APNIC

Network Security Fundamentals

WEBINAR COURSE

Speakers

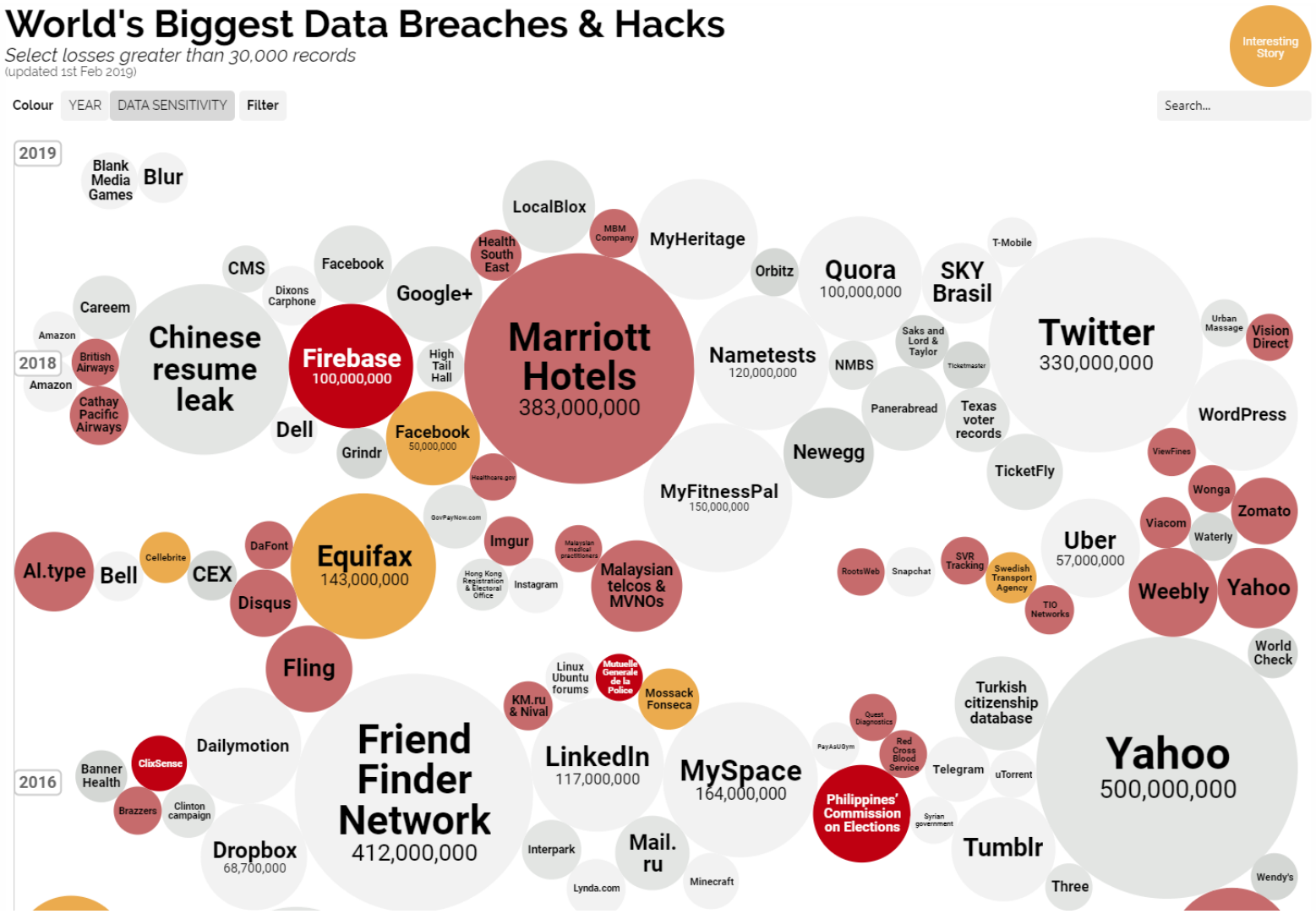
- Jamie Gillespie (APNIC Senior Security Specialist)
- Jessica Wei (APNIC Network Analyst)

Overview

- Information Security Landscape
- Definitions in Information Security
- CSIRT/CERT Introduction
- Infrastructure Security
- Cryptography
- VPN and IPsec
- DoS and DDoS

Information Security Landscape

Security Breaches



Ref: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Shortened: https://goo.gl/P1279w

Security Breaches

- haveibeenpwned.com tracks accounts that have been compromised and released into the public
  - 346 pwned websites
  - 6,931,949,148 pwned accounts
  - 90,470 pastes
  - 111,609,979 paste accounts

Security Breaches

- zone-h.org/archive tracks and archives website defacements

Time	Notifier	H	M	R	L	Domain	OS
2019/02/17	AlFaransi	H				rockwellnc.gov	Linux
2019/02/16	NeT-DeViL			R		www.utahcounty.gov/Dept/ksa.html	Win 2012
2019/02/16	NeT-DeViL					ethics.test.ohio.gov/cogel/dis...	Win 2012
2019/02/12	Nexamos	H				oig.nasa.gov	Linux
2019/01/28	loginner01tr01					www.healthcare.gov/robots.txt	Linux
2019/01/25	RxR					www.perb.ny.gov/BoOX.php	Linux
2019/01/23	darkshadow-tn			R		dickinsoncountymi.gov/images/m...	Win 2008
2019/01/22	./KryptonWave					search.wi.gov/cpp/cs.html?url=...	F5 Big-IP
						maps.nccs.nasa.gov/arcgis/shar...	Linux
						eoimages.gsfc.nasa.gov/images/...	Linux
				R		library.lodi.gov/c.txt	Win 2012

hacked by proxy ~~ guardiran security team

Hello Admin , i am White hat hacker , i am here just for help to you !

i Patched your Vulnerability ;) , now you can delete This html Page. Good Luck Partner <3

zone-h unrestricted information

Home News Events Archive Archive Onhold Notify Stats Register Login

NOTIFIER DOMAIN .au

Special defacements only Fulltext/Wildcard Onhold (Unpublished) only

Date : ALL Apply filter

Total notifications: **157,997** of which **40,701** single ip and **117,296** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	Domain	OS	View
2019/03/04	ErrOr SquaD					riskma.com.au/read.txt	Linux	mirror
2019/03/04	ErrOr SquaD					marciniakhousecoaching.com.au/...	Linux	mirror
2019/03/04	ErrOr SquaD					www.ryzodeg.com.au/read.txt	Linux	mirror
2019/03/04	ErrOr SquaD					garagesaleday.com.au/read.txt	Linux	mirror
2019/03/04	Vijune15			R		www.allmattingsolutions.com.au...	Linux	mirror
2019/03/03	aNis Dz ProD	H				www.aceauto.com.au	Linux	mirror
2019/03/02	zakiloup					easec.com.au/Back.html	Linux	mirror
2019/03/02	suliman_hacker	H	M			human-resource-management.com.au	Linux	mirror
2019/03/02	Ali Afee		M			www.hannahboyd.com.au/ali.txt	Linux	mirror
2019/03/02	Trenggalek Cyber Army		M			getlostcampers.com.au/jembot.txt	Linux	mirror
2019/03/02	Trenggalek Cyber Army		M			durexperiment.com.au/jembot.txt	Linux	mirror
2019/03/01	Simsimi	H	M			mintrestro.com.au	Linux	mirror
2019/02/28	ErrOr SquaD					brightlilyhealthcare.com.au/Hu...	Linux	mirror
2019/02/27	Raiz0WorM					hotpotcreative.com.au/Cookies....	Linux	mirror
2019/02/27	ErrOr SquaD					copysmith.com.au/read.txt	Linux	mirror
2019/02/26	Panataran					ephealthcare.com.au/wp-include...	Linux	mirror
2019/02/26	Panataran					2hmediasolutions.com.au/wp-adm...	Linux	mirror
2019/02/26	Panataran			R		ductsystems.com.au/libraries/c...	Linux	mirror
2019/02/25	Panataran					elearn.qualifyme.edu.au/wp-con...	Linux	mirror

Security Breaches

- Common vulnerabilities can lead to mass compromises

January 08, 2008

Mass SQL injection attack compromises 70,000 websites

Updated Wed., Jan. 9, 2008, at 4:37 p.m. EST

An automated SQL injection attack, which at one point compromised more than 70,000 websites, hijacked visitors' PCs with a variety of exploits last week, according to researchers.

Coordinated Website Compromise Campaigns Continue to Plague Internet

Martin Lee - March 20, 2014 - 18 Comments

Is your website at risk from the 50,000 compromised WordPress sites?

JULY 28, 2014 | IN APPLICATION SECURITY | BY VENKATESH SUNDAR

3 MONTHS AFTER TICKETMASTER ATTACK, BREACHED TOOLS STILL IN USE ON OVER 1000 WEBSITES

By Source Defense Posted September 26, 2018 In Articles

Definition in Information Security

InfoSec Definitions

- Let's start with definitions so we speak a common language
- **Information Security**
  - the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information
  - The purpose of information security management is to ensure business continuity and reduce business damage by preventing and minimizing the impact of security incidents
    - This is done through Prevention, Detection, and Recovery
  - Information, IT, Internet, Cyber… it's all Security

InfoSec Definitions

- **Asset** - what we are trying to protect
  - The “information” part of “information security”
  - Resources
    - Physical – servers, routers, switches
    - Virtual – CPU, memory, bandwidth, network connections

InfoSec Definitions

- **Threat** - a circumstance or event with the potential to negatively impact an asset
  - Intentional
    - Hacking, malware, DDoS, company insiders, theft
  - Accidental
    - Malfunction, user error
  - Natural
    - Natural disaster, earthquakes, storms/floods

InfoSec Definitions

- **Vulnerability** - weakness in an asset's design or implementation
  - Software bugs
    - Most vulnerabilities you'll hear of fall into this category, OS's, applications, services
  - Protocol "bugs" or design flaws
    - SYN flood, predictive sequence numbers, ASN.1, NTLM
  - Misconfigurations
  - Insecure authentication
    - Weak passwords, lack of 2FA/MFA
  - Unvalidated inputs
    - SQL injection, Cross Site Scripting (XSS)
  - Poor physical security
    - Example on next slide…

InfoSec Definitions

The brazen airport computer theft that has Australia's anti-terror fighters up in arms

By Philip Cornford
September 5, 2003

On the night of Wednesday, August 27, two men dressed as computer technicians and carrying tool bags entered the cargo processing and intelligence centre at Sydney International Airport.

They presented themselves to the security desk as technicians sent by Electronic Data Systems, the outsourced customs computer services provider which regularly sends people to work on computers after normal office hours.

After supplying false names and signatures, they were given access to the top-security mainframe room. They knew the room's location and no directions were needed.

Inside, they spent two hours disconnecting two computers, which they put on trolleys and wheeled out of the room, past the security desk, into the lift and out of the building.

InfoSec Definitions

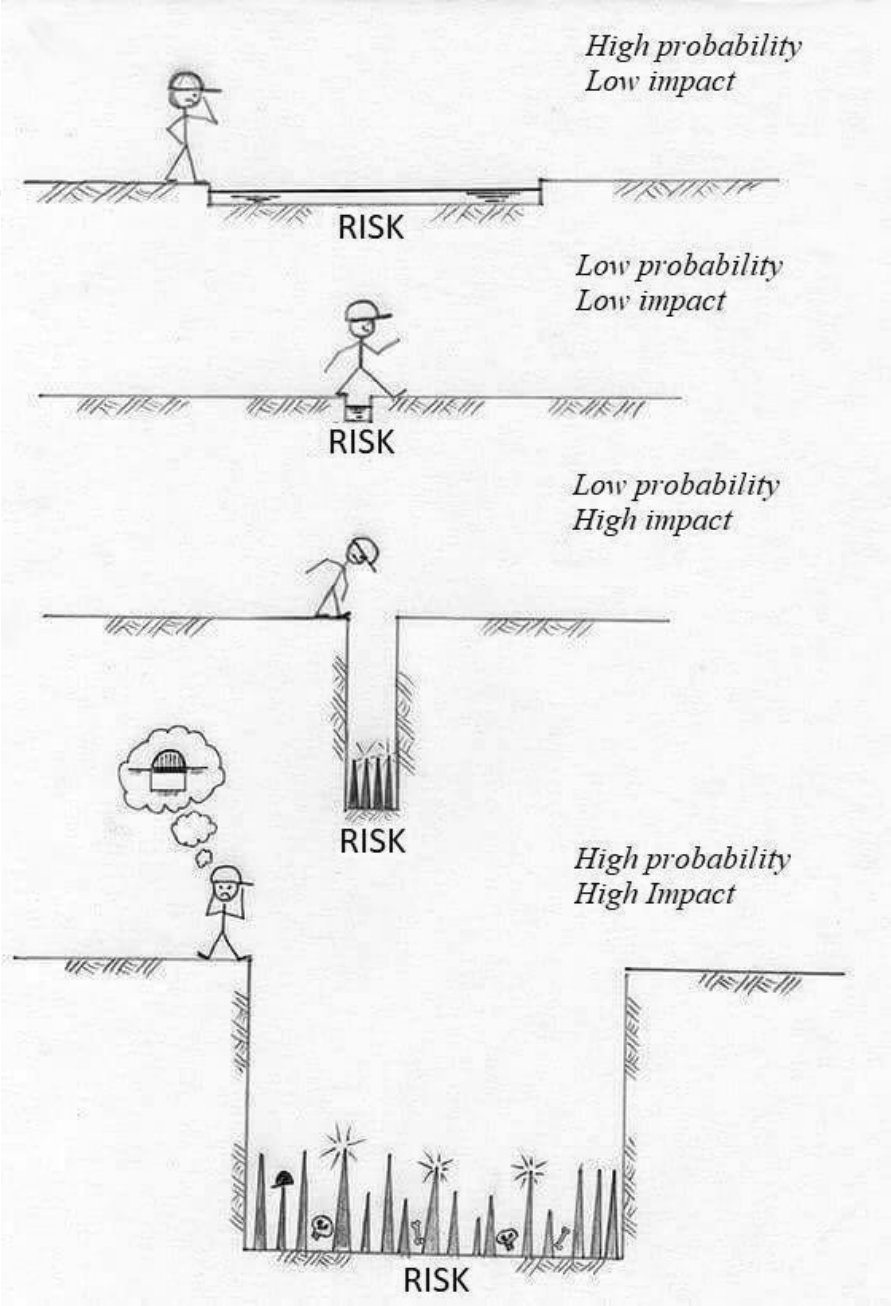
- **Risk** – the potential for loss or damage to an asset caused by a threat exploiting a vulnerability
- Sometimes shown as:
  Risk = Threat x Vulnerability
- Or a more detailed view is:
  Risk = Asset (or Impact) x Threat x Vulnerability

InfoSec Definitions

- **Risk Matrix** – used when performing risk assessments to define a level of risk
  - Commonly used in real-world risk

CONSEQUENCE			
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium
	Low	Medium	High

LIKELIHOOD



InfoSec Definitions

- **Risk Matrix** – used when performing risk assessments to define a level of risk
  - Commonly used in real-world risk

CONSEQUENCE	Low	Medium	High
High	**Medium**	**High**	**High**
Medium	**Low**	**Medium**	**High**
Low	**Low**	**Low**	**Medium**

LIKELIHOOD

- Discuss: What are some recent vulnerabilities?
  How does that fit into the simple risk matrix?
- Remember: Risk = Asset (or Impact) x Threat x Vulnerability

InfoSec Definitions

- **CVSS** – Common Vulnerability Scoring System
  - A system to translate the characteristics and impacts of a vulnerability into a numerical score
  - Interactive calculator is at https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
- The Apache Struts vulnerability in 2017 scored a perfect 10

CVSS Severity (version 3.0):

CVSS v3 Base Score: 10.0 Critical
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Impact Score: 6.0
Exploitability Score: 3.9

CVSS Version 3 Metrics:

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

InfoSec Definitions

- **Mitigate** – to reduce the seriousness or severity
  - This is done by applying **security controls**
  - Controls can be classified by their time of impact:
    - Preventative
    - Detective
    - Corrective
  - or by the type of control:
    - Legal and regulatory compliance
    - Physical
    - Procedural / Administrative
    - Technical

InfoSec Definitions

- **Defence In Depth** – the layering of security controls to provide redundancy in case of a failure or vulnerability
  - These commonly layer controls at different times and types (see prev)
  - Sometimes referred to as a Castle Approach

For more castle defences, see http://tvblogs.nationalgeographic.com/files/2013/08/Castle-Traps-and-Defenses.jpg

Pictured to the left is Caerphilly Castle https://commons.wikimedia.org/wiki/File:Caerphilly_aerial.jpg

InfoSec Definitions

- **Defence In Depth**
- Discuss: Imagine you had a bar of gold to protect
  - What container would you put it in?
  - What room would the container be in?
  - What locks are on the doors?
  - Where is the room located in the building?
  - What cameras are watching the room and building?
  - What humans are watching the cameras?
  - Who will respond with force to a theft attempt?
  - Bonus question: How much did all of this cost?

InfoSec Definitions

- **Threat actor** – a person trying to cause harm to your system or network
  - Commonly called an attacker or hacker, although the definition of a hacker has changed over many years
  - Also known as **malicious actor**
  - Can be further broken down into categories such as:
    - Opportunistic
    - Hacktivists
    - Cybercriminals (organized or not)
    - Nation States / Government Sponsored
    - Insiders (intentional or accidental)

CSIRT/CERT Introduction

CSIRT / CERT

- CSIRT - Computer Security Incident Response Team
  CERT - Computer Emergency Response Teams
- A CSIRT performs, coordinates, and supports the response to security incidents that involve sites within a defined constituency
- Must react to reported security incidents or threat
- In ways which the specific community agrees to be in its general interest
- T = Team = Entity (Unit/Organization) that does IR work!

Constituency

- A CSIRT serves its constituent
- Constituency help define:
  - The purpose & nature of the CSIRT
  - Who is the CSIRT Serving
  - Types of incidents the CSIRT handles
  - The relationship with other CSIRTs

- Example of Constituents:
  - Enterprise / Single Organization
  - Sector Based
  - Critical Infrastructure
  - Product
  - National / Country
  - Customer
- Constituents might overlap
  - Co-ordination is key
  - CSIRT of the “Last Resort”

Different Types of CSIRTs

- **Enterprise CSIRTs**
  - provide incident handling services to their parent organization. This could be a CSIRT for a bank, a manufacturing company, an ISP, a university, or a federal agency.
- **National CSIRTs**
  - provide incident handling services to a country.
- **Coordination Centers**
  - coordinate and facilitate the handling of incidents across various CSIRTs. Examples include the CERT Coordination Center or the United States Computer Emergency Readiness Team (US-CERT).
- **Analysis Centers**
  - focus on synthesizing data from various sources to determine trends and patterns in incident activity. This information can be used to help predict future activity or to provide early warning when the activity matches a set of previously determined characteristics.
- **Vendor Teams**
  - handle reports of vulnerabilities in their software or hardware products. They may work within the organization to determine if their products are vulnerable and to develop remediation and mitigation strategies. A vendor team may also be the internal CSIRT for a vendor organization.
- **Incident Response Providers**
  - offer incident handling services as a for-fee service to other organizations.

(Source: US-CERT https://www.cert.org/incident-management/csirt-development/csirt-faq.cfm)

Why a CSIRT?

- Security Incidents Happen!
  - Execute incident response plans
  - Assurance to customers and stakeholders
  - Best Practice
- Mitigate Loss or Damage
  - Point of Contact
  - Governance
- Compliance to Standards
  - Cyber Security Framework
  - ISO 27001, ITIL
  - Compliance with Law or Regulations
- Security Improvements
  - Analyze Incidents and Provide Lessons Learned
- Resource Allocation
  - Dedicated Service(s)
  - Human Resources, Skills
  - Specific Polices and SOPs
  - Point of Contact

Whois Database: Incident Response Team Object

```
inetnum:        1.1.1.0 - 1.1.1.255
netname:        APNIC-LABS
descr:          Research prefix for APNIC Labs
descr:          APNIC
country:        AU
admin-c:        AR302-AP
tech-c:         AR302-AP
mnt-by:         APNIC-HM
mnt-routes:     MAINT-AU-APNIC-GM85-AP
mnt-irt:        IRT-APNICRANDNET-AU
status:         ASSIGNED PORTABLE
changed:        hm-changed@apnic.net 20140507
changed:        hm-changed@apnic.net 20140512
source:         APNIC

irt:            IRT-APNICRANDNET-AU
address:        PO Box 3646
address:        South Brisbane, QLD 4101
address:        Australia
e-mail:         abuse@apnic.net
abuse-mailbox:  abuse@apnic.net
admin-c:        AR302-AP
tech-c:         AR302-AP
auth:           # Filtered
mnt-by:         MAINT-AU-APNIC-GM85-AP
changed:        hm-changed@apnic.net 20110922
source:         APNIC
```

Infrastructure Security Fundamentals

Device Access Control (Physical)

- Lock up the server room. Equipment kept in highly restrictive environments
- Set up surveillance
- Make sure the most vulnerable devices are in that locked room
- Keep intruders from opening the case
- Protect the portables
- Pack up the backups
- Disable the drives
- Social engineering training and awareness
- Console access
  - password protected
  - access via OOB (Out-of-band) management
  - configure timeouts

Fundamental Device Protection (Logical)

- Secure logical access to routers with passwords and timeouts
- Never leave passwords in clear-text
- Authenticate individual users
- Restrict logical access to specified trusted hosts
- Allow remote vty access only through SSH
- Protect SNMP if used
- Shut down unused interfaces & unneeded services
- Ensure accurate timestamps for all logging
- Create appropriate banners

Management Plane Filters

- Authenticate Access
- Define Explicit Access To/From Management Stations
  - SNMP
  - Syslog
  - TFTP
  - NTP
  - AAA Protocols
  - SSH

Secure Access with Passwords and Logout Timers

- **Secure logical access to routers with passwords and timeouts**
- Never leave passwords in clear-text
- Authenticate individual users
- Restrict logical access to specified trusted hosts
- Allow remote vty access only through SSH
- Protect SNMP if used
- Shut down unused interfaces & unneeded services
- Ensure accurate timestamps for all logging
- Create appropriate banners

```
line console 0
    login
    password console-pwd
    exec-timeout 1 30
!
line vty 0 4
    login
    password vty-pwd
    exec-timeout 5 00
!
enable secret enable-secret
username test secret test-secret
```

Radius Authentication (AAA)

```
aaa new-model
!
aaa authentication login default group radius local
aaa authorization exec default group radius local
!
radius-server host 192.168.1.250 auth-port 1812 acct-port 1813
radius-server key 7 0130310759262E000B69560F
```

Never Leave Passwords in Clear-Text

- Secure logical access to routers with passwords and timeouts
- **Never leave passwords in clear-text**
- Authenticate individual users
- Restrict logical access to spe
- Allow remote vty access onl
- Protect SNMP if used
- Shut down unused interface
- Ensure accurate timestamps
- Create appropriate banners

- ***service password-encryption*** command
- ***password*** command
  - Will encrypt all passwords on the Cisco IOS with Cisco-defined encryption type "7"
  - Use "*command* password 7 <password>" for cut/paste operations
  - Cisco proprietary encryption method
- ***secret*** command
  - Uses MD5 to produce a one-way hash
  - Cannot be decrypted
  - Use "*command* secret 5 <password>" to cut/paste another "enable secret" password

Authenticate Individual Users

- Secure logical access to routers with passwords and timeouts
- Never leave passwords in clear-text
- **Authenticate individual users**
- Restrict logical access to specified truste
- Allow remote vty access only through SS
- Protect SNMP if used
- Shut down unused interfaces & unneede
- Ensure accurate timestamps for all logging
- Create appropriate banners

```
username mike secret mike-secret
username john secret john-secret
username chris secret chris-secret
!
```

~~`username staff secret group-secret`~~

Restrict Access to Trusted Hosts

- Secure logical access to routers with passwords and timeouts
- Never leave passwords in clear-text
- Authenticate individual users
- **Restrict logical access to specified trusted hosts**
- Allow remote vty access only through SSH
- Protect SNMP if used
- Shut dov
- Ensure a
- Create a

```
access-list 103 permit tcp host 192.168.200.7 192.168.1.0 0.0.0.255 eq 22 log-input
access-list 103 permit tcp host 192.168.200.8 192.168.1.0 0.0.0.255 eq 22 log-input
access-list 103 permit tcp host 192.168.100.6 192.168.1.0 0.0.0.255 eq 23 log-input
access-list 103 deny ip any any log-input
!
line vty 0 4
access-class 103 in
transport input ssh
```

Securing SSH

- Secure logical access to routers with passwords and timeouts
- Never leave passwords in clear-text
- Authenticate individual users
- Restrict logical access to specified trusted h
- **Allow remote vty access only through SSH**
- Protect SNMP if used
- Shut down unused interfaces & unneeded s
- Ensure accurate timestamps for all logging
- Create appropriate banners

```
ipv6 access-list AUTHORIZED_IPV6_HOST
 permit ipv6 host 2001:db8:0:6::250 any
 deny ipv6 any any log
!
ip access-list extended AUTHORIZED_IPV4_HOST
 permit tcp host 192.168.75.5 any eq 22
 deny   tcp any any log
!
line vty 0 4
 access-class AUTHORIZED_IPV4_HOST in
 ipv6 access-class AUTHORIZED_IPV6_HOST in
```

Securing SNMP

- Secure logical access to routers with passwords and timeouts
- Never leave passwords in clear-text
- Authenticate individual users
- Restrict logical access to specified trusted hosts
- Allow remote vty access only
- **Protect SNMP if used**
- Shut down unused interface
- Ensure accurate timestamps for all logging
- Create appropriate banners

```
access-list 99 permit 192.168.1.250
access-list 99 permit 192.168.1.240

snmp-server community N3TW0RK-manag3m3nt ro 99
```

Turn Off Unused Services

Feature	Description	Default	Recommendation	Cisco IOS Command
CDP	Proprietary layer 2 protocol between Cisco devices	Enabled		no cdp run
TCP small servers	Standard TCP network services: echo, chargen, etc	IOS V11.3: disabled IOS V11.2: enabled	This is a legacy feature, disable it explicitly	no service tcp-small-servers
UDP small servers	Standard UDP network services: echo, discard, etc	IOS V11.3: disabled IOS V11.2: 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	Cisco IOS 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 (IOS V11.3 & 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
```

Commands on Cisco IOS

Ensure Accurate Timestamps for all Logging

- Secure logical access to routers with passwords and timeouts
- Never leave passwords in
- Authenticate individual us
- Restrict logical access to specified trusted hosts
- Allow remote vty access only thro
- Protect SNMP if used
- Shut down unused interfaces & unneeded services
- **Ensure accurate timestamps for all logging**
- Create appropriate banners

```
service timestamps log datetime localtime msec show-
timezone year
```

```
Router(config)# logging 192.168.0.30
Router(config)# logging trap 3
Router(config)# logging facility local3
```

Configuration change logging

```
Router# configure terminal
Router(config)# archive
Router(config-archive)# log config
Router(config-archive-log-config)# logging enable
Router(config-archive-log-config)# logging size 200
Router(config-archive-log-config)# hidekeys
Router(config-archive-log-config)# notify syslog
```

```
768962: Feb  1 20:59:45.081 UTC: %PARSER-5-CFGLOG_LOGGEDCMD: User:fakrul  logged
command:!exec: enable
768963: Feb  1 21:03:17.160 UTC: %PARSER-5-CFGLOG_LOGGEDCMD: User:fakrul  logged
command:no ipv6 prefix-list dhakacom_AS23956_IN_IPv6 description
768965: Feb  1 21:03:19.182 UTC: %SYS-5-CONFIG_I: Configured from console by fakrul on vty0
(2001:db8:0:6::250)
```

Create Appropriate Banner

- Secure logical access to routers with passwords and timeouts
- Never leave passwords in clear-text
- Authenticate individual users
- Restrict logical access to specified trusted hosts
- Allow remote vty acce
- Protect SNMP if used
- Shut down unused int
- Ensure accurate timestamps for all logging
- **Create appropriate banners**

```
!!!!  WARNING !!!!

You have accessed a restricted device.

All access is being logged and any unauthorized access will
be prosecuted to the full extent of the law.
```

Data Plane (Packet) Filters

- Most common problems
  - Poorly-constructed filters
  - Ordering matters in some devices
- Scaling and maintainability issues with filters are commonplace
- Make your filters as modular and simple as possible
- Take into consideration alternate routes
  - Backdoor paths due to network failures

Filtering Deployment Considerations

- How does the filter load into the router?
- Does it interrupt packet flow?
- How many filters can be supported in hardware?
- How many filters can be supported in software?
- How does filter depth impact performance?
- How do multiple concurrent features affect performance?
- Do I need a standalone firewall?

Filtering Recommendations

- Log filter port messages properly
- Allow only internal addresses to enter the router from the internal interface
- Block packets from outside (untrusted) that are obviously fake or commonly used for attacks
- Block packets that claim to have a source address of any internal (trusted) network.

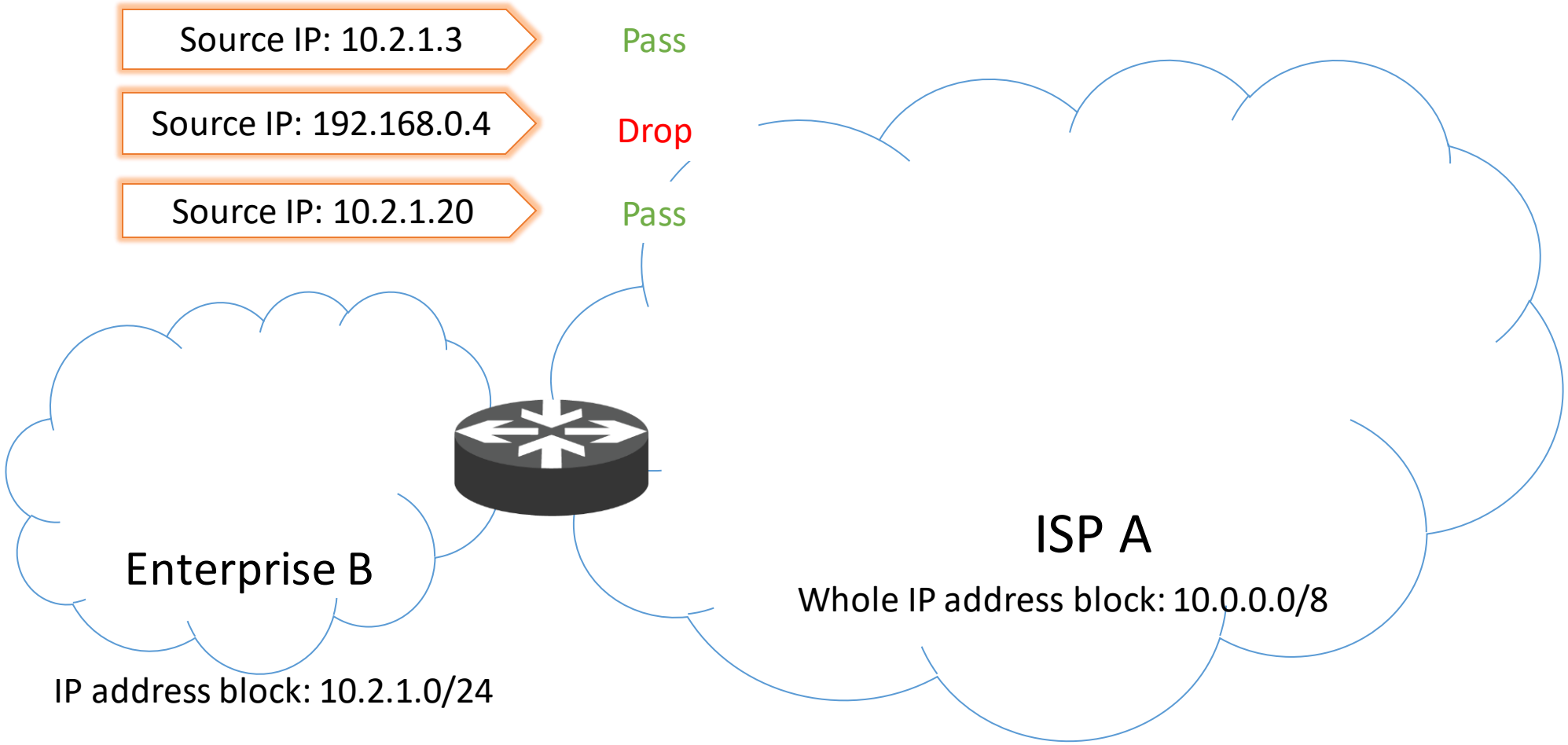
Filtering Recommendations

- Block incoming loopback packets and RFC 1918 networks
  - 127.0.0.0
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.0.0
  - 192.168.0.0 – 192.168.255.255
- Block multicast packets (if NOT using multicast)
- Block broadcast packets (careful of DHCP & BOOTP users)
- Block incoming packets that claim to have same destination and source address

RFC2827 (BCP38) – Ingress Filtering

- If an ISP is aggregating routing announcements for multiple downstream networks, strict traffic filtering should be used to prohibit traffic which claims to have originated from outside of these aggregated announcements.
- The ONLY valid source IP address for packets originating from a customer network is the one assigned by the ISP (whether statically or dynamically assigned).
- An edge router could check every packet on ingress to ensure the user is not spoofing the source address on the packets which he is originating.

BCP38


Source IP: 10.2.1.3
Pass
Source IP: 192.168.0.4
Drop
Source IP: 10.2.1.20
Pass
Enterprise B
IP address block: 10.2.1.0/24
ISP A
Whole IP address block: 10.0.0.0/8

Techniques for BCP38

- Static ACLs on the edge of the network
- Unicast RPF strict mode
- IP source guard

Example of Inbound Packet Filter

```
access-list 121 permit ip 192.168.1.250 0.0.0.255 any
access-list 121 deny ip any any log
!
interface serial 1/1/1.3
    Description Link to XYZ
    ip access-group 121 in
```

Infrastructure Filters Summary

- Permit only required protocols and deny ALL others to infrastructure space
  - Filters now need to be IPv4 and IPv6!
  - Applied inbound on ingress interfaces
- Basic premise: filter traffic destined TO your core routers
- Develop list of required protocols that are sourced from outside your AS and access core routers
  - Example: eBGP peering, GRE, IPsec, etc.
  - Use classification filters as required
- Identify core address block(s)
  - This is the protected address space
  - Summarization is critical for simpler and shorter filters

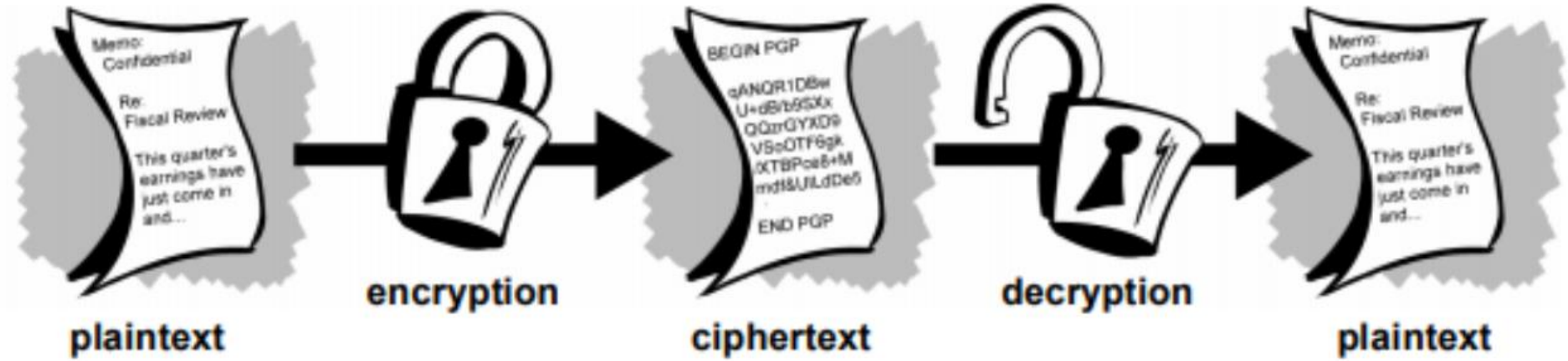
General Filtering Best Practices

- Explicitly deny all traffic and only allow what you need
- The default policy should be that if the firewall doesn't know what to do with the packet, deny/drop it
- Don't rely only on your firewall for all protection of your network
- Implement multiple layers of network protection
- Make sure all of the network traffic passes through the firewall
- Log all firewall exceptions (if possible)

Cryptography

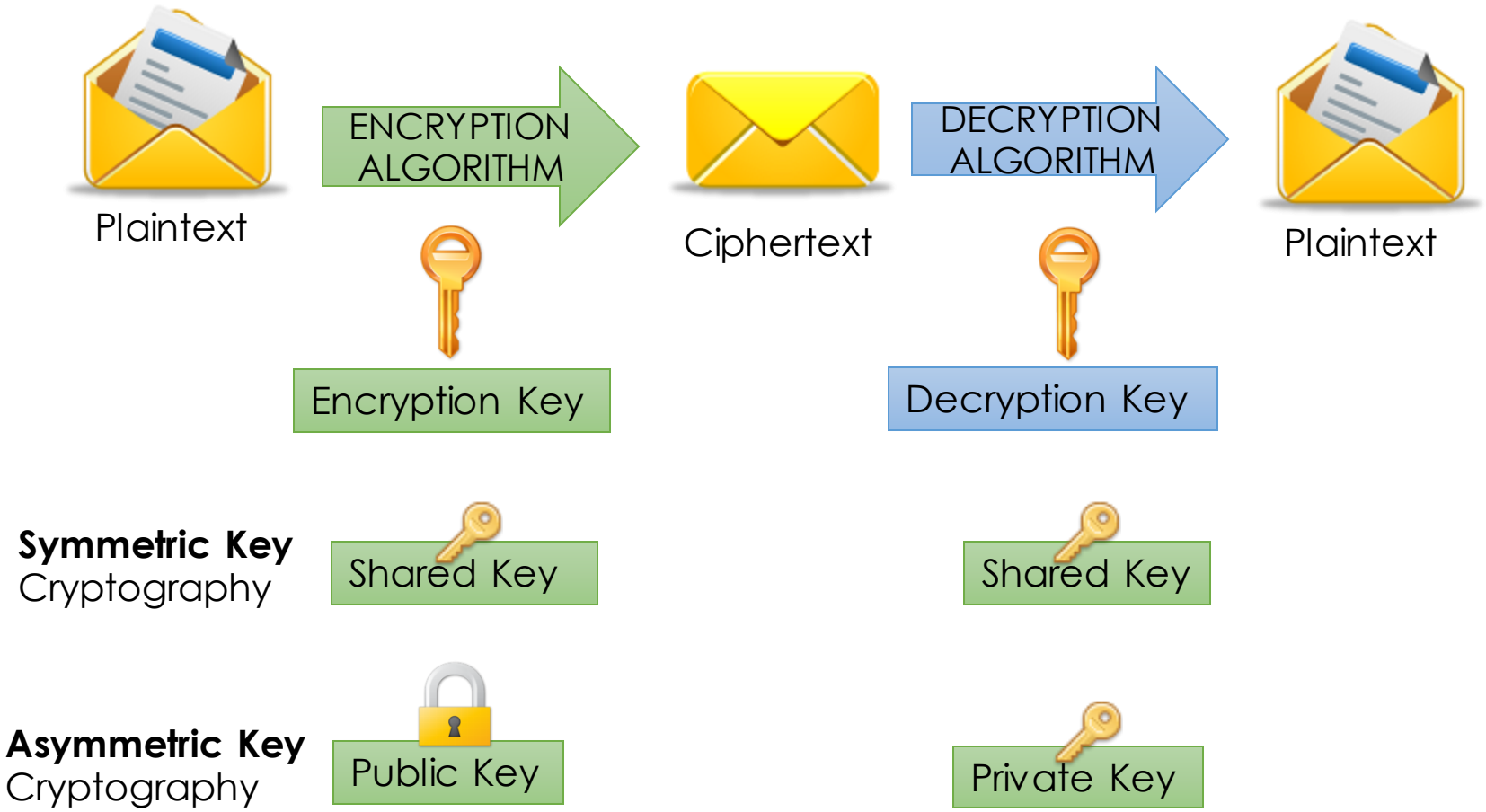
Cryptography

- Terminology



- Cryptography
  - From Greek, “crypto” meaning hidden or secret, “graphy” meaning writing
- Cryptanalysis
  - From Greek, “crypto” meaning hidden or secret, “analysis” meaning to loosen or untie

Cryptography

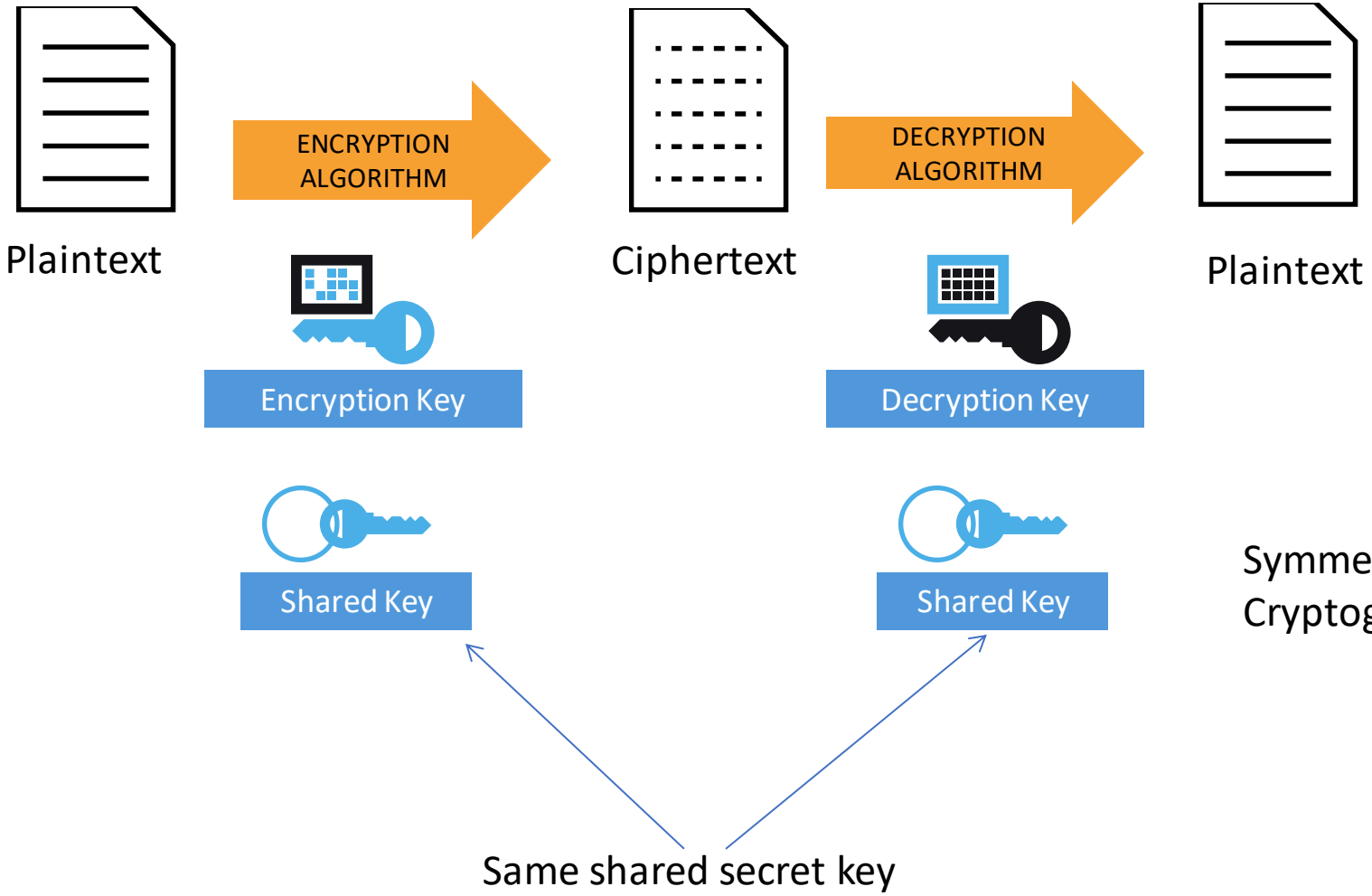


Symmetric Key Algorithm

- Uses a single key to both encrypt and decrypt information
- Also known as a secret-key algorithm
  - The key must be kept a “secret” to maintain security
  - This key is also known as a private key

- Examples:
  - DES, 3DES, AES, RC4, RC6, Blowfish

Symmetric Key Algorithm



Symmetric Key Cryptography

Asymmetric Key Algorithm

- Also called public-key cryptography
  - Keep private key private
  - Anyone can see public key
- Separate keys for encryption and decryption (public and private key pairs)
- Examples:
  - RSA, DSA, Diffie-Hellman, ElGamal, PKCS

How Public Key Cryptography works

Alice and Bob, they are using Public Key pairs to communicate. What are the keys do they have?

Alice knows following keys
Alice's Public Key
Alice's Private Key
Bob's Public Key

Alice's Public Key
Alice's Private Key
Bob's Public Key
Bob's Private Key

Bob knows following keys
Bob's Public Key
Bob's Private Key
Alice's Public Key

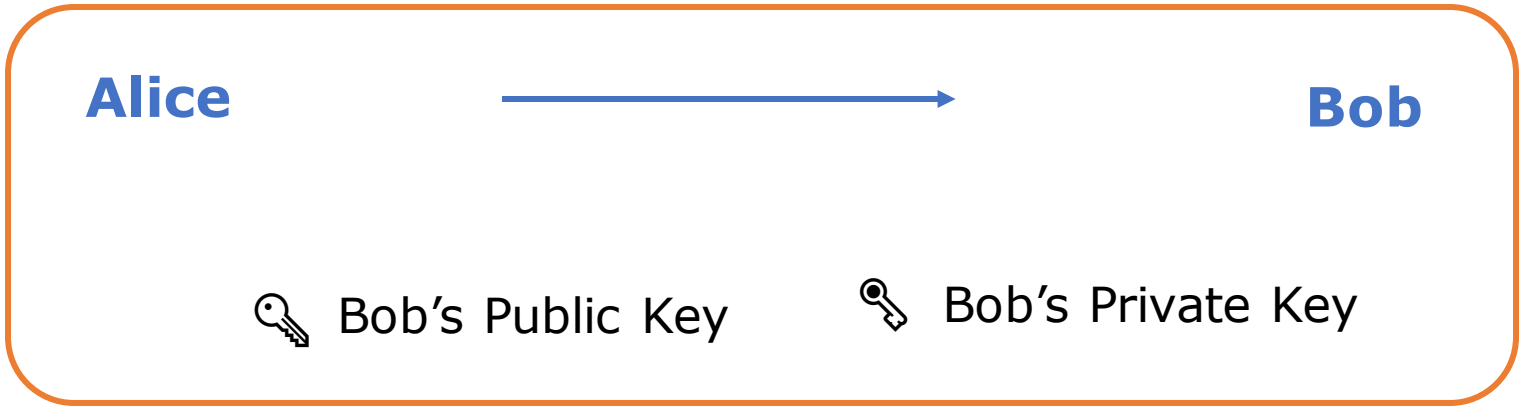
How to Use Public Key Cryptography

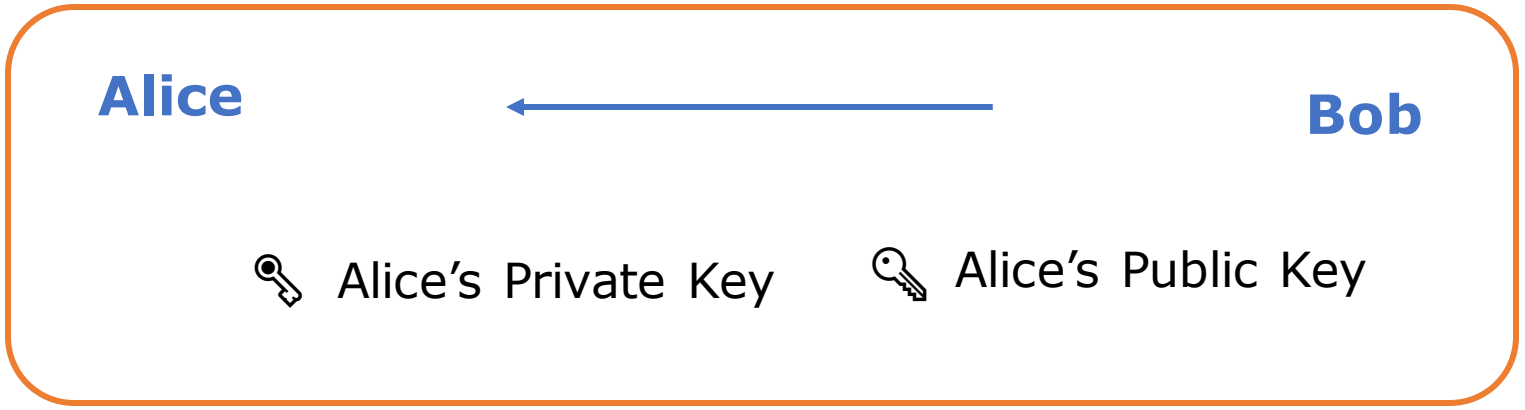
Alice and Bob, they are using Public Key pairs to communicate.

Alice has a message

If encrypted by	Using which key can decrypt it?	Who can decrypt it?	Function
1 Alice's Public Key	Alice's Private Key	Alice	Alice can encrypt the file only for herself.
2 Alice's Private Key	Alice's Public Key	Everyone	Only from Alice (Sign) Integrity
3 Bob's Public Key	Bob's Private Key	Bob	Confidentiality

Communication between Alice and Bob for Encryption



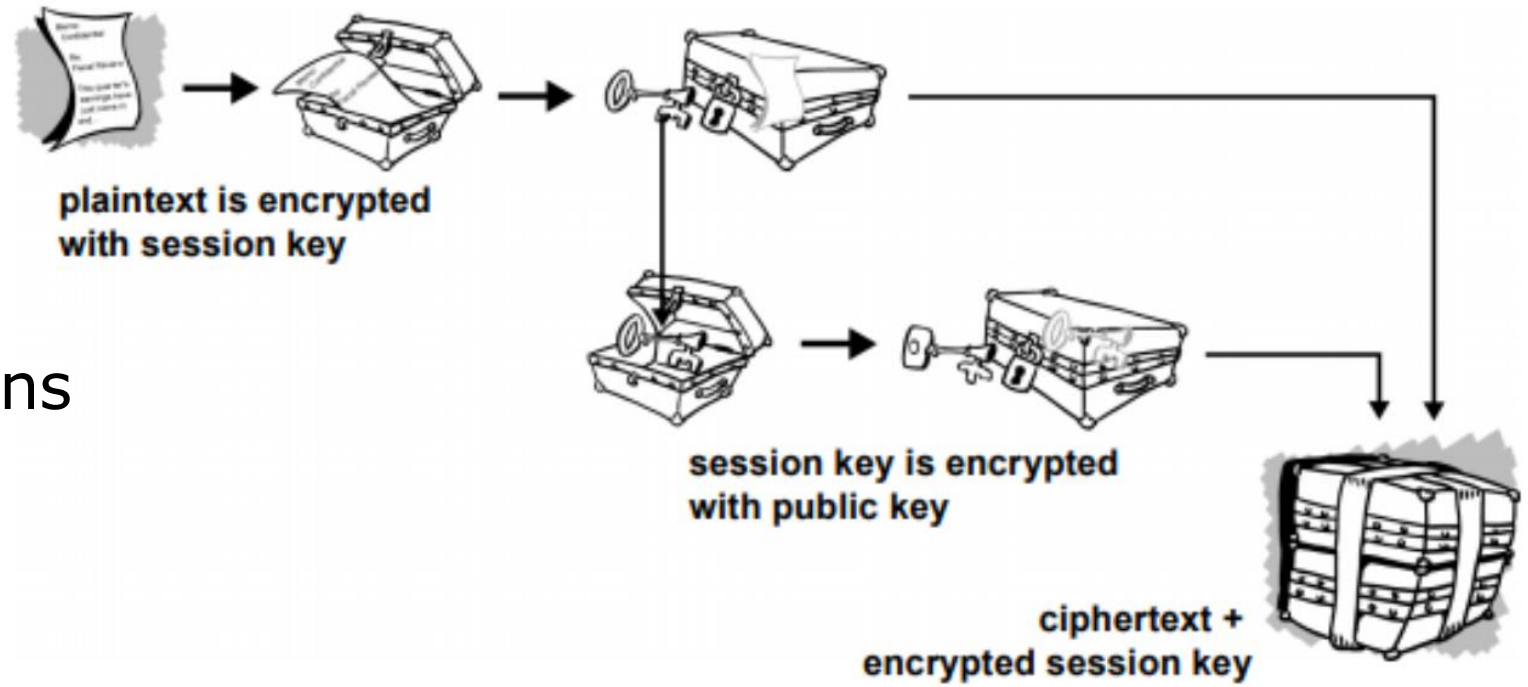


Use Case

- email
  - encrypting: to send confidential information
  - signing: to prove the message actually comes from you and is not modified during delivery
- File distribution
  - signing: to prove the contents is distributed by you and not modified since signed
  - you can generate separate signature file if needed
    - you have the original file and signature file for it

Cryptography

- Asymmetric algorithms are slower and secure, so most implementations use a combination of both to ensure it is both fast and secure



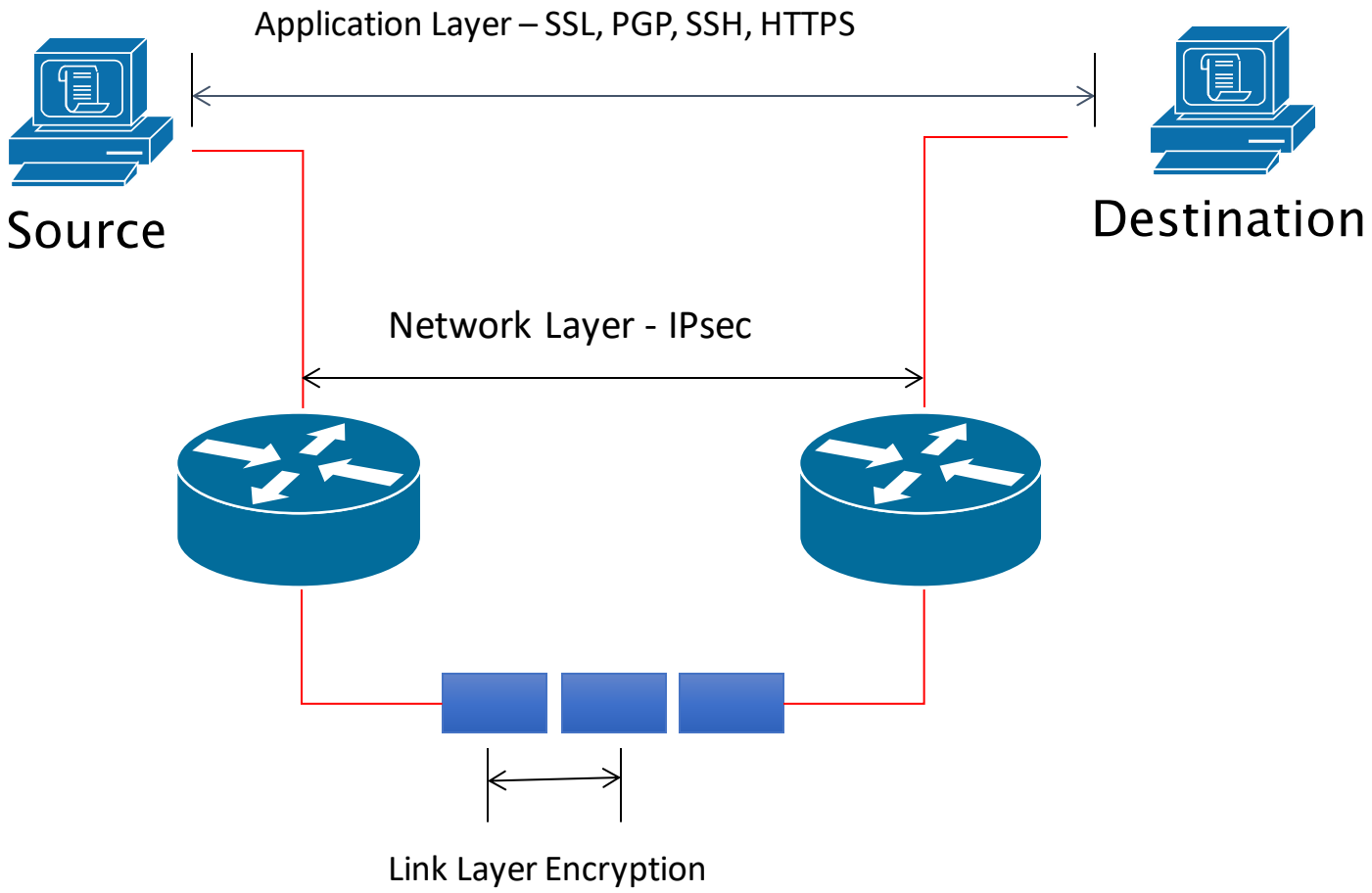
- Common implementations
  - SSL
  - PGP / GPG

VPN and 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
- VPN Protocols
  - PPTP (Point-to-Point tunneling Protocol)
  - L2TP (Layer 2 Tunneling Protocol)
  - IPsec (Internet Protocol Security)
  - TLS (Transport Layer Security)

Different Layers of Encryption



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)
  - Internet Key Exchange (IKE)
  - Authentication headers (AH)
  - Encapsulating security payload (ESP)
- A security context for the VPN tunnel is established via the ISAKMP (Internet Security Association Key Management Protocol)

Benefits of IPsec

- Confidentiality
  - By encrypting data

- 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

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

Benefits of IPsec

- Anti-replay protection
  - Optional; the sender must provide it but the recipient may ignore
- Authentication
  - Signatures and certificates
  - All these while still maintaining the ability to route through existing IP networks
- 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

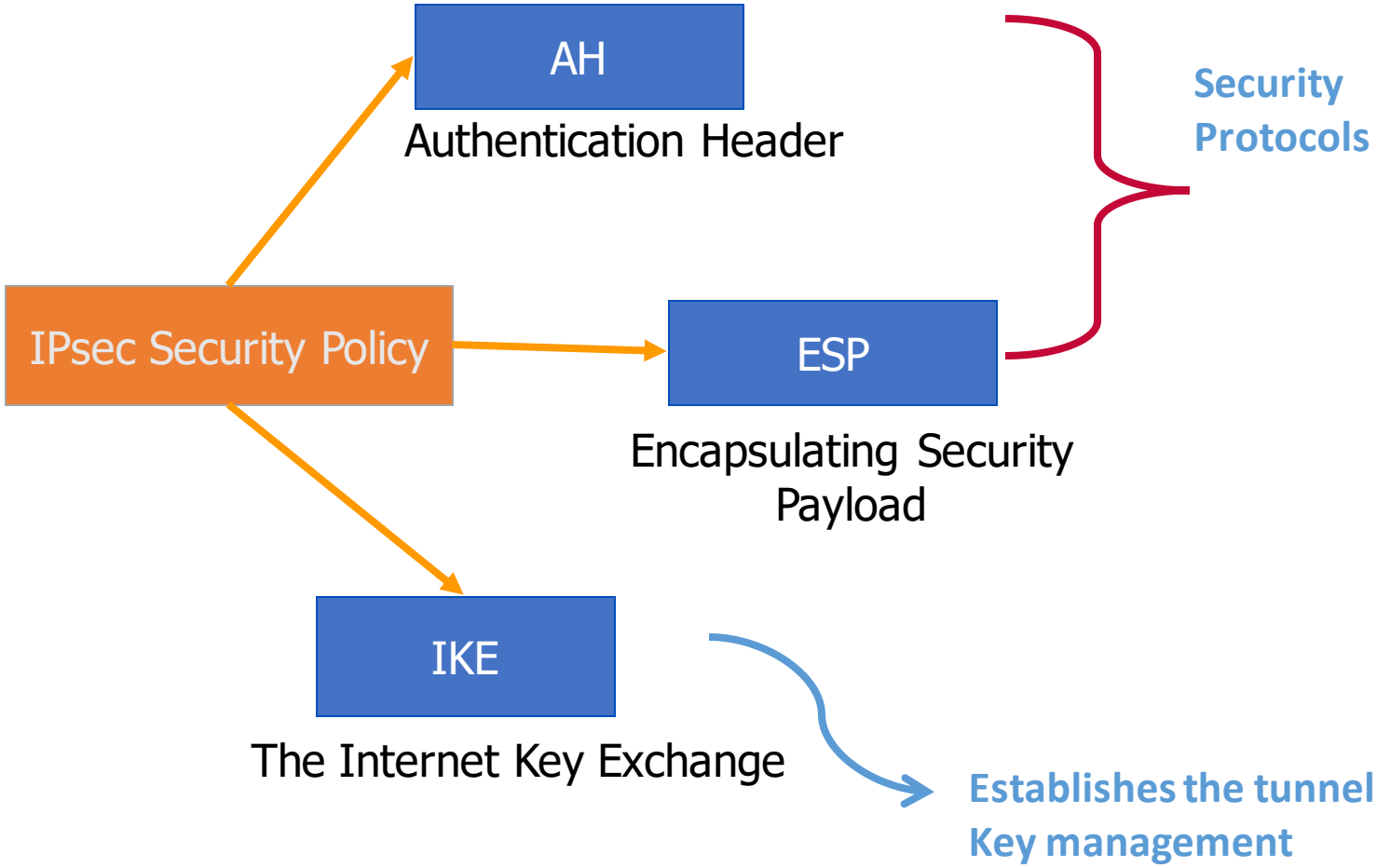
Authentication Header (AH)

- 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

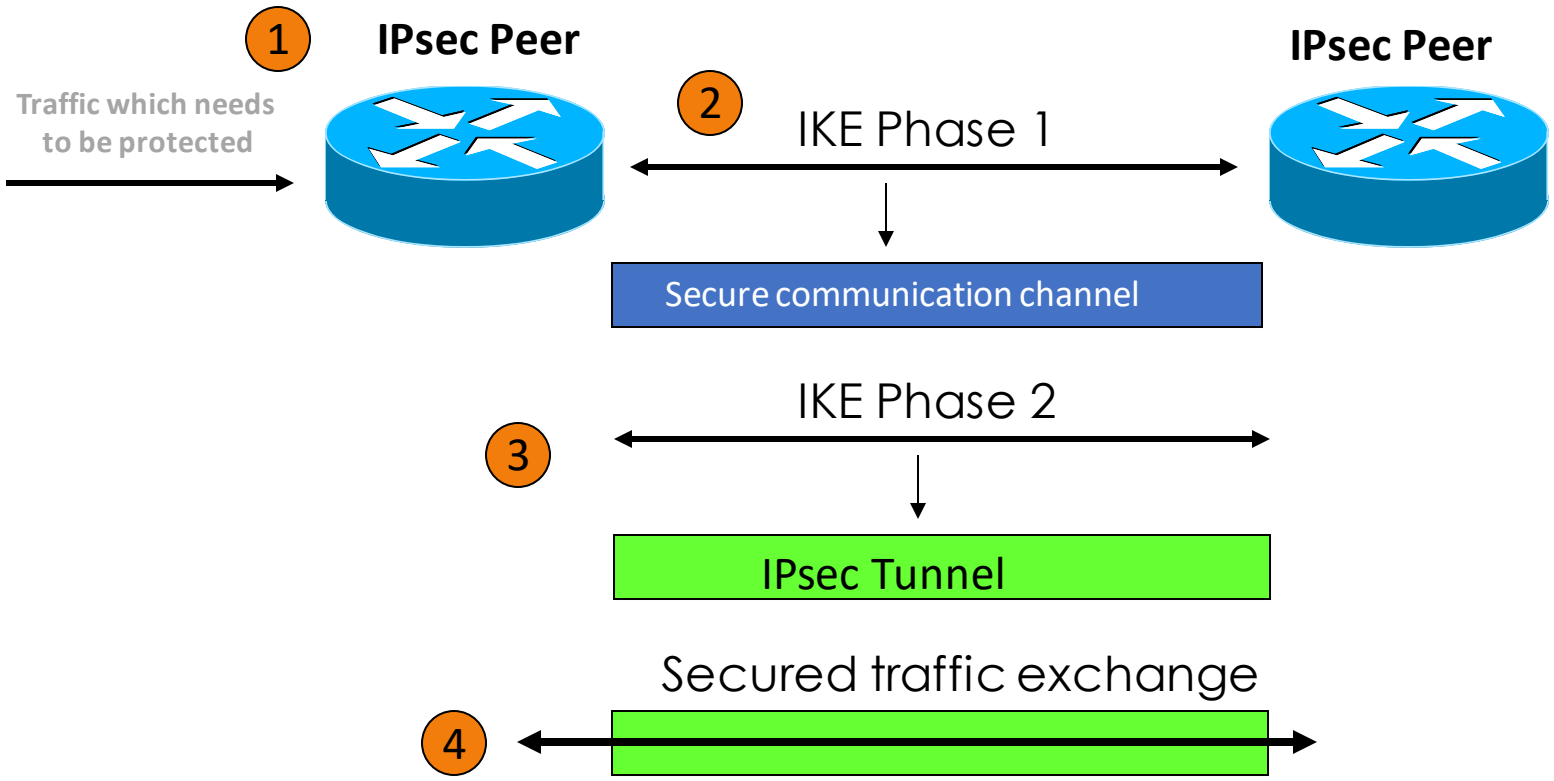
Encapsulating Security Payload (ESP)

- 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

IPsec Architecture



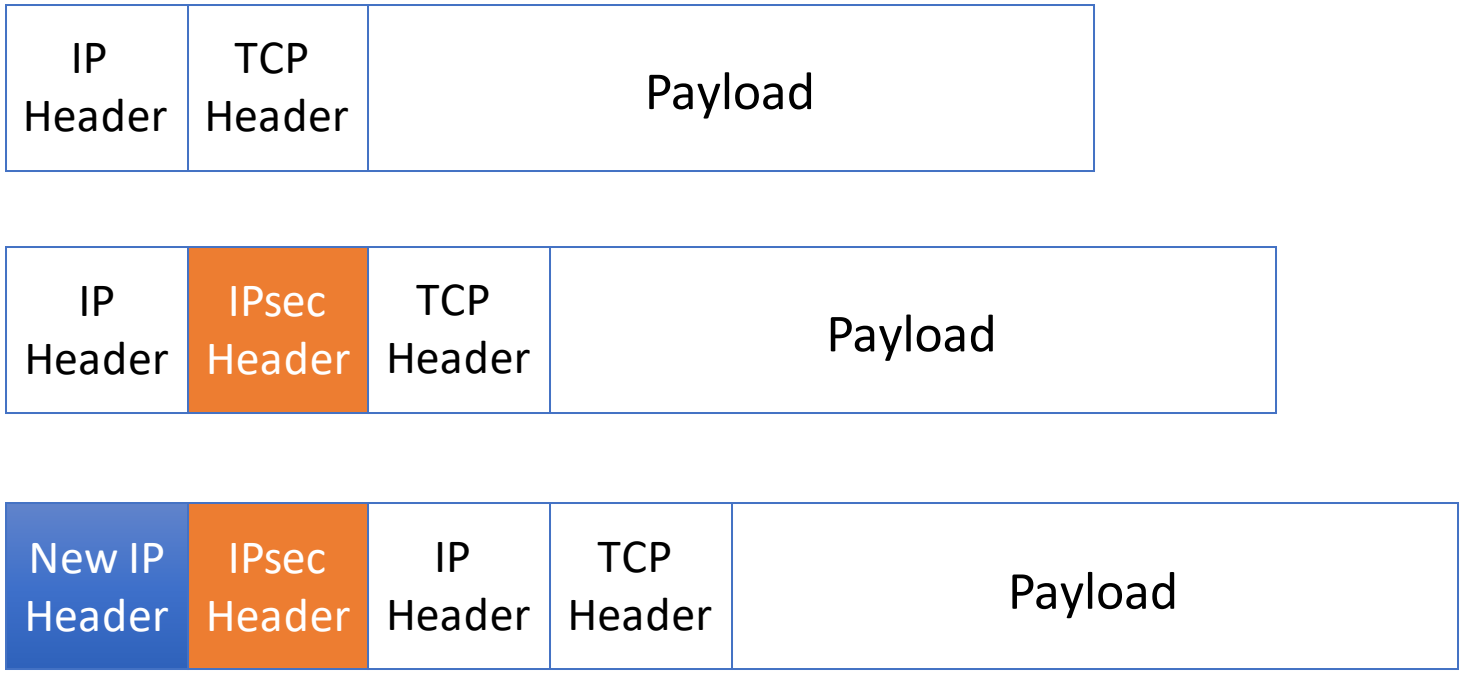
Working Process of IPsec



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



Without IPsec

Transport Mode IPsec

Tunnel Mode IPsec

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				K] Seq=7 Ack=6 Wi
27	4.243593				
28	4.245501				
29	4.245503				K] Seq=8 Ack=7 Wi

Follow TCP Stream

Stream Content

```
..... .....!.......................P....

User Access Verification

Password: .. ..!..!........ apn.......apnic2

router2>

router2>

router2>

router2>eenn

% No password set
router2>

router2>

router2>

router2>

router2>

router2>

router2>

router2>

router2>

router2>sshh  iipp  ??
```

```
router2>sshh  iipp  ??
  accounting            The active IP accounting database
  admission             Network Admission Control information
  aliases               IP alias table
  arp                   IP ARP table
  as-path-access-list   List AS path access lists
  auth-proxy            Authentication Proxy information
  bgp                   BGP information
  cache                 IP fast-switching route cache
  casa                  display casa information
  cef                   Cisco Express Forwarding
  ddns                  Dynamic DNS
  dfp                   DFP information
  dhcp                  Show items in the DHCP database
  dvmrp                 DVMRP information
  eigrp                 IP-EIGRP show commands
  extcommunity-list     List extended-community list
  flow                  NetFlow switching
  helper-address        helper-address table
  host-list             Host list
  http                  HTTP information
  igmp                  IGMP information
  inspect               CBAC (Context Based Access Control) information
 --More-- .........        .........
router2>sh ip .. ... ... .iipp  iinntt.
router2>sh ip interface ??
  Async                 Async interface
  BVI                   Bridge-Group Virtual Interface
  CDMA-Ix               CDMA Ix interface
  CTunnel               CTunnel interface
  Dialer                Dialer interface
```

Capture: Telnet + IPsec

178	67.482685	2001:db0:aa::8	fe02::1:ff00:2	ICMPv6	86 Neighbor Solicitation for 2001:
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)
200	67.770963	192.168.1.1	192.168.1.2	ESP	134 ESP (SPI=0x7ea7f8ed)

IPsec Best Practices

- Use IPsec to provide integrity in addition to encryption.
  - Use ESP option
- Use strong encryption algorithms
  - 3DES and AES instead of DES
- Use a good hashing algorithm
  - SHA instead of MD5

DoS and DDos

What is DoS and DDoS?

- In general, a denial of service is an attack against availability of a service
  - A service can be a network, or a specific service such as a web site
- DoS - Denial of Service
  - Usually from only one source
- DDoS - Distributed Denial of Service
  - Attack originates from multiple sources
  - This is caused through resource exhaustion

Impacts of a DDoS

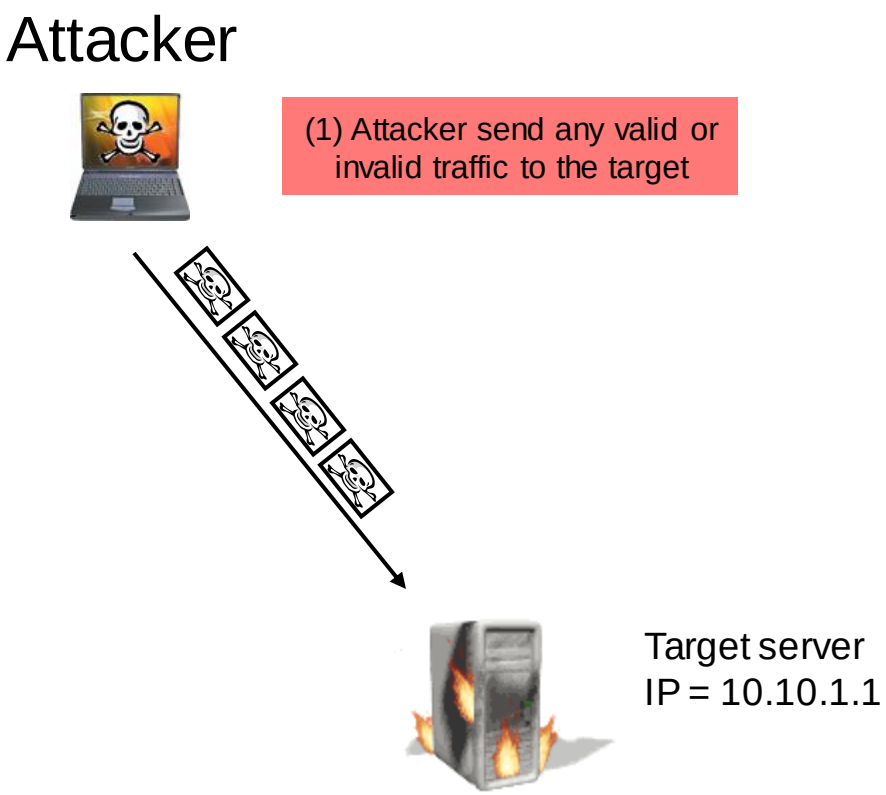
- Users sees DDoS as an outage
- Security team sees DDoS as a loss of availability
  - Think back to CIA triad
- Business management, sees DDoS as impacting the business financially
  - Especially if the business makes money using the Internet
    - ISP, credit card gateway, online casino

DoS by Layers

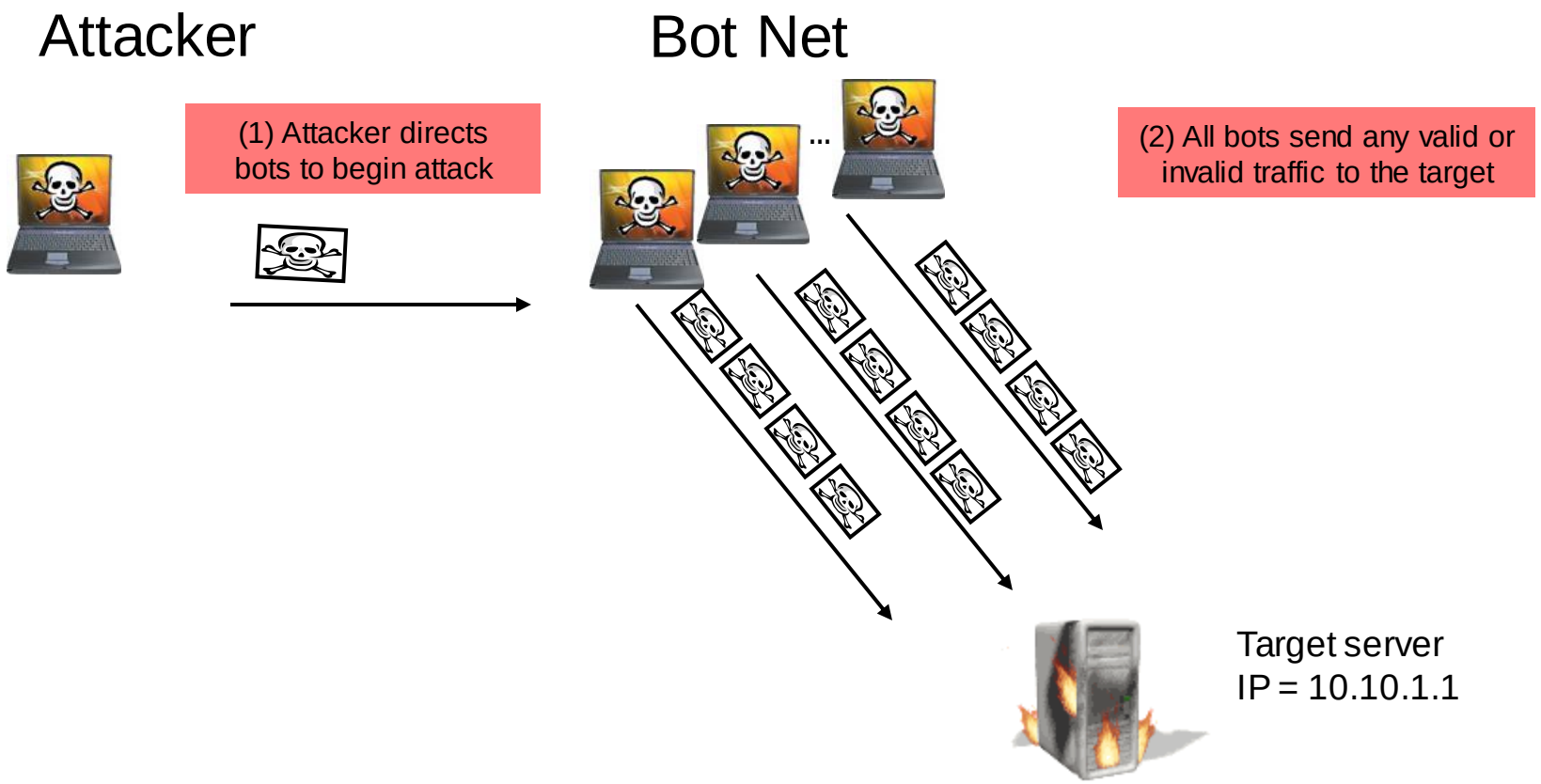
OSI Model	TCP/IP Model	Protocols and Services	Attacks
Application	Application	HTTP, FTP, DHCP, NTP, TFTP, DNS	Reflection and Amplification (DNS, NTP, etc), Slowloris, Complex DB Queries
Presentation			
Session			
Transport	Transport	TCP, UDP	SYN Flood
Network	Internet	IP, ICMP, RIP	ICMP Flood
Data Link	Network Access	WiFi, Ethernet, Fiber, Copper	Electrical Interference Construction Equipment
Physical			

* Colour animated slide

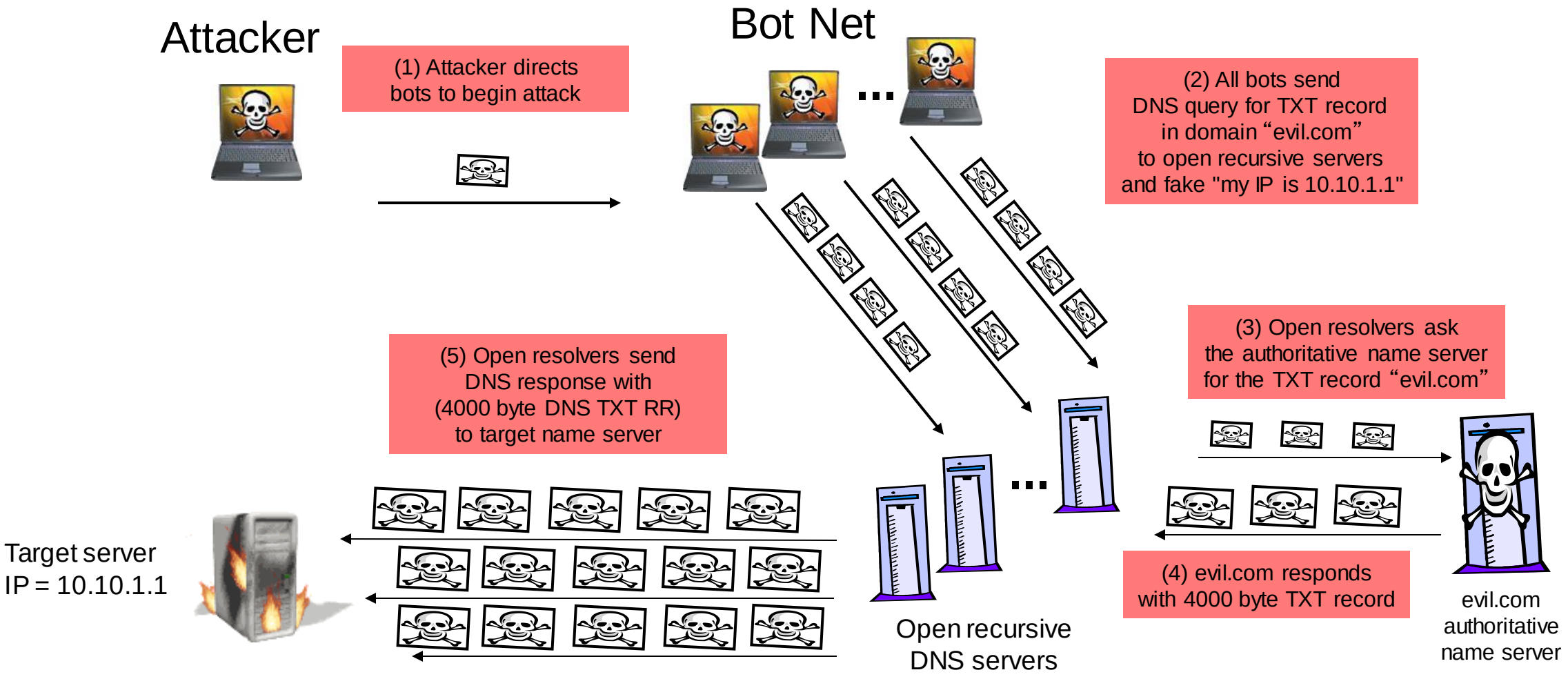
Anatomy of a Plain DoS Attack



Anatomy of a Plain DDoS Attack



Anatomy of a Reflected Amplification Attack



Reflection and Amplification

- What makes for good reflection?
  - UDP
    - Spoofable / forged source IP addresses
    - Connectionless (no 3-way handshake)
- What makes for good amplification?
  - Small command results in a larger reply
    - This creates a Bandwidth Amplification Factor (BAF)
    - Reply Length / Request Length = BAF
      - Example: 3223 bytes / 64 bytes = BAF of 50.4
    - Chart on next slide created with data from https://www.us-cert.gov/ncas/alerts/TA14-017A

Amplification Factors

Protocol	Bandwidth Amplification Factor
Multicast DNS (mDNS)	2-10
BitTorrent	3.8
NetBIOS	3.8
Steam Protocol	5.5
SNMPv2	6.3
Portmap (RPCbind)	7 to 28
DNS	28 to 54
SSDP	30.8

Protocol	Bandwidth Amplification Factor
LDAP	46 to 55
TFTP	60
Quake Network Protocol	63.9
RIPv1	131.24
QOTD	140.3
CHARGEN	358.8
NTP	556.9
Memcached	10,000 to 51,000

DNS Amplification Example

Protocol	Length	Info
DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
DNS	372	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR google-public-dns…
DNS	73	Standard query 0x0002 ANY microsoft.com
DNS	539	Standard query response 0x0002 ANY microsoft.com TXT TXT TXT TXT TXT TXT

```
> dig ANY microsoft.com @8.8.8.8
microsoft.com.   21599      IN    NS    ns1.msft.net.
microsoft.com.   3599 IN    SOA ns1.msft.net. msnhst.microsoft.com. 2018052001  7200 600 2419200 3600
microsoft.com.   3599 IN    MX    10 microsoft-com.mail.protection.outlook.com.
microsoft.com.   3599 IN    TXT  "facebook-domain-verification=bcas5uzlvu0s3mrw139a00os3o66wr"
microsoft.com.   3599 IN    TXT  "adobe-sign-verification=c1fea9b4cdd4df0d5778517f29e0934"
microsoft.com.   3599 IN    TXT  "facebook-domain-verification=gx5s19fp3o8aczby6a22clfhzm03as"
microsoft.com.   3599 IN    TXT  "v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com
                                 include:_spf-ssg-a.microsoft.com include:spf-a.hotmail.com ip4:147.243.128.24 ip4:147.243.128.26
                                 ip4:147.243.1.153 ip4:147.243.1.47 ip4:147.243.1.48 -all"
microsoft.com.   3599 IN    TXT  "FbUF6DbkE+Aw1/wi9xgDi8KVrIIZus5v8L6tbIQZkGrQ/rVQKJi8CjQbBtWtE64ey4NJJwj5J65PIggVY
                                 NabdQ=="
```

Mitigation Strategies

- Protect your services from attack
  - Anycast
  - IPS / DDoS protection
  - Overall network architecture
- Protect your services from attacking others
  - Rate-limiting
  - BCP38 (outbound filtering) source address validation
  - Securely configured DNS, NTP and SNMP servers
  - No open resolvers!
    Only allow owned or authorised IP addresses to connect

Any questions?

Please remember to fill out the feedback form
https://www.surveymonkey.com/r/apnic-20190305-AF-webinar

Video will be shared after the session.

Acknowledgements

- Jamie Gillespie (APNIC Senior Security Specialist)
- Adli Wahid (APNIC Senior Security Specialist)

APNIC Helpdesk Chat

Helpdesk

APNIC Helpdesk provides assistance to all on matters related to APNIC Services, such as membership and IP address enquiries.

APNIC Helpdesk offers (through prior arrangement) multi-language phone support for the following: Bahasa Indonesia, Bahasa Malaysia, Burmese, Cantonese, English, Filipino (Tagalog), Hindi, Japanese, Mandarin, Sinhalese, Tamil and Telugu.

You may also find our FAQs helpful with your enquiries.

Contact details

Helpdesk hours	09:00 to 21:00 (UTC +10) Monday – Friday (closed for some public holidays)
Chat	APNIC Live Chat Online Click here to chat
Skype	Call ID: apnic-helpdesk
Email	helpdesk@apnic.net
Phone	+61 7 3858 3188
VoIP	helpdesk@voip.apnic.net Using VoIP
Fax	+ 61 7 3858 3199

Service Updates

Upgrade edge router firmware

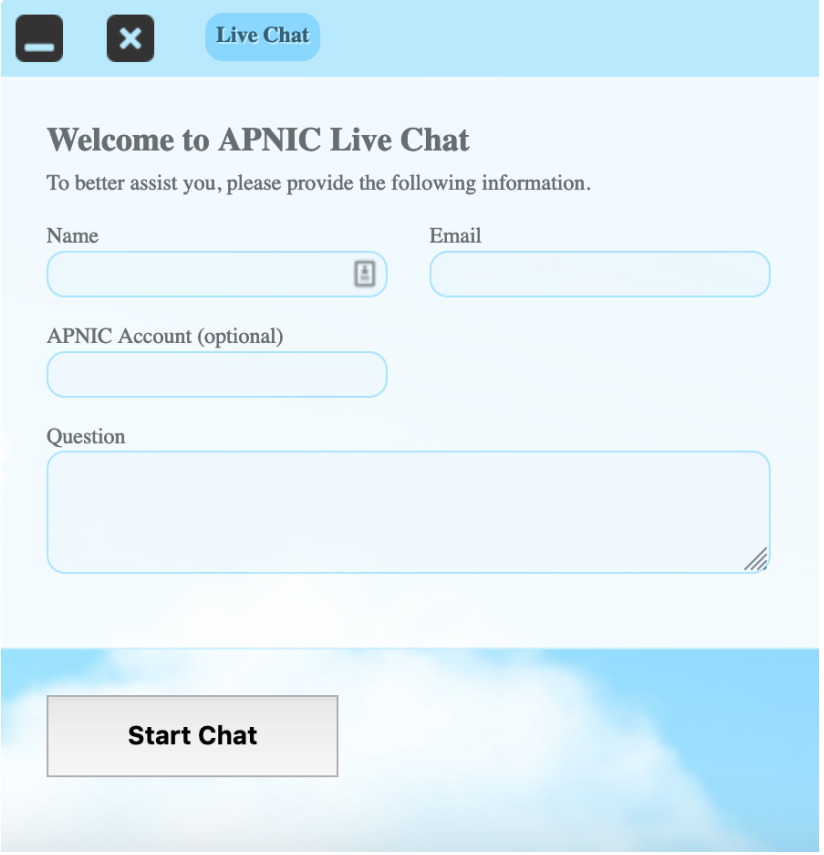
Start: Thursday, 31 January 2019 07:00 AM (UTC +10)
End: Thursday, 31 Jan 2019 08:00 AM (UTC +10)

This maintenance is required to upgrade our edge router firmware in DC2. There may be one or two interruptions to the services listed above for a maximum of 30 minutes within the change window.

More Updates

Subscribe to APNIC Service Announcements

Learn more about system maintenance



Thank You!

APNIC