Security Risks posed by Temperature Measurements in Mobile Platforms

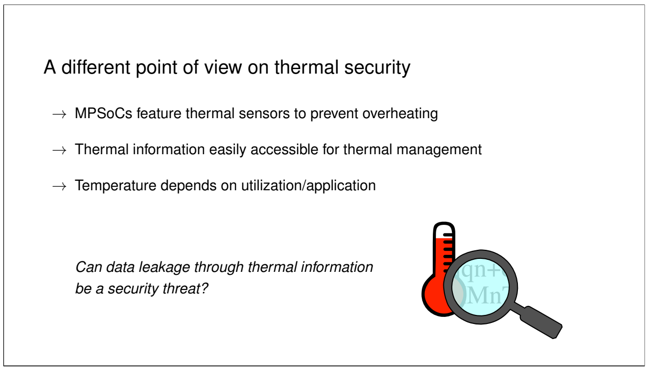
P. Miedl, R. Ahmed & L. Thiele

ETHZ

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644080."

SAFURE

SAFety and secURity by dEsign for interconnected mixed-critical cyber-physical systems



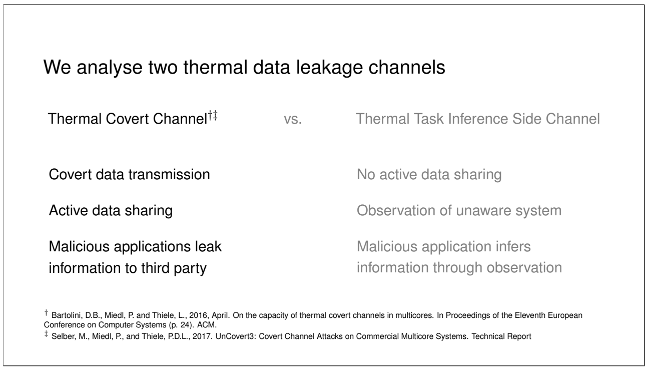
A different point of view on thermal security

→ MPSoCs feature thermal sensors to prevent overheating

→ Thermal information easily accessible for thermal management

→ Temperature depends on utilization/application

Can data leakage through thermal information be a security threat?

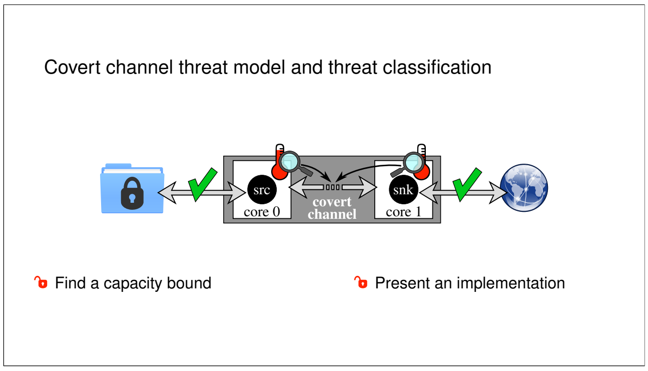


We analyse two thermal data leakage channels

Thermal Covert Channel[†‡]	vs.	Thermal Task Inference Side Channel
Covert data transmission		No active data sharing
Active data sharing		Observation of unaware system
Malicious applications leak information to third party		Malicious application infers information through observation

[†] Bartolini, D.B., Miedl, P. and Thiele, L., 2016, April. On the capacity of thermal covert channels in multicores. In Proceedings of the Eleventh European Conference on Computer Systems (p. 24). ACM.

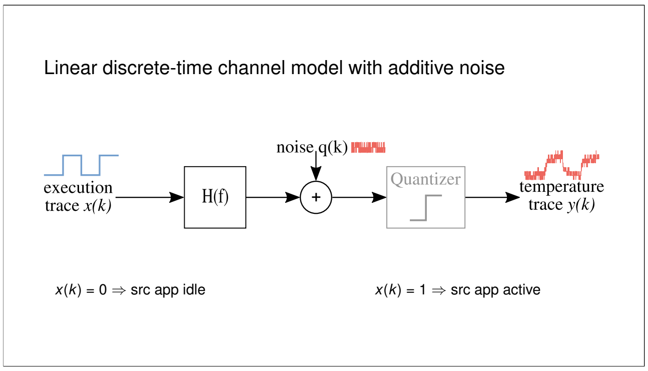
[‡] Selber, M., Miedl, P., and Thiele, P.D.L., 2017. UnCovert3: Covert Channel Attacks on Commercial Multicore Systems. Technical Report



Covert channel threat model and threat classification

Find a capacity bound

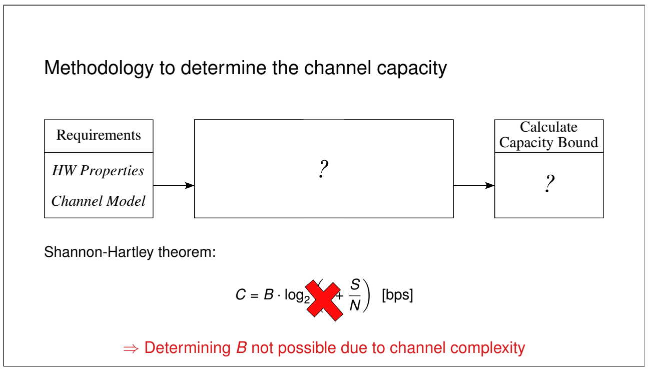
Present an implementation



Linear discrete-time channel model with additive noise

$x(k) = 0 \Rightarrow$ src app idle

$x(k) = 1 \Rightarrow$ src app active

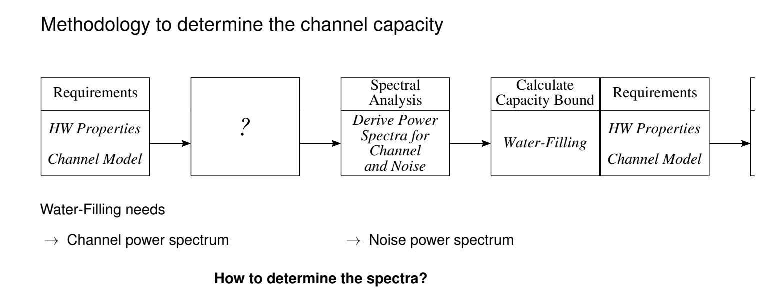


Methodology to determine the channel capacity

Shannon-Hartley theorem:

$$C = B \cdot \log_2 \cancel{\Big(1 +} \frac{S}{N}\Big) \text{ [bps]}$$

⇒ Determining *B* not possible due to channel complexity



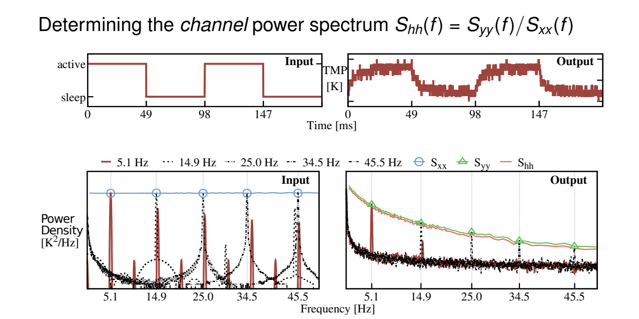
Methodology to determine the channel capacity

Water-Filling needs

→ Channel power spectrum

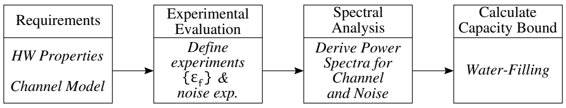
→ Noise power spectrum

How to determine the spectra?



Determining the *channel* power spectrum $S_{hh}(f) = S_{yy}(f)/S_{xx}(f)$

Methodology to determine the channel capacity



Estimation of the noise power spectrum

- Only needs one experiment
- Is not input dependent

Ability to determine capacity of complex covert channel

Experimental evaluation on two distinct platforms...

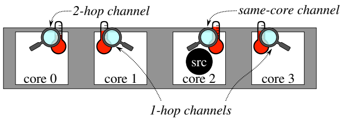
→ Odroid XU-3 representative of smartphones

→ Lenovo T440s representative of business laptops

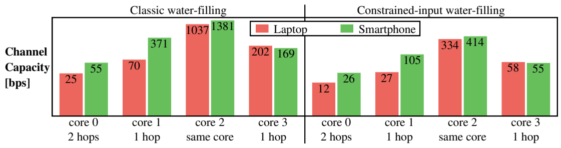
...under controlled conditions

- ✓ Core pinning
- ✓ Real time scheduling
- ✓ Limited wakeup latency
- ✓ Maximum fan speed
- ✓ Fixed operating frequency
- ✓ Ambient temperature ≈ 23 °C

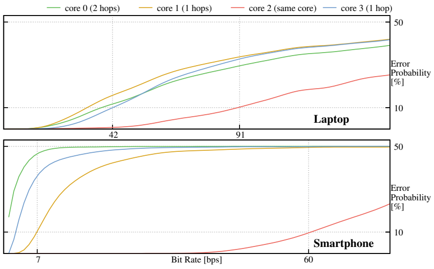
Assumption of linear core-alignment



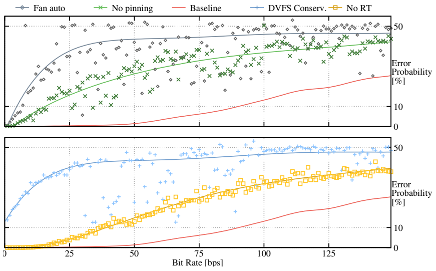
Capacity estimation ⇒ Thermal covert channel is security threat



Experimental evaluation shows feasibility of channel



High influence of external factors on channel performance



Leaked data 13′432 bits from a virtual machine under realistic conditions

Laptop with native Ubuntu and Ubuntu in a VirtualBox

System idle but no controlled environment

Advanced data encoding

Leaked information included a private SSH Key

Application Level Throughput (Goodput) of 1.358 bps

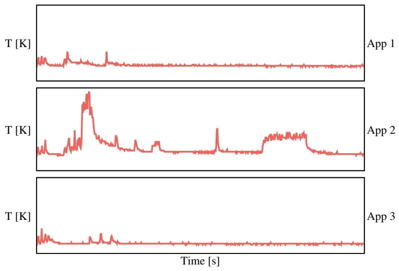
We analyse two thermal data leakage channels

Thermal Covert Channel[†‡]	vs.	Thermal Task Inference Side Channel
Covert data transmission		No active data sharing
Active data sharing		Observation of unaware system
Malicious applications leak information to third party		Malicious application infers information through observation

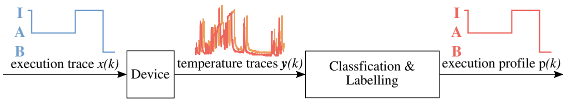
[†] Bartolini, D.B., Miedl, P. and Thiele, L., 2016, April. On the capacity of thermal covert channels in multicores. In Proceedings of the Eleventh European Conference on Computer Systems (p. 24). ACM.

[‡] Selber, M., Miedl, P., and Thiele, P.D.L., 2017. UnCovert3: Covert Channel Attacks on Commercial Multicore Systems. Technical Report

Different applications cause different thermal patterns



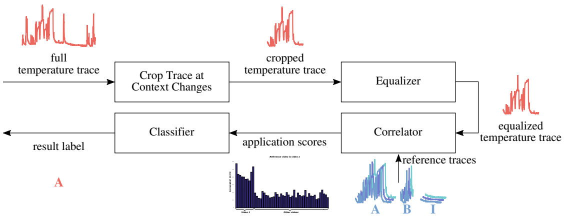
Basic concept thermal task inference side channel


I
A
B
execution trace $x(k)$
Device
temperature traces $y(k)$
Classfication & Labelling
I
A
B
execution profile $p(k)$

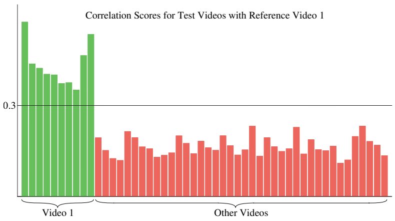
Possible outcomes:

- Allow advanced platform/user profiling
- New attack vector for side channel attacks

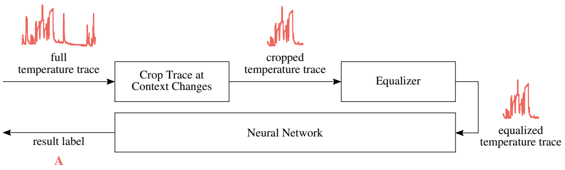
Feasibility study for thermal task inference using correlation on a Dragonboard 810


full temperature trace
Crop Trace at Context Changes
cropped temperature trace
Equalizer
equalized temperature trace
Correlator
reference traces
A
B
I
application scores
Classifier
result label
A

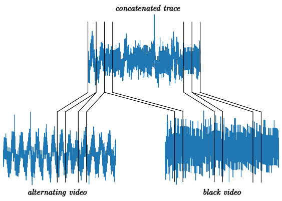
Thermal task inference using correlation with videos is feasible



Feasibility study for thermal task inference using neural networks


full temperature trace
Crop Trace at Context Changes
cropped temperature trace
Equalizer
equalized temperature trace
Neural Network
result label
A

Feasibility study using simple neural networks and augmented thermal data from Dragonboard 810



Simple neural networks work for augmented data but show weaknesses

Very simple dataset

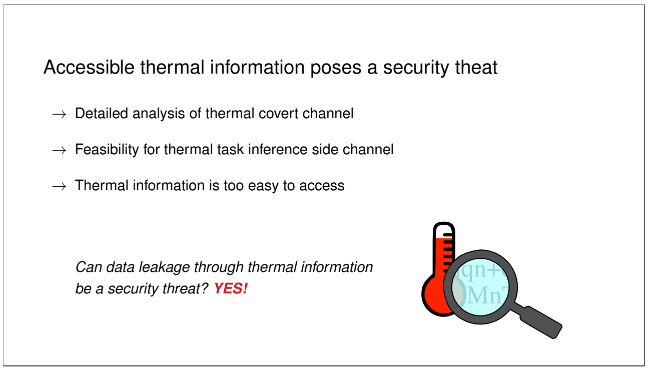
Very simple networks using LSTM (recurrent neural networks) or dense layers

Trace classification possible ⇒ Feasibility proven

Exponential growth for number of parameters & training time

Many open questions on thermal task inference

- Does it work for applications instead of videos?
- What are thermal features and thermal patterns?
- Are there relevant statistical measures?
- Can we use the temporal connection between features?
- Can we apply advanced machine learning techniques?



Accessible thermal information poses a security theat

→ Detailed analysis of thermal covert channel

→ Feasibility for thermal task inference side channel

→ Thermal information is too easy to access

Can data leakage through thermal information be a security threat? ***YES!***

SAFURE Grant Agreement No. 644080

"This project has received funding from the European Unions Horizon 2020 research and innovation programme under grant agreement No 644080."

"This work was supported by the Swiss State Secretariat for Education Research and Innovation (SERI) under contract number 15.0025. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Swiss Government."

If you need further information, please contact the coordinator:
TECHNIKON Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a, 9500 Villach, AUSTRIA
Tel: +43 4242 233 55, Fax: +43 4242 233 55 77
E-Mail: coordination@safure.eu

The information in this document is provided as is, and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

17th January 2018

2 / 2

SAFURE SAFety and secURity by dEsign for interconnected mixed-critical cyber-physical systems