Malicious Design

IE-0411 MICROELECTRÓNICA

Andrés Alvarado Velázquez
B30316
email: andres.alvaradovelazquez@ucr.ac.cr

1. INTRODUCCIÓN

Los circuitos maliciosos ocultos proporcionan a un atacante un vector de ataque furtivo. Como ocupan una capa debajo de la pila de software completa, los circuitos maliciosos pueden eludir las técnicas defensivas tradicionales. Sin embargo, el trabajo actual en circuitos de troyanos considera solo ataques simples contra el hardware mismo y defensas directas. No se han explorado los diseños más complejos que atacan el software, así como las contramedidas que un atacante puede tomar para eludir las defensas propuestas..

2. MALWARE DESING

Malware Desing es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información. El término malware se utiliza mucho por profesionales de la informática para poder referirse a una variedad de software hostil, intrusivo o molesto [1].

Los atacantes pueden insertar circuitos encubiertamente en circuitos integrados (IC) utilizados en los sistemas informáticos actuales; un informe reciente del Departamento de Defensa [3] identifica varias tendencias actuales que contribuyen a esta amenaza. En primer lugar, se ha convertido en económicamente inviable adquirir IC de alto rendimiento que no sean proveedores comerciales. En segundo lugar, estos proveedores comerciales están trasladando cada vez más las etapas de diseño, fabricación y pruebas de producción de circuitos integrados a un conjunto diverso de países, lo que hace que no sea factible asegurar la cadena de suministro de circuitos integrados.

Los dispositivos modificados maliciosamente ya son una realidad. En 2006, Apple envió iPods infectados con el virus RavMonE. Durante la guerra fría, la CIA saboteó el software de control de oleoductos, que luego fue robado"por espías rusos. Por el contrario, los agentes rusos interceptaron y modificaron las máquinas de escribir que debían utilizarse en la embajada de los EE. UU. Aunque ninguno de estos ataques usa circuitos maliciosos, muestran claramente la factibilidad de insertar elementos maliciosos de manera encubierta en la cadena de suministro de COTS.

El uso de hardware modificado proporciona a los atacantes una ventaja fundamental en comparación con los ataques basados en software.

REFERENCIAS

[1] Microsoft (14 de abril de 2009). «Documento informativo sobre seguridad de Microsoft (951306), Una vulnerabilidad en Windows podría permitir la elevación de privilegios». Microsoft Tech Net.

[2] Bob Brown, Network World. «Sony BMG rootkit scandal: 5 years later, Shocking rootkit revelation seen as "seminal moment in malware history"

[3] Von Neumann, John: "Theory of Self-Reproducing Automata", Part 1: Transcripts of lectures given at the University of Illinois, Dec. 1949, Editor: A. W. Burks, University of Illinois, USA, (1966).