Research trio crack RSA encryption keys by listening to computer noise

December 19 2013, by Bob Yirka

Physical setup of a key recovery attack. A mobile phone (Samsung Note II) is placed 30 cm from a target laptop. The phone's internal microphone points towards the laptop's fan vents. Full key extraction is possible in this configuration and distance. Credit: Daniel Genkin et al.

(Phys.org) —A trio of researchers in Israel has discovered that it is possible to crack 4096-bit RSA encryption keys using a microphone to listen to high-pitch noises generated by internal computer components. Adi Shamir (co-inventor of RSA), Daniel Genkin and Eran Tromer have published a research paper describing the technique on a Tel Aviv University server.

Computers make noises, the researchers explain, far beyond the whirring of the fan. The CPU, for example, emits a high pitched noise as it operates, fluctuating depending on which operations it is performing—other components do likewise. Suspecting that they might be able to exploit this characteristic of computers, the researchers set about creating software to interpret noise data obtained using simple microphones and very little other equipment. They also focused exclusively on trying to achieve one single feat: deciphering an RSA encryption key. After much trial and effort, the researchers found it could be done without much effort.

Listening and detecting the noise made by a computer as it processes a single character in an encryption key would be impossible, of course, so the researchers devised a method that causes the noise to be repeated enough times in a row to enable capture of its signal. And that can only happen if the attacker is able to send a cyphertext to the machine that is to be attacked and have it processed. The cyphertext contains code that causes looping. By listening to how the computer processes the cyphertext, the researchers can map the noises made by the computer as it crunches different characters, thereby allowing encryption keys sent by others to be cracked.

What's perhaps most frightening about this method is how easily it can be ported to various machines. The researchers found, for example, that by using a laptop and simple hardware and software they were able to crack encryption keys on a second laptop. Next, they did the same thing using a cell phone as the listening device. They suggest it could also be packaged completely in software and sent out as malware, hacking encryption keys on infected devices and sending them back to the hacker.

As a side-note, the researchers also found that low-bandwidth attacks on computers are also possible by measuring the electrical potential of a

computer's chassis while the circuitry is busy doing its work.

More information: RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis: www.tau.ac.il/~tromer/papers/acoustic-20131218.pdf