Se ha revelado un método de ataque novedoso contra una pieza de tecnología crucial llamada ethernet activada por tiempo (TTE), que se utiliza en infraestructura crítica para la seguridad, lo que podría causar la falla de los sistemas que alimentan naves espaciales y aeronaves.

Nombrada como PCspooF por un grupo de académicos e investigadores de la Universidad de Michigan, la Universidad de Pensilvania y el Centro Espacial Johnson de la NASA, la técnica está diseñada para romper las garantías de seguridad de TTE e inducir a los dispositivos TTE a perder la sincronización hasta por un segundo, un comportamiento que incluso puede conducir a maniobras incontroladas en misiones de vuelos espaciales y amenazar la segurida de la tripulación.

TTE es una de las tecnologías de red que forma parte de lo que se denomina una red de criticidad mixta en la que el tráfico con diferentes requisitos de tiempo y tolerancia a fallas coexiste en la misma red física. Esto siginifica que tanto los dispositivos críticos, que, por ejemplo, permiten el control de vehículos, como los dispositivos no críticos, que se usan para monitorear y recopilar datos, comparten la misma red.

Una ventaja obvia de este enfoque es el hecho de que existen menores requisitos de peso y potencia, así como menores costos de desarrollo y tiempo derivados de depender de una sola tecnología. Pero esto también cuenta con sus propios inconvenientes.

> *«Este enfoque de criticidad mixta ejerce mucha más presión sobre el diseño de la red para proporcionar aislamiento. Ahora que los elementos críticos y no críticos pueden conectarse al mismo conmutador, el protocolo de red y el hardware deben hacer un trabajo adicional para garantizar que el tráfico crítico siempre se transmita con éxito y a tiempo»*, dijo Andrew Loveless, autor principal del estudio.

Además, mientras que los dispositivos críticos en la red están sujetos a una investigación exhaustiva, las contrapartes no críticas no solo son dispositivos comerciales listos para usar (COTS), sino que también carecen del mismo proceso riguroso, lo que lleva a posibles vías de suministro, compromisos de cadena que podrían armarse para activar el ataque mediante la integración de un componente de terceros no autorizado en el sistema.

Aquí es donde una red de criticidad mixta ayuda a garantizar que, aún si el dispositivo COTS es malicioso, no puede interferir con el tráfico crítico.

> *«En PCspooF, descubrimos una forma en que un dispositivo malicioso no crítico puede romper esta garantía de aislamiento en una red TTE»,* dijo Baris Kasikci, profesor asistente en el departamento de ingeniería eléctrica e informática de la Universidad de Michigan.

Esto, a su vez, se logra mediante el uso del dispositivo malicioso para inyectar interferencia electromagnética (EMI) en un conmutador TTE por medio de un cable Ethernet, engañando efectivamente al conmutador para que envíe mensajes de sincronización de apariencia auténtica (es decir, marcos de control de protocolo o PCF) y obtener aceptados por otros dispositivos TTE.

Un circuito de generación de *«ruido eléctrico»* de este tipo puede ocupar solo 2.5 cm x 2.5 cm en una placa de circuito impreso de una sola capa, que requiere solo una potencia mínima y que puede ocultarse en un dispositivo de mejor esfuerzo e integrarse en un sistema TTE sin levantar cualquier bandeja roja.

Como mitigaciones, el estudio recomienda usar optoacopladores o protectores contra sobretensiones para bloquear la interferencia electromagnética, verificar las direcciones MAC de origen para asegurarse de que sean auténticas, ocultar los campos PCF clave, usar un protocolo de autenticación de capa de enlace como IEEE 802.1AE, aumentar la cantidad de sincronización de maestros y deshabilitar transiciones de estado peligrosas.

Los hallazgos muestran que el uso de hardware común en un sistema diseñado para proporcionar garantías estrictas de aislamiento a veces puede anular las mismas protecciones, dijeron los investigadores, agregando que los sistemas de software de criticidad mixta deben examinarse de forma meticulosa similar para garantizar que los mecanismos de aislamiento sean infalibles.

> *«Los protocolos TTE son muy maduros y están bien examinados, y muchas de las partes más importantes están formalmente probadas»,* dijo Kasikci.

> *«En cierto modo, eso es lo que hace que nuestro ataque sea interesante: que pudimos descubrir cómo violar algunas garantías del protocolo a pesar de su madurez. Pero para hacer eso, tuvimos que pensar fuera de la caja y descubrir cómo hacer que el hardware se comporte de una forma que el protocolo no espera».*