Network Security Tutorial

Daejeon, South Korea

19 February 2019

As part of:

APNIC

Outline

- Network Security Fundamentals
- Infrastructure Security
- Secure Routing with RPKI
- VPN & IPsec
- IPv6 Security
- Network Security Monitoring

APNIC

Network Security Fundamentals

Internet Evolution

LAN connectivity

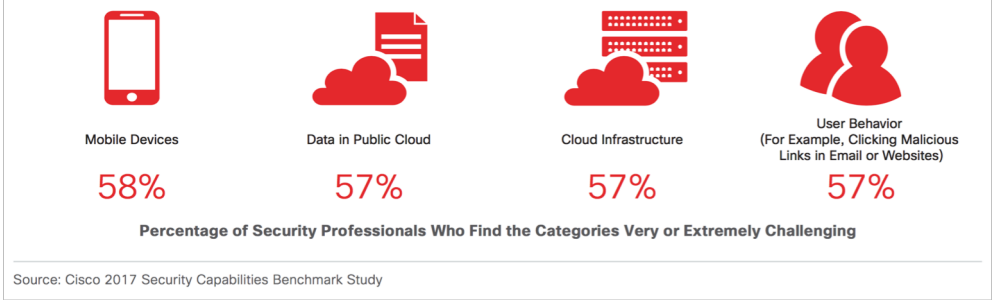
Application-specific
More online content

Application/data
hosted in the “cloud”

Different ways to handle security as the Internet evolves

Threat Landscape

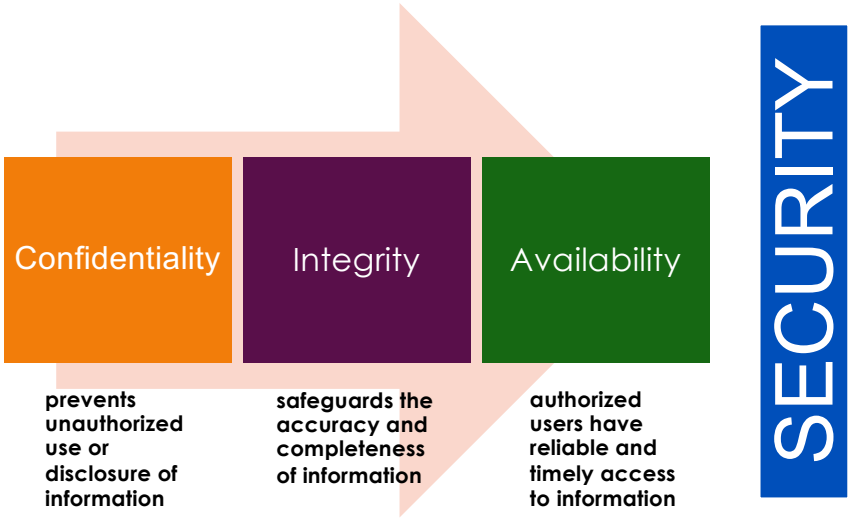
Figure 1 Security Professionals' Biggest Sources of Concern Related to Cyber Attacks



Percentage of Security Professionals Who Find the Categories Very or Extremely Challenging

Source: Cisco 2017 Security Capabilities Benchmark Study

Goals of Information Security



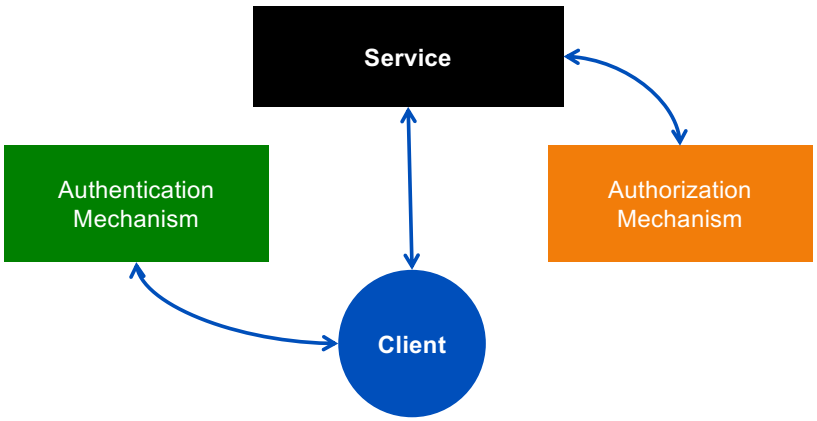
APNIC

Access Control

- provides 3 essential services:
  - Authentication (identification of a user)
  - Authorization (who is allowed to use a service)
  - Accountability (what did a user do)

APNIC

Authentication vs. Authorization



"Authentication simply identifies a party, authorization defines whether they can perform certain action" – RFC 3552

Integrity

- Security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity
- Data integrity
  - The property that data has when it has not been altered in an unauthorized manner
- System integrity
  - The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation

Source: NIST Risk Management Guide for Information Technology Systems

Risk, Threats, and Vulnerability

- Threat
  - Any circumstance or event with the potential to cause harm to a networked system
- Vulnerability
  - A weakness in security procedures, network design, or implementation that can be exploited to violate a corporate security policy
- Risk
  - The possibility that a particular vulnerability will be exploited

Threat

- "a motivated, capable adversary"
- Examples:
  - Human Threats
    - Intentional or unintentional
    - Malicious or benign
  - Natural Threats
    - Earthquakes, tornadoes, floods, landslides
  - Environmental Threats
    - Long-term power failure, pollution, liquid leakage

Vulnerability

- A weakness in security procedures, network design, or implementation that can be exploited to violate a corporate security policy
  - Software bugs
  - Configuration mistakes
  - Network design flaw
  - Lack of encryption
- Where to check for vulnerabilities?
- Exploit
  - Taking advantage of a vulnerability

Risk

- Likelihood that a vulnerability will be exploited
- Some questions:
  - How likely is it to happen?
  - What is the level of risk if we decide to do nothing?
  - Will it result in data loss?
  - What is the impact on the reputation of the company?
- Categories:
  - High, medium or low risk

Risk = Threat * Vulnerability (* Impact)

What Are You Protecting?

- Identify Critical Assets
  - Hardware, software, data, people, documentation
- Place a Value on the Asset
  - Intangible asset – importance or criticality
  - Tangible asset – replacement value, training costs and/or immediate impact of the loss
- Determine Likelihood of Security Breaches
  - What are threats and vulnerabilities ?

Attack Motivation

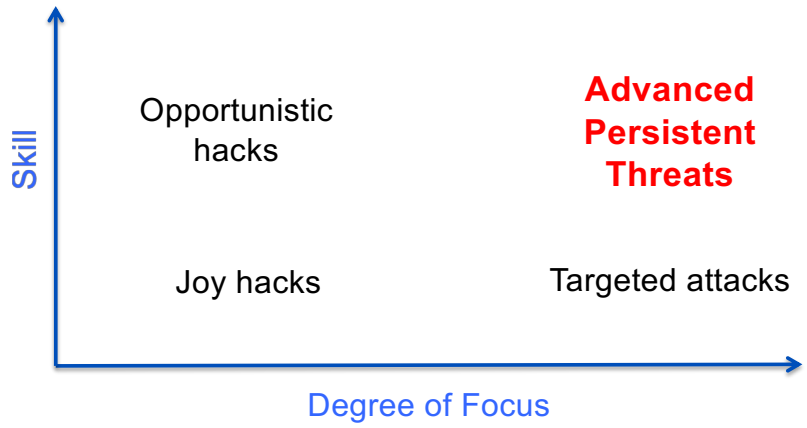
- Criminal
  - Criminal who use critical infrastructure as a tools to commit crime
  - Their motivation is money
- War Fighting/Espionage/Terrorist
  - What most people think of when talking about threats to critical infrastructure
- Patriotic/Principle
  - Large groups of people motivated by cause - be it national pride or a passion aka Anonymous

Attack Motivation

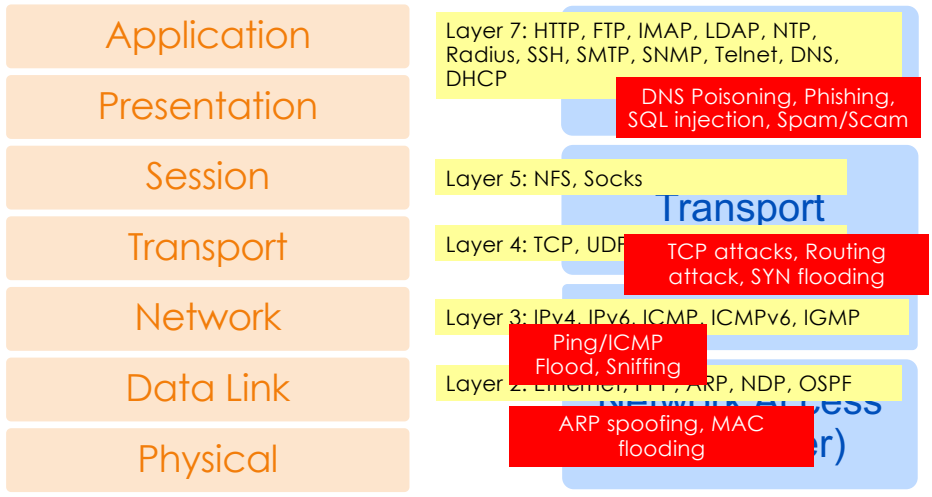
- Nation States want SECRETS
- Organized criminals want MONEY
- Protesters or activists want ATTENTION
- Hackers and researchers want KNOWLEDGE

Source: NANOG60 keynote presentation by Jeff Moss, Feb 2014

The Threat Matrix



Attacks on Different Layers



Host and Infrastructure Security

Think of ALL the devices

- Oct 2016
  - ~1Tbps attack on Dyn
- Nov 2016
  - 900k+ Deutsche Telecom subscribers offline
- Feb 2018
  - 1.35Tbps attack on Github
  - Memcache with spoofed source address

Turn Off Unused Services

Feature	Description	Default	Recommendation	Command
CDP	Proprietary layer 2 protocol between Cisco devices	Enabled		no cdp run
TCP small servers	Standard TCP network services: echo, chargen, etc	11.3: disabled 11.2: enabled	This is a legacy feature, disable it explicitly	no service tcp-small-servers
UDP small servers	Standard UDP network services: echo, discard, etc	11.3: disabled 11.2: enabled	This is a legacy feature, disable it explicitly	no service udp-small-servers
Finger	Unix user lookup service, allows remote listing of logged in users.	Enabled	Unauthorized persons don't need to know this, disable it.	no service finger
HTTP server	Some Cisco IOS devices offer web-based configuration	Varies by device	If not in use, explicitly disable, otherwise restrict access	no ip http server
Bootp server	Service to allow other routers to boot from this one	Enabled	This is rarely needed and may open a security hole, disable it	no ip bootp server

Turn Off Unused Services

Feature	Description	Default	Recommendation	Command
PAD Service	Router will support X.25 packet assembler service	Enabled	Disable if not explicitly needed	no service pad
IP source routing	Feature that allows a packet to specify its own route	Enabled	Can be helpful in attacks, disable it	no ip source-route
Proxy ARP	Router will act as a proxy for layer 2 address resolution	Enabled	Disable this service unless the router is serving as a LAN bridge	no ip proxy-arp
IP directed broadcast	Packets can identify a target LAN for broadcasts	Enabled (11.3 & earlier)	Directed broadcast can be used for attacks, disable it	no ip directed-broadcast

Configuration Example

```
! Per-interface
interface <interface-ID>
 no ip redirects
 no ip directed-broadcast
 no ip proxy arp
 no cdp enable
!
interface Null0
 no ip unreachables
 no ipv6 unreachables
!
```

```
! Globally
no ip domain-lookup
no cdp run
no ip http server
no ip http secure-server
no ip source-route
no ipv6 source-route
no service finger
no ip bootp server
no service udp-small-servers
no service tcp-small-server
```


Route Filters - Inbound

```
router bgp 17821
 neighbor x6:x6::x6 remote-as <transit|peer>
 neighbor x6:x6::x6 description v6 peering with upstream|peer
 neighbor x4.x4.x4.x4 remote-as <transit|peer>
 neighbor x4.x4.x4.x4 description v4 peering with upstream|peer
 !
 address-family ipv4
  neighbor x4.x4.x4.x4 prefix-list <prefix-filter> in
 !
 address-family ipv6
  neighbor x6:x6::x6 prefix-list <prefix-filter> in
```

Transit provider: Block bogus routes and accept everything
Peer: Only accept their prefixes (and downstream)

IPv4 Transit - Inbound

```
no ip prefix-list in-filter
ip prefix-list in-filter deny 0.0.0.0/0             ! Default
ip prefix-list in-filter deny 0.0.0.0/8 le 32       ! Network Zero
ip prefix-list in-filter deny 10.0.0.0/8 le 32      ! RFC1918
ip prefix-list in-filter deny 100.64.0.0/10 le 32   ! RFC6598 shared address
ip prefix-list in-filter deny <your prefix>/X le 32 ! Your address space
ip prefix-list in-filter deny 127.0.0.0/8 le 32     ! Loopback
ip prefix-list in-filter deny 169.254.0.0/16 le 32  ! APIPA
ip prefix-list in-filter deny 172.16.0.0/12 le 32   ! RFC1918
ip prefix-list in-filter deny 192.0.0.0/24 le 32    ! IETF Protocol
ip prefix-list in-filter deny 192.0.2.0/24 le 32    ! TEST1
ip prefix-list in-filter deny 192.168.0.0/16 le 32  ! RFC1918
ip prefix-list in-filter deny 198.18.0.0/15 le 32   ! Benchmarking
ip prefix-list in-filter deny 198.51.100.0/24 le 32 ! TEST2
ip prefix-list in-filter deny 203.0.113.0/24 le 32  ! TEST3
ip prefix-list in-filter deny 224.0.0.0/4 le 32     ! Multicast
ip prefix-list in-filter deny 240.0.0.0/4 le 32     ! Future Use
ip prefix-list in-filter deny 0.0.0.0/0 ge 25       ! Prefixes >/24
ip prefix-list in-filter permit 0.0.0.0/0 le 32
```


IPv6 Transit - Inbound

```
no ipv6 prefix-list v6in-filter
ipv6 prefix-list v6in-filter deny 2001::/32 le 128          ! Teredo subnets
ipv6 prefix-list v6in-filter deny 2001:db8::/32 le 128      ! Documentation
ipv6 prefix-list v6in-filter deny 2002::/16 le 128          ! 6to4 subnets
ipv6 prefix-list v6in-filter deny <your::/32> le 128        ! Your prefix
ipv6 prefix-list v6in-filter deny 3ffe::/16 le 128          ! Old 6bone
ipv6 prefix-list v6in-filter deny fc00::/7 le 128           ! ULA
ipv6 prefix-list v6in-filter deny fe00::/9 le 128           ! Reserved IETF
ipv6 prefix-list v6in-filter deny fe80::/10 le 128          ! Link-local
ipv6 prefix-list v6in-filter deny fec0::/10 le 128          ! Link-local
ipv6 prefix-list v6in-filter deny ff00::/8 le 128           ! Link-local
ipv6 prefix-list v6in-filter permit 2000::/3 le 48          ! Global Unicast
ipv6 prefix-list v6in-filter deny ::/0 le 128
```

IPv4/IPv6 Peer - Inbound

```
no ip prefix-list peer-in-filter
ip prefix-list peer-in-filter permit A.A.A.A/18 le 24       ! Peer's prefix
ip prefix-list peer-in-filter permit B.B.B.B/19 le 24       ! Peer's prefix
ip prefix-list peer-in-filter deny 0.0.0.0/0 ge 32          ! Deny everything else
!
!
no ipv6 prefix-list peerv6-in-filter
ipv6 prefix-list peerv6-in-filter permit 2002:A::/32 le 48  ! Peer's prefix
ipv6 prefix-list peerv6-in-filter deny ::/0 le 128          ! Deny everything else
```


Outbound Routes

```
router bgp 17821
 neighbor x6:x6::x6 remote-as <transit|peer>
 neighbor x6:x6::x6 description v6 peering with upstream|peer
 neighbor x4.x4.x4.x4 remote-as <transit|peer>
 neighbor x4.x4.x4.x4 description v4 peering with upstream|peer
 !
 address-family ipv4
  neighbor x4.x4.x4.x4 prefix-list <out-filter> out
 !
 address-family ipv6
  neighbor x6:x6::x6 prefix-list <outv6-filter> out
!
!
no ip prefix-list <out-filter>
ip prefix-list peer-filter permit M.M.M.M/19 le 24     ! Your prefix
ip prefix-list peer-filter permit N.N.N.N/19 le 24     ! Your prefix
ip prefix-list peer-filter deny 0.0.0.0/0 ge 32        ! Deny everything else
!
no ipv6 prefix-list <outv6-filter>
ipv6 prefix-list peerv6-filter permit 2002:M::/32 le 48 ! Your prefix
ipv6 prefix-list peerv6-filter deny ::/0 le 128         ! Deny everything else
```

Transit/Peer - Only advertise your prefixes (and your downstream)

Bogons

- Not all IP (v4 and v6) have been allocated by IANA
- Addresses that should not be seen on the Internet are called “Bogons”
  - RFC1918 + Reserved space
- IANA publishes a list of number resources that have been delegated to RIRs and end-users

Bogons

- Commonly found as source addresses of DDoS packets
- We should have ingress and egress filters for bogon routes
  - Should not route them nor accept them from peers
- We could manually craft prefix filters based on the bogon list from IANA
  - But Bogon list is dynamic
  - New allocations made from reserved blocks frequently

Bogon Route Server Project

- project by Team Cymru that provides bogon tracking and notification through a multihop eBGP peering session.
  - makes the automation of filters simple for even the largest network
  –
- Traditional bogons (AS65333)
  - Martians + prefixes not allocated by IANA
- Full-bogons (AS65532)
  - Traditional + prefixes allocated to RIRs but not yet assigned to ISPs or end-users

https://www.team-cymru.com/bogon-reference-bgp.html

Bogon Config

```
router bgp 17821
 neighbor cymru-bogons peer-group
 neighbor cymru-bogons remote-as 65332
 neighbor cymru-bogons description Peering with Cymru Bogon RS
 neighbor cymru-bogons ebgp-multihop 255
 neighbor cymru-bogons password <md5-pw>
 neighbor cymru-bogons update-source Loopback0
 !
 neighbor cymru-v6bogons peer-group
 neighbor cymru-v6bogons remote-as 65332
 neighbor cymru-v6bogons description Peering with Cymru IPv6 Bogon RS
 neighbor cymru-v6bogons ebgp-multihop 255
 neighbor cymru-v6bogons password <md5-pw>
 neighbor cymru-v6bogons update-source Loopback0
 !
 neighbor 2620:0:6B0:XXXX::20 peer-group cymru-v6bogons
 neighbor 38.XXX.XXX.20 peer-group cymru-bogons
 !
 address-family ipv4
  neighbor cymru-bogons prefix-list DENY-ALL out
  neighbor cymru-bogons maximum-prefix 10000 90
  neighbor 38.XXX.XXX.20 activate
 !
 address-family ipv6
  neighbor cymru-v6bogons prefix-list DENYv6-ALL out
  neighbor cymru-v6bogons maximum-prefix 100000 90
  neighbor 2620:0:6B0:XXXX::20 activate
```

Bogon Config

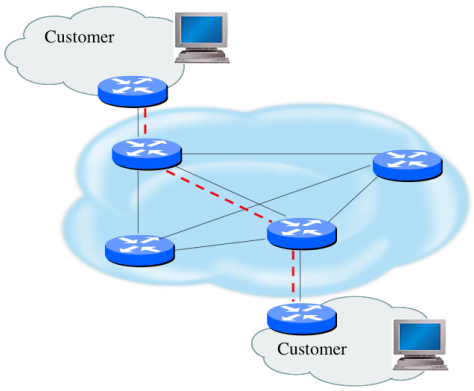
```
!Do not announce anything to Bogon RS
ip prefix-list DENY-ALL seq 5 deny 0.0.0.0/0 le 32
ipv6 prefix-list DENYv6-ALL seq 5 deny ::/0 le 128
!
!Define communities for Bogons
!Cymru full-bogons are tagged with the community 65332:888
ip bgp-community new-format
ip community-list 10 permit 65332:888
ip community-list 11 permit 17821:888  !our own bogon tag for iBGP peers

!Define route-map to set the next-hop address for the bogons (null routed)
!Set local (no-export) community to propagate bogons to partial iBGP peers
route-map CYMRU-BOGONS permit 10
 match community 10
 set local-preference 1000
 set community 17821:888 no-export
 set ip next-hop 192.0.2.1
!
route-map CYMRU-v6BOGONS permit 10
 match community 10
 set local-preference 1000
 set community 17821:888 no-export
 set ipv6 next-hop 2001:db8::1
```


Bogon Config

```
!Null route the bogon next hops (this is also needed on all iBGP peers)
ip route 192.0.2.1 255.255.255.255 null0
ipv6 route 2001:db8::1/128 null0
!
!Define route-map to propagate the bogons to partial iBGP peers:
route-map iBGP-BOGONS permit 10
 description allow our bogons
 match community 11
!
route-map v6-iBGP-BOGONS permit 10
 description allow our bogons
 match community 11
!
```

Securing The Data Path

- Filtering and rate limiting are primary mitigation techniques
- Edge filter guidelines for ingress filtering (BCP38/BCP84)
- Null-route and black-hole any detected malicious traffic
- Netflow is primary method used for tracking traffic flows
- Logging of Exceptions



Packet Filtering

```
ip access-list extended TRAFFIC-IN
 deny udp/tcp any any eq 19                  ! Chargen
 deny udp/tcp any any range 135 139          ! netbios stuff
 deny udp any any eq 123                     ! no one should use  our NTP
 deny tcp any any eq 445                     ! Blaster/SMB worm
 deny tcp any any eq 1025                    ! uSoft RPC exploit
 deny tcp any any eq 1337                    ! Redshell backdoor
 deny tcp any any eq 1433                    ! MS SQL worm
 deny udp any any eq 1434                    ! MS SQL worm
 deny udp any any eq 2049                    ! Sun NFS
 deny tcp any any eq 2745                    ! Blaster worm
 deny tcp any any eq 3001                    ! NessusD backdoor
 deny tcp any any eq 3127                    ! MyDoom worm
 deny tcp any any eq 3128                    ! MyDoom worm
 deny tcp any any eq 5000                    ! WindowsXP UPnP port
 deny tcp any any eq 6129                    ! Dameware backdoor
 deny udp/tcp any any eq 11211               ! Memcached exploit
 deny tcp any any eq 11768                   ! Dipnet/Oddbob worm
 deny tcp any any eq 15118                   ! Dipnet/Oddbob worm
 deny icmp any any fragments                 ! Block ICMP fragments
 permit icmp any any
 deny ip <your-address> <wildcard> any
 permit ip any any
```

BCP38

- Network Ingress Filtering

- Only allow traffic with valid source addresses to
  - Leave your network
    - Only packets with source address from your own address space
  - To enter/transit your network
    - Accept only source addresses from downstream or customer address space

https://tools.ietf.org/html/bcp38

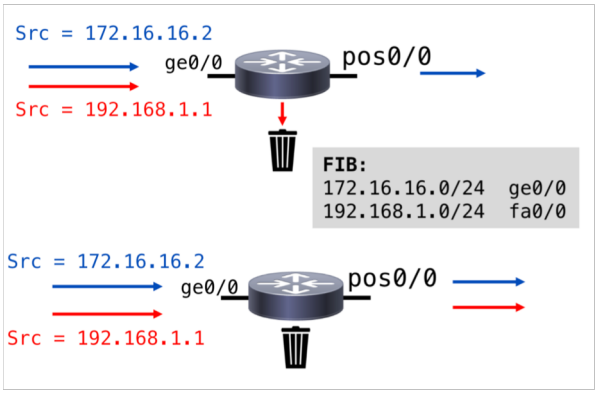
uRPF – Unicast Reverse Path

- Unicast Reverse Path Forwarding (uRPF)
  - Router verifies if the source address of any packet received is in the FIB table and reachable (routing table)
    - DROP if not!
  - Recommended on customer facing interfaces

```
(config-if)#ip/ipv6 verify unicast source reachable-via {rx | any}
```

uRPF – Unicast Reverse Path

- Modes of Operation
  - **Strict**: verifies both source address and incoming interface with FIB entries
  - **Loose**: verifies existence of route to source address



Configuration Files

- Be careful sending config files
  - MD5 validation
  - SCP to copy files and images
- Use tools like **rancid** and **oxidized** to periodically check them against modified config files

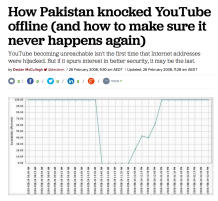
Secure Routing with RPKI

Misdirection / Hijacking Incidents

- Amazon (AS16509) Route53 hijack – April2018
  - AS10279 (eNET) announced/originated more specifics (/24s) of Amazon Route53's prefix (205.251.192.0/21)
    - 205.251.192.0/24 ……. 205.251.199.0/24
    - https://ip-ranges.amazonaws.com/ip-ranges.json
  - Its peers, like AS6939 (HE), shared these routes with 1000s of their own peers…
  - The motive?
    - During the period, DNS servers in the hijacked range only responded to queries for myetherwallet.com
    - Responded with addresses associated with AS41995/AS48693)

Misdirection / Hijacking Incidents

- YouTube Incident
  - Occurred 24 Feb 2008 (for about 2 hours)
  - Pakistan Telecom announced YT block
- Google (AS15169) services downed
  - Occurred 5 Nov 2012 (for 30 minutes)
  - Moratel Indonesia (AS23947)


How Pakistan knocked YouTube offline (and how to make sure it never happens again)


Why Google Went Offline Today and a Bit about How the Internet Works

How frequent do these hijacking incidents happen?

Cyber Criminals exploiting the vulnerability

- BGP Hijacking for Cryptocurrency Profit (2014)
  - http://www.secureworks.com/cyber-threat-intelligence/threats/bgp-hijacking-for-cryptocurrency-profit/
- Spamhaus DDoS Attack (2013)
  - http://www.bgpmon.net/looking-at-the-spamhouse-ddos-from-a-bgp-perspective/
- Detecting BGP Attacks in 2014
  - https://pacsec.jp/psj14/PSJ2014_Guillaum_presentation.pdf

How we address this…

A network should only originate his own prefix
How do we verify & avoid false advertisement?

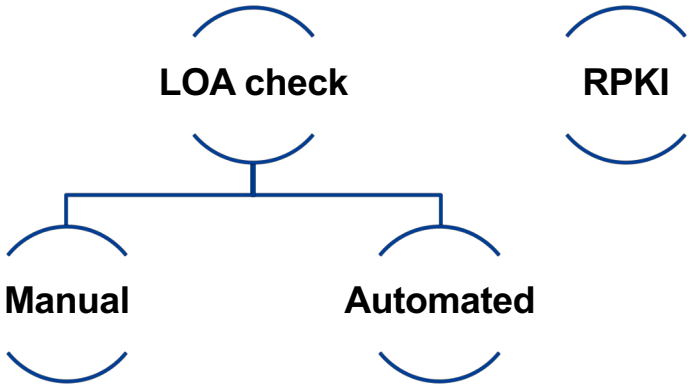
A provider should filter prefixes they propagate from customers
Transitive trust; BGP is a trust-based system
Check the legitimacy of address (LoA)
Passive Countermeasure

Strict filter on Interconnection
BGP router can filter in UPDATE Messages
Useful filtering can be done by upstream provider

Automate Filter Maintenance
Use the Route Object

Current practice

Tools and techniques



Technology and learning curve

What is RPKI?

What is RPKI?

- A robust security framework for verifying the association between resource holder and Internet resource
- Helps to secure Internet routing by validating routes

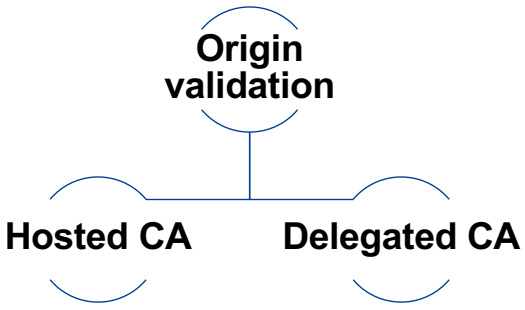
What does it solve?

- Prevents **route hijacking**
  - A prefix originated by an AS without authorization due to malicious intent
- Prevents **mis-origination**
  - A prefix that is mistakenly originated by an AS which does not own it
  - Also route leakage
  - due to configuration mistake or fat finger

How does it work?

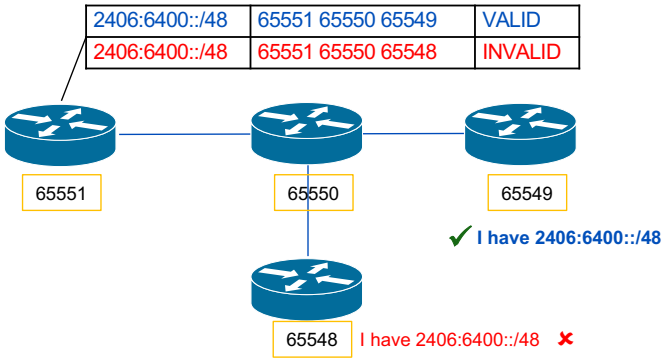
Is this AS number (ASN) authorized to announce this IP address range?

RPKI implementation

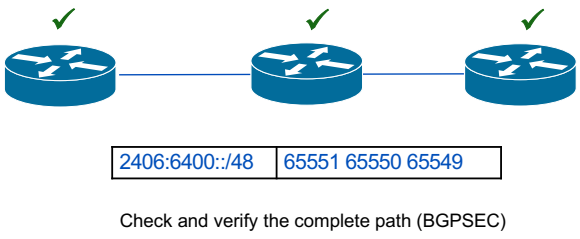


*upgrade at least ASBRs to RPKI capable code

RPKI Origin Validation



RPKI Path Validation



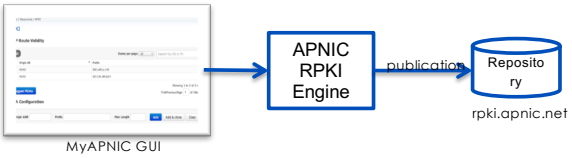
Check and verify the complete path (BGPSEC)

Main Components

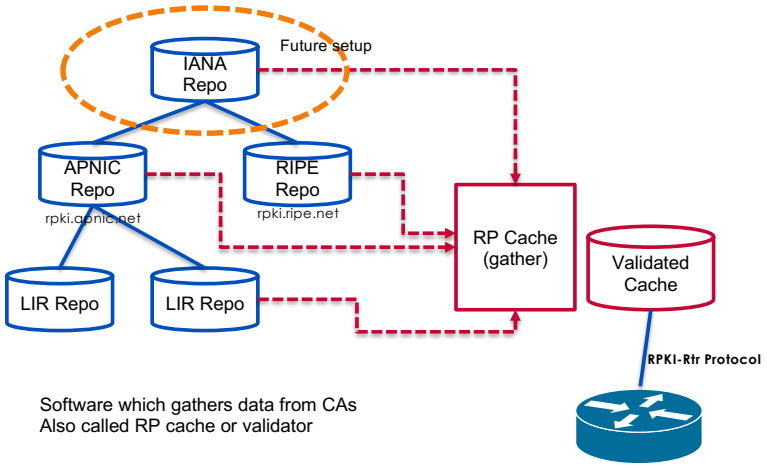
- Certificate Authority (CA)
  - Internet registries (RIR, NIR, LIR)
  - Issues certificates to members (delegates with resources)
  - Allows address holders to use the CA system to issue ROAs for their prefixes
- Relying Party (RP)
  - Software that gathers data from the CA

Issuing Party

- Internet Registries (RIR, NIR, Large LIRs)
- Acts as a Certificate Authority and issues certificates to members with resources
- Often provides a web interface to issue ROAs for customer prefixes
- Publishes the ROA records into a repository



Relying Party



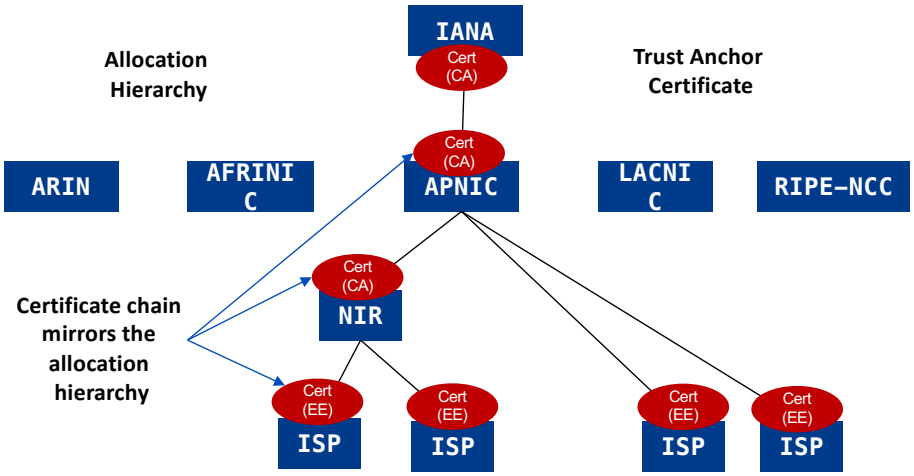
RPKI Building Blocks

1. PKI and Trust anchors
2. Route Origin Authorizations (ROA)
3. RPKI Validators

X.509 Certificate with 3779 Extension

- Resource certificates are based on the X.509 v3 certificate format defined in RFC 5280
- Extended by RFC 3779 – binds a list of resources **(IP, ASN)** to the subject of the certificate
- SIA – Subject Information Access; contains a URI that references the directory

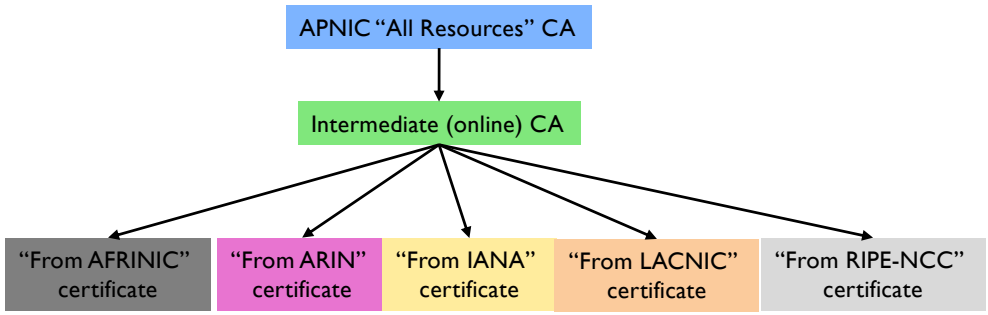
Trust Anchor (TA)



Source : http://isoc.org/wp/ietfjournal/?p=2438

Single Trust anchor

- 27 Feb 2018: a single expanded trust anchor
  - https://blog.apnic.net/2018/02/27/updating-rpki-trust-anchor-configuration/



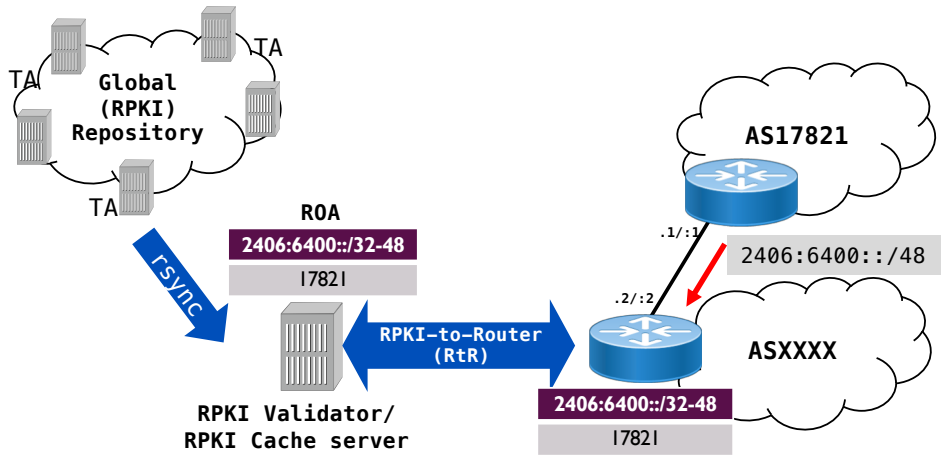
Route Origin Authorization (ROA)

- A signed digital object that contains a list of address prefixes and one AS number
- It is an authority created by a prefix holder to authorize an AS Number to originate one or more specific route advertisements

Prefix originated	203.176.189.0
Maximum prefix length	/24
Origin ASN	AS17821

- ROA is valid if a valid certificate which signs it has the prefix in its RFC 3779 extension

Origin Validation



RPKI Validation

- RPKI-capable routers can fetch the validated ROA dataset from a validated cache

VALID	Indicates that the prefix and ASN pair has been found in the database
INVALID	Indicates that the prefix is found, but • ASN received did not match, or • the prefix length is longer than the maximum length
NOT FOUND / UNKNOWN	Indicates that the prefix does not match any in the database

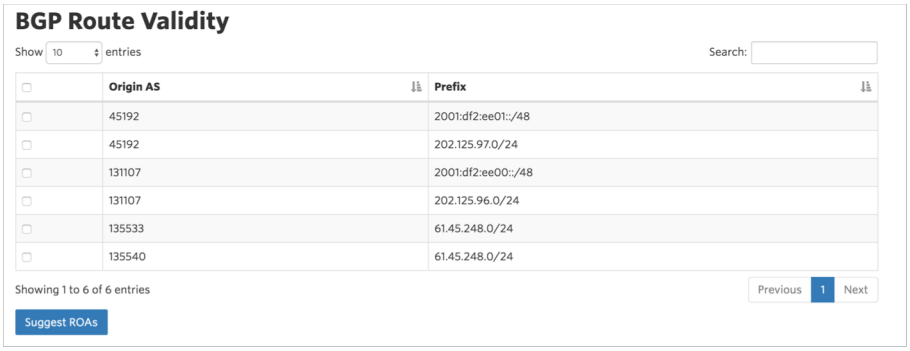
Create & publish your ROA

- MyAPNIC portal
  - Reso
  - Here is a detailed guide:

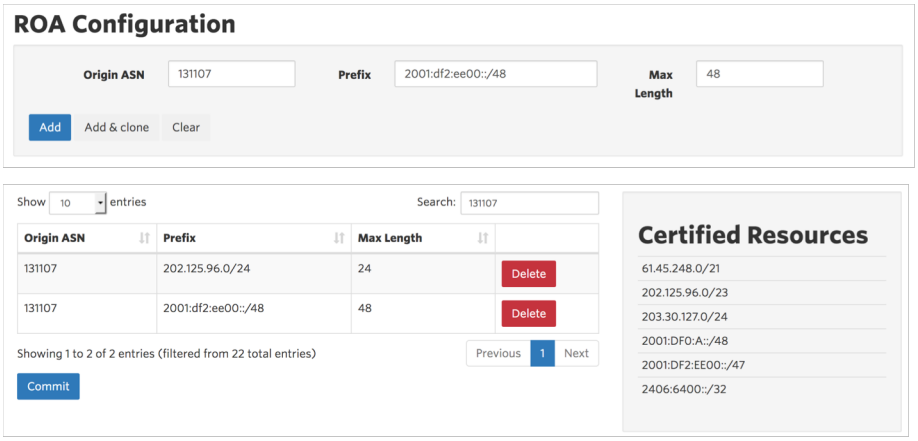
https://www.apnic.net/wp-content/uploads/2017/12/ROUTE_MANAGEMENT_GUIDE.pdf

Create (publish) your ROA

- Available prefixes for which you can create ROA



Create (publish) your ROA



Check your ROA

```
# whois -h rr.ntt.net 2001:df2:ee00::/48

route6:     2001:df2:ee00::/48
descr:      RPKI ROA for 2001:df2:ee00::/48
remarks:    This route object represents routing data retrieved from the RPKI
remarks:    The original data can be found here:
https://rpki.gin.ntt.net/r/AS131107/2001:df2:ee00::/48
remarks:    This route object is the result of an automated RPKI-to-IRR conversion
process.
remarks:    maxLength 48
origin:     AS131107
mnt-by:     MAINT-JOB
changed:    job@ntt.net 20180802
source:     RPKI  # Trust Anchor: APNIC RPKI Root
```

Check your ROA

```
# whois -h whois.bgpmon.net 2001:df2:ee00::/48

Prefix:                 2001:df2:ee00::/48
Prefix description:     APNICTRAINING-DC
Country code:           AU
Origin AS:                          131107
Origin AS Name:         APNICTRAINING LAB DC
RPKI status:            ROA validation successful
First seen:             2016-06-30
Last seen:              2018-01-21
Seen by #peers:         97
```

```
# whois -h whois.bgpmon.net "--roa 131107 2001:df2:ee00::/48"

------------------------
ROA Details
------------------------
Origin ASN:       AS131107
Not valid Before: 2016-09-07 02:10:04
Not valid After:  2020-07-30 00:00:00  Expires in 2y190d9h34m23.2000000029802s
Trust Anchor:     rpki.apnic.net
Prefixes:         2001:df2:ee00::/48 (max length /48) 202.125.96.0/24 (max length /24)
```


Check your ROA

https://bgp.he.net/

Announced By		
Origin AS	**Announcement**	**Description**
AS131107	2001:df2:ee00::/48	testing

Deploy RPKI Validator

- Multiple options:
  - RIPE RPKI Validator

```
https://www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources
```

  - Dragon Research Labs RPKI Toolkit

```
https://github.com/dragonresearch/rpki.net
```

  - Routinator

```
https://github.com/NLnetLabs/routinator
```

  - RTRlib (bird, FRR, Quagga…)

```
https://rtrlib.realmv6.org/
```


RIPE - Validator

- Download RPKI Validator

```
# wget https://lirportal.ripe.net/certification/content/static/validator/rpki-validator-app-2.25-dist.tar.gz
```

- Installation

```
tar -zxvf rpki-validator-app-2.25-dist.tar.gz
cd rpki-validator-app-2.25
./rpki-validator.sh start
```

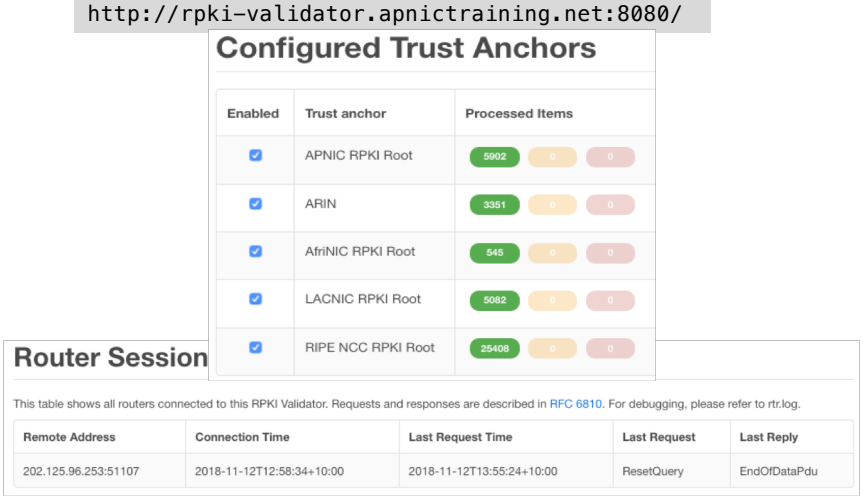
  - Need to download ARIN's TAL separately

```
wget https://www.arin.net/resources/rpki/arin-ripevalidator.tal
```

    - Move it to "<base-folder>/conf/tal" and restart

RIPE - Validator

`http://rpki-validator.apnictraining.net:8080/`



Dragon Research - Validator

- Installation on Ubuntu 16.04 Xenial

`https://github.com/dragonresearch/rpki.net/blob/master/doc/quickstart/xenial-rp.md`

- Installation
  - Add the GPG public key

```
# wget -q -O /etc/apt/trusted.gpg.d/rpki.gpg https://download.rpki.net/APTng/apt-gpg-key.gpg
```

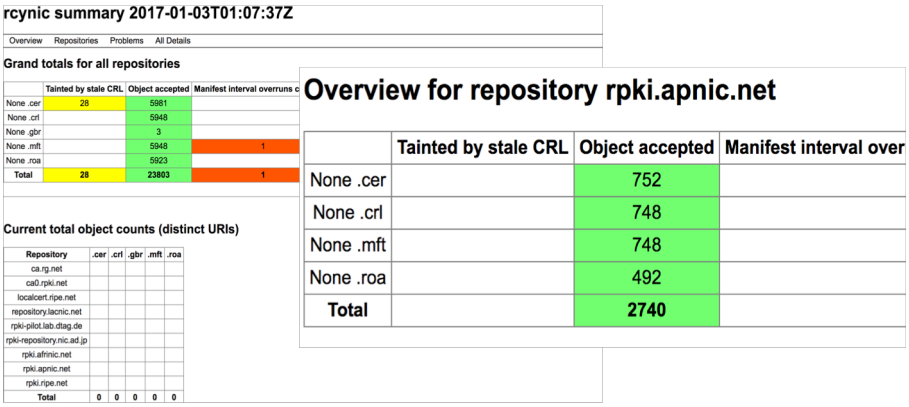
  - Add the repo to the APT source list

```
# wget -q -O /etc/apt/sources.list.d/rpki.list https://download.rpki.net/APTng/rpki.xenial.list

-q: quite (wget output)
-O: output to <file>
```

```
# apt update
# apt install rpki-rp
```

Dragon Research - Validator

```
http://rpki-dragonresearch.apnictraining.net/rcynic/
```



rcynic summary 2017-01-03T01:07:37Z

Overview Repositories Problems All Details

Grand totals for all repositories

	Tainted by stale CRL	Object accepted	Manifest interval overruns c
None .cer	28	5981	
None .crl		5948	
None .gbr		3	
None .mft		5948	1
None .roa		5923	
Total	28	23803	1

Current total object counts (distinct URIs)

Repository	.cer	.crl	.gbr	.mft	.roa
ca.rg.net					
ca0.rpki.net					
localcert.ripe.net					
repository.lacnic.net					
rpki-pilot.lab.dtag.de					
rpki-repository.nic.ad.jp					
rpki.afrinic.net					
rpki.apnic.net					
rpki.ripe.net					
Total	0	0	0	0	0

Overview for repository rpki.apnic.net

	Tainted by stale CRL	Object accepted	Manifest interval over
None .cer		752	
None .crl		748	
None .mft		748	
None .roa		492	
Total		**2740**	

Configuration - IOS

- Establishing session with the validator

```
router bgp 131107
 bgp rpki server tcp <validator-IP> port 323 refresh 120
```

- Policies based on validation:

```
route-map ROUTE-VALIDATION permit 10
 match rpki valid
 set local-preference 110
!
route-map ROUTE-VALIDATION permit 20
 match rpki not-found
 set local-preference 100
!
route-map ROUTE-VALIDATION permit 10
 match rpki invalid
 set local-preference 90
!
```

Configuration - IOS

- Apply the route-map to inbound updates

```
router bgp 131107
!---output omitted-----!
 address-family ipv4
  neighbor X.X.X.169 activate
  neighbor X.X.X.169 route-map ROUTE-VALIDATION in
 exit-address-family
 !
 address-family ipv6
  neighbor X6:X6:X6:X6::151 activate
  neighbor X6:X6:X6:X6::151 route-map ROUTE-VALIDATION in
 exit-address-family
!
```


Configuration - JunOS

- Establishing session with the validator

```
routing-options {
   autonomous-system 131107;
   validation {
       group rpki-validator {
           session <validator-IP> {
               refresh-time 120;
               port 8282;
               local-address X.X.X.253;
           }
       }
   }
}
```

Router Configuration - JunOS

```
policy-options {
   policy-statement ROUTE-VALIDATION {
       term valid {
           from {
               protocol bgp;
               validation-database valid;
           }
           then {
               local-preference 110;
               validation-state valid;
               accept;
           }
       }
       term invalid {
           from {
               protocol bgp;
               validation-database invalid;
           }
           then {
               local-preference 90;
               validation-state invalid;
               accept;
           }
       }
```

```
term unknown {
           from {
               protocol bgp;
               validation-database
unknown;
           }
           then {
               local-preference 100;
               validation-state unknown;
               accept;
           }
       }
   }
}
```

- Define policies based on the validation states

Router Configuration - JunOS

- Apply the policy to inbound updates

```
protocols {
   bgp {
       group external-peers {
           #output-ommitted
           neighbor X.X.X.1 {
               import ROUTE-VALIDATION;
               family inet {
                   unicast;
               }
           }
       }
```

```
       group external-peers-v6 {
           #output-ommitted
           neighbor X6:X6:X6:X6::1 {
               import ROUTE-VALIDATION;
               family inet6 {
                   unicast;
               }
           }
       }
   }
}
```

RPKI Verification - IOS

- IOS has only

```
#sh bgp ipv6 unicast rpki ?
  servers Display RPKI cache server information
  table   Display RPKI table entries


#sh bgp ipv4 unicast rpki ?
  servers Display RPKI cache server information
  table   Display RPKI table entries
```


RPKI Verification - IOS

- Check the RTR session

```
#sh bgp ipv4 unicast rpki servers

BGP SOVC neighbor is X.X.X.47/323 connected to port 323
Flags 64, Refresh time is 120, Serial number is 1516477445, Session ID is
8871
InQ has 0 messages, OutQ has 0 messages, formatted msg 7826
Session IO flags 3, Session flags 4008
 Neighbor Statistics:
 Prefixes 45661
 Connection attempts: 1
 Connection failures: 0
 Errors sent: 0
 Errors received: 0

Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled, Mininum incoming TTL 0, Outgoing TTL 255
Local host: X.X.X.225, Local port: 29831
Foreign host: X.X.X.47, Foreign port: 323
```

RPKI Verification - IOS

- Check the RPKI cache

```
#sh bgp ipv4 unicast rpki table
37868 BGP sovc network entries using 6058880 bytes of memory
39655 BGP sovc record entries using 1268960 bytes of memory

Network            Maxlen Origin-AS Source Neighbor
1.9.0.0/16         24     4788      0      202.125.96.47/323
1.9.12.0/24        24     65037     0      202.125.96.47/323
1.9.21.0/24        24     24514     0      202.125.96.47/323
1.9.23.0/24        24     65120     0      202.125.96.47/323
```

```
#sh bgp ipv6 unicast rpki table
5309 BGP sovc network entries using 976856 bytes of memory
6006 BGP sovc record entries using 192192 bytes of memory

Network             Maxlen Origin-AS Source Neighbor
2001:200::/32       32     2500      0      202.125.96.47/323
2001:200:136::/48   48     9367      0      202.125.96.47/323
2001:200:900::/40   40     7660      0      202.125.96.47/323
2001:200:8000::/35  35     4690      0      202.125.96.47/323
```


Check routes - IOS

```
#sh bgp ipv4 unicast 202.144.128.0/19
BGP routing table entry for 202.144.128.0/19, version 3814371
Paths: (1 available, best #1, table default)
 Advertised to update-groups:
    2
 Refresh Epoch 15
 4826 17660
   49.255.232.169 from 49.255.232.169 (114.31.194.12)
     Origin IGP, metric 0, localpref 110, valid, external, best
     Community: 4826:5101 4826:6570 4826:51011 24115:17660
     path 7F50C7CD98C8 RPKI State valid
     rx pathid: 0, tx pathid: 0x0
```

```
#sh bgp ipv6 unicast 2402:7800::/32
BGP routing table entry for 2402:7800::/32, version 1157916
Paths: (1 available, best #1, table default)
 Advertised to update-groups:
    2
 Refresh Epoch 15
 4826
   2402:7800:10:2::151 from 2402:7800:10:2::151 (114.31.194.12)
     Origin IGP, metric 0, localpref 100, valid, external, best
     Community: 4826:1000 4826:2050 4826:2110 4826:2540 4826:2900 4826:5203
     path 7F50B266CBD8 RPKI State not found
     rx pathid: 0, tx pathid: 0x0
```

RPKI Verification - JunOS

- Check the RTR session

```
>show validation session
Session                                 State Flaps   Uptime #IPv4/IPv6
records
202.125.96.46                            Up       75 09:20:59 40894/6747


>show validation session 202.125.96.46
Session                                 State Flaps   Uptime #IPv4/IPv6
records
202.125.96.46                            Up       75 09:21:18 40894/6747
```


RPKI Verification - JunOS

- Check the RPKI cache

```
>show validation database
RV database for instance master

Prefix               Origin-AS    Session               State      Mismatch
1.9.0.0/16-24             4788 202.125.96.46             valid
1.9.12.0/24-24           65037 202.125.96.46             valid
1.9.21.0/24-24           24514 202.125.96.46             valid
1.9.23.0/24-24           65120 202.125.96.46             valid

----------
2001:200::/32-32          2500 202.125.96.46             valid
2001:200:136::/48-48      9367 202.125.96.46             valid
2001:200:900::/40-40      7660 202.125.96.46             valid
2001:200:8000::/35-35     4690 202.125.96.46             valid
2001:200:c000::/35-35    23634 202.125.96.46             valid
2001:200:e000::/35-35     7660 202.125.96.46             valid
```

RPKI Verification - JunOS

- Can filter per origin ASN

```
>show validation database origin-autonomous-system 45192
RV database for instance master


Prefix               Origin-AS    Session                State     Mismatch
202.125.97.0/24-24       45192    202.125.96.46           valid
203.176.189.0/24-24      45192    202.125.96.46           valid
2001:df2:ee01::/48-48    45192    202.125.96.46           valid


 IPv4 records: 2
 IPv6 records: 1
```

- IOS should have something similar!

Check routes - JunOS

```
>show route protocol bgp 202.144.128.0

inet.0: 693024 destinations, 693024 routes (693022 active, 0 holddown, 2
hidden)
+ = Active Route, - = Last Active, * = Both

202.144.128.0/20 *[BGP/170] 1w4d 21:03:04, MED 0, localpref 110, from
202.125.96.254
                      AS path: 4826 17660 I, validation-state: valid
                    >to 202.125.96.225 via ge-1/1/0.0
```

```
>show route protocol bgp 2001:201::/32

inet6.0: 93909 destinations, 93910 routes (93909 active, 0 holddown, 0
hidden)
+ = Active Route, - = Last Active, * = Both

2001:201::/32     *[BGP/170] 21:18:14, MED 0, localpref 100, from
2001:df2:ee00::1
                      AS path: 65332 I, validation-state: unknown
                    >to fe80::dab1:90ff:fedc:fd07 via ge-1/1/0.0
```

Configuration - Reference Link

- Cisco
  - https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-3s/irg-xe-3s-book/irg-origin-as.pdf
- Juniper
  - https://www.juniper.net/documentation/en_US/junos/topics/topic-map/bgp-origin-as-validation.html
- RIPE:
  - https://www.ripe.net/manage-ips-and-asns/resource-management/certification/router-configuration

IPsec

Virtual Private Network

- Creates a secure tunnel over a public network
  - Client to firewall
  - Router to router
  - Firewall to firewall
- Uses the Internet as the public backbone to access a secure private network
  - Remote employees can access their office network
- Two types:
  - Remote access
  - Site-to-site VPN

VPN Implementation

- Hardware
  - Usually a VPN-type router
  - Pros: highest network throughput, plug and play, dual purpose
  - Cons: cost and lack of flexibility
- Software
  - Ideal for two end-points in different organisations
  - Pros: flexible, and low relative cost
  - Cons: lack of efficiency, more labor training required, lower productivity; higher labor costs
- Firewall
  - Pros: cost effective, tri-purpose, hardens the operating system
  - Cons: still relatively costly

VPN Protocols

- PPTP (Point-to-Point tunneling Protocol)
  - Developed by Microsoft to secure dial-up connections
  - Operates in the data-link layer
- L2F (Layer 2 Forwarding Protocol)
  - Developed by Cisco
  - Similar as PPTP
- L2TP (Layer 2 Tunneling Protocol)
  - IETF standard
  - Combines the functionality of PPTP and L2F
- IPsec (Internet Protocol Security)
  - Open standard for VPN implementation
  - Operates on the network layer

Other Modern VPNs

- MPLS VPN
  - Used for large and small enterprises
  - Pseudowire, VPLS, VPRN
- GRE Tunnel
  - Packet encapsulation protocol developed by Cisco
  - Not encrypted
  - Implemented with IPsec
- L2TP IPsec
  - Uses L2TP protocol
  - Usually implemented along with IPsec
  - IPsec provides the secure channel, while L2TP provides the tunnel

Advantages of VPN

- Cheaper connection
  - Use the Internet connection instead of a private lease line
- Scalability
  - Flexibility of growth
  - Efficiency with broadband technology
- Availability
  - Available everywhere there is an Internet connection

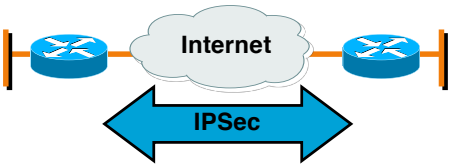
Disadvantages of VPN

- VPNs require an in-depth understanding of public network security issues and proper deployment precautions
- Availability and performance depends on factors largely outside of their control
- VPNs need to accommodate protocols other than IP and existing internal network technology

IPsec

- Provides Layer 3 security (RFC 2401)
  - Transparent to applications (no need for integrated IPsec support)
- A set of protocols and algorithms used to secure IP data at the network layer
- Combines different components:
  - Security associations (SA)
  - Authentication headers (AH)
  - Encapsulating security payload (ESP)
  - Internet Key Exchange (IKE)
- A security context for the VPN tunnel is established via the ISAKMP

What is IPSec?



- IETF standard that enables encrypted communication between peers:
  - Consists of open standards for securing private communications
  - Network layer encryption ensuring data confidentiality, integrity, and authentication
  - Scales from small to very large networks

IPsec Standards

- RFC 4301 “The IP Security Architecture”
  - Defines the original IPsec architecture and elements common to both AH and ESP
- RFC 4302
  - Defines authentication headers (AH)
- RFC 4303
  - Defines the Encapsulating Security Payload (ESP)
- RFC 2408
  - ISAKMP
- RFC 5996
  - IKE v2 (Sept 2010)
- RFC 4835
  - Cryptographic algorithm implementation for ESP and AH

Benefits of IPsec

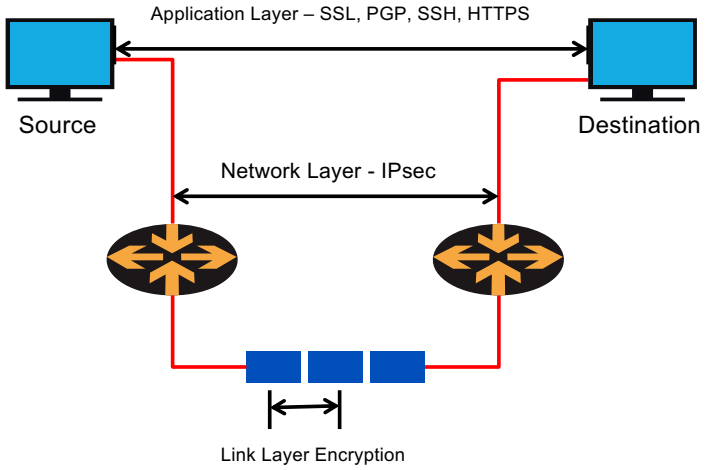
- Confidentiality
  - By encrypting data
- Integrity
  - Routers at each end of a tunnel calculates the checksum or hash value of the data
- Authentication
  - Signatures and certificates
  - All these while still maintaining the ability to route through existing IP networks

"IPsec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6" - (RFC 2401)

Benefits of IPsec

- Data integrity and source authentication
  - Data "signed" by sender and "signature" is verified by the recipient
  - Modification of data can be detected by signature "verification"
  - Because "signature" is based on a shared secret, it gives source authentication
- Anti-replay protection
  - Optional; the sender must provide it but the recipient may ignore
- Key management
  - IKE – session negotiation and establishment
  - Sessions are rekeyed or deleted automatically
  - Secret keys are securely established and authenticated
  - Remote peer is authenticated through varying options

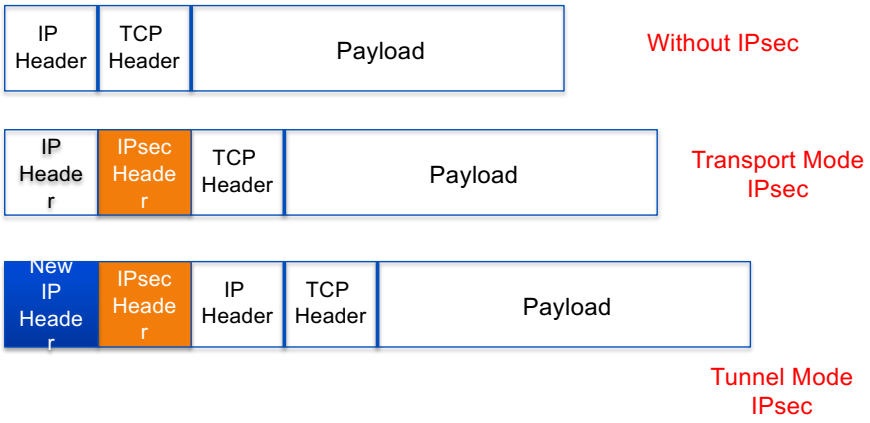
Different Layers of Encryption



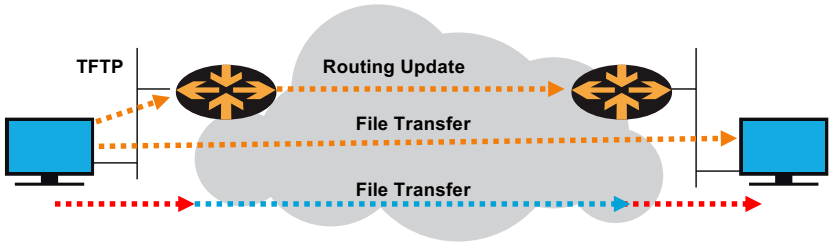
IPsec Modes

- Tunnel Mode
  - Entire IP packet is encrypted and becomes the data component of a new (and larger) IP packet.
  - Frequently used in an IPsec site-to-site VPN
- Transport Mode
  - IPsec header is inserted into the IP packet
  - No new packet is created
  - Works well in networks where increasing a packet's size could cause an issue
  - Frequently used for remote-access VPNs

Tunnel vs. Transport Mode IPsec



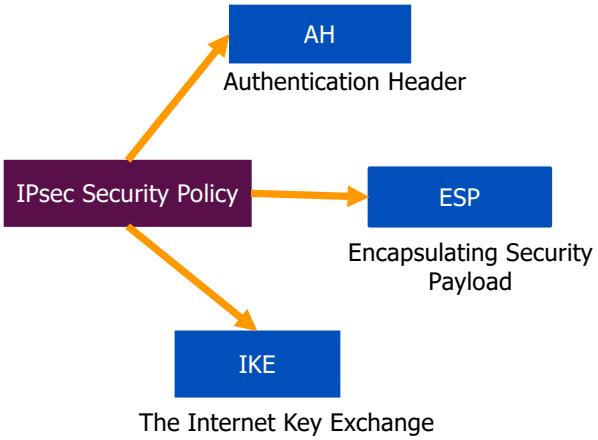
Transport vs Tunnel Mode



Transport Mode: End systems are the initiator and recipient of protected traffic

Tunnel Mode: Gateways act on behalf of hosts to protect traffic

IPsec Architecture



Security Associations (SA)

- A collection of parameters required to establish a secure session
- Uniquely identified by three parameters consisting of
  - Security Parameter Index (SPI)
  - IP destination address
  - Security protocol (AH or ESP) identifier
- An SA is either uni- or bidirectional
  - IKE SAs are bidirectional
  - IPsec SAs are unidirectional
    - Two SAs required for a bidirectional communication
- A single SA can be used for AH or ESP, but not both
  - must create two (or more) SAs for each direction if using both AH and ESP

Security Parameter Index (SPI)

- A unique 32-bit identification number that is part of the Security Association (SA)
- It enables the receiving system to select the SA under which a received packet will be processed.
- Has only local significance, defined by the creator of the SA.
- Carried in the ESP or AH header
- When an ESP/AH packet is received, the SPI is used to look up all of the crypto parameters

How to Set Up SA

- Manually
  - Sometimes referred to as “manual keying”
  - You configure on each node:
    - Participating nodes (I.e. traffic selectors)
    - AH and/or ESP [tunnel or transport]
    - Cryptographic algorithm and key
- Automatically
  - Using IKE (Internet Key Exchange)

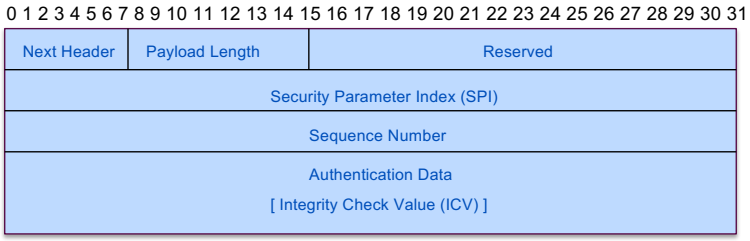
ISAKMP

- Internet Security Association and Key Management Protocol
- Used for establishing Security Associations (SA) and cryptographic keys
- Only provides the framework for authentication and key exchange, but key exchange is independent
- Key exchange protocols
  - Internet Key Exchange (IKE)
  - Kerberized Internet Negotiation of Keys (KINK)

Authentication Header (AH)

- Provides source authentication and data integrity
  - Protection against source spoofing and replay attacks
- Authentication is applied to the entire packet, with the mutable fields in the IP header zeroed out
- If both AH and ESP are applied to a packet, AH follows ESP
- Operates on top of IP using protocol 51
- In IPv4, AH protects the payload and all header fields except mutable fields and IP options (such as IPsec option)

AH Header Format

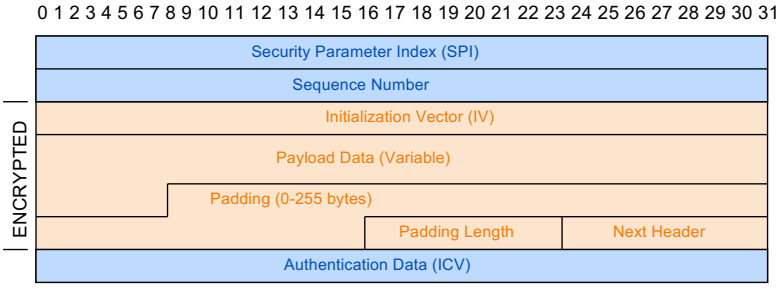


- Next Header (8 bits): indicates which upper layer protocol is protected (UDP, TCP, ESP)
- Payload Length (8 bits): size of AH in 32-bit longwords, minus 2
- Reserved (16 bits): for future use; must be set to all zeroes for now
- SPI (32 bits): arbitrary 32-bit number that specifies to the receiving device which security association is being used (security protocols, algorithms, keys, times, addresses, etc)
- Sequence Number (32 bits): start at 1 and must never repeat. It is always set but receiver may choose to ignore this field
- Authentication Data: ICV is a digital signature over the packet and it varies in length depending on the algorithm used (SHA-1, MD5)

Encapsulating Security Payload (ESP)

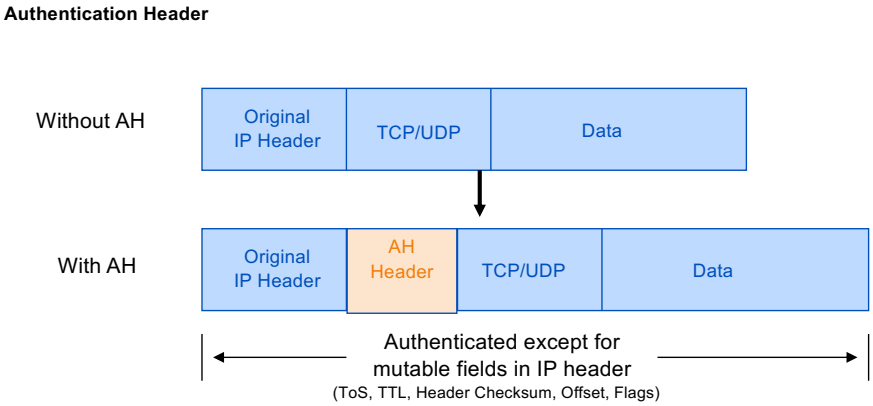
- Uses IP protocol 50
- Provides all that is offered by AH, plus data confidentiality
  - uses symmetric key encryption
- Must encrypt and/or authenticate in each packet
  - Encryption occurs before authentication
- Authentication is applied to data in the IPsec header as well as the data contained as payload

ESP Header Format

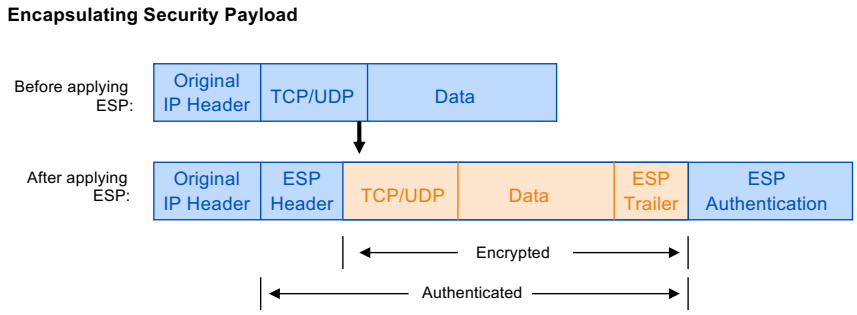


- SPI: arbitrary 32-bit number that specifies SA to the receiving device
- Seq #: start at 1 and must never repeat; receiver may choose to ignore
- IV: used to initialize CBC mode of an encryption algorithm
- Payload Data: encrypted IP header, TCP or UDP header and data
- Padding: used for encryption 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
- Authentication Header: ICV is a digital signature over the packet and it varies in length depending on the algorithm used (SHA-1, MD5)

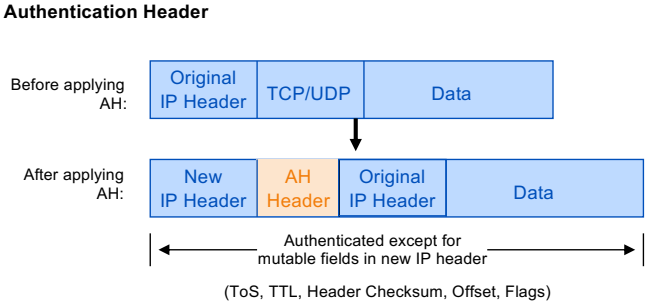
Packet Format Alteration for AH Transport Mode



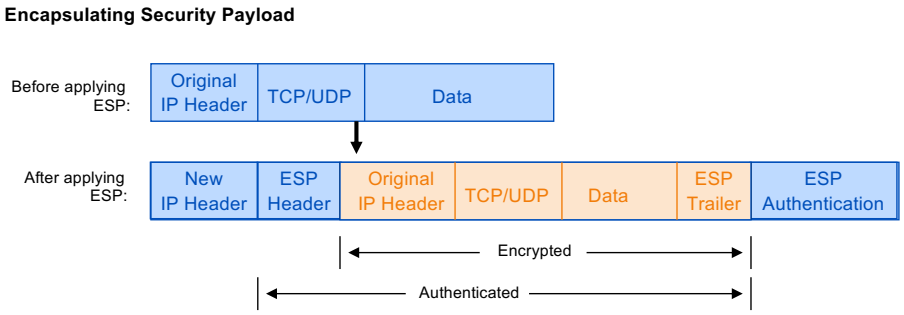
Packet Format Alteration for ESP Transport Mode



Packet Format Alteration for AH Tunnel Mode



Packet Format Alteration for ESP Tunnel Mode



Internet Key Exchange (IKE)

- "An IPsec component used for performing mutual authentication and establishing and maintaining Security Associations." (RFC 5996)
- Typically used for establishing IPsec sessions
- A key exchange mechanism
- Five variations of an IKE negotiation:
  - Two modes (aggressive and main modes)
  - Three authentication methods (pre-shared, public key encryption, and public key signature)
- Uses UDP port 500

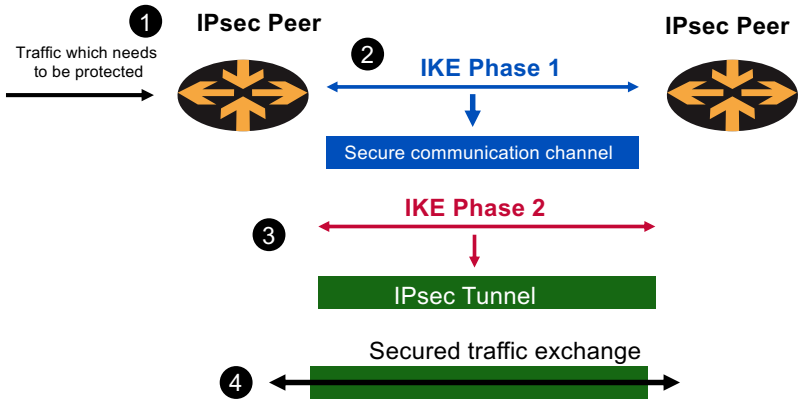
IKE Modes

Mode	Description
Main mode	Three exchanges of information between IPsec peers. Initiator sends one or more proposals to the other peer (responder) Responder selects a proposal
Aggressive Mode	Achieves same result as main mode using only 3 packets First packet sent by initiator containing all info to establish SA Second packet by responder with all security parameters selected Third packet finalizes authentication of the ISAKMP session
Quick Mode	Negotiates the parameters for the IPsec session. Entire negotiation occurs within the protection of ISAKMP session

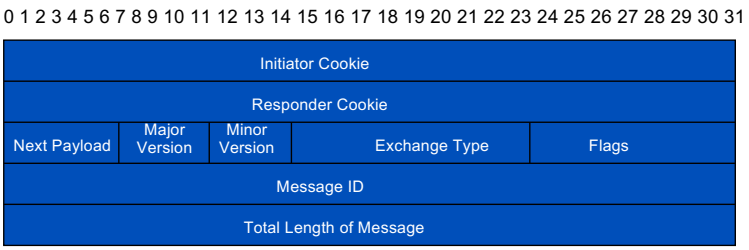
Internet Key Exchange (IKE)

- Phase I
  - Establish a secure channel (ISAKMP SA)
  - Using either main mode or aggressive mode
  - Authenticate computer identity using certificates or pre-shared secret
- Phase II
  - Establishes a secure channel between computers intended for the transmission of data (IPsec SA)
  - Using quick mode

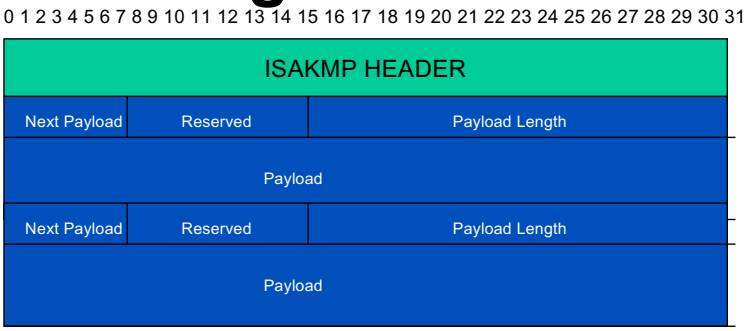
Overview of IKE



ISAKMP Header Format



ISAKMP Message Format



Next Payload: 1byte; identifier for next payload in message. If it is the last payload It will be set to 0

Reserved: 1byte; set to 0

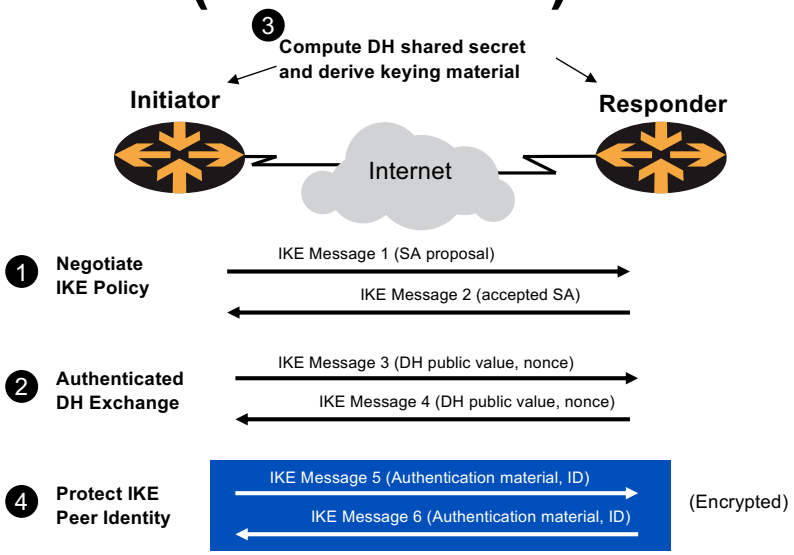
Payload Length: 2 bytes; length of payload (in bytes) including the header

Payload: The actual payload data

IKE Phase 1 (Main Mode)

- Main mode negotiates an ISAKMP SA which will be used to create IPsec SAs
- Three steps
  - SA negotiation (encryption algorithm, hash algorithm, authentication method, which DF group to use)
  - Do a Diffie-Hellman exchange
  - Provide authentication information
  - Authenticate the peer

IKE Phase 1 (Main Mode)



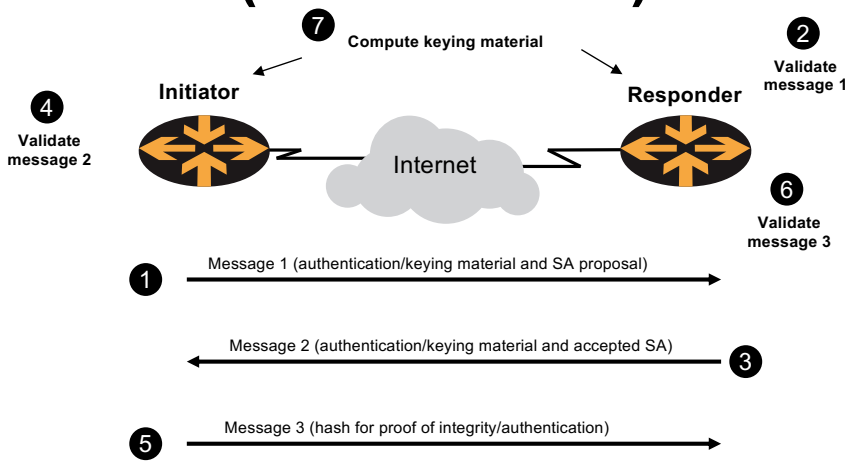
IKE Phase 1 (Aggressive Mode)

- Uses 3 (vs 6) messages to establish IKE SA
- No denial of service protection
- Does not have identity protection
- Optional exchange and not widely implemented

IKE Phase 2 (Quick Mode)

- All traffic is encrypted using the ISAKMP Security Association
- Each quick mode negotiation results in two IPsec Security Associations (one inbound, one outbound)
- Creates/refreshes keys

IKE Phase 2 (Quick Mode)



IKE v2: Replacement for Current IKE Specification

- Feature Preservation
  - Most features and characteristics of baseline IKE v1 protocol are being preserved in v2
- Compilation of Features and Extensions
  - Quite a few features that were added on top of the baseline IKE protocol functionality in v1 are being reconciled into the mainline v2 framework
- Some New Features

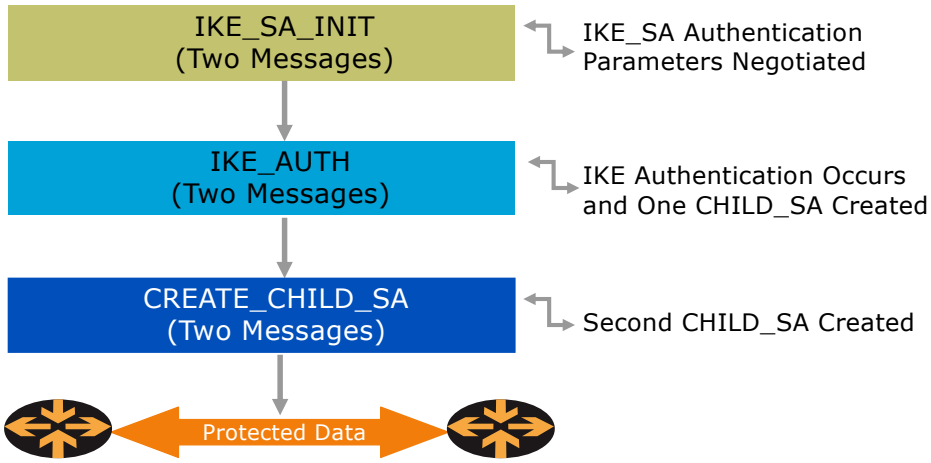
IKE v2: What Is Not Changing

- Features in v1 that have been debated but are ultimately being preserved in v2
  - Most payloads reused
  - Use of nonces to ensure uniqueness of keys
- v1 extensions and enhancements being merged into mainline v2 specification
  - Use of a 'configuration payload' similar to MODECFG for address assignment
  - 'X-auth' type functionality retained through EAP
  - Use of NAT Discovery and NAT Traversal techniques

IKE v2: What Is Changing

- Significant Changes Being to the Baseline Functionality of IKE
  - EAP adopted as the method to provide legacy authentication integration with IKE
  - Public signature keys and pre-shared keys, the only methods of IKE authentication
  - Use of 'stateless cookie' to avoid certain types of DOS attacks on IKE
  - Continuous phase of negotiation

How Does IKE v2 Work?



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

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

IPsec Concerns

- Are enough people aware that IKEv2 is not backwards compatible with IKEv1?
  - IKEv1 is used in most 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 and host requirements is changed from MUST to SHOULD implement
- 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

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
- ESP – how determine if ESP-Null vs Encrypted

IPsec Best Practices

- Use IPsec to provide integrity in addition to encryption
  - Use ESP option
- Use strong encryption algorithms
  - AES instead of DES
- Use a good hashing algorithm
  - SHA instead of MD5
- Reduce the lifetime of the Security Association (SA) by enabling Perfect Forward Secrecy (PFS)
  - Increases processor burden so do this only if data is highly sensitive

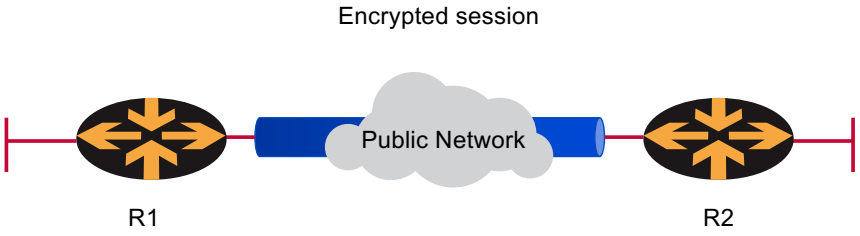
Configuring IPsec

- Step 1: Configure the IKE Phase 1 Policy (ISAKMP Policy)
  - crypto isakmp policy [priority]
- Step 2: Set the ISAKMP Identity
  - crypto isakmp identity {ipaddress|hostname}
- Step 3: Configure the IPsec transfer set
  - crypto ipsec transform-set transform-set-name <transform1> <transform2> mode [tunnel|transport]
  - crypto ipsec security-association lifetime seconds seconds

Configuring IPsec

- Step 5: Creating map with name
  - crypto map crypto-map-name seq-num ipsec-isakmp
  - match address access-list-id
  - set peer [ipaddress|hostname]
  - set transform-set transform-set-name
  - set security-association lifetime seconds seconds
  - set pfs [group1|group2]
- Step 6: Apply the IPsec Policy to an Interface
  - crypto map crypto-map-name local-address interface-id

IPsec Layout



Router Configuration

```
crypto isakmp policy 1
  authentication pre-share
  encryption aes
  hash sha
  group 5
crypto isakmp key Training123 address 172.16.11.66
!
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
!
crypto map LAB-VPN 10 ipsec-isakmp
  match address 101
  set transform-set ESP-AES-SHA
  set peer 172.16.11.66
```

Phase 1 SA

Encryption and authentication

Phase 2 SA

Router Configuration

```
int fa 0/1
crypto map LAB-VPN
Exit
!
access-list 101 permit ip 172.16.16.0
0.0.0.255 172.16.20.0 0.0.0.25
```

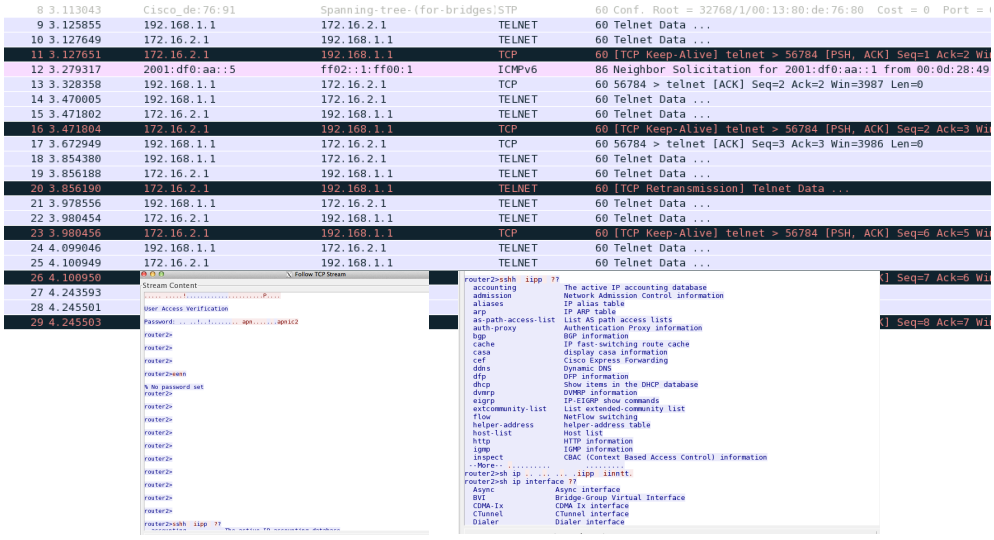
Apply to an outbound interface

Define interesting VPN traffic

IPsec Debug Commands

- sh crypto ipsec sa
- sh crypto isakmp peers
- sh crypto isakmp sa
- sh crypto map

Capture: Telnet



8	3.113043	Cisco_de:76:91	Spanning-tree-(for-bridges)	STP	60 Conf. Root = 32768/1/00:13:80:de:76:80 Cost = 0 Port =
9	3.125855	192.168.1.1	172.16.2.1	TELNET	60 Telnet Data ...
10	3.127649	172.16.2.1	192.168.1.1	TELNET	60 Telnet Data ...
11	3.127651	172.16.2.1	192.168.1.1	TCP	60 [TCP Keep-Alive] telnet > 56784 [PSH, ACK] Seq=1 Ack=2 Wi
12	3.279317	2001:df0:aa::5	ff02::1:ff00:1	ICMPv6	86 Neighbor Solicitation for 2001:df0:aa::1 from 00:0d:28:49
13	3.328358	192.168.1.1	172.16.2.1	TCP	60 56784 > telnet [ACK] Seq=2 Ack=2 Win=3987 Len=0
14	3.470005	192.168.1.1	172.16.2.1	TELNET	60 Telnet Data ...
15	3.471802	172.16.2.1	192.168.1.1	TELNET	60 Telnet Data ...
16	3.471804	172.16.2.1	192.168.1.1	TCP	60 [TCP Keep-Alive] telnet > 56784 [PSH, ACK] Seq=2 Ack=3 Wi
17	3.672949	192.168.1.1	172.16.2.1	TCP	60 56784 > telnet [ACK] Seq=3 Ack=3 Win=3986 Len=0
18	3.854380	192.168.1.1	172.16.2.1	TELNET	60 Telnet Data ...
19	3.856188	172.16.2.1	192.168.1.1	TELNET	60 Telnet Data ...
20	3.856190	172.16.2.1	192.168.1.1	TELNET	60 [TCP Retransmission] Telnet Data ...
21	3.978556	192.168.1.1	172.16.2.1	TELNET	60 Telnet Data ...
22	3.980454	172.16.2.1	192.168.1.1	TELNET	60 Telnet Data ...
23	3.980456	172.16.2.1	192.168.1.1	TCP	60 [TCP Keep-Alive] telnet > 56784 [PSH, ACK] Seq=6 Ack=5 Wi
24	4.099046	192.168.1.1	172.16.2.1	TELNET	60 Telnet Data ...
25	4.100949	172.16.2.1	192.168.1.1	TELNET	60 Telnet Data ...
26	4.100950				] Seq=7 Ack=6 Wi
27	4.243593				
28	4.245501				
29	4.245503				] Seq=8 Ack=7 Wi

Capture: Telnet + IPsec

179	67.594031	192.168.1.1	192.168.1.2	ESP	134 ESP (SPI=0x7ea7f8ed)
180	67.601908	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
181	67.601910	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
182	67.605809	192.168.1.1	192.168.1.2	ESP	118 ESP (SPI=0x7ea7f8ed)
183	67.626089	192.168.1.2	192.168.1.1	ESP	134 ESP (SPI=0x742f79b4)
184	67.626091	192.168.1.2	192.168.1.1	ESP	134 ESP (SPI=0x742f79b4)
185	67.627695	192.168.1.2	192.168.1.1	ESP	166 ESP (SPI=0x742f79b4)
186	67.627697	192.168.1.2	192.168.1.1	ESP	166 ESP (SPI=0x742f79b4)
187	67.631728	192.168.1.1	192.168.1.2	ESP	118 ESP (SPI=0x7ea7f8ed)
188	67.632884	192.168.1.1	192.168.1.2	ESP	118 ESP (SPI=0x7ea7f8ed)
189	67.751716	192.168.1.1	192.168.1.2	ESP	150 ESP (SPI=0x7ea7f8ed)
190	67.765217	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
191	67.765219	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
192	67.766634	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
193	67.766636	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
194	67.768056	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
195	67.768058	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
196	67.769385	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
197	67.769387	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
198	67.770803	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
199	67.770804	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)

Pretty Good IPsec Policy

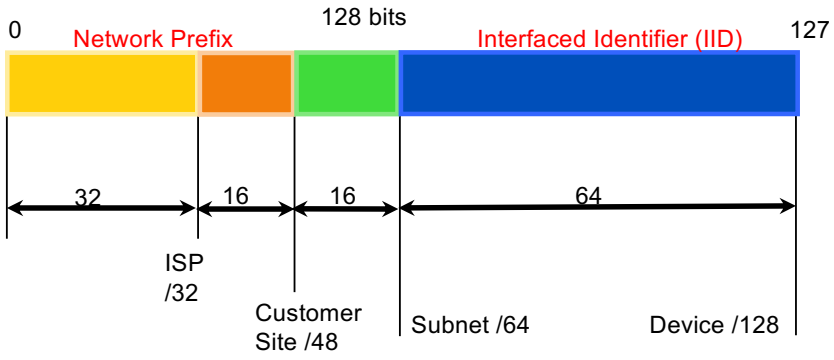
- IKE Phase 1 (aka ISAKMP SA or IKE SA or Main Mode)
  - 3DES (AES-192 if both ends support it)
  - Lifetime (8 hours = 480 min = 28800 sec)
  - SHA-2 (256 bit keys)
  - DH Group 14 (aka MODP# 14)
- IKE Phase 2 (aka IPsec SA or Quick Mode)
  - 3DES (AES-192 if both ends support it)
  - Lifetime (1 hour = 60 min = 3600 sec)
  - SHA-2 (256 bit keys)
  - PFS 2
  - DH Group 14 (aka MODP# 14)

IPv6 Security

IPv6 Operations

- ✓128-bit addresses
- ✓Uses Extension Headers
- ✓Has built-in security features
- ✓Uses ICMPv6 to discover other hosts and routers in the network

IPv6 Addressing Structure

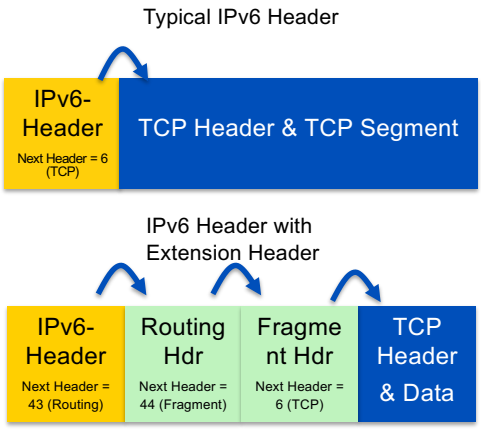


IPv6 Addressing Issues

- Privacy Issue
  - The Interface ID (IID) part is assigned using modified EUI-64. Part of the address is based on the machine's MAC address.
  - While it is unique worldwide, a host uses the same trackable IID even when network prefix changes
  - Solved by temporary addresses (RFC7217)
- Scanning the IPv6 network
  - IPv6 network is too big, it will take a long time to scan it entirely
  - It is possible to scan, based on a few factors

IPv6 Extension Header

- IPv6 extension headers extend the functionality of the protocol
- The number of extension headers are not fixed, so the total length of the extension header chain is variable.
- The order of extension header is a recommendation, not a requirement

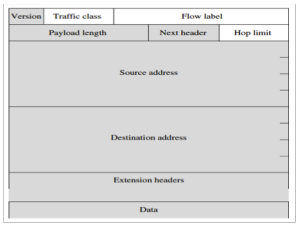


Extension Header Threats

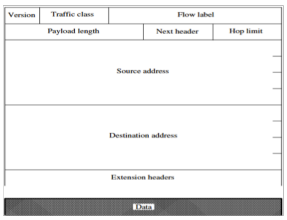
- An attacker could manipulate this feature as follows:
  - Create an IPv6 packet with long list of extension headers that cause a DoS to the routers along the path or to the destination host
  - Lengthy extension headers could consume system resource or could crash the the host protocol stack
  - Could be used as an attack vector to inject malicious code to the network by avoiding firewall and IDS (Numerous extension header in a single packet could spread the payload in to second fragment that could not be checked by the firewall)

IPv6 Security Features

- IPsec is mandatory in IPv6
- It is part of the IPv6 protocol, all nodes can secure their IP traffic if they have required keying infrastructure
- IPsec does not replace standard network security requirement but introduce added layer of security with existing IP network



Integrity of the IPv6 header & data



Confidentiality of the IPv6 data

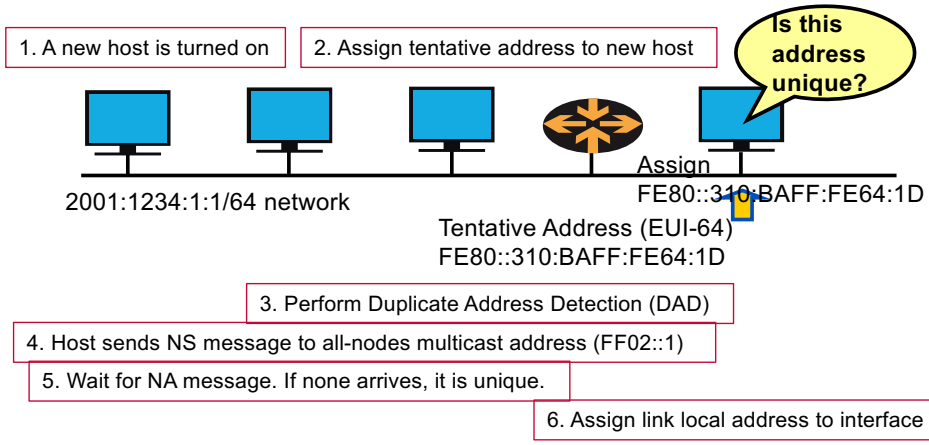
IPv6 Neighbor Discovery Protocol

- IPv6 uses multicast instead of broadcast to find out target host MAC address
- NDP uses ICMPv6 as transport
  - Compared to IPv4 ARP, there is no need to write different ARP for different L2 protocols
- Used for:
  - Stateless Address Autoconfiguration (SLAAC)
  - Neighbor discovery (NS/NA) and router discovery (RS/RA)
  - Duplicate Address Detection (DAD)

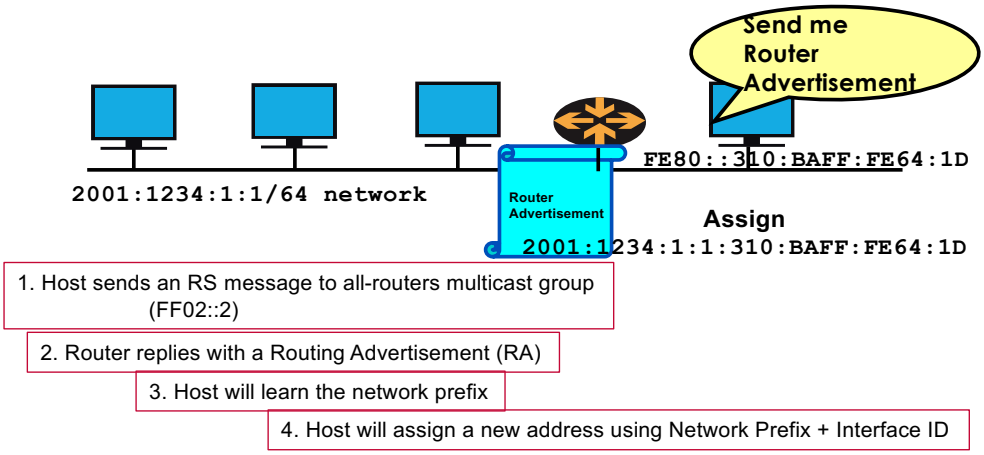
NDP Message Types

133 **Router Solicitation** Prompts a router to send a Router Advertisement.
134 **Router Advertisement** Sent by routers to tell hosts on the local network the router exists and describe its capabilities
135 **Neighbor Solicitation** Sent by a device to request the layer two address of another device while providing its own as well
136 **Neighbor Advertisement** Provides information about a host to other devices on the network
137 **Redirect** Router informs host of a better first hop to destination

IPv6 Autoconfiguration



IPv6 Autoconfiguration



NDP Attacks

- Attacks related to Neighbor Discovery (ND)
  - NDP Spoofing
  - DAD DoS attack
- Attacks related to Router Advertisement (RA)
  - RA Flooding
  - Rogue RA
- Note that anyone can send an advertisement (NA or RA)

IPv6 Attack Frameworks

- "The Hackers' Choice" THC-IPv6
  - https://www.thc.org/thc-ipv6/
- SI6 Networks IPv6 Toolkit
  - http://www.si6networks.com/tools/ipv6toolkit/
- Chiron
  - http://www.secfu.net/tools-scripts/

THC-IPv6 Tools

alive6	Checks for live interfaces with ipv6 address
parasite6	“ARP spoofer” for ipv6
redir6	Redirects all traffic into a target
implementation6	Test what the firewall supports
firewall6	Performs various ACL bypass attempts
thcping6	Test for anti-spoofing (RPF check) thcping6 <interface> <src-addr> <dest-addr>
fake_router26	Pretend to be a router (replaces fake_router6)
ndpexhaust26	Attack with ICMPv6 toobig and echorequest
thcsyn6	Flood the target with SYN packets

http://tools.kali.org/information-gathering/thc-ipv6

SI6 IPv6 Toolkit Commands

addr6	IPv6 address analysis and manipulation tool
Blackhole6	Troubleshooting tool which can find IPv6 where in the network topology packet with specific Extension header is being dropped
flow6	Tool to perform security assessment of the IPv6 Flow Label
frag6	Tool to perform IPv6 fragmentation-based attacks
icmp6	Attacks based on ICMPv6 error messages
na6	Tool to send arbitrary Neighbor Advertisement messages
ra6	Tool to send arbitrary Router Advertisement messages
scan6	IPv6 address scanning tool
tcp6	Send arbitrary TCP segments and perform a variety of TCP-based attacks

https://www.si6networks.com/tools/ipv6toolkit/index.html

Scanning an IPv6 Network

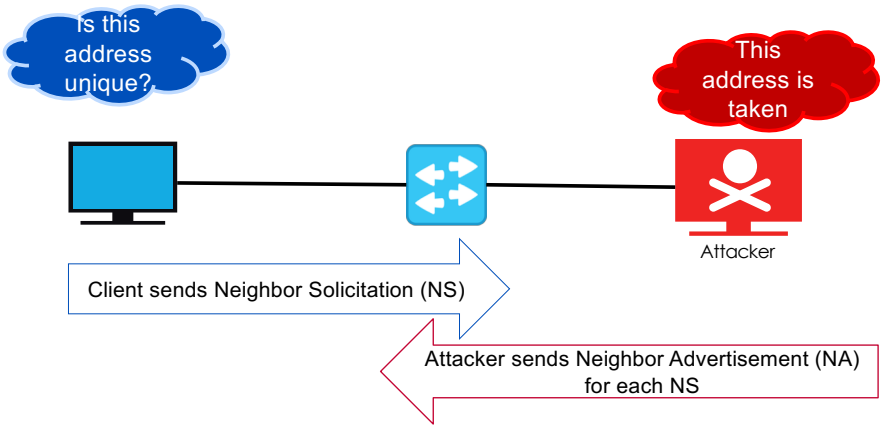
- IPv6 networks are too big to scan sequentially, but still possible
- Admins adopt easy-to-remember addresses
- Vanity names (::CAFÉ, ::BEEF, ::FADE, etc)
- Use IPv4 address in the last 32-bits of the IPv6 address
- Simple address for the infrastructure devices
- Loopback using 2001:DB8::1, 2001:DB8::2, etc..
- Read RFC 7707

Scanning – Attack Tool

- **Dnsdict -** to find all subdomains and enumerate IPv6 addresses
- **Alive26 -** shows alive addresses in the segment.

```
root@kali:~# atk6-dnsdict6 -d apnic.net
Starting DNS enumeration work on apnic.net. ...
Gathering NS and MX information...
NS of apnic.net. is sec1.apnic.net. => 2001:dc0:2001:a:4608::59
NS of apnic.net. is ns1.apnic.net. => 2001:dc0:2001:0:4608::25
NS of apnic.net. is sec3.apnic.net. => 2001:dc0:1:0:4777::140
NS of apnic.net. is ns3.apnic.net. => 2001:dc0:1:0:4777::131
NS of apnic.net. is sec4.apnic.net. => 2001:dc0:4001:1:0:1836:0:141
MX of apnic.net. is ao-mailgw.apnic.net. => 2001:dd8:8:701::25
MX of apnic.net. is ia-mailgw.apnic.net. => 2001:dd8:a:851::25
MX of apnic.net. is nx-mailgw.apnic.net. => 2001:dd8:9:801::25

Starting enumerating apnic.net. - creating 8 threads for 1419 words...
Estimated time to completion: 1 to 2 minutes
6to4.apnic.net. => 2001:dc0:2001:11::234
api.apnic.net. => 2001:dd8:9:2::101:29
as.apnic.net. => 2001:dd8:9:2::101:12
blog.apnic.net. => 2001:dd8:8:701::11
```

Duplicate Address Detection - DOS



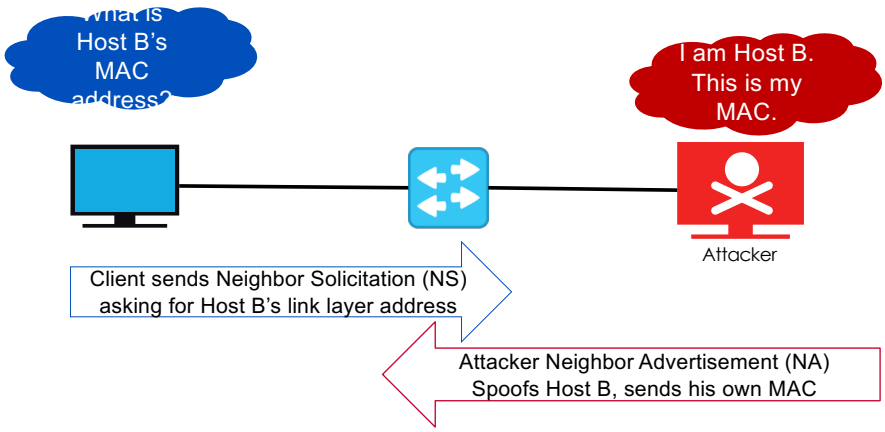
DAD – Attack Tool

dos-new-ip6

This tool prevents new ipv6 interfaces to come up by sending answers to duplicate ip6 checks. This results in a DOS for new IPv6 devices.

```
root@kali:~# atk6-dos-new-ip6 eth0

Started ICMP6 DAD Denial-of-Service (Press Control-C to end) ...

Spoofed packet for existing ip6 as 2400:6401::1

Spoofed packet for existing ip6 as fe80::5054:ff:fe42:e97a

poofed packet for existing ip6 as 2001:d35d:b33f:0:5054:ff:fe42:e97a

Spoofed packet for existing ip6 as 2001:d35d:b33f:0:5054:ff:fe42:e97a
```

Neighbor Discovery Spoofing



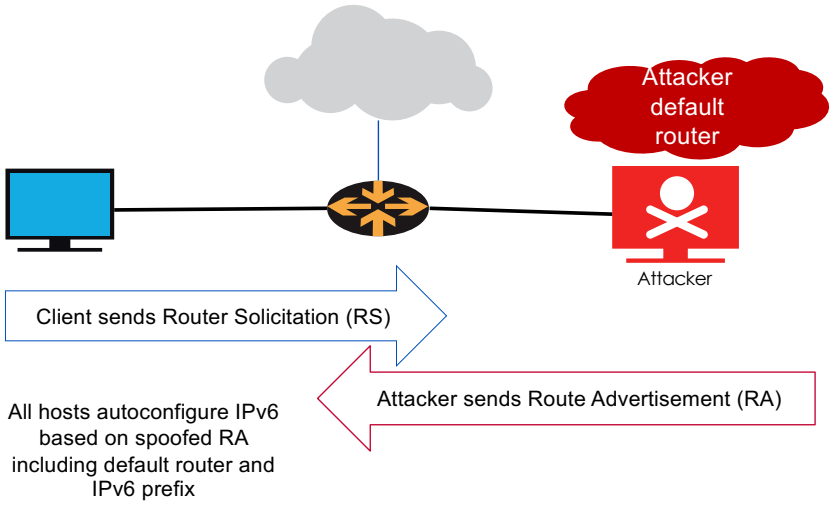
NDP Spoofing – Attack Tool

Parasite6

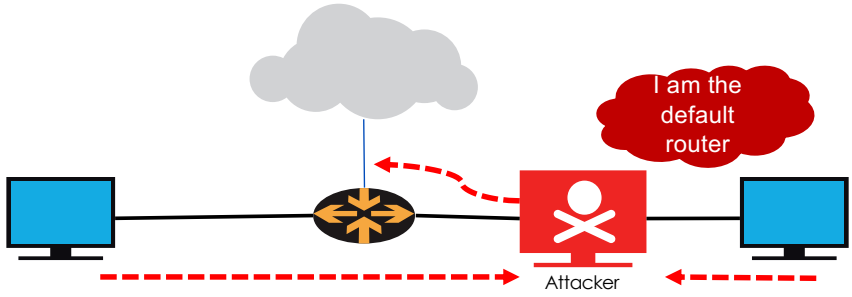
This is an "ARP spoofer" for IPv6, redirecting all local traffic to your own system (or nirvana if fake-mac does not exist) by answering falsely to Neighbor Solicitation requests, specifying FAKE-MAC results in a local DOS.

```
root@kali:~# atk6-parasite6 -l eth0 aa:bb:cc:11:22:33
Remember to enable routing (ip_forwarding), you will denial service otherwise!
 =>  echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
Started ICMP6 Neighbor Solitication Interceptor (Press Control-C to end) ...
Spoofed packet to fe80::3636:3bff:fed0:3030 as fe80::4af8:b3ff:fe9a:d29e
Spoofed packet to fe80::3636:3bff:fed0:3030 as fe80::4af8:b3ff:fe9a:d29e
```

Rogue RA



Rogue RA



Attacker can now intercept, listen and modify the packets coming from Host A and B

Rogue RA – Attack Tool

fake_router6 / fake_router26

Announce yourself as a router and try to become the default router.

```
root@kali:~# atk6-fake_router26 -A 2001:D35D:B33F::/64 eth0
Starting to advertise router (Press Control-C to end) ...
```

```
[nsadmin@server1 ~]$ ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:00:42:E9:7A
          inet addr:192.168.1.1  Bcast:192.168.255.255  Mask:255.255.0.0
          inet6 addr: 2001:d35d:b33f:0:5054:ff:fe42:e97a/64 Scope:Global
          inet6 addr: 2001:db8::5054:ff:fe42:e97a/64 Scope:Global
          inet6 addr: fe80::5054:ff:fe42:e97a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:299646 errors:0 dropped:0 overruns:0 frame:0
          TX packets:89280 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:220558509 (210.3 MiB)  TX bytes:6622864 (6.3 MiB)
```

Output after *fake_router26* is run

APNIC

RA Flooding – Tool

Attacker

```
root@kali:~# atk6-flood_router6 eth0
!
! Please note: flood_router6 is deprecated, please use flood_router26!
!
Starting to flood network with router advertisements on eth0 (Press Control-C to end, a dot is printed for every 1000 packets):
............................................
............................................
............................................
............................................
............................................
............................................
............................................
............................................
............................................
............................................
................
```

Victim

```
[nsadmin@server1 ~]$ ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:00:42:E9:7A
          inet addr:192.168.1.1  Bcast:192.168.255.255  Mask:255.255.0.0
          inet6 addr: 2a01:d07b:1aca:eccb:5054:ff:fe42:e97a/64 Scope:Global
          inet6 addr: 2a01:d86e:5318:d649:5054:ff:fe42:e97a/64 Scope:Global
          inet6 addr: 2a01:364a:768d:3b38:5054:ff:fe42:e97a/64 Scope:Global
          inet6 addr: 2a01:cea:f971:b02b:5054:ff:fe42:e97a/64 Scope:Global
          inet6 addr: 2a01:3a55:4067:f66a:5054:ff:fe42:e97a/64 Scope:Global
          inet6 addr: 2a01:206e:57f1:c2fa:5054:ff:fe42:e97a/64 Scope:Global
          inet6 addr: 2a01:3b81:65c6:317b:5054:ff:fe42:e97a/64 Scope:Global
          inet6 addr: 2a01:de28:2da1:2a1b:5054:ff:fe42:e97a/64 Scope:Global
          inet6 addr: 2a01:53aa:d153:a394:5054:ff:fe42:e97a/64 Scope:Global
          inet6 addr: 2a01:8c7f:8bb0:1611:5054:ff:fe42:e97a/64 Scope:Global
```

APNIC

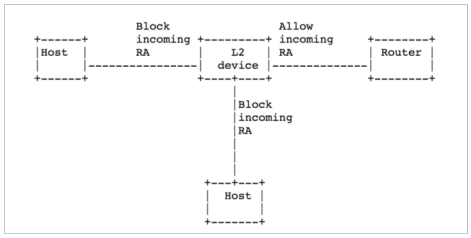
Detect Rogue RAs & ND Spoofing

- With a generic **Intrusion Detection System**
  - signatures needed
  - decentralized sensors in all network segments needed
- With **NDPmon**
  - can monitor RAs, NAs, DAD-DOS
  - generates syslog-events and/or sends e-mails
  - free available at ndpmon.sourceforge.net
- Using Deprecation Daemons:
  - ramond, rafixd

RA Guard

- Router Advertisement Guard (RFC 6105)
- All messages between IPv6 end-devices traverse the controlled L2 networking device.
- Filter RA messages based on a set of criteria
- Note that RA Guard can be circumvented (RFC7113)

RA-Guard can be circumvented

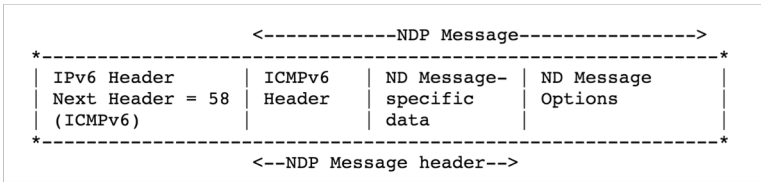


RA Guard – 3 Types

- Stateless RA-Guard
  - filter incoming RAs based on information found in the message (Link Layer address, IP source address, Prefix List, Router Priority) or in the L2-device configuration (Switch-Port).
- Stateful RA-Guard
  - Stateful RA-Guard learns dynamically about legitimate RA senders and stores this information for allowing subsequent RAs ("Learning-Mode").
- SEND-based RA-Guard
  - Filtering RAs based on SEND considerations

SEND

- Secure Neighbor Discovery (RFC 3971)
- A crypto solution for securing NDP messages
- A set of new ND options added
- Virtually no support for this protocol in IETF



IPv6 Filters

- Filter out some ICMPv6 messages
- Rate limit
- Block Routing Header 0
  - Use no ipv6 source-route at intermediate nodes
  - This is now the default from RFC 5095
- BGP route filters

ICMPv6 Messages

- List of all ICMPv6 type and code value
  - http://www.iana.org/assignments/icmpv6-parameters
- RFC 4890 – recommendations for filtering ICMPv6
- Some of the type values are defined so far
  - So undefined type should be blocked
    - Unallocated error messages: Type 5-99 and type 102-126
    - Unallocated informational message: Type 156-199 and type 202-254
    - Experimental message: Type 100, 101, 200, 201
    - Extension type message: Type 127, 255
- Following messages need to be blocked through the network perimeter if those functions are not used for specific purpose:
  - Type 138: Router Renumbering
  - Type 129: Echo Reply
  - Type 139 & 140: Node Information Query Messages

ICMPv6 Messages

- ICMPv6 is used for many legitimate purpose so following messages must be permitted through the network perimeter
  - Type 1: Destination Unreachable
  - Type 2: Packet Too Big [PMTUD]
  - Type 3: Time Exceeded
  - Type 4: Parameter Problem
- Following messages can be permitted as an option through the network perimeter (If Source & Destination of the packet can be controlled)
  - Type 128: Echo Request
  - Type 129: Echo Reply

ICMPv6 Messages

- Rate limiting ICMPv6 traffic from overwhelming the router

```
!
ipv6 access-list ICMPv6
 permit icmp any any
!
class-map match-all ICMPv6
 match protocol ipv6
 match access-group name ICMPv6
!
!
policy-map ICMPv6_RATE_LIMIT
 class ICMPv6
    police 100000 200000 conform-action transmit  exceed-action drop
!
Interface fa0/0
 service-policy input ICMPv6_RATE_LIMIT
```

Full bogons (IPv4 Transport)

```
address-family ipv6
  ! Session 1
  neighbor A.B.C.D activate
  neighbor A.B.C.D soft-reconfiguration inbound
  neighbor A.B.C.D prefix-list cymru-out-v6 out
  neighbor A.B.C.D route-map CYMRUBOGONS-V6 in
  ! Session 2
  neighbor E.F.G.H activate
  neighbor E.F.G.H soft-reconfiguration inbound
  neighbor E.F.G.H prefix-list cymru-out-v6 out
  neighbor E.F.G.H route-map CYMRUBOGONS-V6 in
!
```

```
ipv6 route 2001:DB8:0:DEAD:BEEF::1/128 Null0
!
ipv6 prefix-list cymru-out-v6 seq 5 deny ::/0 le
128
!
route-map CYMRUBOGONS-V6 permit 10
description IPv6 Filter bogons learned from
cymru.com bogon route-servers
match community 100
set ipv6 next-hop 2001:DB8:0:DEAD:BEEF::1
!
```

http://www.team-cymru.org/bgp-examples.html#cisco-full-v4trans

Route Filter Recommendation

```
3-1-2. Route Filters

  3-1-2-1. Ingress Prefix Filters

    [1] Reject following special-use prefix.

       - Default Route             :  ::/0 exact
       - IETF reserved Address(formerly IPv4-compatible IPv6
         Address                   :  ::/96 or longer
       - Unspecified Address       :  ::/128 exact
       - Loop back Address         :  ::1/128 exact
       - IPv4-mapped IPv6 Address  :  ::ffff:0:0/96 or longer
       - Discard-Only Address      :  100::/64 or longer
       - TEREDO Address            :  2001::/32 or longer
       - Benchmarking Address      :  2001:2::/48 or longer
       - ORCHID Address            :  2001:10::/28 or longer
       - Documentation Address     :  2001:db8::/32 or longer
       - Unique-local Address      :  fc00::/7 or longer
       - Link-local Address        :  fe80::/10 or longer
       - IETF reserved Address(formerly Site-local Address)
                                   :  fec0::/10 or longer
       - Multicast Address         :  ff00::/8 or longer

    [2] Reject your own prefix.

       (Example)
         You have 2001:db8::/32 for your xSP network, you should
         reject 2001:db8::/32 or longer prefix.
```

http://www.team-cymru.org/Reading-Room/Templates/IPv6Routers/xsp-recommendations.txt

IPv6 Security Practices

- Check if you're running IPv6
  - It's possible that you are
- Learn IPv6
- Adapt similar practices as in IPv4
  - Implement BCP38, uRPF
  - Replicate IPv4 policies
- Check if your security equipment supports IPv6
- Always include security in the overall IPv6 deployment plan

Network Security Monitoring and Incident Handling

What is a SOC?

- Security Operations Centre
- Centralized command center for network security event monitoring and incident response.
- responsible for detecting, analyzing, and reporting unauthorized or malicious network activity

SOC vs NOC

Security Operations Centre

- Focus on incidents and alerts that affect the security of information assets
- SOC analyst require security and reverse engineering skills

Network Operations Centre

- Monitor and maintain the network infrastructure
- Meet SLAs and manage incidents to reduce downtime
- Focus on availability and performance

SOC and NOC should complement each other

Types of SOC

Threat-centric SOCs

proactively hunts for malicious threats on network; a simpler, scalable, threat-centric approach that addresses security across the entire attack continuum: before, during, and after an attack.

Compliance-based SOCs

focused on comparing the compliance posture of network systems to reference configuration templates and standard system builds

Operational-based SOCs

internally focused organization that is tasked with monitoring the security posture of an organization's internal network

Security Analysts

Tier 1	Tier 2	Tier 2
•Continuously monitors the alert queue. •Triages security alerts. •Monitors the health of the security sensors and endpoints.	•Performs deep-dive incident analysis by correlating data from various sources. •Determines if a critical system or data set has been impacted.	•Possesses in-depth technical knowledge on the network, endpoint, threat intelligence, forensics, malware reverse engineering, and the functioning of specific applications or underlying IT infrastructure •Acts as an incident hunter, not waiting for escalated incidents.

231

SOC Playbook

- Collection of plays, which are effectively custom reports that are generated from a set of data sources
- Complexity is the enemy of reliability and maintainability. The playbook is an answer to this complexity.
- Plays are self-contained, fully documented, prescriptive procedures for finding and responding to undesired activity

Hacking Industry

- Hacking is a lucrative industry
- It creates faster, more effective and more efficient criminal economy profiting from attacks to our IT infrastructure
- Cybercrime costs the global economy **$450 billion** in 2016*

*Source: Hiscox Cyber Readiness Report 2017

Incident Analysis

Kill Chain Model

process by which a threat actor would build a plan or strategy to affect a specific goal or end-state against a target

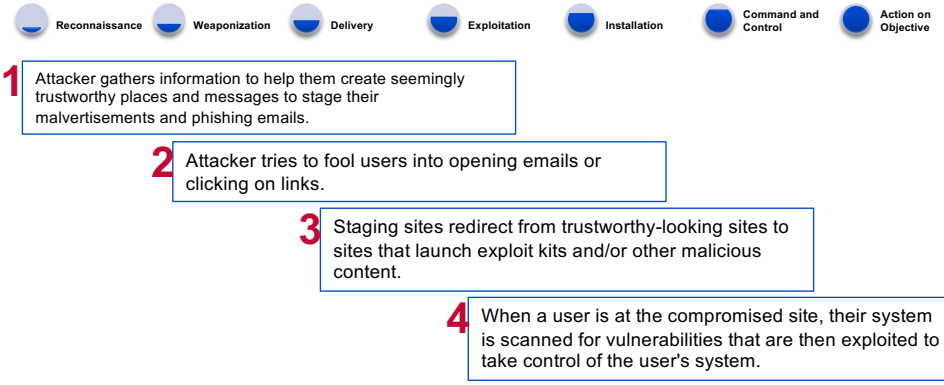
part of an intelligence-driven defense model that is used to identify, detect, and prevent intrusions by threat actors

Diamond Model

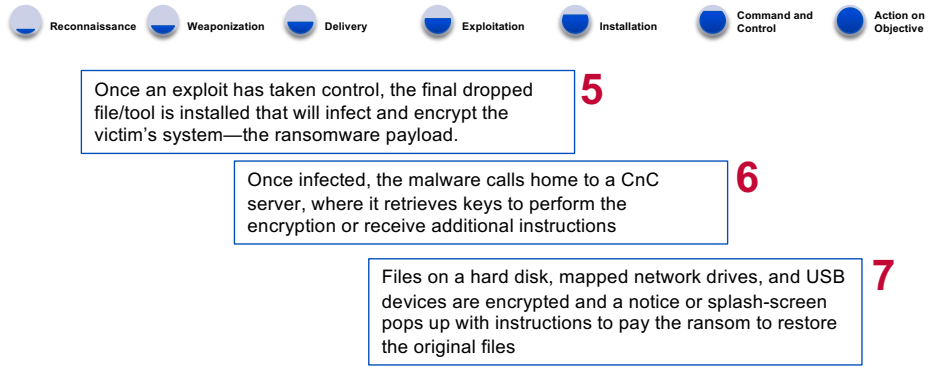
systematic method to analyze events in a repeatable way so that the threats can be organized, tracked, sorted, and countered

framework by which an SOC team can organize and verify APTs and then use that knowledge to thwart malicious adversaries

Kill Chain Model - Example



Kill Chain Model - Example



Diamond Model

Adversary

An adversary is the entity responsible for conducting an intrusion. An intrusion is considered any malicious activity.

Capability

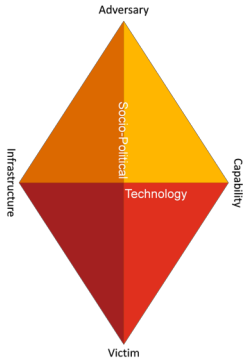
A capability is a tool or technique that the adversary may use in an event

Victim

The victim is the target of the adversary. As a SOC analyst, the victim is the customer.

Infrastructure

Infrastructure is the physical or logical communications nodes that the adversary uses to establish and maintain command and control over their capabilities



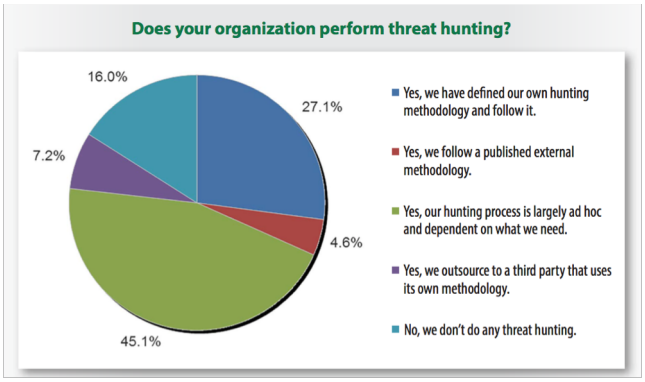
Source: PwC

Hunting Cyber Threats

a proactive approach to detect malicious activity that is not identified by traditional alerting mechanisms

threathunting.net

Hunting Cyber Threats



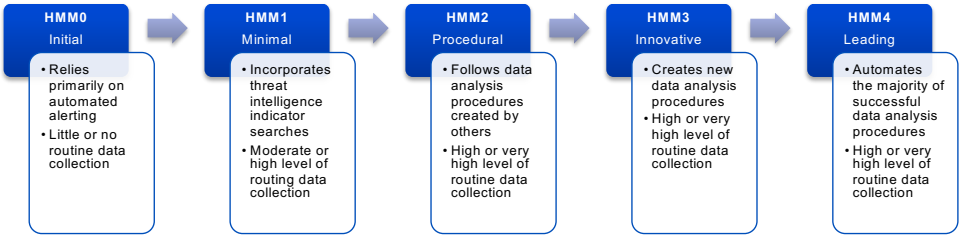
Survey Results:

- Most hunting organizations are reactive
- Continuous hunting is not there yet

Source: The Who, What, Where, When, Why and How of Effective Threat Hunting

APNIC

Hunting Maturity Model



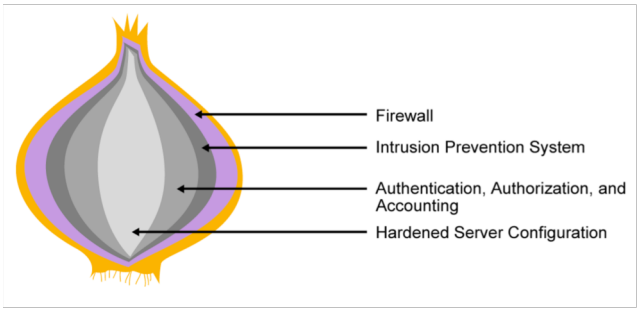
Source: A Simple Hunting Maturity Model

APNIC

Network Security Technologies

Defense-in-Depth Strategy

A building block of other security design principles that applies a layers approach to security. It is aimed at providing redundancy controls at multiple levels to mitigate risk.

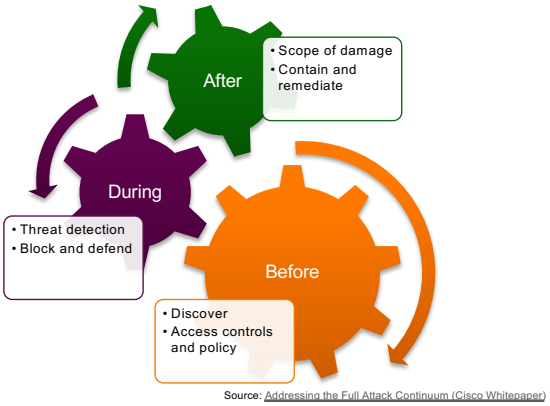


Network Security Technologies

Defend across the attack continuum

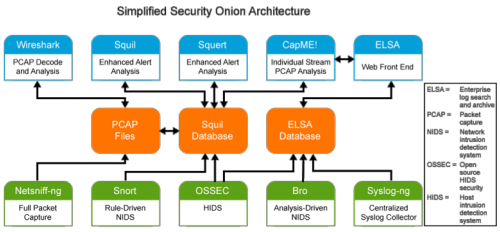
A continuous model that is consistent with how companies secure, defend and audit their networks.

It is divided into 3 phases: before, during and after an attack.



Source: Addressing the Full Attack Continuum (Cisco Whitepaper)

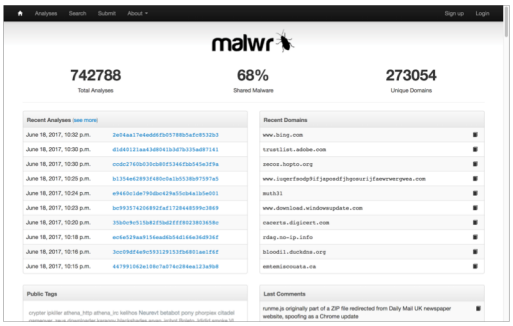
Security Tools



Network Security Monitoring (NSM)

Source: Security Onion

Security Tools

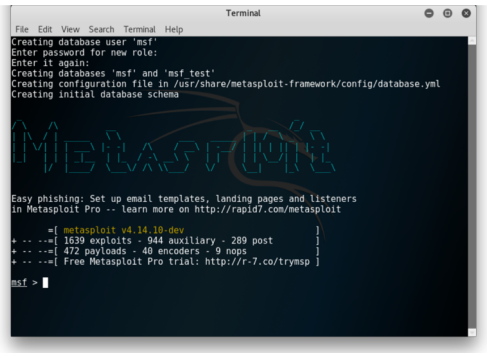


Malware analysis

Source: Cuckoo Sandbox

Security Tools

- **Metasploit**



Penetration Testing Tools

Honeypots and Honeynets

How do you know if there's something malicious in your network?
Are people interested to attack me?
Are my security controls working?

A **honeypot** is an information system resource whose value lives in the unauthorised or illicit use of that resource

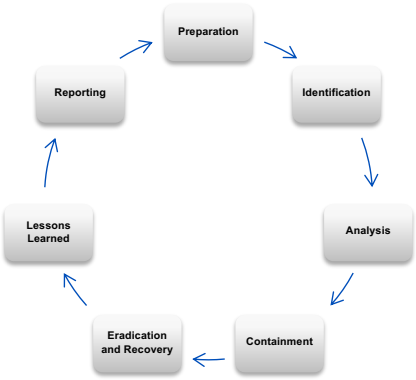
Honeypot systems have no production value, so any activity going to or from a honeypot is likely a probe, attack or compromise

For a list of honeypots, see https://github.com/paralax/awesome-honeypots

A **honeynet** is simply a network of honeypots. Information gathering and early warning are the primary benefits to most organizations

HN/P
http://honeynet.org/

Incident Response



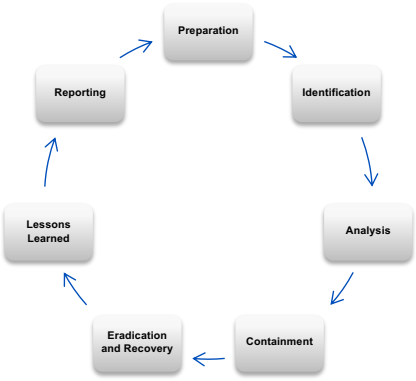
Preparation
Get the company and resources ready to handle security incident

Identification
When a true positive incident has been detected, the IR team is activated.

Analysis
The IR Team should work quickly to analyze and validate each incident, following a pre-defined process

Containment
Find scope of incident, network reachability, and how quickly containment is needed

Incident Response



Eradication and Recovery
Investigate to find origin of the incident and all traces of malicious code removed.

Lessons Learned
Analysis of how the incident happened and performs a Failure Mode and Effects Analysis (FMEA)

Reporting
Notify parties (internal and external) which occur at pre-defined intervals based on incident severity

CVSS 3.0

CVSS is a vendor agnostic, industry open standard that is designed to convey vulnerability severity and to help determine urgency and priority of response; does not calculate the chances of being attacked, but the chances of being compromised in the event of an attack and potential severity of damage.

https://www.first.org/cvss/calculator/3.0

249

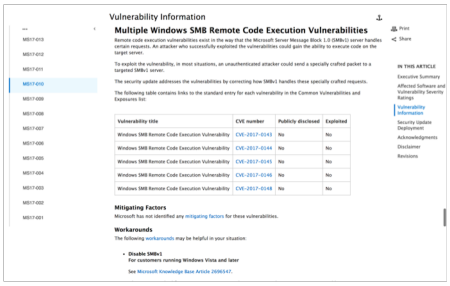
GNU Bourne-Again Shell (Bash) 'Shellshock' Vulnerability (CVE-2014-6271)

GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "Shellshock."

Metric	Value	Comments
Attack Vector	Network	Considering the worst case scenario: (web server attack vector).
Attack Complexity	Low	An attacker needs to only gain access to a listening service that uses the GNU Bash shell as an interpreter or interact with a GNU Bash shell directly.
Privileges Required	None	Some attack vectors do not require any privileges (e.g. CGI in web server).
Scope	Unchanged	No user interaction is required for an attacker to launch a successful attack.
Confidentiality Impact	High	The **vulnerable component** is the GNU Bash shell which is used as an interpreter for various services or can be accessed directly, therefore no change in scope occurs during the attack.
Integrity Impact	High	Allows an attacker to take complete control of the affected system.
Availability Impact	High	Allows an attacker to take complete control of the affected system.

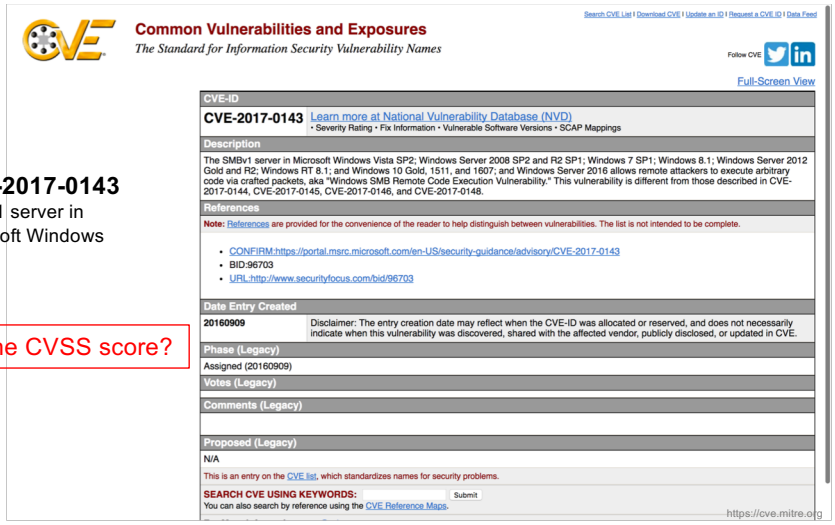
https://www.first.org/cvss/examples

Case: WannaCry Ransomware

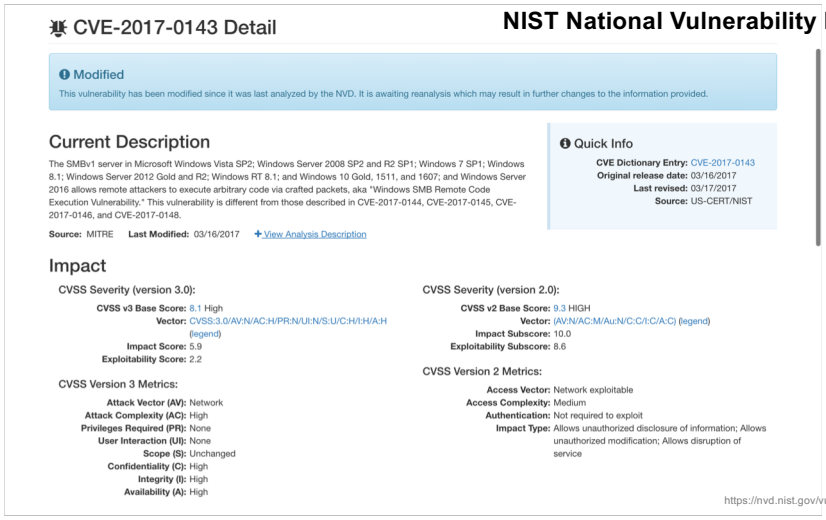


CVE-2017-0143
SMBv1 server in Microsoft Windows

What is the CVSS score?



NIST National Vulnerability Database



CVE-2017-0143 Detail

Modified

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

Source: MITRE **Last Modified:** 03/16/2017 + View Analysis Description

Quick Info

CVE Dictionary Entry: CVE-2017-0143
Original release date: 03/16/2017
Last revised: 03/17/2017
Source: US-CERT/NIST

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 8.1 High
Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H (legend)
Impact Score: 5.9
Exploitability Score: 2.2

CVSS Version 3 Metrics:

Attack Vector (AV): Network
Attack Complexity (AC): High
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

CVSS Severity (version 2.0):

CVSS v2 Base Score: 9.3 HIGH
Vector: (AV:N/AC:M/Au:N/C:C/I:C/A:C) (legend)
Impact Subscore: 10.0
Exploitability Subscore: 8.6

CVSS Version 2 Metrics:

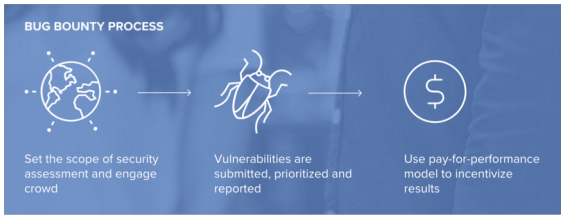
Access Vector: Network exploitable
Access Complexity: Medium
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

https://nvd.nist.gov/vuln/detail/CVE-2017-0143

Bug Bounty

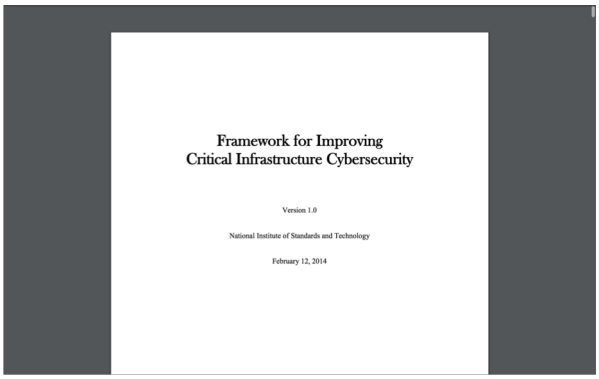
"**Crowdsourced security**"

Develops can receive recognition and compensation for reporting bugs, exploits and vulnerabilities



Source: Bugcrowd

Cybersecurity Framework



https://www.nist.gov/cyberframework

Thank You!

END OF SESSION