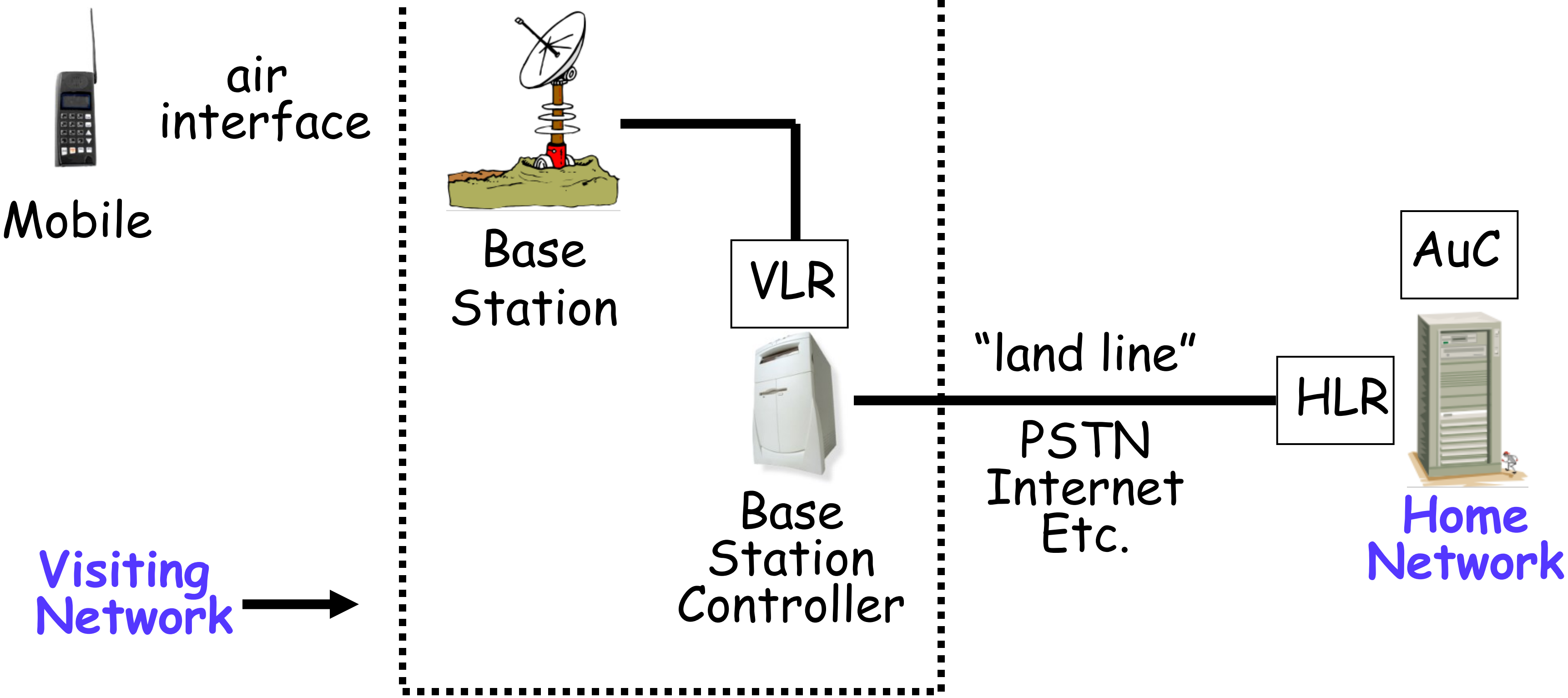
Security Requirements

- Service Providers' perspective:
  - Only legitimate subscribers can access the network
    - Soln: fight against cloning
  - Service providers have ***no*** interest on ***who*** is using the SIM (subscriber identity module) card.
  - Make SIM difficult if not impossible to clone.
  - Make sure that SIM card associating with a 15-digit IMSI (International Mobile Subscriber Identity) is valid:
    - Registered
    - Authenticated

Security Requirements – what Users want

- Data Confidentiality
  - keep one's conservation secret by scrambling digitized data
- Anonymity
  - Hide the identity of the SIM card and prevent from tracking the SIM card when it roams from one network to another.
- Adversaries
  - eavesdroppers
  - service providers
  - Can GSM provide data confidentiality and anonymity against these two types of enemies?
- Prevent malicious users from using your phone
  - Misuse: Phone lock (password/gesture)
  - Stolen: GSM's EIR (Equipment Identity Register)
    - stores all IMEIs (Intl Mobile Equipment Identities)
    - black list of stolen (or locked) devices

Mobile System Overview



Mobile

air interface

Base Station

VLR

Base Station Controller

"land line"

PSTN Internet Etc.

HLR

AuC

Home Network

Visiting Network

GSM System Components

- Mobile phone
    - Contains SIM (Subscriber Identity Module)
- SIM is the **security module**
    - IMSI (International Mobile Subscriber ID)
    - User key Ki (128 bits)
    - Tamper resistant (smart card)

GSM System Components

- **Visiting network** — network where mobile is currently located
  - Base station — one "cell"
  - Base station controller — manages many cells
  - VLR (Visitor Location Register) — info on all visiting mobiles currently in the network
- **Home network** — "home" of the mobile
  - HLR (Home Location Register) — keeps track of most recent location of mobile
  - AuC (Authentication Center) — contains IMSI/Ki

GSM: Anonymity

- IMSI used to initially identify caller
- Then TMSI (Temporary Mobile Subscriber ID) used
- TMSI changed frequently
- TMSI's encrypted when sent
- Not a strong form of anonymity
- But probably sufficient for most uses

GSM: Authentication

- Caller is authenticated to base station
- Authentication is **not** mutual
- Authentication via **challenge-response**
  - AuC generates RAND and computes XRES = A3(RAND, Ki) where A3 is a hash
  - Then (RAND,XRES) are sent to base station
  - Base station sends **challenge** RAND to mobile
  - Mobile's **response** is SRES = A3(RAND, Ki)
  - Base station verifies SRES = XRES
- **Note:** Ki never leaves AuC!

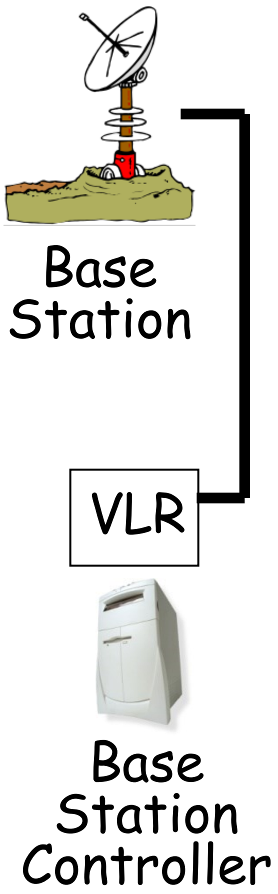
- The response length should be long enough to discourage online guessing. E.g. 32 bits
- Random challenge should be long enough to reduce the chance of generating repeated challenge numbers. E.g. 128 bits

GSM: Confidentiality

- Data encrypted with stream cipher, A5
- Encryption key Kc
  - AuC computes Kc = A8(RAND, Ki), where A8 is a hash
  - Then Kc is sent to base station with RAND
  - Mobile computes Kc = A8(RAND, Ki) after receiving RAND
  - The value of RAND is the same as the one used for authentication
  - Keystream generated from A5(Kc)
- **Note:** Ki never leaves home network!
- Ki is 128 bits long
- Kc is 64 bits long

GSM Insecurity (1)

- Hash used in A3/A8:
  - Broken after 160,000 chosen plaintexts
  - With SIM, can get Ki in 2 to 10 hours
- Encryption between mobile and base station but **no encryption** from base station to base station controller
  - When transmitted over microwave link…
- Encryption algorithm A5/1
  - Broken with 2 seconds of known plaintext



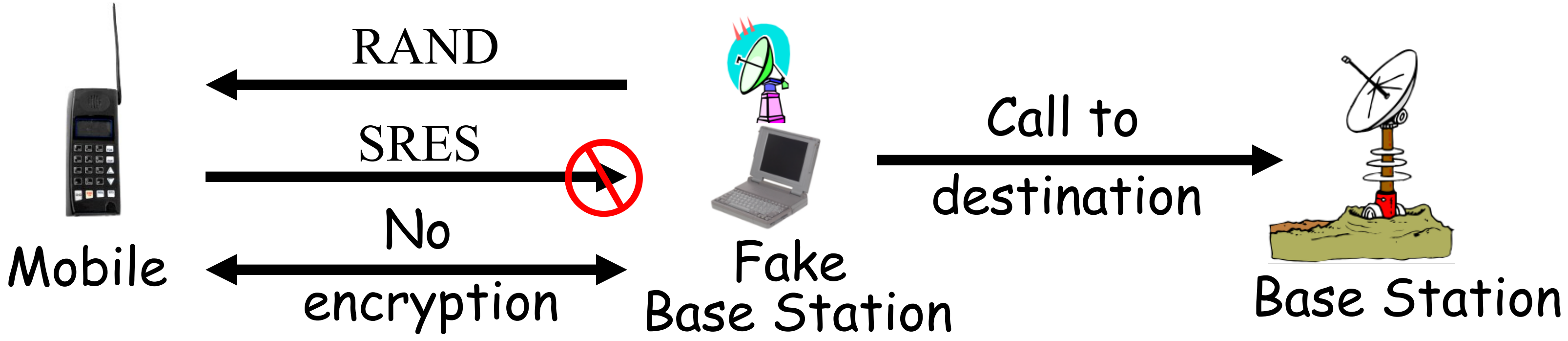
Base Station

VLR

Base Station Controller

GSM Insecurity (2)

- **Fake base station** exploits two flaws
  - Encryption not automatic
  - Base station not authenticated



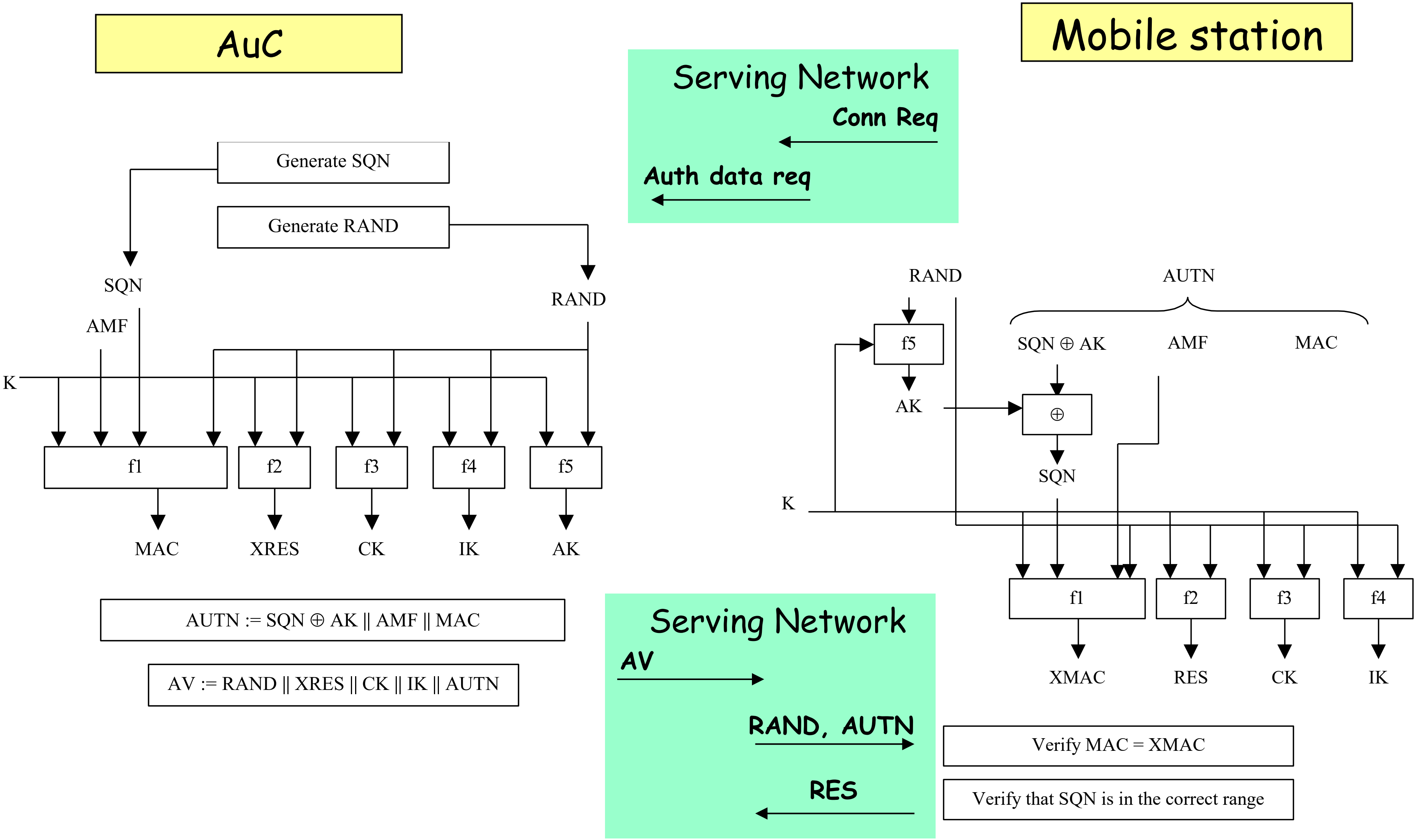
GSM Conclusion

- Did GSM achieve its goals?
  - Eliminate cloning? **Somehow…**
  - Make air interface as secure as PSTN? **Perhaps…**
  - But design goals were clearly too limited
- GSM insecurities — weak crypto, fake base station, replay, etc.
- PSTN insecurities — tapping
- No integrity check (no message authentication)

3GPP: 3rd Generation Partnership Project

- 3G fixes known GSM security problems
  - Mutual authentication
  - Keys (encryption/integrity) cannot be reused
  - Triples cannot be replayed
  - Strong encryption algorithm (AES)
  - Message authentication
  - Encryption extended to base station controller
- http://www.3gpp.org

3GPP - AKA (Authentication and Key Agreement)



AUTN := SQN ⊕ AK || AMF || MAC

AV := RAND || XRES || CK || IK || AUTN

Verify MAC = XMAC

Verify that SQN is in the correct range

3GPP - AKA Details

K, CK, IK	128 bits
RAND	128 bits
RES	32 - 128 bits
AUTN	128 bits
SQN, AK	48 bits
Concealment of SQN by AK is optional: prevent serving network from knowing the value of SQN?	
AMF (authentication management field)	16 bits
MAC (message authentication code)	64 bits

- CK is used for encryption
- IK is used for integrity check (message authentication)
- f1, f2, f3, f4, f5 are based on the AES block cipher (Rijndael)
  - Consider them as distinct one-way functions
- Both encryption and integrity check algorithms are also based on the AES

WLAN Security

Introduction

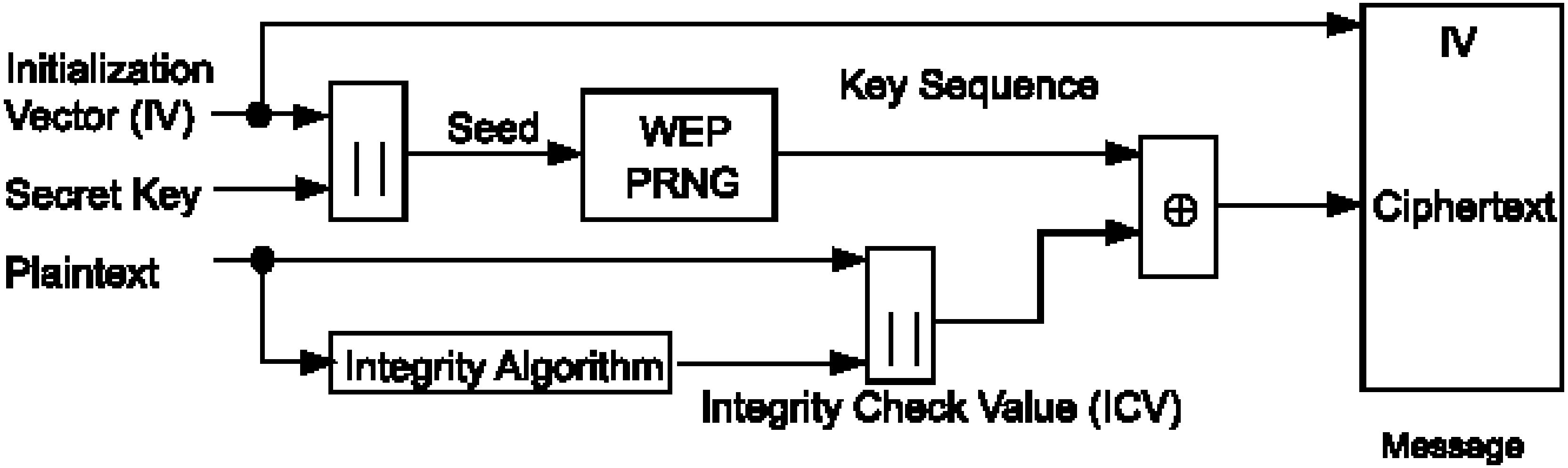
- Everyone uses wireless networks…
- Topologies:
  - Infrastructure: Access Point (AP) serves as a 'hub' for wireless clients (star topology)
  - Ad Hoc: peer to peer (mesh topology)
- IEEE 802.11 standard defines
  - an authentication scheme and
  - a Wired Equivalent Privacy (WEP) algorithm
- Wi-Fi Alliance creates
  - class of Wi-Fi Protected Access (WPA and WPA2) systems
- The authentication scheme
  - one-way authentication (simple challenge-response)
- WEP, WPA & WPA2
  - Data confidentiality
- Symmetric key based

Key Management

- IEEE 802.11 does not specify any key management scheme
- The secret, shared key (as in the Shared Key Authentication above) is presumed to have been delivered to participating wireless stations (both the laptop and the AP) via a secure channel that is independent of IEEE 802.11.
- Vendors have implemented their own proprietary, and out-of-band mechanism to establish the shared keys.
- What's the common practice nowadays?...
  - Manually key in the key.

WEP

- WEP encipherment block diagram



- Secret Key: 40 bits or 104 bits
  - Distributed to communicating entities (wireless stations and access points) via external key management service (e.g. manually key in)
- Integrity Algorithm
  - CRC-32
- WEP PRNG
  - RC4
  - Initialized by Seed
  - Outputs a long binary stream called Key Sequence

WEP Weaknesses

- 2001: WEP was broken. Attacking Principles
  - The first byte of an encrypted message is always equal to 0xAA. Hence the first byte of key sequence is always obtainable.
  - For some special pattern of the 24-bit IV, one can deduce one byte of the secret key at one time. When enough IVs and ciphertexts have been collected, all bytes of the secret key can be obtained.
- Several other weaknesses have been identified since the publication of the algorithm.
  - Static key (difficult to update), weak linear (CRC) integrity
- Open-source cracking software is now available on the Internet.
  - AirSnort (http://airsnort.shmoo.com)
  - WEPcrack (http://wepcrack.sourceforge.net/)
  - Aircrack (http://aircrack-ng.org/doku.php)

Solutions

- Higher protocol level solutions
  - Application layer authentication
  - Encryption with IPSec or PPTP (use VPN)
  - Important websites should have HTTPS

- Improve Wi-Fi Protected Access
  - Dynamically varying encryption keys
  - Use stronger encryption algorithm

WPA/WPA2

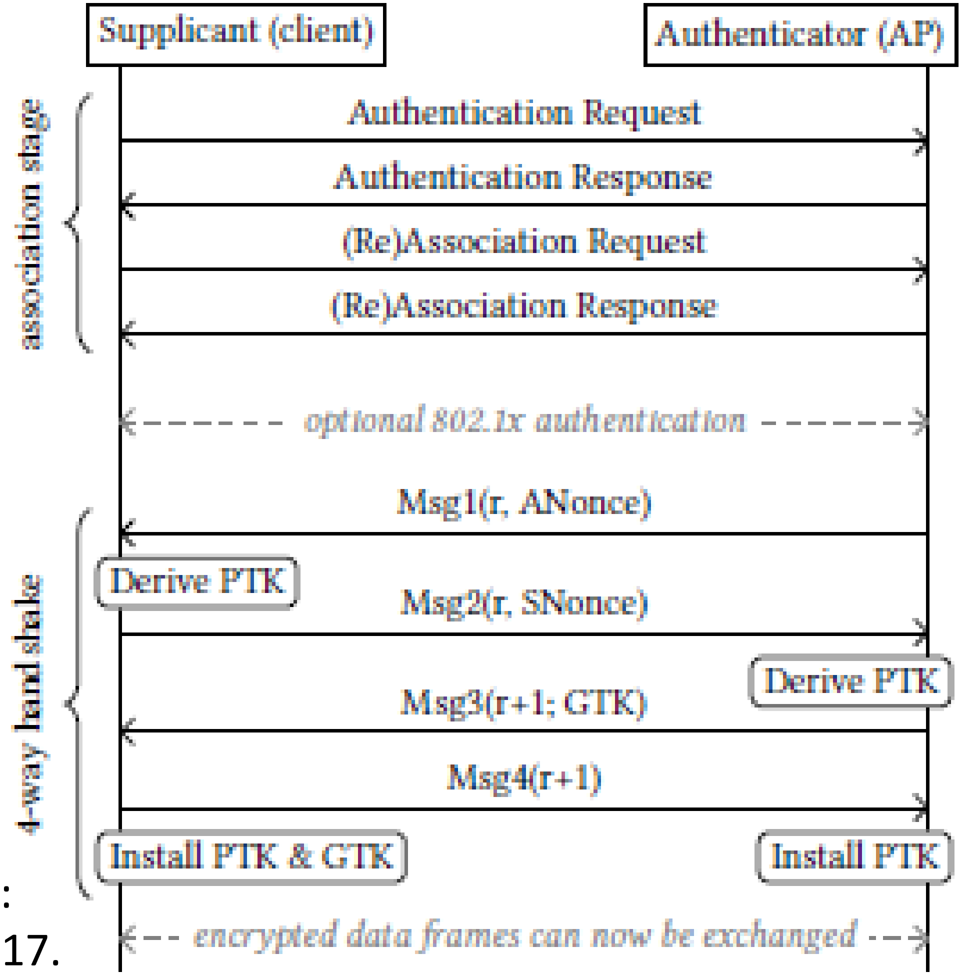
- Created by the Wi-Fi Alliance; supersedes WEP in 2003

- WPA (go for very regular key changes)
  - 802.1x with Extensible Authentication Protocol (EAP) for authentication
    - Allows for session keys
  - Temporal Key Integrity Protocol (TKIP) for encryption
    - Dynamically generated 128-bit key (updated ±10,000 packets)
    - Still uses RC4 stream cipher (WPA)
  - Proprietary Michael integrity check algorithm

- WPA2 (go for stronger cryptography and session keys)
  - CCMP (IEEE 802.11i)
    - AES (still operating like a stream cipher in Counter Mode)
    - CBC-MAC for integrity
  - GCMP (802.11ad)
    - AES in GCM mode (Galios/Counter Mode)
    - GHASH for integrity
  - Allows alternative to have a password shared between an AP and a user (Pre-shared key "WPA2-PSK" mode)

WPA2-PSK KRACK (basic)

- WPA2 has a four-way key establishment handshake
  - Pairwise Transient Key (PTK)
  - Groupwise Transient Key (GTK)
- CCMP/GCMP only secure if IV does not repeat
  - CCMP (IV = MAC/48-bit Nonce)
  - GCMP (IV = MAC/48-bit Nonce)
- KRACK
  - Replay Msg3
  - Allowed: Msg3 might have error
  - Key reinstalled..
  - …but nonce also reset
  - Encrypted data reusing old IV
- Some OS/WPA2 version
  - Reinstall cause key = 0
- Large scale patching…



Vanhoef and Piessens. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2, ACM CCS, Nov 2017.

DoS and DDoS

Defining DoS

"A transient or persistent set of actions by a third party preventing authorised users from access to or use of a resource or service"

- Although this definition assumes that a DoS is the result of actions by a third party, these need not be malicious
  - Resources may also simply become exhausted by legitimate users (flash crowds)
  - Where malicious agency can be established, this is referred to as a DoS attack

Consumption of Scarce Resources

- Network connectivity
  - To prevent hosts or networks from communicating on the network
  - Does not depend on the attacker being able to consume your network bandwidth. For example, the attacker consumes local resources on a server involved in establishing a network connection.
- Bandwidth consumption
  - Consume all the available bandwidth on your network by generating a large number of packets directed to your network.

ICMP Echo or Ping Flooding

- Uses common diagnostic tool *ping*
- *ping* is a simple loopback test that sends an *ICMP Echo* to a host which responds with an *ICMP Echo Reply*
- In the Ping Flooding Attack, attacker floods victim with *IP Ping packets*
- *Ping of Death* send oversized ping message
  - The attacker constructs datagrams that appear to be fragments from a single datagram
  - The sum of the sizes of these fragment datagrams is greater than 2^16
  - When the recipient puts the fragments together and copies the resulting datagram to a buffer an overflow occurs
    - Unpredictable result(System crash? Overflow exploit?)

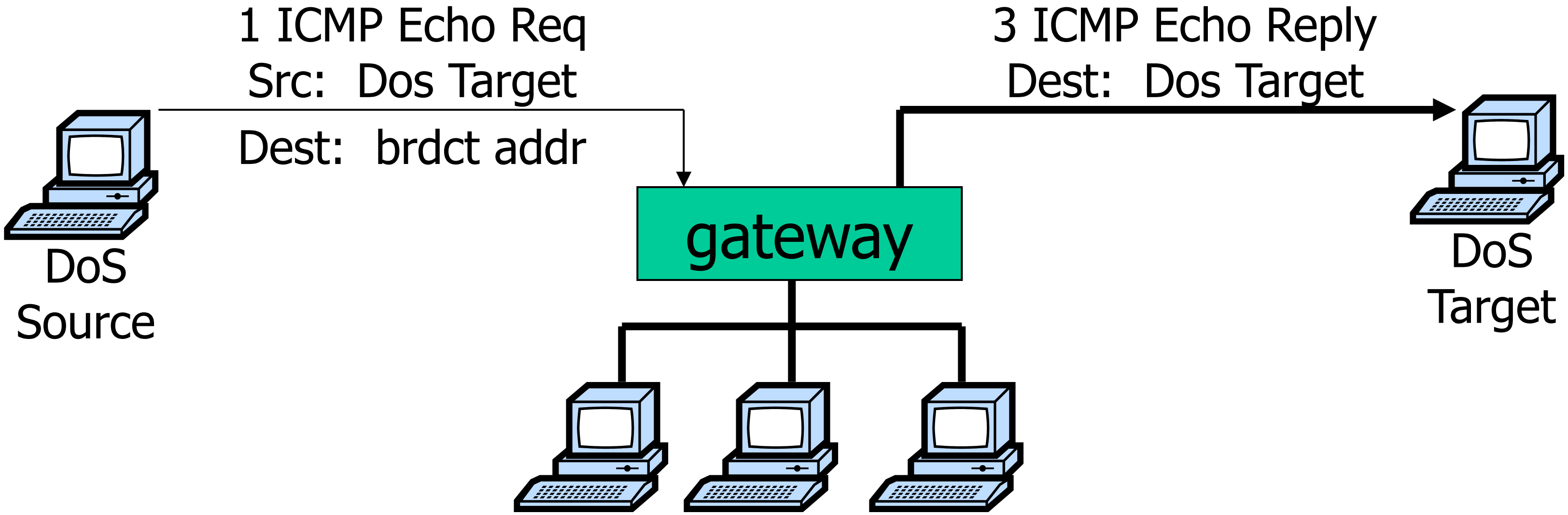
Consumption of Scarce Resources

- Consumption of other resources
  - State storage/processing structures (TCP SYN)
  - Consume disk space (large anonymous ftp uploads)
  - Disrupt specific person's resource (email bombs)
  - Power (forced to remain resource-intensive state)
  - Security features (Login attempts?)

Effort Amplification

- Key concept for DoS attacker is resource amplification
  - The factor between the effort expended by an attacker and effort required of a victim during the attack
  - Sending a file vs verifying signature of file or parsing (XML) file
  - Smurf attack: Send single message vs receive many messages

Smurf Attack

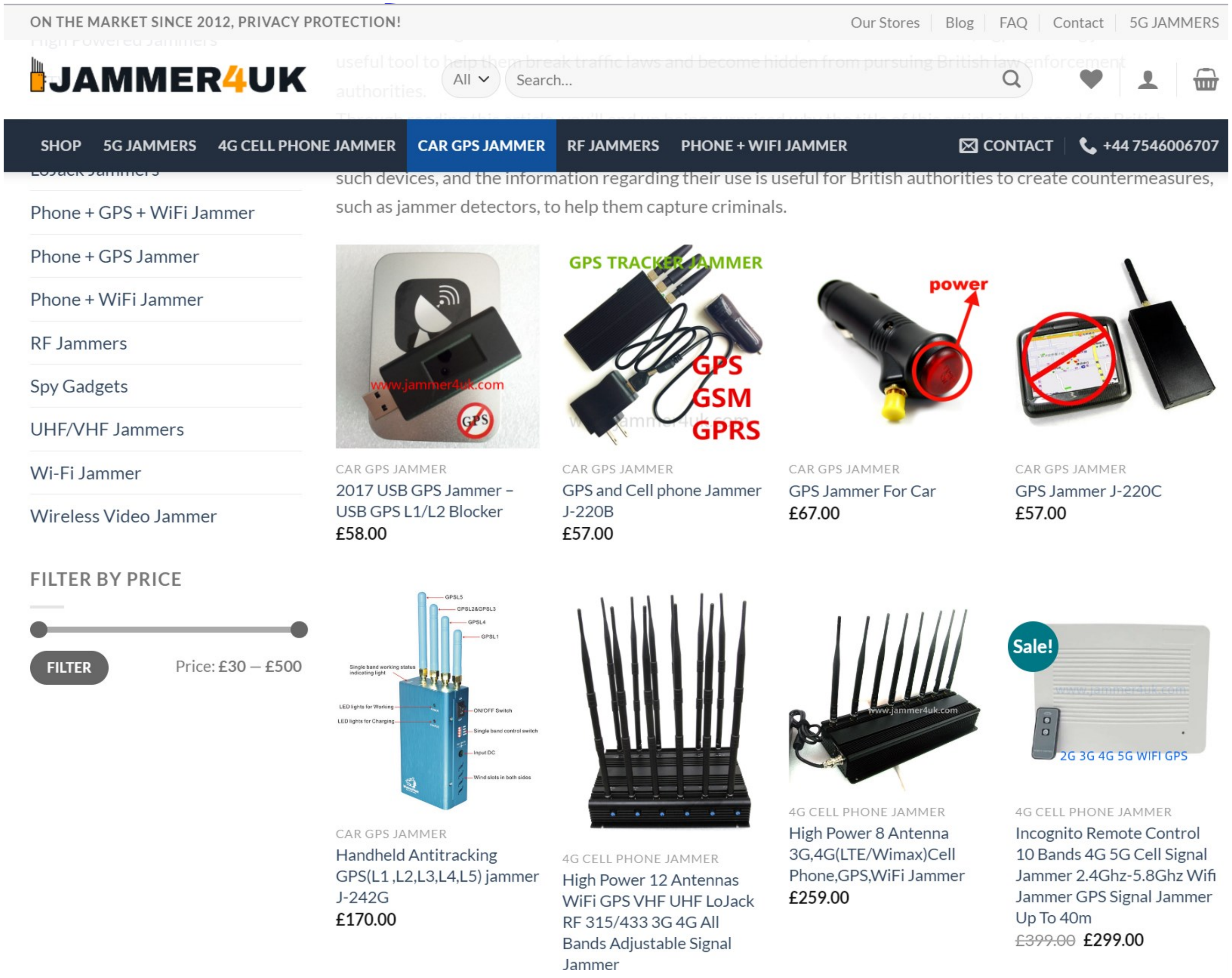


- Variant of the *Ping Flooding Attack*
- *Smurf* is installed on a computer using a stolen account
- Attacker sends a series of *IP Ping packets* to the directed broadcast address of the target network
- *IP Ping packets* have forged source address
- Upon arrival at the gateway directly connected to the target network, the gateway forwards the *ICMP Echo* message to all hosts on the target network
- All hosts send *ICMP Response* packets to the forged source address, which is the actual target of the attack

Disruption of Physical Resources

- Physical resources can be damaged or destroyed or service disrupted.
- Cutting cables, power cuts.
- Wireless networks are particularly vulnerable to jamming attacks, which can be affected both at the protocol and physical layers.
- Physical jammers exist for a number of frequencies and protocols including GSM/UMTS, GPS and IEEE 802.11

Disruption of Physical



ON THE MARKET SINCE 2012, PRIVACY PROTECTION!

Our Stores | Blog | FAQ | Contact | 5G JAMMERS

JAMMER4UK

All ⌄ Search...

SHOP 5G JAMMERS 4G CELL PHONE JAMMER CAR GPS JAMMER RF JAMMERS PHONE + WIFI JAMMER

✉ CONTACT ☎ +44 7546006707

High Powered Jammers

Lojack Jammers

- Phone + GPS + WiFi Jammer
- Phone + GPS Jammer
- Phone + WiFi Jammer
- RF Jammers
- Spy Gadgets
- UHF/VHF Jammers
- Wi-Fi Jammer
- Wireless Video Jammer

FILTER BY PRICE

FILTER Price: £30 — £500

useful tool to help them break traffic laws and become hidden from pursuing British law enforcement authorities.

such devices, and the information regarding their use is useful for British authorities to create countermeasures, such as jammer detectors, to help them capture criminals.

CAR GPS JAMMER
2017 USB GPS Jammer – USB GPS L1/L2 Blocker
£58.00

CAR GPS JAMMER
GPS and Cell phone Jammer J-220B
£57.00

CAR GPS JAMMER
GPS Jammer For Car
£67.00

CAR GPS JAMMER
GPS Jammer J-220C
£57.00

CAR GPS JAMMER
Handheld Antitracking GPS(L1 ,L2,L3,L4,L5) jammer J-242G
£170.00

4G CELL PHONE JAMMER
High Power 12 Antennas WiFi GPS VHF UHF LoJack RF 315/433 3G 4G All Bands Adjustable Signal Jammer

4G CELL PHONE JAMMER
High Power 8 Antenna 3G,4G(LTE/Wimax)Cell Phone,GPS,WiFi Jammer
£259.00

4G CELL PHONE JAMMER
Incognito Remote Control 10 Bands 4G 5G Cell Signal Jammer 2.4Ghz-5.8Ghz Wifi Jammer GPS Signal Jammer Up To 40m
~~£399.00~~ £299.00

And So To DDoS

- DoS attacks are restricted by the attacker having more resources at his disposal than the victim, or on forcing an asymmetric workload on the victim.
- If neither can be assured, attackers may simply 'gang up' and use multiple attackers on a network – this makes it more difficult to trace the origin.
- Bot net architectures provide scalability & anonymity – and are often synchronised.

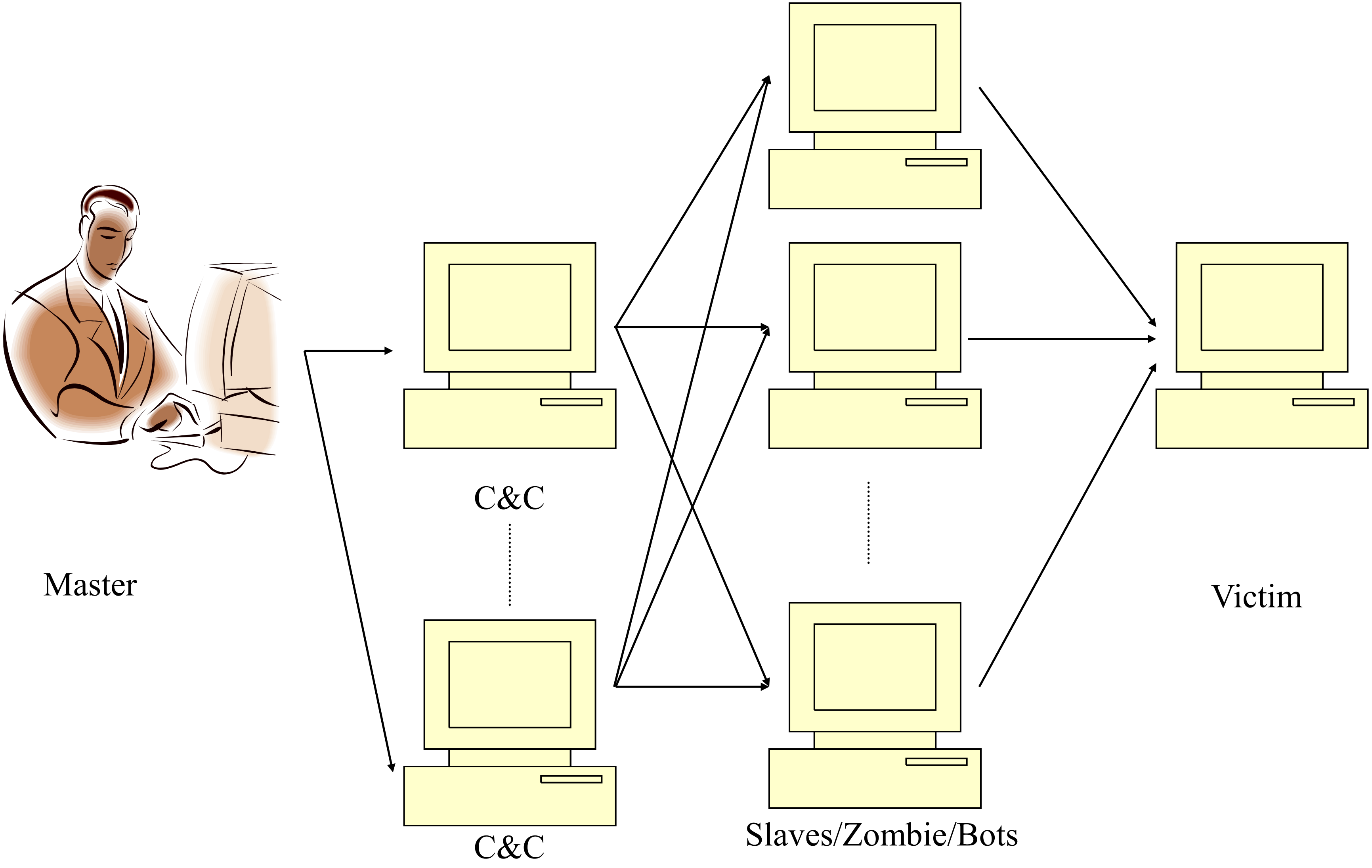
Distributed Denial of Service

- Many computers are used to launch a coordinated DoS attack against one or more targets
- A DDoS “master” program is installed on one computer
- Master program communicates to a number of “agent” programs, installed on compromised computers anywhere on the Internet
- Agents initiate attack simultaneously

Bot Networks (Botnets)

- Modern DDoS approach…
- Victim machines are compromised e.g. through Trojans or worms using software vulnerabilities.
- Malware deploys a number of components, including rootkit functions and command & control mechanisms
- Zombies use more than one channel and handlers can be deployed in multiple layers and may be able to control hundreds or thousands of nodes each.
  - Botnet architecture and tools are complex/advanced!
  - Heavily protected channels! Botnets are valuable – you lose control of the channel you lose the botnet.

Botnet



Master

C&C

C&C

Slaves/Zombie/Bots

Victim

Botnet operation: Basics

- Infection Mechanisms
  - Web download, mail attachments, scan/exploit
  - Automated process…
- Command and Control (C&C)
  - Centralized, P2P, unstructured
- Communication Protocols
  - IRC, HTTP, P2P, proprietary…
- Payload/Actions
  - Spam, DDoS, Keyloggers, Clickfraud, Bitcoin mining

Dismantling a Botnet

- Dismantling takes time and effort
  - Building one could be a one man job
  - Easier to disable than to destroy
- Some examples SANS Newsbites :
  - Kelihos
    - Microsoft shuts it down (45,000 hosts) (Sept 2011)
    - Alleged Mastermind named in lawsuit (Jan 2012)
    - Regaining Momentum (Feb-April 2012)
      - Kelihos.b (110,000 hosts by February, shut down March)
      - Kelihos.c (70,000 hosts by April….)
  - Bamital
    - Microsoft Shuts Down Bamital (February 2013)

IoT: New generation of botnets

- ❑ Mirai Worm (there are newer ones, such as Torii)
  - o Builds IoT-based botnets
  - o Source code publicly available (Hackforums, October)
  - o Mirai-based DDoS (KrebsOnSecurity 665 Gbps, Dyn > 1 Tbps)
- ❑ Attack of the Things
  - o Numbers vary 50k-400k for observed (advertised) botnets.
  - o IoT devices (IP Cameras and DVR)
- ❑ Device Security Issue
  - o Fixed, hardcoded passwords in firmware (Telnet, SSH)
  - o Tries about 50 username, password combinations.
  - o For example: root (none); admin password; root root; root 12345; user user; admin (none); root pass; root 1111

Imperva. Incapsula, Breaking Down Mirai: An IoT DDoS Botnet Analysis. Octo 2016.

The end!

?

Any questions…