Physical Key Extraction Attacks on PCs

D. Genkin, L. Pachmanov, I. Pipman, A. Shamir, and E. Tromer, "Physical key extraction attacks on PCs," Communications of the ACM, vol. 59, pp. 70-79, 2016. doi:10.1145/2851486

Presented by Kuo-Hsing Chen

Summary

take advantage of information leakage from physical objects

- The article implements side-channel attacks to extract secret keys from RSA and ElGamal algorithm.

SIDE-CHANNEL ATTACKS

- Acoustic attacks
- Electric attacks
- Electromagnetic attacks

SIDE-CHANNEL ATTACK TECHNIQUES

- Internal value poisoning
- Leakage self-amplification

COUNTERMEASURES

- ✓ Sound-absorbing enclosures against acoustic attacks
- ✓ Fiber-optic connections against electric attacks
- ✓ Faraday cages against electromagnetic attacks

RESULTS

- ❑ **4,096-bit RSA keys** are extracted in about **one hour** in acoustic attacks
- ❑ RSA and ElGamal encryption are cracked in **a few seconds** in electric and electromagnetic attacks.

Aspect

- In Genkin 2016, the authors assert that side-channel attacks can be implemented by using **inexpensive equipment**.
  - This article did not mention how much these “inexpensive equipment” actually cost.
  - In my presentation, I will discuss **cost effectiveness** in terms of acoustic attacks and try to find out how much the authors actually spent.

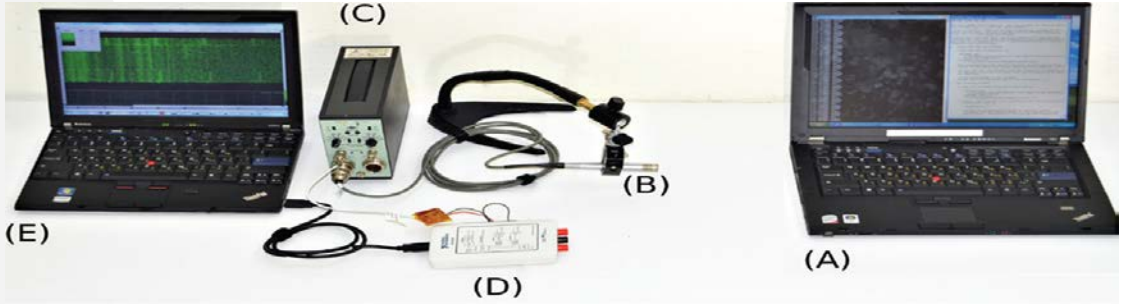
Acoustic Attacks

- **DEMONSTRATION**

Acoustic Attacks (cont.)

EQUIPMENT COST

	Price/NZD
a. A target computer	a. Priceless
b. A microphone	b. $10 – $1,000
c. A amplifier	c. $10 – $1,000
d. A digitizer	d. $10 – $1,000
e. Attacker's laptop with acoustic analysis software	e. Free acoustic software



Discussion

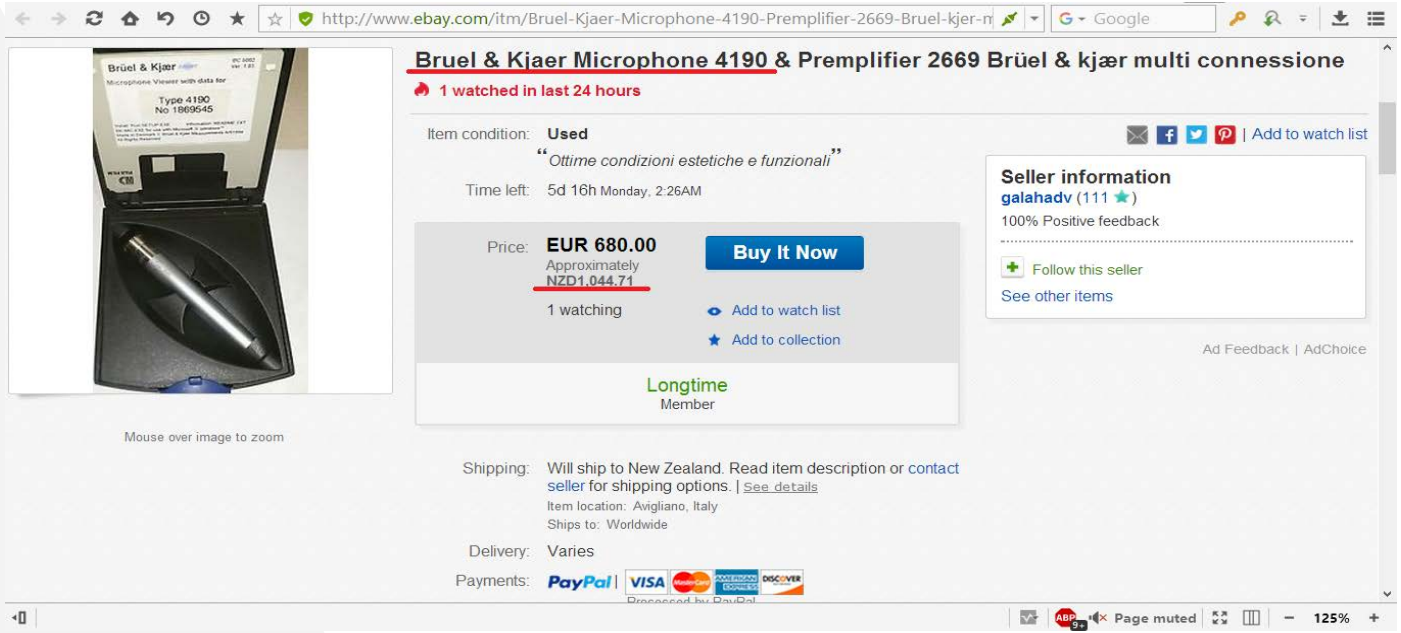
- **How much did the authors actually spend ?**

Fig. 2. Photograph of our portable setup. In this photograph, *a* is a Lenovo ThinkPad T61 target, *b* is a Brüel&Kjær 4190 microphone capsule mounted on a Brüel&Kjær 2669 preamplifier held by a flexible arm, *c* is a Brüel&Kjær 5935 microphone power supply and amplifier, *d* is a National Instruments MyDAQ device with a 10 kHz RC high-pass filter cascaded with a 150 kHz RC low-pass filter on its A2D input, and *e* is a laptop computer performing the attack. Full key extraction is possible in a similar configuration from a distance of 1 m (see Sect. 5.4).

D. Genkin, A. Shamir, and E. Tromer, "Acoustic Cryptanalysis," Journal of Cryptology, p1-52, 2016. doi:10.1007/s00145-015-9224-2

Discussion (cont.)

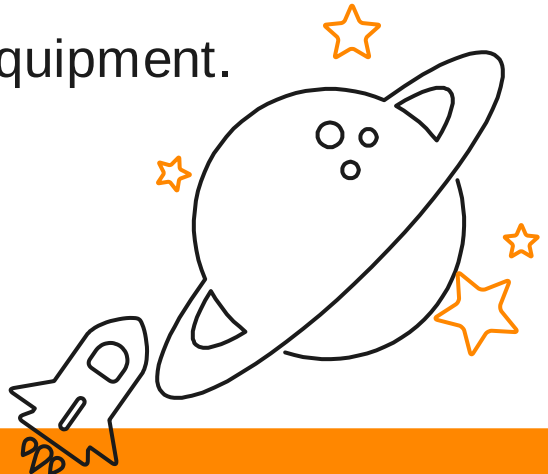
- Screenshot from ebay



http://www.ebay.com/itm/Bruel-Kjaer-Microphone-4190-Premplifier-2669-Bruel-kjer-multi-connessione-/142118402557?hash=item2116eab9fd:g:CogAAOSw0UdXsrkv

Conclusion

- Cost effectiveness?
- One hour to get RSA secret keys using costly equipment, what if using inexpensive exquipment?
- To persuade audience by using inexpensive equipment.



THANK YOU !

Any questions?