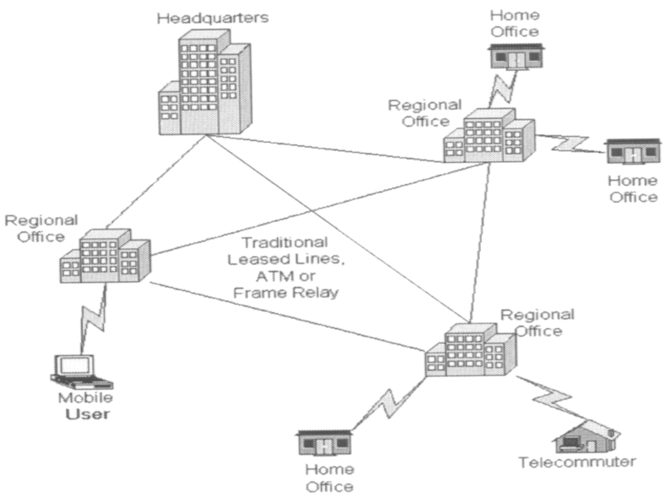
COMP9332 Network Routing and Switching
www.cse.unsw.edu.au/~cs9332

Virtual Private Network (VPN)

Outline

- VPN overview
- IPsec
  - IPsec Security Services
  - IPsec modes
  - ESP
- IKE
  - IKE two phases
- Network Address Translation

Traditional Connectivity



•[From Gartner Consulting]

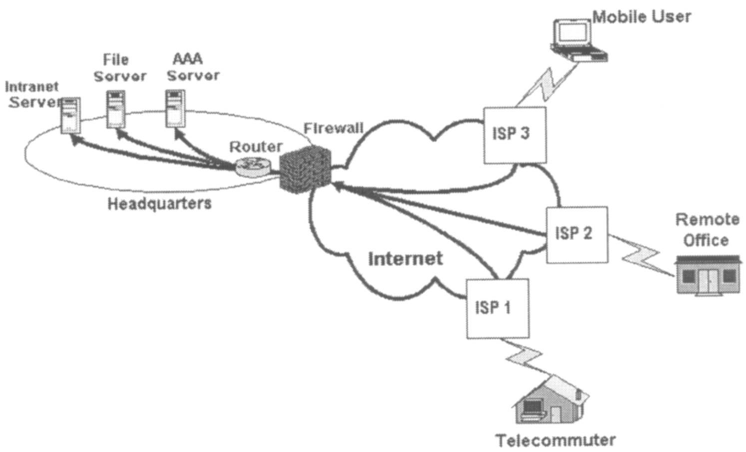
What is VPN?

- Virtual Private Network is a type of private network that uses public telecommunication, such as the Internet, instead of leased lines to communicate.
- Became popular as more employees worked in remote locations.

Private Networks vs. Virtual Private Networks

- Employees can access the network (Intranet) from remote locations.
- Secured networks.
- The Internet is used as the backbone for VPNs
- Saves cost tremendously from reduction of equipment and maintenance costs.
- Scalability

Remote Access Virtual Private Network



•(From Gartner Consulting)

Brief Overview of How it Works

- ✓ Two connections – one is made to the Internet and the second is made to the VPN.
- ✓ Datagrams – contains data, destination and source information.
- ✓ Firewalls – VPNs allow authorized users to pass through the firewalls.
- ✓ Protocols – protocols create the VPN tunnels.

Three Critical Functions

- ❑ Authentication – validates who sender is.
- ❑ Confidentiality – preventing the data to be read or copied as the data is being transported.
- ❑ Data Integrity – ensuring that the data has not been altered

Outline

- VPN overview
- IPsec
  - IPsec Security Services
  - IPsec modes
  - ESP
- IKE
  - IKE two phases
- Network Address Translation
- Layer Two Tunneling Protocol

IP Network Security Issues

- Eavesdropping
- Modification of packets in transit
- Spoofing (forged source IP addresses)
- Man-in-the-middle attack
- Denial of service

IPsec: Network Layer Security

- Internet Key Exchange (IKE)
  - Authentication between two VPN parties
  - Establish security association for AH or ESP
  - Provide keys for AH or ESP
  - If IKE is broken, AH and ESP are not secure
- AH and ESP rely on an existing security association (SA)
  - Two parties must agree on
    - » Crypto algorithms
    - » A set of secret keys
    - » IP addresses

•IPsec = IKE + ESP + AH + Compression

Authentication + deriving keys for AH and ESP

Securing IP traffic
- ESP: confidentiality + integrity
- AH: integrity

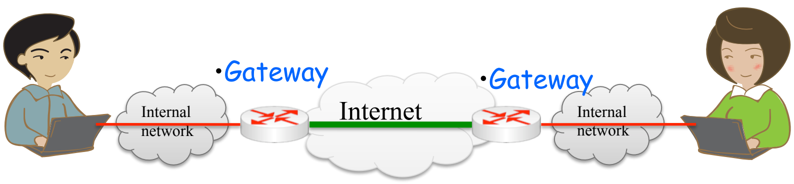
IPsec Security Services

- ESP and AH:
  - Authentication and integrity for packet sources
    - » Connectionless integrity (for a single packet)
    - » Partial sequence integrity (prevent packet replay)
- ESP:
  - Confidentiality (encapsulation) for packet contents
  - AES is supported
- Authentication and encapsulation can be used separately or together: However, encryption without authentication is not secure
- Both ESP and AH are provided in transport or tunnel mode
- These services are transparent to applications above transport (TCP/UDP/SCTP) layer

IPsec Modes

- Transport mode
  - Protection from
    - Host to host
    - Host to gateway
- Tunnel mode
  - Protection from
    - Gateway to gateway
      - Two gateways owned by the same organization
    - Host to gateway

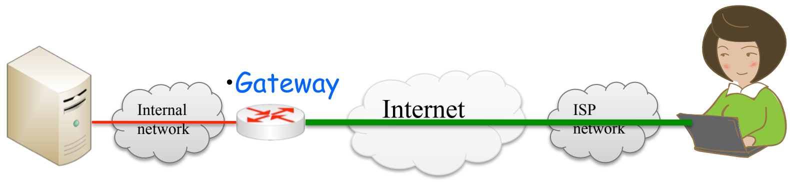
IPsec in Tunnel Mode



- Gateway-to-gateway security
  - Internal traffic inside gateway is not protected (color: red)
  - Virtual private network (VPN) across insecure Internet (color: green)
- Hosts do not need IPsec
- Gateways typically are routers configured with IPsec

Host to gateway

- Remote access to corporate network
  - Either tunnel or transport mode



Transport Mode vs. Tunnel Mode

- Transport mode
  - Protects packet payload
  - Uses original IP header

IP header (original)	IPsec header	TCP/UDP header + data

- Tunnel mode
  - Encapsulates both IP header and payload into IPsec payload

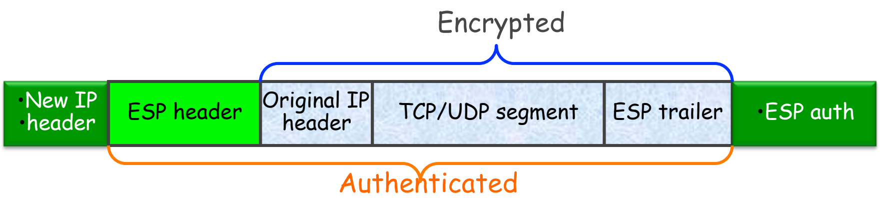
IP header (by IPsec)	IPsec header	IP header (original)	TCP/UDP header + data

Encapsulating Security Payload (ESP)

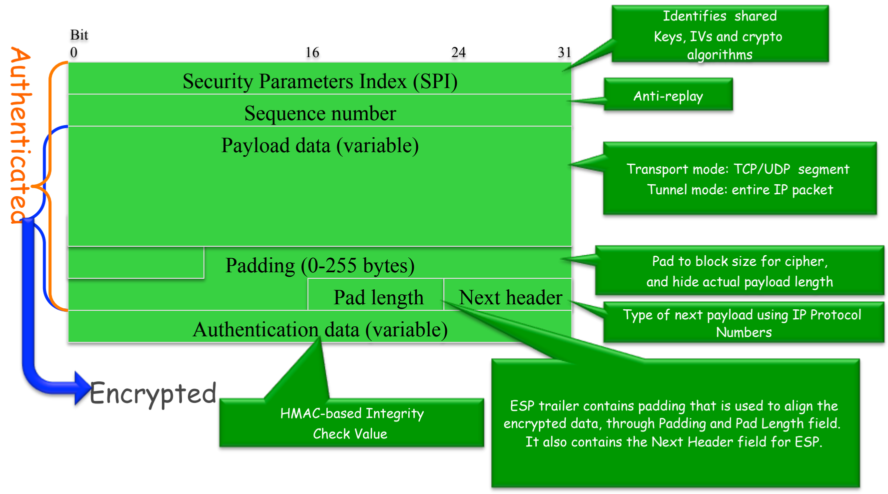
- Adds new header and trailer fields to every packet
- Tunnel mode
  - Confidentiality of packets between
    - Two gateways
    - A host and a gateway
  - Implements VPN tunnels

ESP Security in IPv4

- Both Confidentiality and integrity for packet payload
  - Symmetric cipher is negotiated as part of Security Association (SA) during IKE
- Tunnel mode



ESP Packet format



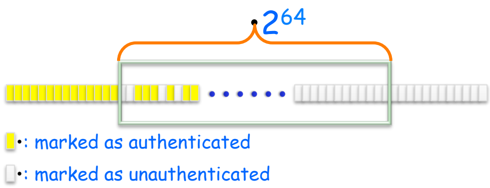
Virtual Private Networks (VPN) tunnel

- ESP is often used to provide a VPN tunnel
  - Secure communication between two sites of the same organization over public unsecure Internet
  - Packets go from internal network to a gateway
    - IP headers contains source and destination IP addresses
  - Packets go from sending gateway to receiving gateway
    - Entire packet is hidden by encryption
    - Encryption Includes original headers so that source and destination IP addresses are hidden
    - The new IP header generated by the sending gateway indicates the source and destination IP addresses as the sending gateway and receiving gateway, respectively
  - Packets go from receiving gateway to receiving host
    - Gateway decrypts packet and forwards original IP packet to receiving host in the network that it protects

Sliding Window: Prevention of Replay Attacks

- Sliding Window and anti-replay: Optional for receiver
- Sender
  - Initializes 32-bit counter to 0, increments by 1 for each packet
  - If it wraps around 2^{32}-1, new SA must be established
- Recipient
  - Maintains a 64-bit sliding window (A minimum window size of 32 must be supported)
  - Slide window when a received packet is authenticated

•Recipient:



 21

Sequence number checking and authentication

- Sequence number checking
  - Anti-replay is used only if authentication is selected
  - Sequence number should be the first check on a packet
  - The receiver proceeds to Integrity Check Value (ICV) verification
  - Duplicate packets are rejected
- Without authentication, malicious packets with large sequence numbers can unnecessarily
  - Valid packets would be dropped by falsely
  - Resulting in denial of service attacks

 22

Denial of service attacks and replay

- Sliding Window should not be advanced until the packet has been authenticated
  - To prevent falsely moving the Sliding Window by attacker, resulting in denial of service attacks
  - To protect against denial of service attacks the IPsec protocols use a sliding window
    - » Each packet gets assigned a sequence number and is only accepted if the packet's number is within the window
    - » Older packets are immediately discarded
    - » This protects against replay attacks where the attacker records the original packets and replays them later.

Outline

- VPN overview
- IPsec
  - IPsec Security Services
  - IPsec modes
  - ESP
- IKE
  - IKE two phases
- Network Address Translation

Key Management in IPSec

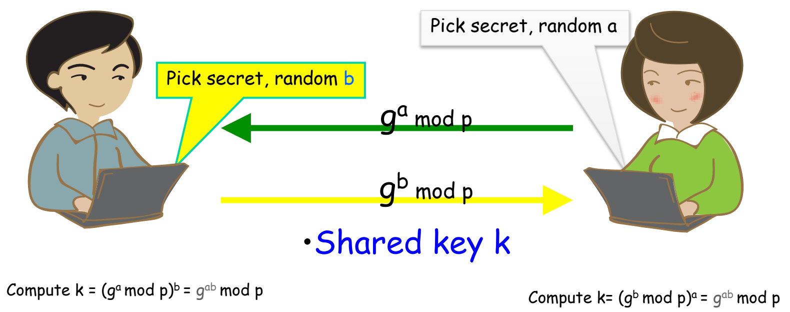
- Manual key management
  - Keys and parameters of crypto algorithms exchanged offline (e.g., by phone or face-to-face)
  - Security associations established by hand
- Pre-shared symmetric keys
  - New session key is derived for each session by hashing pre-shared key with fresh nonces (random number used once)
  - Standard symmetric-key authentication and encryption
- Online key establishment
  - Internet Key Exchange (IKE) protocol
  - Use Diffie-Hellman to derive shared symmetric key

Secure Key Establishment

- Need: Dynamically generate a shared session key and authenticate identities
  - Authentication: ensure the identity of other party
  - Secrecy: generated shared key is fresh and only known to the sender and receiver
  - Forward secrecy: compromise of one session key does not lead to the compromise of keys in other sessions
  - Protect privacy (identities) from eavesdroppers
  - Prevent replay of old key material
  - Prevent denial of service

Diffie-Hellman Key Exchange

- Protocol
  - Alice, Bob share a secret key g^{ab} mod p
  - The key is fresh and not known to anyone else
  - No authentication of identities



IKE cocktail

- IKE = Diffie-Hellman (a shared, fresh secret key) +
  Signature (Authentication) +
  Encryption (Privacy for hiding identities) +
  DDoS resistance (Photuris)
- Shared, fresh secret key: Diffie-Hellman
  Alice → Bob: g^a mod p
  Bob → Alice: g^b mod p
- Shared secret is g^{ab}, compute key as k = hash(rand, g^{ab} mod p)
- Diffie-Hellman guarantees perfect forward secrecy

Authentication by PKI

- Let $m = g^a \bmod p$ and $n = g^b \bmod p$ to start existing D-H protocol
- Protocol:

  $A \rightarrow B$: m, A

  $B \rightarrow A$: n, $sig_B(m, n, A)$

  $A \rightarrow B$: $sig_A(m, n, B)$
- Alice receives the signature signed by Bob's private key and deduces that Bob is on the other end
- Similar for Bob
- ISO 9798-3 protocol:

  $A \rightarrow B$: $g^a \bmod p$, A

  $B \rightarrow A$: $g^b \bmod p$, $sig_B(g^a \bmod p, g^b \bmod p, A)$

  $A \rightarrow B$: $sig_A(g^a \bmod p, g^b \bmod p, B)$

Encryption for protecting privacy

- Encrypt signatures and ID to protect identity for both initiator and responder:

  $A \rightarrow B$: $g^a \bmod p$, N_A

  $B \rightarrow A$: $g^b \bmod p$, N_B, $E_K(sig_B(g^a \bmod p, g^b \bmod p, N_A)$, Bob)

  $A \rightarrow B$: $E_K(sig_A(g^a \bmod p, g^b \bmod p, N_B)$, Alice)

where K is derived according to Diffie-Hellman

IKE overview

- The first/two pair of messages (IKE_SA_INIT) negotiate cryptographic algorithms, exchange nonces, and do a Diffie-Hellman exchange
- The second pair of messages (IKE_AUTH) authenticate the previous messages, exchange identities and certificates, and establish the first Child SA
  - Parts of these messages are encrypted and integrity protected with keys established through the IKE_SA_INIT exchange, so the identities are hidden from eavesdroppers and all fields in all the messages are authenticated

The SA payload in the IKE_SA_INIT exchange

- The SA payload contains 24 proposal transforms, which are the proposed security suite supported by the VPN client
  - The first transform (Transform # 0) includes 256 bit AES-CBC for IKE encryption, SHA for hash, 1024-bit DH, XAUTH and Pre-Shared key for client authentication, and lifetimes of keys

```
•Type Payload: Security Association (1)
•        Next payload: Key Exchange (4)
•        Payload length: 932
•                    .... .... .... .... ....
•
•        Type Payload: Proposal (2) # 0
•            Next payload: NONE / No Next Payload  (0)
•            Payload length: 920
•            Proposal number: 0
•            Protocol ID: ISAKMP (1)
•            SPI Size: 0
```

```
• Proposal transforms: 24
•           Type Payload: Transform (3) # 0
•               Next payload: Transform (3)
•               Payload length: 40
•               Transform number: 0
•               Transform ID: KEY_IKE (1)
•               Transform IKE Attribute Type (t=14,l=2) Key-Length : 256
•                   1... .... .... .... = Transform IKE Format: Type/Value (TV)
•                   Transform IKE Attribute Type: Key-Length (14)
•                   Value: 0100
•                   Key Length: 256
•               Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : AES-CBC
•                   1... .... .... .... = Transform IKE Format: Type/Value (TV)
•                   Transform IKE Attribute Type: Encryption-Algorithm (1)
•                   Value: 0007
•                   Encryption Algorithm: AES-CBC (7)
•               Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : SHA
•                   1... .... .... .... = Transform IKE Format: Type/Value (TV)
•                   Transform IKE Attribute Type: Hash-Algorithm (2)
•                   Value: 0002
•                   HASH Algorithm: SHA (2)
•               Transform IKE Attribute Type (t=4,l=2) Group-Description : Alternate 1024-bit MODP group
•                   1... .... .... .... = Transform IKE Format: Type/Value (TV)
•                   Transform IKE Attribute Type: Group-Description (4)
•                   Value: 0002
•                   Group Description: Alternate 1024-bit MODP group (2)
•               Transform IKE Attribute Type (t=3,l=2) Authentication-Method : XAUTHInitPreShared
•                   1... .... .... .... = Transform IKE Format: Type/Value (TV)
•                   Transform IKE Attribute Type: Authentication-Method (3)
•                   Value: fde9
•                   Authentication Method: XAUTHInitPreShared (65001)
•               Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
•                   1... .... .... .... = Transform IKE Format: Type/Value (TV)
•                   Transform IKE Attribute Type: Life-Type (11)
•                   Value: 0001
•                   Life Type: Seconds (1)
•               Transform IKE Attribute Type (t=12,l=4) Life-Duration : 32
•                   0... .... .... .... = Transform IKE Format: Type/Length/Value (TLV)
•                   Transform IKE Attribute Type: Life-Duration (12)
•                   Length: 4
•                   Value: 0020c49b
•                   Life Duration: 2147483
•.................
```


The VPN gateway

- The VPN gateway selected Transform #6 as the security suite to be used for the following IKE protection as shown below and sent it as the SA payload in the response packet to the VPN client
- The Transform # 6 includes 3DES-CBC for IKE encryption, SHA for hash, 1024-bit DH, XAUTH and Pre-Shared key for client authentication, and the lifetimes of keys as shown below

```
Type Payload: Security Association (1)
       Next payload: Key Exchange (4)
       Payload length: 56
       Domain of interpretation: IPSEC (1)
       Situation: 00000001
           .... .... .... .... .... .... .... ...
Type Payload: Transform (3) # 6
              Next payload: NONE / No Next Payload  (0)
              Payload length: 36
```

```
Transform number: 6
Transform ID: KEY_IKE (1)
Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : 3DES-CBC
    1... .... .... .... = Transform IKE Format: Type/Value (TV)
    Transform IKE Attribute Type: Encryption-Algorithm (1)
    Value: 0005
    Encryption Algorithm: 3DES-CBC (5)
Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : SHA
    1... .... .... .... = Transform IKE Format: Type/Value (TV)
    Transform IKE Attribute Type: Hash-Algorithm (2)
    Value: 0002
    HASH Algorithm: SHA (2)
Transform IKE Attribute Type (t=4,l=2) Group-Description : Alternate 1024-bit MODP group
    1... .... .... .... = Transform IKE Format: Type/Value (TV)
    Transform IKE Attribute Type: Group-Description (4)
    Value: 0002
    Group Description: Alternate 1024-bit MODP group (2)
Transform IKE Attribute Type (t=3,l=2) Authentication-Method : XAUTHInitPreShared
    1... .... .... .... = Transform IKE Format: Type/Value (TV)
    Transform IKE Attribute Type: Authentication-Method (3)
    Value: fde9
    Authentication Method: XAUTHInitPreShared (65001)
Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
    1... .... .... .... = Transform IKE Format: Type/Value (TV)
    Transform IKE Attribute Type: Life-Type (11)
    Value: 0001
    Life Type: Seconds (1)
Transform IKE Attribute Type (t=12,l=4) Life-Duration : 32
    0... .... .... .... = Transform IKE Format: Type/Length/Value (TLV)
    Transform IKE Attribute Type: Life-Duration (12)
    Length: 4
    Value: 0020c49b
    Life Duration: 2147483
```


The key Exchange payload (1)

- The DH public parameter and nonce payload contained in the IKE packet sent from the VPN client to the VPN gateway

```
• Type Payload: Key Exchange (4)
•         Next payload: Nonce (10)
•         Payload length: 132
•         Key Exchange Data:
ccbdd3b044c418f7375ef2c63e38f5ff01ddcdff95321ee9...
•     Type Payload: Nonce (10)
•         Next payload: Identification (5)
•         Payload length: 24
•         Nonce DATA: fa1d67d486a42310ec43741a3d07dc6e54d38949
•.....................
```

The key Exchange payload (2)

- The key Exchange payload contained in the first packet sent from the VPN gateway to the VPN client also includes a public DH parameter g^b mod p and the next payload is a fresh nonce
- The 3DES key will be derived from g^{ab} mod p and fresh nonces in order to protect the IKE protocol packets following the IKE_SA_INIT packets. The IKE_AUTH are encrypted and cannot be understood by Wireshark

```
•Type Payload: Key Exchange (4)
•        Next payload: Nonce (10)
•        Payload length: 132
•        Key Exchange Data:
1b36deee7d00ad5d42b8647b15a0483df68a3d1e651ceebd...
•    Type Payload: Nonce (10)
•        Next payload: Identification (5)
•        Payload length: 24
•        Nonce DATA: 0befdd7b2c1abc2dcd3d41823d90eb2086e605d2
•…………….. .
```


AUTH: proof possessing the private key/pre-shared secret

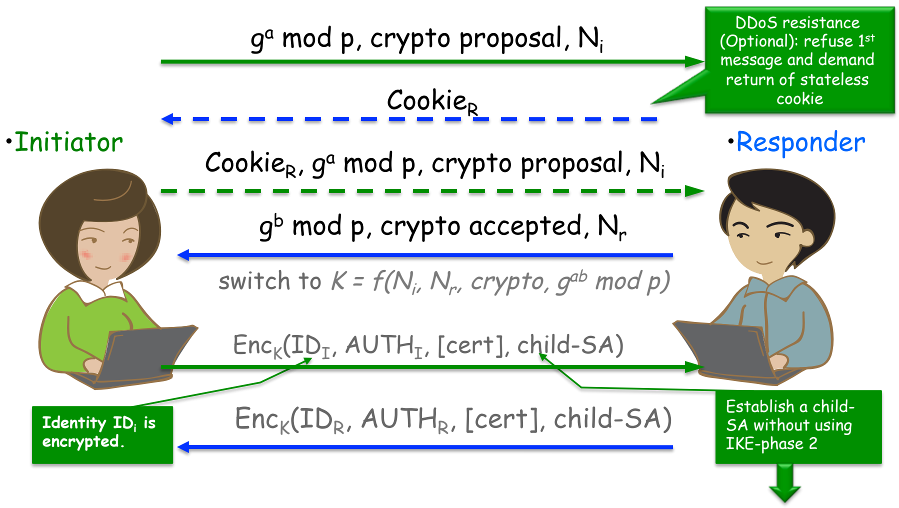
- The Authentication Payload (AUTH):

Bit

0	8	16 31
Next Payload	Reserved	Payload length
Auth method	Reserved	
Authentication data		

- Auth Method (1 octet): Specifies the method of authentication used. Values defined are:
  - RSA Digital Signature (1) using RSA private key
  - Shared Key Message Integrity Code (2): for pre-shared secret authentication method using Hash
  - DSS Digital Signature (3) using DSS private key

IKE: Phase One



- The initiator begins negotiation of a Child SA using the SAi2 payload in phase one

IKE two phases

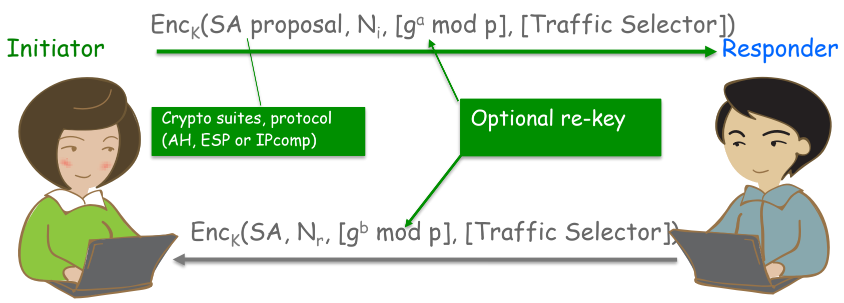
- Motivation
  - Expensive 1st phase creates the main SA
  - Cheap 2nd phase permits the creation of multiple child SAs (based on the main SA) between initiator and responder
- 1st phase
  - Establishes security association (IKE-SA) for the 2nd phase
  - Always uses Diffie-Hellman (expensive) protocol
- 2nd phase uses IKE-SA to create an actual security association (child-SA) to be used by AH and ESP (or IPsec)
  - Use keys derived in the 1st phase to avoid DH exchange
  - The IPsec SAs for ESP or AH that get set up through that IKE SA are called Child SAs
  - New child-SA can be generated cheaply in a quick mode
    - » To create a fresh key, hash old DH value and new nonces

Use of Two-Phase IKE

- IKE phase 1 creates an IKE SA
- IKE phase 2 creates an IPsec SA through a channel protected by the IKE SA
- Example: one SA for AH, another SA for ESP
  - Different conversations may need different protection
    - » Some traffic only needs integrity protection or short-key crypto
    - » Too expensive to always use strongest available protection
  - Avoid multiplexing several conversations over same SA
    - » For example, if encryption is used without integrity protection, it may be possible to splice the conversations using different SA's
  - Different SAs for different classes of service

IKE: Phase Two (Create Child-SA)

After IKE Phase One, I and R share key K



Child SA Key = $f(N_i, N_r, crypto, g^{ab} \bmod p)$

IKE phase 2 can be repeated several times to create multiple child SAs

Pre-shared secret

- Both initiator and responder need to have certificates in order to use signature-based authentication
- Pre-shared secret is used if no PKI is in place
- In the case of a pre-shared key, the AUTH value is computed as:

  AUTH = prf(prf(Shared Secret,"Key Pad for IKEv2"), <message octets>)

  - Where the string "Key Pad for IKEv2" is 17 ASCII characters without null termination
  - Shared Secret is ASCII strings of at least 64 octets

Attacks to Pre-shared Key

- Crack pre-shared key using a brute force dictionary attack
- Free attacking tools:
  - IKECrack: http://sourceforge.net/projects/ikecrack/
  - Cain: http://www.oxid.it/cain.html
  - IKEProbe: http://www.ernw.de/download/ikeprobe.zip
  - IKE-scan: http://www.nta-monitor.com/ike-scan/
  - FakeIKEd: http://linux.softpedia.com/get/Security/FakeIKEd-7926.shtml.
- Solution:
  - Do not use pre-shared key
  - Use Public-key encryption or signature

Extended Authentication (XAUTH) (1)

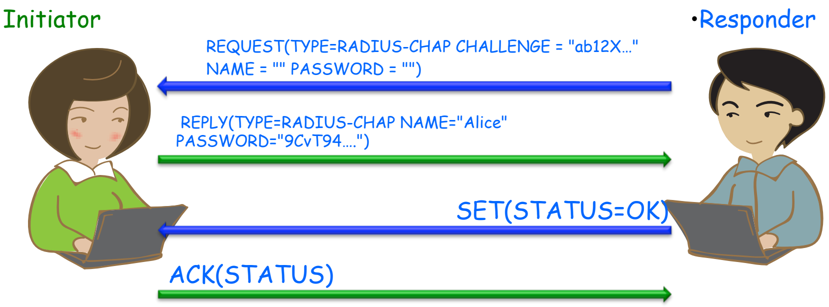
- Due to limited deployment of the PKI certificate, a password and pre-shared secret are used together for user authentication in most IKE deployments
- XAUTH provides a method for using existing unidirectional authentication mechanisms such as a password, SecurID, and OTP within IKE
- Extended Authentication (XAUTH) provides this capability of authenticating a user within IKE through the use of
  - Terminal Access Controller Access-Control System (TACACS+) or
  - Remote Authentication Dial In User Service (RADIUS), if they are already deployed in an organization

Extended Authentication (XAUTH) (2)

- Both peers must authenticate each other via the IKE authentication methods
- A VPN gateway requests extended authentication from an IPsec initiator, thus forcing the initiator to respond with its extended authentication credentials
- The VPN gateway will then respond with a failed or passed message
- This method provides unidirectional authentication only, meaning that only one initiator is authenticated using both IKE authentication methods and Extended Authentication

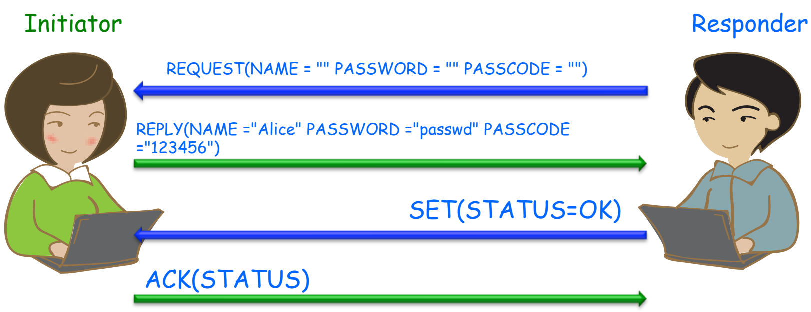
Challenge Handshake Authentication Protocol (CHAP)

- Challenge Handshake Authentication Protocol (CHAP) is used to periodically verify the identity of the peer using a 3-way handshake
  - This is done upon initial link establishment and may be repeated any time after the link has been established



Two-Factor Authentication

- Two-factor authentication method combines something the user knows (password) and something that the user has (a token card)



IKE deployment

- Password authentication
  - Due to limited deployment of a PKI certificate, a password and pre-shared secret are used together for user authentication
  - Extended Authentication (XAUTH) provides this capability of authenticating a user within IKE using TACACS+ or RADIUS that is already deployed in an organization
  - Certificates are more secure authentication in IKE
- IKE/IPsec protocol management
  - Rekeying period (lifetime): 24 hours recommended by NIST
  - Dead peer detection

NIST Recommended Key Sizes (bits)

Date	Symmetric Crypto	RSA (modulus)	ECC
2010 (Legacy)	80	1024	160-223
2011–2030	112	2048	224-255
> 2030	128	3072	256-383
>> 2030	192	7680	384-511
>>> 2030	256	15360	521 or more

Outline

- VPN overview
- IPsec
  - IPsec Security Services
  - IPsec modes
  - ESP
- IKE
  - IKE two phases
- Network Address Translation

Network Address Translation (NAT)

- NAT problems
  - AH does not work with NAT
    - » NAT must change information in the packet headers such as source IP address and source port number that are mapped by the NAT router
  - Encapsulating Security Payload (ESP) protocol:
    - » Transport mode
      - If NAT is being used, one or both of the IP addresses are altered, so NAT needs to recalculate the TCP checksum
      - If ESP is encrypting packets, the TCP header is encrypted; NAT cannot recalculate the checksum, so NAT fails
      - TCP checksum calculation and verification is required in IPv4 whereas UDP can disable checksum in IPv4
      - UDP/TCP checksum calculation and verification is required in IPv6
    - » Tunnel mode: compatible with NAT

UDP encapsulation for ESP and IKE

- Perform NAT before applying IPsec
    - » This can be accomplished by arranging the devices in a particular order, or by using an IPsec gateway that also performs NAT
    - » For example, the gateway can perform NAT first and then IPsec for outbound packets
  - Use UDP encapsulation of ESP packets
- UDP encapsulation can be used with tunnel mode
    - » ESP over transport mode ESP
      - UDP encapsulation appends a UDP header to each packet, which provides an IP address and UDP port that can be used by NAT
      - This removes conflicts between IPsec and NAT in most environments

NAT Traversal (NAT-T 1)

- An IKE enhancement known as IPsec NAT Traversal (NAT-T) allows IKE to negotiate the use of UDP encapsulation
  - During the IKE phase one exchange, both endpoints declare their support of NAT-T through a vendor ID payload (containing the hash of a well-known vendor ID value and static phrase), then perform NAT discovery to determine if NAT services are running between the two IPsec endpoints
  - NAT discovery involves each endpoint sending a hash of its original source address and port to the other endpoint, which compares the original values to the actual values
- NAT Traversal (NAT-T) needs to be used: RFC 3947 and 3948
  - NAT-T adds a UDP header that encapsulates the ESP header
    - » Header inserted between the ESP header and the outer IP header
  - This gives the NAT device a UDP header containing UDP ports that can be used for multiplexing IPSec data streams

NAT-T 2

- NAT-T
  - NAT-T also puts the sending host's original IP address into a NAT-OA (Original Address) payload
    - » This gives the receiving host access to that information so that the source and destination IP addresses and ports can be checked and the checksum validated
  - In order for IPsec to work through a NAT, the following ports need to be allowed on the firewall:
    - » Internet Key Exchange (IKE) - User Datagram Protocol (UDP) port 500
    - » IPsec NAT-T - UDP port 4500
    - » Encapsulating Security Payload (ESP) - Internet Protocol (IP) 50