IPV6 SECURITY

ITU IPv6 and IoT Workshop

GENERAL SECURITY CONCEPTS

"I've installed a comprehensive program that will protect our computer against viruses, trojan horses, worms, cooties, hissy fits, conniptions, and the heebie-jeebies."

WEAKNESS OF GENERAL SECURITY

The following is a list of some possible points of weakness general security:

- Insufficient or nonexistent IT security concepts and corresponding provisions
- Nonobservance or insufficient control of IT security provisions
- Usurping of rights (password theft, privilege escalation)
- Incorrect use or faulty administration of IT systems

GENERAL SECURITY CONCEPTS….

- Abuse of rights
- Weaknesses in software (e.g., buffer/heap overflows in conjunction with applications running with superuser rights, cross-site scripting)
- Manipulation, theft, or destruction of IT devices, software, or data (physical security)

GENERAL SECURITY CONCEPTS....

- Trojan horses, viruses, and worms
- Security attacks such as masquerading, IP spoofing, Denial of Service (DoS) attacks, man-in-the-middle attacks, or DNS poisoning
- Routing misuse

CIA

Standard security practices involve two “triads” of thought, CIA and AAA. The CIA triad includes:

- **Confidentiality**: Stored or transmitted information cannot be read or altered by an unauthorized party.
- **Integrity**: Any alteration of transmitted or stored information can be detected.
- **Availability**: The information in question is readily accessible to authorized users at all times.

AAA

The AAA triad includes:

- **Authentication**: Ensuring an individual or group is who they say they are. The act of clarifying a claimed identity. Common forms of authentication include usernames and passwords or ATM card/PIN combinations.

- **Authorization**: Ensuring that the authenticated user or group has the proper rights to access the information they are attempting to access. Common implementations include Access Control Lists (ACLs).

- **Accounting**: The act of collecting information on resource usage. The log of an HTTP server would be a common form of accounting.

NONREPUDIATION

Nonrepudiation is not included in the CIA/AAA triads.

Nonrepudiation means a specified action, such as sending, receiving, or deleting of information, cannot be denied by any of the parties involved.

BASIC SECURITY ELEMENTS

These security requirements need to be provided by two basic security elements:

- encryption (to provide confidentiality)
- Secure checksums or hash (to provide integrity).

Suitable combinations of these two elements may then be used to provide more complex services, such as authenticity and nonrepudiation.

ENCRYPTION - SECRET KEY *CRYPTOGRAPHY*

There are two forms of encryption that are commonly used.

Secret Key Cryptography

- also termed *symmetric key encryption*, which requires the sender and recipient to agree on a shared secret (i.e., a key or password) that is then used to encrypt and decrypt the information exchanged.
- Common symmetric key algorithms are AES, DES, 3DES, IDEA, and RC-4.

ENCRYPTION – PUBLIC KEY CRYPTOGRAPHY

Public Key Cryptography

- also termed *asymmetric encryption.*
- An asymmetric encryption algorithm uses a key pair consisting of a known and distributed public key and an individual private key.

ENCRYPTION – PUBLIC KEY CRYPTOGRAPHY

- When a message is encrypted using the public key and decrypted by the receiver with the corresponding private key, only the intended recipient is capable of seeing the encrypted message.

- This form of encryption can be used to establish a confidential data exchange. If in addition, the message was also encrypted with the sender's private key and then decrypted by the recipient with a corresponding public key, the security services of data origin authentication and nonrepudiation are added.

- Common asymmetric key algorithms are RSA, ElGamal, and elliptic curves cryptography (ECC).

SECURE CHECKSUMS OR HASH FUNCTIONS

Secure checksums or hash functions often provide data integrity.

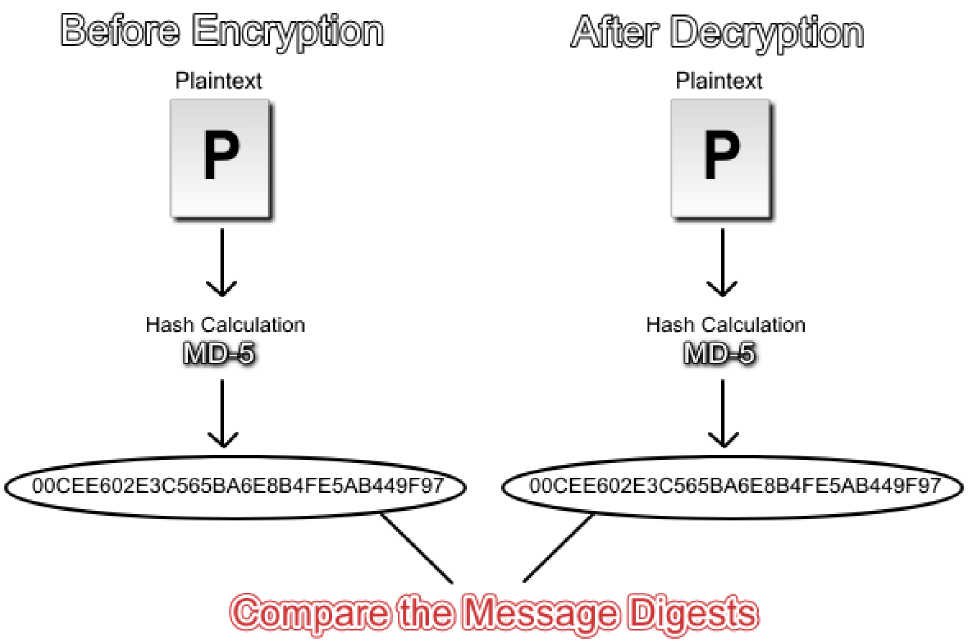
A hash function takes input of an arbitrary length and outputs fixed-length code.

The fixed-length output is called the *message digest*, or the *hash*, of the original input message. These hashes are unique and thereby provide the integrity of the message.

Common one-way hash functions are SHA-1 and MD-5.

HASHING FOR DATA INTEGRITY

Verification that the data has not been modified



Checksum, Seal or Message Digest

- **Is created by processing cleartext using a Hashing algorithm**
- **If data has changed, the checksum will be different.**

Demo: http://www.fileformat.info/tool/hash.htm

DIGITAL SIGNATURES FOR VERIFICATION

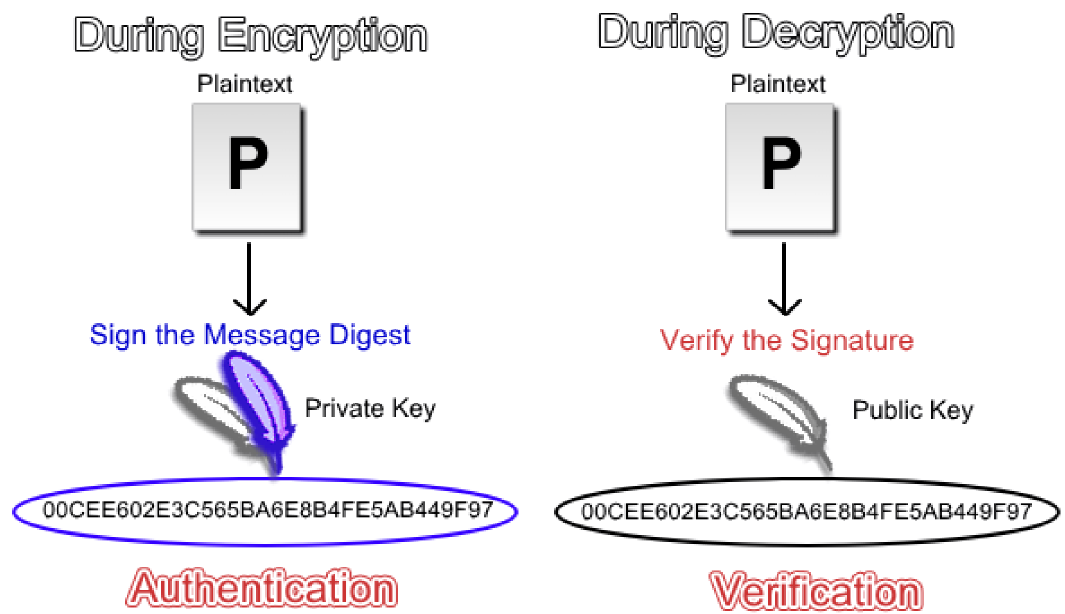
Verify the sender of the data that you decrypt

Sign with Private Key

- Authentication when signing

Verify with Public Key

- Sender is confirmed



SECURITY CONCERNS

- How will IPv6 affect the organization's network?
- How secure is IPv6 compared to IPv4?
- How to implement security practices similar to IPv4?
- Are the current devices capable of blocking and filtering IPv6 traffic?

IPV6 SECURITY ISSUES

RFC 4942, published in 2007, contains a wealth of information and is a good starting point. It groups the security area into three groups:

- Issued caused by the IPv6 protocol
- Issued caused by IPv6 transition solutions
- Issued caused by IPv6 deployment

SECURITY ATTACK VECTORS

- Misuse of protocol
- Implementation at OS level
- Implementation at application layer
  - Co-existance mechanisms i.e. tunnels and translators.
- Key services vital for IPv6 sustainability.

SECURITY ADVANTAGES OF IPV6 OVER IPV4

IPv4 - NAT breaks end-to-end network security

IPv6 - Huge address range – No need of NAT

IPv4 – IPSec is Optional

IPv6 - Mandatory in v6

IPv4 - Security extension headers(AH,ESP) – Back ported

IPv6 - Built-in Security extension headers

IPv4 - External Firewalls introduce performance bottlenecks

IPv6 - Confidentiality and data integrity without need for additional firewalls

SECURITY ADVANTAGES OF IPV6 OVER IPV4....

IPv4 - Security issues related to ICMPv4.

IPv6 - ICMPv6 uses IPSEC authentication and encryption.

IPV4 - Doesn’t support Auto configuration

IPv6 - Built in Auto configuration support

Ignorance of network administrator to IPV6
But, Thanks to the transitional efforts of IETF

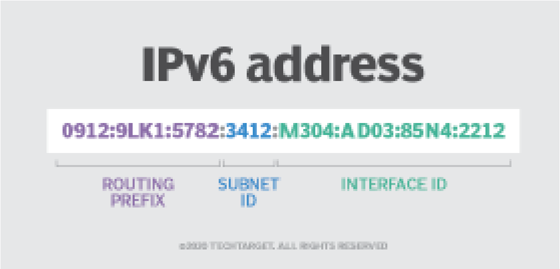
THE BIG IPV6 SECURITY QUESTION

Does IPv6 help or hinder network security?

The answer is not that simple!

MYTH 1

IPv6 - Huge address range – No need of NAT



Reality

- The RFC6296 has provision for NATv6.
- NPTv6 provides a simple and compelling solution to meet the address- independence requirement in IPv6.

MYTH 2

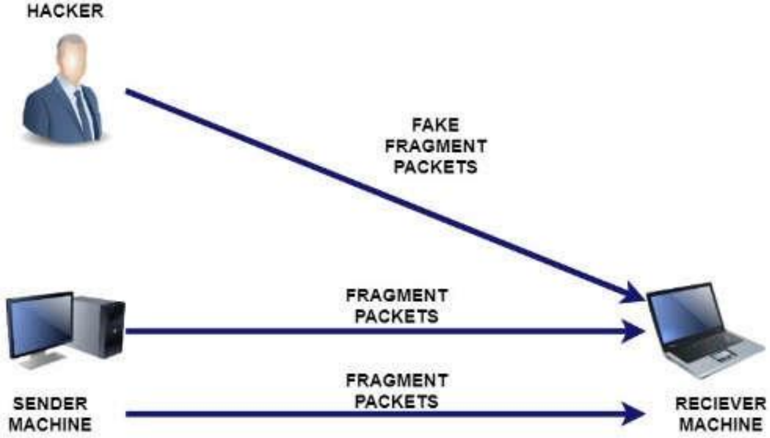
IPSec Mandatory in IPv6

Reality

- It was not implemented because of Bootstrapping problem.
- IPSec required functional IP address to built the tunnel but when a new host joints any network there would not be any functional IPv6 address available.
- Most of the organisation whom deployed IPv6 has not implemented this feature.

MYTH 3

IPv6 - Built-in Security extension headers

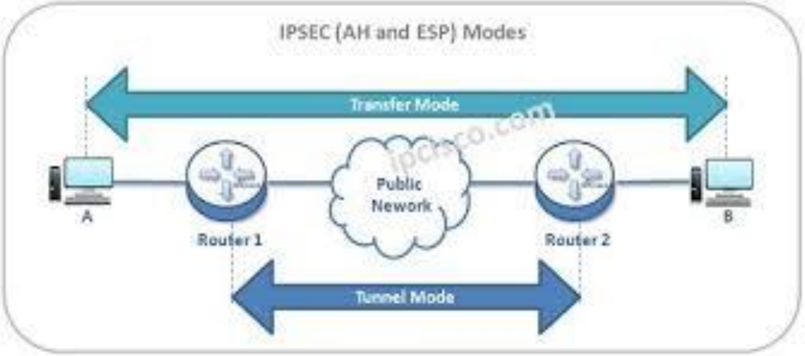


Reality

- There are security techniques can bypass secure extension headers such as Fragmentation Attack

MYTH 4

IPv6 - Confidentiality and data integrity without need for additional firewalls

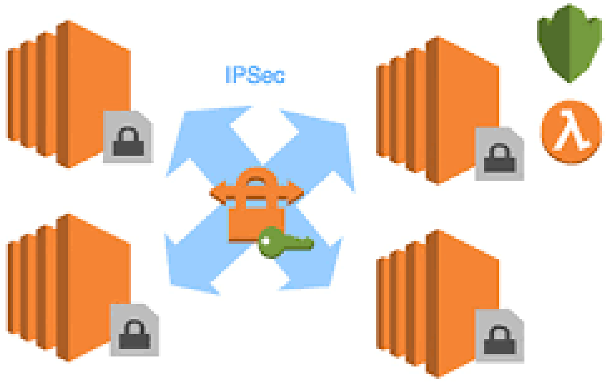


Reality

- There are attacks techniques can bypass secure extension for example Fragmentation Attack

MYTH 5

IPv6 - ICMPv6 uses IPSEC authentication and encryption.



Reality

- It was not implemented by most of the organisation when implementing because of the bootstrapping problem.
- IPSec required functional IP address to built the tunnel but when a new host joints any network there would be not any functional IPv6 address available.

MYTH 6

IPv6 - Built in Auto-configuration support

Reality

- Auto-configuration support does not overcome security issues in IPv6 because the standard NDP protocol does not have secure Router or Neighbor discovery process
- Refer RFC 4942 for more information about IPv6 Security

TALKING BEHIND MY BACK?

Within the confines of your network, **many devices may be communicating over IPv6**, even if they are not sending packets to and from the Internet!

REMEMBER…

Visibility is Security

…Which means…

<u>In</u>visibility is <u>In</u>security!

IPV6 SECURITY – AREAS OF CONCERNS

Internet and Network Security are areas of significant concern to organizations planning to (or already starting to) deploy IPv6 in their networks. There are several subtopics of this fairly broad topic:

- **System security** – protection at the node level. This involves host-based firewalls, Operating System vulnerabilities and understanding the threat model of a node that has enabled IPv6.
- **Network security** – protection at the network level.

IPV6 SECURITY - AREAS OF CONCERNS

- **Application security** – protection of network applications.

Training and experience – Engineers do not have much knowledge or real-world experience with IPv6.

Hackers – many hackers have had years to learn IPv6 and have done so.

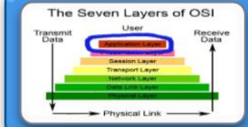
IPV6 SECURITY – SIMILARITIES TO IPV4 SECURITY

IPv6 is based heavily on IPv4, and has many similarities. Many existing network threats and defenses are independent of which IP family is being used:

- **Authentication** – username/password schemes are just as vulnerable over IPv6.
- **Privacy** – unencrypted traffic over IPv6 is just as easy to sniff (iNetmon, Wireshark and other tools fully supports IPv6).
- **DNS** can be attacked just as easily over IPv6 as over IPv4.
- **Application weaknesses** – Weaknesses in application layer protocols (e.g. web vulnerabilities) can be exploited in exactly the same ways as in IPv4.
- OS and application security patches still need to be applied on a timely basis.

EXTRA: THE SAME

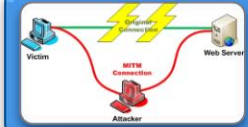
There are some security issues that IPv6 has little effect on:



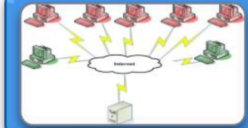
- Application-layer attacks

- Sniffing

- Rogue Devices



- Man-in-the-Middle Attacks



- Flooding/DoS Attacks

IPV6 SECURITY – DIFFERENCES FROM IPV4 SECURITY

- Address resolution (mapping Internet Layer IP addresses to Link Layer addresses) no longer uses ARP (which lives in the *Link Layer*). In IPv6 this is done with the ND (Neighbor Discovery) protocol (which lives in the *Internet Layer*)
- Fragmentation attacks are more easily detected. If a hacker somehow fragmented packets after the source, it can usually be detected and rejected.
- No NAT to hide behind. NAT does not increase security in any way.

IPV6 SECURITY – DIFFERENCES WITH IPV4 SECURITY (CONTINUED)

Header extensions – It is possible that hackers could exploit this new mechanism (e.g. force all packets to go via their node using source routing).

Since there is no NAT to break it, IPsec (AH and ESP) work great on IPv6, even between organizations.

IPSEC

IPSEC

IPsec, described in RFC 4301, defines a security architecture for both versions of IP for IPv4 and IPv6.

The following elements are part of the IPsec framework:

- A general description of security requirements and mechanisms at the network layer.
- A protocol for encryption (Encapsulating Security Payload, or ESP).
- A protocol for authentication (Authentication Header, or AH)
- A definition for the use of cryptographic algorithms for encryption and authentication
- A definition of security policies and security associations between communication peers
- Key management

WHY IPSEC?

- IP packets have no inherent security
  - No way to verify
    - The claimed sender is the true sender
- Nonrepudiation
    - The data has not been modified in transit
    - The data has not been viewed by a third party
- IPSec provides an automated solution for these three areas
    - Authentication
    - Integrity
    - Confidentiality

IPSEC COMPONENTS

The configuration of IPsec creates a boundary between a protected and an unprotected area.

The boundary can be around a single host or a network.

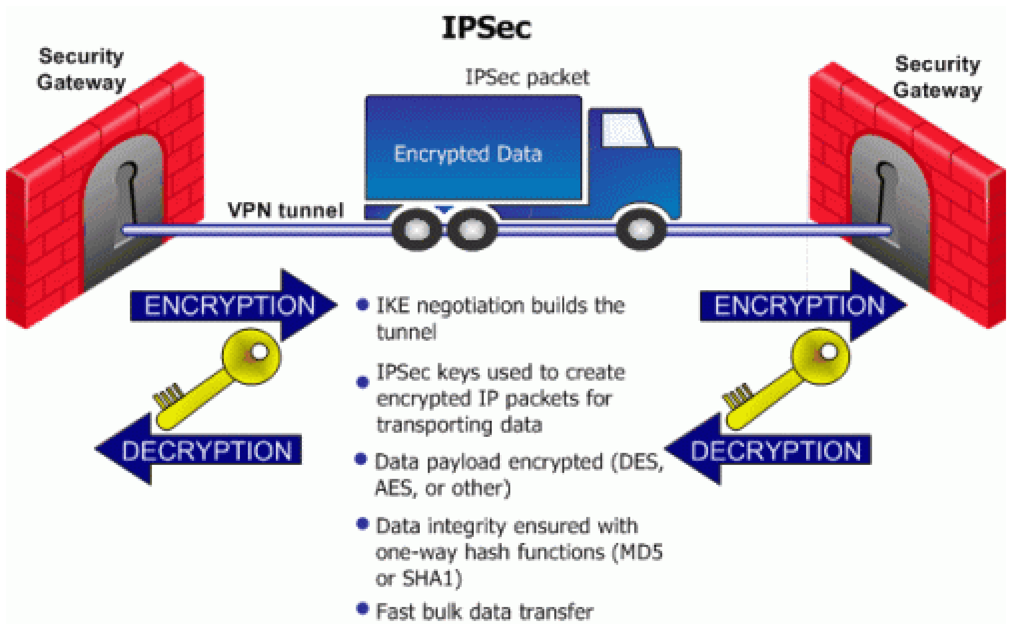
The access control rules specified by the administrator determine what happens to packets traversing the boundary.

The security requirements are defined by a *Security Policy Database* (SPD).

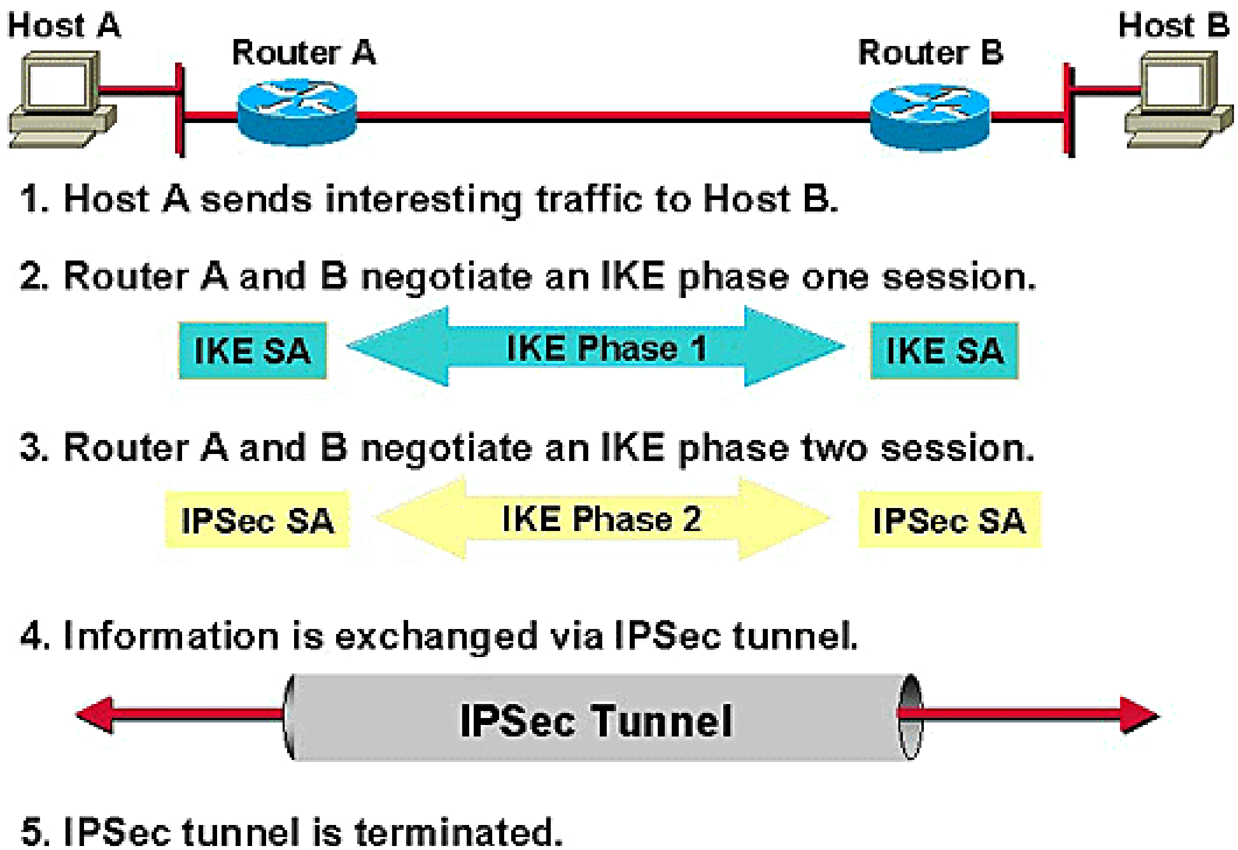
Generally, each packet is either protected using IPsec security services, discarded, or allowed to bypass IPsec protection, based on the applicable SPD policies identified by the *selectors*.

The selectors are the specific traffic-match criteria defined by an administrator— for example, a specific application being transmitted from a subnet to a specific end-host.

HOW IPSEC WORKS



HOW IPSEC WORKS……



IPSEC MODES OF TRANSPORT

IPsec differentiates two modes of transport:

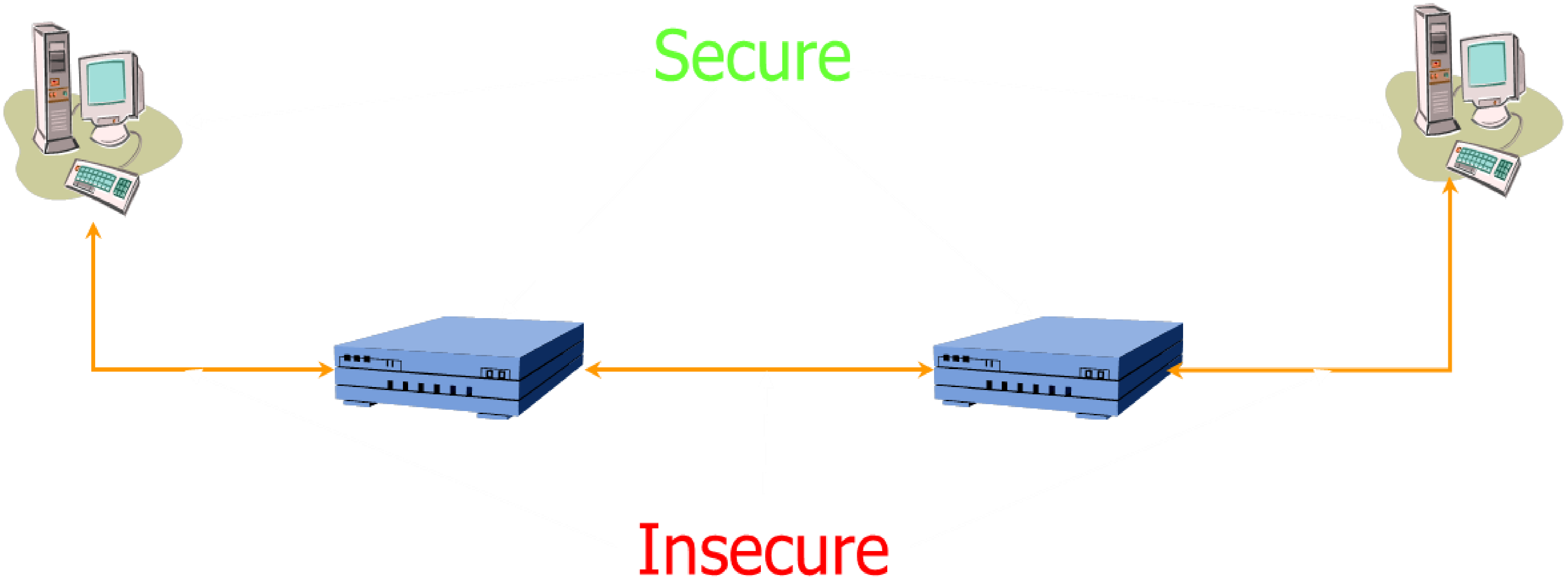
Transport mode:

- The SA is made between two end nodes and defines the encryption or authentication for the payload of all IP packets for that connection.
- The IP header is not encrypted.

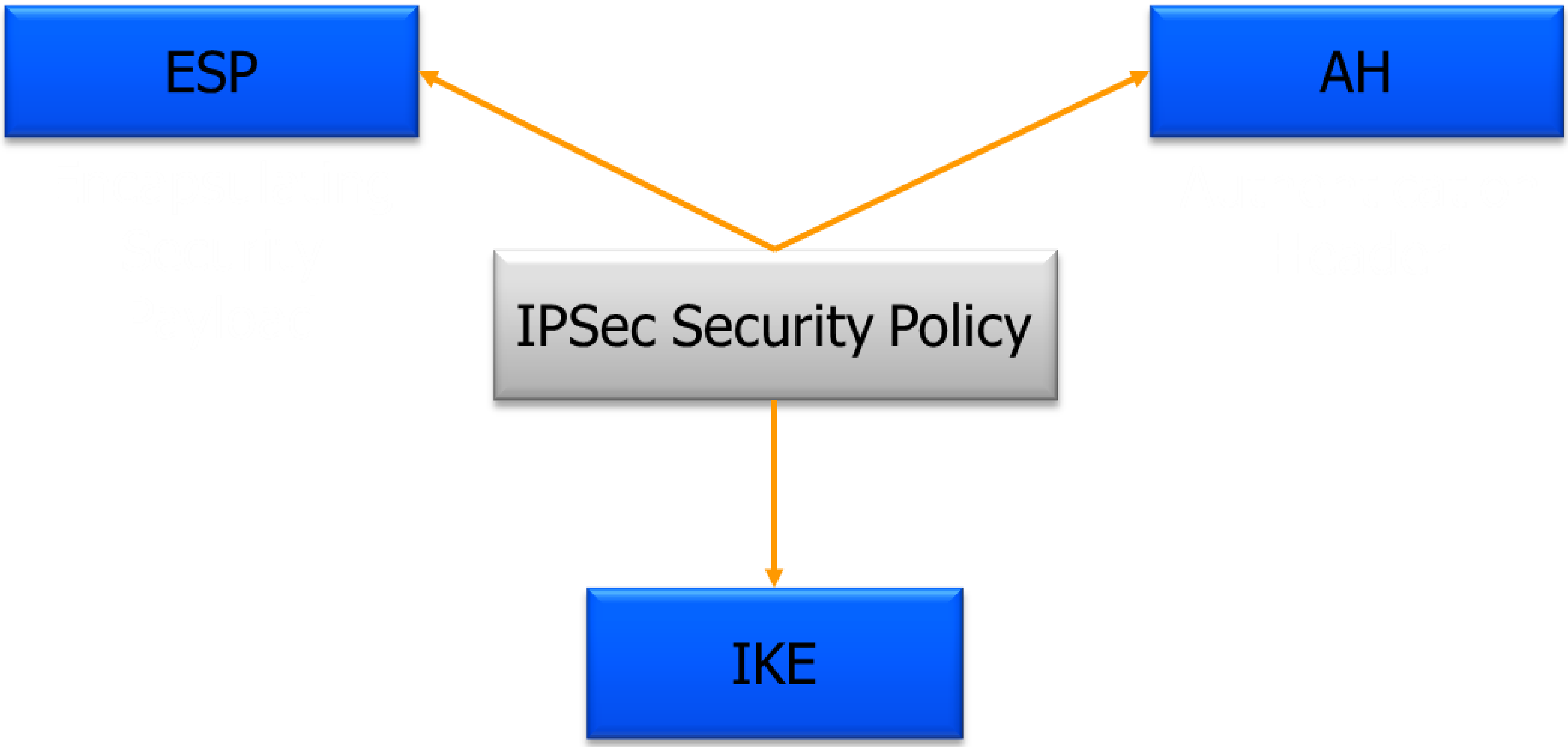
Tunnel mode:

- The SA is usually made between two security gateways (usually a firewall).
- The whole packet including the original IP header is encrypted or authenticated by encapsulating it in a new header.
- This is the foundation for a virtual private network (VPN).

SECURITY MODEL



IPSEC ARCHITECTURE

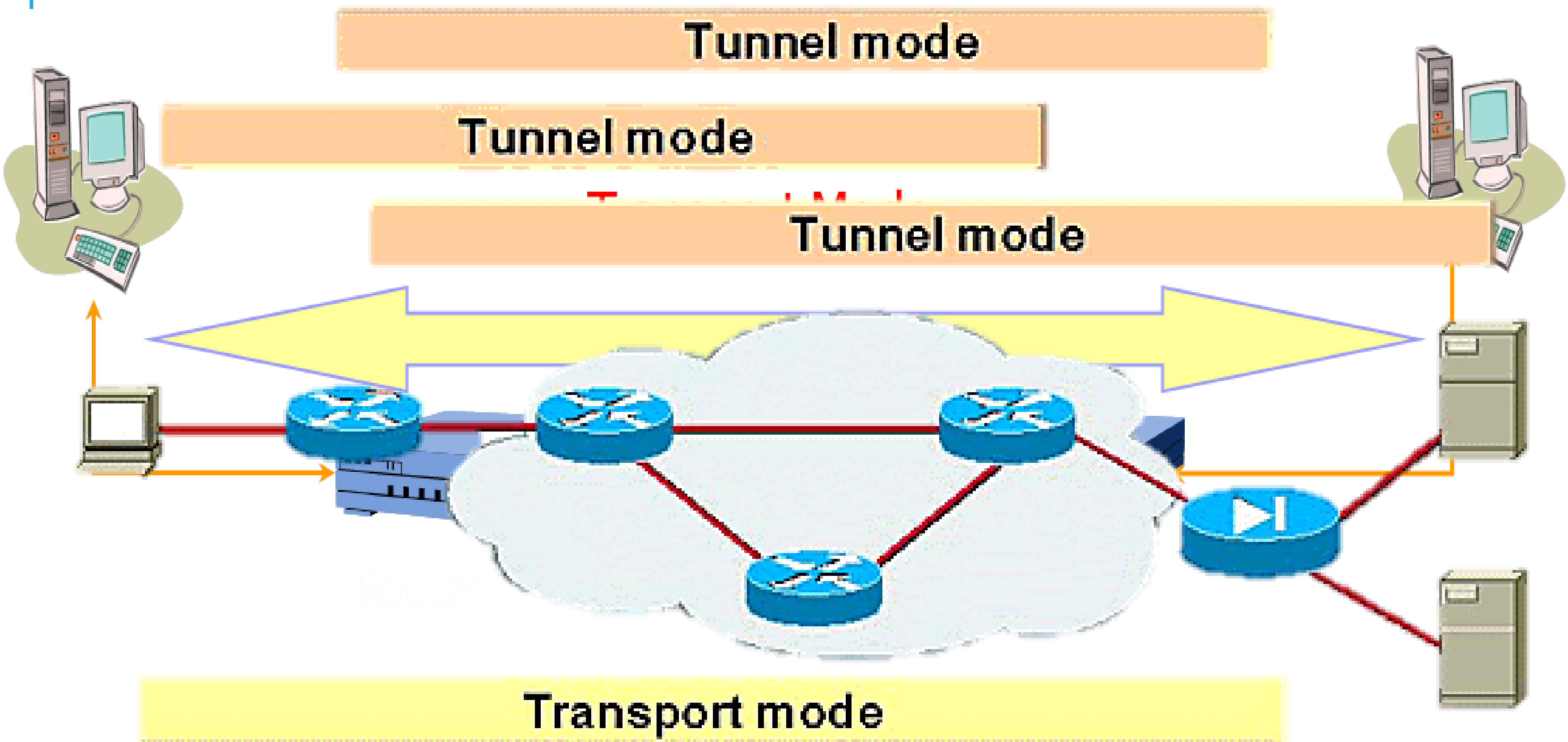


IPSEC ARCHITECTURE

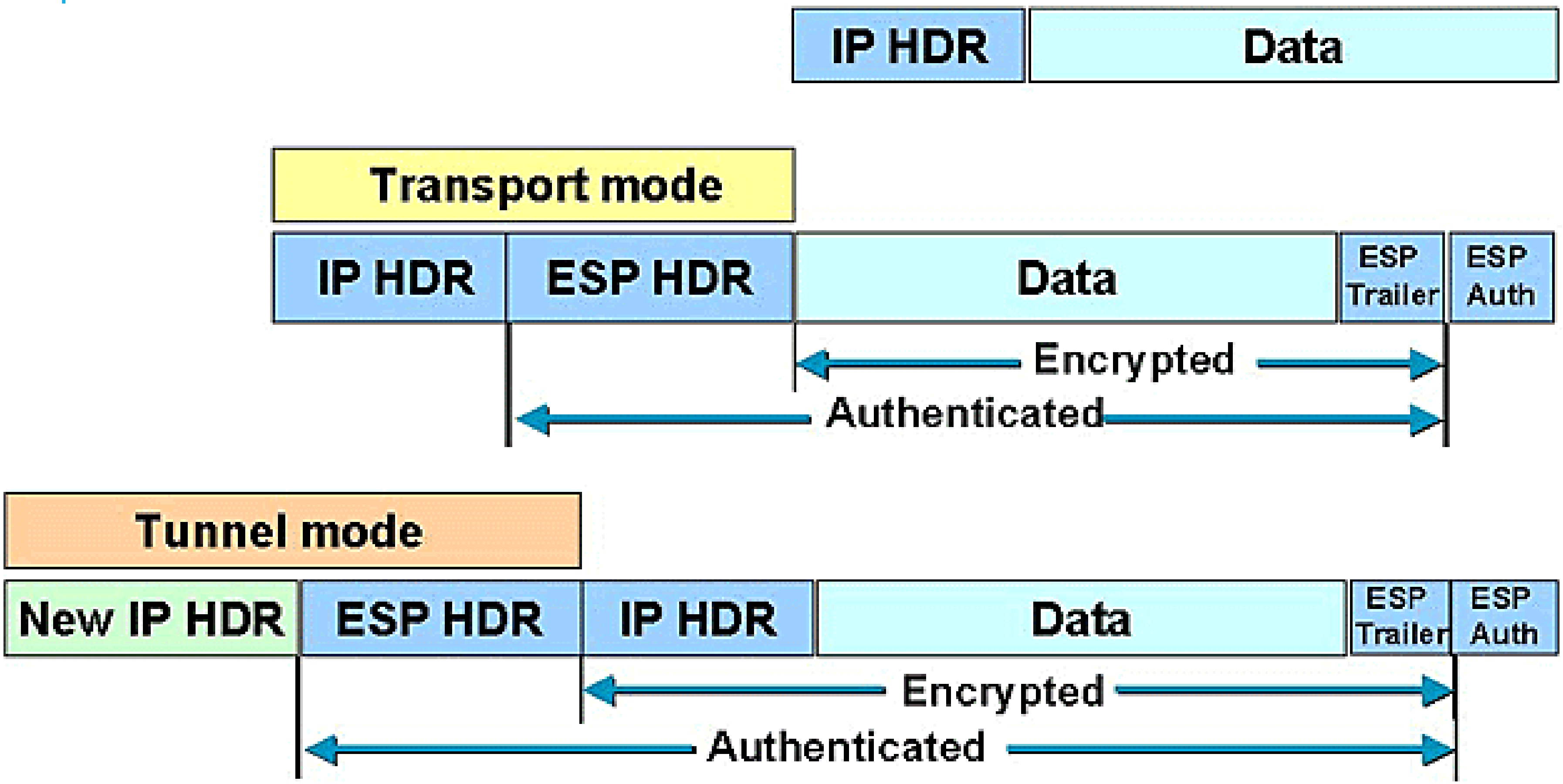
- Provides security in three situations:
  - Host-to-host, host-to-gateway and gateway-to-gateway

- Operates in two modes:
  - Transport mode (for end-to-end)
  - Tunnel mode (for VPN)

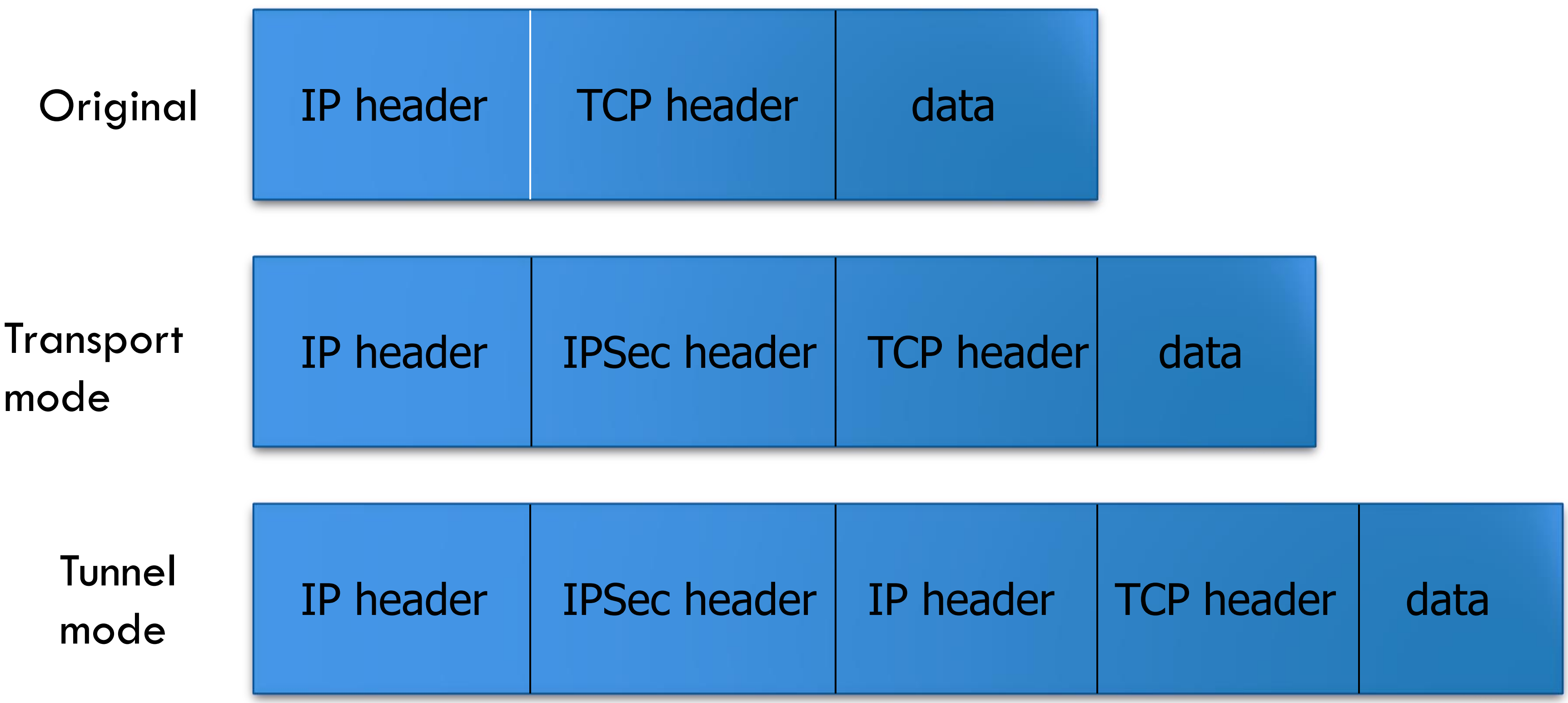
ARCHITECTURE



ARCHITECTURE

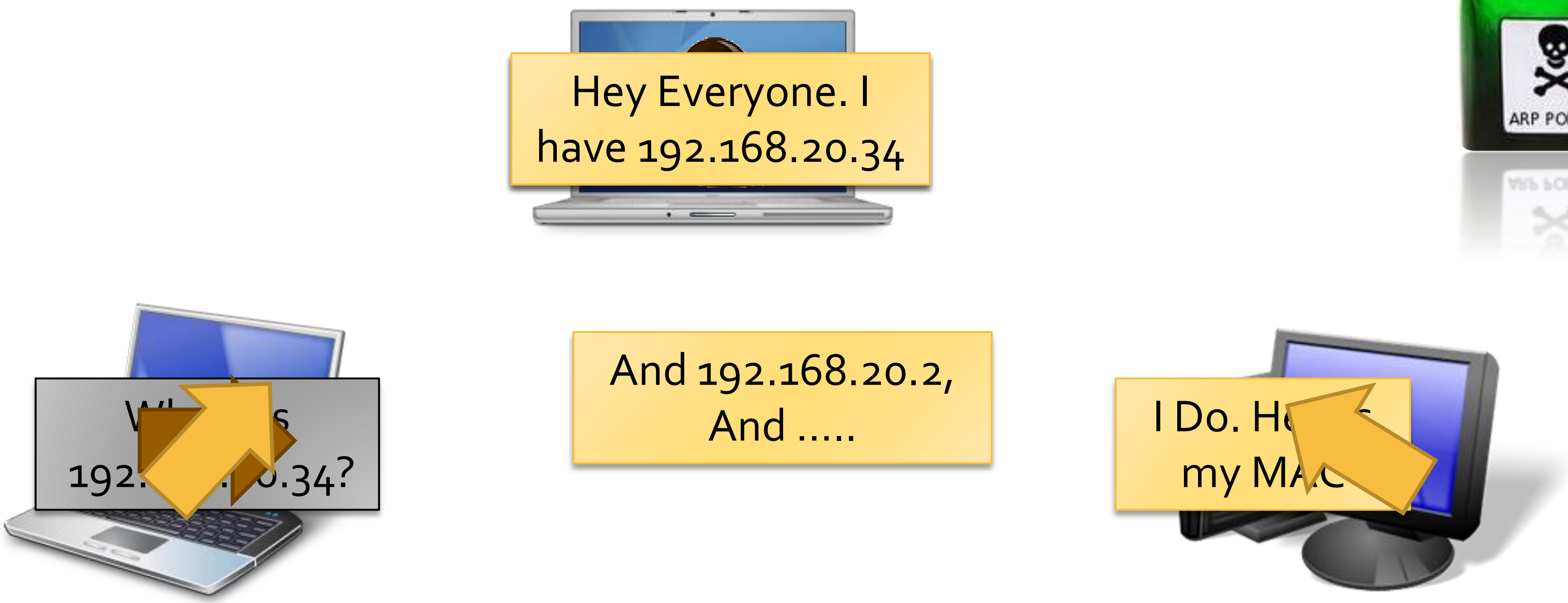


VARIOUS PACKETS



Secure Neighbour Discovery (SeND)

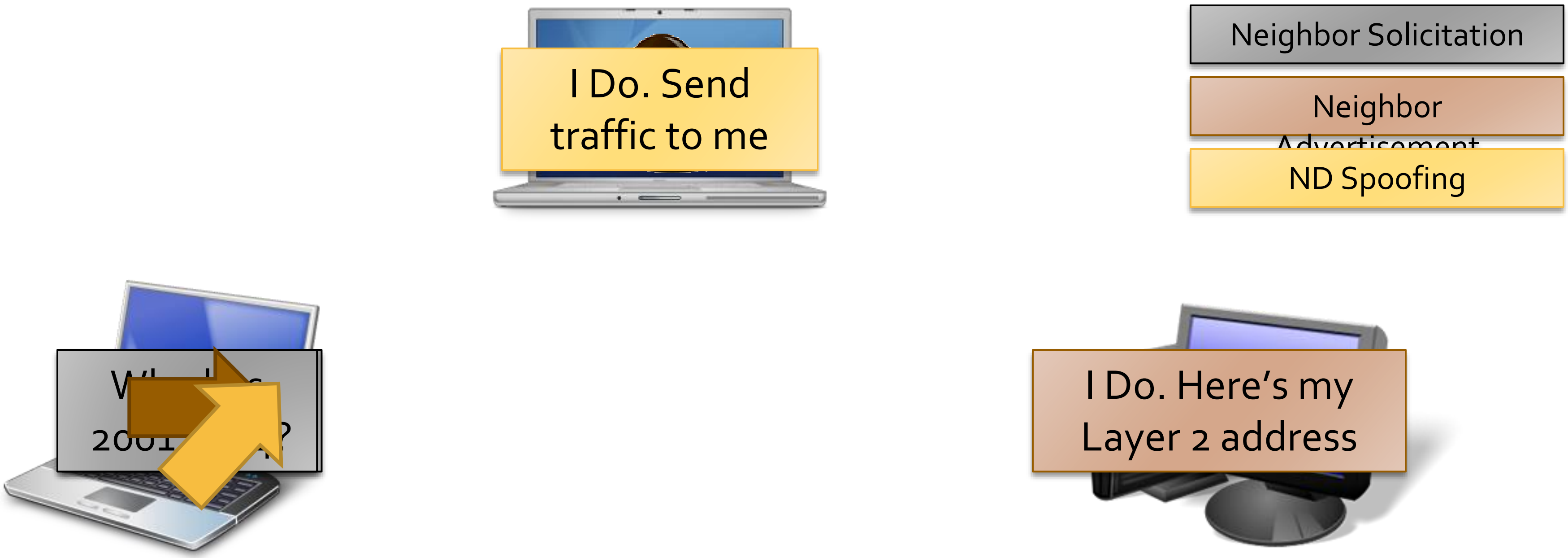
A LOOK BACK AT IPV4 ARP POISONING



Problem:

No authentication or security

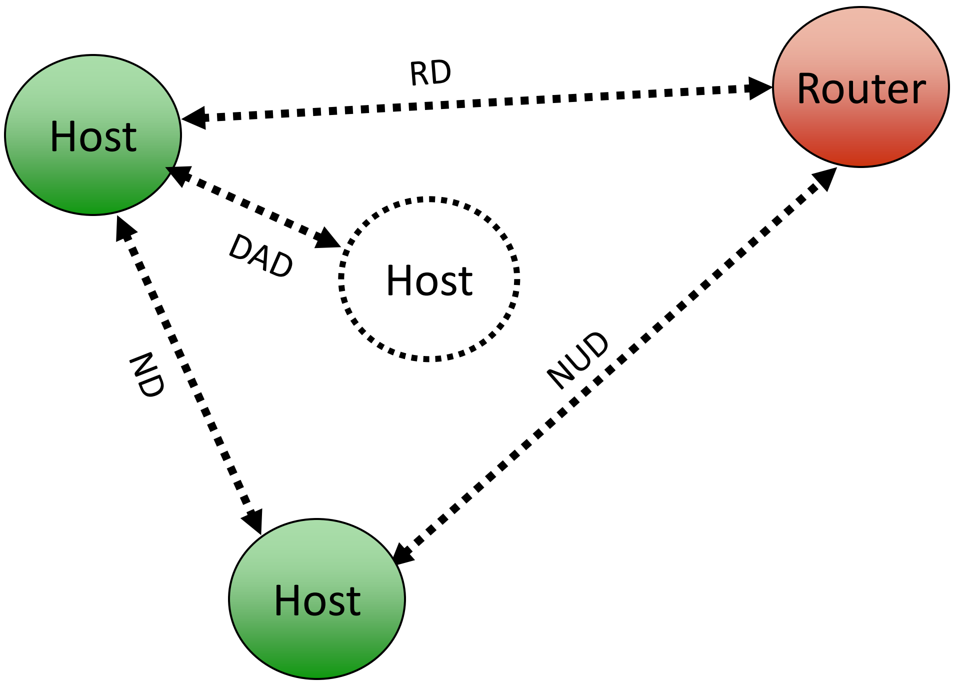
NEIGHBORHOOD DISCOVERY SUFFERS FROM SIMILAR ISSUES



Again:

No authentication or security

NEIGHBOR AND ROUTER DISCOVERY SECURITY



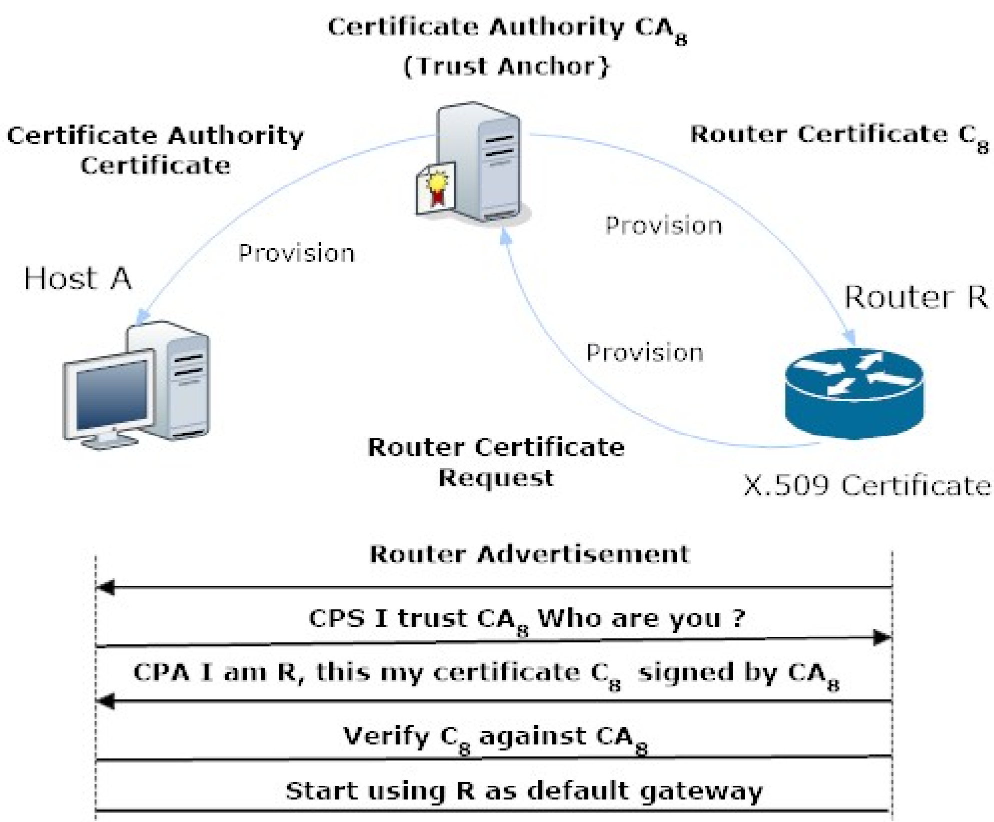
Vulnerabilities:

- Routers could be spoofed
- Neighbors could be spoofed
- Blocking address allocation
- Secure upper layers help, but do not prevent all attacks

Problems with “just use IPsec”

- Number of SAs very high
  - 2*N+2 per node
- Chicken-and-egg problem
- Does not help with authorization

SEND'S AUTHORIZATION DELEGATION DISCOVERY (ADD)

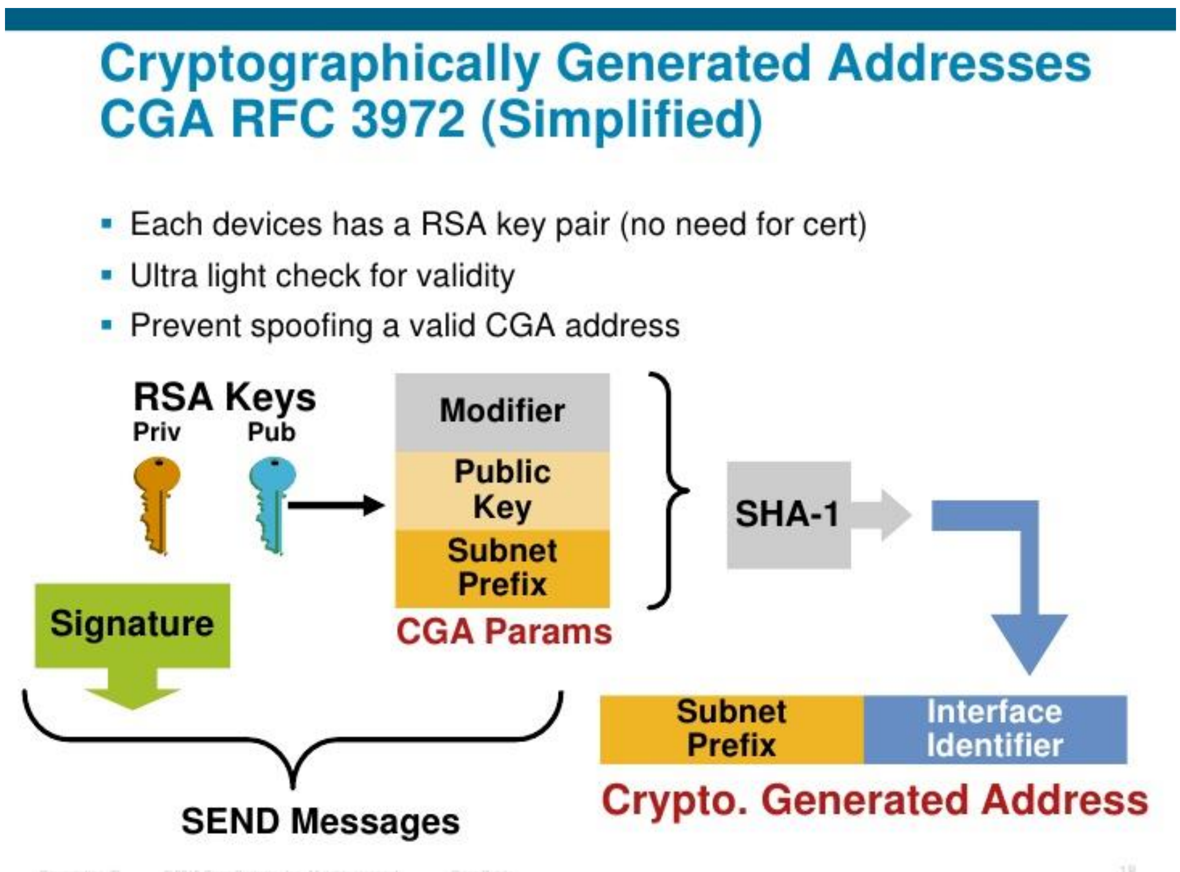


AlSa'deh, A. and C. Meinel, "Secure neighbor discovery: Review, challenges, perspectives, and recommendations", Security & Privacy, IEEE, 2012, 10(4): pp. 26-34

SEND CGA (CRYPTOGRAPHICALLY GENERATED ADDRESS)

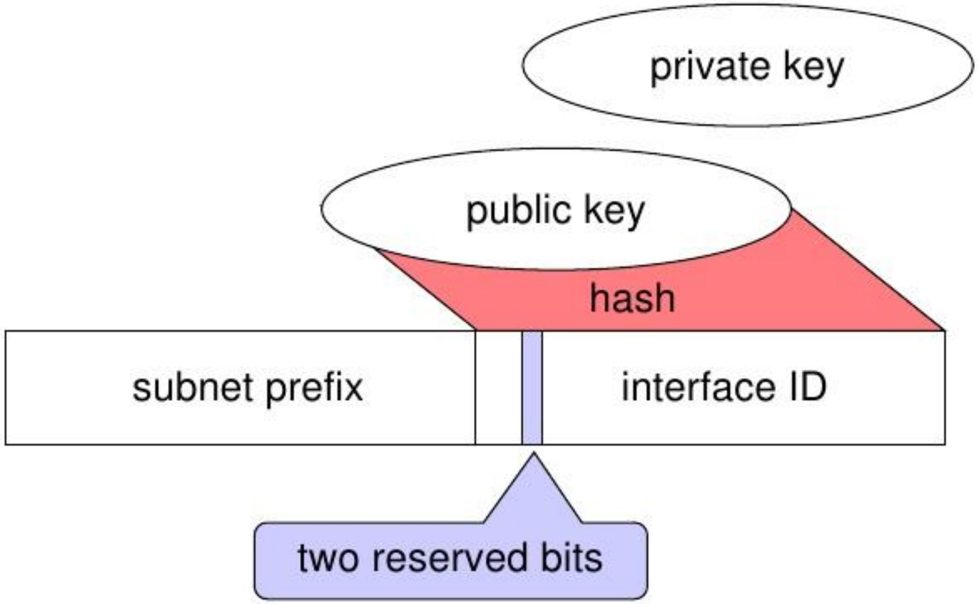
- An IPv6 address that has a host identifier computed from a cryptographic one-way hash function.
- A method for binding a public signature key to an IPv6 address in the secure neighbor discovery protocol (SeND).
- Formed by replacing the least-significant 64 bits of the 128-bit ipv6 address with the cryptographic hash of the public key of the address owner.
- Messages are signed with the corresponding private key.
- Only if the source address and the public key are known can the verifier authenticate the message from that corresponding sender.
- Requires no public-key infrastructure.
- Valid CGAs may be generated by any sender, including a potential attacker, but they cannot use any existing CGAs.

CGA METHOD


Cryptographically Generated Addresses
CGA RFC 3972 (Simplified)
Each devices has a RSA key pair (no need for cert)
Ultra light check for validity
Prevent spoofing a valid CGA address
RSA Keys
Priv
Pub
Modifier
Public Key
Subnet Prefix
CGA Params
SHA-1
Signature
SEND Messages
Subnet Prefix
Interface Identifier
Crypto. Generated Address

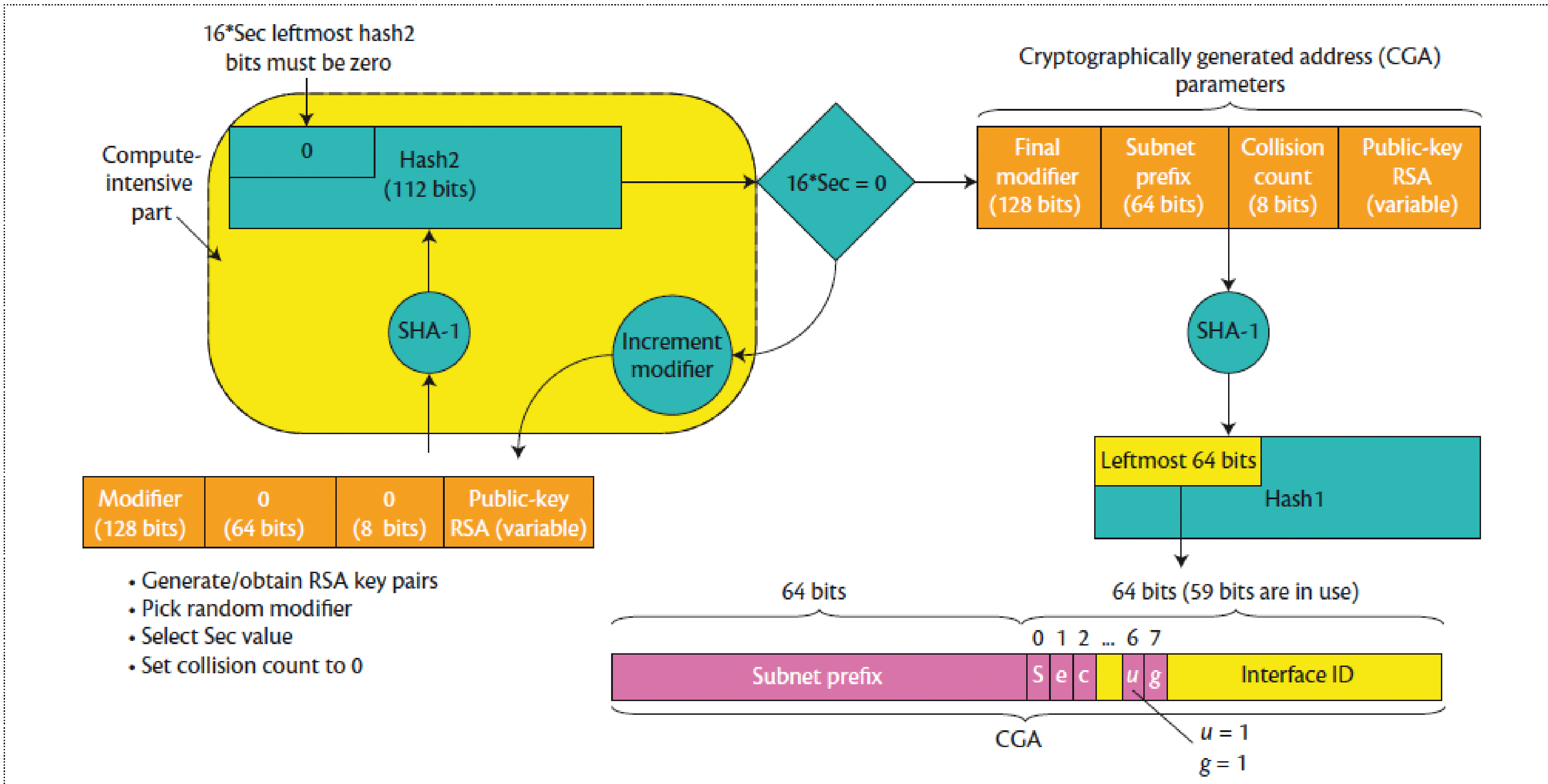
CGA METHOD

Cryptographically Generated Addresses (basic idea)



www.wiley.co.uk/go/gollmann

CGA METHOD


16*Sec leftmost hash2 bits must be zero
Compute-intensive part
0
Hash2 (112 bits)
SHA-1
Increment modifier
16*Sec = 0
Cryptographically generated address (CGA) parameters
Final modifier (128 bits)
Subnet prefix (64 bits)
Collision count (8 bits)
Public-key RSA (variable)
SHA-1
Leftmost 64 bits
Hash1
Modifier (128 bits)
0 (64 bits)
0 (8 bits)
Public-key RSA (variable)
• Generate/obtain RSA key pairs
• Pick random modifier
• Select Sec value
• Set collision count to 0
64 bits
64 bits (59 bits are in use)
0 1 2 ... 6 7
Subnet prefix
S e c
u g
Interface ID
CGA
u = 1
g = 1

CGA METHOD

1. A private/public key pair is generated for a node
2. Interface ID is calculated as an public key fingerprint
3. Subnet prefix and interface ID are concatenated
4. DAD is performed (CGA is recalculated if necessary – up to 3 times)
5. CGA parameter is formed:
   a) IPv6 address
   b) Private/Public key
   c) Some additional parameters
   d) DNS and other records are updated

THE RANDOM MODIFIER ALLOWS TO CHANGE THE FINGERPRINT (IP ADDRESS) PERIODICALLY)

CGA VERIFICATION

1. The verifier know the sender IP address (CGA)
2. The verifier gets the sender public/private key from CGA parameter
3. The verifier checks the association between IPv6 CGA and the corresponding public key
4. After that, the digital signature of ND message is verified

NO PKI, CA OR TRUSTED SERVERS NEEDED

CGA METHOD

Table 1: CGA generation time for different sec values

Source	Specification of setup	sec = 0	sec = 1	sec = 2	sec = 3
[8]	Pentium 4.3GHz, Memory 1GB. Linux (Kernel 2.4)	15.57µs	just over 0.1 seconds	100 seconds	more than 200 hours
[9]	Machine with moderate processing power	n/a	1 minute	16 days	n/a
[2]	A modern PC (AMD64)	n/a	0.2 seconds	3.2 hours	24 years

PROBLEM WITH CGA-BASED DRAFTS: QUOTE FROM FRC 3972 SECTION 7.4

A strong cautionary note has to be made about using CGA for purpose other than SEND

- *"Each protocol MUST define its own type tag values as explained":* to defend against "related protocol" attacks
- *"The minimum RSA key length of 384 bits may be too short for many applications and the impact of key compromise on the particular protocol must be evaluated":* more considerations are necessary
- *"If the goal is not to verify claims about IPv6 addresses, CGA signatures are probably not the right solution":* not a sufficient security mechanism

THREATS COUNTERED BY SEND

Threats	How SEND counters?
Neighbor Solicitation/Advertisement Spoofing	SEND requires the RSA Signature and CGA options to be present in solicitations
Neighbor Unreachability Detection Failure	SEND requires a node responding to Neighbor Solicitations probes to include an RSA Signature option and proof of authorization to use the interface identifier in the address being probed.
Duplicate Address Detection DoS Attack	SEND requires to include an RSA Signature option and proof of authorization in the Neighbor Advertisements sent as responses to DAD
Router Solicitation and Advertisement Attacks	SEND requires Router Advertisements to contain an RSA Signature option and proof of authorization.
Replay Attacks	SEND includes a Nonce option in the solicitation and requires the advertisement to include a matching option.

Unique Local Address

PRIVACY ADDRESSES (UNIQUE LOCAL ADDRESS)

Introduction

- Globally unique prefix (with high probability of uniqueness).
- Well-known prefix to allow for easy filtering at site boundaries.
- Allow sites to be combined or privately interconnected without creating any address conflicts or requiring renumbering of interfaces that use these prefixes.
- Internet Service Provider independent and can be used for communications inside of a site without having any permanent or intermittent Internet connectivity.
- If accidentally leaked outside of a site via routing or DNS, there is no conflict with any other addresses.
- In practice, applications may treat these addresses like global scoped addresses.

HISTORY

- In 1995, block fec0::/10 was reserved for site-local addresses.
- This was deprecated due do confusion of what “site” constitutes.
- In October 2005, block fc00::/7 was reserved for use in private IPv6 networks, and defining the associated term unique local addresses.

DEFINITION

- The address block fc00::/7 is divided into two /8 groups:
- The block fc00::/8 has not been defined yet.
- The block fd00::/8 is defined for /48 prefixes, formed by setting the 40 least-significant bits of the prefix to a randomly-generated bit string.
- This results in the format fdxx:xxxx:xxxx:: for a prefix in this range.

PROPERTIES

- Prefixes in the fd00::/8 range have similar properties as those of the IPv4 private address ranges:
  - They are not allocated by an address registry and may be used in networks by anyone without outside involvement.
  - They are not guaranteed to be globally unique.
  - Reverse DNS entries (under ip6.arpa) for fd00::/8 ULAs cannot be delegated in the global DNS.
- As fd00::/8 ULAs are not meant to be routed outside their administrative domain (site or organization), administrators of interconnecting networks normally do not need to worry about the uniqueness of ULA prefixes.

IPV6 ATTACKS

IPv6 Application Remote Exploit

Stack-Based Buffer Overflow Exploitation

Format String Exploitation

IPv6 Protocol Vulnerability

Man In The Middle

Denial of Services

Others

- IPv6 Fragmentation
- Transition Mechanism
- ICMP attacks against TCP

KNOWN ICMPV4 ATTACKS

Below are known ICMPv4 Attacks that also can be present in ICMPv6

ICMP Sweep

Inverse mapping

Trace Route network mapping

OS fingerprinting

ICMP route re-direct

Ping of Death

ICMP Smurf attack

ICMP Nuke attack

Attack using source quench

UNIQUE ICMPV6 ATTACKS

In IPv6 networks, there are attacks that are only specific to ICMPv6. These attacks would not be present in IPv4 networks.

MITM WITH SPOOFED ICMPV6 NEIGHBOR ADVERTISEMENT

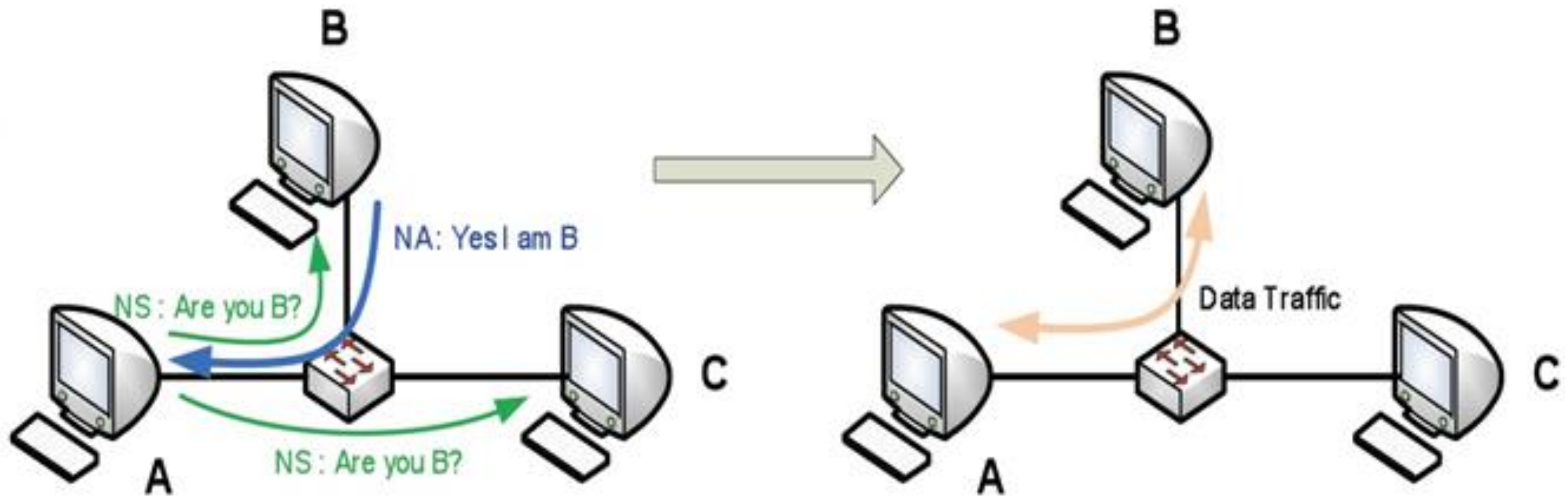


Figure – Establishing communication and data transfer between Node A and Node B (Atik Pilihanto, 2011)

MITM WITH SPOOFED NEIGHBOR ADVERTISEMENT

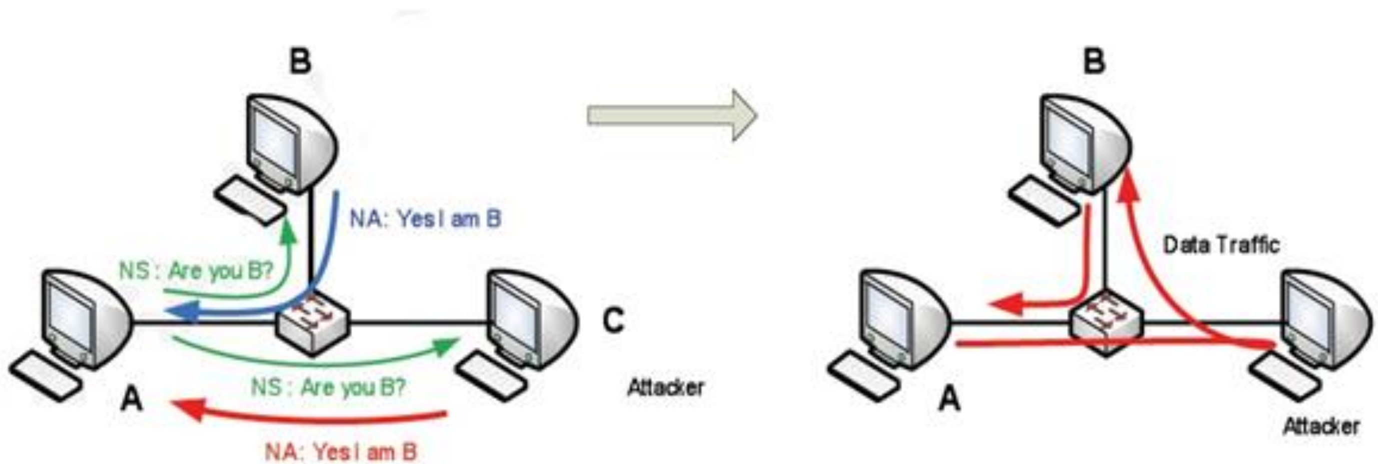


Figure – MITM Attack with spoofed ICMPv6 Neighbour Advertisement (Atik Pilihanto,2011)

MAN IN THE MIDDLE ATTACK WITH SPOOFED ICMPV6 NEIGHBOUR ADVERTISEMENT

- The attacker can gain access to communication between two nodes. Gaining access to the communication between two nodes will leads to sniffing and session hijacking attacks.

- IPv4 - MITM carried out using ARP Cache Poising and DHCP spoofing. Since in IPv6, ARP is replaced by ICMPv6 neighbor discovery process, so this attacks only unique to IPv6 networks only

- ICMPv6 - heavier presence of Type 135 and 136

- Since the RFC 792 (ICMPv4) does not have provision for NS and NA, so the attack would not be present in the IPv4 networks.

DUPLICATE ADDRESS DETECTION (DAD)

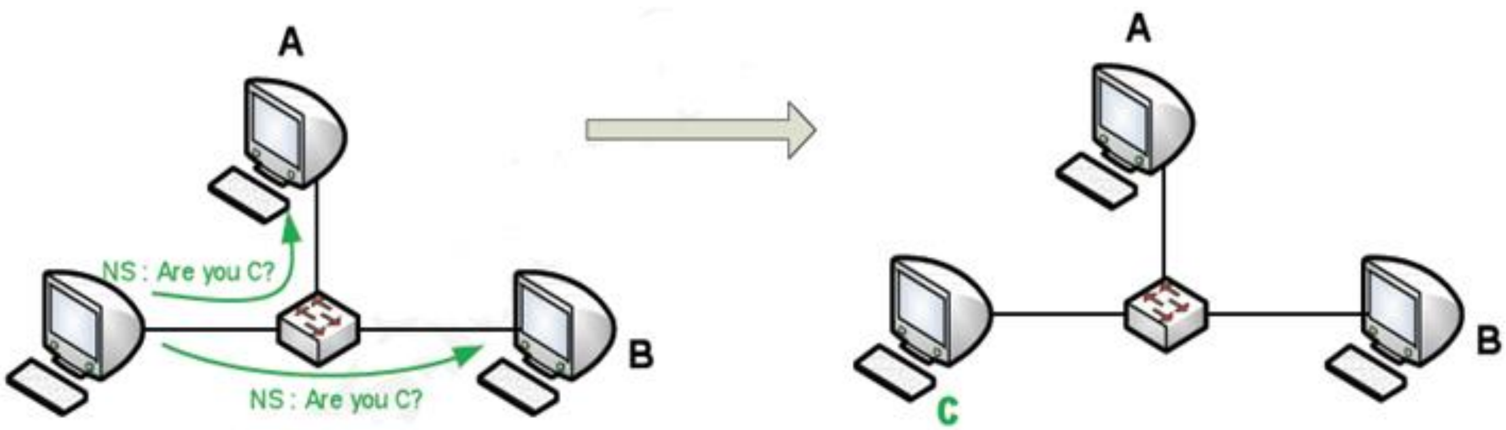


Figure – **Duplicate Address Detection (DAD) (Atik Pilihanto, 2011)**

DUPLICATE ADDRESS DETECTION (DAD)

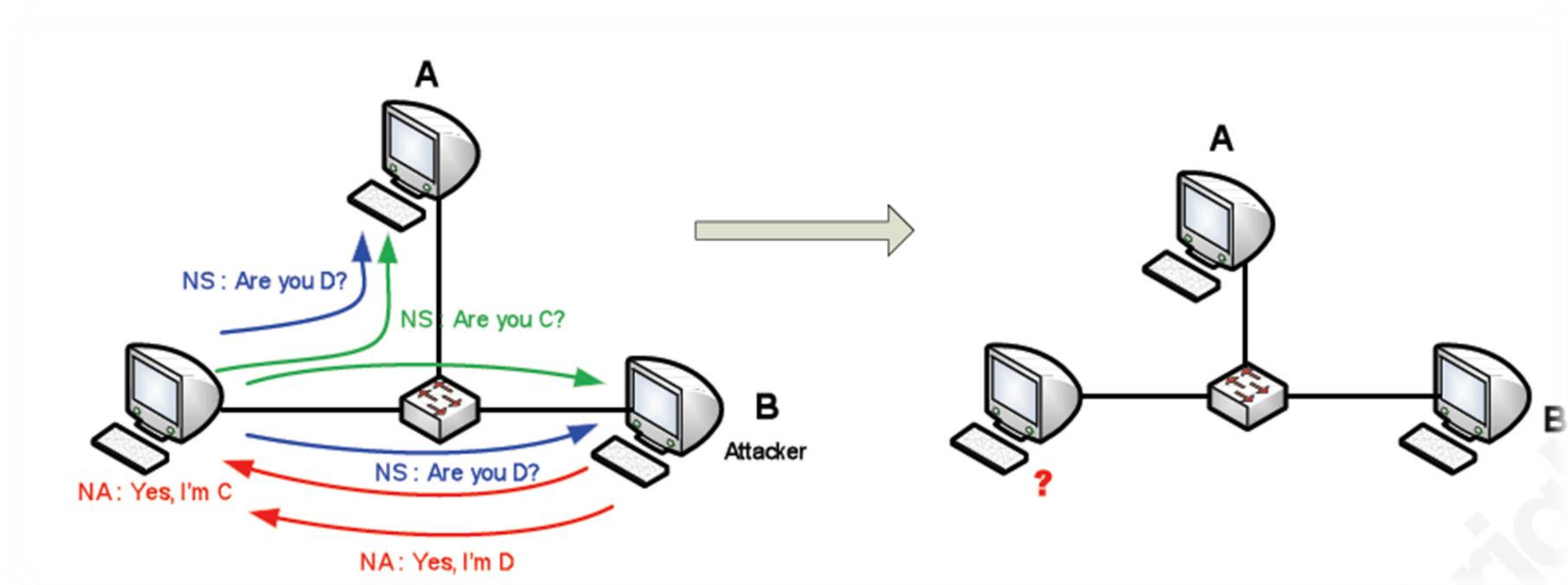


Figure – **Duplicate Address Detection (DAD) (Atik Pilihanto, 2011)**

DUPLICATE ADDRESS DETECTION (DAD)

- In order to detect whether an IPv6 address already exist in the network under the IPv6 stateless auto configuration, Duplicate Address Detection (DAD) protocol is used to detect the duplication.

- DAD uses ICMPv6 neighbor solicitation by sending to all the nodes multicast addresses. If there are no IPv6 addresses exist on the network, no response will be sent back to the solicitation source host

- ICMPv6 - heavier presence of Type 135 and 136

- Since the RFC 792 (ICMPv4) does not have provision for NS and NA, so the attack would not be present in the IPv4 networks.

IPV6 HACKING TOOLS – SNIFFERS, PACKET CAPTURE

Snort – Intrusion detection tool - http://www.snort.org/

WinPcap – Promiscuous mode packet capture tool for Windows (used by other tools such as WireShark) - http://www.winpcap.org/

TCPdump / LibPCap – command line promiscuous mode packet capture tool for FreeBSD / Linux / Mac OS X - http://www.tcpdump.org/

Windump - TCPDump for Windows - http://www.winpcap.org/windump/

COLD - (Supports IPv6 since 1.0.12) - http://www.ipv4.it/cold/

Wireshark - GUI based packet capture and protocol analysis tool (IPv4 + IPv6) for Windows, Mac OS X - http://www.wireshark.org/

IPV6 HACKING TOOLS – PACKET FORGERS/ COMPLETE TOOLKIT

Packet forgers

- **Scapy** - generate any IPv4/IPv6 packet (even pathological)
  - IPv6 functionality merged into main project (no longer separate scapy6)
  - Embedded in python scripting language (must learn python to use scapy)
  - http://hg.scdev.org/scapy
- **SendIP** – send any IPv4/IPv6 packet (no need to learn python)
  - http://freshmeat.net/projects/sendip
- **Packit** – Packet Toolkit - Network injection and capture
  - http://packetfactory.openwall.net/projects/packit

Complete toolkit – **THC-IPv6** – attacking the IPv6 protocol suite

- Contains many tools, runs on FreeBSD / Linux / Mac OS X
- http://thc.org/thc-ipv6/

IPV6 HACKING TOOLS – SCANNERS, REDIRECTION, DENIAL OF SERVICE

parasite6: icmp neighbor solitication/advertisement spoofer, puts you as man-in-the-middle, same as ARP mitm (and parasite)

alive6: an effective alive scanning, which will detect all systems listening to this address

dnsdict6: parallized dns ipv6 dictionary bruteforcer

fake_router6: announce yourself as a router on the network, with the highest priority

redir6: redirect traffic to you intelligently (man-in-the-middle) with a clever icmp6 redirect spoofer

toobig6: mtu decrease with the same intelligence as redir6

detect-new-ip6: detect new ip6 devices which join the network, you can run a script to automatically scan these systems etc.

IPV6 HACKING TOOLS – SCANNERS, REDIRECTION, DENIAL OF SERVICE

- dos-new-ip6: detect new ip6 devices and tell them that their chosen IP collides on the network (DOS).

trace6: very fast traceroute6 with supports ICMP6 echo request and TCP-SYN

flood_router6: flood a target with random router advertisements

flood_advertise6: flood a target with random neighbor advertisements

fuzz_ip6: fuzzer for ipv6

implementation6: performs various implementation checks on ipv6

implementation6d: listen daemon for implementation6 to check behind a FW

fake_mld6: announce yourself in a multicast group of your choice on the net

fake_mld26: same but for MLDv2

fake_mldrouter6: fake MLD router messages

fake_mipv6: steal a mobile IP to yours if IPSEC is not needed for authentication

fake_advertiser6: announce yourself on the network

IPV6 HACKING TOOLS – SCANNERS, REDIRECTION, DENIAL OF SERVICE

smurf6: local smurfer

rsmurf6: remote smurfer, known to work only against linux at the moment

exploit6: known ipv6 vulnerabilities to test against a target

denial6: a collection of denial-of-service tests againsts a target

thcping6: sends a hand crafted ping6 packet

sendpees6: a tool which generates a neighbor solicitation requests with a lot of CGAs (crypto stuff ;-) to keep the CPU busy

THANK YOU