RESEARCH INSTITUTE FOR
SECURE HARDWARE &
EMBEDDED SYSTEMS

THUNDERCLAP CASE STUDY

Funded by

in association with
National Cyber Security Centre

EPSRC
Pioneering research and skills

THUNDERCLAP

UK RESEARCHERS IDENTIFY USB SECURITY FLAWS – LEADING TO IMPROVED USB STANDARDS

Security researchers at Cambridge University, members of the UK Research Institute for Secure Hardware & Embedded Systems (RISE), have identified vulnerabilities with USB and Thunderbolt interface standards. The researchers demonstrated that connecting a malicious peripheral device allowed access to secret data and changes to system behaviour.

The vulnerability was found to be applicable to any devices incorporating a Thunderbolt port (Apple laptops and desktops since 2011, some Linux and Windows laptops and desktops since 2016), or devices supporting USB-C, Mini DisplayPort connectors and PCI Express peripherals.

Vulnerability

The attacks exploit Direct Memory Access (DMA) communications, an approach intended to improve the high-speed exchange of data between peripherals and PC memory, without the need for processor involvement.

Although DMA may be secured using an Input-Output Memory Management Unit (IOMMU), it was found that existing IOMMU implementations could be circumvented, or were disabled by default in operating systems to reduce performance overheads.

It is possible to imagine a wide-scale attack making use of compromised devices in the supply chain, such as HDMI/Ethernet dongles, power adapters, or USB-C storage devices. Such attacks would enable remote access of documents, encryption keys, passwords, injection of malicious code etc.

Industry Engagement and Response

Prior to publishing results, researchers contacted affected industry participants to notify them of the vulnerabilities. This led to a series of patches and updates to mitigate against the threats. The hardware platform used to develop the attacks was also shared with industry and is now used in-house for further research and vulnerability analysis.

Since the proposed USB 4 standard incorporates substantial parts of the Thunderbolt specification, including PCI Express DMA transfers, engagement took place with USB 4 standards committee. This led to the incorporation of security recommendations into the upcoming USB 4 standard.

Impact

- Research identified serious weaknesses in existing computer peripheral interfaces.
- Collaboration with industry to disseminate research and understand the threats.
- Industry response with patches and mitigations against the threats.
  - MacOS 10.12.4 – Mitigated specific exploit
  - Windows 10 1803 – Kernel DMA Protections for Thunderbolt 3.
  - Linux 5.0 onwards – Thunderbolt devices assumed less trustworthy by operating system
  - Intel – Published guidance on ‘Thunderclap’ DMA threats and mitigations.
- Research disseminated via academic papers, website www.thunderclap.io and numerous industry publications.
- Thunderclap FPGA research platform in use by industry for hardening against these vulnerabilities
- Security recommendations for hardening systems incorporated in USB 4 standard.

About RISE

The UK Research Institute in Secure Hardware and Embedded Systems (RISE), funded by the Engineering and Physical Science Research Council (EPSRC) and the National Cyber Security Centre (NSCS) seeks to identify and address key issues that underpin hardware security.

A key focus is to accelerate the industrial uptake of the Institute’s research output and its translation into new products, services and business opportunities for the wider benefit of the UK economy.

ukrise.org