

The £200 device that could steal your bank PIN

Wednesday 19 August, 2015

The increasing availability of cheap thermal imaging equipment – once the sole preserve of only the best-equipped attacker – is creating an ever-increasing risk to push-button security devices. Using a readily available iPhone accessory costing less than £200, Sec-Tec tested a wide range of push-button security devices, including ATMs, locks and safes, and found that certain devices could leak the digits pressed by a legitimate user for over a minute after use.

While identifying the keys in use is straightforward, pinpointing the order in which they were pressed is considerably more difficult. However, Sec-Tec has created two undisclosed methods that assist considerably in the identification of key ordering, and many of the devices utilise no lock-out mechanism; this means that testing all combinations of a four-digit code once the digits are known is easy.

[Sec-Tec](#) makes the following recommendations to limit the risk of attack:

1. The use of devices with metallic (as opposed to plastic or rubber) keys makes such attacks impossible.
2. Palming the keypad after use, even for only a few seconds, prevents attacks in the majority of cases.

Sec-Tec has combined this attack vector with existing RFID cloning equipment to successfully compromise two-factor door locks on a physical-penetration test.

Media:



Related Sectors:

[Computing & Telecoms](#)

Related Keywords:

[Penetration Testing](#) :: [Thermal Imaging](#) :: [ATM](#) :: [Push Locks](#) :: [Pin Number](#)

Scan Me:



Company Contact:

[Sec-Tec Ltd](#)

T. 02083177962

E. davev@sec-tec.co.uk

W. <https://www.sec-tec.co.uk>

[View Online](#)

Additional Assets:

Newsroom: Visit our Newsroom for all the latest stories:

<https://www.sec-tec.pressat.co.uk>