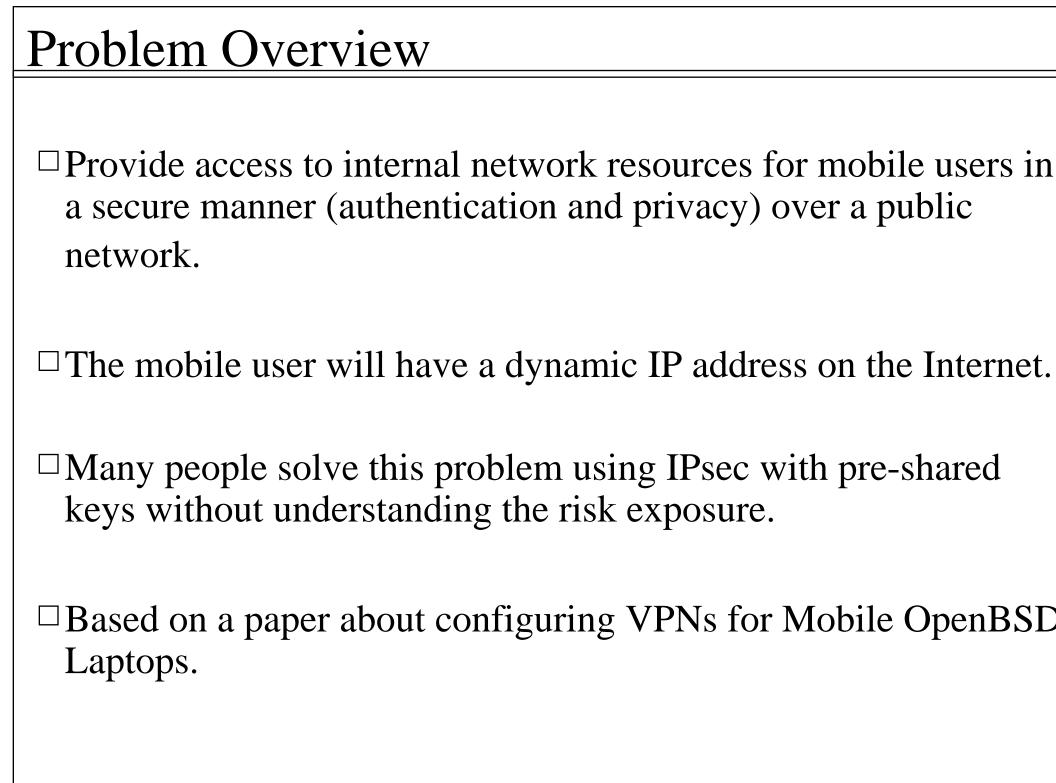
# Mobile IPsec VPN Weaknesses & Solutions

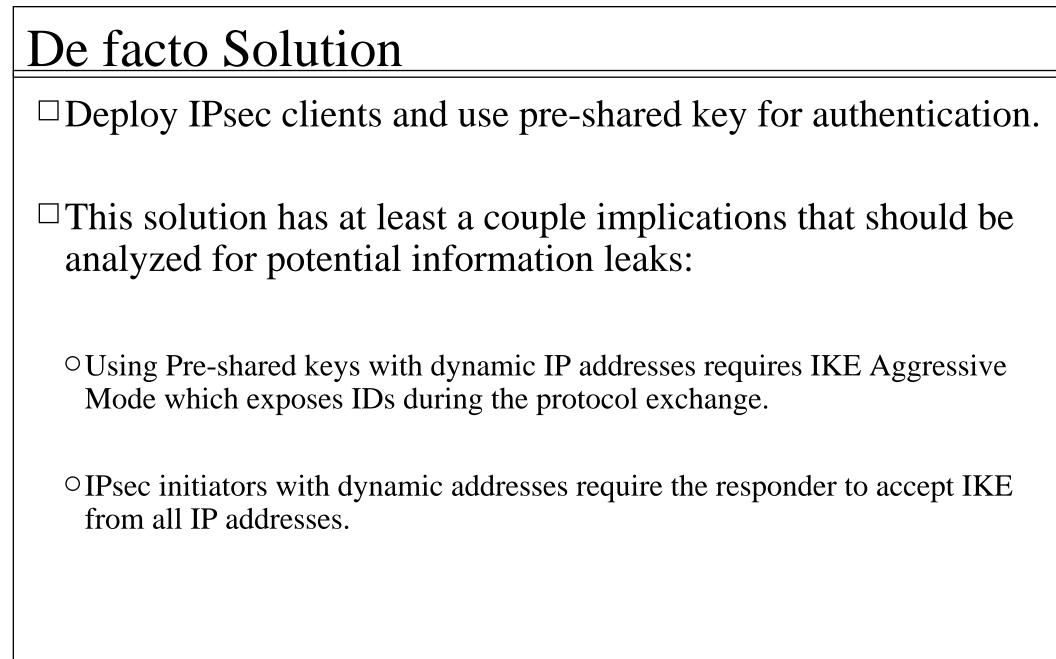
(with a heavy dose of IPsec info)

Brett Eldridge beldridg@pobox.com http://pobox.com/~beldridg/

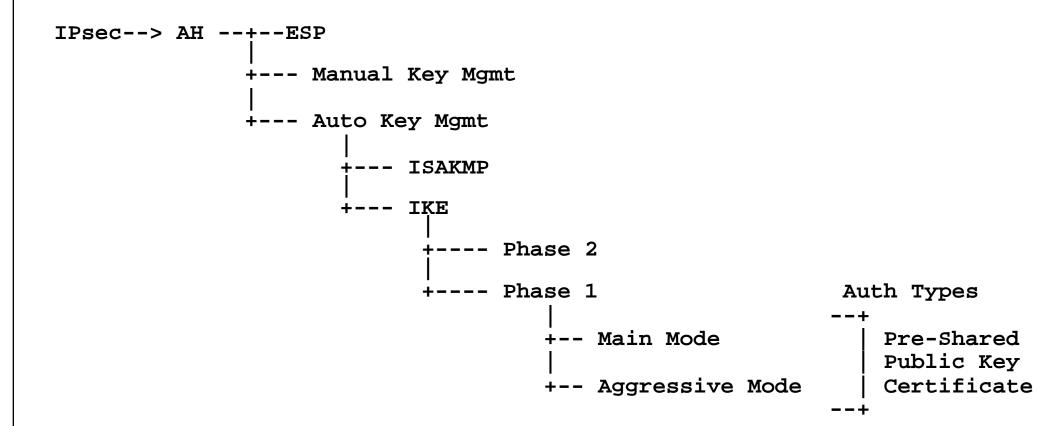
Copyright (c) 2002 Brett Eldridge

# Outline □ Problem Overview □ IPsec Overview OIKE Details ▶Phase 1 Negotiation □ Potential Mobile VPN Solutions Using IPsec OPre-shared keys Certificates □ IKE Daemon Fingerprinting Concepts





# IPsec Diagram



#### **IPsec Overview**

- ☐ Two primary security protocols:
  - OAuthentication Header (AH) provides data integrity and authentication but no confidentiality. (ip\_proto 51)
  - Encapsulating Security Payload (ESP) provides data integrity, authentication, and/or confidentiality. (ip\_proto 50).
- □ Need to cover the details of IPsec to understand the concepts discussed later in the presentation.

Source: RFC2401

# More Terminology

- □SA (Security Association): Tuple consisting of SPI + Dst. IP + Protocol Type (AH or ESP)
- □ SPI (Security Parameter Index): An unique reference (or "cookie") used to uniquely identify a SA. Required to lookup the correct decryption and authentication method for that SA.
- □ Nonce = Randomly generated value used to defeat playback attacks.
- □ Initiator = The device that starts or initiates the IKE protocol negotiation. In this case, the mobile user.
- □ Responder = The device that receives the first IKE message. In this case, the gateway to the internal network.

# Key Management

- □ The crux of the IPsec problem is key distribution and SA management. IPsec defines two broad classes of key management.
- ☐ Manual Key Management
  - OMust manually configure all IPsec parameters for a Security Association to occur. Requires n(n-1)/2 key exchanges for a fully meshed VPN with n nodes.
- □ Using Automatic Key Exchange Protocols
  - ○ISAKMP
  - $\circ$ IKE
  - oetc.

# Manual Key Management

- ☐ Manually configure encryption keys, SPI, src address, dst address, etc. on both ends.
  - Requires pre-negotiated keys for both encryption and authentication. This is usually done via voice or encrypted email.
- □ This doesn't scale because the keys are static and adding a new node involves manually distributing keys to all the existing nodes.
- □ Static keys imply that if an attacker figures out one key, they own the whole VPN until the key is manually changed by hand on all nodes.

# Manual Key Example (OpenBSD)

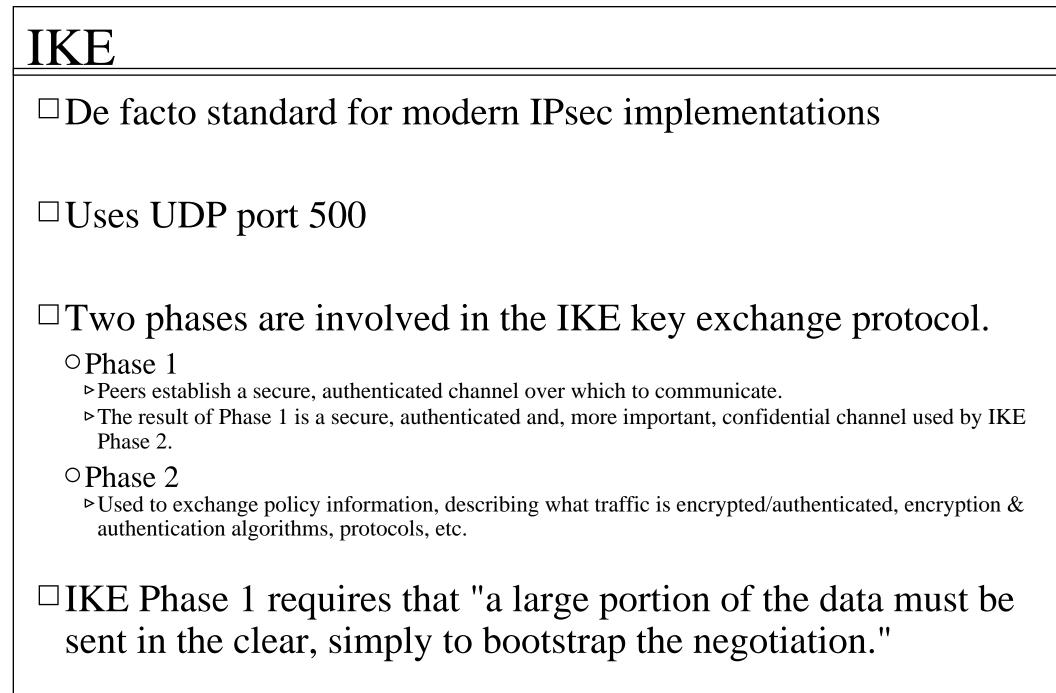
□On each host, you must perform the following:

```
ipsecadm new esp -spi 1000 -src 192.168.5.1 -dst 192.168.25.9
-enc blf -auth sha1 -key 7762d8707255d974168cbb1d274f8bed4cbd3364
-authkey 6a20367e21c66e5a40739db293cf2ef2a4e6659f

ipsecadm new esp -spi 1001 -dst 192.168.5.1 -src 192.168.25.9
-enc blf -auth sha1 -key 7762d8707255d974168cbb1d274f8bed4cbd3364
-authkey 6a20367e21c66e5a40739db293cf2ef2a4e6659f
```

# Automatic Key Management Protocols

- □ Automate the create of SA, SPI values and the encryption, authentication keys.
- □ Example Protocols
  - OISAKMP (rfc 2408) Internet Security Association and Key Management Protocol.
  - OAKLEY (rfc2412)
  - OIKE (rfc 2409) Internet Key Exchange. A conglomeration of various pieces of ISAKMP, OAKLEY, SKEME. Therefore, it is the only protocol used for automated key management of IPsec.



Source: draft-ietf-ipsec-properties

#### IKE Phase 1 Authentication Methods

- □ Applies to both Main Mode and Aggressive Mode
- □ Digital Signatures
  - ox509 based
- ☐ Two types of Public Key Encryption
  - OMust Pre-exchange public keys
  - ONot many implementations support this
- □ Pre-Shared Keys
  - OProbably the most widely deployed method

# Phase 1 Modes: Aggressive vs. Main Mode

- ☐ Main Mode uses 6 messages while Aggressive Mode uses 3 messages; therefore Aggressive Mode is generally faster.
- □ In Aggressive Mode, due to the fewer exchanges, fewer attributes can be negotiated during the exchange.
- □ Cannot negotiate DH groups during Aggressive Mode
  - OBoth sides must have pre-configured the same DH group and agree prior to Phase 1.
- ☐ Main Mode protects user identities by not sending them untithey are encrypted (also called ID\_PROT mode).

### Back to the problem...

- ☐ If the Initiator has a dynamic IP address (i.e., a mobile laptop user) you only have a few choices for authentication and modes:
  - "When using pre-shared key authentication with Main Mode, the key can only be identified by the IP address of the peer..."
- □ The implication is that the initiator and responder must both have static IP addresses in Main Mode w/ pre-shared keys.

Source: RFC2409

# Why Not?

□ In Main Mode with pre-shared keys, ID is not sent in Message 1 Can only identify the other party by IP address:

```
Initiator
                                          Responder
Message
          HDR, SA
   2
                                        HDR, SA
          HDR, KE, Ni
                                        HDR, KE, Nr
   5
          HDR*, IDii, HASH I
                                        HDR*, IDir, HASH R
                                <--
         is an ISAKMP HDR (cookies, etc)
   HDR
   SA
         is a SA Negotiation payload (transforms, etc)
         is a nonce
   Nx
         is the DH Key Exchange payload
   \mathbf{KE}
         is the identification payload
   IDxx
   HASH is the hash payload
         indicates encrypted payload
   HDR*
```

### Dynamic IP Address Auth Methods

□ Table illustrates whether dynamic or static IP addresses can be used and whether the ID is encrypted for a given auth method and Phase 1 mode.

<b>.</b>	Main Mode	Aggressive
Pre-Shared	Static	Static/Dynamic
Keys	ID Encrypted	ID Exposed
X509v3	Static/Dynamic	Static/Dynamic
Certificates	ID Encrypted	ID Exposed
Public	Static/Dynamic	Static/Dynamic
Keys	ID Encrypted	ID Encrypted

□ If you want to use pre-shared keys with mobile users, you must use Aggressive Mode which exposes the ID.

# Aggressive Mode w/ Pre-Shared Keys

☐ Many people use this solution because pre-shared keys are easy to configure.

□ With Aggressive mode, the user identity must be sent in the clear as part of the Initiator's Phase 1 initial message.

# Aggressive Mode w/ Pre-Shared Keys

```
Initiator
                                          Responder
Message
         HDR, SA, KE, Ni,
          TDii
                                       HDR, SA, KE, Nr,
                               <--
                                       IDir, HASH R
   3
         HDR, HASH I
  HDR
         is an ISAKMP HDR (cookies, etc)
         is a SA Negotiation payload (transforms, etc)
   SA
         is a nonce
  Nx
  KE
         is a Key Exchange payload
  IDxx is the identification payload
  HASH is the hash payload
```

□ Note: Initiator/Responder ID is not encrypted.

# IKE - Aggressive Mode Example - Message 1

```
16:46:31.186253 24.0.73.59.500 > 24.0.73.58.500: [udp sum ok] isakmp v1.0
exchange AGGRESSIVE
        cookie: 0b010baa691aff18->000000000000000 msgid: 00000000 len: 261
        payload: SA len: 52 DOI: 1(IPSEC) situation: IDENTITY ONLY
            payload: PROPOSAL len: 40 proposal: 1 proto: ISAKMP spisz: 0
xforms:
 1
                payload: TRANSFORM len: 32
                    transform: 0 ID: ISAKMP
                        attribute ENCRYPTION ALGORITHM = 3DES CBC
                        attribute HASH ALGORITHM = SHA
                        attribute AUTHENTICATION METHOD = RSA SIG
                        attribute GROUP DESCRIPTION = MODP_1024
                        attribute LIFE TYPE = SECONDS
                        attribute LIFE DURATION = 3600
        payload: KEY EXCH len: 132
        payload: NONCE len: 20
        payload: ID len: 29 type: USER FQDN = "brett@atomicgears.com" (ttl
64, id 16678)
```

# Implications of exposing User ID

- □ Traffic Analysis
  - OWhat if you are using IPsec in a government oppressed country?
- □ Potential risks if you are passing ID and using legacy authentication on back-end systems (e.g., RADIUS).
- □ Correlate individual with a specific IP address. Since the mobile user is now outside the corporate firewall...
  - obill@microsoft.com
- □ It is more important to realize what you are exposing in a given situation and assess those risks for your organization.

# Possible Solution: Use Certificates with Main Mode

- □ Potentially high deployment costs:
  - ○CA infrastructure
  - Create pub/priv key pairs
  - ○Sign CSR
  - OTransport to end user
  - ○Install at end user
  - <sup>o</sup>Create and constantly update CRLs
- □ Should you protect certificate with passphrase?

# IKE - Main Mode Example - Message 1

# IKE Fingerprinting

- □ The other implication of requiring support for initiators with dynamic IP addresses is that the responder must answer requests from any IP address.
- □ Probe a remote gateway that has a IKE daemon to determine the system details. Two prime examples are:
  - Vendor ID
  - Encryption/Auth algorithms supported

# Vendor ID Payload

- □ "The vendor defined constant MUST be unique"
- □RFC recommended usage is to hash a string of vendor name plu version, etc.
  - OProvides the capability to determine not only the vendor, but also the exact version of code running.
  - ONeed to develop a table of hashes vs. vendor ID's.
- □ Most vendors don't alarm on failed negotiations some log.
- □Great way to fingerprint systems similar to NMAP.

Source: RFC2409

### IKE - Main Mode - Message 2

```
16:49:59.505470 24.0.73.58.500 > 24.0.73.59.500: [udp sum ok] isakmp v1.0
exchange ID PROT
        cookie: bd2bd9fb3452e431->f70de4ff98926f04 msgid: 00000000 len: 136
        payload: SA len: 52 DOI: 1(IPSEC) situation: IDENTITY ONLY
            payload: PROPOSAL len: 40 proposal: 1 proto: ISAKMP spisz: 0
xforms: 1
                payload: TRANSFORM len: 32
                    transform: 1 ID: ISAKMP
                        attribute ENCRYPTION ALGORITHM = 3DES CBC
                        attribute HASH ALGORITHM = SHA
                        attribute GROUP DESCRIPTION = MODP_1024
                        attribute AUTHENTICATION METHOD = RSA SIG
                        attribute LIFE TYPE = SECONDS
                        attribute LIFE DURATION = 3600
        payload: VENDOR len: 32
        payload: VENDOR len: 24 (ttl 64, id 29109)
```

# Example Vendor ID

VENDOR len: 24 48 65 61 72 74 42 65 61 74 5f 4e 6f 74 69 66 79

eartbeat Notify

# Encryption Algorithms/Authentication

□ Send different transforms to the remote side to map which encryption and authentication algorithms are supported.

□ Some implementations support NULL for encryption.

#### Recommendations

- □ If possible, limit IKE connections to specific IP addresses or ranges.
- □ If you must support mobile users:
  - OUse Main Mode with certificates if possible
  - Ouse a single dial-up provider and limit connections to their IP address range.
  - Ounderstand IKE log messages of your specific implementation.
  - OIf your vendor doesn't log failed IKE negotiations, bug them.