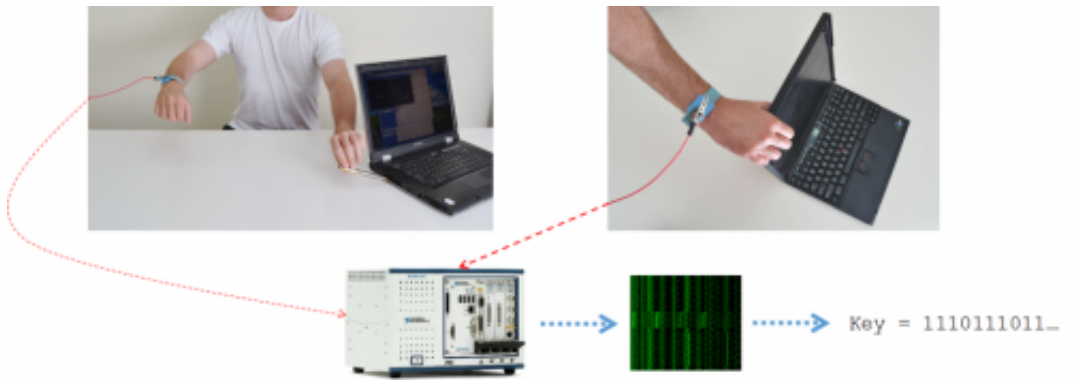
Security event to learn about side-channel attacks on PCs

August 21 2014, by Nancy Owano



Credit: Daniel Genkin et al.

A paper to be presented at next month's Workshop on Cryptographic Hardware and Embedded Systems (CHES) in Busan, South Korea, will discuss physical side-channel attacks on laptop computers, in findings from a team from the Technion and Tel Aviv University. "We demonstrated physical side-channel attacks on a popular software implementation of RSA and ElGamal, running on laptop computers," they said, using novel side channels. They said their attacks were based on the observation that the ground electric potential in many computers fluctuates in a computation-dependent way. An attacker can measure the signal by touching exposed metal on the computer chassis with a plain wire or even with a bare hand. The signal can also be measured at the remote end of Ethernet, VGA or USB cables They noted "non-negligible" impedance between the grounding point(s) and other points

in the chassis. "Due to currents and electromagnetic fields inside the computer, voltages of large magnitude develop across this impedance (often 10mV RMS or more, after filtering out the 50 or 60 Hz mains frequency). This is the voltage we measure."

Does this sort of effort require special sophisticated gear? The authors said that while professional lab equipment yields the most effective attack, a mobile phone can sometimes do. They used a mobile phone to measure the key-dependent chassis potential from the far side of a 10m Ethernet cable, they added.

One key concern would be what kind of information could be obtained from such an attack. They tested numerous laptops and they found the following in almost all the machines: it is possible to distinguish an idle CPU from a busy CPU, and it is possible to note the different patterns of CPU operations and different programs.

Also, "Using GnuPG as our study case, we can, on some machines distinguish between the spectral signatures of different RSA secret keys (signing or decryption), and fully extract decryption keys, by measuring the laptop's chassis potential during decryption of a chosen ciphertext."

Two other attacks they discussed do not require physically touching the laptop, just being near the laptop, via antenna or sound. Electromagnetic emanations, measured via an antenna, convey essentially the same leakage and can be used for key extraction; acoustic emanations measured via microphone can be used to extract keys also.

Mitigation techniques include Faraday cages, insulating enclosures against chassis and touch attacks, and photoelectric decoupling or fiberoptic connections against end of cable attacks. However, they said, inexpensive protection of consumer-grade PCs appears difficult.

"Alternatively, the cryptographic software can be changed, and algorithmic techniques employed to render the emanations less useful to the attacker."

The title of their paper is "Get Your Hands Off My Laptop: Physical Side-Channel Key Extraction Attacks On PCs," by Daniel Genkin, Itamar Pipman and Eran Tromer. According to a report about their work in MIT Technology Review, Tromer notified cryptography software makers. What is more, developers of one cryptographic software package, GnuPG, incorporated a patch into the latest version of their software.

More information: — www.cs.tau.ac.il/~tromer/handsoff/

— www.technologyreview.com/news/ … with-your-bare-hands

Citation: Security event to learn about side-channel attacks on PCs (2014, August 21) retrieved 3 May 2024 from https://techxplore.com/news/2014-08-event-side-channel-pcs.html