|  |  |  |
| --- | --- | --- |
| **Módulo 3 – Tema 4** | Srini Devadas |  |

**Video 1:**

Ransonware: ataque a un individuo amenazado con la pérdida de sus documentos. Virus o gusano que obtiene permisos y encriptar los archivos de la persona, eliminar los no encriptados y configurar las cosas para que el individuo tenga que pagar en bitcoins o moneda digital para obtener una clave secreta para desencriptar y poder tenerlos nuevamente.

Ataque a servicios: los servidores son atacados y los daños importantes / hacer mucho dinero porque obtienen mucha información. Ejemplo Target donde la tecnología “Chip on card” hubiese evitado el robo de identidad aún teniendo el nro. de tarjeta.

Stuxnex: más relacionado a IoT: gusano que atacó 14 sitios industriales en Irán. Incluyendo una instalación nuclear. Daño físico porque las centrífugas nucleares giraban en descontrol (inestabilidad de la infraestructura). Kaperskylabs lo rastreo sino hubiese sido peor.

Porque pasa esto:

* **Seguridad** difícil porque es una **meta negativa**: hay que hacer todas las restricciones necesarias para que no se pueda efectivizar. **Ejemplos de cómo se puede “robar“ un archivo.**

**Es imposible pensar en todas las maneras de atacar.**

**Video 2**

Modelos de amenazas: nos dicen el poder del adversario.

Podemos suponer que el adversario tiene el control de algunas computadoras, no todas. Algunos programas, usuarios, conoce las contraseñas pero no todas.

Generalmente conoce los errores en la infraestructura.

En IoT ataques de soft pero también físicos (invasivos abrir un dispositivo y obtener contraseña o no invasivos a partir de la comunicación) e ingeniería social (corromper una persona que tiene acceso).

En IoT sistemas comprometidos por suposiciones pocos realistas sobre el atacante (mucho más débil).

Filosofía:

* **Ciber seguridad**: es una propiedad del sistema como el rendimiento.
* Generalmente se lo toma a la ligera y solo se da importancia a funcionalidades de usuario.
* El atacante descubre las vulnerabilidades.
* Luego arreglamos y proseguimos.
* Esto continúa con nuevos errores.
* CURAR Y REZAR.

**Filosofía holística:**

* Criterio de primera clase.
* Diseñarlo desde cero.
* Revisar interfaces.
* Diseñar componentes individuales y componer estos componentes en un sistema holístico seguro.

**Video 3**

Mecanismos:

* Prevención: hacer que el trabajo del adversario sea dificultoso a través e mecanismos de diseño.
* Resiliencia: permitir que el sistema continúe.
* Detección y recuperación: pueden ocurrir los 2 anteriores.

Ejemplo prevención ataque físico:

* Cada dispositivo identidad y que sea autenticado (secret key). Sobre todo si está corriendo soft de seguridad.
* Criptografía para autenticar. Necesidad de almacenar la secret key.
* Asociada a esto una public key asociada que se utilizará.
* Secure keys se pueden obtener con ataques invasivos.
* En IoT con tantos dispositivos, no supervisado. Obtiene la clave de 1 y clona el resto.
* Crear hard resistente a esto.
* También puede pasar que no se pueda utilizar este mecanismo ya que es costoso.

**Video 4**

Physical Unclonable Function (**prevención**): protección de circuitos integrados de ataques físicos para extraer secret key.

* Se identifican los circuitos en base a la variación de fábrica (retrasos distintos).
* Osciladores de anillo.
* Usar estos IDs como secret key.
* Solo existen cuando el circuito está encendido.
* No siempre es la misma.

Extractor difuso: fuente difusa como la del oscilador de anillo o por ejemplo huella digital y obtiene una secret key segura.

**Video 5**

**Problema de aprendizaje de paridad con ruido**. Requiere para el adversario mucho tiempo incluso con algoritmos más conocidos.

Las keys se generan en el encendido y físicamente mucho más seguro que mecanismos FLASH, etc.

**Video 6**

**Resiliencia**

Base informática confiable: soft + hard que debe ser confiable para funcionar correctamente. Sin enormes actualmente.

Como reducirla:

* Encriptación de datos.
* Derivación de trabajo. Computación encriptada. Cifrado completamente homomórfico. Asegura que el descifrado es el correcto.

**Desventaja: es sumamente lento. No podemos utilizarlos para cálculos complicados. PROX. VIDEO.**

* Des encriptación de datos.

**Video 7**

Procesador seguro que almacena la clave (hard de confianza).

Asumimos que es inviolable.

Puede desencriptar y trabajar con los datos descifrados.

Falencias en bancos de memoria.

**Procesador Ascend. Procesador elegido en IoT.**

**Video 8**

**Detección y recuperación (integridad de computación)**

Es probable que solo quiera corromper los datos.

Garantizar integridad => integridad en almacenamiento y computación.

* De datos: redundancia. Fácil.
* De computación. Mucho más difícil. Cálculos paralelos o redundantes.

Reto: mantener rendimiento alto.

Detectar los más vulnerables para reducir la redundancia.