INT205:Network II

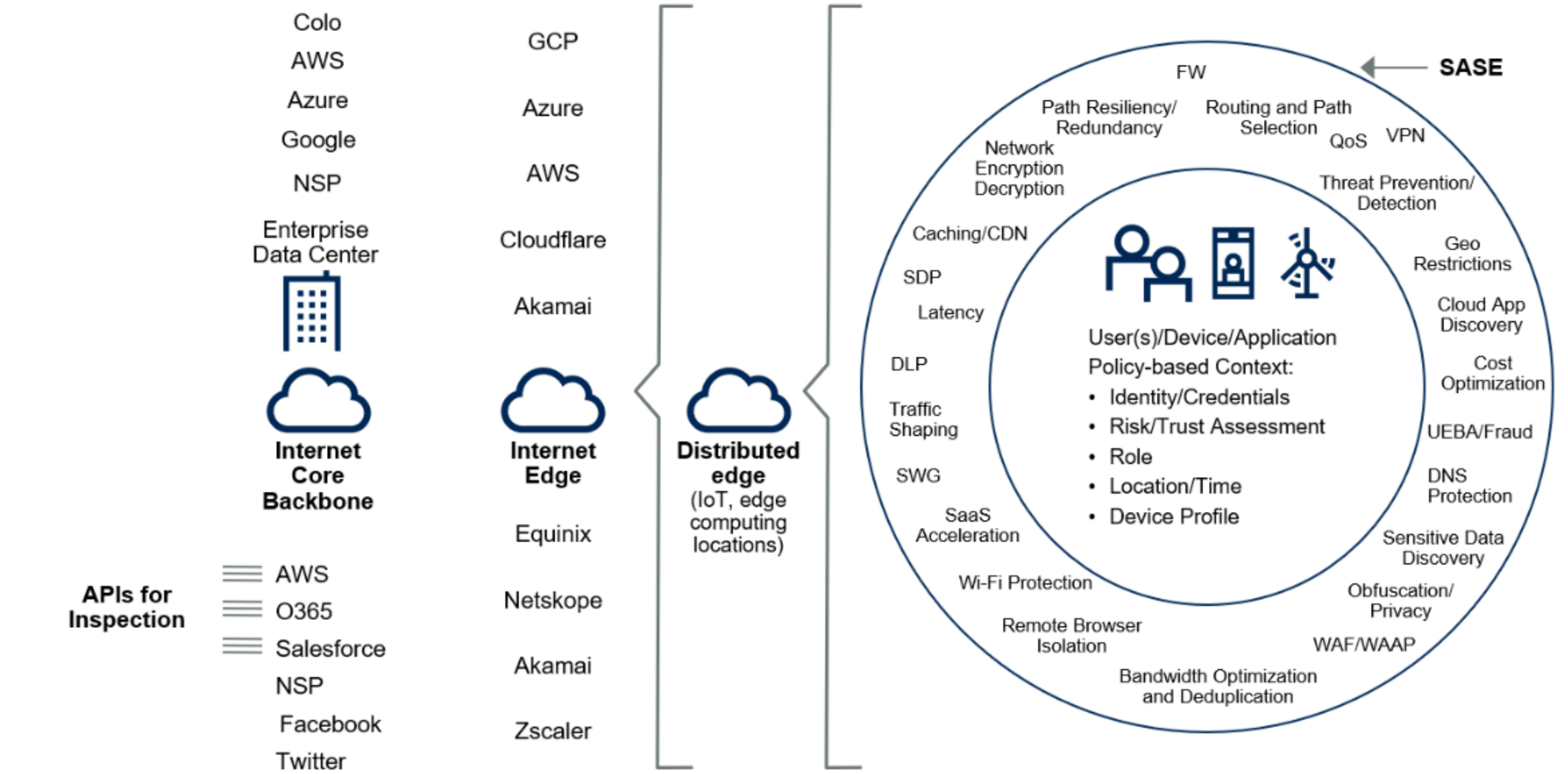
Present

SCHOOL OF INFORMATION TECHNOLOGY

NETWORK & INTERNET SECURITY

The SASE Identity-Centric Architecture

SASE — Convergence and Inversion of the Network and Security Architectures



AWS: Amazon Web Services; DLP: data loss prevention; GCP: Google Cloud Platform; O365: Office 365; SDP: service delivery platform; UEBA: user and entity behavior analytics.

Source: Gartner

ID: 441737

Security components?

end-to-end

ARUBA ESP (EDGE SERVICES PLATFORM)

Next-generation, cloud-native architecture to accelerate digital business transformation

AI & Automation
Onboarding | Provisioning | Management & Orchestration | AIOps | Analytics | Location

Edge-to-Cloud Security
Visibility | Authentication & Authorization | Dynamic Segmentation | Zero Trust | SASE

Unified Infrastructure
Wireless | Wired | SD-WAN | 5G | IoT

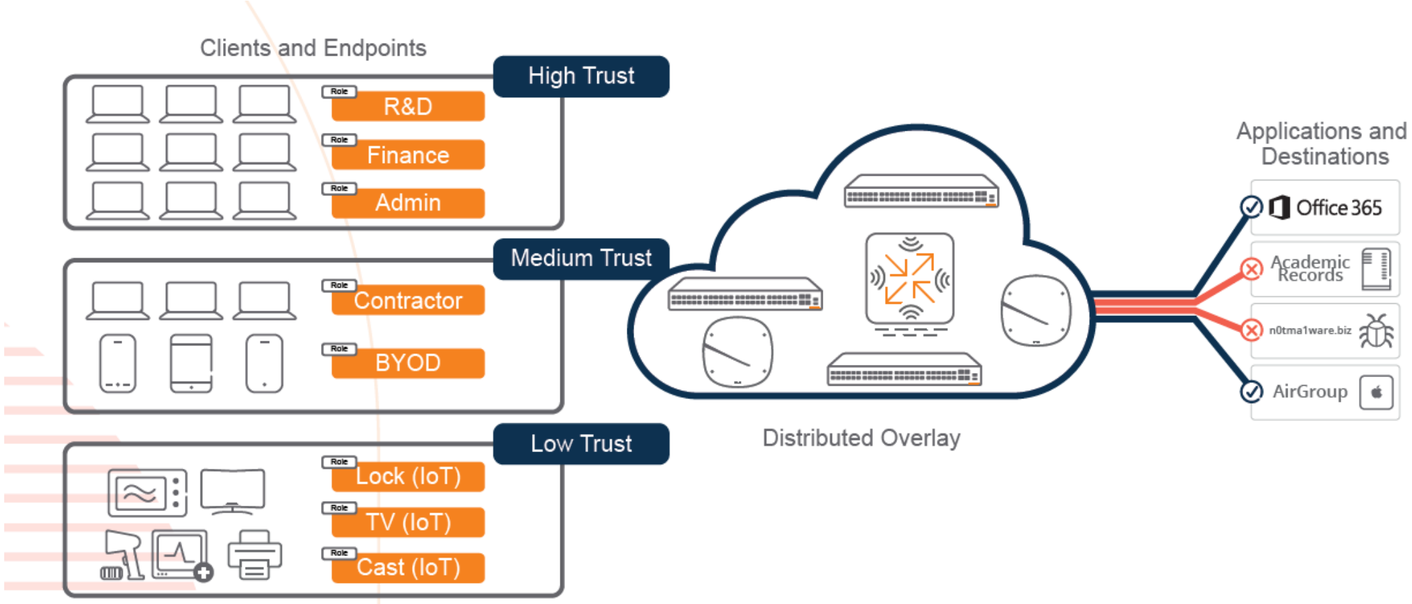
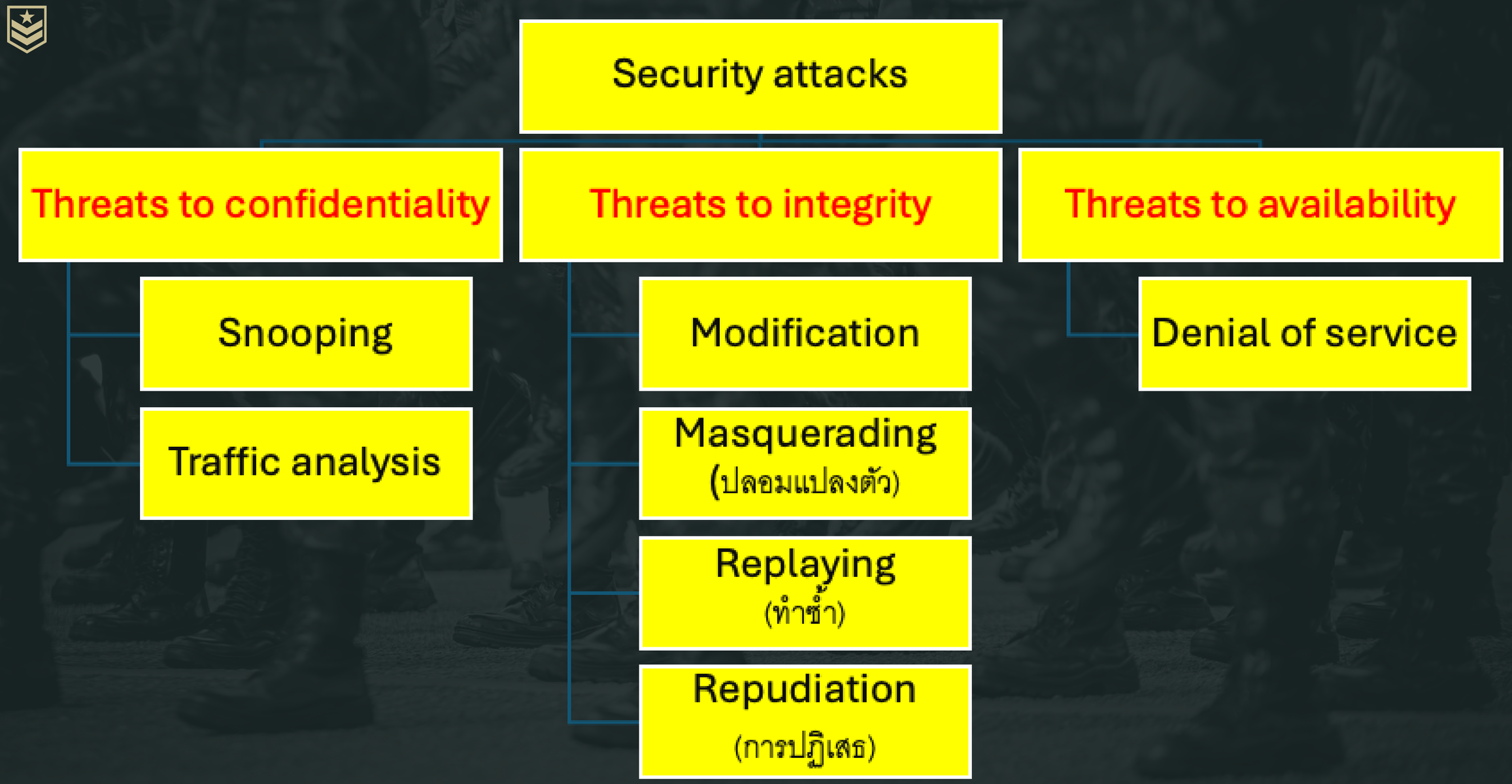


Figure 1: Dynamic Segmentation with a distributed overlay fabric

aruba
a Hewlett Packard Enterprise company

INFORMATION (VISUALIZATION) ERA

- information needs to be hidden from unauthorized access : confidentiality การรักษาความลับ
- protected from unauthorized change : integrity ความคงที่ ไม่แปรเปลี่ยน
- available to an authorized entity when it is needed: availability สภาพพร้อมใช้งาน


Security attacks
Threats to confidentiality
Threats to integrity
Threats to availability
Snooping
Traffic analysis
Modification
Masquerading
(ปลอมแปลงตัว)
Replaying
(ทำซ้ำ)
Repudiation
(การปฏิเสธ)
Denial of service

Facility security

https://www.youtube.com/watch?v=XZmGGAbHqa0

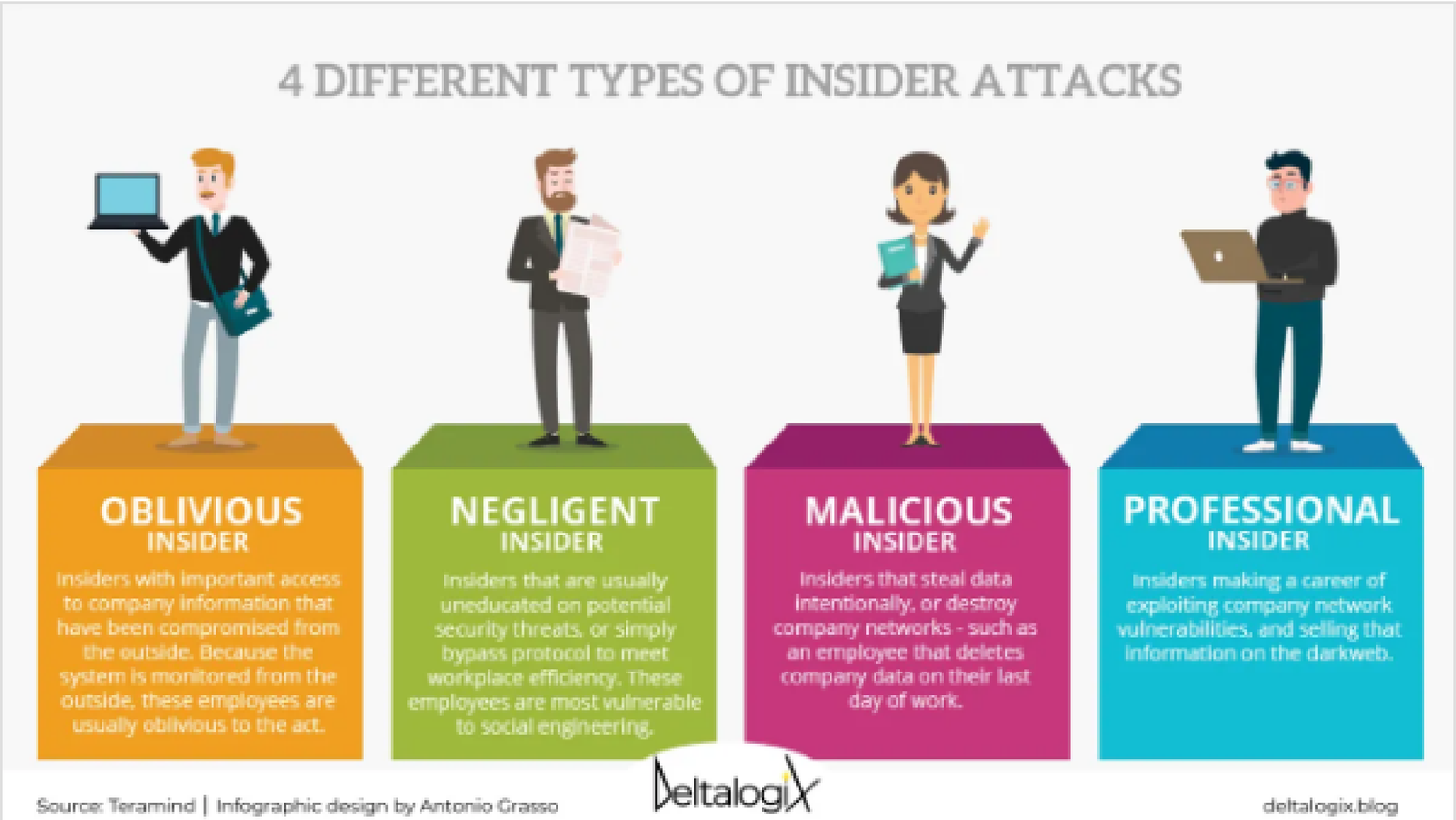
INTRANET
RISKS

01 Intercepting (**ดักจับ**)network messages
– sniffing: interception of user IDs, passwords, confidential Emails, and financial data files

02 Accessing corporate databases
– connections to central databases increase the risk that data will be accessible by employees

03 Privileged (**สิทธิ์พิเศษ**)employees
– override privileges may allow unauthorized access to mission-critical data

04 Reluctance (**ความลังเลใจ**)to prosecute (**เอาผิด/ดำเนินคดี**)
– fear of negative publicity leads to such reluctance but encourages criminal behavior



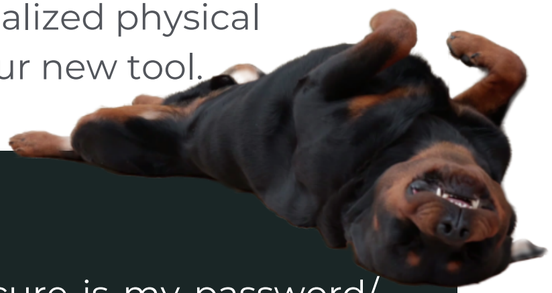
Insider threat: 4 potential threats to your business

Insider threat: this is when the threat of a cyber attack comes from internal resources. Here are 4 sketches to identify the culprit.

DeltalogiX / Jul 7, 2021

HOW SECURE IS MY PASSWORD?

Entries are 100% secure and not stored in any way or shared with anyone. Period.
Interested in getting your personalized physical and digital security score? Visit our new tool.

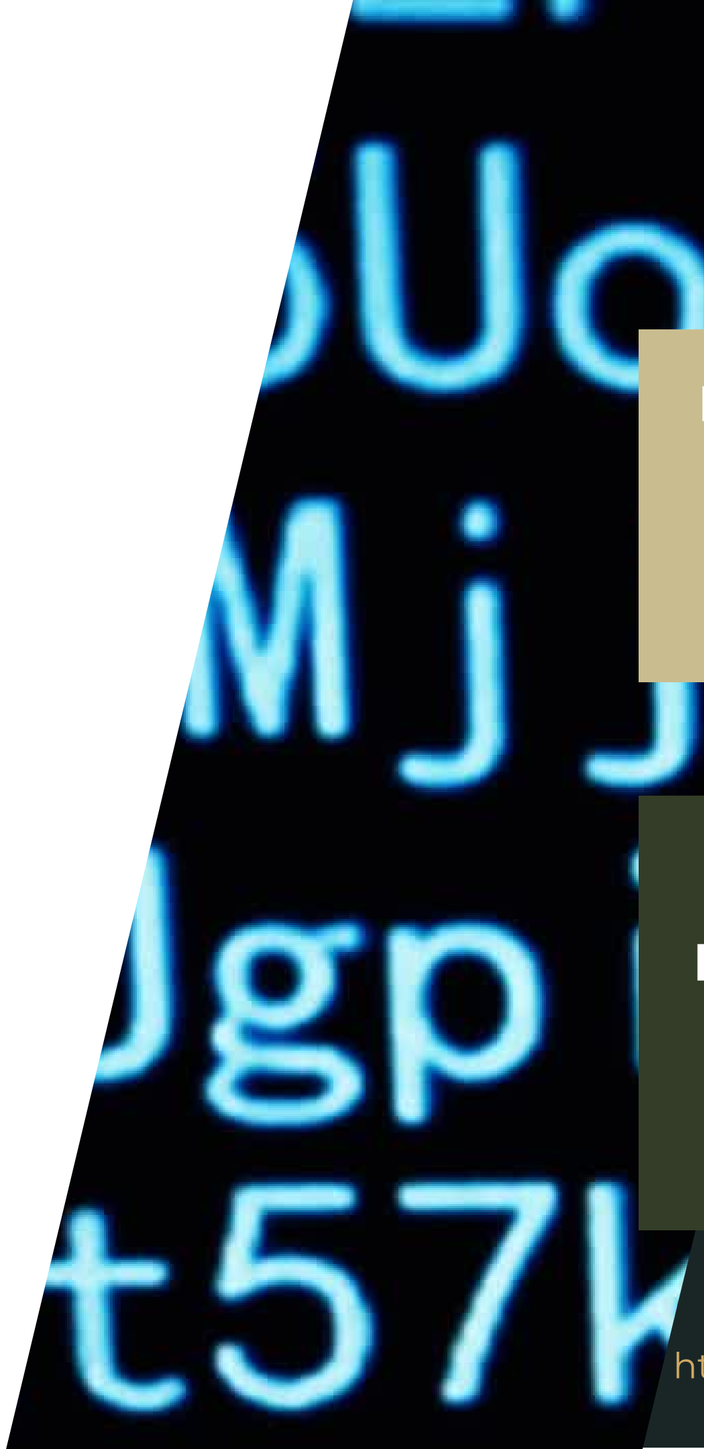


https://www.security.org/how-secure-is-my-password/

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST'S NEW PASSWORD RULES

Special Publication 800-63-3: Digital Authentication Guidelines



Favor the user, Size matters, Check new passwords against a dictionary of known-bad choices

No composition rules, No password hints, Knowledge-based authentication (KBA) is out, No more expiration without reason

https://pages.nist.gov/800-63-3/sp800-63-3.html

External threats

NEWS

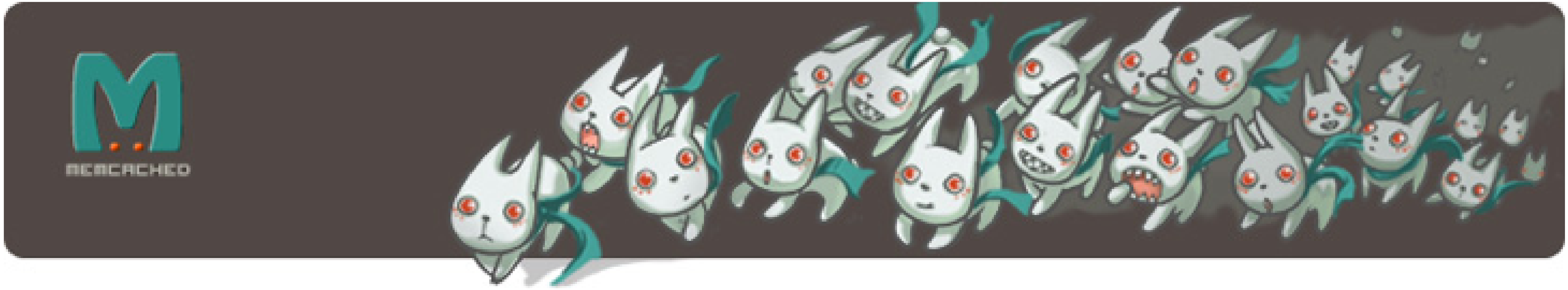
Armies of hacked IoT devices launch unprecedented DDoS attacks

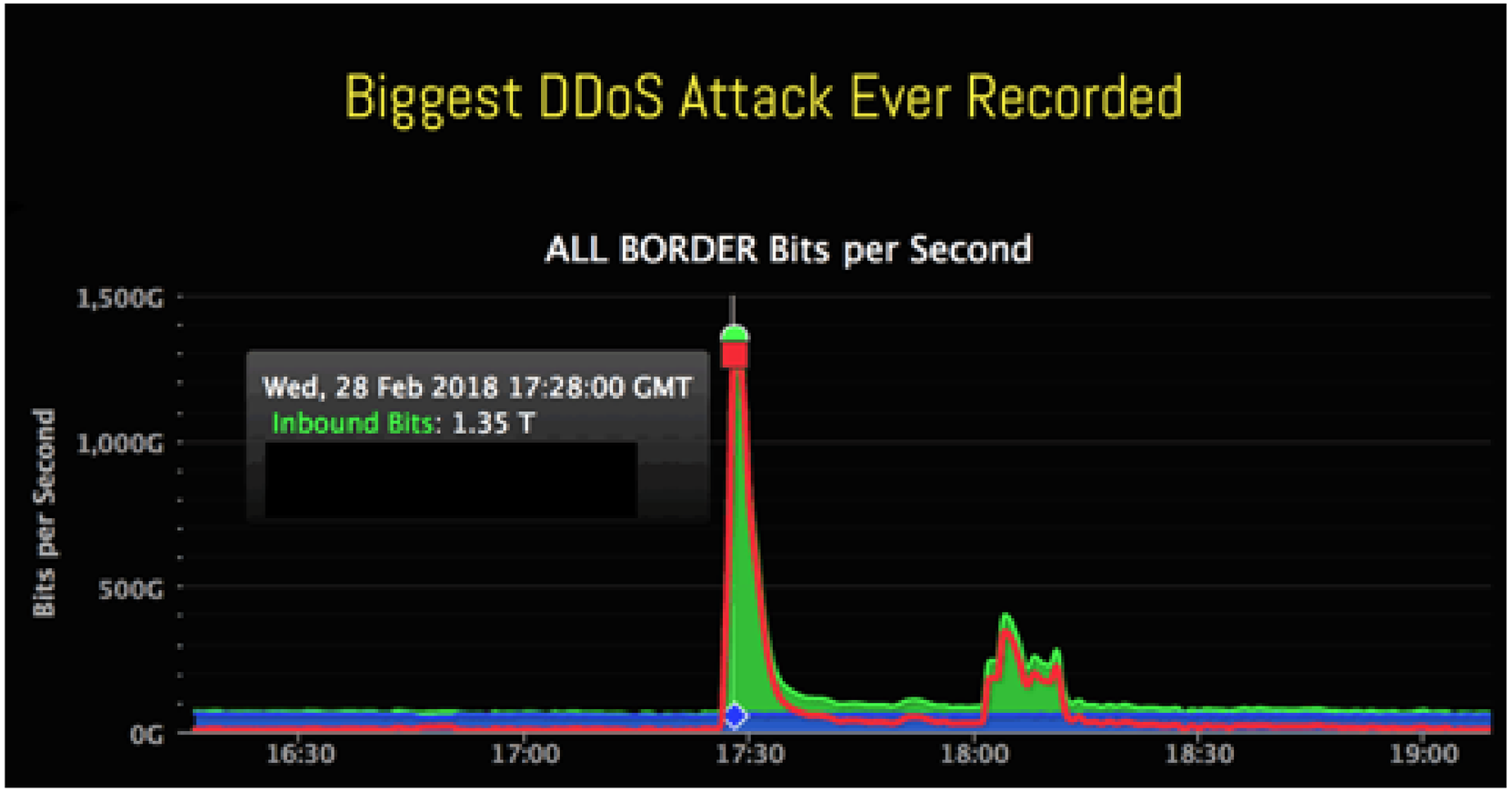
By Lucian Constantin | Follow
IDG News Service | Sep 26, 2016 10:17 AM PT

Octave Klaba, the founder and CTO of French hosting firm OVH, sounded the alarm on Twitter last week when his company was hit with two concurrent DDoS attacks whose combined bandwidth reached almost 1 terabit per second. One of the two attacks peaked at 799Gbps alone, making it the largest ever reported.

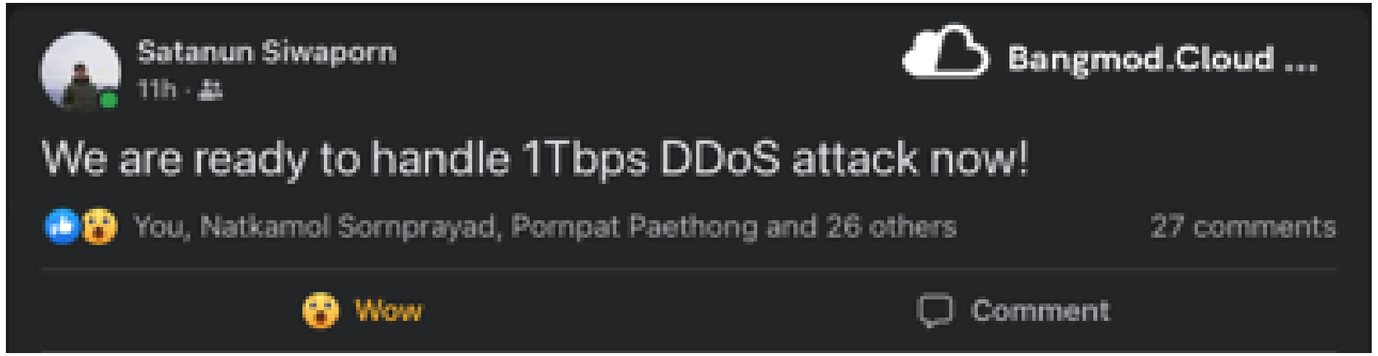
According to Klaba, the attack targeted Minecraft servers hosted on OVH's network, and the source of the junk traffic was a botnet made up of 145,607 hacked digital video recorders and IP cameras.

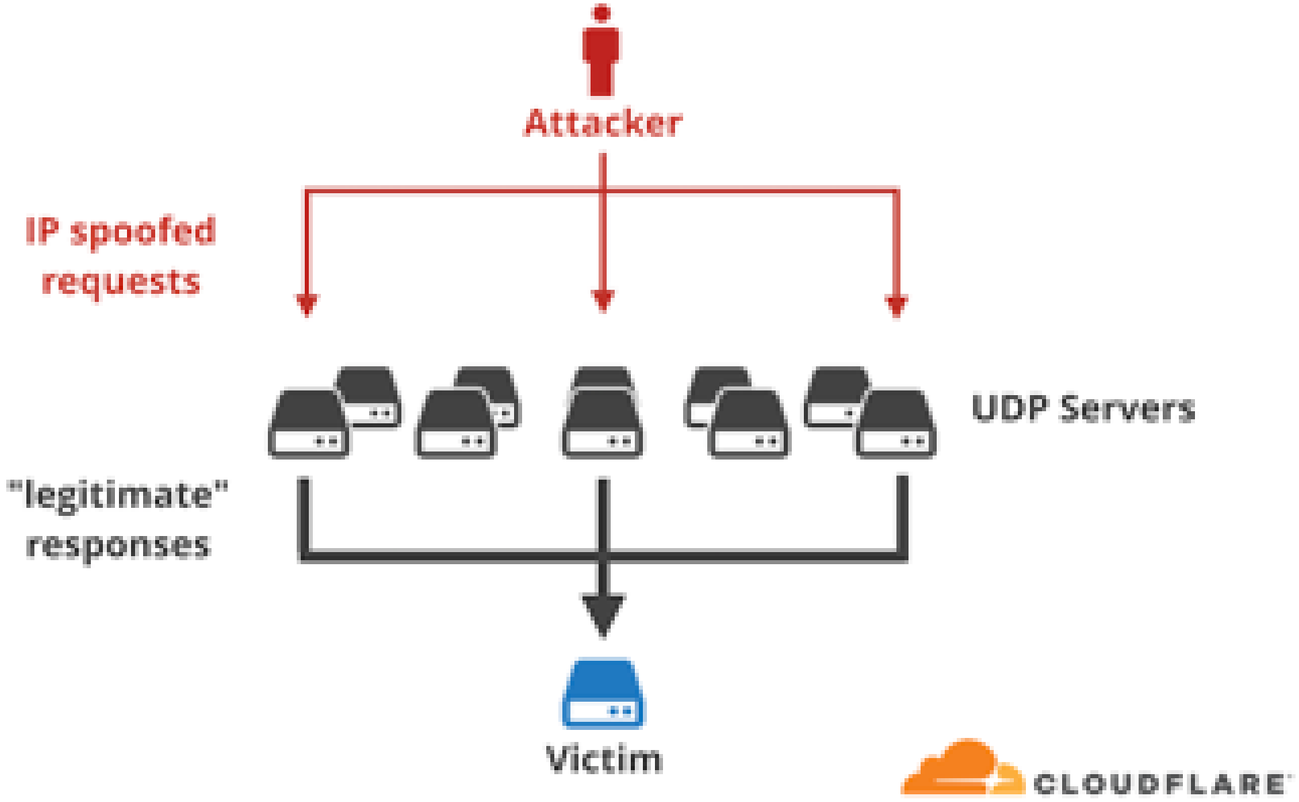
http://www.csoonline.com/article/3124344/internet-of-things/armies-of-hacked-iot-devices-launch-unprecedented-ddos-attacks.html



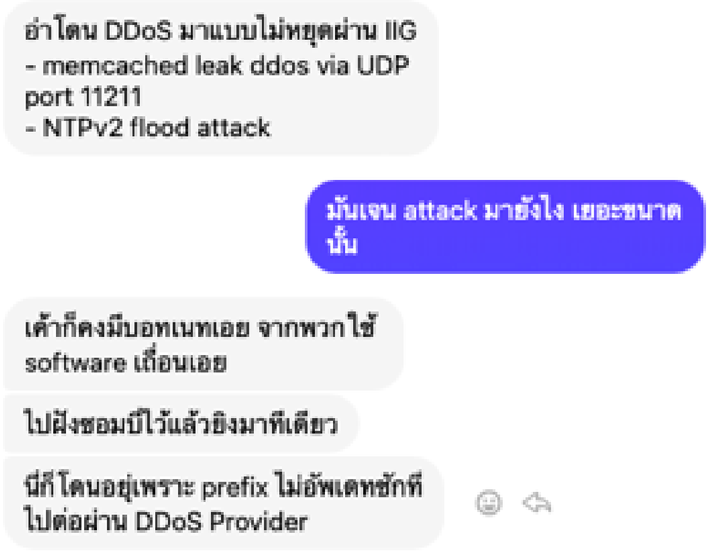


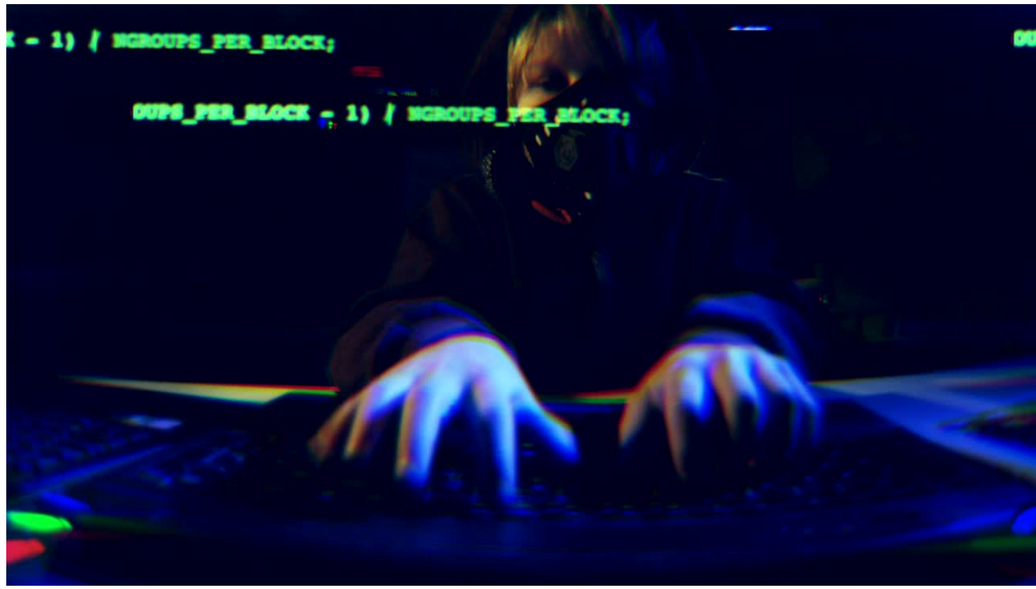
Github said, "The attack originated from over a thousand different autonomous systems (ASNs) across tens of thousands of unique endpoints. It was an amplification attack using the memcached-based approach described above that peaked at 1.35Tbps via 126.9 million packets per second."





https://blog.cloudflare.com/memcrashed-major-amplification-attacks-from-port-11211/



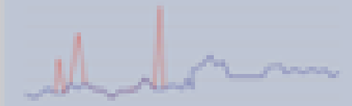
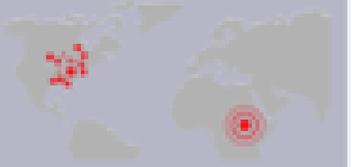


Known-Known
Detect the exactly known infection, as seen before

Known-Unknown
Detect previously unseen variations of known threats, subfamilies or related new threats

Unknown-Unknown
Detect zero-days, unrelated to any known malware

Threat Type vs. Suitable Detection Technique

	Static Signatures	Dynamic Signatures	Behavioral Signatures	High-Level Patterns	Unsupervised Anomalies
Examples	Concrete malicious domain name associated to trojan **server1.39sksx3bw.ru**	Houdini RAT telemetry pattern **regex: .*\([a-z]{ready|ri-noy|gnfoh)**	Two illustrative found instances **hxxp://crazyerror.su/b/opt/9681BAE3DB3A2F9D446CD5E3** **hxxp://50.63.147.69:8080/b/req/3D111E6821F373015C646CA4**	Generic characteristics of suspicious traffic 	Expected vs. unexplained and unexpected 
What it Does	**Manual definition, possibly tooling-assisted** Exact matching of predefined character or numeric sequences Definitions human-readable	**Manual definition, possibly tooling-assisted** Matching of predefined rules (for example, regex) Definitions human-readable	**Applicable through supervised machine-learning** Matching of machine-learned rules or recognition of machine-learned behavioral patterns in transformed feature space	**Task for semi-supervised machine learning** Very high-level patterns, machine-learned to distinguish generic behavior	**Unsupervised machine learning** Cases significantly distant to all known normal behavior, where the model of known behavior is machine-learned Distance measures can be highly abstract
Technique Properties	**Very high precision** **No generalization** Recall limited to the exact same cases **Good explainability** **Does not scale** **Requires manual definition** *Not applicable to encrypted data without MITM*	**Very high precision** **Generalization limited** Recall limited to predefined pattern; finds variations explicitly covered by the pattern **Good explainability** **Does not scale well** **Requires manual definition** *Not applicable to encrypted data without MITM*	**High precision** **Generalization based on similarity to known malware** Ideal for finding previously unseen variations/subfamilies of known infections **Good explainability but more complex** **Scales somewhat well** **Learned (semi)auto from data** *Applicable to encrypted data without decryption*	**Good precision** **Generalization based on common suspicious behaviors** High recall, good chance to find true zero-days, at the cost of more false alarms **Explainability limited** Findings may be difficult to attribute to known infections **Scales well** **Learned (semi)auto from data** *Applicable to encrypted data without decryption*	**Low precision** **Generalization based on unusual behaviors** Best chance to find true zero-days; highest risk of false alarms **Explainability difficult** Findings may be difficult to attribute to known infections **Scales well** **Learned auto from data** *Applicable to encrypted data without decryption*

Better Precision and Explainability, Simplicity of Proof ← Technique Trade-Off → Better Recall, Scalability, Applicability to Encrypted Data, Ability to Detect Zero-Days

Please note: scaling statements refer to human time required to maintain detection system

Please note: this diagram represents a simplified illustration of machine learning capabilities in security

Source: Cisco Security Research

Download the 2018 graphics at: cisco.com/go/acr2018graphics

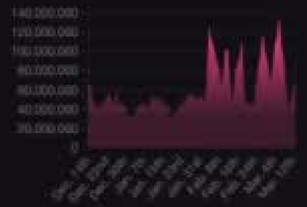
CHECK POINT

THREATCLOUD

LIVE CYBER THREAT MAP

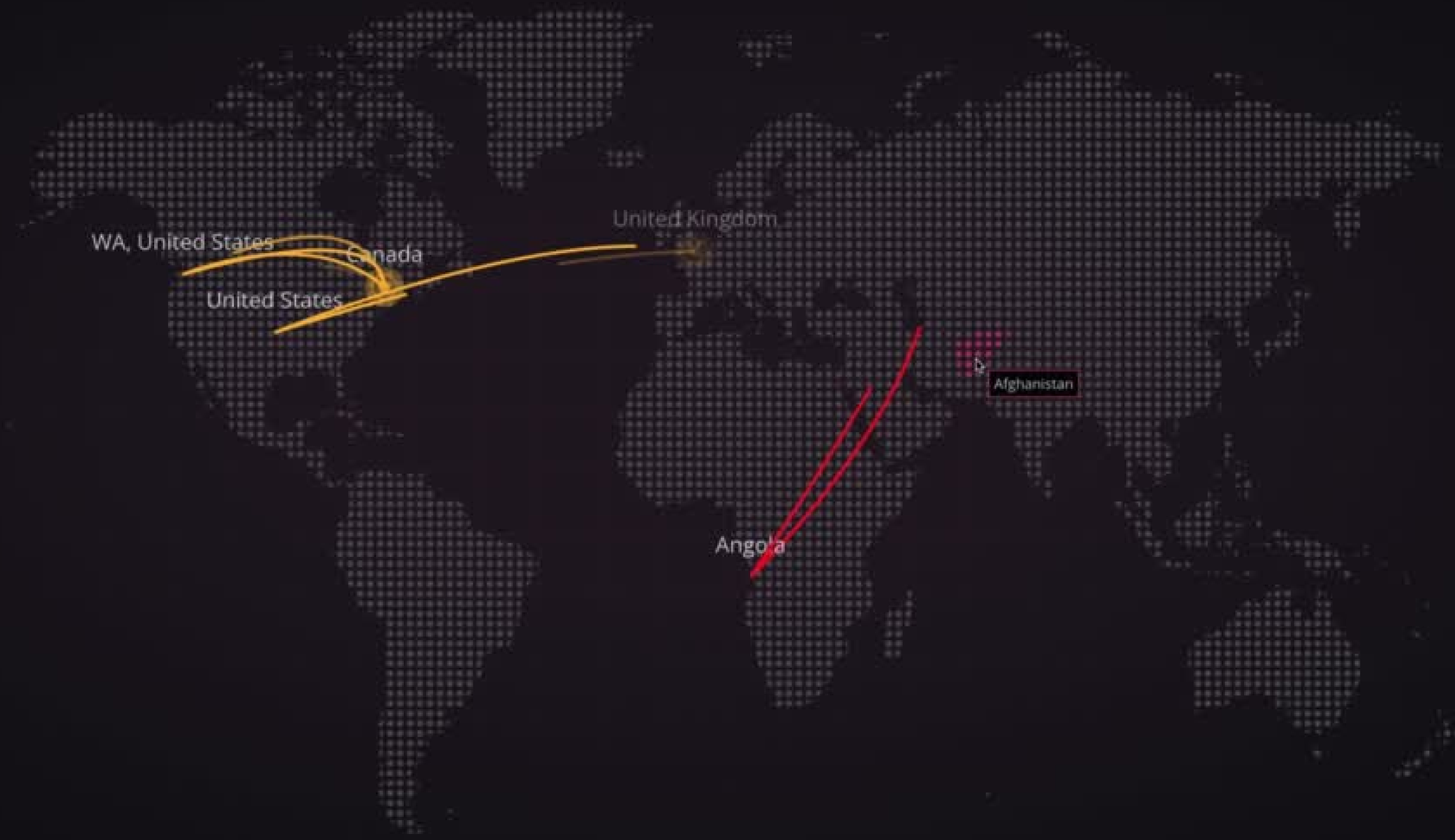
78,947,221 ATTACKS ON THIS DAY

RECENT DAILY ATTACKS



ATTACKS ⊙ Current rate — 4 +

- Worm.WIN32.Phorpiex.B
  12:40:15 Angola → Kazakhstan
- Web Server Enforcement Violation
  12:40:14 United States → United Kingdom
- Worm.WIN32.Phorpiex.B
  12:40:14 Angola → Kazakhstan
- Worm.WIN32.Phorpiex.B
  12:40:14 Angola → Kazakhstan
- Web Server Enforcement Violation
  12:40:14 United States → United Kingdom
- Web Server Enforcement Violation
  12:40:13 WA, United States → Canada
- Web Server Enforcement Violation
  12:40:13 WA, United States → Canada



Malware Phishing Exploit

TOP TARGETED COUNTRIES

Highest rate of attacks per organization in the last day.

- Mongolia
- Nepal
- Georgia
- Vietnam
- Indonesia

TOP TARGETED INDUSTRIES

Highest rate of attacks per organization in the last day.

- Education
- Healthcare
- Government

TOP MALWARE TYPES

Malware types with the highest global impact in the last day.

- Backdoor
- Phishing
- Adware

Basic device access security

Advantages

- Complete separation of management and data planes
- Very difficult to lock yourself out

Disadvantages

- Less flexibility
- Remote access possible, but can be complex

Connection	Protocol	Interface
Console	Serial	CLI (or Menu)

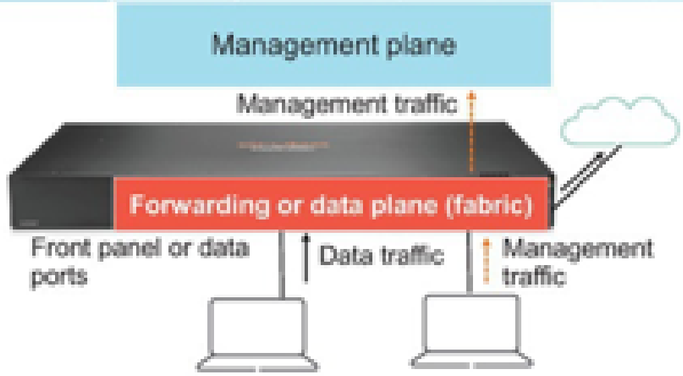
Advantages

- No separate infrastructure required

Disadvantages

- Less resistant to traffic issues
- Requires additional settings to segregate data and management traffic

Connection	Protocol	Interface
IP	Telnet*	CLI
	SSH	CLI
	HTTP*	Web UI and REST
	HTTPS	Web UI and REST
	SNMP	No interface (accesses MIB objects)



*AOS-CX switches do not support Telnet or HTTP for security

aruba

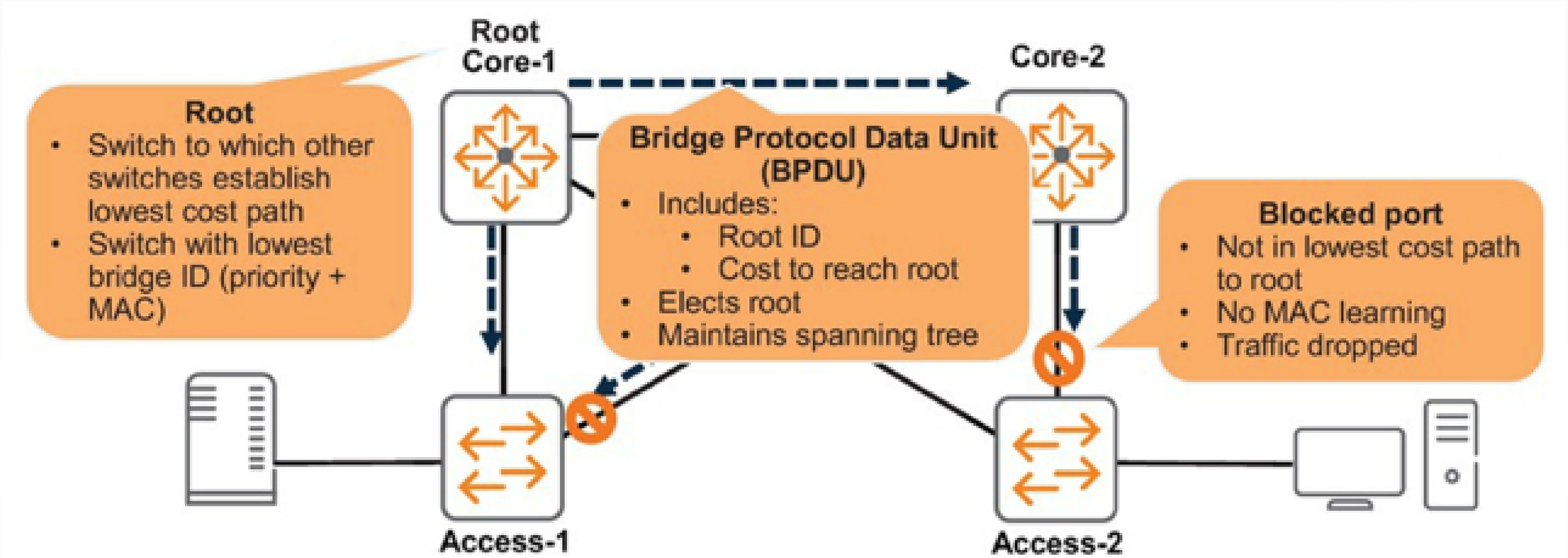
Network protocol security

Cisco Press

Spanning Tree Protocol Features > Security Features on Switches | Cisco...

This chapter describes Layer 2 security basics and security features on switches available to combat...

ciscopress.com

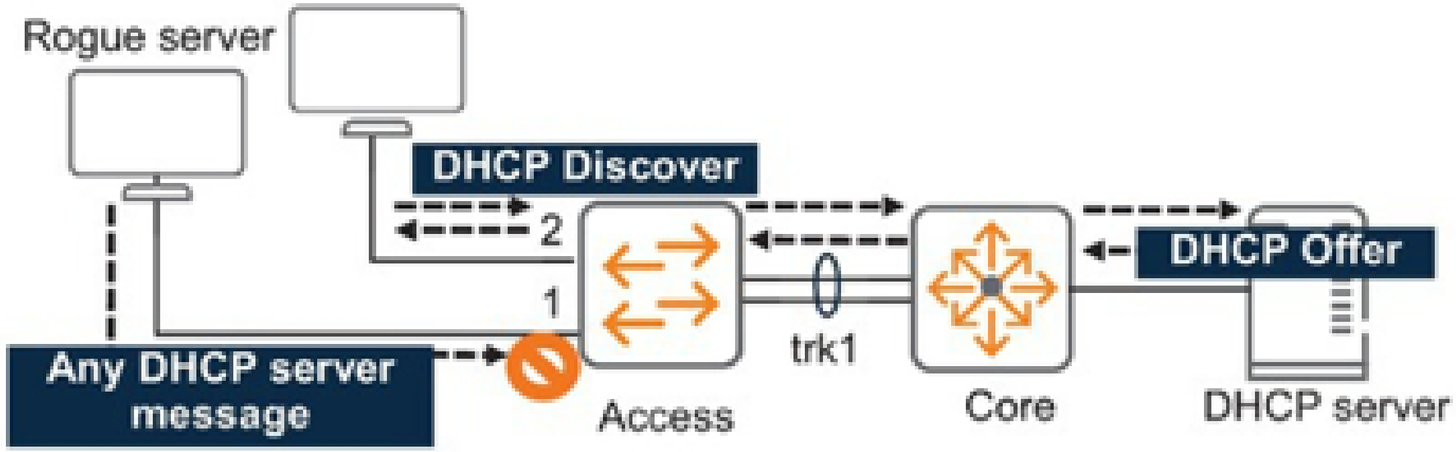


aruba
a Hewlett Packard Enterprise company

Network protocol security

Access ArubaOS-Switch config

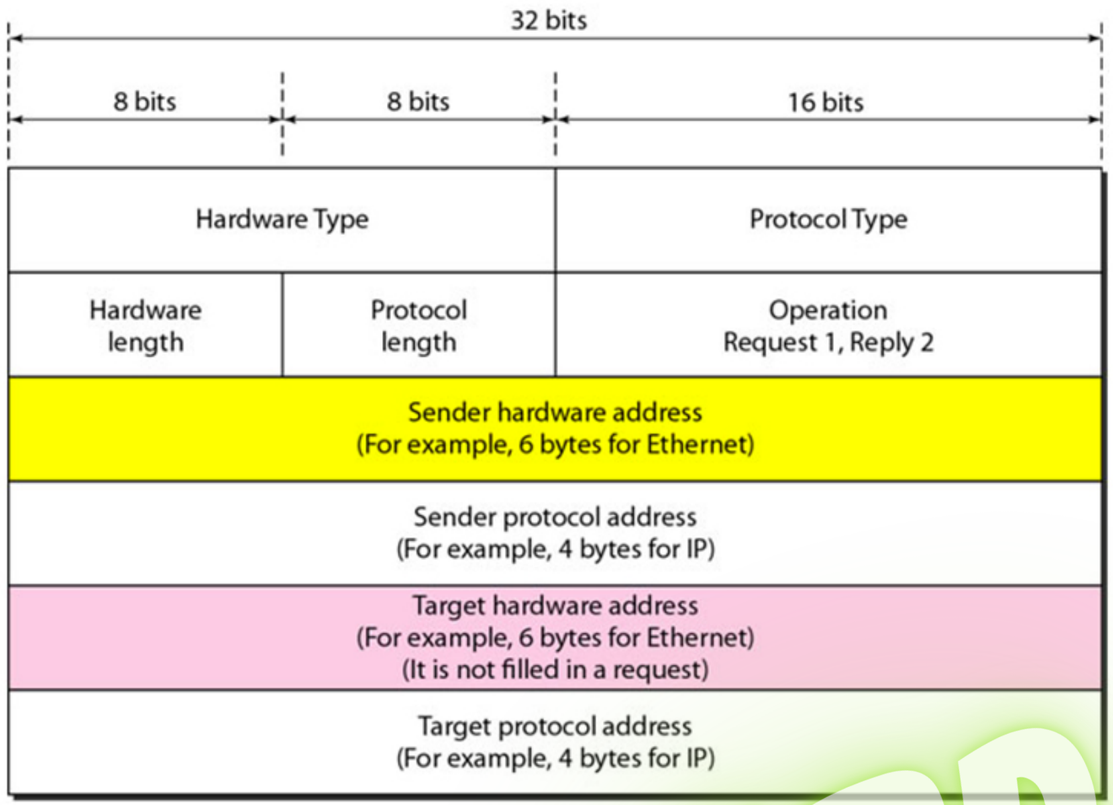
```
dhcp-snooping vlan 11

dhcp-snooping trust trk1

dhcp-snooping max-binding 1

dhcp-snooping
```



Ports	Status	Port behavior
1-2	Untrusted (default status)	Accepts valid DHCP client packets Drops DHCP server packets Does not forward DHCP client packets from other ports
Trk1	Trusted	Accepts and forwards any DHCP packet

aruba
a Hewlett Packard Enterprise company

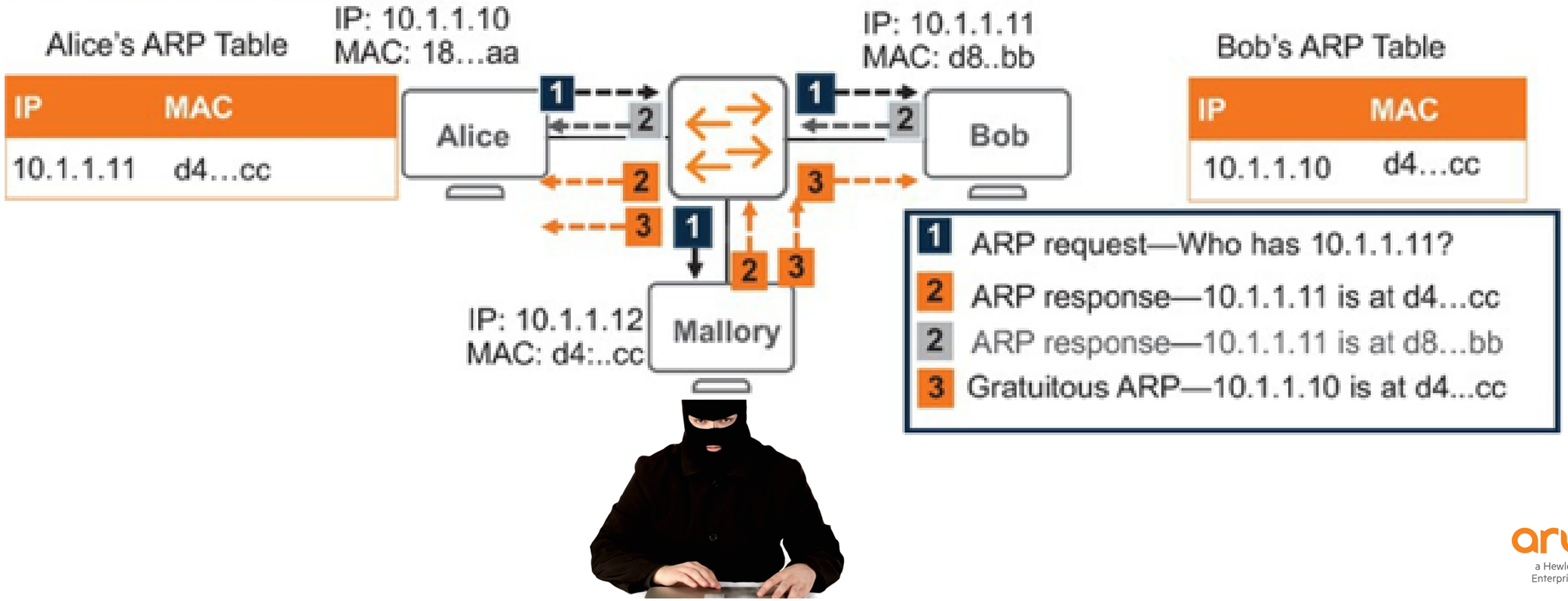
WHAT IS ADDRESS RESOLUTION PROTOCOL ?



ARP

ARP vulnerabilities

- ARP poisoning
- ARP snooping
- DoS attacks



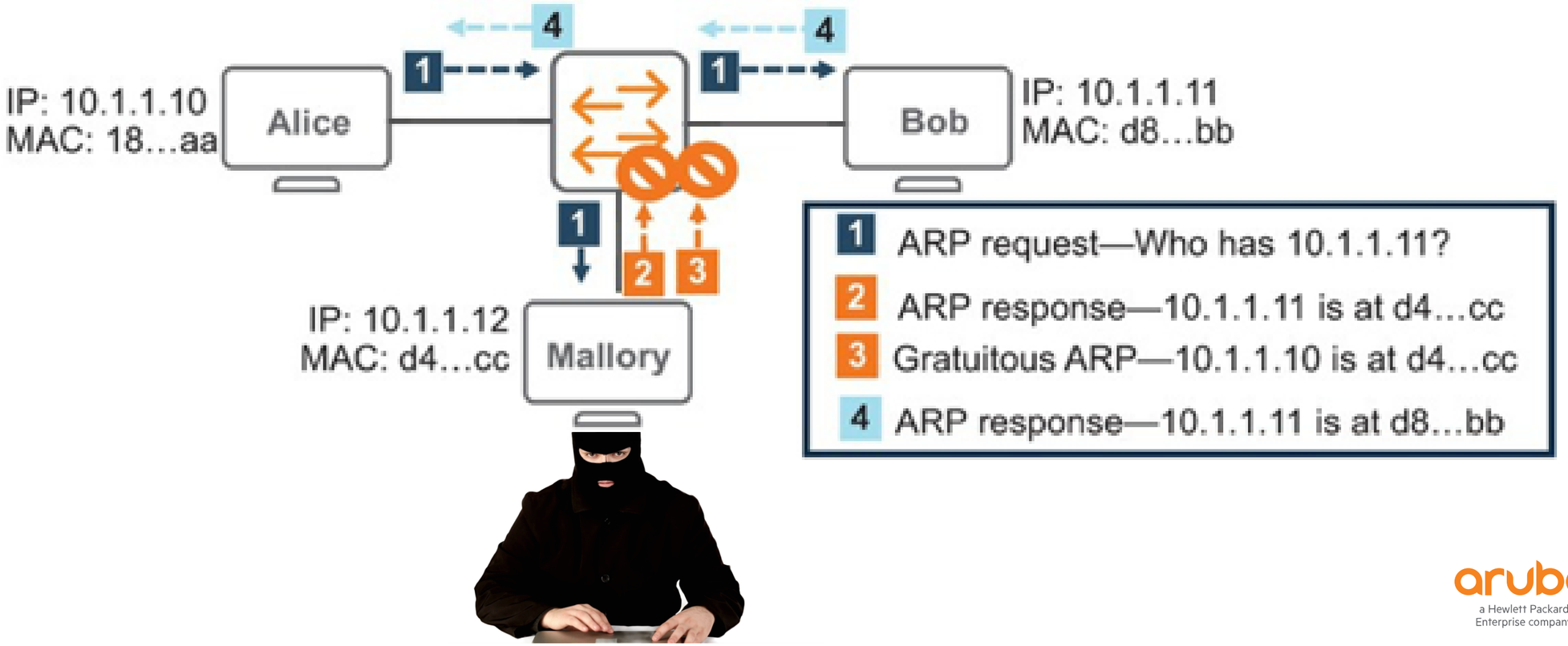
aruba
a Hewlett Packard Enterprise company

Alice's ARP Table

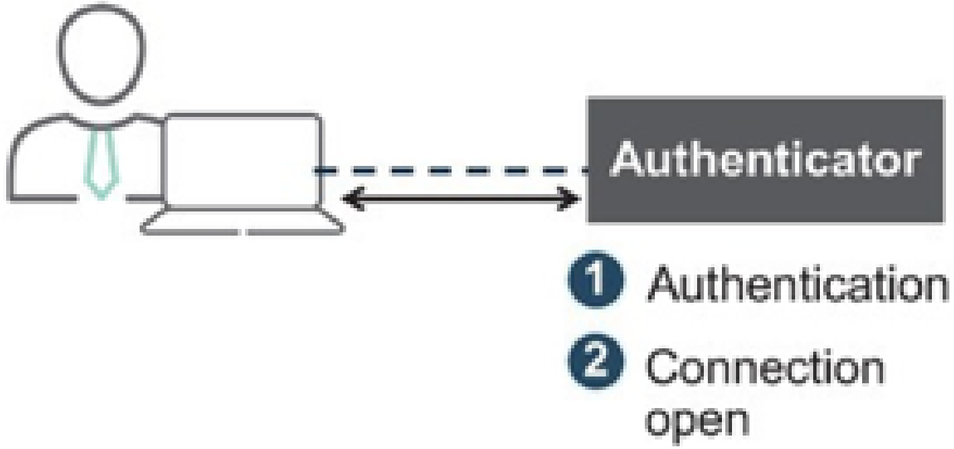
IP	MAC
10.1.1.11	d8…bb

IP-to-MAC binding table

IP	MAC
10.1.10.10	18…aa
10.1.10.11	d8…bb
10.1.10.12	d4…cc

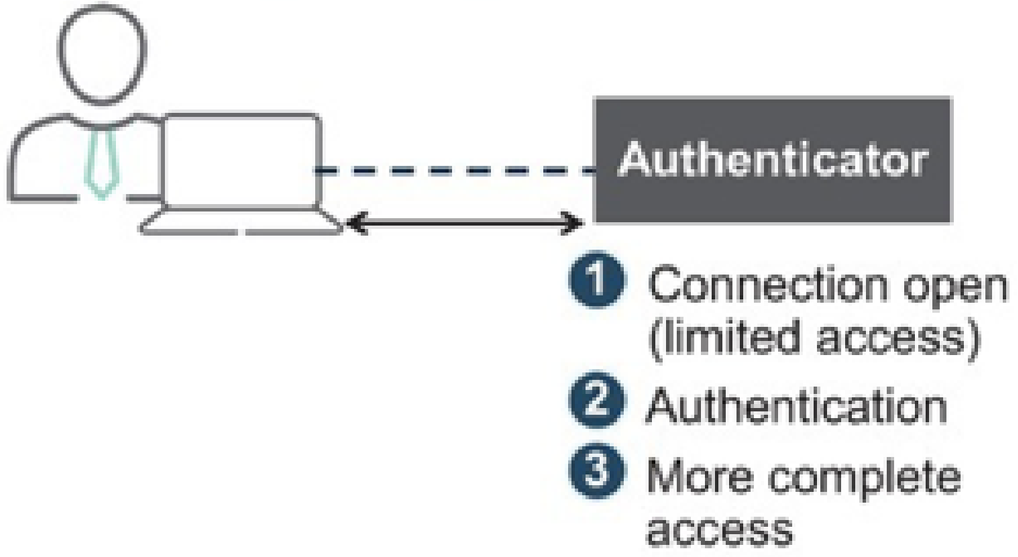


Layer 2 authentication



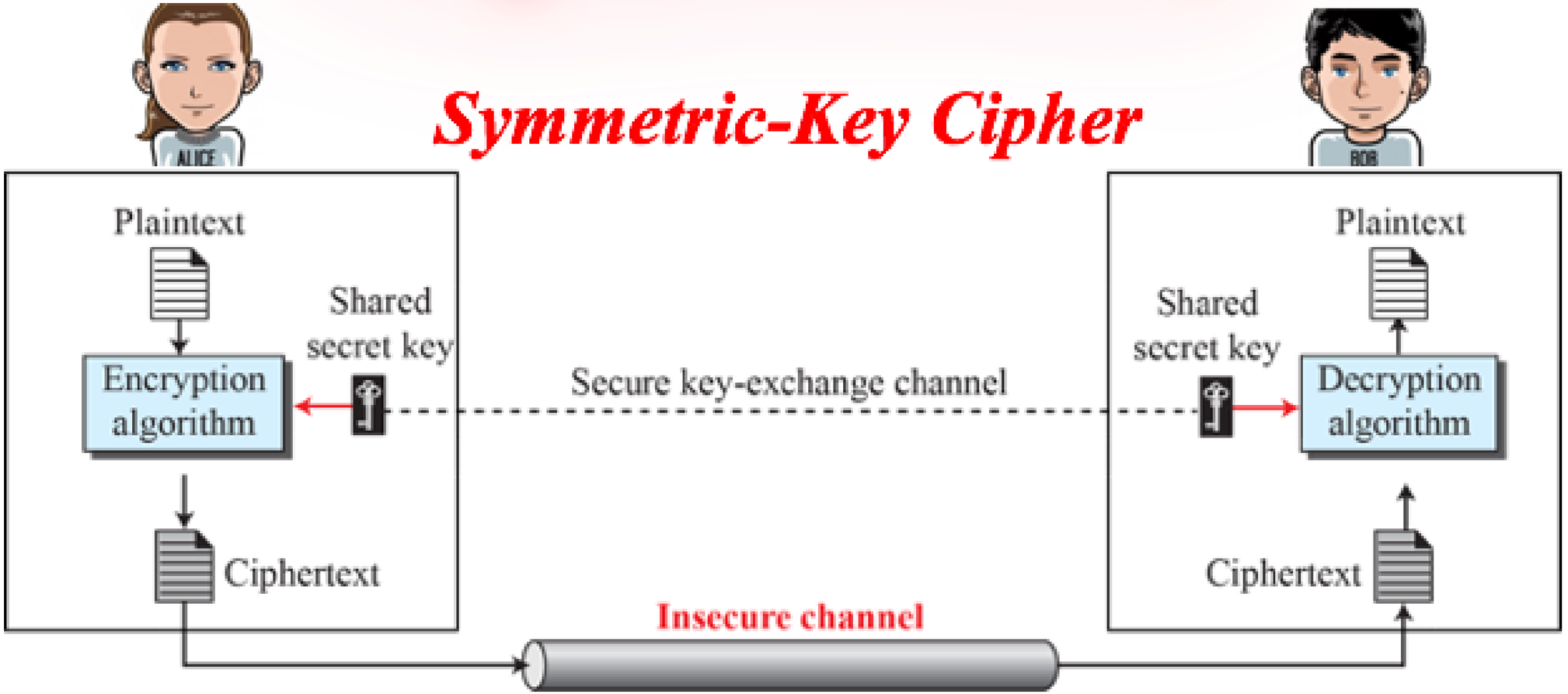
- Examples
  - MAC authentication (MAC-Auth)
  - 802.1X

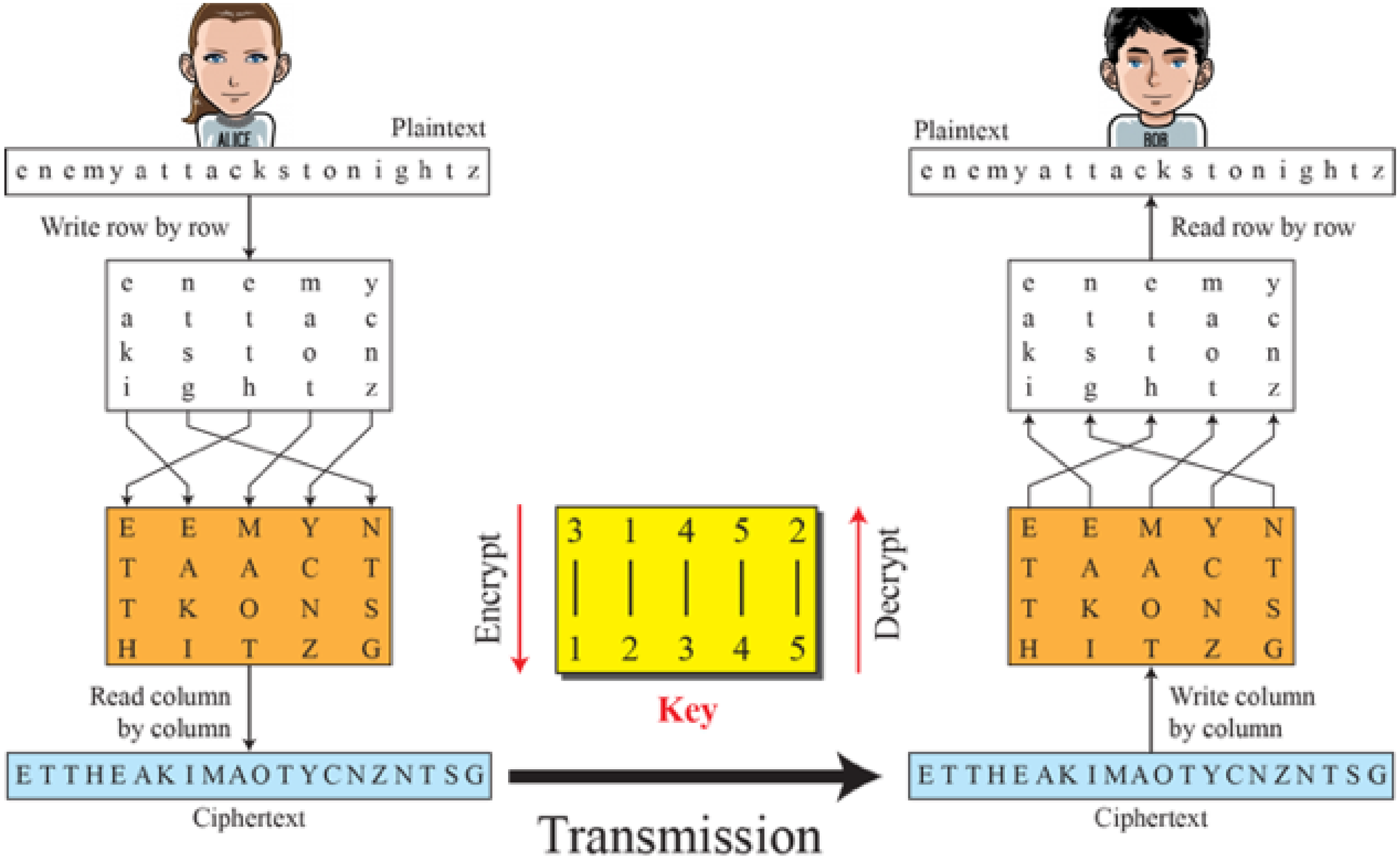
Layer 3 authentication



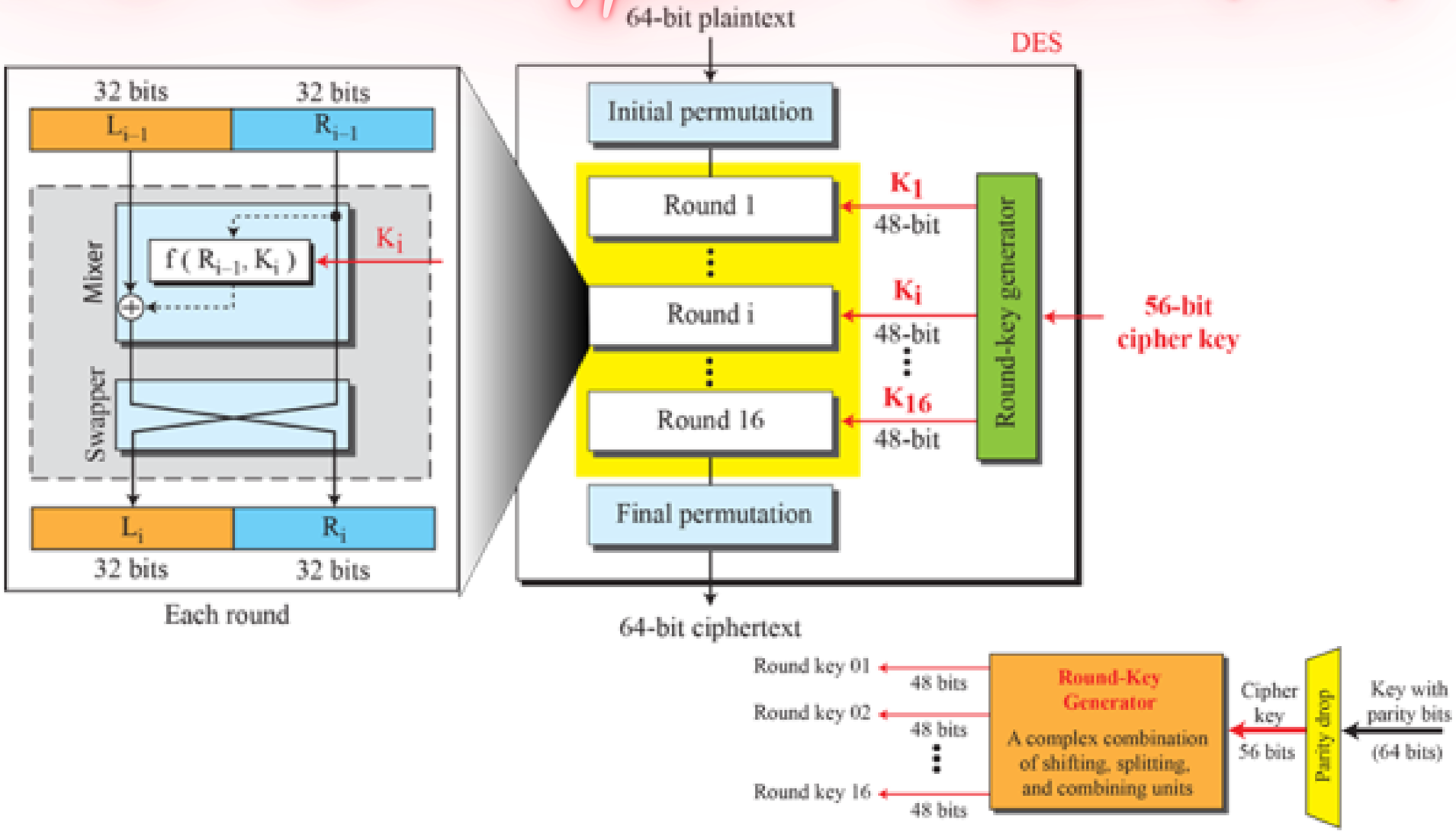
- Example
  - Captive portal authentication

Confidentiality

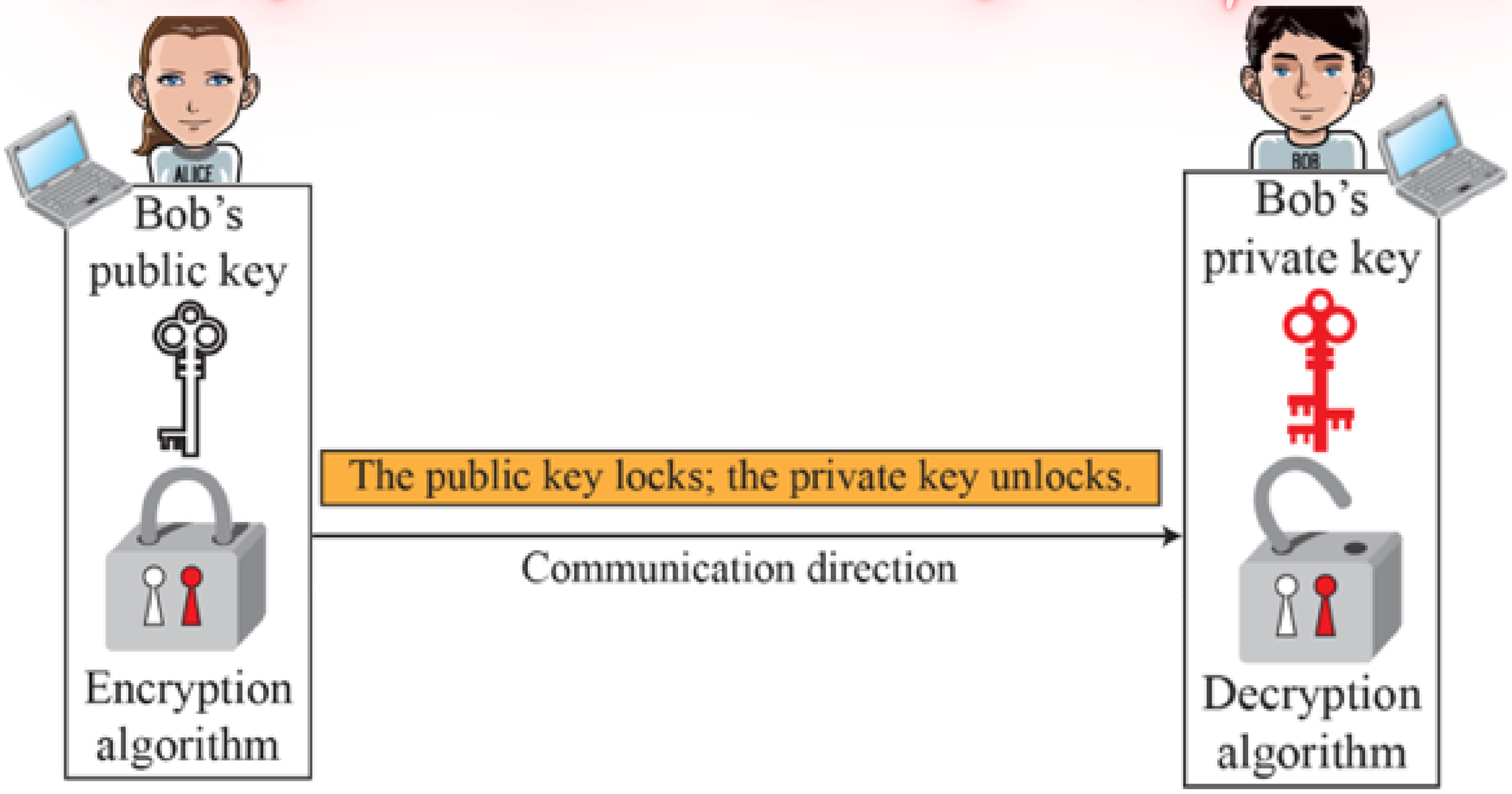



ALICE
Plaintext
e n e m y a t t a c k s t o n i g h t z
Write row by row
e n e m y
a t t a c
k s t o n
i g h t z
E E M Y N
T A A C T
T K O N S
H I T Z G
Read column by column
E T T H E A K I M A O T Y C N Z N T S G
Ciphertext
Encrypt
3 1 4 5 2
1 2 3 4 5
Key
Decrypt
Transmission
BOB
Plaintext
e n e m y a t t a c k s t o n i g h t z
Read row by row
e n e m y
a t t a c
k s t o n
i g h t z
E E M Y N
T A A C T
T K O N S
H I T Z G
Write column by column
E T T H E A K I M A O T Y C N Z N T S G
Ciphertext

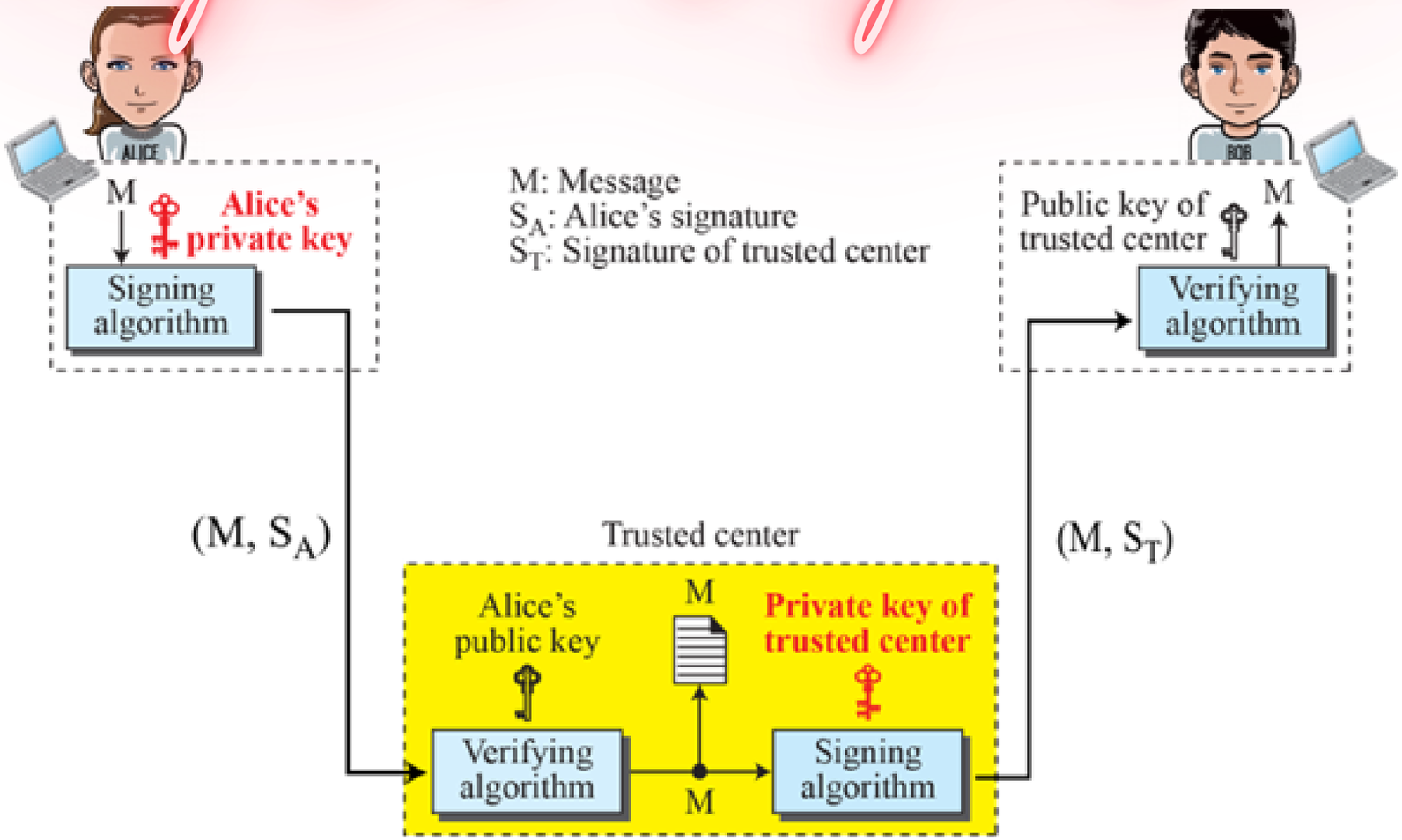
Data Encryption Standard



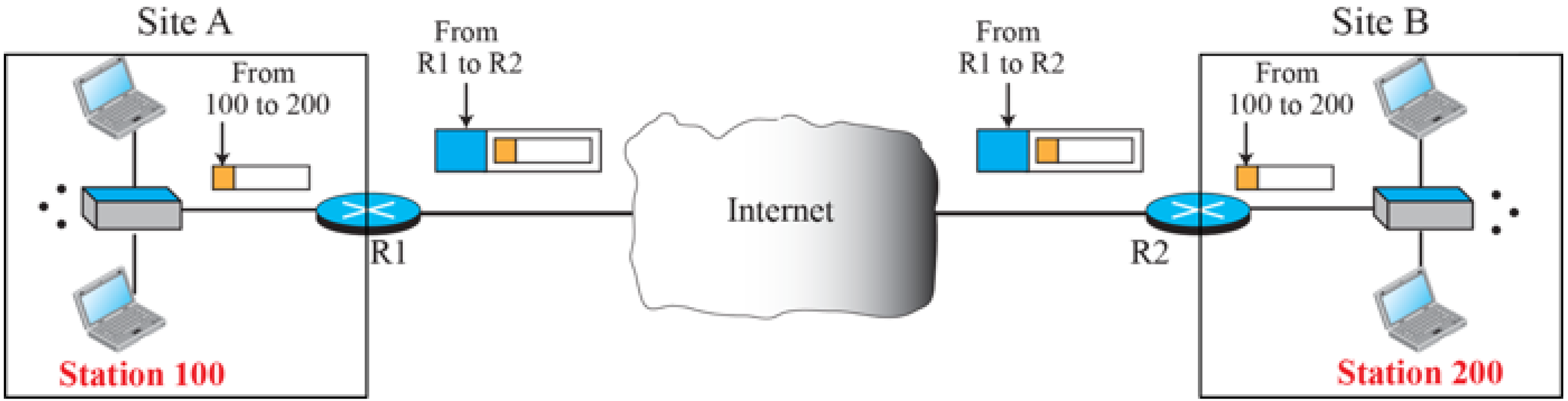
Asymmetric-Key Ciphers



Digital Signature

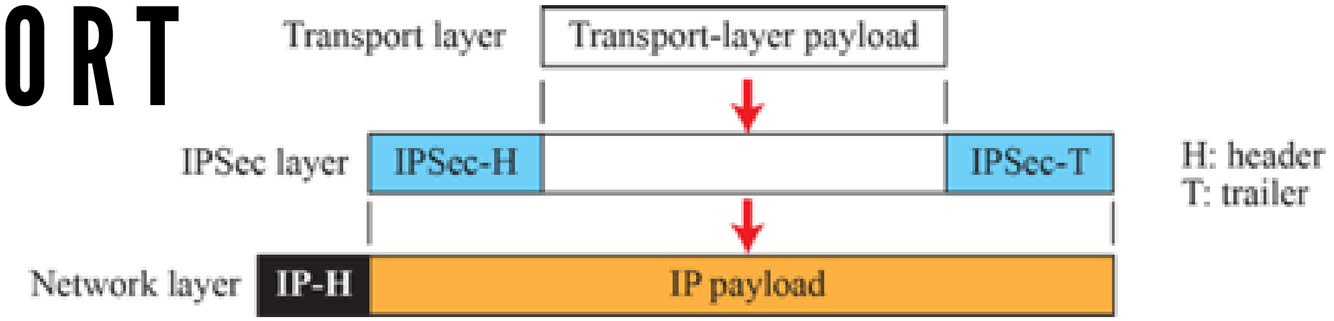


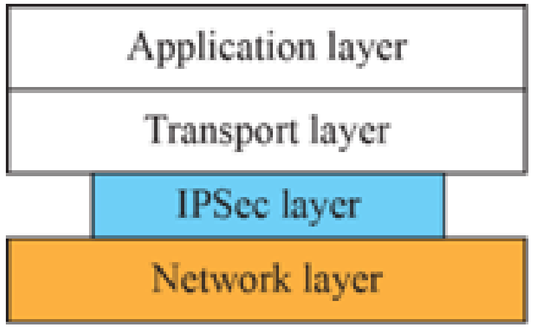
WHAT IS
VIRTUAL PRIVATE NETWORK PROTOCOL ?



IPSec

TRANSPORT MODE

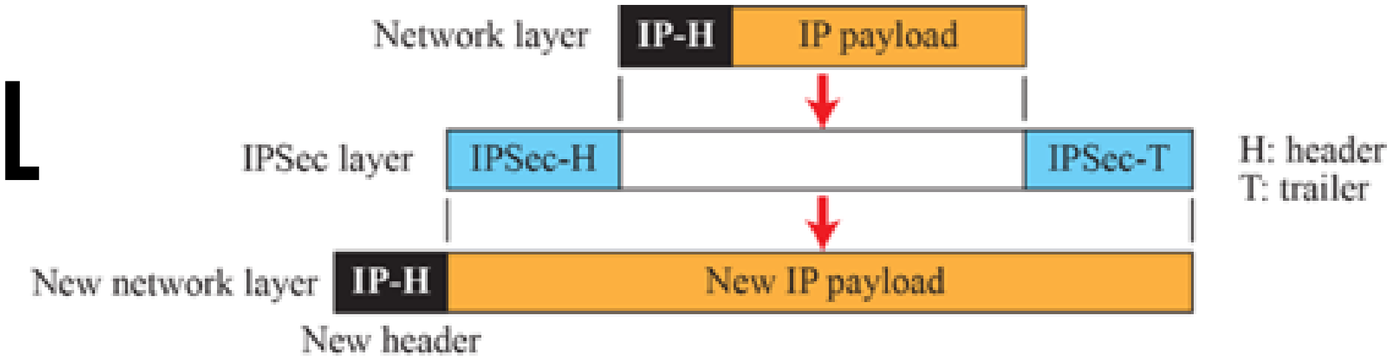


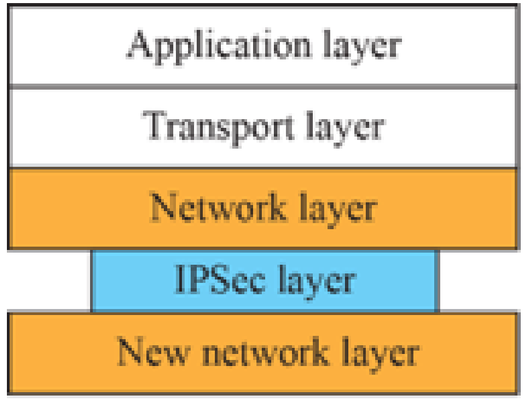


Transport mode

IPSec

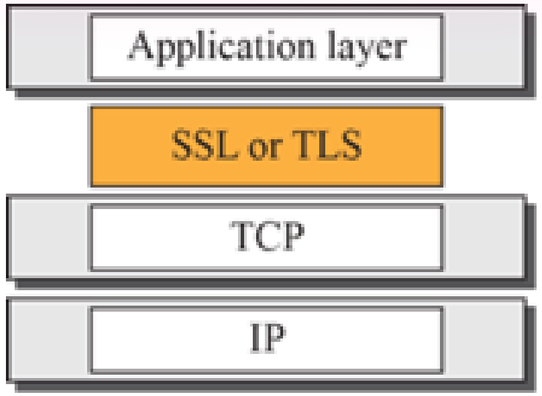
TUNNEL MODE

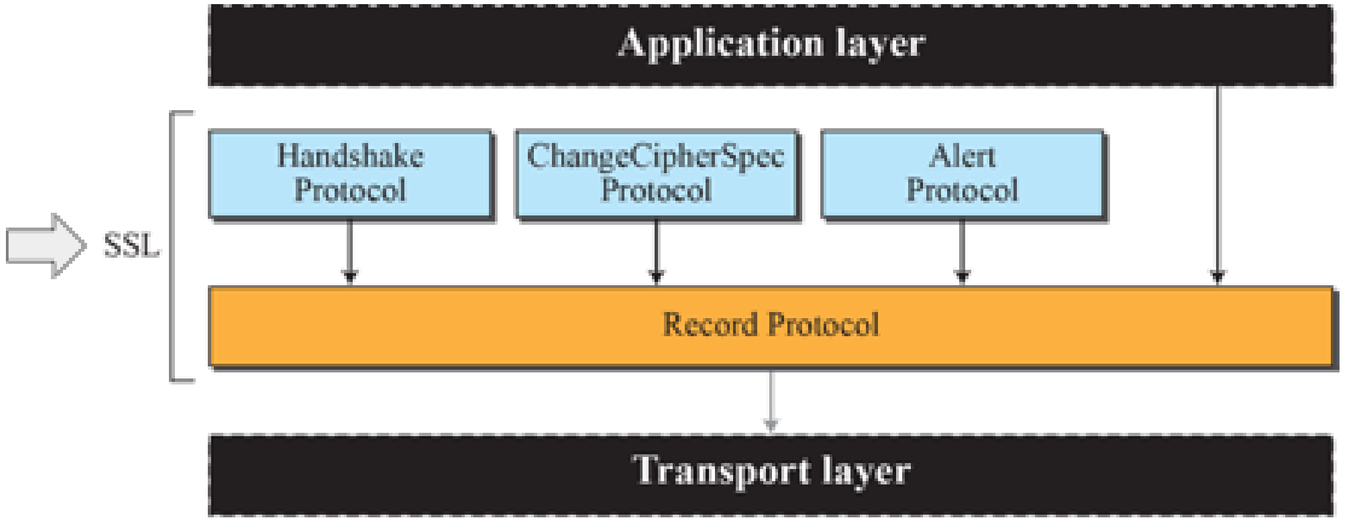




Tunnel mode

SSL ARCHITECTURE





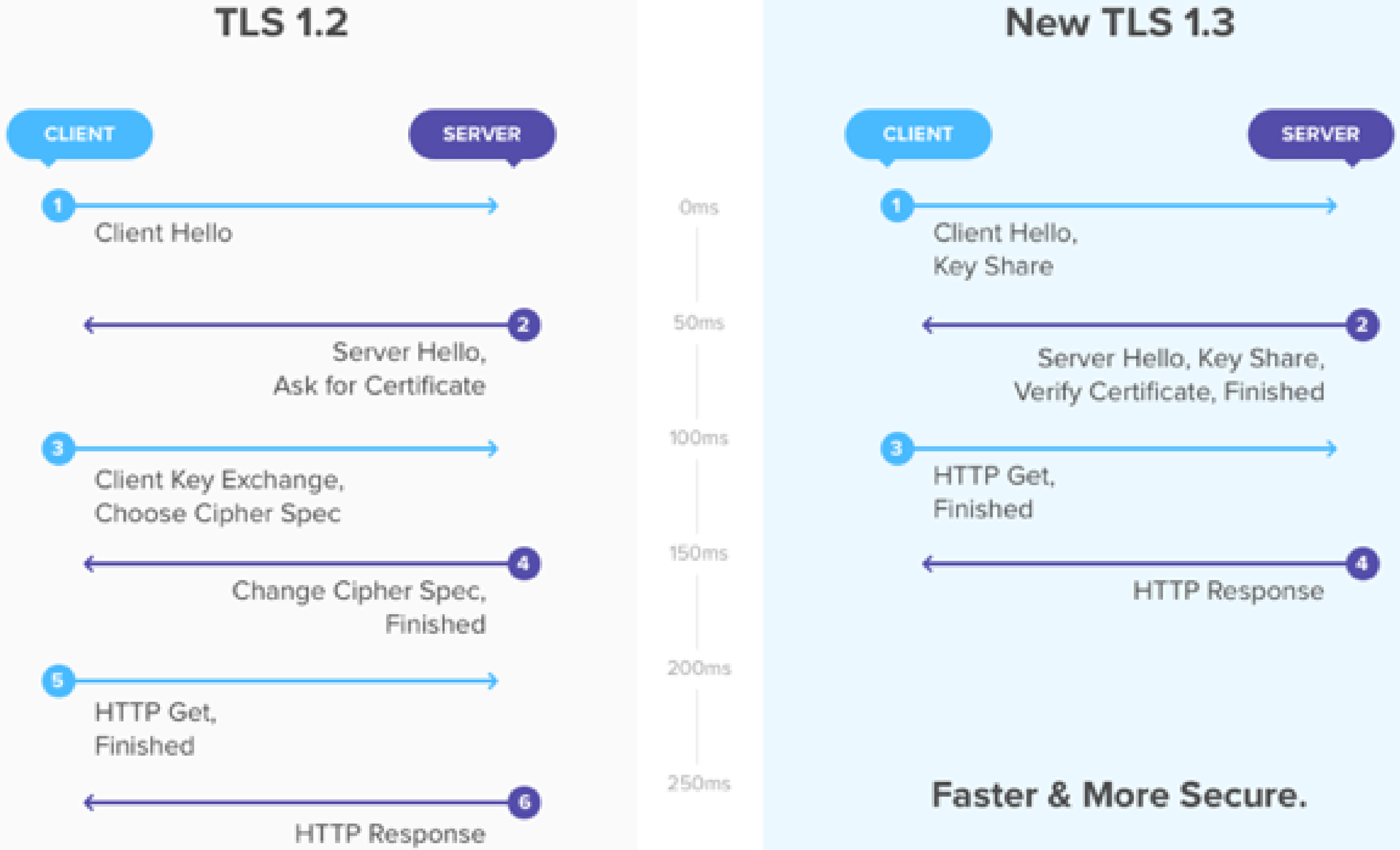
Protocol	Published
SSL 1.0	Unpublished
SSL 2.0	1995
SSL 3.0	1996
TLS 1.0	1999
TLS 1.1	2006
TLS 1.2	2008
TLS 1.3	2018

Cipher security summary

This article summarizes publicly known at
against block ciphers and stream ciphers.
there are perhaps attacks that are not pu

W Wikipedia / Oct 29, 2023

Cipher	Security claim	Best attack	Publish date	Comment
AES128	2^{128}	$2^{126.1}$ time, 2^{88} data, 2^{8} memory	2011-08-17	Independent biclique attack.[1]
AES192	2^{192}	$2^{189.7}$ time, 2^{80} data, 2^{8} memory		
AES256	2^{256}	$2^{254.4}$ time, 2^{40} data, 2^{8} memory		
Blowfish	Up to 2^{448}	4 of 16 rounds; 64-bit block is vulnerable to SWEET32 attack.	2016	Differential cryptanalysis.[2] Author of Blowfish (Bruce Schneier) recommends using Twofish instead.[3] SWEET32 attack demonstrated birthday attacks to recover plaintext with its 64-bit block size, vulnerable to protocols such as TLS, SSH, IPsec, and OpenVPN, without attacking the cipher itself.[4]
Twofish	2^{128} – 2^{256}	6 of 16 rounds (2^{256} time)	1999-10-05	Impossible differential attack.[5]
Serpent-128	2^{128}	10 of 32 rounds (2^{89} time, 2^{118} data)	2002-02-04	Linear cryptanalysis.[6]
Serpent-192	2^{192}	11 of 32 rounds (2^{187} time, 2^{118} data)		
Serpent-256	2^{256}			
DES	2^{56}	2^{39} – 2^{43} time, 2^{43} known plaintexts	2001	Linear cryptanalysis.[7] In addition, broken by brute force in 2^{56} time, no later than 1998-07-17, see EFF DES cracker.[8] Cracking hardware is available for purchase since 2006.[9]
Triple DES	2^{168}	2^{113} time, 2^{32} data, 2^{88} memory; 64-bit block is vulnerable to SWEET32 attack.	2016	Extension of the meet-in-the-middle attack. Time complexity is 2^{113} steps, but along with proposed techniques, it is estimated to be equivalent to 2^{90} single DES encryption steps. The paper also proposes other time–memory tradeoffs.[10] SWEET32 attack demonstrated birthday attacks to recover plaintext with its 64-bit block size, vulnerable to protocols such as TLS, SSH, IPsec, and OpenVPN.[4]
KASUMI	2^{128}	2^{32} time, 2^{26} data, 2^{30} memory, 4 related keys	2010-01-10	The cipher used in 3G cell phone networks. This attack takes less than two hours on a single PC, but isn't applicable to 3G due to known plaintext and related key requirements.[11]
RC4	Up to 2^{2048}	2^{20} time, $2^{16.4}$ related keys (95% success probability)	2007	Commonly known as PTW attack, it can break WEP encryption in Wi-Fi on an ordinary computer in negligible time.[12] This is an improvement of the original Fluhrer, Mantin and Shamir attack published in 2001.[13]

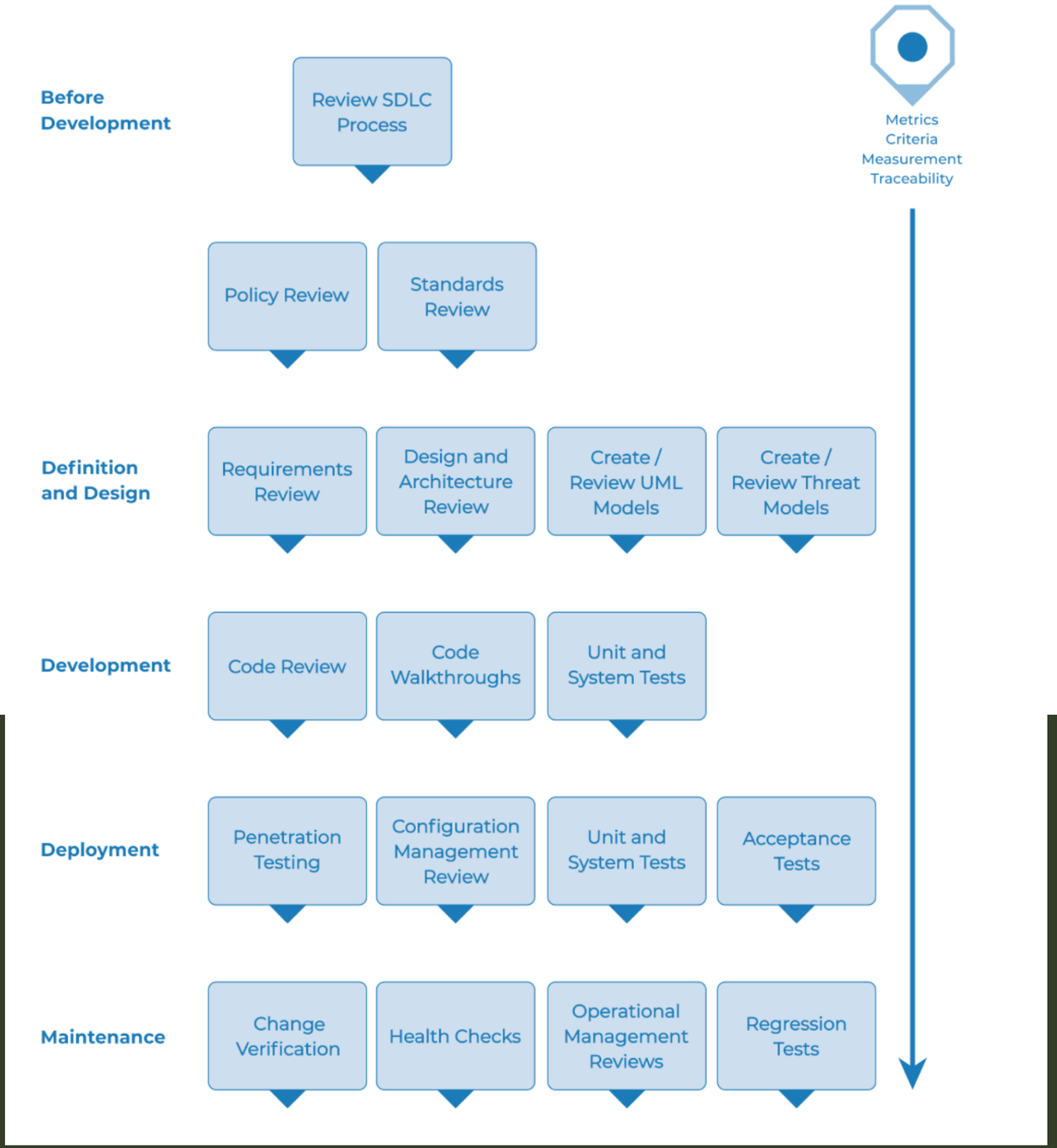

TLS 1.2
CLIENT
SERVER
1
Client Hello
2
Server Hello,
Ask for Certificate
3
Client Key Exchange,
Choose Cipher Spec
4
Change Cipher Spec,
Finished
5
HTTP Get,
Finished
6
HTTP Response
0ms
50ms
100ms
150ms
200ms
250ms
New TLS 1.3
CLIENT
SERVER
1
Client Hello,
Key Share
2
Server Hello, Key Share,
Verify Certificate, Finished
3
HTTP Get,
Finished
4
HTTP Response
Faster & More Secure.

WEB APPLICATION FIREWALL

Application firewall for HTTP applications. It applies a set of rules to an HTTP conversation.
These rules cover common attacks such as cross-site scripting (XSS) and SQL injection.

Intrusion Detection System
Intrusion Prevention System

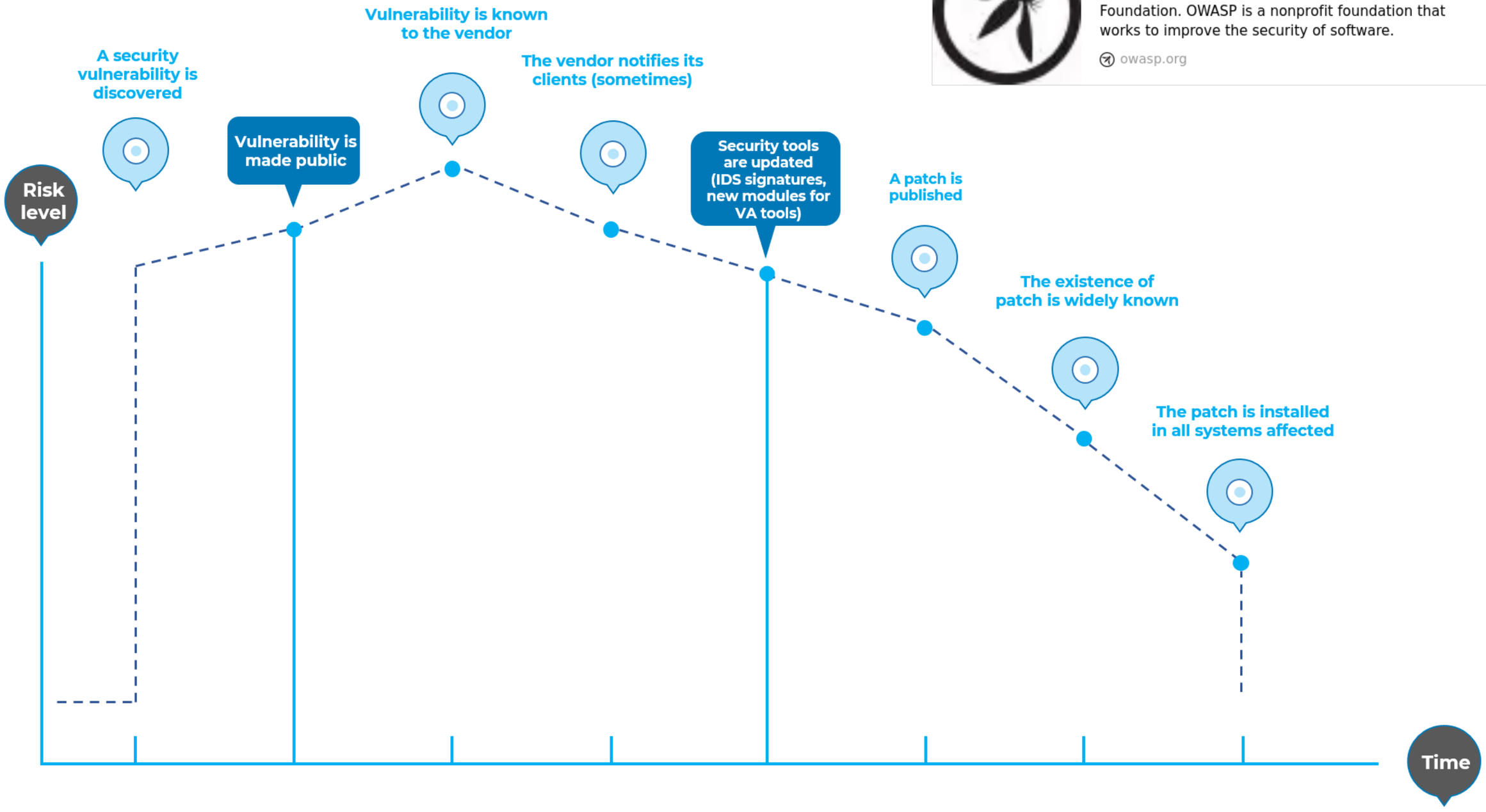
Next-Generation Intrusion Prevention System (NGIPS)



WSTG - Latest | OWASP Foundation

WSTG - Latest on the main website for The OWASP Foundation. OWASP is a nonprofit foundation that works to improve the security of software.

owasp.org



THANK YOU

FOR JOINING US

Back To Home