SCIENCE
PASSION
TECHNOLOGY

Power-Related Side-Channel Attacks using the Android Sensor Framework

Mathias Oberhuber Martin Unterguggenberger Lukas Maar Andreas Kogler Stefan Mangard

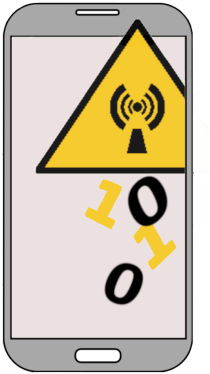
Graz University of Technology

NDSS 2025

› isec.tugraz.at

About

Android **power-related** side channel



About

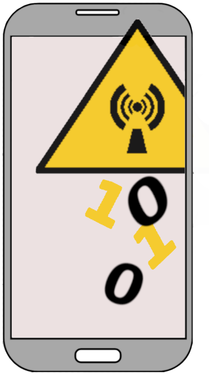
Android **power-related** side channel

- Android sensor interface as a proxy for power measurements purely from software

About

Android **power-related** side channel

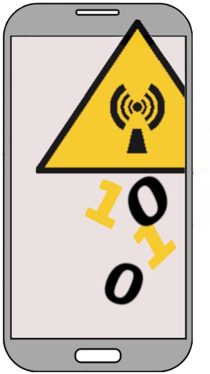
- Android sensor interface as a proxy for power measurements purely from software
- Systematic analysis of 9 Android smartphones:
  - Recovering leakage properties: Integration interval, rotation-dependent leakage



About

Android **power-related** side channel

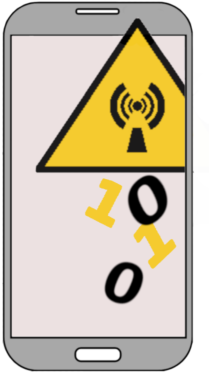
- Android sensor interface as a proxy for power measurements purely from software
- Systematic analysis of 9 Android smartphones:
  - 🕵 Recovering leakage properties: Integration interval, rotation-dependent leakage
- Local attack:
  - 🕵 Malicious app leaking processed AES key bytes



About

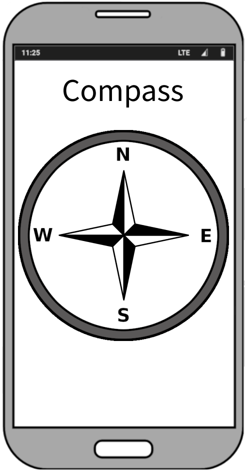
Android **power-related** side channel

- Android sensor interface as a proxy for power measurements purely from software
- Systematic analysis of 9 Android smartphones:
  - Recovering leakage properties: Integration interval, rotation-dependent leakage
- Local attack:
  - Malicious app leaking processed AES key bytes
- Remote web-based JavaScript attack:
  - JavaScript sensor-based pixel-stealing attack leaking cross-origin pixels up to 5 $\mathrm{s}/\mathrm{pixel}$

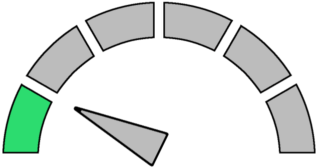


Motivation & Background

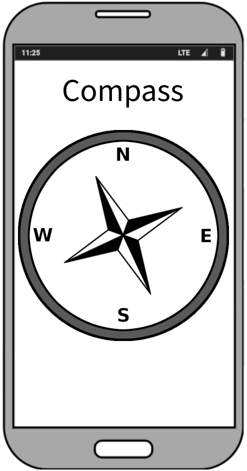
Motivation



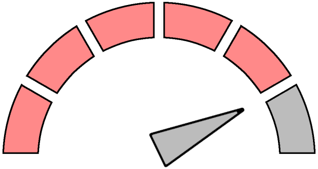
CPU utilization



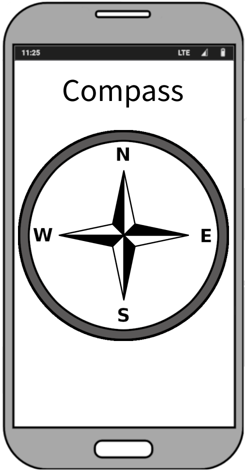
Motivation



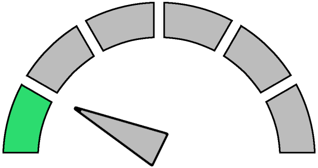
CPU utilization



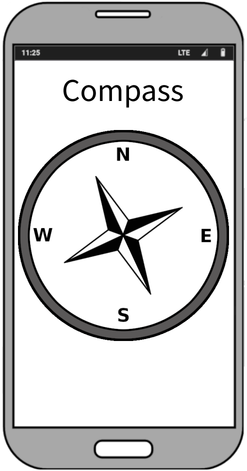
Motivation



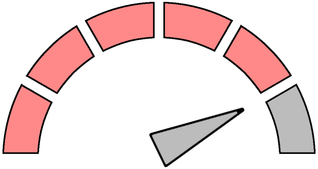
CPU utilization



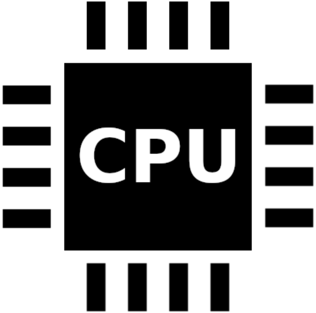
Motivation



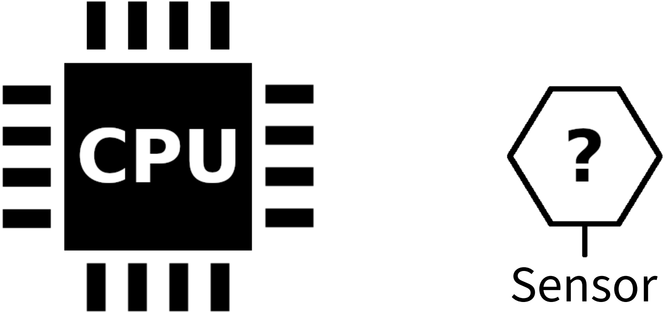
CPU utilization



Motivation

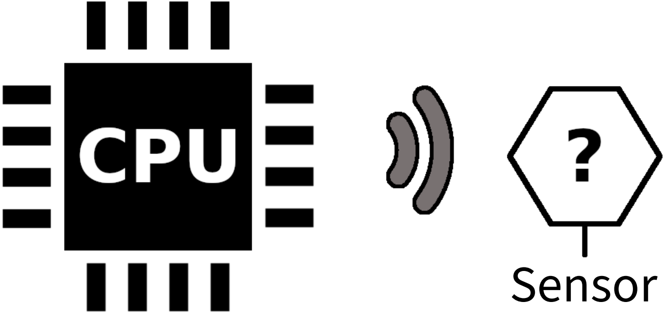


Motivation

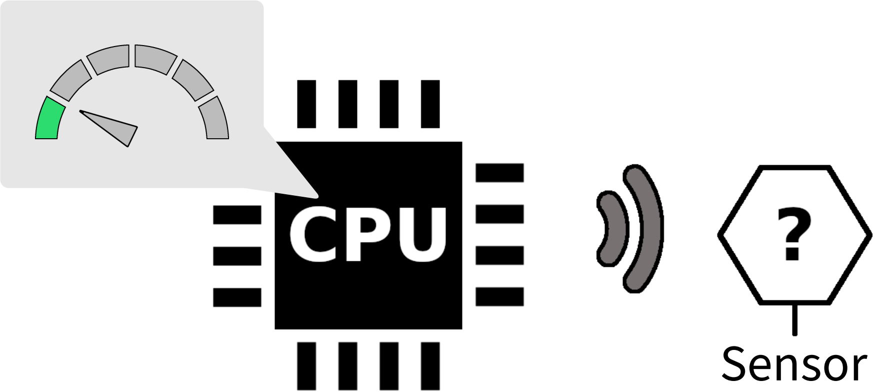


Sensor

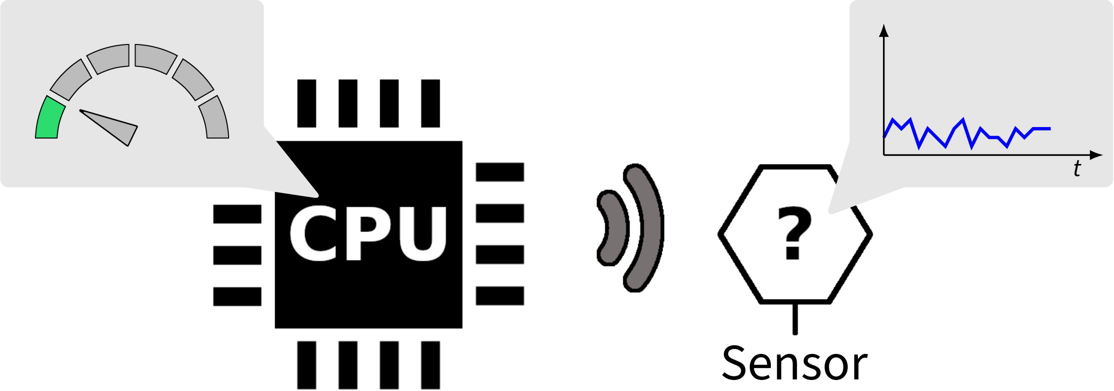
Motivation



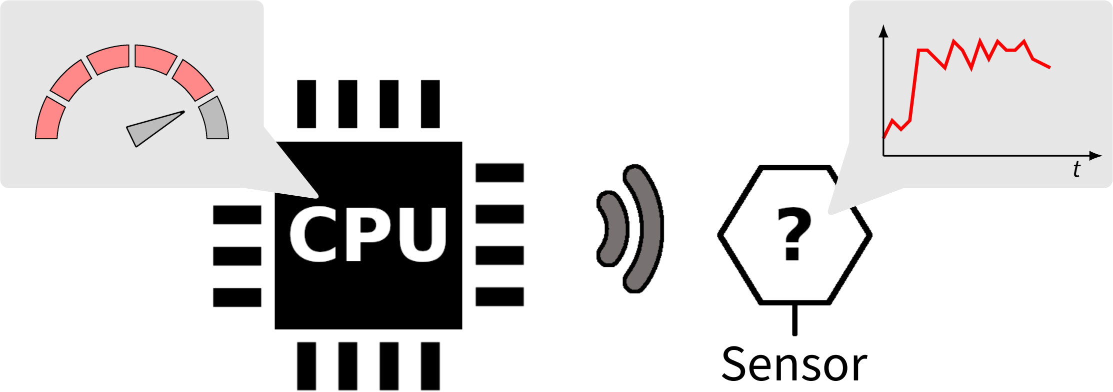
Motivation



Motivation

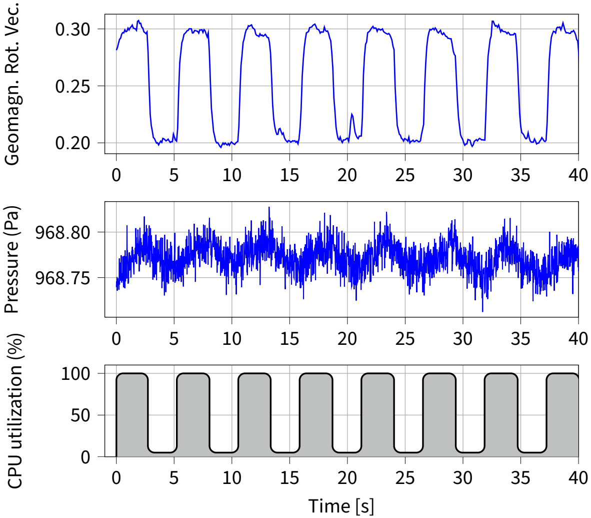


Motivation

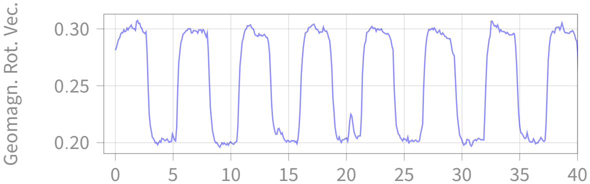


Systematic Evaluation

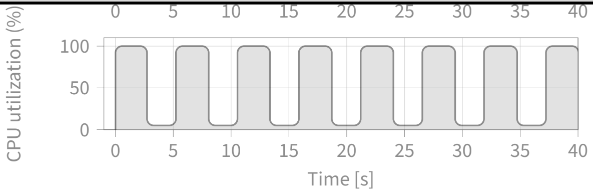
Systematic Evaluation: Varying CPU Utilization



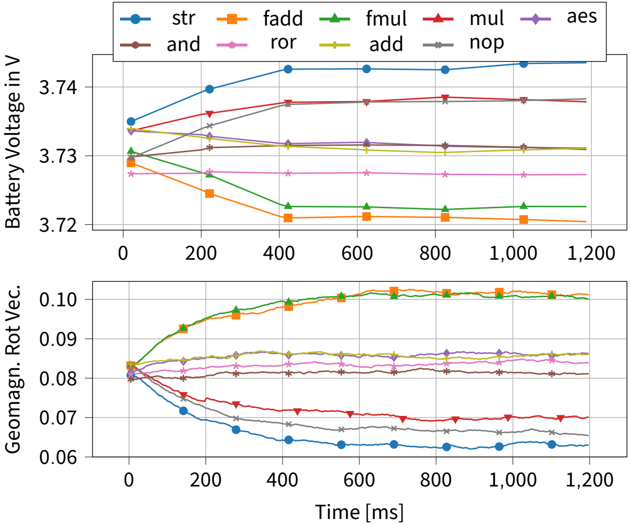
Systematic Evaluation: Varying CPU Utilization



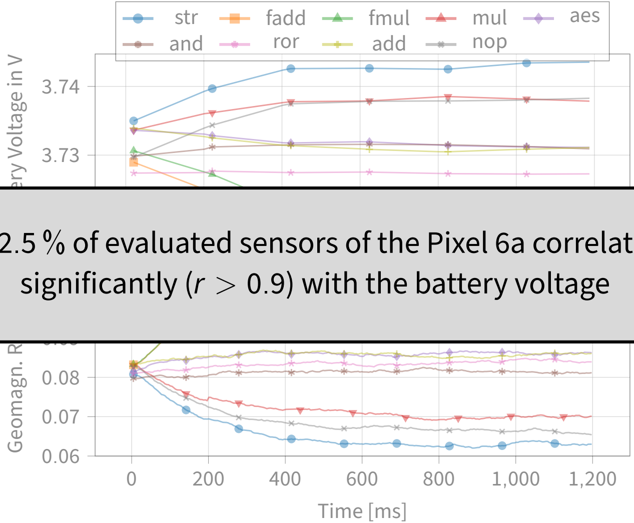
18.9 % of evaluated sensors expose significant influence of CPU utilization ($r > 0.7$)



Systematic Sensor Analysis: Executed Instructions

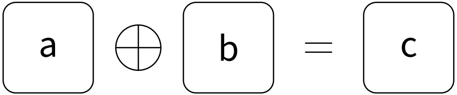


Systematic Sensor Analysis: Executed Instructions



12.5 % of evaluated sensors of the Pixel 6a correlate significantly ($r > 0.9$) with the battery voltage

Systematic Sensor Analysis: Varying Data Operands



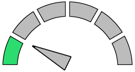
$a \oplus b = c$

Systematic Sensor Analysis: Varying Data Operands

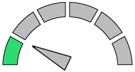
$$\boxed{a} \oplus \boxed{b} = \boxed{c}$$

$$a_0 \oplus b_0 = 00_2$$

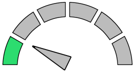
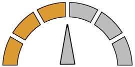
Systematic Sensor Analysis: Varying Data Operands

a	$\oplus$	b	=	c	Power
a_0	$\oplus$	b_0	=	00_2	

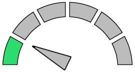
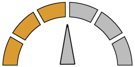
Systematic Sensor Analysis: Varying Data Operands

a	$\oplus$	b	=	c	Power
a_0	$\oplus$	b_0	=	00_2	
a_2	$\oplus$	b_2	=	01_2	

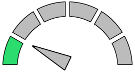
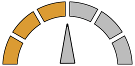
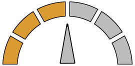
Systematic Sensor Analysis: Varying Data Operands

a	$\oplus$	b	=	c	Power
a_0	$\oplus$	b_0	=	00_2	
a_2	$\oplus$	b_2	=	01_2	

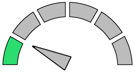
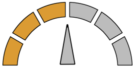
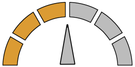
Systematic Sensor Analysis: Varying Data Operands

a	⊕	b	=	c	Power
a_0	$\oplus$	b_0	$=$	00_2	
a_2	$\oplus$	b_2	$=$	01_2	
a_2	$\oplus$	b_2	$=$	10_2	

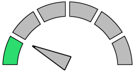
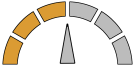
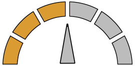
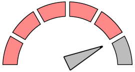
Systematic Sensor Analysis: Varying Data Operands

a	⊕	b	=	c	Power
a_0	$\oplus$	b_0	$=$	00_2	
a_2	$\oplus$	b_2	$=$	01_2	
a_2	$\oplus$	b_2	$=$	10_2	

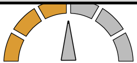
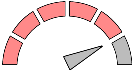
Systematic Sensor Analysis: Varying Data Operands

a	⊕	b	=	c	Power
a_0	⊕	b_0	=	00_2	
a_2	⊕	b_2	=	01_2	
a_2	⊕	b_2	=	10_2	
a_4	⊕	b_4	=	11_2	

Systematic Sensor Analysis: Varying Data Operands

a	⊕	b	=	c	Power
a_0	$\oplus$	b_0	=	00_2	
a_2	$\oplus$	b_2	=	01_2	
a_2	$\oplus$	b_2	=	10_2	
a_4	$\oplus$	b_4	=	11_2	

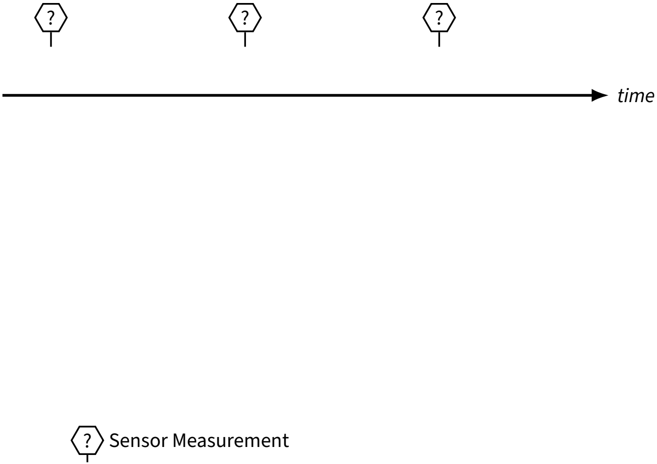
Systematic Sensor Analysis: Varying Data Operands

a	⊕	b	=	c	Power
a_2	$\oplus$	b_2	=	10_2	
a_4	$\oplus$	b_4	=	11_2	

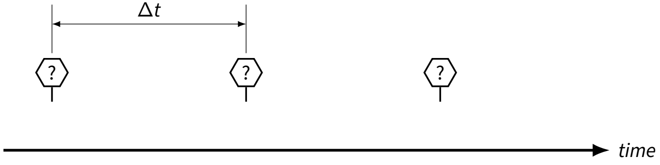
43.8 % of evaluated sensors demonstrate statistically significant correlation ($r > r_{noise}$) with executed data operands

Geomagnetic Rotation Leakage Properties

Geomagnetic Rotation: Analysis of Integrating Behavior

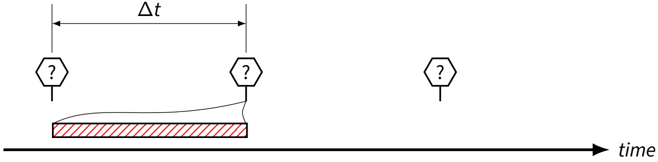


Geomagnetic Rotation: Analysis of Integrating Behavior



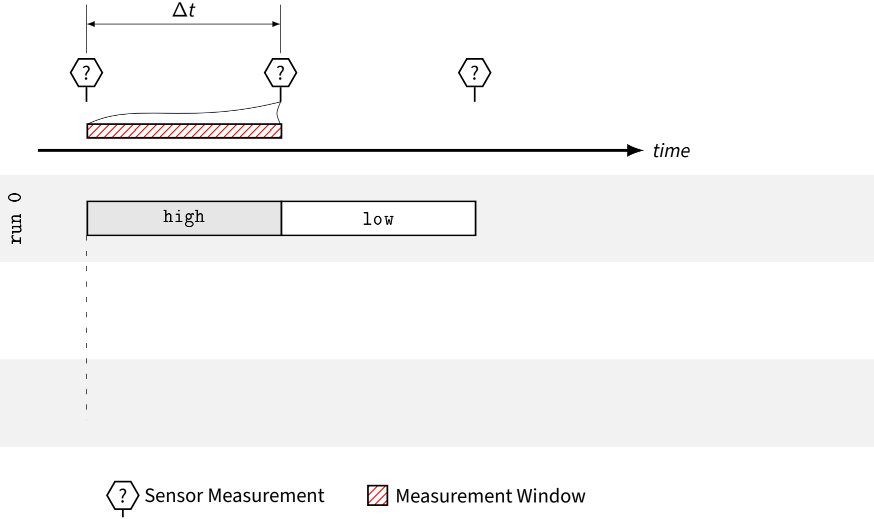
? Sensor Measurement

Geomagnetic Rotation: Analysis of Integrating Behavior

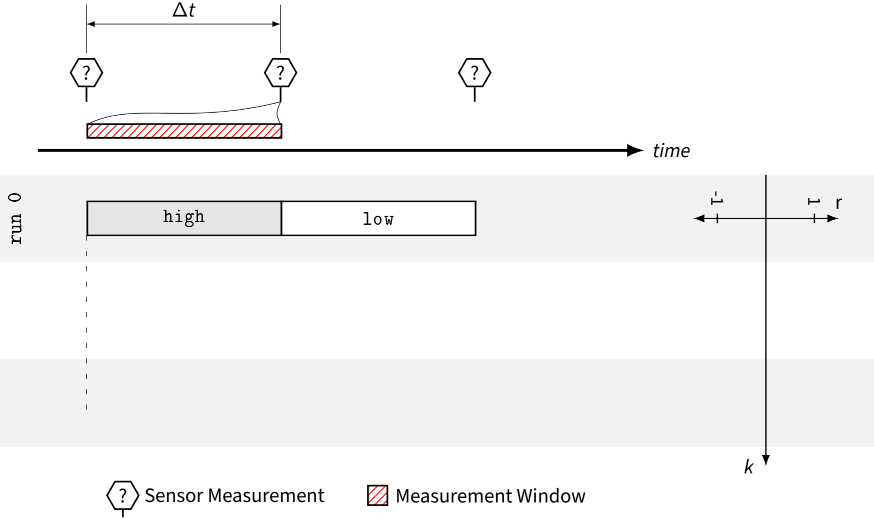


⬡ Sensor Measurement ▨ Measurement Window

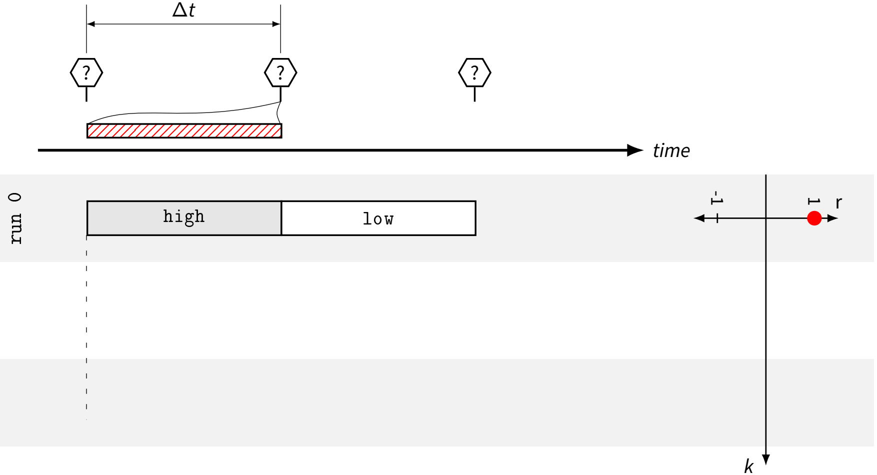
Geomagnetic Rotation: Analysis of Integrating Behavior



Geomagnetic Rotation: Analysis of Integrating Behavior

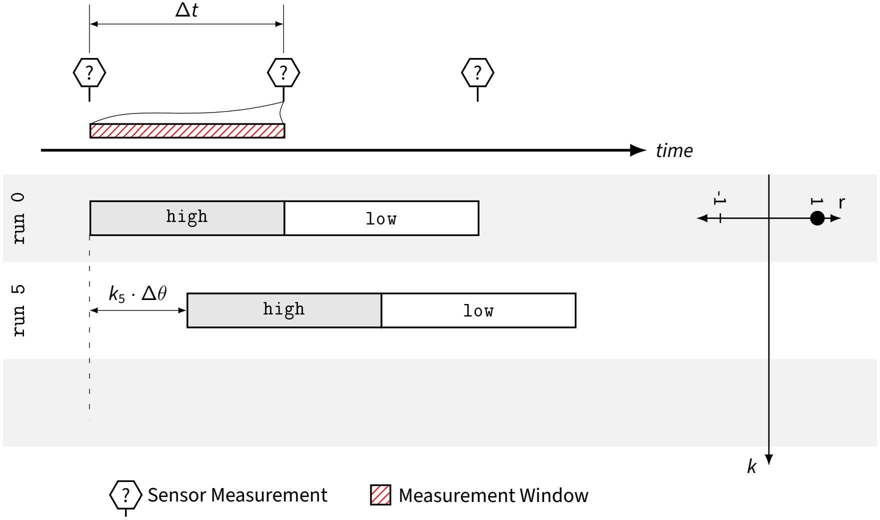


Geomagnetic Rotation: Analysis of Integrating Behavior

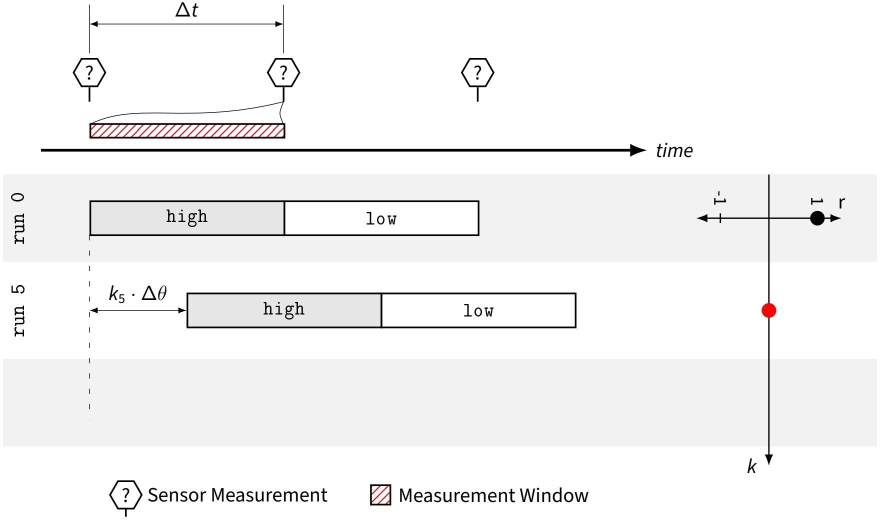


? Sensor Measurement ▨ Measurement Window

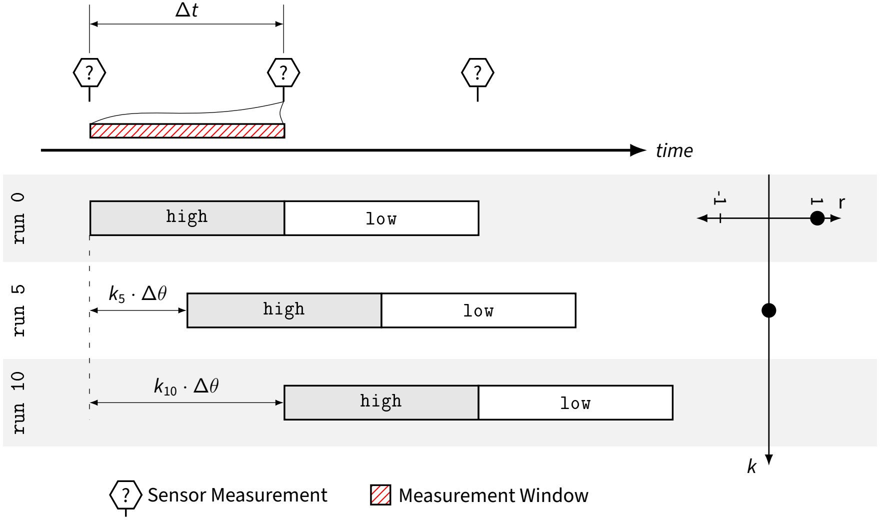
Geomagnetic Rotation: Analysis of Integrating Behavior



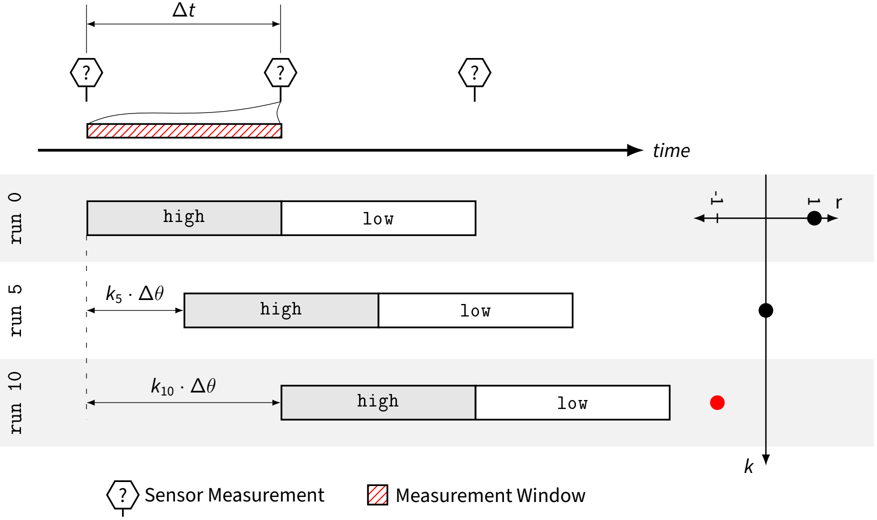
Geomagnetic Rotation: Analysis of Integrating Behavior



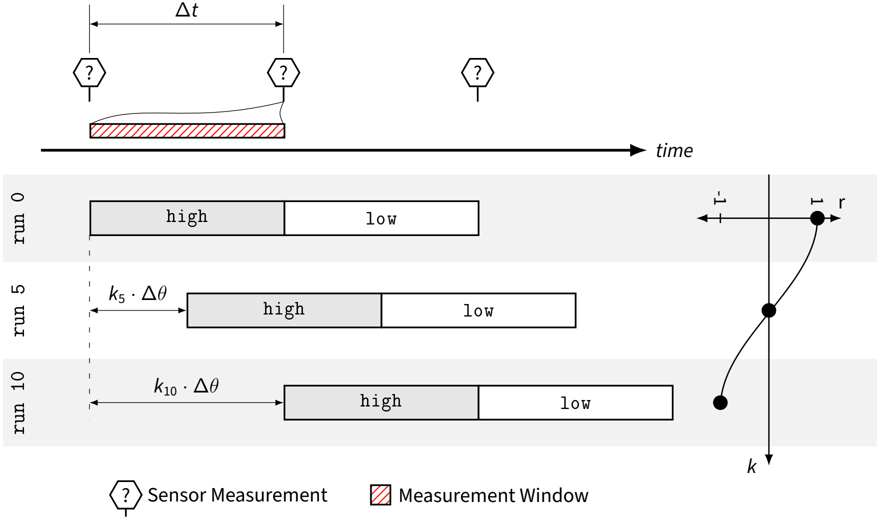
Geomagnetic Rotation: Analysis of Integrating Behavior



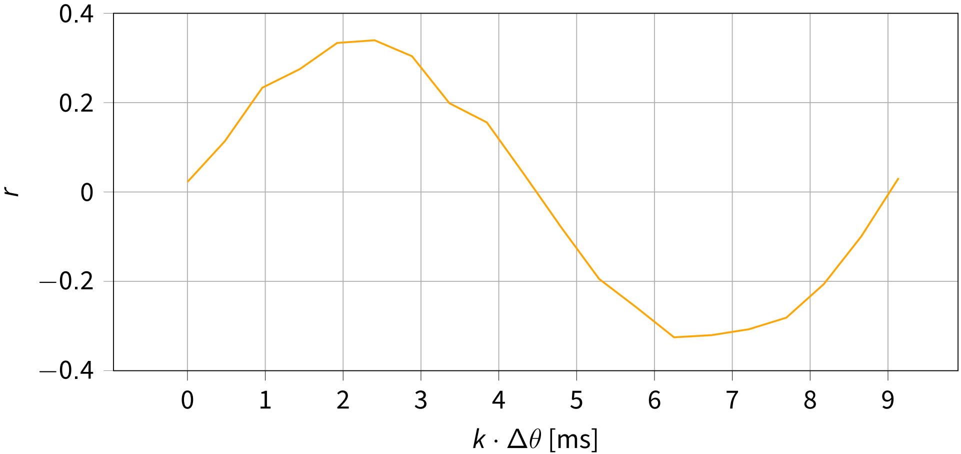
Geomagnetic Rotation: Analysis of Integrating Behavior



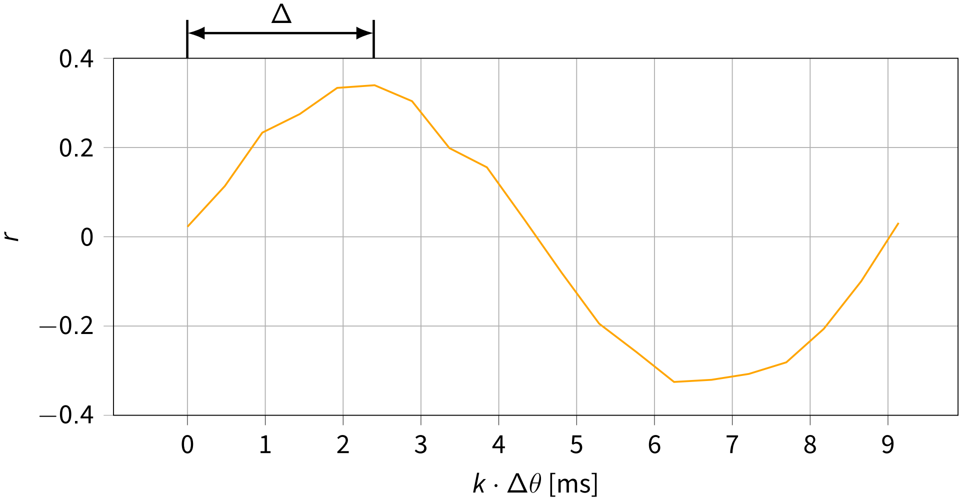
Geomagnetic Rotation: Analysis of Integrating Behavior



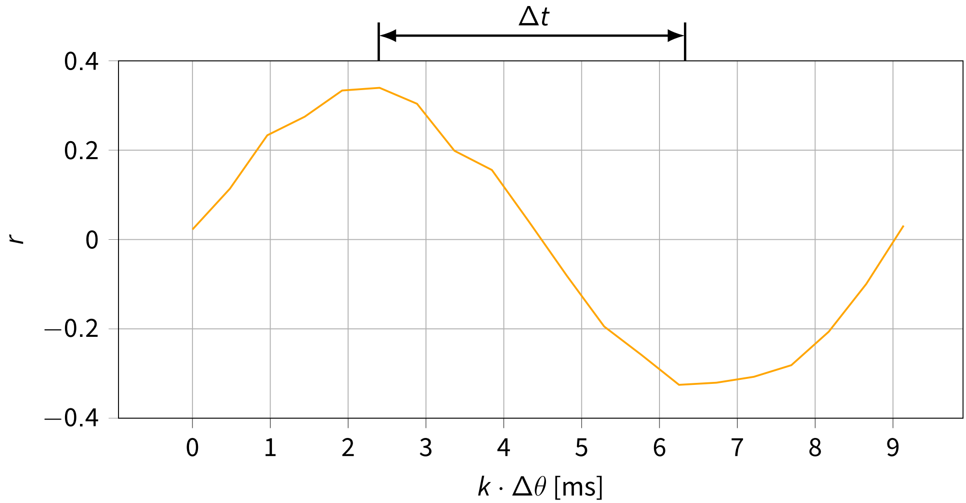
Geomagnetic Rotation: Analysis of Integrating Behavior



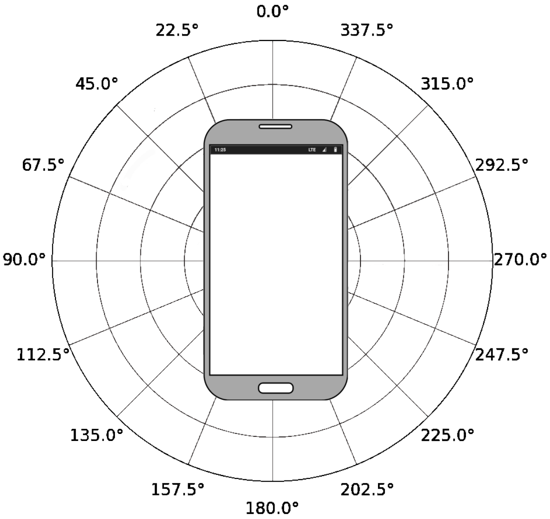
Geomagnetic Rotation: Analysis of Integrating Behavior



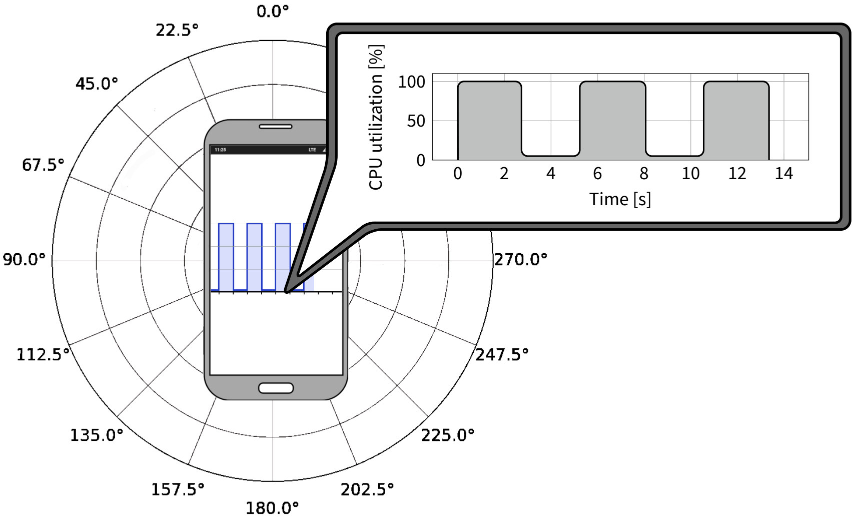
Geomagnetic Rotation: Analysis of Integrating Behavior



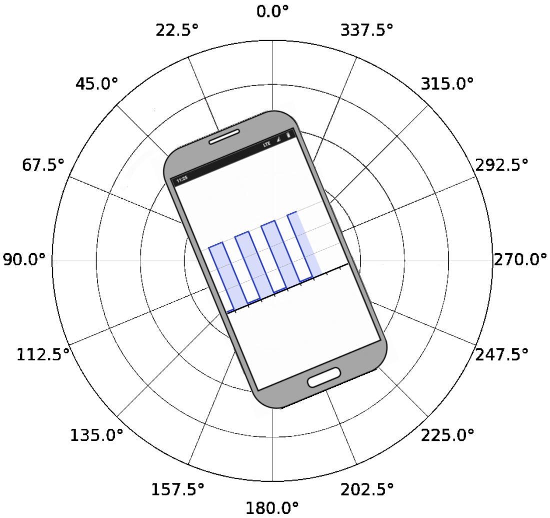
Geomagnetic Rotation: Orientation Dependent Leakage



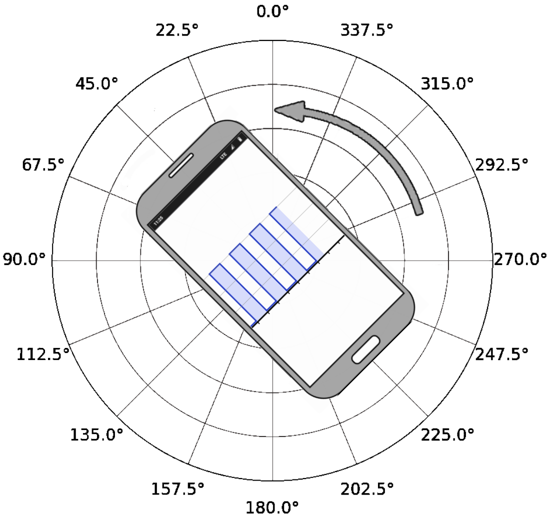
Geomagnetic Rotation: Orientation Dependent Leakage



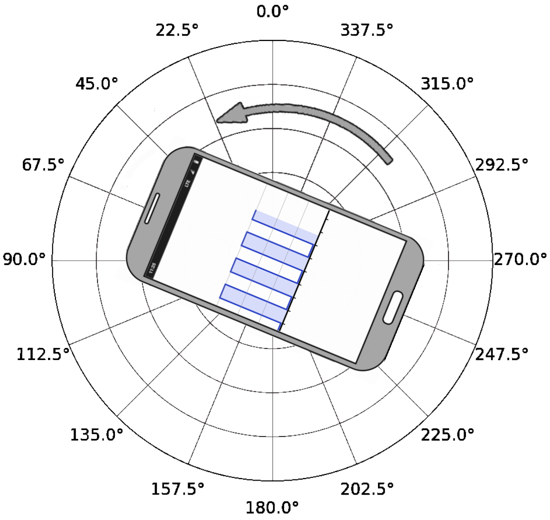
Geomagnetic Rotation: Orientation Dependent Leakage



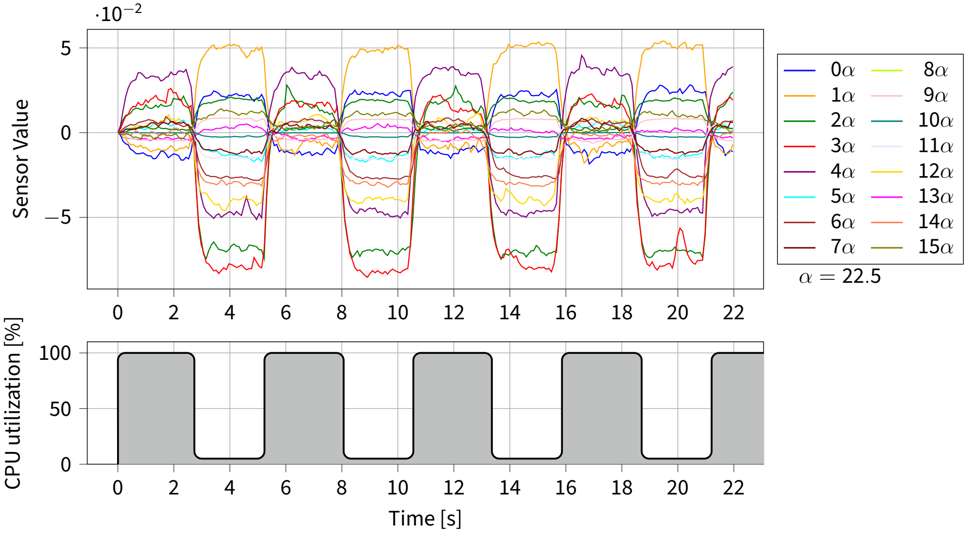
Geomagnetic Rotation: Orientation Dependent Leakage



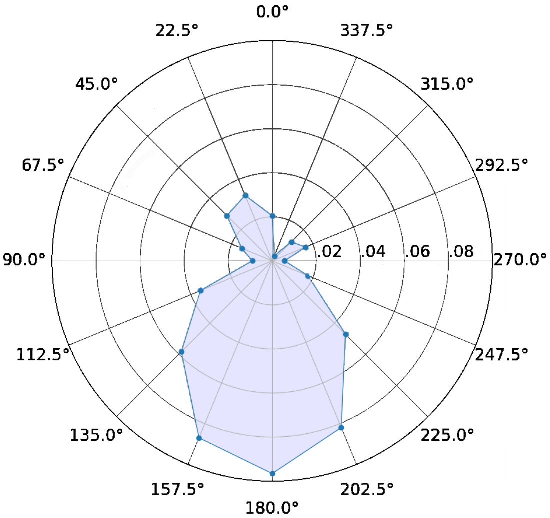
Geomagnetic Rotation: Orientation Dependent Leakage



Geomagnetic Rotation: Orientation Dependent Leakage

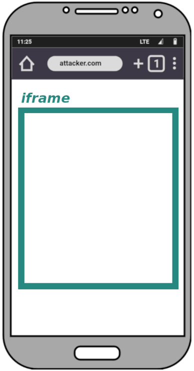


Geomagnetic Rotation: Orientation Dependent Leakage

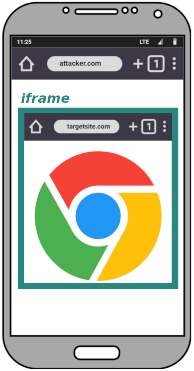


Attack Case Study:
JavaScript Pixel Stealing

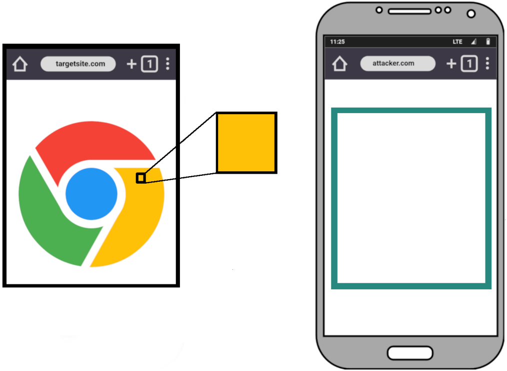
JavaScript Pixel-Stealing Attack



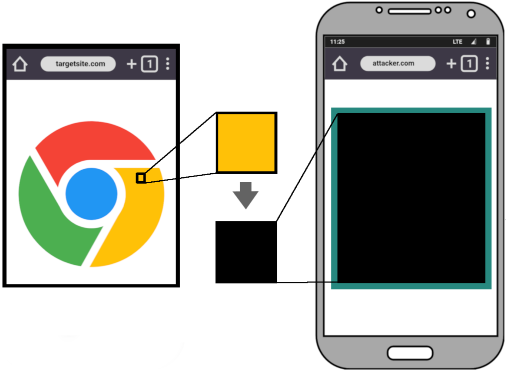
JavaScript Pixel-Stealing Attack



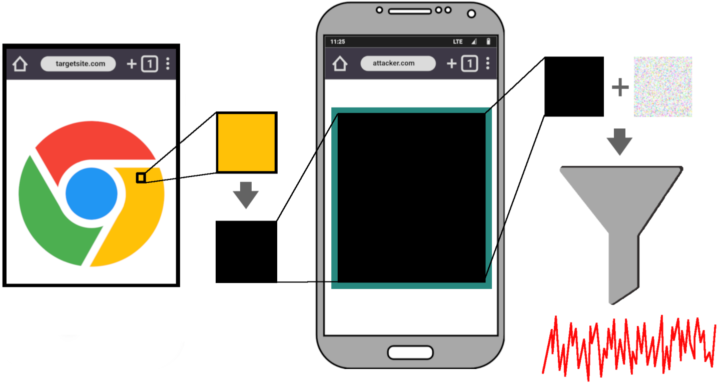
JavaScript Pixel-Stealing Attack



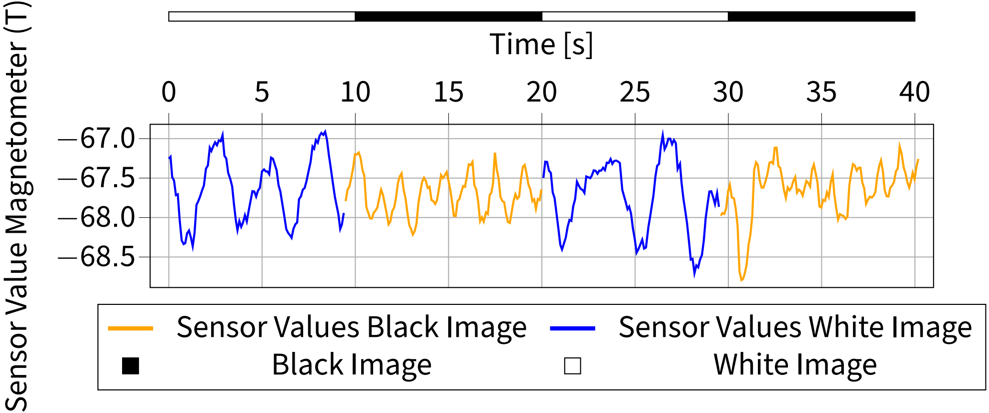
JavaScript Pixel-Stealing Attack



JavaScript Pixel-Stealing Attack



JavaScript Sensor Leakage Primitive: Magnetometer



JavaScript Pixel Stealing: Evaluation

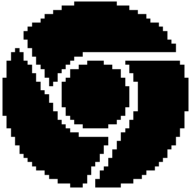
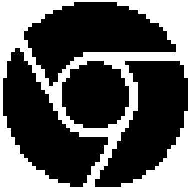
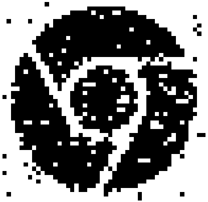
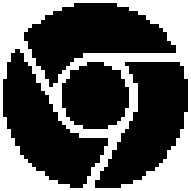
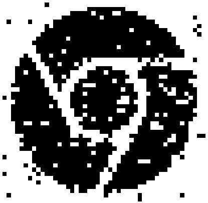
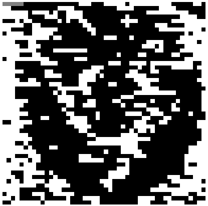
			

Image:
Time/Pixel (s):
Accuracy (%):
	Original		

JavaScript Pixel Stealing: Evaluation

			
Image:	Original	Magnetometer	
Time/Pixel (s):		5	
Accuracy (%):		90.2	

JavaScript Pixel Stealing: Evaluation

			
Image:	Original	Magnetometer	Abs. Orientation
Time/Pixel (s):		5	10
Accuracy (%):		90.2	70

Attack Case Study:
AES Correlation Power Analysis

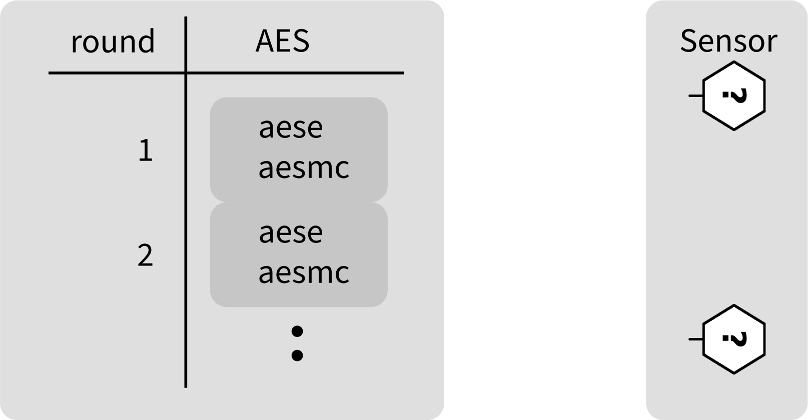
AES Attack Case Study

round	AES
1	aese aesmc

AES Attack Case Study

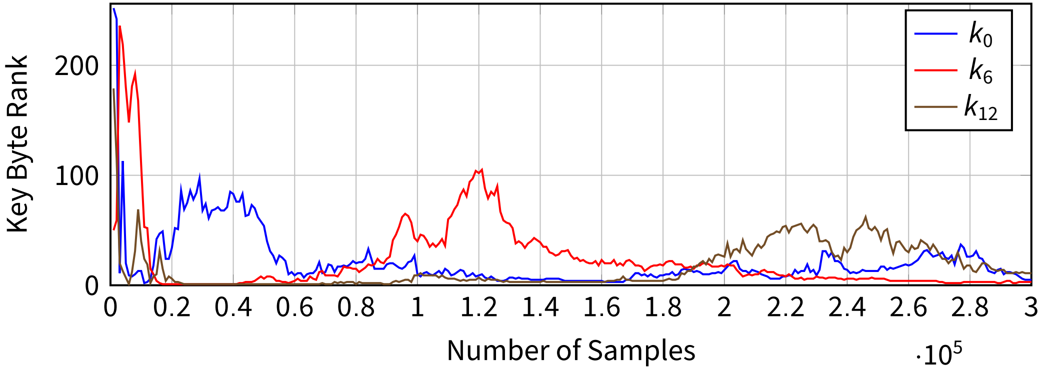
round	AES
1	aese aesmc
2	aese aesmc
	⋮

AES Attack Case Study



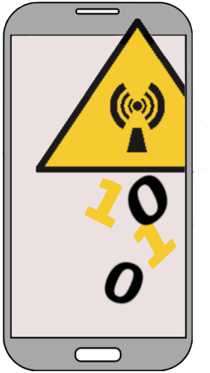
round	AES
1	aese aesmc
2	aese aesmc
	⋮

AES Correlation Power Analysis



Conclusion

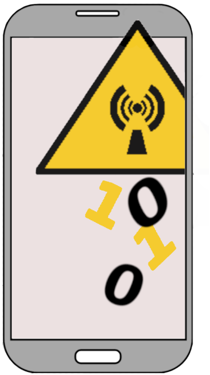
We presented an Android **power-related** side channel



Conclusion

We presented an Android **power-related** side channel

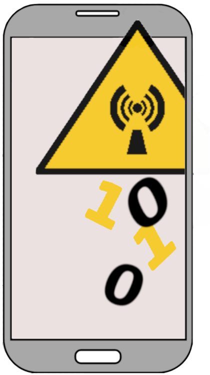
- We demonstrated that the Android sensor interface serves as a **proxy for power measurements** from software



Conclusion

We presented an Android **power-related** side channel

- We demonstrated that the Android sensor interface serves as a **proxy for power measurements** from software
- We presented a **systematic analysis** of 9 Android smartphones, discovering leakage properties



Conclusion

We presented an Android **power-related** side channel

- We demonstrated that the Android sensor interface serves as a **proxy for power measurements** from software
- We presented a **systematic analysis** of 9 Android smartphones, discovering leakage properties
- We demonstrated a **local attack** leaking processed AES key bytes

Conclusion

We presented an Android **power-related** side channel

- We demonstrated that the Android sensor interface serves as a **proxy for power measurements** from software
- We presented a **systematic analysis** of 9 Android smartphones, discovering leakage properties
- We demonstrated a **local attack** leaking processed AES key bytes
- We demonstrated a **remote web-based JavaScript pixel-stealing attack**

SCIENCE
PASSION
TECHNOLOGY

Power-Related Side-Channel Attacks using the Android Sensor Framework

Mathias Oberhuber Martin Unterguggenberger Lukas Maar Andreas Kogler Stefan Mangard

Graz University of Technology

NDSS 2025

› isec.tugraz.at