PUBLICATION

Hackers Can Steal Encryption Keys From a Distance Using Video

Authors: Michael S. Klipstein
June 22, 2023

On June 13, security researchers disclosed their findings that encryption keys for wireless devices are vulnerable to theft. This research found that cameras in cellular phones or commercial surveillance systems can be used to record power light emitting diodes (LEDs) from up to 60 feet away from a device, thus capturing encryption keys. This new weakness exploits two previously known side-channel attacks, a class of attacks measuring physical effects "leaking" from a device as it performs its operations. Companies should review their systems for this vulnerability, including smart card readers used for access or authentication. All industries are vulnerable to this exploitation; however, health care may be especially hard hit in the future due to the potential to expose electronic medical records. Defense contractors with sensitive information are also highly targeted and should review how this could impact their systems and networks. But the reality is that any secured physical area could be impacted by an attacker's ability to physically break into buildings and facilities.

Risks rapidly increase to both cybersecurity and physical access security when proximity access control systems for both physical access to areas and authentication to computers and other devices is implicated. In this potential attack vector, the devices "leak" electromagnetic fields that can manifest in the pulsing of lights or interference sounds in audio equipment, both often imperceptible to the naked eye or ear. However, high-resolution cameras in cell phones and surveillance equipment can record pulses of light, enabling the attacker to gain the keys to the encryption, and therefore, access. These attacks can lead to theft of sensitive confidential information, including intellectual property. The potential for attack is immense, as these proximity readers are ubiquitous in doors and computers.

Mitigation Strategies

In response to this threat, all organizations using these access control devices should consider the following mitigation steps:

1. Switching to biometric or two-factor access for sensitive areas or systems. The use of a keypad or the use of fingerprints or retina scans for access control to sensitive areas mitigates this threat (when permitted by law).

2. If continuing to use proximity access for sensitive areas, place an individual near the door for a human to visually control access.

3. Reviewing encrypted systems and networks, considering vulnerabilities, and continuing to monitor this potential exploitation.

4. Updating security and access policies to align with mitigations and therefore increase the difficulty for attackers.

Many organizations use card readers and other tokens with proximity connectivity for access to sensitive areas and information. These attacks increase the risk of physical access, as well as access to computers and the

data therein. Liability and loss of intellectual property present reputational and monetary damage to organizations.

Baker Donelson can assist in reviewing your data mapping considerations, creation of security programming, disaster recovery and incident response, and further ensuring that your policies and procedures reflect the correct operating stance to protect your information and devices, as well as implementation. For any questions about how this vulnerability might affect your business or your clients, or how you can better prepare for these types of threats, please contact Michael Klipstein or any member of the Baker Donelson Data Protection, Privacy, and Cybersecurity Team.