Realities of IPv6 IPsec Deployment APNIC 26 – Christchurch, New Zealand August 2008

Merike Kaeo merike@doubleshotsecurity.com



Topics Covered

- IPsec standard done but still evolving (that's a good thing)
- Practical Deployment Considerations
- Personal Observations
- Sample Configurations



IPsec Components

- AH (Authentication Header)
 - Authentication is applied to the entire packet, with the mutable fields in the IP header zeroed out
 - If both ESP and AH are applied to a packet, AH follows ESP
 - Standard requires HMAC-MD5-96 and HMAC-SHA1-96....older implementations also support keyed MD5
- ESP (Encapsulating Security Payload)
 - Must encrypt and/or authenticate in each packet
 - Encryption occurs before authentication
 - Authentication is applied to data in the IPsec header as well as the data contained as payload
 - Standard requires DES 56-bit CBC and Triple DES. Can also use RC5, IDEA, Blowfish, CAST, RC4, NULL
- IKE (Internet Key Exchange)
 - Automated SA (Security Association) creation and key management



Relevant Standard(s)

- IETF specific
 - rfc2409: IKEv1
 - rfc4301: IPsec Architecture (updated)
 - rfc4303: IPsec ESP (updated)
 - rfc4306: IKEv2
 - rfc4718: IKEv2 Clarifications
 - rfc4945: IPsec PKI Profile
- IPv6 and IPsec
 - rfc4294: IPv6 Node Requirements
 - Rfc4552: Authentication/Confidentiality for OSPFv3
 - rfc4877: Mobile IPv6 Using IPsec (updated)
 - rfc4891: Using IPsec to secure IPv6-in-IPv4 Tunnels



IPsec Maintenance Working Group

- First Meeting in Dublin IETF (July 2008)
- A charter item specific for IPv6
 - standards-track extension to IKEv2 that provides full IPv6 support for IPsec remote access clients that use configuration payloads. This work will be based on draft-eronen-ipsec-ikev2-ipv6-config. The WG shall solicit help and reviews from the 6MAN WG to ensure that all aspects of IPv6 are properly considered.



Considerations For Using IPsec

- Security Services
 - Data origin authentication
 - Data integrity
 - Replay protection
 - Confidentiality
- Size of network
- How trusted are end hosts can apriori communication policies be created?
- Vendor support
- What other mechanisms can accomplish similar attack
 risk mitigation



Non-Vendor Specific Deployment Issues

- Historical Perception
 - Configuration nightmare
 - Not interoperable
- Performance Perception
 - Need empirical data
 - Where is the real performance hit?
- Standards Need Cohesion
- IPv6 Certification Entities Need Cohesion



Vendor Specific Deployment Issues

- Lack of interoperable defaults
 - A default does NOT mandate a specific security policy
 - Defaults can be modified by end users
- Configuration complexity
 - Too many knobs
 - Vendor-specific terminology
- Good News: IPv6 support in most current implementations



Transport vs Tunnel Mode



Transport Mode:End systems are the initiator and recipient of protected trafficTunnel Mode:Gateways act on behalf of hosts to protect traffic



Protecting Against Scanning Attacks



	IPsec Security Policy Database									
From	То	Protocol	Dst Port	Policy						
2001:DB8:6665:0100::DE	2001:DB8:6665:01C8::3B	TCP / UDP	53 (DNS)	ESP: SHA1, AES-256						
2001:DB8:6665:0100::DE	2001:DB8:6665:AF75::3B	TCP	25 (SNMP)	ESP: SHA1, AES-256						
2001:DB8:6665:0100::DE	2001:DB8:6665:AF75::3D	UDP	1812/1813 (RADIUS)	ESP: SHA1, AES-128						
2001:DB8:6665:0100::DE	2001:DB8:6665:AF75::3D	UDP	514 (Syslog)	ESP: SHA1, 3DES						
2001:DB8:6665:0100::DE	2001:DB8:6665:AF75::/48	TCP / UDP	ANY	ESP: SHA1						



IPv6 Architectures using IPsec

- Protect all traffic using IPsec for data origin authentication and integrity
- Add confidentiality as dictated by security policy

Need to dispel myth that using IPsec mandates the demise of network layer defense mechanisms



IPv6 IPsec Concerns

- Are enough people aware that IKEv2 is not backwards compatible with IKEv1?
 - IKEv1 is used in most IPv6 IPsec implementations
 - Will IKEv2 implementations first try IKEv2 and then revert to IKEv1?
- Is IPsec implemented for IPv6?
 - Some implementations ship IPv6 capable devices without IPsec capability....this needs to change
- OSPFv3
 - All vendors 'IF' they implement IPsec used AH
 - Latest standard to describe how to use IPsec says MUST use ESP w/Null encryption and MAY use AH



IPv6 IPsec Concerns (cont)

- What is transport mode interoperability status?
 - Will end user authentication be interoperable?
- PKI Issues
 - Which certificates do you trust?
 - How does IKEv1 and/or IKEv2 handle proposals with certificates?
 - Should common trusted roots be shipped by default?
 - Who is following and implementing pki4ipsec-ikecert-profile (rfc4945)
- Have mobility scenarios been tested?
 - Mobility standards rely heavily on IKEv2



Enhancements Needed

- Standards Modifications
 - Need to take into consideration Stateless Autoconfiguration where Router Advertisement sends network prefix
 - Need to be able to differentiate between encrypted versus integrity protected traffic
- Usability
 - Interoperable defaults
 - Consistent terminology



IPv6 IPsec ESP





ESP Header Format

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

	Security Parameter Index (SPI)								
	Sequence Number								
	Initialization Vector (IV)								
үрте	Payload Data (Variable)								
ICR	Padding (0-255 bytes)								
Ш	Padding Length Next Header								
	Authentication Data (ICV)								

SPI:	Arbitrary 32-bit number that specifies SA to the receiving device
Seq #:	Start at 1 and must never repeat; receiver may choose to ignore
IV:	Used to initialize CBC mode of an encryption algorithm
Payload Data:	Encrypted IP header, TCP or UDP header and data
Padding:	Used for encryption algorithms which operate in CBC mode
Padding Length:	Number of bytes added to the data stream (may be 0)
Next Header:	The type of protocol from the original header which appears in the
	encrypted part of the packet
Auth Data:	ICV is a digital signature over the packet and it varies in length
	depending on the algorithm used (SHA-1, MD5)



Default Issues

Vendor A	Vendor B	Vendor C
IKE Phase 1	IKE Phase 1	IKE Phase 1
-SHA1	-MD5	-SHA1
-RSA-SIG	-Pre-Share Key	-Pre-Share Key
-Group 1	-Group 5	-Group 2
-Lifetime 86400 Sec	-Lifetime 86400 Sec	-Lifetime 86400 Sec
-Main Mode	-Main Mode	-Aggressive Mode
IKE Phase 2	IKE Phase 2	IKE Phase 2
-PFS	-PFS	-PFS
-Group 1	-Group 5	-Group 2



Terminology Issues

IKE Phase 1	DH Key Length	IKE Phase 2
IKE Phase 1 SA	DH Group	IKE Phase 2 SA
IKE SA	Modp #	IPsec SA
ISAKMP SA	Group #	Quick Mode
Main Mode		

Configuration complexity increased with vendor specific configuration terms



Potentially Easy Configuration



Syslog server 2001:DB8:6665:AF75::3D authenticate esp-null sha1 pre-share 'secret4syslog'

TFTP server 2001:DB8:6665:AF75::3D authenticate esp-null aes128 pre-share 'secret4tftp'

BGP peer 2001:DB8:8888:BAD::66 authenticate esp-null aes128 pre-share 'secret4AS#XXX'



Interoperable Defaults For SAs

 Security Association groups elements of a conversation together



- ESP encryption algorithm and key(s)
- Cryptographic synchronization
- SA lifetime
- SA source address
- Mode (transport or tunnel)

Do we want integrity protection of data ? Do we want to keep data confidential ? Which algorithms do we use ? What are the key lengths ? When do we want to create new keys ? Are we providing security end-to-end ?

How Do We Communicate Securely ?



IPv6 IPsec WishList

- Common Terminology
- Interoperable Defaults
 - RFC 4308 was a good start but needs to be updated
- Interoperability Tests
 - Both transport and tunnel mode
 - Mobility scenarios
- API Standards
- Repeatable performance data



Pretty Good IPsec Policy

- IKE Phase 1 (aka ISAKMP SA or IKE SA or Main Mode)
 - 3DES (AES-192 if both ends support it)
 - Lifetime (480 min = 28800 sec)
 - SHA-1
 - DH Group 14 (aka MODP# 14)
- IKE Phase 2 (aka IPsec SA or Quick Mode)
 - 3DES (AES-192 if both ends support it)
 - Lifetime (60 min = 3600 sec)
 - SHA-1
 - PFS 2
 - DH Group 14 (aka MODP# 14)



Routers: Configuring IPsec

- For IPv6, consider using transport mode between routers and syslog servers, tftp servers, snmp servers, etc.
- Document for Cisco IPv6 IPsec configuration:
 - http://www.lseltd.com/univercd/cc/td/doc/product/software/ ios123/123cgcr/ipv6_c/v6_ipsec.pdf
- Document for Juniper IPsec configuration:
 - http://www.pacificbroadband.com/techpubs/software/junos/ junos83/feature-guide-83/html/fg-ipsec13.html#1139838



STEP 1 Configure the IKE Phase 1 Policy (ISAKMP Policy)

Cisco literature refers to IKE Phase 1 as the ISAKMP policy. It is configured using the command: crypto isakmp policy *priority*

Multiple policies can be configured and the priority number, which ranges from 1 to 10,000, denotes the order of preference that a given policy will be negotiated with an ISAKMP peer. The lower value has the higher priority. Once in the ISAKMP configuration mode, the following parameters can be specified are:

Encryption Algorithm Hash Algorithm Authentication Method Group Lifetime



STEP 2 Set the ISAKMP Identity

The ISAKMP identity specifies how the IKE Phase 1 peer is identified, which can be either by IP address or host name. The command to use is:

crypto isakmp *identity* {*IP address* | *hostname*}

By default, a peer's ISAKMP identity is the peer's IP address. If you decide to change the default just keep in mind that it is best to always be consistent across your entire IPsec-protected network in the way you choose to define a peer's identity.



STEP 3 Configure the IPsec AH and ESP Parameters

The AH and ESP parameters are configured with the following commands:

crypto ipsec transform-set *transform-set-name* <transform 1> <transform 2> mode [tunnel | transport] crypto ipsec security-association lifetime seconds

STEP 4 Configure the IPsec Traffic Selectors

The traffic selectors are configured by defining extended access-lists. The *permit* keyword causes all IP traffic that matches the specified conditions to be protected by IPsec



STEP 5 Configure the IKE Phase 2 (IPsec SA) Policy

This step sets up a crypto map which specifies all the necessary parameters to negotiate the IPsec SA policy. The following commands are required:

crypto map crypto-map-name seq-num ipsec-isakmp match address access-list-id set peer [IP address | hostname] set transform-set transform-set-name set security-association lifetime seconds seconds set pfs [group1 | group 2]



STEP 6 Apply the IPsec Policy to an Interface

The configured crypto map is then applied to the appropriate interface using the crypto map *crypto-map-name* command. It is possible to apply the same crypto map to multiple interfaces. This case would require the use of the command:

crypto map crypto-map-name local-address interface-id

Using this command, the identifying interface will be used as the local address for IPsec traffic originating from or destined to those interfaces sharing the same crypto map. A loopback interface should be used as the identifying interface.



Unix IPsec IKE Daemons

- Racoon2 (IKEv1 and IKEv2 and KINK)
 - http://www.racoon2.wide.ad.jp/w/
- Ipsec-tools (IKEv1)
 - port of KAME's IPsec utilities to the Linux-2.6 IPsec implementation; it supports NetBSD and FreeBSD as well
 - http://ipsec-tools.sourceforge.net/
- Strongswan (IKEv1 and IKEv2)
 - http://www.strongswan.org/
- Openikev2 (IKEv2)
 - http://openikev2.sourceforge.net/



LINUX and MACOSX machines

- Type command ' man racoon '
 - Read how to set-up racoon, the name for this particular IKE software
- Type command ' man setkey '
 - This command is used to set up the SA database
- The following files are located in */etc/raccoon*:
 - *psk.txt* file which contains the shared secrets
 - *raccoon.conf* file which configures IKE phase 1 and IKE phase 2 parameters



Set Up Security Policy Database

- Create a file named ' *ipsec.conf* ' which will be used with *setkey* to establish the correct security associations. The file should have the following information:
 - flush;
 - spdflush;
 - spdadd 2001:DB8:6665:AF75::3D/128
 2001:DB8:8888:BAD::66/128 any -P out
 ipsec esp/transport//require ;
 - spdadd 2001:DB8:8888:BAD::66/128 2001:DB8:6665:AF75::3D/128 any -P in ipsec esp/transport//require ;



Creating SA Database

- Test to see what happens when you try and create an SA database:
- Type the following:
 - setkey -f /etc/racoon/ipsec.conf
- Use the 'setkey -P -D ' command to see if appropriate entries have been created



Pre-Shared Key Configuration

- Edit the psk.txt file to add the peer IP address and the pre-shared secret key:
 - # file for pre-shared keys used for IKE authentication
 - # format is: 'identifier' 'key'
 - *# For example:*
 - # 10.1.1.1 flibbertigibbet
 - # www.example.com 12345
 - # foo@www.example.com micropachycephalosaurus
 - <peer IPv6 address> <shared secret>
- Since the psk.txt file contains sensitive information make sure that the file is appropriately protected:
 - chmod 600 /etc/raccoon/psk.txt



Racoon.conf file

```
# Racoon IKE daemon configuration file.
# See 'man racoon.conf' for a description of the format
    and entries.
path include "/etc/racoon";
path pre shared key "/etc/racoon/psk.txt";
path certificate "/etc/racoon/certs";
log debug;
remote anonymous
        exchange mode main;
        lifetime time 480 min;
        proposal {
            encryption algorithm 3des;
             hash_algorithm sha1;
             authentication method pre shared key;
             dh_group 14;
```

```
sainfo anonymous
```

```
{
```

pfs_group 2; lifetime time 60 min ; encryption_algorithm 3des, blowfish 448, rijndael ; authentication_algorithm hmac_sha1 hmac_md5 ; compression_algorithm deflate ;



Testing Racoon

• Test racoon with the following command:

- racoon -v -f /etc/racoon/ racoon.conf -l /etc/racoon/test.log

• The '-l /etc/racoon/test.log ` file is used to write any debug information in the event that there are problems.



Vista: Configuring IPsec

- Defaults work great in a MS-only environment
- Else, need to edit firewall (wf.mmc)

🔍 🗸 🕌 « Start M	lenu 🕨 Programs 🕨 Administr	ative Tools	↓ 4	Search	
Organize ▼ III Viev	ws ▼ 🗔 Open 🚯 Burn Name	Date modified	Туре	Size	
Decuments	🛃 Computer Management	11/2/2006 5:53 AM	Shortcut	2 KB	
Documents	Data Sources (ODBC)	11/2/2006 5:52 AM	Shortcut	2 KB	
Pictures	🔝 Event Viewer	11/2/2006 5:53 AM	Shortcut	2 KB	
Music	🔝 iSCSI Initiator	11/2/2006 5:53 AM	Shortcut	2 KB	
Recently Changed	Memory Diagnostics T	11/2/2006 5:51 AM	Shortcut	2 KB	
Searches	🕞 Print Management	11/2/2006 5:54 AM	Shortcut	2 KB	
Public	🛞 Reliability and Perform	11/2/2006 5:52 AM	Shortcut	2 KB	
	Security Configuration	11/2/2006 5:54 AM	Shortcut	2 KB	
	a services	11/2/2006 5:52 AM	Shortcut	2 KB	
	System Configuration	11/2/2006 5:51 AM	Shortcut	2 KB	
	Task Scheduler	11/2/2006 5:53 AM	Shortcut	2 KB	
	Windows Firewall with	11/2/2006 5:52 AM	Shortcut	2 KB	



Vista: Configuring IPsec





Vista: Customizing IPsec Settings

	Customize IPsec Settings
ndows Firewall with Advanced Security on Local Computer	IPsec will use these settings to establish secured connections when there are active connection security rules.
IPsec defaults	When you use the default, settings that have been specified at a higher precedence Group Policy object will be used.
Specify settings used by IPsec to	
establish secured connections.	Key exchange (Main Mode)
	Default (recommended)
IPsec exemptions	Advanced Customize
Exempting ICMP from all IPsec requirements can simplify	
	Data protection (Quick Mode)
Formet ICMB from IBases	Default (recommended)
Exempt ICIVIF from IFSec: [No (default)	Advanced Customize
	Authentication Method
	O Default
	Computer and User (using Kerberos V5)
	 Computer (using Kerberos V5)
	 User (using Kerbergs V5)
	Computer certificate from this certification authority:
	Drowse
	Customize
OK Cancel <u>Apply</u>	
	Learn more about IPsec settings
	What are the default values?
	OK Cancel



Vista IPsec Defaults

indows Firewall with Advanced Security	arch Favorites Default Settings Firewall with Advanced Security						
	Default settin Advanced Set These are the default Windows Firewall with are made.	ngs for V curity IPsec configu Advanced Se	Vindows Firewall with aration settings for connection security rules that courity uses before any configuration changes	rity			
	Settings		Value	E	Default Sett	ings	
	Key lifetime (minute	s)	480 minutes	.,	Data megney	0.01	
					Key lifetimes	60 minutes/100,000 KB	
	Key lifetime (session	ns)	U sessions*		Data encryption		
	Key exchange algori	ithm	Diffie-Hellman Group 2		Setting	Value	
	Security methods (in	ntegrity)	SHA1		Protocol	ESP	
	Security methods (e	ncryption)	AES-128 (primary)/3-DES (secondary)		Data integrity	SHA1	
	*A session limit of zer	*A session limit of zero (0) causes rekeys to be determined only by the Key				AES-128 (primary)/3-DES (secondary)	
	Data Integrity	setting.		Key lifeti	Key lifetimes	60 minutes/100,000 KB	
	Setting	Value	e (primary)/AH (secondary)		Authentication Met	hod	
	Protocol	ESP (p			By default, computer authentication metho	Kerberos (Kerberos version 5 authentication) is used as the d.	
	Data integrity	SHA1			How default set	ttings work with Group Policy	
4	Kev lifetimes	60 mir	utes/100.000 KB	-	Policies created using distributed with Group	the Windows Firewall with Advanced Security snap-in and Policy, are applied in this order of precedence:	
					1. Highest preced	ence Group Policy object (GPO)	
					a annuality		



Vista: Customizing Data Protection

)ata integrit Protect data ntegrity algo	y a from modifica orithms. Those ity algorithms:	ation on the network with these higher in the list are tried first.		Data integrity Protect data the network Those higher	and encrypt from modific with these in r in the list ar	ion ation and prese tegrity and enc e tried first. stion algorithms	erve confidentiality on ryption algorithms.
Protocol	Integrity	Key Lifetime (minutes/KB)		Protocol	Integrity	Encryption	Key Lifetime (min
ESP AH	SHA1 SHA1	60/100,000 60/100,000	*	ESP ESP AH and	SHA1 SHA1 SHA1,	AES-128 3DES AES-256	60/100,000 60/100,000 60/100,000
Add	Edi	t Remove		Add	Ed	it] [R	emove



Vista: Customizing Key Exchange

security method	5	Key exchange algorithm	
Use the followin	g security methods for key exch	ange. O Elliptic Curve Diffie-Hellman P-384	
Security method	ls:	Strongest security, highest resources usage. Compatible only with Windows Vista and later systems.	
Integrity	Encryption	Elliptic Curve Diffie-Hellman P-256	
SHA1 SHA1	AES-128 3DES	 Stronger security, medium resource usage. Compatible only with Windows Vista and later systems. 	
		Diffie-Hellman Group 14	
		Stronger than DH Group 2.	
		Diffie-Hellman Group 2 (default)	
Add	Edit Remove	Stronger than DH Group 1.	
Key lifetimes		Diffie-Hellman Group 1	
Determine wher options are sele irst threshold is	a new key is generated. If both cted, a new key is generated wh reached.	hen the Compatibility only.	
Key lifetime (in n	ninutes):	480 🚖	
	essions):	0	
Key lifetime (in s			
Key lifetime (in s am more about	key exchange settings		



Vista: Customizing Authentication

First authentication Specify computer authentication methods to use during IPsec negotiations. Those higher in the list are tried first. First authentication methods: Method		Second authentication Specify user authentication methods use during IPsec negotiations. Thos	or a health certificate to e higher in the list are	
		Second authentication methods:	First Authentication Method Select the credential to use for first authentication:	
Add	Additional Information ros V5) Edit Remove	*	Additional Additional Additional Add Edit Second authentication is optional	 Computer (Kerberos V5) Computer (NTLMv2) Computer certificate from this certification authority (CA): Browse Accept only health certificates Enable certificate to account mapping Preshared key (not recommended):
m more about aut at are the default	hentication settings values?		A second authentication cannot be s preshared key is in the first authentica	Preshared key authentication is less secure than other authentication methods. Preshared keys are stored in plaintext. When preshared key authentication is used, Second Authentication cannot be used. Leam more about the first authentication method OK Cance



Conclusions

- IPsec is a complex standard but user configurations shouldn't be
- Using IPsec does NOT mean you have to encrypt the data (providing traffic integrity can be useful too)
- Don't leave IPsec out when you are trying to gain experience with IPv6 - time to fix usability issues is NOW

