Kevin Villagrán - 23584

Tarea 6.
Desarrollo Seguro
Parte 1

Descripción del caso Chapter 1: Hacking the Casinos for a Million Bucks:

El caso comienza con un reto de saber si las maquinas de casino se podían manipular al tratarse de computadoras, entonces Alex Mayfield y otros tres amigos, todos consultores tecnológicos comenzaron a investigar patentes de las máquinas, luego compraron una de esas máquinas en Nevada donde a partir de esta fue que comenzaron a desarmarla y analizar el código del ROM. Allí, descubrieron que el generador de números aleatorios, el RNG de esas máquinas tenía fallos que permitían saber las cartas futuras. Con base a eso, comenzaron a programar su propio software y usando relojes Casio, una computadora oculta con un botón en el zapato y vibradores en los bolsillos fue que sabían en qué momento presionarle a Play para poder obtener altas cantidades de ganancia. Así comenzaron y evidentemente comenzaron a levantar algunas sospechas, así que decidieron ajustar la técnica para poder ir ganando cantidades más pequeñas y así hacerlo todo más discreto. Así estuvieron durante unos tres años extrayendo dinero de los casinos de Las Vegas, Reno, Atlantic City, entre otros. Todo terminó cuando atraparon a Marco, otro integrante del grupo. Si bien no fue arrestado como tal si le confiscaron todo su dinero y equipo y lo dejaron libre con la condición de que jamás volvería. A raíz de eso el grupo dejó atrás por lo riesgoso que se estaba volviendo, quedándose así con varios cientos de millones de dólares.

Vulnerabilidad explotada:

El generador de números aleatorios, el RNG, realmente no era tan aleatorio, si no que utilizaba un algoritmo determinista, así que si se conocía el estado que tenía la máquina internamente en algún momento específico, se podía calcular toda la secuencia futura de cartas que iban a salir. Además, el simple hecho de poder extraer todo el código a partir de una máquina demuestra otra vulnerabilidad con cómo estaba protegida la ROM de estas.

Propuestas de solución:

- Utilizar chips seguros o empaquetados para que no se pueda retirar.
- Epoxy con aluminio para destruir el chip si intentan removerlo con calor.
- Diseño en ball grid array (BGA) para dificultar extraer las señales.
- Quitar información de identificación del chip.
- Probar ataques reales con los RNG.