Covert Channels Using Mobile Device's Magnetic Field Sensors

Nikolay Matyunin, Jakub Szefer,

Sebastian Biedermann, Stefan Katzenbeisser

TECHNISCHE UNIVERSITÄT DARMSTADT

Yale University

Security Engineering Group, TU Darmstadt

Computer Architecture and Security Lab, Yale University

Covert channels: scenario

A target computer

- protected by firewalls, IDS etc.
- or even isolated into an **air-gap**
- infected by the attacker

An attacker

- has no network access
- may have no physical access
- wants to exfiltrate data from the target

➡ The attacker needs a **covert channel** to transmit data

Covert channels: examples

- **Electromagnetic**
  - CPU emissions and a dedicated receiver [1]
  - CPU-RAM emissions and a mobile phone with patched firmware [2]
- **Acoustic**
  - transmission using ultrasonic sounds [3,4]
- **Thermal**
  - using built-in thermal sensors [5]

Covert channels: requirements

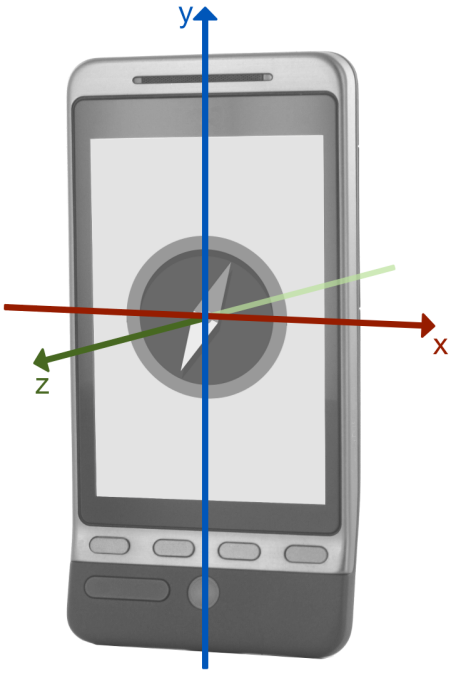
Use of hardware is restricted in air-gapped networks	→	Covert channel should not require dedicated hardware
Physical access is limited	→	Covert channel should be easily deployed to victim's device

Our motivation: a new covert channel, applicable to any commonly used hardware

Covert channels: a new approach

Idea: Use of smartphone's magnetic sensors

- installed in every modern smartphone
- used to measure magnetic field along 3 axes
- available through OS API

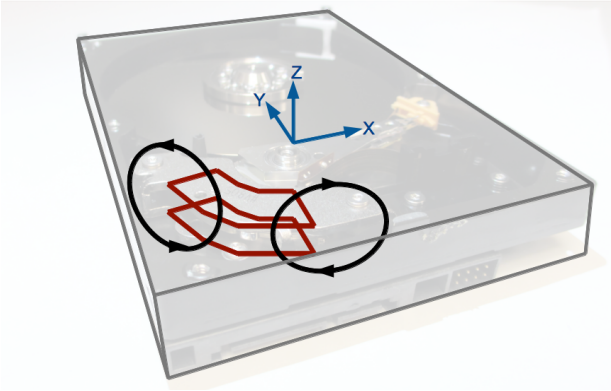


Basic use case: track phone orientation in space

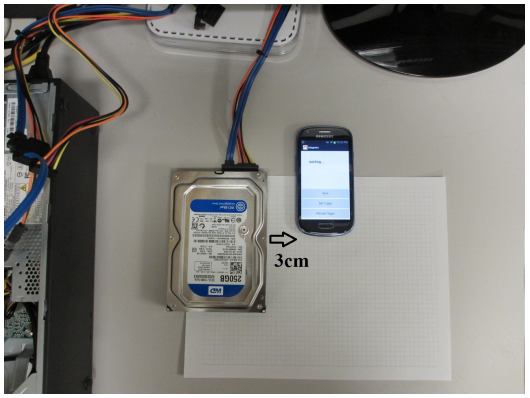
Our approach: measure magnetic signals emanated from a target device

Hard drive side-channel attack

Previous results: side-channel attack on hard drives (FC'2015)



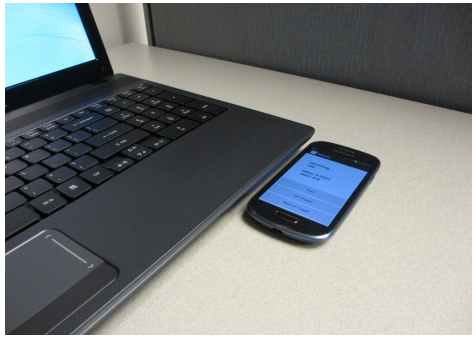
Head movements lead to EM fluctuations

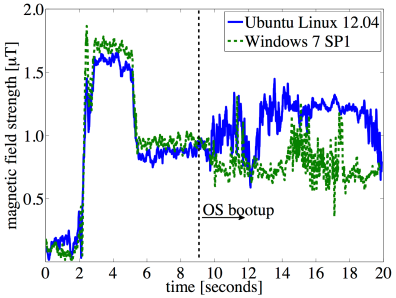


Magnetic sensors can detect hard drive activity

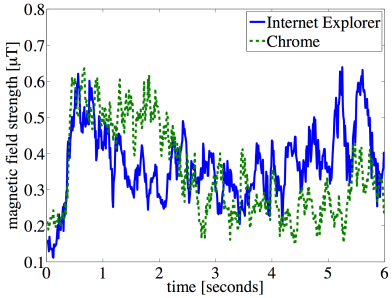
Hard drive side-channel attack (2)

1. Attacks against a laptop



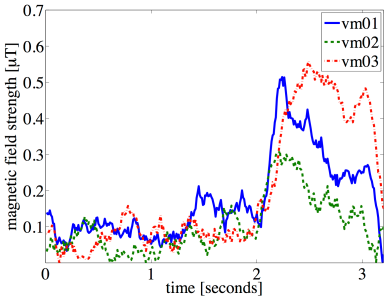


OS boot fingerprint

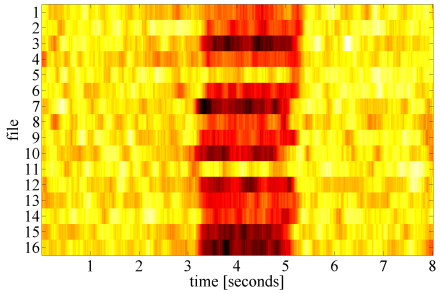


Application detection

2. Attacks against a server



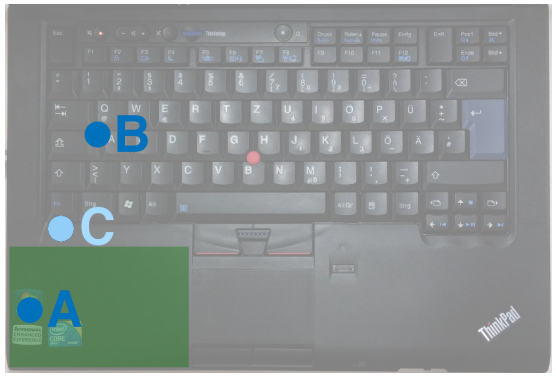
VM boot detection



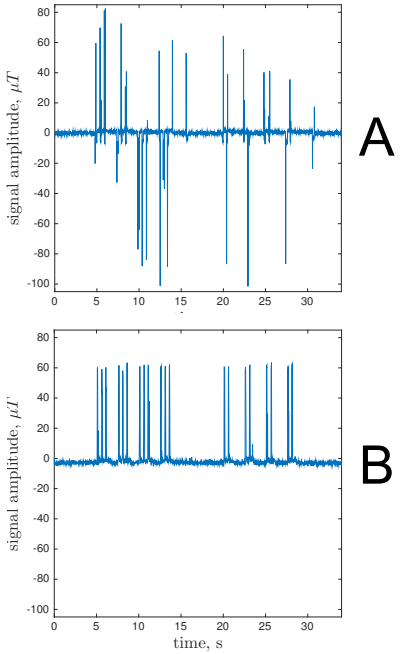
File caching detection

Electromagnetic covert channel

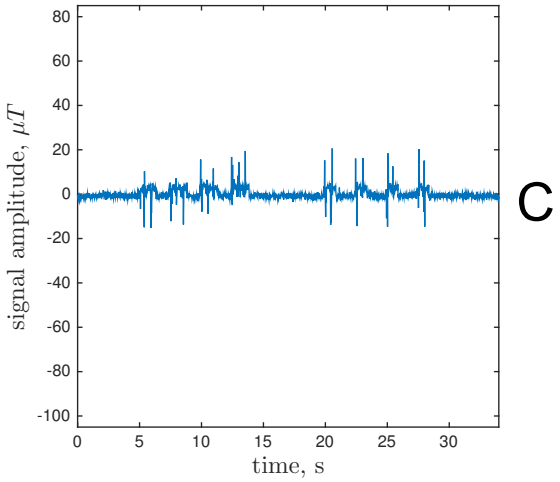
Basic operation: writing random data to the hard drive produces a single peak



Two sources of the signal



Peaks are different for sources A and B



Signals interfere in the intermediate position C

Amplitude modulation

Transmitter:

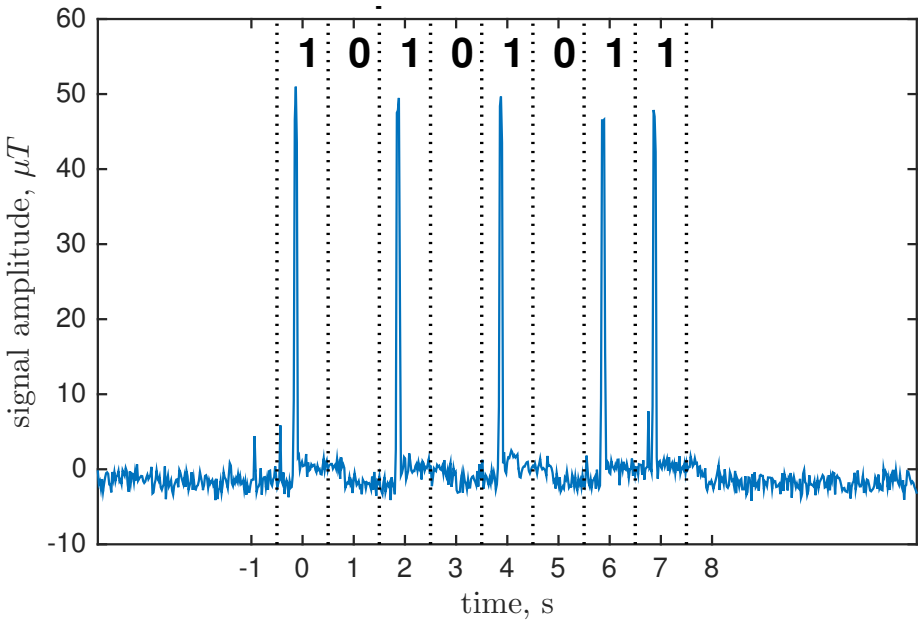
Emit a single peak for ‘1’,

no activity for ‘0’

Receiver:

Cross-correlation with

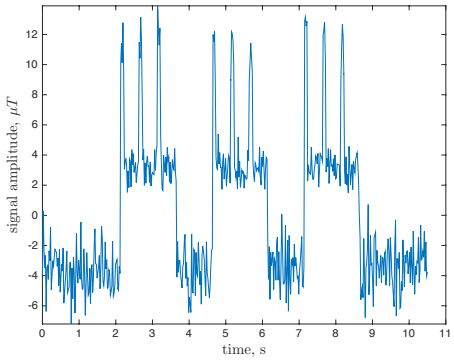
predefined patterns



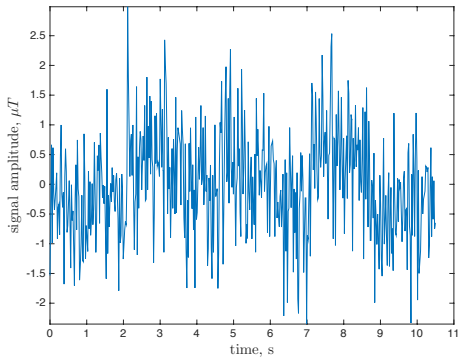
Amplitude modulation example

Amplitude modulation: limitations

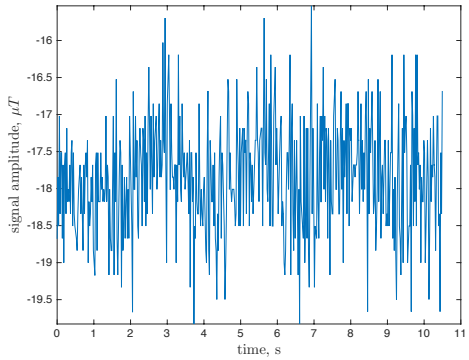
- **Signal fading** (theoretically $B \propto \frac{1}{d^2}$)



~3cm



~16cm



~20cm

- **Shape of peaks depends on**
  - hardware
  - distance → We still expect disturbance of the field
  - interference

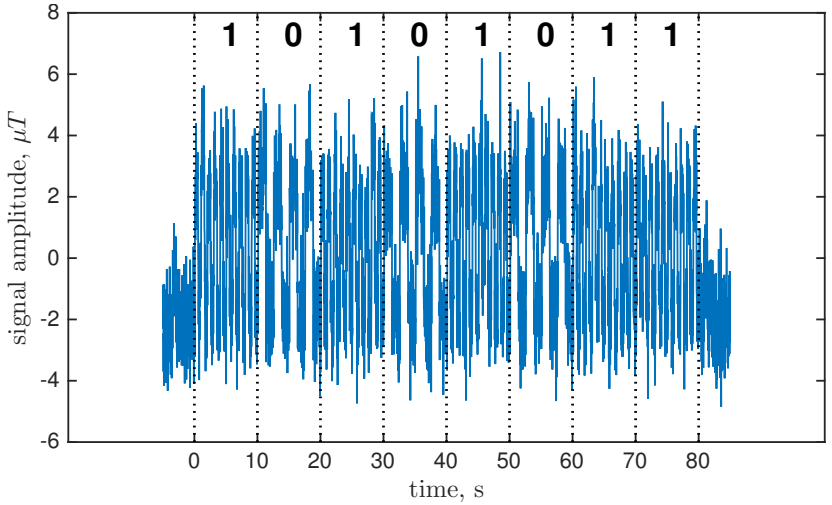
Periodic-based modulation

Transmitter:

Periodically emit consecutive peaks followed by pause, with two different frequencies

Receiver:

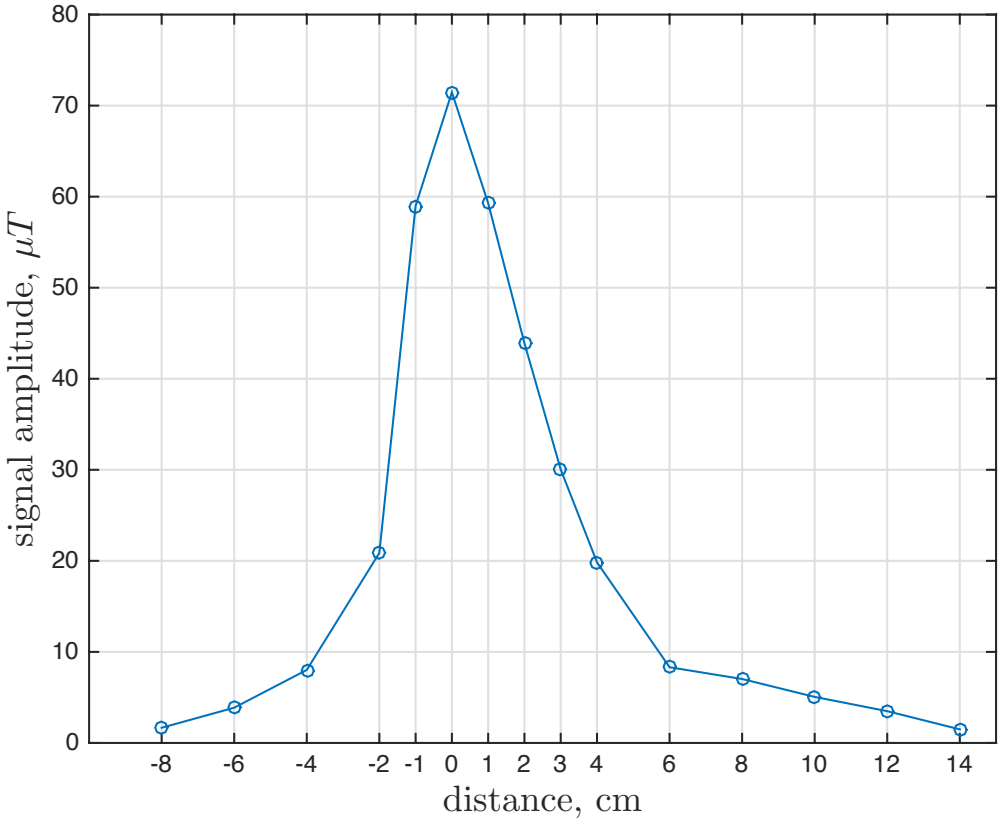
Perform the FFT, detect peaks and choose the corresponding peak frequency



Periodic-based modulation example

Results: signal fading

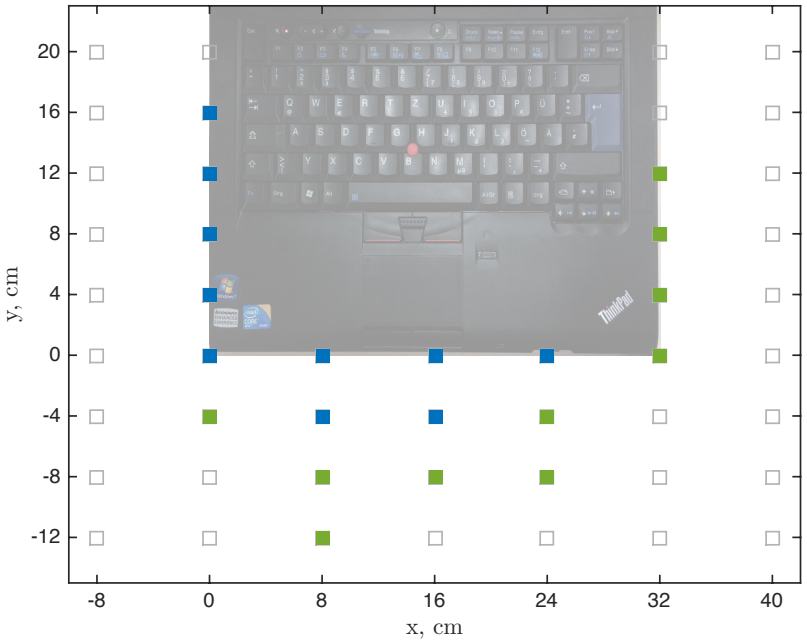
Amplitude of the signal depending on the distance from the source



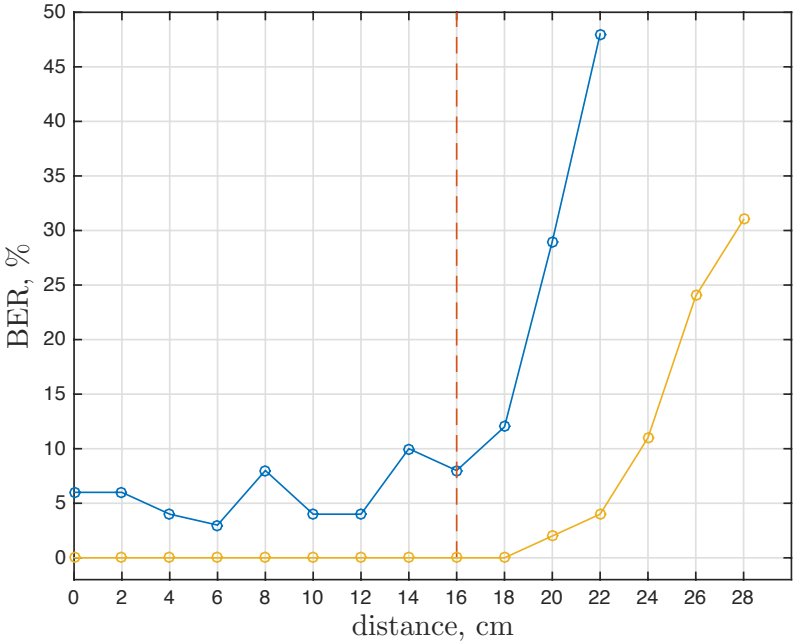
Signal fades conforming to $B \propto \frac{1}{d^2}$ and becomes comparable to noise at the distance of 14cm

Results: transmission distance

Presence of the signal



BER depending on the distance



Using periodic-based modulation, a signal is successfully decoded in the area up to 12cm in front of the laptop

Summary

- A new covert channel is presented
- Dedicated hardware or explicit permissions are not required
- Transmission distance is up to 12cm
- Protection against covert channels is necessary

Thank you!

Countermeasures

1. **Hardware level:** shield electronic components

2. **Software level:** limit access to magnetic sensors data

3. **OS level:** generate random I/O operations on a target system

References

[1] Callan, et al. "A practical methodology for measuring the side-channel signal available to the attacker for instruction-level events." *Proceedings of the 47th Annual IEEE/ACM International Symposium on Microarchitecture*. 2014.

[2] Guri, Mordechai, et al. "GSMem: data exfiltration from air-gapped computers over GSM frequencies." *24th USENIX Security Symposium*. 2015.

[3] M. Hanspach and M. Goetz. Recent developments in covert acoustical communications. In Sicherheit, pages 243–254, 2014.

[4] Deshotels, Luke. "Inaudible sound as a covert channel in mobile devices." *Proc. 8th USENIX Conf. Offensive Technologies*. 2014.

[5] Guri M. et al. BitWhisper: Covert Signalling Channel between Air-Gapped Computers using Thermal Manipulations //arXiv preprint arXiv:1503.07919. – 2015.