



UNIVERSIDADE DA CORUÑA

# Fundamentos y categorías de ataques

LSI - 2019/2020

José Manuel Vázquez Naya  
jose@udc.es

# Contenido

- Conceptos básicos y definiciones
- Categorías o tipos de ataques
- Servicios y mecanismos de seguridad
- Modelo de defensa en profundidad

# Introducción

- Seguridad Informática:

- El nombre genérico que se da al grupo de herramientas diseñadas para proteger los datos y evitar la intrusión de los hackers. (Stallings)

- Seguridad de la Información:

- Todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener:

- **Confidencialidad** (*Confidentiality*)

- **Integridad** (*Integrity*)

**(CIA)**

- **Disponibilidad** (*Availability*)

# Introducción



Extraído de <http://www.iso27000.es/download/seguridad%20informaticavsinformacion.pdf>

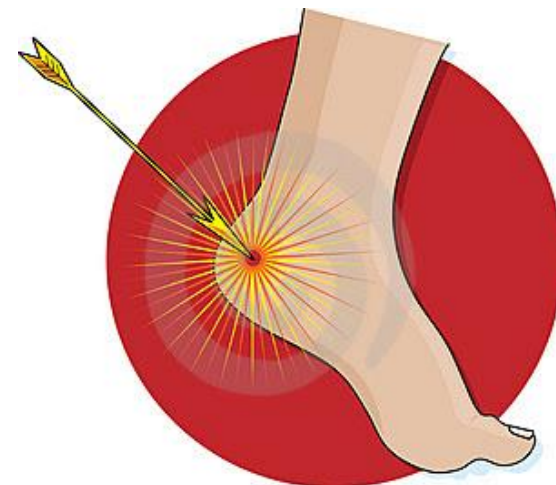
# CONCEPTOS DE SEGURIDAD

# Conceptos de seguridad

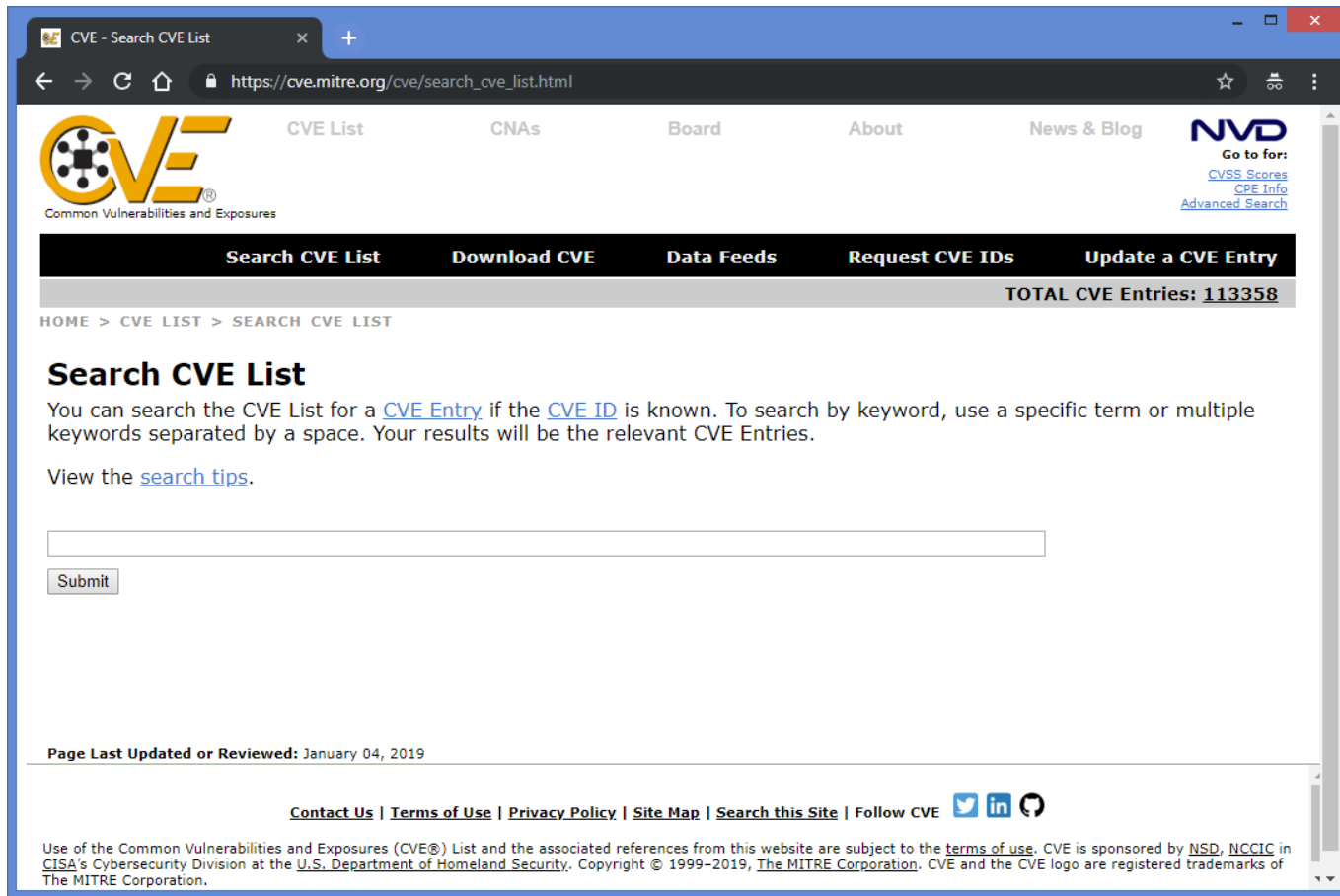
- Vulnerabilidad
- Amenaza
- Ataque

# Vulnerabilidad (*Vulnerability*)

- Debilidad de un activo o control que puede ser explotada por una **amenaza** (ISO 27000:2009. Overview and Vocabulary).
- Posibilidad de que una **amenaza** se materialice sobre un activo.
- Es una vía de **ataque** potencial.
- Ejemplos:
  - Defectos en HW o SW
    - Rowhammer, configuración por defecto, Buffer overflow, consultas no parametrizadas, ...
  - Carencia de políticas y procedimientos
    - Falta de formación en seguridad por parte de los usuarios, controles de acceso no definidos, ...



# Estándar de nomenclatura de vulnerabilidades



The screenshot shows the CVE Search CVE List page. The browser address bar displays the URL [https://cve.mitre.org/cve/search\\_cve\\_list.html](https://cve.mitre.org/cve/search_cve_list.html). The page features the CVE logo (Common Vulnerabilities and Exposures) and a navigation menu with links to CVE List, CNAs, Board, About, News & Blog, and NVD. A secondary navigation bar includes links to Search CVE List, Download CVE, Data Feeds, Request CVE IDs, and Update a CVE Entry. A banner indicates the total number of CVE entries is 113358. The main content area is titled 'Search CVE List' and provides instructions on how to search for a CVE entry. It includes a search input field and a 'Submit' button. The page footer contains contact information, terms of use, privacy policy, site map, and social media links.

CVE - Search CVE List

[https://cve.mitre.org/cve/search\\_cve\\_list.html](https://cve.mitre.org/cve/search_cve_list.html)

**CVE**  
Common Vulnerabilities and Exposures

[CVE List](#) [CNAs](#) [Board](#) [About](#) [News & Blog](#) [NVD](#)

Go to for:  
[CVSS Scores](#)  
[CPE Info](#)  
[Advanced Search](#)

[Search CVE List](#) [Download CVE](#) [Data Feeds](#) [Request CVE IDs](#) [Update a CVE Entry](#)

**TOTAL CVE Entries: 113358**

HOME > CVE LIST > SEARCH CVE LIST

## Search CVE List

You can search the CVE List for a [CVE Entry](#) if the [CVE ID](#) is known. To search by keyword, use a specific term or multiple keywords separated by a space. Your results will be the relevant CVE Entries.

View the [search tips](#).

Page Last Updated or Reviewed: January 04, 2019

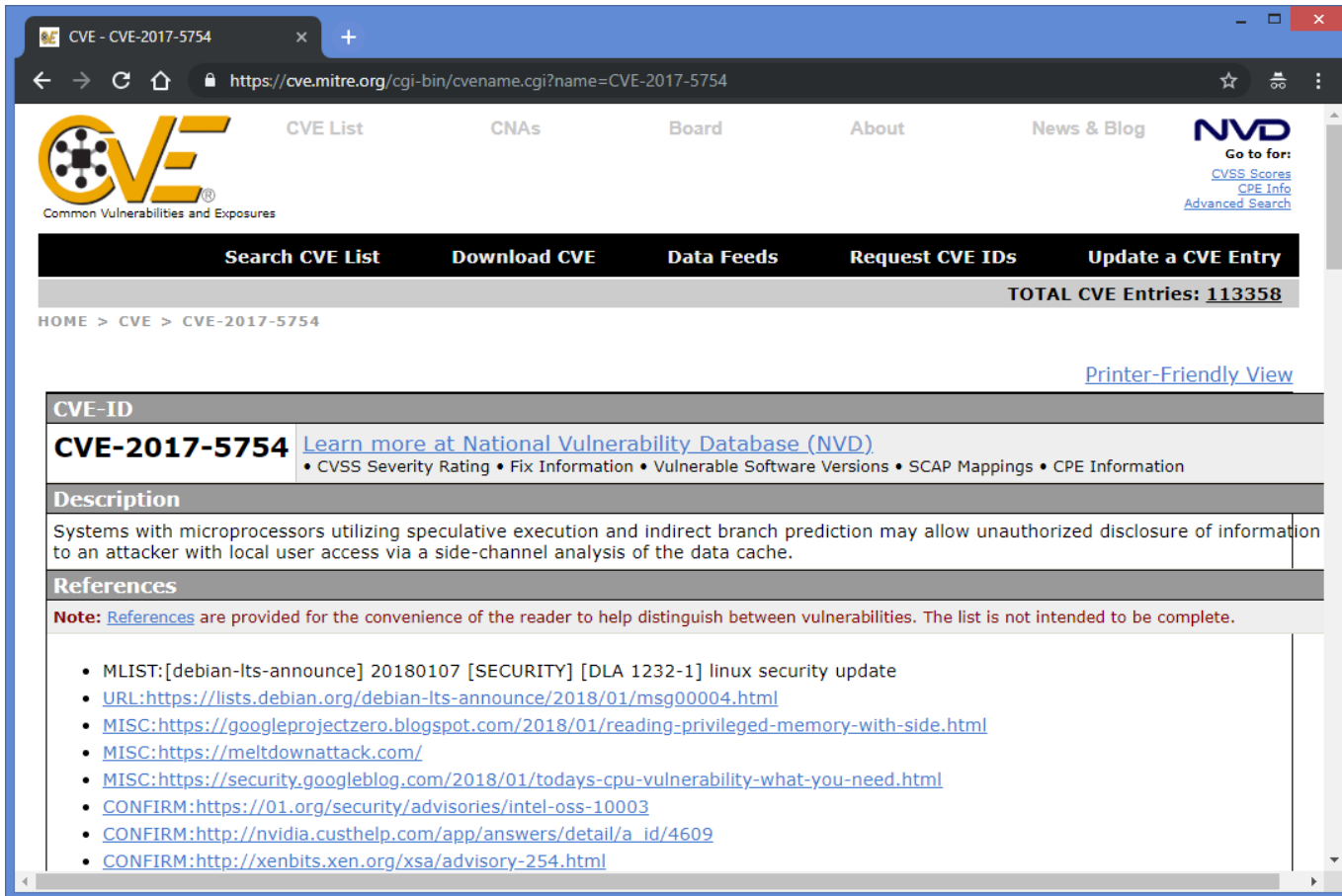
[Contact Us](#) | [Terms of Use](#) | [Privacy Policy](#) | [Site Map](#) | [Search this Site](#) | Follow CVE [Twitter](#) [LinkedIn](#) [GitHub](#)

Use of the Common Vulnerabilities and Exposures (CVE®) List and the associated references from this website are subject to the [terms of use](#). CVE is sponsored by [NSD](#), [NCCIC](#) in [CISA's](#) Cybersecurity Division at the [U.S. Department of Homeland Security](#). Copyright © 1999–2019, [The MITRE Corporation](#). CVE and the CVE logo are registered trademarks of The MITRE Corporation.

[https://cve.mitre.org/cve/search\\_cve\\_list.html](https://cve.mitre.org/cve/search_cve_list.html)



# Estándar de nomenclatura de vulnerabilidades



The screenshot shows the MITRE CVE website page for CVE-2017-5754. The browser address bar displays the URL <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5754>. The page header includes the CVE logo, navigation links (CVE List, CNAs, Board, About, News & Blog), and the NVD logo. A search bar and a list of actions (Search CVE List, Download CVE, Data Feeds, Request CVE IDs, Update a CVE Entry) are present. The total number of CVE entries is 113358. The page content for CVE-2017-5754 includes the CVE ID, a link to learn more at the National Vulnerability Database (NVD), and a description of the vulnerability. The description states: "Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis of the data cache." The References section lists several links to related information, including MLIST, URL, MISC, and CONFIRM entries.

**CVE-ID**

**CVE-2017-5754** [Learn more at National Vulnerability Database \(NVD\)](#)

- CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

**Description**

Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis of the data cache.

**References**

**Note:** [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MLIST:[debian-lts-announce] 20180107 [SECURITY] [DLA 1232-1] linux security update
- URL:<https://lists.debian.org/debian-lts-announce/2018/01/msg00004.html>
- MISC:<https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html>
- MISC:<https://meltdownattack.com/>
- MISC:<https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html>
- CONFIRM:<https://01.org/security/advisories/intel-oss-10003>
- CONFIRM:[http://nvidia.custhelp.com/app/answers/detail/a\\_id/4609](http://nvidia.custhelp.com/app/answers/detail/a_id/4609)
- CONFIRM:<http://xenbits.xen.org/xsa/advisory-254.html>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5754>

# Estándar de nomenclatura de vulnerabilidades

The screenshot shows the NIST NVD website interface. The header includes the NIST logo, 'Information Technology Laboratory', 'NATIONAL VULNERABILITY DATABASE', and an 'NVD MENU' button. The main content area is titled 'VULNERABILITIES' and features a 'CVE-2017-5754 Detail' section. This section includes a 'MODIFIED' status note, a 'Current Description' of a side-channel analysis vulnerability, and a 'QUICK INFO' sidebar with details like 'CVE Dictionary Entry: CVE-2017-5754', 'NVD Published Date: 01/04/2018', and 'NVD Last Modified: 12/07/2018'. Below the description, there is an 'Impact' section with two columns of severity metrics: CVSS v3.0 and CVSS v2.0. The CVSS v3.0 metrics include a Base Score of 5.6 (MEDIUM), a Vector of AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N, an Impact Score of 4.0, and an Exploitability Score of 1.1. The CVSS v2.0 metrics include a Base Score of 4.7 (MEDIUM), a Vector of (AV:L/AC:M/Au:N/C:C/I:N/A:N), an Impact Subscore of 6.9, and an Exploitability Subscore of 3.4. The page also includes a 'Source: MITRE' and a 'Description Last Modified: 01/04/2018' date.

**CVE-2017-5754 Detail**

**MODIFIED**

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

**Current Description**

Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis of the data cache.

**Source:** MITRE  
**Description Last Modified:** 01/04/2018  
[View Analysis Description](#)

**QUICK INFO**

**CVE Dictionary Entry:**  
CVE-2017-5754  
**NVD Published Date:**  
01/04/2018  
**NVD Last Modified:**  
12/07/2018

**Impact**

| CVSS v3.0 Severity and Metrics:                                | CVSS v2.0 Severity and Metrics:                         |
|--|---|
| <b>Base Score:</b> 5.6 MEDIUM                                  | <b>Base Score:</b> 4.7 MEDIUM                           |
| <b>Vector:</b> AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N (V3 legend) | <b>Vector:</b> (AV:L/AC:M/Au:N/C:C/I:N/A:N) (V2 legend) |
| <b>Impact Score:</b> 4.0                                       | <b>Impact Subscore:</b> 6.9                             |
| <b>Exploitability Score:</b> 1.1                               | <b>Exploitability Subscore:</b> 3.4                     |

**Attack Vector (AV):** Local  
**Attack Complexity (AC):** High  
**Privileges Required (PR):** Low

**Access Vector (AV):** Local  
**Access Complexity (AC):** Medium  
**Authentication (Au):** None

<https://nvd.nist.gov/vuln/detail/CVE-2017-5754>

# Estándar de nomenclatura de vulnerabilidades

- *Common Vulnerabilities and Exposures* (Vulnerabilidades y “Exposiciones” comunes), **CVE**, es una lista de vulnerabilidades de ciberseguridad conocidas públicamente.
- Las entradas de CVE se usan en numerosos productos y servicios de ciberseguridad de todo el mundo, incluyendo la National Vulnerability Database (NVD).
- CVE está patrocinado por varios organismos estadounidenses y es mantenido por la corporación MITRE.
- Su uso es público.
- CVE no contiene información sobre el riesgo, impacto, información sobre cómo corregir la vulnerabilidad o detalles técnicos. La NVD proporciona esta información sobre las entradas de CVE.

# Estándar de nomenclatura de vulnerabilidades

- **Para cada vulnerabilidad, el CVE tiene:** un identificador numérico (CVE-ID), una descripción, y al menos una referencia pública

## CVE-ID Syntax Change

| Old Syntax   | New Syntax  |
|--|---|
| <b>CVE-YYYY-NNNN</b><br>4 fixed digits, supports a maximum of 9,999 unique identifiers per year. | <b>CVE-YYYY-NNNN...N</b><br>4-digit minimum and no maximum, provides for additional capacity each year when needed. |
| Fixed 4-Digit Examples<br><b>CVE-1999-0067</b><br><b>CVE-2005-4873</b><br><b>CVE-2012-0158</b>   | Arbitrary Digits Examples<br><b>CVE-2014-0001</b><br><b>CVE-2014-12345</b><br><b>CVE-2014-7654321</b>               |


YYYY indicates year the ID is issued to a CVE Numbering Authority (CNA) or published.

**Implementation date: January 1, 2014**


Source: <http://cve.mitre.org>

NVD - Home
+
https://nvd.nist.gov
NIST
NVD MENU
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NVD


General +
Vulnerabilities +
Vulnerability Metrics +
Products +
Configurations (CCE)
Contact NVD
Other Sites +
Search +



### JSON Feed 1.0 Released



### CPE Ranges



### Vulnerability Visualizations

The NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

#### Last 20 Scored Vulnerability IDs & Summaries

**CVE-2010-5312** — Cross-site scripting (XSS) vulnerability in jquery.ui.dialog.js in the Dialog widget in jQuery UI before 1.10.0 allows remote attackers to inject arbitrary web script or HTML via the title option.

**Published:** November 24, 2014; 11:59:00 AM -05:00

**CVE-2016-7103** — Cross-site scripting (XSS) vulnerability in jQuery UI before 1.12.0 might allow remote attackers to inject arbitrary web script or HTML via the closeText parameter of the dialog function.

**Published:** March 15, 2017; 12:59:00 PM -04:00

#### CVSS Severity

V2: **4.3 MEDIUM**

V3: **6.1 MEDIUM**

V2: **4.3 MEDIUM**

<https://nvd.nist.gov/>

## Search Vulnerability Database

Try a product name, vendor name, CVE name, or an OVAL query.

NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

### Search Type

☐ Basic ☒ Advanced

### Results Type

☒ Overview ☐ Statistics

### Keyword Search

☐ Exact Match

### CVE Identifier

### Category (CWE)

Any..... ▾

### CPE Name

Begin typing your keyword to find the CPE.

[Reset CPE Info](#)

### Vendor

### Product

### CVSS Metrics

☒ Version 3 ☐ Version 2 ☐ All

#### Severity Score Range

Any  
None (0.0)  
Low (0.1-3.9)  
Medium (4-6.9)  
High (7-8.9)  
Critical (9-10)

#### Attack Vector (AV)

Any  
Network (N)  
Adjacent (A)  
Local (L)  
Physical (P)

#### Attack Complexity (AC)

Any  
Low (L)  
High (H)

#### Privileges Required (PR)

Any  
None (N)  
Low (L)  
High (H)

#### User Interaction (UI)

Any  
None (N)  
Required (R)

#### Scope (S)

Any  
Unchanged (U)  
Changed (C)

#### Confidentiality (C)

Any  
None (N)  
Low (L)  
High (H)



#### Integrity (I)

Any  
None (N)  
Low (L)  
High (H)

#### Availability (A)

Any  
None (N)  
Low (L)  
High (H)

### Published Date Range

//  // 

### Last Modified Date Range

//  // 

### Contains HyperLinks

- ☐ US-CERT Technical Alerts  
☐ US-CERT Vulnerability Notes  
☐ OVAL Queries

[Search](#)

[Reset](#)

<https://nvd.nist.gov/vuln/search>



# Gravedad de una vulnerabilidad

- Common Vulnerability Scoring System

- v2.0

- v3.0



# Algunos ejemplos de vulnerabilidades críticas

- Shellshock (CVE-2014-6271 y otras)
- Heartbleed (CVE-2014-0160)
- Poodle (CVE-2014-3566)



# Algunas más recientes...

- Meltdown (CVE-2017-5754)
- Spectre (CVE-2017-5753 and CVE-2017-5715)
- Krack attacks (múltiples CVEs asignados)

**CERTSI****CERT de Seguridad e Industria**

♦ Blog

♦ [Alerta Temprana](#)[Avisos de seguridad](#)[Vulnerabilidades](#)[Bitácora de ciberseguridad](#)

♦ Guías y Estudios

♦ Infraestructuras críticas

♦ Respuesta y Soporte

**Encuesta de calidad de contenidos**

¿Ha encontrado en el portal web los contenidos que buscaba?

[Participa en nuestra encuesta](#)**Buscador de vulnerabilidades**

Para realizar una búsqueda simplemente elija las opciones que desee del formulario de búsquedas. Por ejemplo puede buscar todas las vulnerabilidades de un determinado software que puedan ser explotadas remotamente.

También puede buscar por palabras clave, por fabricante y producto, tipo de vulnerabilidad, tipo de ataque, etc. Todos los criterios son excluyentes, se deben cumplir todos en el resultado de la búsqueda.

Para obtener más información sobre esta base de datos de vulnerabilidades en español, o entender en detalle cada criterio de búsqueda, pulse en el formulario el campo 'Ayuda' asociado.

Texto: **Fecha de publicación**Desde:  (dd/mm/aaaa)Hasta:  (dd/mm/aaaa)

Debe seleccionar un fabricante para cargar los productos

Fabricante: [Ayuda](#)Producto: [Ayuda](#)Gravedad: [Ayuda](#)Tipo de Vulnerabilidad: [Ayuda](#)

Con enlace al parche:

Filas: [Buscar](#)[Limpiar](#)

En colaboración con NVD

**National Vulnerability Database** **NIST**  
a comprehensive cyber vulnerability resource  
National Institute of Standards and Technology

# Zero-day (0 day)

- Vulnerabilidades Zero-day

- No conocidas hasta el momento
- En el momento de su publicación:
  - Los desarrolladores han tenido cero días para parchear la vulnerabilidad
  - El vendedor no ha podido proporcionar un parche oficial
  - Los administradores han tenido cero días para protegerse de la vulnerabilidad
- Dejan de ser Zero-day una vez el parche esté disponible

- Ataques Zero-day:

- Explotan una vulnerabilidad Zero-day

# Zero-day (0 day)

- The Zero Day Initiative (ZDI)

- <http://www.zerodayinitiative.com/>

- Zerodium

- <https://zerodium.com/>

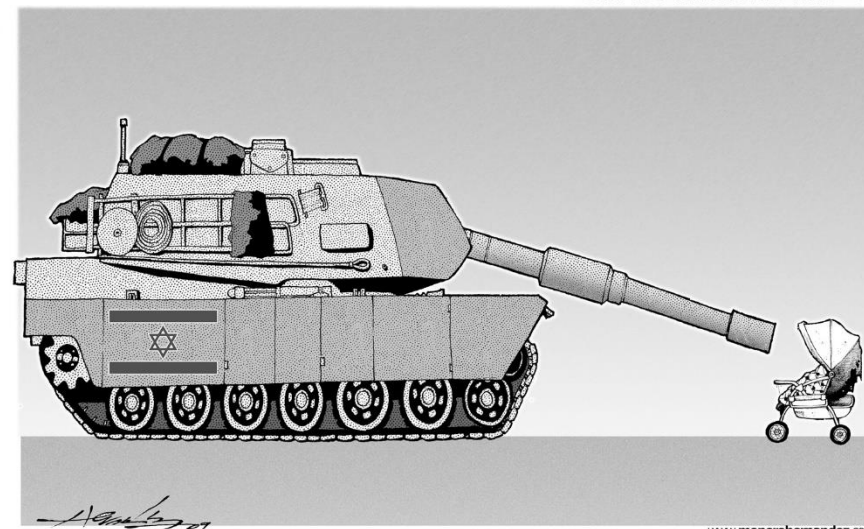
- Mitnick's Exploit Exchange

- <https://www.mitnicksecurity.com/shopping/absolute-zero-day-exploit-exchange>

# Amenaza (*Threat*)

- Una posibilidad de violación de la seguridad, que existe cuando se da una circunstancia, capacidad, acción o evento que pudiera romper la seguridad y causar perjuicio. Es decir, una amenaza es un peligro posible que podría explotar una **vulnerabilidad**. (RFC 2828)
- Posible causa de un incidente no deseado, que puede resultar en daños a un sistema u organización. (ISO 27000:2009. Overview and Vocabulary)

❖ UNA SERIA AMENAZA



# Amenaza (*Threat*)

- REVERSE TROJAN (Server-to-Client)
  - TIME BOMB
  - BOTS
  - KEY LOGGERS
  - SNIFFERS
  - BACKDOORS
  - ROOTKITS
  - VIRUS
  - WORM
  - SPYWARE
  - TROJAN HORSE
- 
- Más en: <https://www.owasp.org/index.php/Category:Threat>



# Amenaza

## ■ Stuxnet

- Gusano/virus informático descubierto en junio de 2010
- Primer gusano conocido que espía y reprograma sistemas industriales, en concreto sistemas SCADA de control y monitorización de procesos, pudiendo afectar a infraestructuras críticas como centrales nucleares
- El 60% de los ordenadores contaminados por el gusano se encuentran en Irán
- El objetivo más probable del gusano pudieron ser infraestructuras de alto valor pertenecientes a Irán y con sistemas de control de Siemens
- Algunos medios han atribuido su autoría a los servicios secretos estadounidenses e israelíes



# Ataque (*Attack*)

- Cualquier **acción** que comprometa la seguridad de la información de una organización (Stallings).
- Un asalto a la seguridad del sistema, derivado de una **amenaza** inteligente; es decir, un acto inteligente y deliberado (especialmente en el sentido de método o técnica) para eludir los servicios de seguridad y violar la política de seguridad de un sistema (RFC 2828).



# Ataque (*Attack*)

- Brute Force: Fuerza Bruta
- Cache Poisoning: Envenenamiento de Caché
- DNS Poisoning: Envenenamiento de DNS
- Cross-Site Request Forgery (CSRF) o Falsificación de petición en sitios cruzados
- Cross-Site Scripting (XSS) o Secuencias de comandos en sitios cruzados
- Denial of Service (DoS)
- LDAP injection
- Man-in-the-middle
- Session hijacking attack
- Sniffing Attacks
- SQL Injection: Inyección SQL
  
- Más en: <https://www.owasp.org/index.php/Category:Attack>



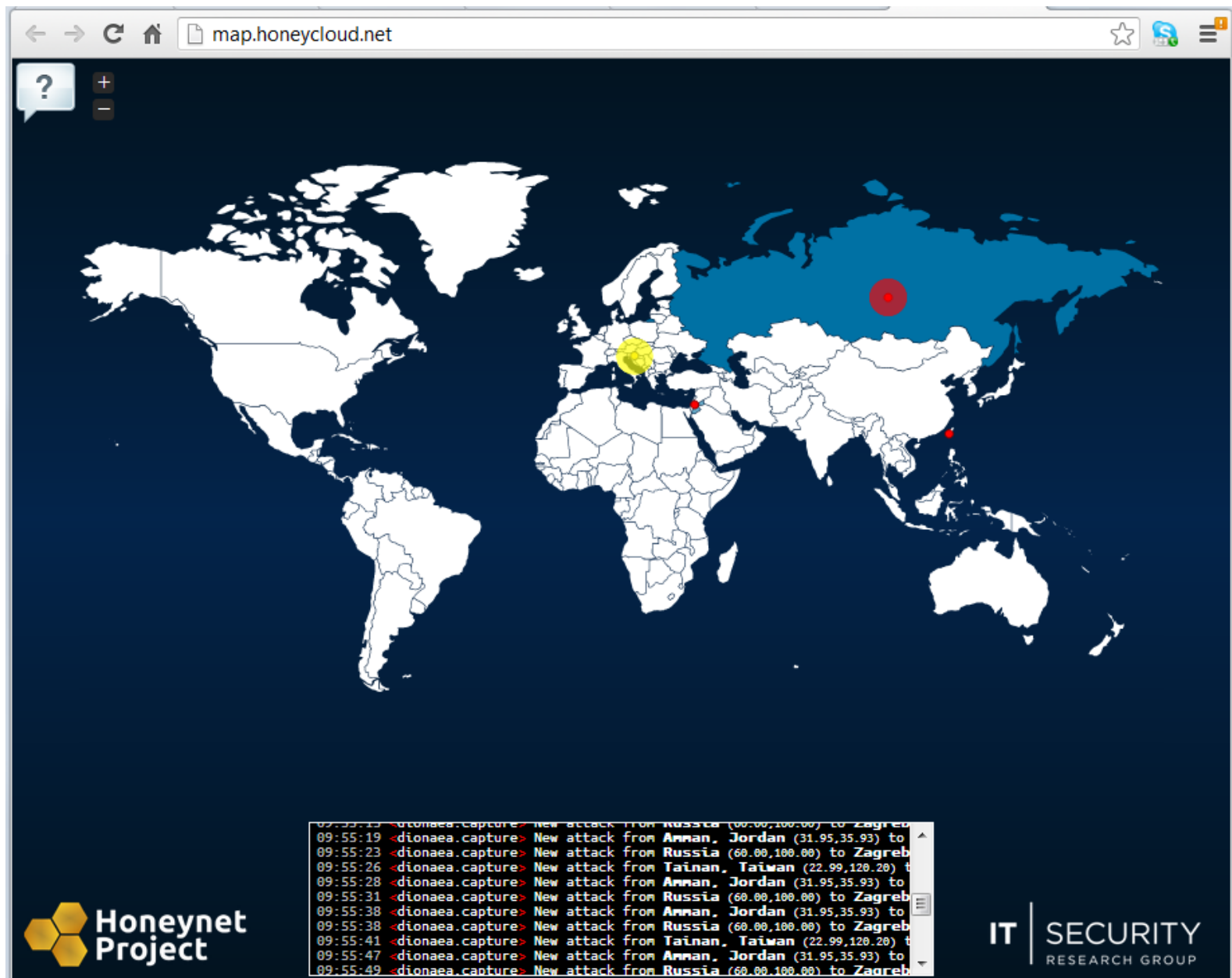
# Aclarando conceptos...

- Un sistema de autenticación que permite un número ilimitado de intentos <- VULNERABILIDAD
- Un software que permite realizar pruebas de autenticación de forma automática (fuerza bruta) <- AMENAZA
- Ejecutar el software para que actúe sobre un sistema <- ATAQUE



# OWASP Top 10 - 2017

Los diez riesgos más críticos en Aplicaciones Web



# CYBERTHREAT REAL-TIME MAP

EN

Download Trial

MAP STATISTICS DATA SOURCES BUZZ WIDGET

Share f t g+



[ENABLE FILTERS]

Total notifications: **142,093** of which **64,444** single ip and **77,649** 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                   |
|------------|------------------------|---------|--|---|---|-------------------------------------|----------|------------------------|
| 2013/01/24 | HackEd By LaMIN3 DK    | M       |   | ★   |   | proteccioncivil.hidalgo.gob.mx...   | Linux    | <a href="#">mirror</a> |
| 2013/01/24 | HackEd By LaMIN3 DK    | M       |   | ★   |   | gobierno.hidalgo.gob.mx/images...   | Linux    | <a href="#">mirror</a> |
| 2013/01/24 | HackEd By LaMIN3 DK    | M       |   | ★   |   | coordsephorganismosinternacion...   | Linux    | <a href="#">mirror</a> |
| 2013/01/24 | HackEd By LaMIN3 DK    | M       |   | ★   |   | pruebaomig.hidalgo.gob.mx/imag...   | Linux    | <a href="#">mirror</a> |
| 2013/01/24 | HackEd By LaMIN3 DK    | M       |   | ★   |   | portalhidalgo1.hidalgo.gob.mx/...   | Linux    | <a href="#">mirror</a> |
| 2013/01/24 | HackEd By LaMIN3 DK    |         |   | ★   |   | artesanias.hidalgo.gob.mx/imag...   | Linux    | <a href="#">mirror</a> |
| 2013/01/24 | 越南国家首相                 | M       |   | ★   |   | www.ls93.gov.cn/1937cN.html         | Win 2003 | <a href="#">mirror</a> |
| 2013/01/24 | 越南国家首相                 | M       |   | ★   |   | wsjd.klmy.gov.cn/1937cN.html        | Win 2003 | <a href="#">mirror</a> |
| 2013/01/24 | Ashiyane Security Team | Digital | M  | R   |    | ★ technotrain.agritech.doae.go.t... | Linux    | <a href="#">mirror</a> |
| 2013/01/24 | Ashiyane Security Team | Digital |  | R   |    | ★ www.agritech.doae.go.th/km/cry... | Linux    | <a href="#">mirror</a> |
| 2013/01/24 | ArTiN                  |         | R  |    | ★   | zgh.songjiang.gov.cn/404.html       | Win 2003 | <a href="#">mirror</a> |
| 2013/01/24 | ArTiN                  |         | R  |    | ★   | timebank.njyjdj.gov.cn/404.html     | Win 2003 | <a href="#">mirror</a> |
| 2013/01/24 | ArTiN                  |         | R  |    | ★   | dulich.sotuphapninhbinh.gov.vn...   | Win 2003 | <a href="#">mirror</a> |
| 2013/01/24 | ulow                   | M       |   | ★   |   | www.rzguotu.gov.cn/a.htm            | Win 2003 | <a href="#">mirror</a> |
| 2013/01/24 | HighTech               | M       |   | ★   |   | finance.ajk.gov.pk/ck.htm           | Win 2003 | <a href="#">mirror</a> |
| 2013/01/24 | HighTech               | M       |   | ★   |   | agriculture.ajk.gov.pk/ck.htm       | Win 2003 | <a href="#">mirror</a> |
| 2013/01/24 | HighTech               | H       |   | ★   |   | anaissenapegs2011.cariri.ufc.br     | Linux    | <a href="#">mirror</a> |
| 2013/01/24 | HighTech               | M       |   | ★   |   | www.senadocatamarca.gob.ar/ck.htm   | Linux    | <a href="#">mirror</a> |
| 2013/01/24 | ArTiN                  | M       |   | ★   |   | www.issirfa.cnr.it/download/x.htm   | Linux    | <a href="#">mirror</a> |
| 2013/01/24 | ArTiN                  | M       |   | ★   |   | www.igag.cnr.it/2ridente/x.htm      | Linux    | <a href="#">mirror</a> |
| 2013/01/24 | SA3D HaCk3D            |         |  | ★   |   | www.arsam.am.gov.br/x.php           | Linux    | <a href="#">mirror</a> |
| 2013/01/24 | SLYHACKER              | H       | M  | R   |  | ★ www.sema.gov.lk                   | Win 2003 | <a href="#">mirror</a> |
| 2013/01/24 | SLYHACKER              | H       | M  |  | ★   | www.epf.gov.lk                      | Win 2003 | <a href="#">mirror</a> |
| 2013/01/24 | ArTiN                  | H       | M  |  | ★   | www.seas-era.cnr.it                 | Linux    | <a href="#">mirror</a> |
| 2013/01/24 | ArTiN                  | H       | M  |  | ★   | www.dsp.cnr.it                      | Linux    | <a href="#">mirror</a> |

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

**DISCLAIMER:** all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified **anonymously** to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents. [Read more](#)

# **CATEGORÍAS O TIPOS DE ATAQUES**



# Tipos de ataques

- X.800 y RFC 2828 distinguen
  - **Ataques pasivos**
  - **Ataques activos**



# Ataques pasivos

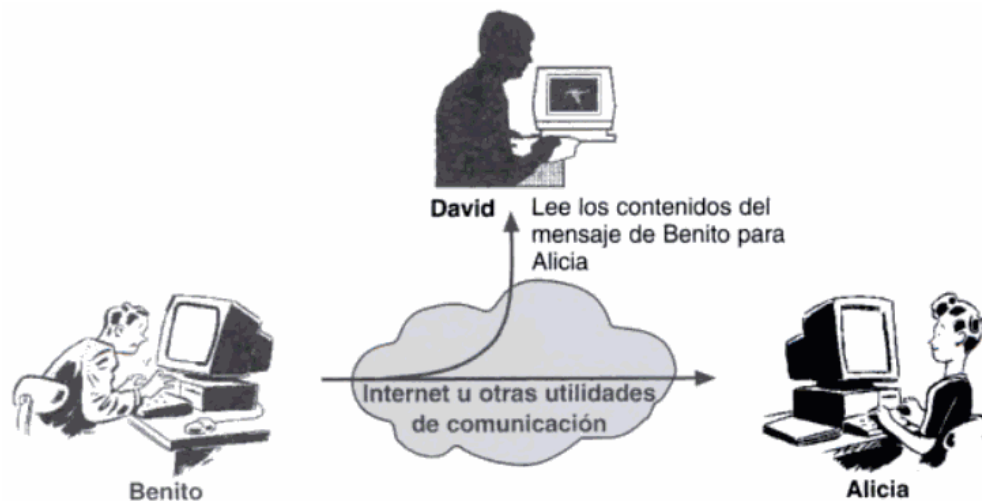
- Un **ataque pasivo** intenta conocer o hacer uso de información del sistema, pero no afecta a los recursos del mismo
- Los ataques pasivos se dan en forma de **escucha** o de observación no autorizada de las transmisiones. El objetivo del oponente es obtener información que se esté transmitiendo

# Ataques pasivos

- Muy difíciles de detectar, ya que no implican alteraciones en los datos
- Contra estos ataques se debe poner más énfasis en la **prevención** que en la detección
- Posible solución: **cifrado**

# Ataques pasivos

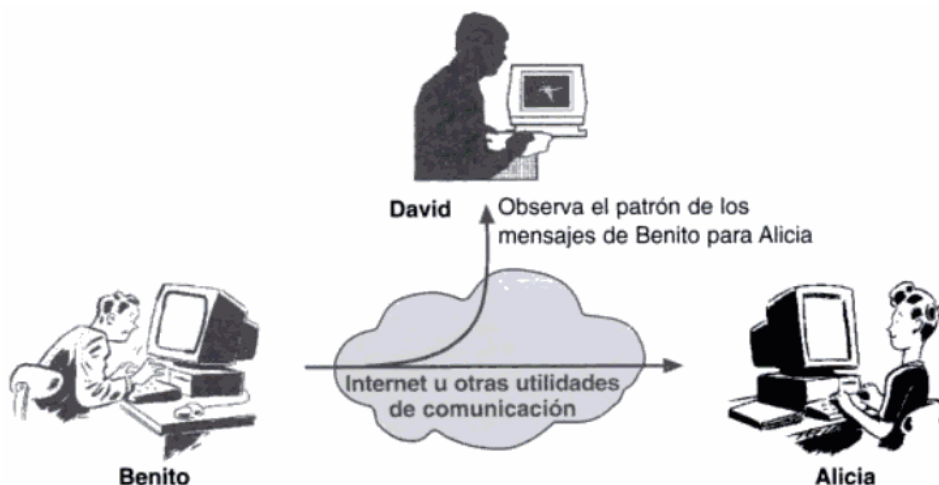
- **Obtención del contenido del mensaje**



# Ataques pasivos

## ■ Análisis del tráfico

- Aún con protección mediante cifrado, un oponente puede observar el patrón de los mensajes, determinar la **localización** y la **identidad** de los servidores que se comunican y descubrir la **frecuencia** y la **longitud** de los mensajes que se están intercambiando.
- Esta información puede ser útil para averiguar la naturaleza de la comunicación que está teniendo lugar.



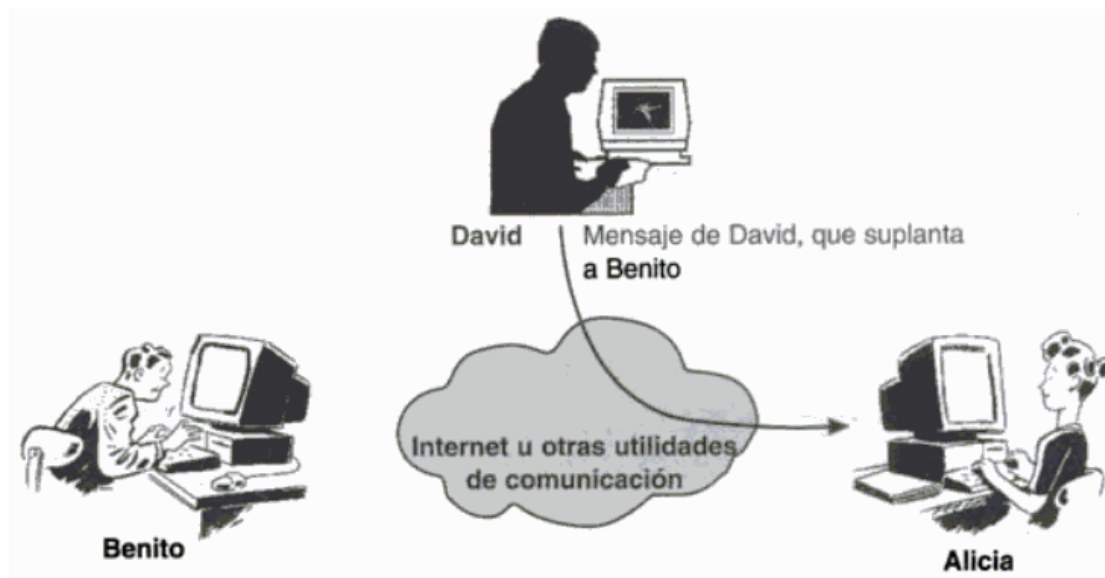
# Ataques activos

- Intentan alterar los recursos del sistema o afectar a su funcionamiento
- Implican alguna modificación del flujo de datos o la creación de un flujo falso
- Presentan características opuestas a los pasivos:
  - Son difíciles de prevenir por completo
  - El objetivo es **detectarlos** y recuperarse de ellos
    - La detección tiene efecto disuasivo -> contribuye a la prevención
- Se pueden dividir en cuatro categorías

# Ataques activos

## ■ Suplantación de identidad

- Se produce cuando una entidad finge ser otra
- Un ataque de este tipo incluye habitualmente una de las otras formas de ataque activo. Por ejemplo, las secuencias de autenticación pueden ser capturadas y repetidas después de que una secuencia válida haya tenido lugar



# Ataques activos

## ■ Repetición

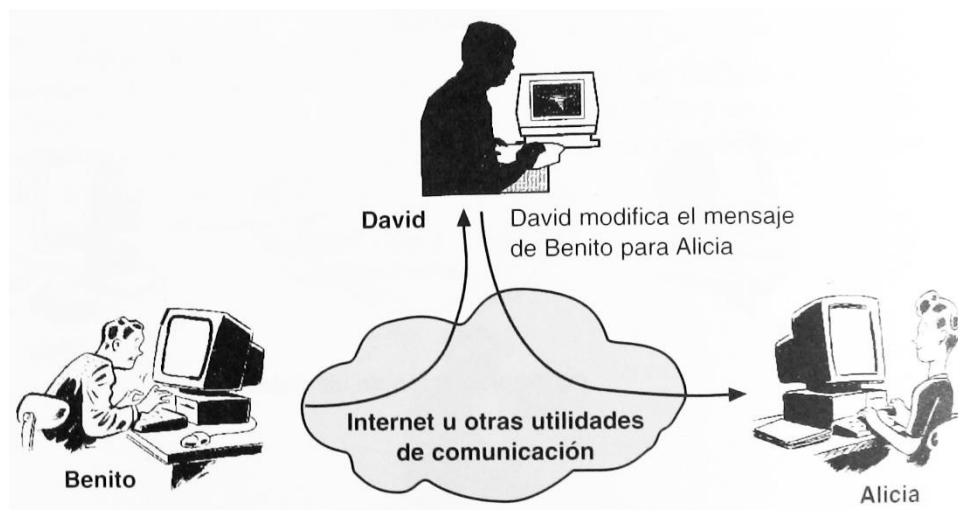
- Implica la captura pasiva de una unidad de datos y su retransmisión posterior para producir un efecto no autorizado



# Ataques activos

## ■ Modificación de mensajes

- Una parte de un mensaje es alterada, o los mensajes se han retrasado o reordenado, para producir un efecto no autorizado

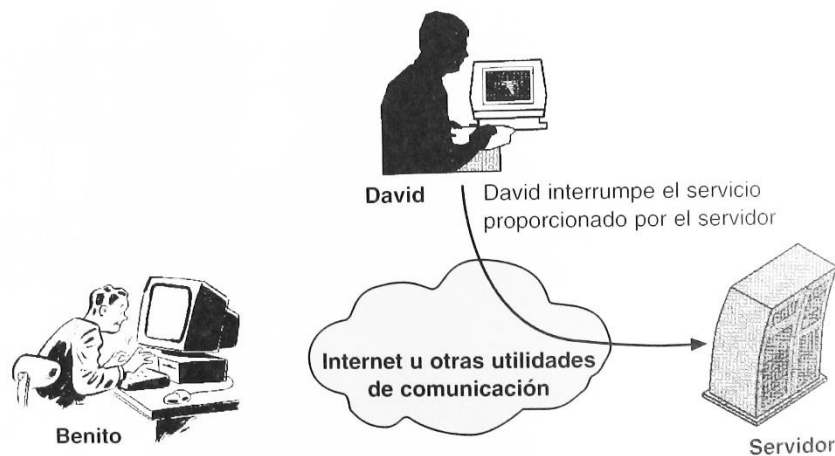




# Ataques activos

## ■ Interrupción del servicio

- Impide el uso o la gestión normal de las utilidades de comunicación



# Tipos de ataques: otra clasificación

- Ataques sobre la **identidad** de las entidades:
  - Interceptación
  - Suplantación
- Ataques sobre la **información**:
  - Revelación
  - Reenvío
  - Manipulación
  - Repudio
- Ataques sobre los **servicios**:
  - Negación del servicio



# **SERVICIOS Y MECANISMOS DE SEGURIDAD**



# Servicios de seguridad

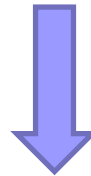
- Un servicio proporcionado por una capa de protocolo, que garantiza la seguridad adecuada de los sistemas y de las transferencias de datos (X.800)
- Un servicio de procesamiento o de comunicación proporcionado por un sistema para dar un tipo especial de protección a los recursos del sistema; **los servicios de seguridad implementan políticas de seguridad y son implementados, a su vez, por mecanismos de seguridad** (RFC 2828)

**Mecanismos de seguridad**  
(cifrado, firma digital, ...)



implementan

**Servicios de seguridad**  
(autenticación, control de acceso, ...)



implementan

**Políticas de seguridad**

# Servicios de seguridad (X.800)

## ■ **Autenticación** (*Authentication*)

- Garantiza que alguien es quien dice ser (auténtico)
- M: login/password, huella dactilar, certificado digital, ...

## ■ **Control de acceso** (*Access Control*)

- Evita el acceso no autorizado a un recurso
- M: ACLs

## ■ **Confidencialidad de los datos** (*Data confidentiality*)

- Protección de los datos (y del flujo de tráfico) de su revelación no autorizada
- M: cifrado

# Servicios de seguridad (X.800)

## ■ **Integridad de los datos** (*Data integrity*)

- Garantiza que los mensajes se reciben tal y como son enviados (sin duplicación, inserción, modificación, reordenación ni destrucción)
- M: hash, firma digital

## ■ **No repudio** (*Non-repudiation*)

- Evita que emisor o receptor nieguen la transmisión o la recepción de un mensaje, respectivamente
- M: firma digital, notaría

# Más servicios de seguridad (OO.AA.)

## ■ **Disponibilidad** (*Availability*)

- ☐ Evita que se interrumpa el servicio
- ☐ M: duplicación de servicios, discos en RAID, fuentes de alimentación redundantes, servidores en clúster, etc.



# Mecanismos de seguridad

- Característica diseñada para detectar, prevenir o recuperarse de un ataque
- No hay un único mecanismo que soporte todos los servicios de seguridad requeridos
- Sin embargo, hay un elemento que es común a muchos de los mecanismos: las **técnicas criptográficas**

# Mecanismos de seguridad (X.800)

- **Específicos** (pueden ser incorporados en la capa de protocolo adecuada):
  - Cifrado, Firma digital, Control de acceso, Integridad de los datos, Intercambio de autenticación, Relleno del tráfico, Control de enrutamiento y Notarización
- **Generales** (no son específicos de ninguna capa de protocolo o sistema de seguridad OSI en particular):
  - Funcionalidad fiable, Etiquetas de seguridad, Detección de acciones, Informe para la auditoría de seguridad y Recuperación de la seguridad

# Servicios vs. ataques

|                   | Ataques pasivos         |                     | Ataques activos |            |              |              |
|-------------------|-------------------------|---------------------|-----------------|------------|--------------|--------------|
|                   | Obtención del Contenido | Análisis de Tráfico | Suplantación    | Repetición | Modificación | Interrupción |
| Autenticación     |                         |                     | ✓               |            |              |              |
| Control de Acceso |                         |                     | ✓               |            |              |              |
| Confidencialidad  | ✓                       | ✓                   |                 |            |              |              |
| Integridad        |                         |                     |                 | ✓          | ✓            |              |
| No Repudio        |                         |                     |                 |            |              |              |
| Disponibilidad    |                         |                     |                 |            |              | ✓            |

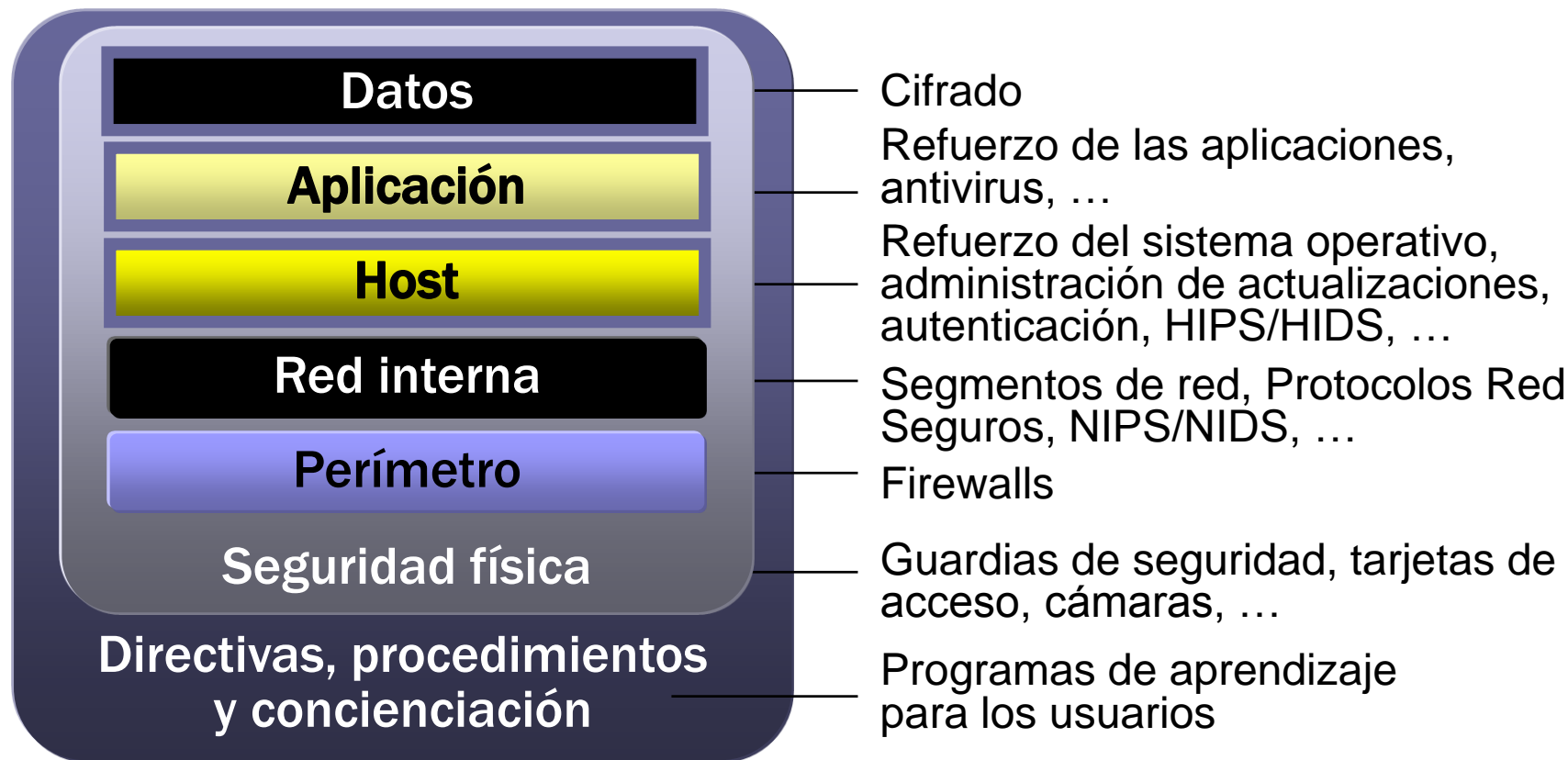
# Servicios vs. mecanismos seguridad

|                   | Cifrado | Firma Digital | Control Acceso | Integridad de datos | Interc. de autenticación | Relleno de tráfico | Control enrutamiento | Notarización |
|-------------------|---------|---------------|----------------|---------------------|--------------------------|--------------------|----------------------|--------------|
| Autenticación     | ✓       | ✓             |                |                     | ✓                        |                    |                      |              |
| Control de Acceso |         |               | ✓              |                     |                          |                    |                      |              |
| Confidencialidad  | ✓       |               |                |                     |                          | ✓                  | ✓                    |              |
| Integridad        | ✓       | ✓             |                | ✓                   |                          |                    |                      |              |
| No Repudio        |         | ✓             |                | ✓                   |                          |                    |                      | ✓            |
| Disponibilidad    |         |               |                | ✓                   | ✓                        |                    |                      |              |

# **DEFENSA EN PROFUNDIDAD O MODELO POR CAPAS**



# Defensa en profundidad o modelo por capas



# Bibliografía

- Stallings, W. (2004). ***Fundamentos de Seguridad en Redes.*** Aplicaciones y estándares. (2ª ed.): Pearson. <- Capítulo 1.

# Documentos y Sitios de Interés

- ITU-T. (1991). **Recommendation X.800**. Ginebra. Disponible en: <http://www.itu.int/rec/T-REC-X.800-199103-I/e>.
- Shirey, R. (2000). **Internet Security Glossary. IETF RFC 2828**. Disponible en: <http://www.ietf.org/rfc/rfc2828.txt>.
- **OWASP Top Ten Project**.  
[https://www.owasp.org/index.php/OWASP\\_Top\\_Ten\\_Project](https://www.owasp.org/index.php/OWASP_Top_Ten_Project)