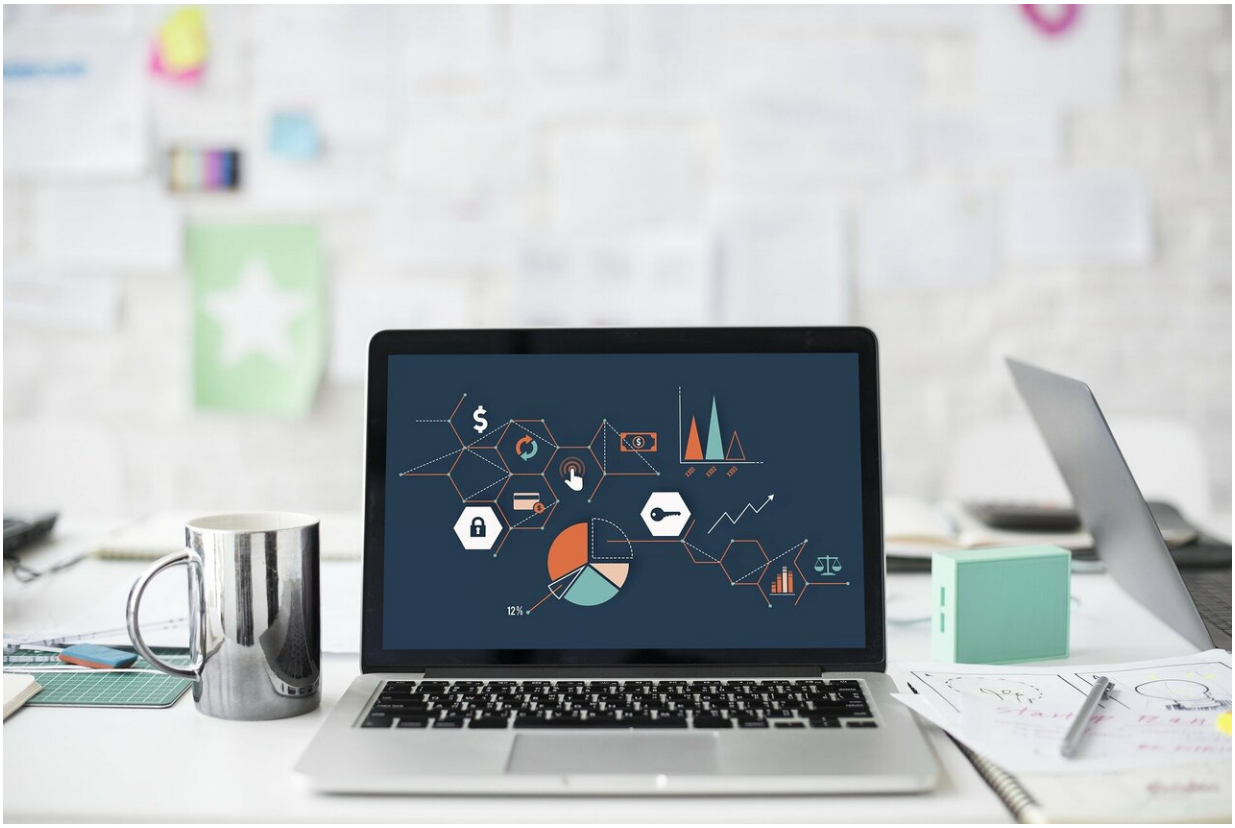
Most laptops vulnerable to attack via peripheral devices, say researchers

February 25 2019



Credit: CC0 Public Domain

Many modern laptops and an increasing number of desktop computers are much more vulnerable to hacking through common plug-in devices than previously thought, according to new research.

The research, to be presented today at the Network and Distributed Systems Security Symposium in San Diego, shows that attackers can compromise an unattended machine in a matter of seconds through devices such as chargers and docking stations.

Vulnerabilities were found in computers with Thunderbolt ports running Windows, macOS, Linux and FreeBSD. Many modern laptops and an increasing number of desktops are susceptible.

The researchers, from the University of Cambridge and Rice University, exposed the vulnerabilities through Thunderclap, an open-source platform they have created to study the security of computer peripherals and their interactions with operating systems. It can be plugged into computers using a USB-C port that supports the Thunderbolt interface and allows the researchers to investigate techniques available to attackers. They found that potential attacks could take complete control of the target computer.

The researchers, led by Dr. Theodore Markettos from Cambridge's Department of Computer Science and Technology, say that in addition to plug-in devices like network and graphics cards, attacks can also be carried out by seemingly innocuous peripherals like chargers and projectors that correctly charge or project video but simultaneously compromise the host machine.

Computer peripherals such as network cards and graphics processing units have direct memory access (DMA), which allows them to bypass operating system security policies. DMA attacks abusing this access have been widely employed to take control of and extract sensitive data from target machines.

Current systems feature input-output memory management units (IOMMUs) which can protect against DMA attacks by restricting

memory access to peripherals that perform legitimate functions and only allowing access to non-sensitive regions of memory. However, IOMMU protection is frequently turned off in many systems and the new research shows that, even when the protection is enabled, it can be compromised.

"We have demonstrated that current IOMMU usage does not offer full protection and that there is still the potential for sophisticated attackers to do serious harm," said Brett Gutstein, a Gates Cambridge Scholar, who is one of the research team.

The vulnerabilities were discovered in 2016 and the researchers have been working with technology companies such as Apple, Intel and Microsoft to address the security risks. Companies have begun to implement fixes that address some of the vulnerabilities that the researchers uncovered; several vendors have released security updates in the last two years.

However, the Cambridge research shows that solving the general problem remains elusive and that recent developments, such as the rise of hardware interconnects like Thunderbolt 3 that combine power input, video output and peripheral device DMA over the same port, have greatly increased the threat from malicious devices, charging stations and projectors that take control of connected machines. The researchers want to see technology companies taking further action, but also stress the need for individuals to be aware of the risks.

"It is essential that users install security updates provided by Apple, Microsoft and others to be protected against the specific vulnerabilities we have reported," said Markettos. "However, platforms remain insufficiently defended from malicious peripheral devices over Thunderbolt and users should not connect devices they do not know the origin of or do not trust."

More information: More information is available at thunderclap.io

Provided by University of Cambridge