*** 北米連携センター情報***

2014 年 8 月 22 日

●ラップトップのわずかな電圧変動で暗号鍵を盗み出すことが可能に

【Ars Technica, 2014/08/21】

テルアビブ大学の研究チームは、GnuPG から暗号鍵を入手できる攻撃手段を発見。先頃、その実演を行った。　暗号化システムを攻撃する手段には幅広いものがあり、暗号化のアルゴリズム自体に含まれる脆弱性を攻撃する手段はその一極といえる。

対極にあるのが、利用する人間を狙う手段。中間にはアルゴリズムそのものではなく、それが導入された形態に潜む脆弱性を狙う様々な手段がある。

これらは、暗号化システムのソフト、ハードはシステムのキャッシュの動きや暗号・復号にかかる時間などから間接的に情報を漏らすことも多い点に着目したもの。このような間接的情報を使って暗号化システムを攻撃する手段は「サイドチャンネル」攻撃と総称される。

今回のテルアビブ大学の研究はこのサイドチャンネル攻撃にあたり、USB ポート周りのシールド部やヒートシンクファンなどラップトップの金属部位が共通の基準電位にあるが、このレベルがラップトップ内の電場により、わずかに上下することに注目している。

その変動はデジタイザで計測が可能で、暗号鍵の情報を盗み出すために用いることもできるとのことで、金属部を直接、デジタイザで計測するだけでなく、金属部に触れている人間を通じて変動を計測することも可能。この場合、汗によって電気抵抗が低下する気温が高い環境の方が計測はやりやすいことが判明している。

研究チームは、高品質な実験装置以外に、ヘッドフォン端子からイーサネットのシールド部位にスマートフォンを接続して、同様に暗号鍵を盗み出すことにも成功した。

電圧の変化を生み出すとくに重要な源はプロセッサだが、数 MHz 程度の電圧変化をサンプリングすることで、RSA、ELGamal 暗号アルゴリズムの鍵を数秒で抽出することができるという。

研究チームは、既にこれまで判明したことを GnuPG 開発者に伝えており、この結果、ソフトウェアには修正が施されている。しかし、それでもハードウェアが原因であるサイドチャンネル攻撃の可能性を完全に排除できていない。

情報を漏らす可能性についてはそれぞれ対策もあるが、すべてをラップトップに導入することは現実性に欠け、費用も跳ね上がることになる。

（参考）本件報道記事

Stealing encryption keys through the power of touch

Researchers pilfer decryption keys through Ethernet and human touch side channel.

by Peter Bright - Aug 21 2014, 7:50pm -0400
Ars Technica

Researchers from Tel Aviv University have demonstrated an attack against the GnuPG encryption software that enables them to retrieve decryption keys by touching exposed metal parts of laptop computers.

There are several ways of attacking encryption systems. At one end of the spectrum, there are flaws and weaknesses in the algorithms themselves that make it easier than it should be to figure out the key to decrypt something. At the other end, there are flaws and weaknesses in human flesh and bones that make it easier than it should be to force someone to offer up the key to decrypt something.

In the middle are a range of attacks that don't depend on flaws on the encryption algorithms but rather in the way they've been implemented. Encryption systems, both software and hardware, can leak information about the keys being used in all sorts of indirect ways, such as the performance of the system's cache, or the time taken to perform encryption and decryption operations. Attacks using these indirect information leaks are known collectively as side channel attacks.

This research is a side-channel attack. The metal parts of a laptop, such as the shielding around USB ports, and heatsink fins, are notionally all at a common ground level. However, this level undergoes tiny fluctuations due to the electric fields within the laptop. These variations can be measured, and this can be used to leak information about encryption keys.

The measurements can be done by directly attaching a digitizer to a metal part of the laptop, but they don't have to be this obvious. The researchers showed that they could retrieve information with connections at the far end of shielded USB, VGA, and Ethernet connections. They also used human touch: a person in

contact with metal parts of the laptop can in turn be connected to a digitizer, and the voltage fluctuations can be measured.

The researchers note that this works better in hot weather, due to the lower resistance of sweaty fingers.

While the information retrieval was better when used with high-end lab equipment, the researchers also experimented with using a smartphone connected to Ethernet shielding via its headphone port, and found that this was sufficient to perform some attacks.
The major importance source of the voltage variations is the processor. The simplest thing to detect is probably whether the processor is active or sleeping, with the researchers saying that on almost all machines, the difference between an active processor and a processor suspended with the "HLT" instruction could be detected. On many machines, finer grained information was visible. The research recorded the fluctuations with a sample rate of between a few tens of kilohertz, and a few megahertz. These sample rates are far lower than the several gigahertz that processors operate, and so these measurements can't give insight into individual instructions—but this wasn't actually necessary.

During encryption and decryption operations, the processor has to perform certain long-running operations (for example, exponentiation of various large numbers), and these operations caused a consistent, characteristic set of voltage fluctuations. When sampling the voltages at a rate of a few MHz, keys for the RSA and ElGamal encryption algorithms could be extracted in a few seconds.

This attack required a single piece of encrypted data to be decrypted a few times.

Lower sampling rates of a few tens of kilohertz needed an adaptive attack, where multiple, specially chosen pieces of encrypted data are decrypted. The voltage fluctuations reveal a characteristic pattern that varies depending on whether a particular bit of the decryption key is a 1 or a 0. With enough chosen pieces of encrypted data, each bit of the decryption key can be determined.

The researchers have reported their findings to the GnuPG developers, and the software has been altered to reduce some of the information leaked this way.

Even with this alteration, the software is not immune to this side channel attack, and different encryption keys can be distinguished from one another. Robust protection is hard to do, because the side-channel is largely a feature of the hardware. Faraday cages can protect against electromagnetic side channels, insulation can protect against this kind of "touching metal parts" attack, and optical fibres can protect against measuring fluctuations in Ethernet connections, but all these drive up costs and are of limited practicality.

Source :
http://arstechnica.com/security/2014/08/stealing-encryption-keys-through-the-power-of-touch/

以　上