Mobile IPsec VPN Weaknesses & Solutions

(with a heavy dose of IPsec info)

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

Outline

- Problem Overview
- IPsec Overview
  - IKE Details
    - Phase 1 Negotiation
- Potential Mobile VPN Solutions Using IPsec
  - Pre-shared keys
  - Certificates
- IKE Daemon Fingerprinting Concepts

Problem Overview

- Provide access to internal network resources for mobile users in a secure manner (authentication and privacy) over a public network.
- The mobile user will have a dynamic IP address on the Internet.
- Many people solve this problem using IPsec with pre-shared keys without understanding the risk exposure.
- Based on a paper about configuring VPNs for Mobile OpenBSD Laptops.

De facto Solution

- Deploy IPsec clients and use pre-shared key for authentication.

- This solution has at least a couple implications that should be analyzed for potential information leaks:

  - Using Pre-shared keys with dynamic IP addresses requires IKE Aggressive Mode which exposes IDs during the protocol exchange.

  - IPsec initiators with dynamic addresses require the responder to accept IKE from all IP addresses.

IPsec Diagram

```
IPsec--> AH --+--ESP
              |
              +--- Manual Key Mgmt
              |
              +--- Auto Key Mgmt
                     |
                     +--- ISAKMP
                     |
                     +--- IKE
                           |
                           +---- Phase 2
                           |
                           +---- Phase 1                  Auth Types
                                    |                    --+
                                    +-- Main Mode          | Pre-Shared
                                    |                      | Public Key
                                    +-- Aggressive Mode    | Certificate
                                                         --+
```

IPsec Overview

- Two primary security protocols:
  - Authentication 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
  - Must 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
  - IKE
  - etc.

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
  - ISAKMP (rfc 2408) - Internet Security Association and Key Management Protocol.
  - OAKLEY (rfc2412)
  - IKE (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.

IKE

- De facto standard for modern IPsec implementations
- Uses UDP port 500
- Two phases are involved in the IKE key exchange protocol.
  - Phase 1
    - Peers establish a secure, authenticated channel over which to communicate.
    - The result of Phase 1 is a secure, authenticated and, more important, confidential channel used by IKE Phase 2.
  - Phase 2
    - Used to exchange policy information, describing what traffic is encrypted/authenticated, encryption & authentication algorithms, protocols, etc.
- IKE Phase 1 requires that "a large portion of the data must be sent in the clear, simply to bootstrap the negotiation."

Source: draft-ietf-ipsec-properties

IKE Phase 1 Authentication Methods

- Applies to both Main Mode and Aggressive Mode
- Digital Signatures
  - x509 based
- Two types of Public Key Encryption
  - Must Pre-exchange public keys
  - Not many implementations support this
- Pre-Shared Keys
  - Probably 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
  - Both sides must have pre-configured the same DH group and agree prior to Phase 1.
- **Main Mode protects user identities by not sending them unti they 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:

```
Message      Initiator                          Responder
-------    ---------------                   ---------------
   1       HDR, SA                    -->
   2                                  <--      HDR, SA
   3       HDR, KE, Ni                -->
   4                                  <--      HDR, KE, Nr
   5       HDR*, IDii, HASH_I         -->
   6                                  <--      HDR*, IDir, HASH_R
```

```
   HDR    is an ISAKMP HDR  (cookies, etc)
   SA     is a SA Negotiation payload (transforms, etc)
   Nx     is a nonce
   KE     is the DH Key Exchange payload
   IDxx   is the identification payload
   HASH   is the hash payload
   HDR*   indicates encrypted payload
```

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.

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

```
Message       Initiator                        Responder
-------    ---------------                  ---------------
   1       HDR, SA, KE, Ni,     -->
           IDii
   2                            <--     HDR, SA, KE, Nr,
                                        IDir, HASH_R
   3       HDR, HASH_I          -->



   HDR   is an ISAKMP HDR  (cookies, etc)
   SA    is a SA Negotiation payload (transforms, etc)
   Nx    is a nonce
   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->0000000000000000 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
  - What 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...
  - bill@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
  - Transport to end user
  - Install at end user
  - Create and constantly update CRLs
- Should you protect certificate with passphrase?

IKE - Main Mode Example - Message 1

```
16:49:57.846014 24.0.73.59.500 > 24.0.73.58.500:  [udp sum ok] isakmp v1.0
exchange ID_PROT
        cookie: bd2bd9fb3452e431->0000000000000000 msgid: 00000000 len: 80
        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 (ttl 64, id 38502)
```

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.
  - Provides the capability to determine not only the vendor, but also the exact version of code running.
  - Need 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

this is the same packet with the hex dump of the vendor ID information

```
  VENDOR len: 32
  "0d8c0568a230722eedc296f5cc706c63fc88303000000000d0000030a04000018"

  VENDOR len: 24
  "486561727442656174 5f4e6f74696679386b01000a000084"
```

you can see:

```
 VENDOR len: 32  0d8c0568a230722eedc296f5cc706c63fc88303
                 ---------------------------------------
                     SHA1 of (vendor name + version)

 VENDOR len: 24  48 65 61 72 74 42 65 61 74 5f 4e 6f 74 69 66 79
                 -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
                 H  e  a  r  t  b  e  a  t  _  N  o  t  i  f  y
```

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:
  - Use Main Mode with certificates if possible
  - Use a single dial-up provider and limit connections to their IP address range.
  - Understand IKE log messages of your specific implementation.
  - If your vendor doesn’t log failed IKE negotiations, bug them.