Clase 2:
Introducción, definiciones e historia

Herson Esquivel Vargas

IC8071 Seguridad de software

TEC | Tecnológico de Costa Rica

Introducción

Introducción

- ¿Qué tienen en común

sitios web, navegadores web, sistemas operativos, puntos de acceso Wi-Fi, routers, firewalls, edificios inteligentes, aplicaciones de ofimática, equipo de video-conferencias, carros, ...

?

Introducción

- ¿Qué tienen en común

Sitios web, navegadores web, sistemas operativos, puntos de acceso Wi-Fi, routers, firewalls, edificios inteligentes, aplicaciones de ofimática, equipo de video-conferencias, carros, ...

?

¿Por qué se pueden comprometer todas ellas?

$ vulnerability

(I) A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

Tutorial: A system can have three types of vulnerabilities: (a) vulnerabilities in design or specification; (b) vulnerabilities in implementation; and (c) vulnerabilities in operation and management. Most systems have one or more vulnerabilities, but this does not mean that the systems are too flawed to use. Not every threat results in an attack, and not every attack succeeds. Success depends on the degree of vulnerability, the strength of attacks, and the effectiveness of any countermeasures in use. If the attacks needed to exploit a vulnerability are very difficult to carry out, then the vulnerability may be tolerable. If the perceived benefit to an attacker is small, then even an easily exploited vulnerability may be tolerable. However, if the attacks are well understood and easily made, and if the vulnerable system is employed by a wide range of users, then it is likely that there will be enough motivation for someone to launch an attack.

Fuente:
RFC 4949 - Internet Security Glossary, Version 2 - https://tools.ietf.org/html/rfc4949

TECH

Honda key fob hack could leave all vehicle models since 2012 vulnerable: reports

By Thomas Barrabi

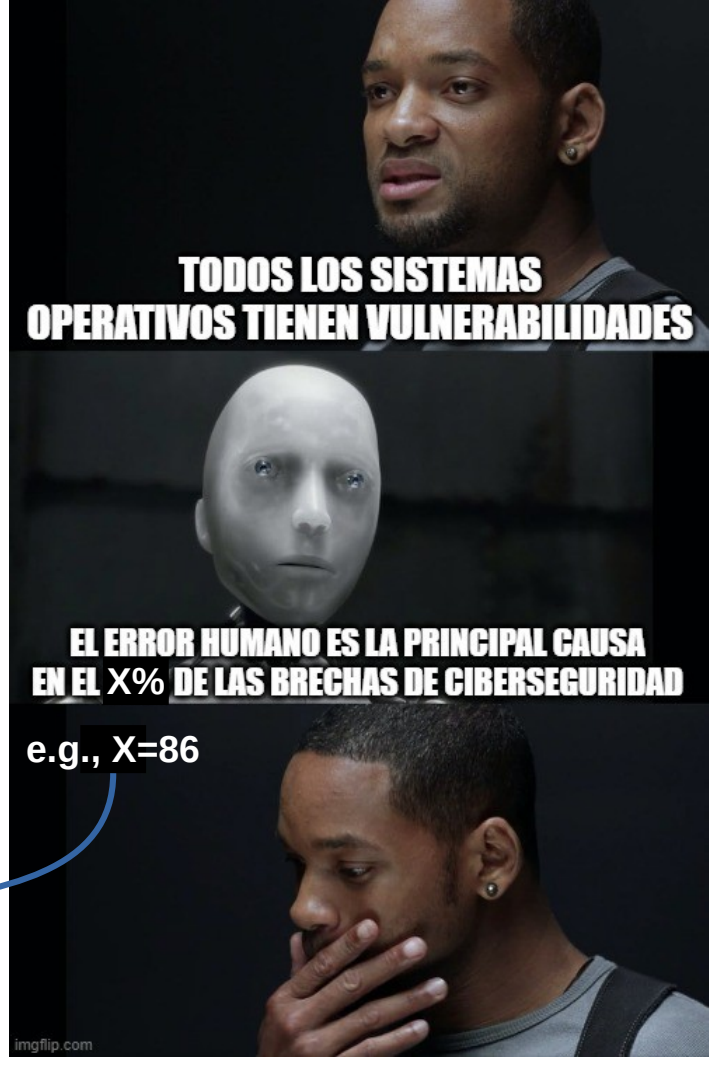
July 12, 2022 | 4:22pm | Updated

The flaw reportedly allows hackers to open car doors and start engines.

Fuente:
https://nypost.com/2022/07/12/honda-key-fob-hack-could-leave-all-vehicle-models-since-2012-vulnerable-reports/

¿Qué es la seguridad del software?

- La idea crear software que continúa funcionando correctamente aún bajo ataque
- El software es el eslabón más débil de la cadena con la única excepción del factor humano



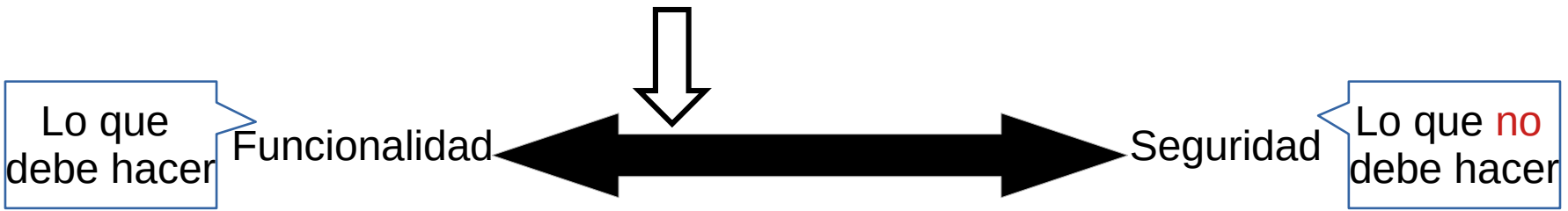
Fuente:
Deloitte (2009). Protecting what matters. 6th Annual Global Security Survey. - https://www.iasplus.com/en/binary/dttpubs/2009securitysurvey.pdf

¿Qué es la seguridad del software?

- Propiedad intrínseca de un sistema (≈ calidad)
- La seguridad debe considerarse desde el inicio
  - Requerimientos, diseño, ...
- Seguridad del software ≠ software de seguridad

¿Qué es la seguridad del software?

- En la práctica, la seguridad es una preocupación secundaria
  - El objetivo principal es proveer alguna funcionalidad



- *“Unless you think like an attacker, you will be unaware of any potential threats”*

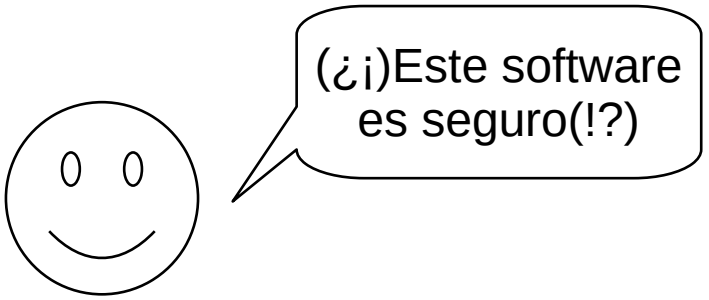
¿Qué es la seguridad del software?

- Ubique los siguientes software
  - Sistemas operativos
  - Lenguajes de programación
  - Navegadores web
  - Clientes de correo

¿Qué es la seguridad del software?

- La seguridad trata de **regular el acceso a activos**
  - e.g., información
- El software provee **funcionalidad**
  - e.g., expedientes médicos digitales (i.e., EDUS)
- Esta funcionalidad conlleva **riesgos**
  - e.g., ¿Cuáles son los riesgos de EDUS?
- La seguridad del software consiste en el **manejo de estos riesgos**

Conceptos de seguridad



Esta pregunta/afirmación no tiene ningún sentido sin contexto

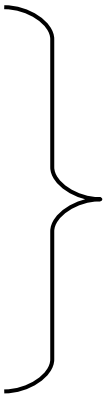
Conceptos de seguridad

- Cualquier discusión sobre seguridad debe iniciar con
  - Participantes
  - Activos
  - Amenazas
  - Modelo de atacante

Cualquier discusión en que no se definan estos aspectos carece de sentido

Conceptos de seguridad

- Cualquier discusión sobre seguridad debe iniciar con
  - Participantes
  - Activos
  - Amenazas
  - Modelo de atacante



Riesgo

Cualquier discusión en que no se definan estos aspectos carece de sentido

Conceptos de seguridad

- Objetivos de seguridad
  - Confidencialidad
    - ¬ autorización ➔ ¬ lectura
  - Integridad
    - ¬ autorización ➔ ¬ escritura
  - Disponibilidad
    - autorización ➔ acceso
  - No-repudio (para establecer responsabilidad)
    - autorización ➔ ¬ negación_de_acciones

Conceptos de seguridad

• Objetivos de seguridad	Cuentas bancarias	Expedientes médicos	Planta eléctrica
– Confidencialidad • ¬ autorización ➔ ¬ lectura			
– Integridad • ¬ autorización ➔ ¬ escritura			
– Disponibilidad • autorización ➔ acceso			

- No-repudio (para establecer responsabilidad)
  - autorización ➔ ¬ negación_de_acciones

Conceptos de seguridad

- **¿Cómo alcanzar los objetivos?** Medidas técnicas como:
  - Autenticación
    - ¿Quién es usted?
  - Control de acceso/Autorización
    - Controlar quién tiene permitido hacer qué
  - Auditar
    - ¿Hay algo mal?
  - Acción
    - Si hay, tomar acciones

Conceptos de seguridad

- **¿Cómo alcanzar los objetivos?** Medidas NO técnicas como:
  - Seguridad física
  - Verificación de antecedentes del personal
  - Leyes
  - Policía especializada
  - …

  Estas están fuera del alcance de este curso

Historia

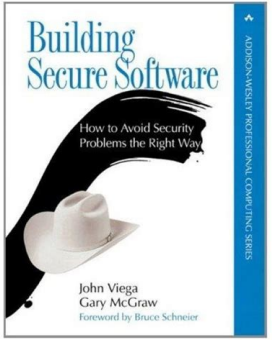
- Primer *gusano* documentado en 1971: **Creeper**

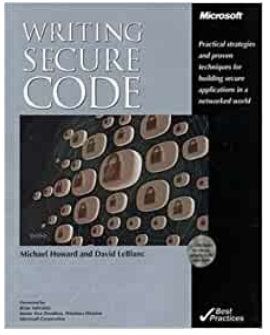
```
"I'M THE CREEPER;
CATCH ME IF YOU CAN"
```


Fuente:
The evolution of viruses and worms - http://ivanlef0u.fr/repo/madchat/vxdevl/papers/avers/statmethods2004.pdf

Historia

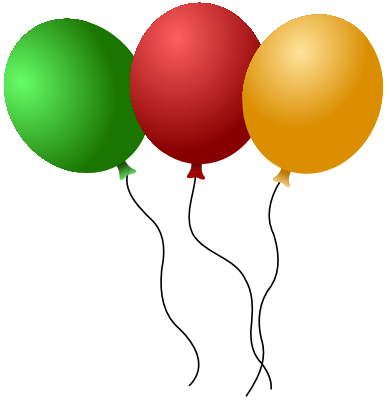
- No fue hasta inicios de siglo que se empezó a discutir la **seguridad del software como disciplina**





Historia

- Después de virus como *nimda* y *code red*
- El 15 de Enero de 2002 a las 17:22 Bill Gates escribió a todo Microsoft el memo titulado Trustworthy Computing
- Memo al que se le celebran los cumpleaños
  - 10
  - 20



Resumen

- ¡El software está en todas partes!
- Las vulnerabilidades son inherentes al software
- Seguridad del software es la idea crear software que **continúa funcionando correctamente aún bajo ataque**
- Aunque existe malware desde hace 50+ años, la seguridad del software es una disciplina reciente

Lecturas recomendadas

- Dar seguimiento a las alertas y boletines de
  - https://www.cisa.gov/news-events/cybersecurity-advisories
  - https://www.cisa.gov/news-events/bulletins/sb24-036

Lecturas obligatorias

- Investigar sobre alguna (solamente una) de las alertas del slide anterior y explicarla en sus propias palabras
  - **1 semana** (16 de Feb, 2024 a las 11:59pm)
  - **300 palabras**
  - A entregar en el TecDigital