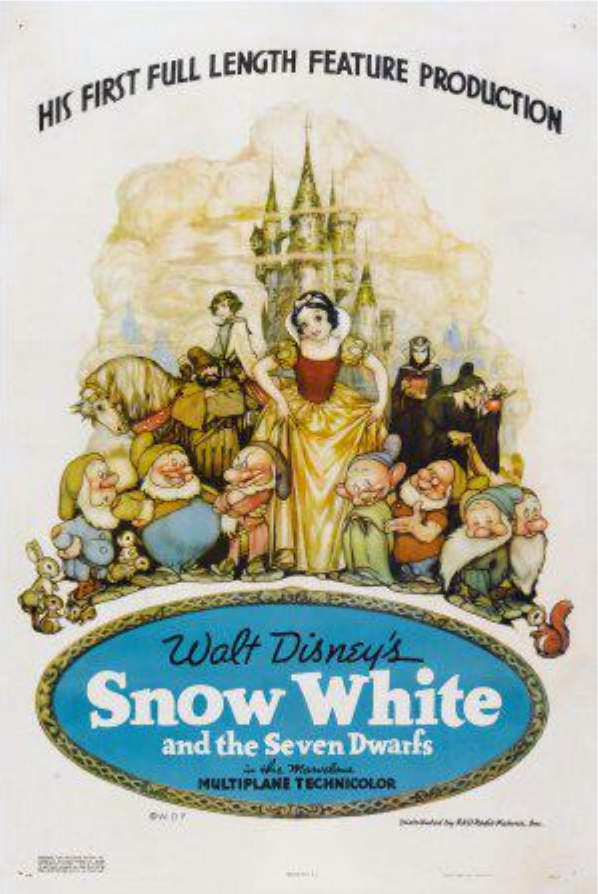
Introduction to Computer Security Lecture Slides

Network Security

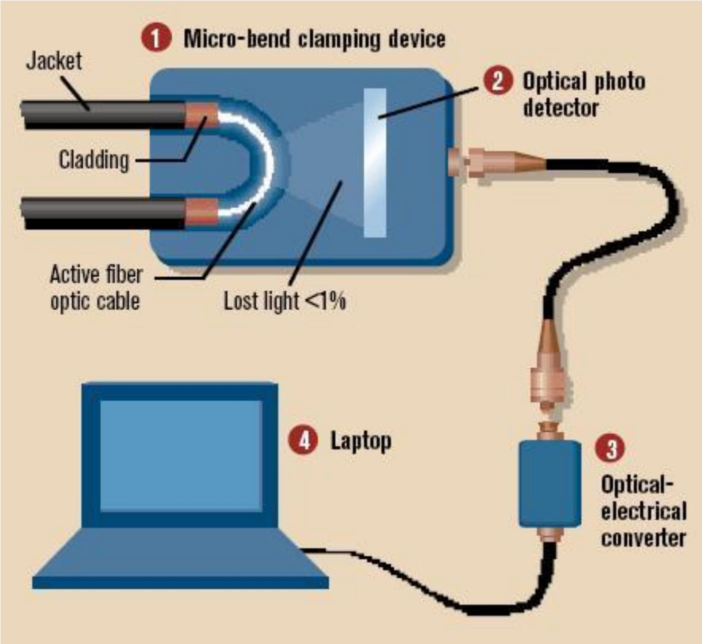
Associate Prof. Mihai Chiroiu

Network 7 Layers [1]

Sleepy	**Physical**	The group new that physical connections are boring, and figured it might as well assign the physical layer to dwarf ``Sleepy''.
Sneezy	**Link**	If you monitor a network and watch the pattern of packets emitted by a computer, you'll immediately understand the relationship between link-layer protocols and ``Sneezy''.
Happy	**Network**	Everyone's happy with the network layer. Well... to be honest, the only network layer protocol that makes everyone's happy is the Internet Protocol.
Doc	**Transport**	This one's obvious -- it definitely takes a Ph.D. to understand the subtleties of a transport layer protocol.
Dopey	**Session**	Yep, even the designers realized that having a separate session layer is a dopey idea. They decided to follow Disney's approach of adding comic relief, so they stuck in a completely unnecessary layer and laughed about it.
Bashful	**Presentation**	The designers realized that sooner or later someone would create a presentation layer protocol. However, the group decided to classify such protocols as too ``bashful'' to appear in public. So, even if a presentation protocol is produced, no one gets to see it.
Grumpy	**Application**	Programmers who design network applications are incredibly grumpy -- they complain about the efficiency of other layers [...]. And users add to the grumpiness, [...] ,they only complain about applications.



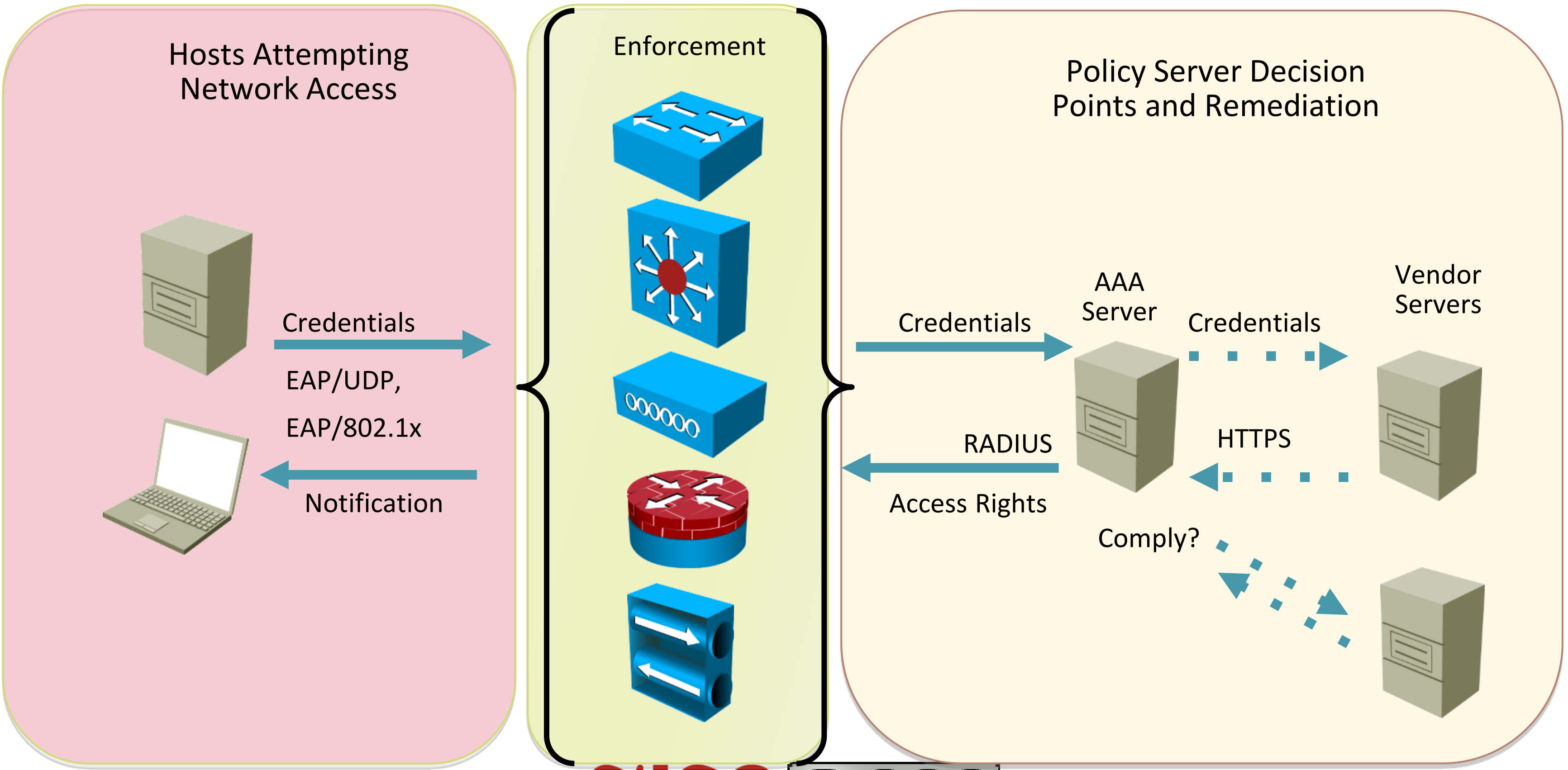
Intercepting at physical



- You can buy one of these for ~350$
- You can detect an attack like this by loss of light (must be lower than 2% in an acceptably quality implementation)

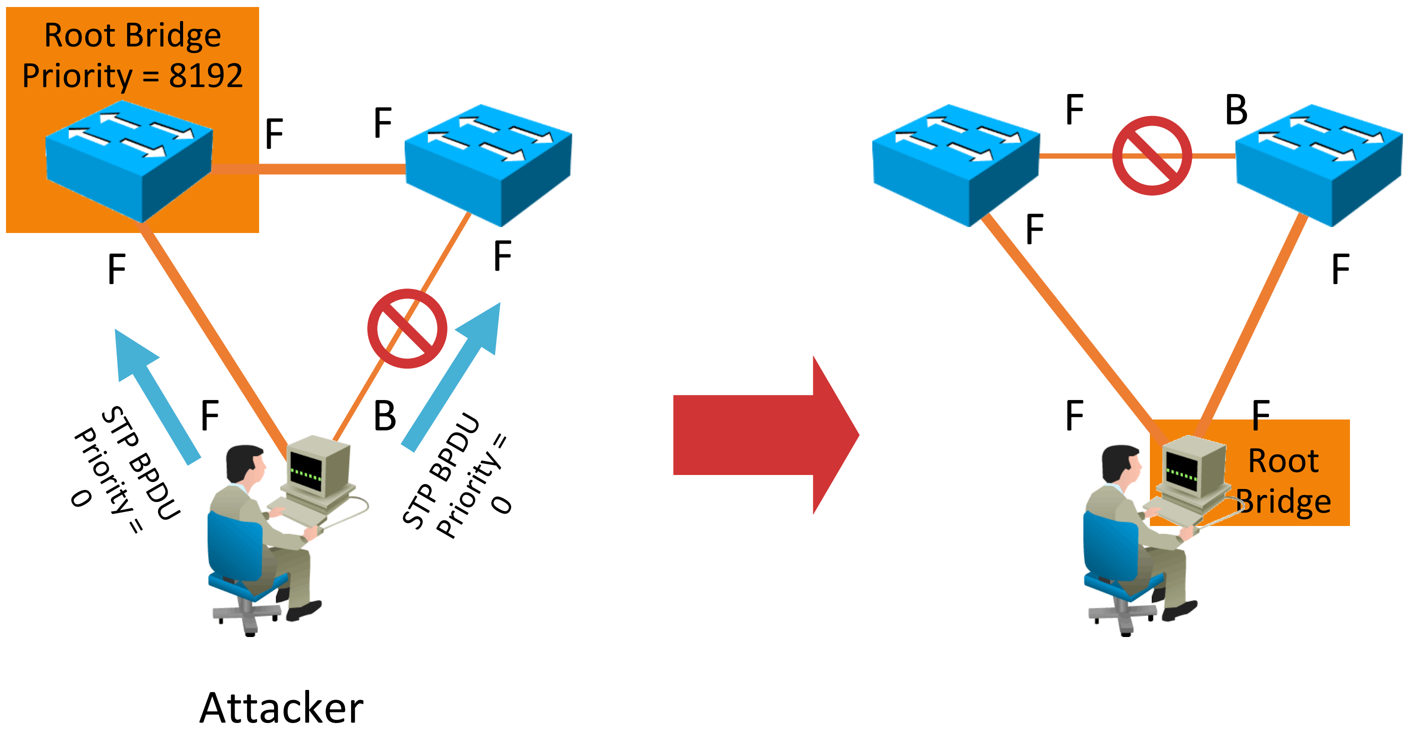
802.1x

- Several devices enforcing different security policies.



L2 Security

- MITM attacks from insiders (ARP Spoofing)
- STP can be broken
- VLAN hopping



L2 Security

- DHCP bindings
- Sticky MAC
- BPDU Guard

Firewall

- Access control over traffic (at different OSI levels)
- Must be fast
- Whitelisting vs. Blacklisting
- Stateful vs. Stateless
- Next level firewalls: Deep Packet Inspection

Intrusion Detection/Prevention Systems

- Intrusion detection is a classification problem
- Based on signatures (how to be fast? – data structures? GPU?)

	Detection Result		
		True	False
Reality	True	True Positive	False Negative
	False	False Positive	True Negative

Attacks directed to the equipment (routers)

- How do you figure out if a router is compromised?
- "There are **6043** CVE Records that match your search." (on keyword "cisco" as of 1st January 2023)
  - "[…] could allow an authenticated, remote attacker to execute arbitrary code on an affected device"

Routing protocols (attacks)

- OSPF
  - TTL Security Check (value should be 255)
  - Add authentication for messages (preferably different for each router-link)
    - HMAC from secret and message
- https://datatracker.ietf.org/doc/html/draft-ietf-rpsec-ospf-vuln-02

Routing protocols (attacks)

- BGP
  - (Sub)Prefix Hijacking (I'm Youtube now ☺)

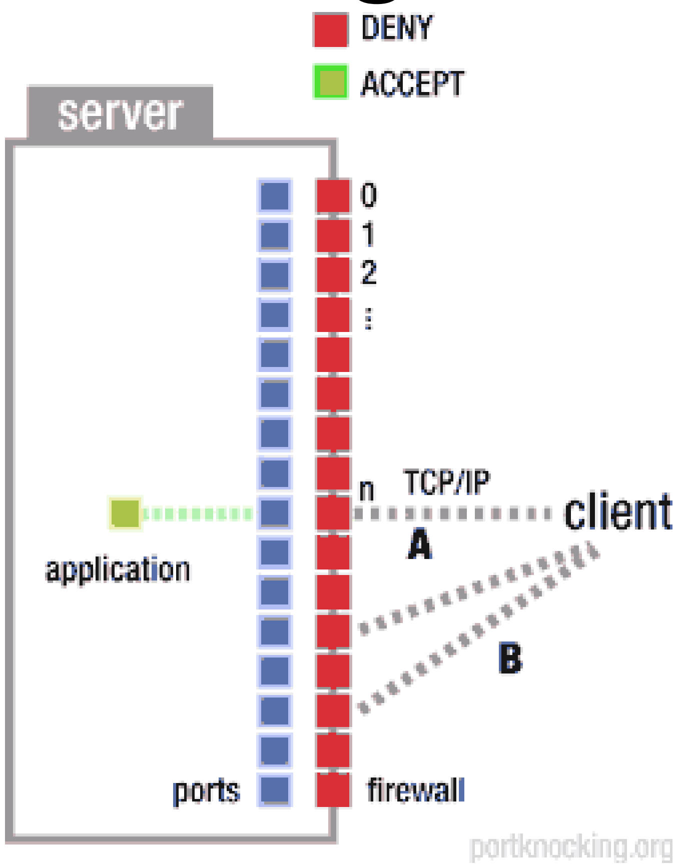
Routing anonymity

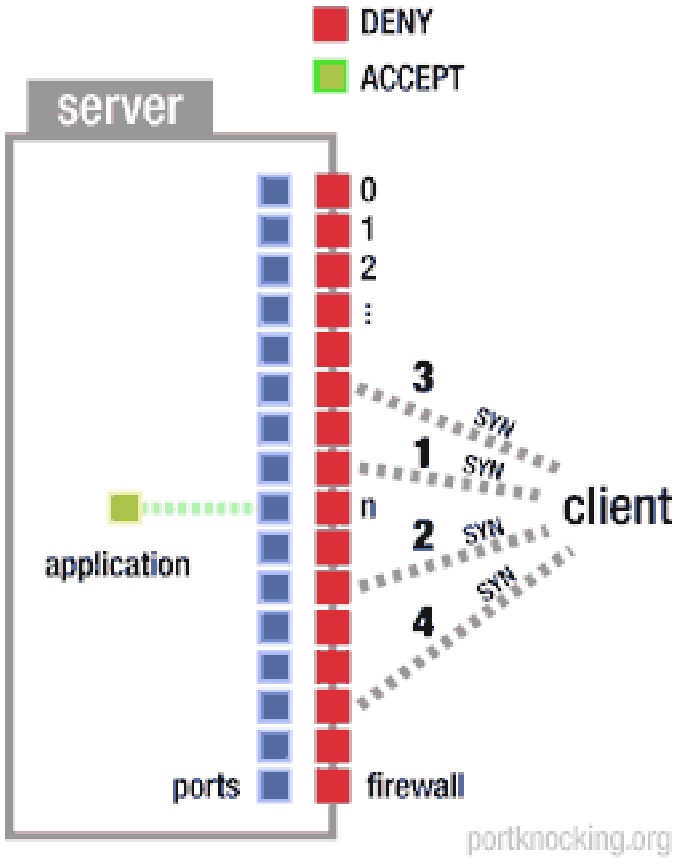
- Mixes routers (1981) [6]
  - nodes may reorder, delay, and pad traffic to complicate traffic analysis
- Onion router (1996) [7]
  - produce virtual circuits within link encrypted connections
  - TOR project (2004) [8]
- Crowds (1998) [9]
  - Relay message to random router: with probability p to another router; with probability 1-p, to its intended destination

TCP/IP Attacks [4]

- Port scanning
- TCP Sequence Numbers guessing
- Source Routing

Port knocking

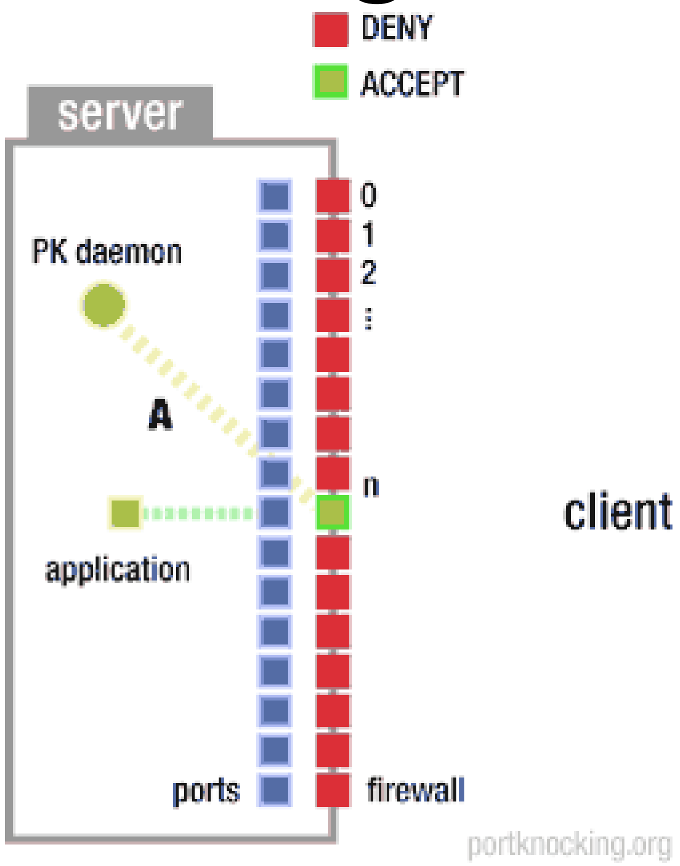




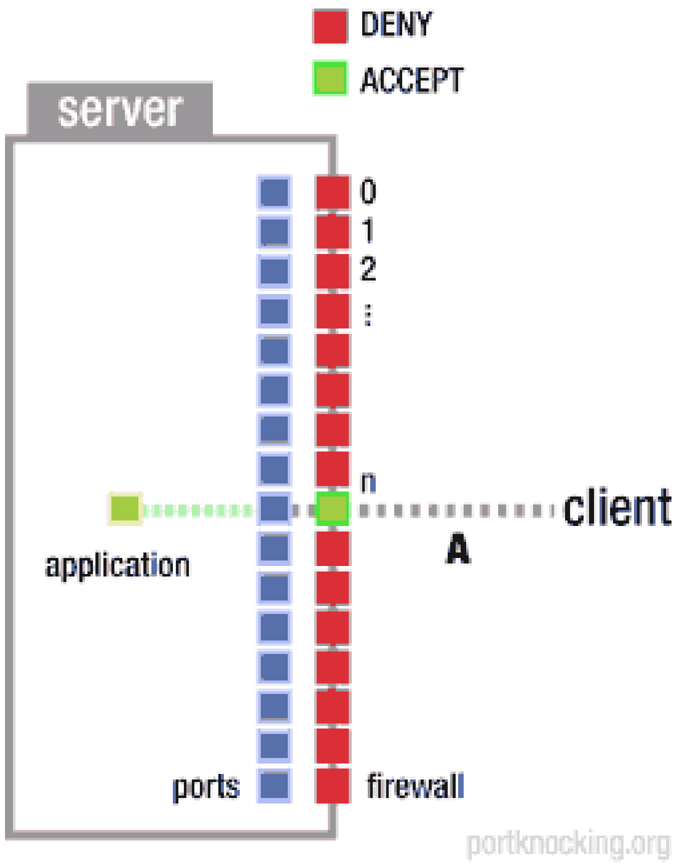
A) The client cannot connect to the application. The client cannot establish a connection to any port.

B) The client attempts connection to a number of ports in a predefined sequence. Client receives no ACKs.

Port knocking



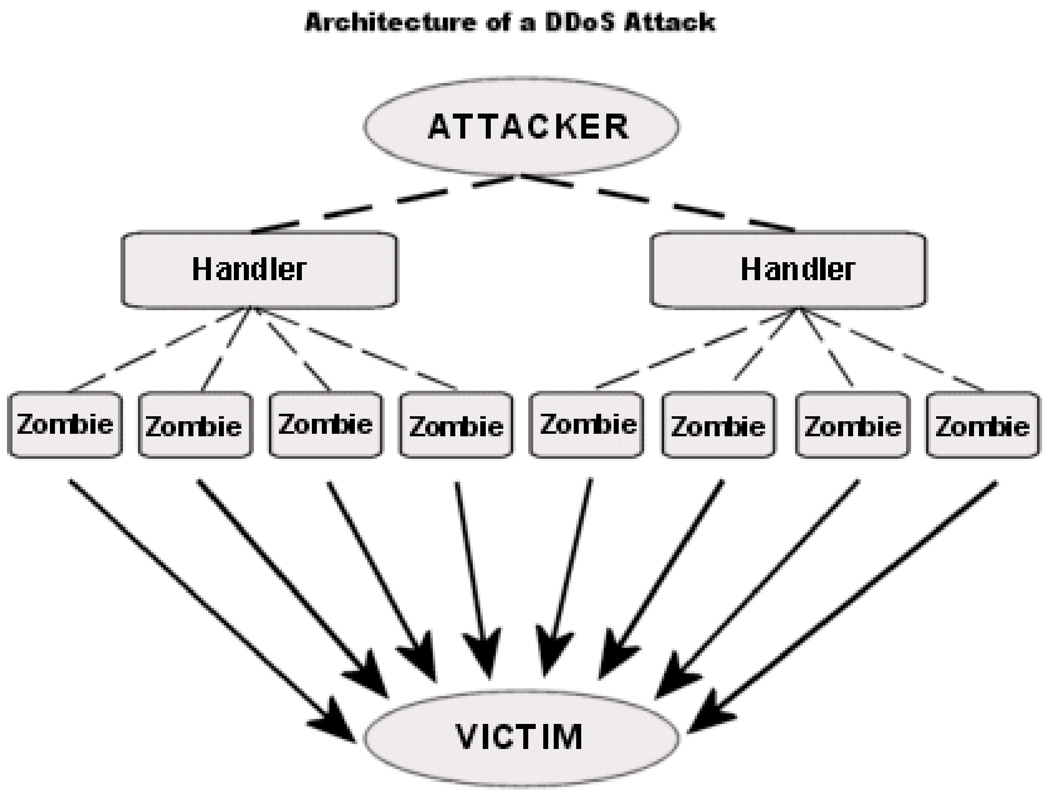
C) The PK daemon interprets the attempts and carries out a task. For example, it opens a specific port (n).



D) The client can now connect to port n.

(Distributed) Denial of Service

- Each network MUST have a benchmark of:
    - Total bandwidth utilization
    - Protocols active in the network
    - Hardware load (For hosts/network devices)
- All the above measured for different times of the day
- These statistics can be used to detect anomalies
- Anomalies can represent attacks
- TCP SYN Flood



VPN topologies

- Remote-access VPNs
  - Remote users must have a broadband Internet connection
  - The VPN parameters are dynamically negotiated
  - The tunnel is established only when required

- Site-to-site VPNs
  - Configured between two VPN-aware devices on both ends
  - Always-on
  - Provides interconnectivity between multiple networks on both sites.
  - Each end of the tunnel acts as a gateway for its networks.

IPSec for site-to-site VPN

- IPSec is an IETF standard (RFC 4301-4305)
  - Is a collection of open standards that describe how to secure communication.
- Relies on existing algorithms to provide:
  - Data confidentiality
  - Authentication
  - Data integrity
  - Secure key exchange (freshness, forward secrecy)
- Can be used host2host (transport) or gateway2gateway (tunnel)
  - Zero Trust Networks

IPSec – cryptographic blocks

- Algorithms that provide confidentiality (encryption):
  - Examples: DES, 3DES, AES, SEAL
- Algorithms that ensure integrity:
  - Examples: MD5, SHA1,SHA2 along with other versions
- Algorithms that define the authentication method:
  - Examples: pre-shared keys (PSK) or digitally signed using RSA.
- The mechanism to securely communicate a shared key:
  - Several DH (Diffie-Hellman) groups, ECDH

IPsec SA

- A security association (SA) is a set of policy and key(s) used to protect information.
- Different SAs for inbound and outbound traffic.
- A security association is uniquely identified by a triple consisting of a Security Parameter Index (SPI), an IP Destination Address, and a security protocol (AH or ESP) identifier.
- Security association database.

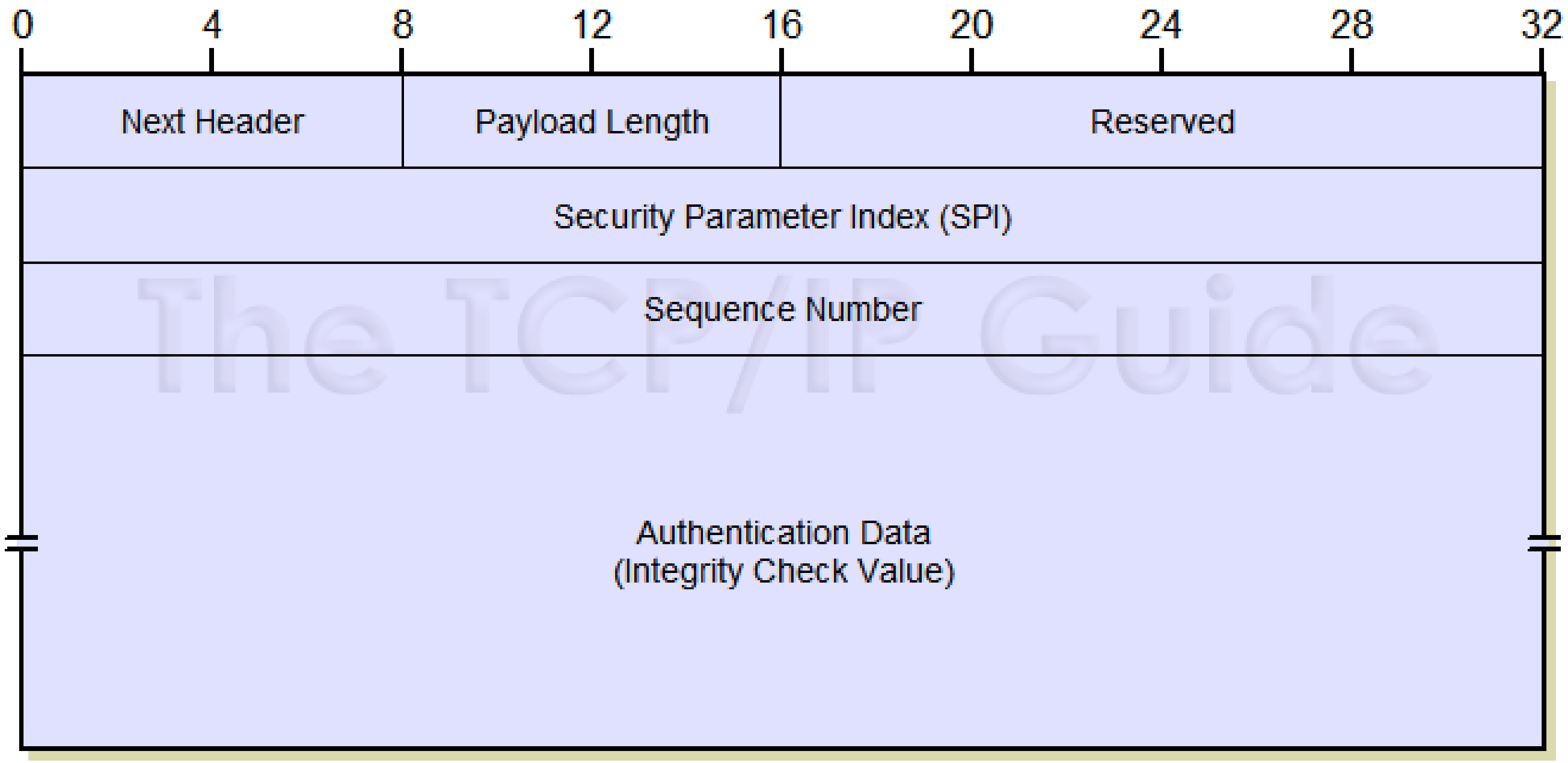
Security policy database

- Allows for implementation of packet protecting policies
  - What traffic to protect
  - What traffic to discard
  - What traffic to ignore

IPSec AH

- RFC 4302 IP Authentication Header
- IP protocol field 51
- Provides IP Header and Data integrity and authentication.
    - Some fields are not protected because they need to be changed in traffic (e.g. TOS, flags, frag offset, TTL, header checksum)
- It uses a Message Authentication Code for integrity
- Not working with NAT/PAT

IPSec AH

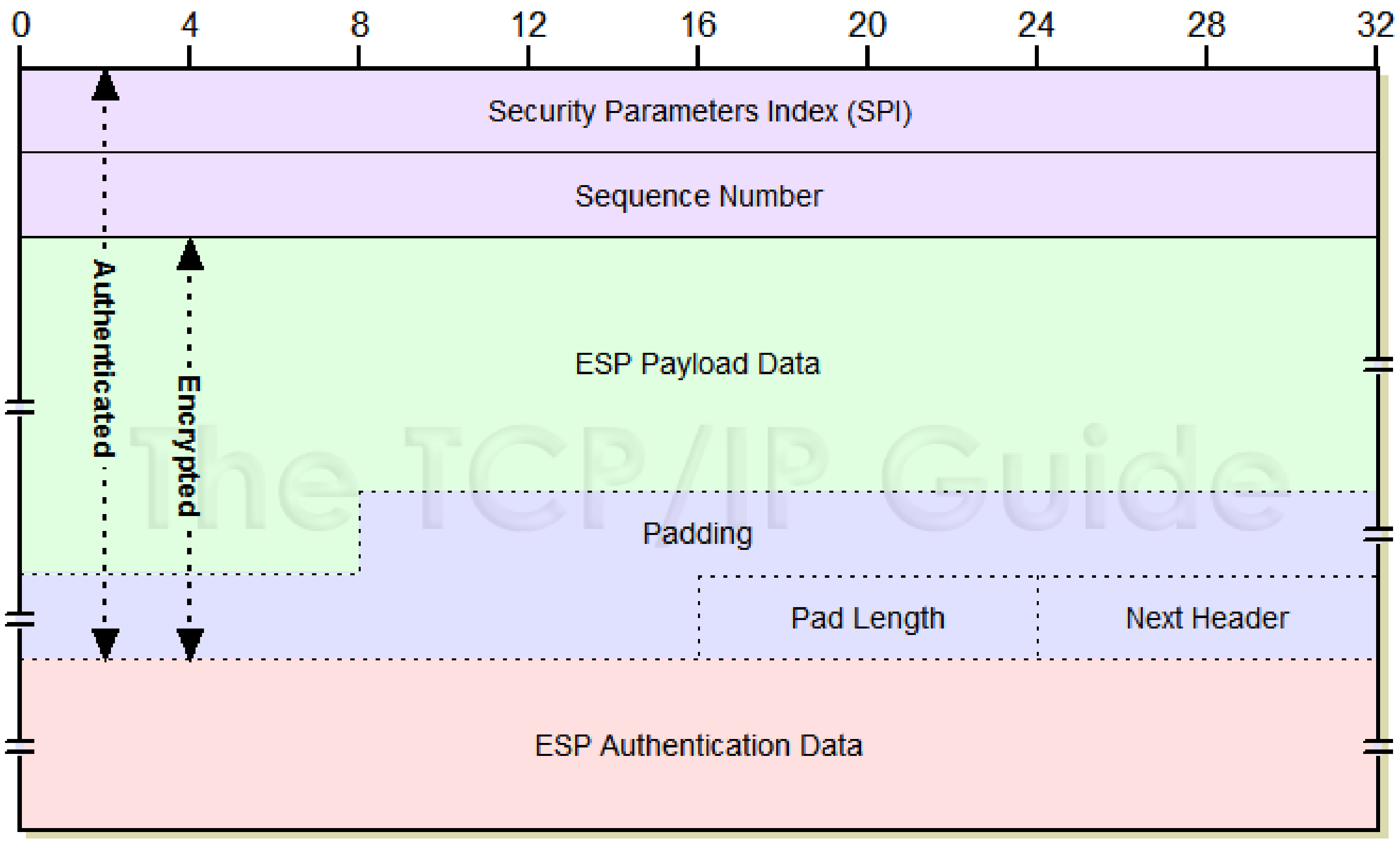


http://www.tcpipguide.com/free/t_IPSecAuthenticationHeaderAH-4.htm

IPSec ESP

- RFC 4303 IP Encapsulating Security Payload
- IP protocol field 51
- Provides Data Confidentiality, Integrity, Authenticity or none.

IPSec ESP



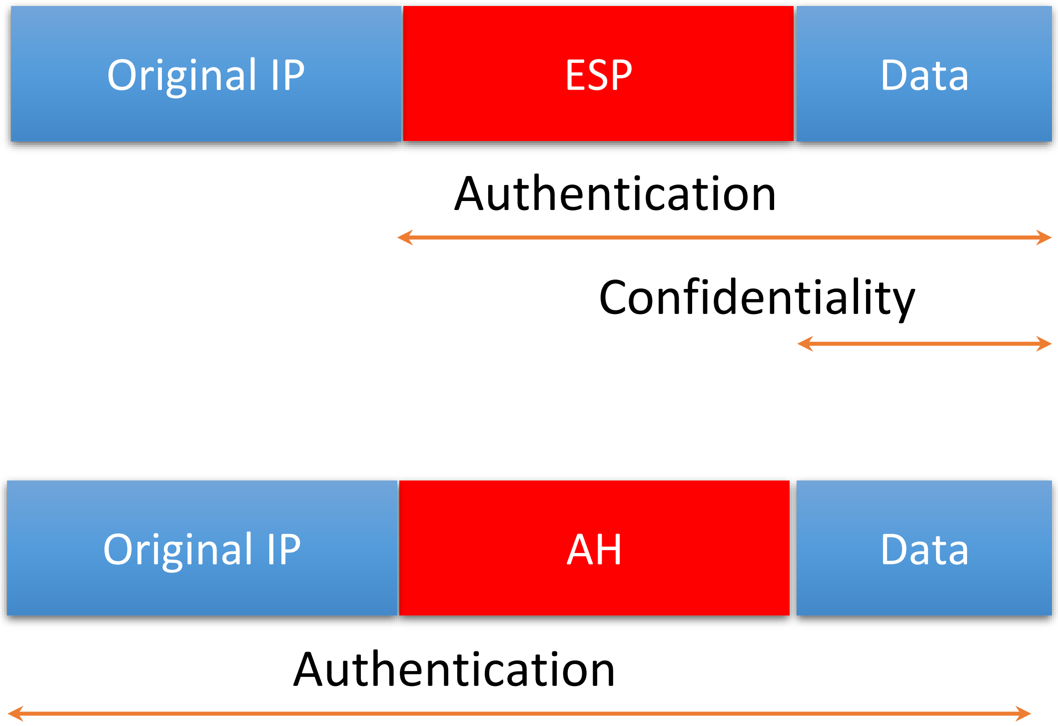
http://www.tcpipguide.com/free/t_IPSecEncapsulatingSecurityPayloadESP-4.htm

IPSec Tunnel vs Transport

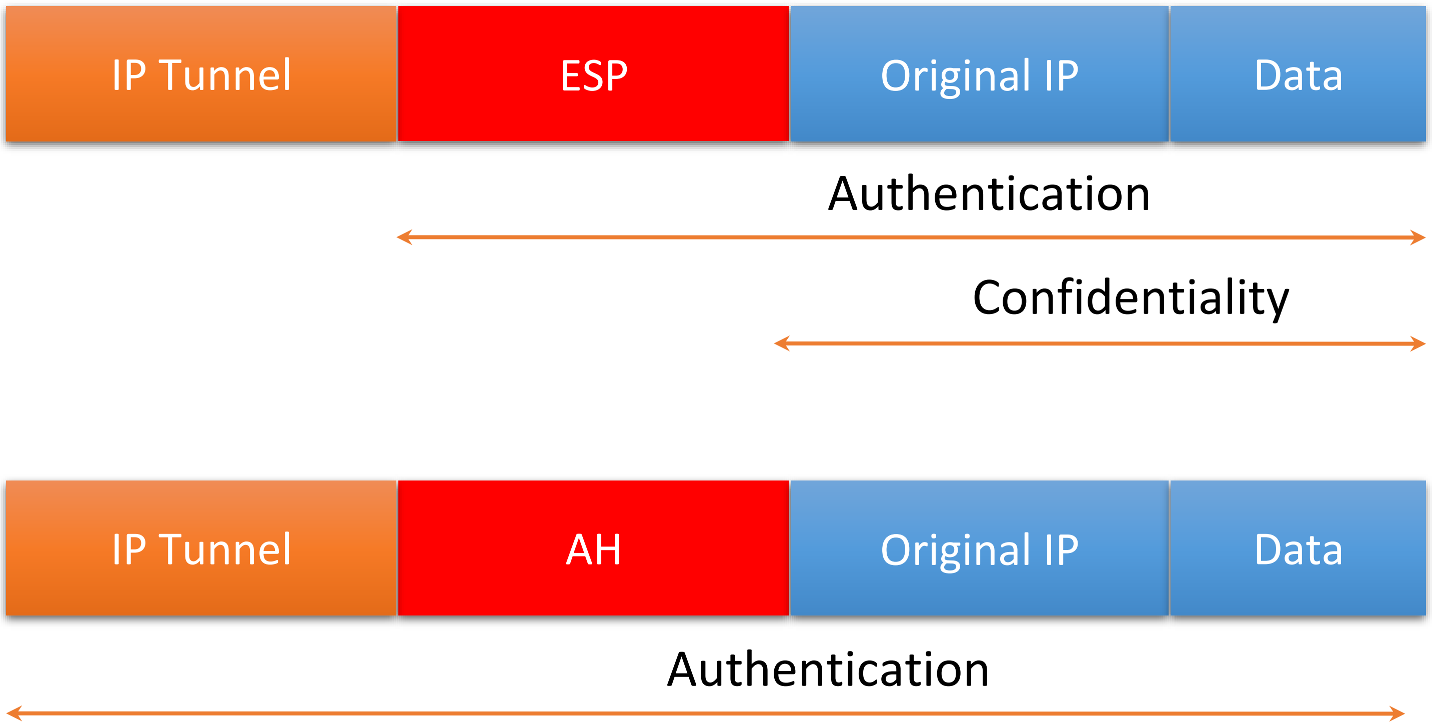
- Transport mode is usually used between 2 hosts
- Tunnel mode is usually the “to go” solution between gateways

- Identified by the next header type in the IPSec Header
  - 4 = Tunnel mode
  - else Transport mode

IPSec transport mode



IPSec tunnel mode



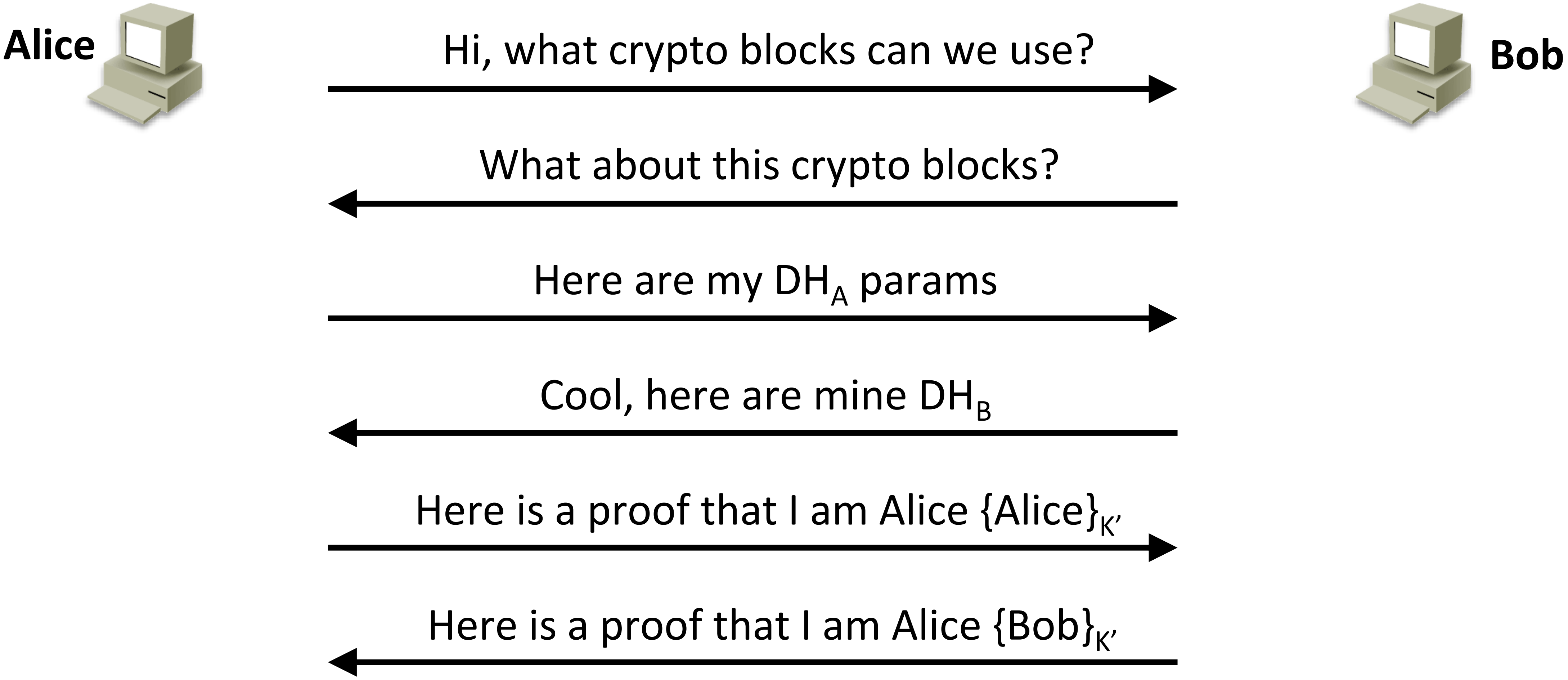
IKE

- Someone needs to provide keys to IPSec …. Welcome IKE
- Allows chosing of crypto blocks to be used (usually first round)
- Based on ephemeral Diffie-Hellman algorithms
- 2 phases
  - Phase 1 = ISAKMP SA = control channel
    - 2 modes of operation
    - Main mode (mandatory implemented)
    - Aggressive mode (optional implementation)
  - Phase 2 = IPSec SA = data channel
    - Quick mode

ISAKMP Main mode

- Oakley conservative protocol (similar to STS protocol) example
- A -> B: OK
- B -> A : CK_B
- A -> B: CK_A,CK_B, list
- B -> A: CK_B,CK_A, algo
- A -> B: CK_A,CK_B,DH_A, $\{ID_A,ID_B, N_A\}_{K'}$
  - K' is a key know by the two parties (derived from shared secret, public key, etc)
- B -> A: CK_B,CK_A, $\{N_B,N_A,ID_B,ID_A,MAC_K(ID_B,ID_A,DH_B,DH_A,algo)\}_{K'}$
- A -> B: CK_A,CK_B,$\{MAC_K(ID_A,ID_B,DH_A,DH_B,algo)\}_{K'}$

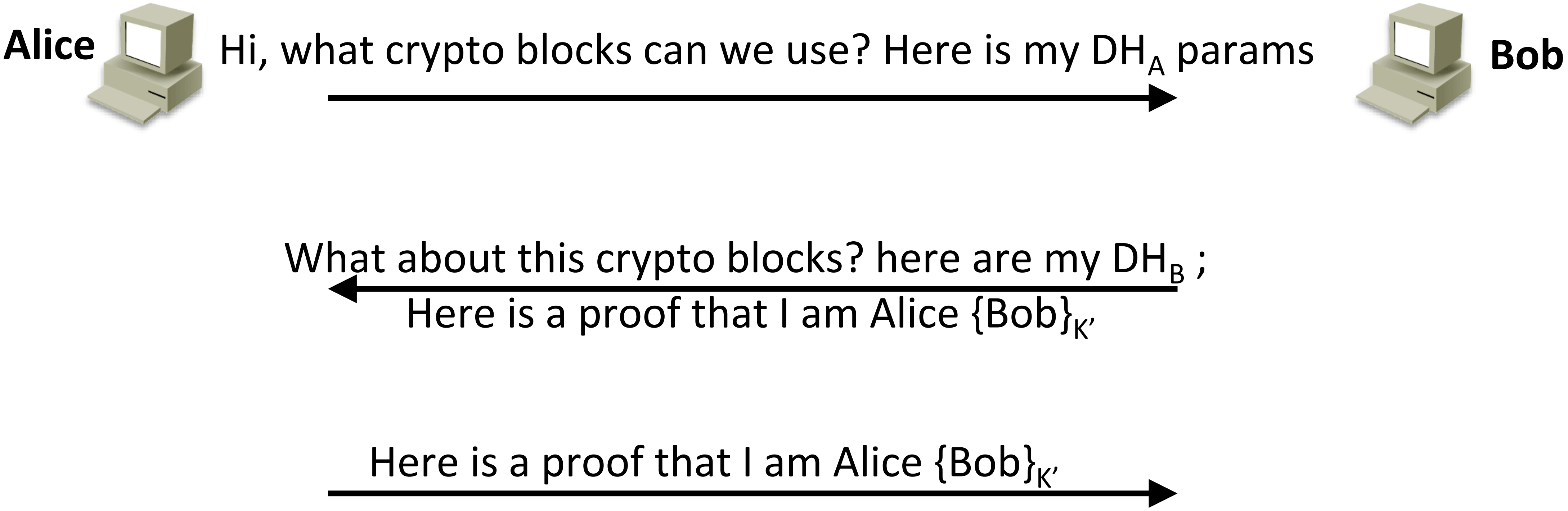
ISAKMP Main mode



ISAKMP Aggressive mode

- Oakley aggressive-mode protocol example
- A -> B: CK_A,**DH_A**,list,ID_A,ID_B,N_A, {ID_A,ID_B,N_A,DH_A,list}$_K$
  - CK_A = cookie A = session association (SA) equivalent = SPI + Dst IP
  - list = what I can use as cypto blocks
- B -> A: CK_B,CK_A,DH_B,algo,ID_B,ID_A,N_B,N_A, {ID_B,ID_A,N_B,N_A, DH_A, DH_B,algo}$_{K'}$
  - algo = what I have selected from the list as crypto blocks
- A -> B: CK_A,CK_B,DH_A,algo,ID_A,ID_B,N_A,N_B, {ID_A,ID_B,N_A,N_B,t_A,t_B,algo}$_{K'}$

ISAKMP Aggressive mode

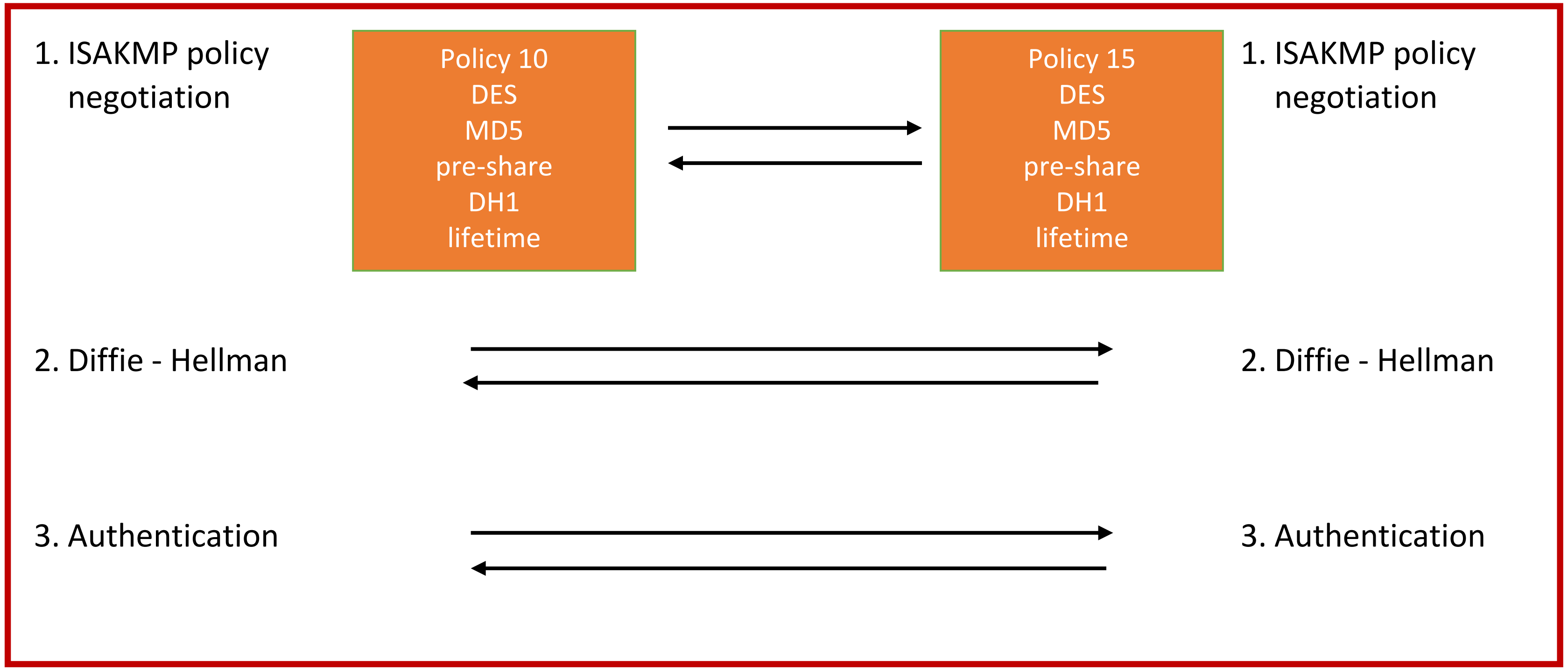


ISAKMP Aggressive mode

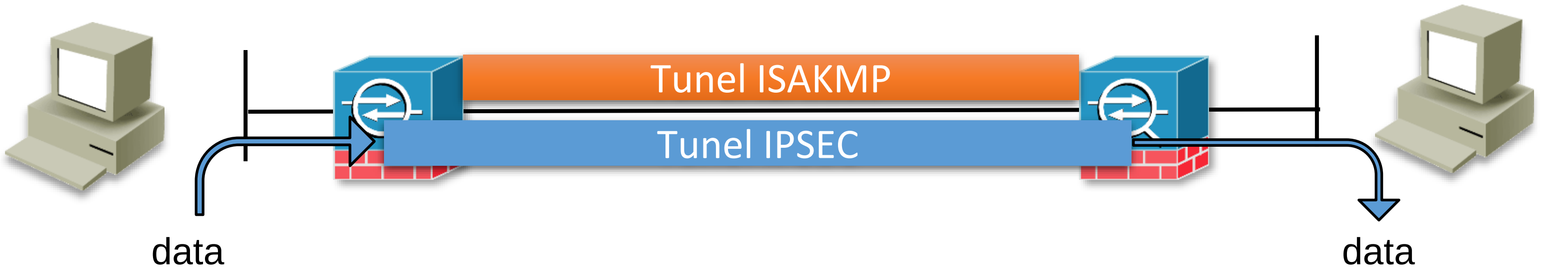
- It only works when B can use the same group as initially proposed and used by A in the first message;

IKE (simplified)

IKE phase 1 (ISAKMP SA)



IKE phase 2 (IPSec SA or Quick Mode)



The NAT problem

- AH hashes the IP header and the TCP header and expects them to remain unaltered.
- NAT(PAT) overwrites the layer 3 and 4 addresses and port numbers.
- How do you solve this?
- Solution: NAT-T (NAT-Traversal or NAT-Transparency)
    - In IKE Phase 1, an unencrypted but hashed message is sent.
    - At destination, if the hashes do not match, there is a NAT router in between.
- NAT-T encapsulates everything (including ESP) in an UDP header
    - There is also a TCP variant available when connection state tracking is required.
        - If an IPS/IDS device is present, for example.

SSL

- Developed by Netscape, now an IETF RFC (TLS Jan '99)
- Protocol for using one or two public/private keys
  - to authenticate a sever to a client
  - and by requiring a client key to authenticate the client to the server
  - establish a shared symmetric key (the session key)
- Gives you authentication, message integrity and confidentiality
- Everything except authorization

SSL

- Negotiate the cipher suite
- Establish a shared session key
- Authenticate the server (optional)
- Authenticate the client (optional)
- Authenticate previously exchanged data

- SSL Attacks [10] [11]
- SSL Stripping
- TLS 1.0 wrong crypto (CBC IV's)
- Broken CA (DigiNotar – 2011)

Honeypots

- Easy-to-hack environment (hopefully) controlled by administrator
- Used to learn about hackers behavior or as decoy
- Low interaction (emulated) vs. High interaction (real OS/apps)
- Virtual Machines as honeypots

DNS Security [5]

- DNS requests and responses are not authenticated
- DNS relies heavily on caching for efficiency, enabling cache pollution attacks

- DNSSec:
  - Each domain signs their “zone” with a private key
  - Public keys published via DNS
  - Zones signed by parent zones

SNMP Security

- Management Information Base = MIB
- SNMPv1 is simple, effective, and provides the majority of SNMP service in the field
- SNMPv2 adds some functionality to v1
- SNMPv3 is a security overlay for either version, not a standalone replacement

References

[1] https://www.cs.purdue.edu/homes/dec/essay.network.layers.html

[2] http://www.faqs.org/faqs/firewalls-faq/

[3] http://www.sans.org/reading-room/whitepapers/protocols/ssl-tls-beginners-guide-1029

[4] https://www.cs.columbia.edu/~smb/papers/ipext.pdf

[5] http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

[6] D. Chaum. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Communications of the ACM, v. 24, n. 2, Feb. 1981, pages 84-88.

References

[7] http://www.onion-router.net/Publications/IH-1996.pdf

[8] http://www.onion-router.net/Publications/tor-design.pdf

[9] http://avirubin.com/crowds.pdf

[10] http://resources.infosecinstitute.com/ssl-attacks/

[11] https://tools.ietf.org/html/rfc7457