Router guest networks lack adequate security, according to researchers

August 15 2019

Credit: CC0 Public Domain

While many organizations and home networks use a host and guest network on the same router hardware to increase security, a new study by Ben-Gurion University indicates that routers from well-known manufacturers are vulnerable to cross-router data leaks through a malicious attack on one of the two separated networks.

According to Adar Ovadya, a master's student in BGU's Department of Software and Information Systems Engineering, "all of the routers we surveyed regardless of brand or price point were vulnerable to at least some cross-network communication once we used specially crafted network packets. A hardware-based solution seems to be the safest approach to guaranteeing isolation between secure and non-secure network devices."

The BGU research was presented at the 13th USENIX Workshop on Offensive Technologies (WOOT) in Santa Clara this week.

Most routers sold today offer consumers two or more network options—one for the family, which may connect all the sensitive smart home and IoT devices and computers, and the other for visitors or less sensitive data.

In an organization, data traffic sent may include mission-critical business documents, control data for industrial systems, or private medical information. Less sensitive data may include multimedia streams or environmental sensor readings. Network separation and network isolation are important components of the security policy of many organizations if not mandated as standard practice, for example, in hospitals. The goal of these policies is to prevent network intrusions and information leakage by separating sensitive network segments from other segments of the organizational network, and indeed from the general internet.

In the paper, the researchers demonstrated the existence of different levels of cross-router covert channels which can be combined and exploited to either control a malicious implant, or to exfiltrate or steal the data. In some instances, these can be patched as a simple software bug, but more pervasive covert cross-channel communication is impossible to prevent, unless the data streams are separated on different hardware.

The USENIX Workshop on Offensive Technologies (WOOT) aims to present a broad picture of offense and its contributions, bringing together researchers and practitioners in all areas of computer security. WOOT provides a forum for high-quality, peer-reviewed work discussing tools and techniques for attack.

All vulnerabilities were previously disclosed to the manufacturers.

More information: For more information about this research, please visit: https://orenlab.sise.bgu.ac.il/publications/CrossRouter

Provided by American Associates, Ben-Gurion University of the Negev

Citation: Router guest networks lack adequate security, according to researchers (2019, August 15) retrieved 26 April 2024 from https://techxplore.com/news/2019-08-router-guest-networks-lack-adequate.html