El SOFTWARE LIBRE y la defensa informática

Daniel Coletti
dcoletti@cadesol.org.ar
@danielcoletti

Hablemos con “propiedad”

- Software propietario libre
  - Tiene propietarios (los programadores||empresas)
  - Cumple con las cuatro libertades
- Software propietario privativo
  - Tiene propietarios (los programadores||empresas)
  - Restringe casi todas las posibles libertades

Software propietario libre ≠ Software propietario privativo

Software libre ≠ Software privativo

Daniel Coletti - dcoletti@cadesol.org.ar

Seguridad por diseño vs seguridad por oscuridad

- Por oscuridad está basada en tener bajo 7 llaves todo el código, algorítmos, diseño, implementación y demás partes de un sistema
- Por diseño está basada en mostrar completamente diseño del sistema, excepto la clave criptográfica (Kerckhoff)

Daniel Coletti - dcoletti@cadesol.org.ar

CAdESoL

¿Cómo se puede confiar en algo que no sabemos como está hecho?

- Generalmente no tenemos acceso a los fuentes
- Cuando se lo tiene no hay forma clara de verificar que el binario es el producto de la compilación de esos fuentes. ¿Y los upgrades?
- ¿Qué pasa con los fuentes de empresas aliadas comercialmente al proveedor?
- ¿Cuánto tiempo estuvimos vulnerables desde que se descubrió el problema hasta que fue resuelto? ¿Lo publican realmente?

Daniel Coletti - dcoletti@cadesol.org.ar

CAdESoL

Experiencias recientes de vulnerabilidades en SL

- Recientemente OpenSSL: HeartBleed (1 de Abril 2014), corregido en el release 1.0.1g de openssl
- “Aparentemente” estuvo sin ser publicado durante 6 meses, la NSA sabía y lo mantuvo en secreto para sus propios propósitos (bloomberg[1])
- Vulnerabilidades en el protocolo SSH han aparecido en muchas ocasiones.

[1] http://en.wikipedia.org/wiki/Heartbleed

Daniel Coletti - dcoletti@cadesol.org.ar

CAdESoL

Viejas historias / nuevas historias

- La famosa _NSAKEY de **1999!**
- Caso “Lotus” y el cifrado por encima de los 40 bits
- Rumores sobre fuga de información de sensores petroleros en Brasil desde la misma base de datos

Daniel Coletti - dcoletti@cadesol.org.ar

CAdESoL

Espionaje en Brasil (2013)

- Dilma ordena utilizar Expresso Livre V3 en todas las reparticiones del Estado Federal (nacional)

Expresso V3 es software libre (basado en tine20.org)

- Desarrollo interno de criptografía con firma digital propia de Brasil

Daniel Coletti - dcoletti@cadesol.org.ar

CAdESoL

Opiniones de la cámara

- Es condición necesaria para garantizar seguridad desde el software, que sea libre o haya pleno conocimiento sobre cómo está hecho
- Poder auditar sin “ayuda” del proveedor es esencial
- El software puede incluso ser privativo, pero en ese caso necesariamente tiene que ser argentino

Daniel Coletti - dcoletti@cadesol.org.ar

CAdESoL

¡Gracias!

Daniel Coletti
dcoletti@cadesol.org.ar
@danielcoletti