NEW DIRECTIONS IN PHYSICAL LAYER SECURITY – FROM PRIVACY PROTECTION TO NUCLEAR WARHEADS

Christof Paar

↘ *Max Planck Institute for Security and Privacy, Bochum, Germany*

Contact: christof.paar@mpi-sp.org

Summer School on Real-world Crypto and Privacy
Vodice, Croatia
June 04, 2024

ACKNOWLEDGEMENT

Paul Staat & Johannes Tobisch

AGENDA

1 Who We Are
2 Introduction to Wireless Sensing for Security and Privacy
3 Case Study I: Remote monitoring of nuclear warheads
4 Case Study II: Anti-Tamper Radio
5 Case Study III: IRShield
6 Conclusion

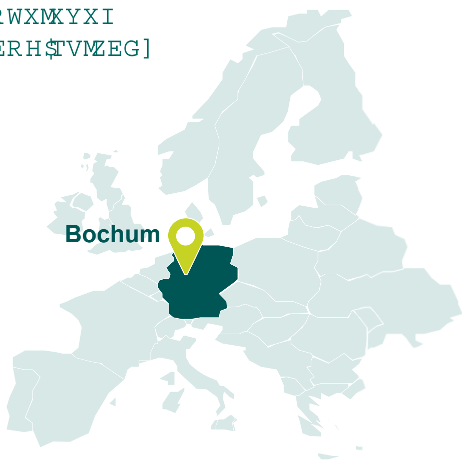
THE BOCHUM CYBERSECURITY ECOSYSTEM

QE\$TPERGO$MRWXMXYXI
JSV$WIGYVMX]$ERH$TVMZEG]

Ruhr University Bochum

CUBE 5 Creating Security

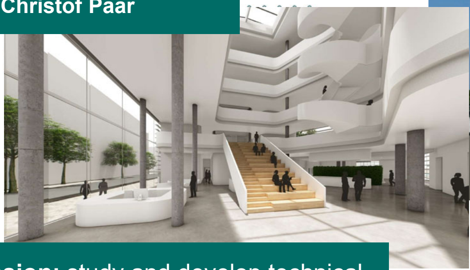
CASA CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES



HORST GÖRTZ INSTITUTE

MAX PLANCK INSTITUTE FOR SECURITY AND PRIVACY (MPI-SP)

Founded in May 2019 by Gilles Barthe and Christof Paar

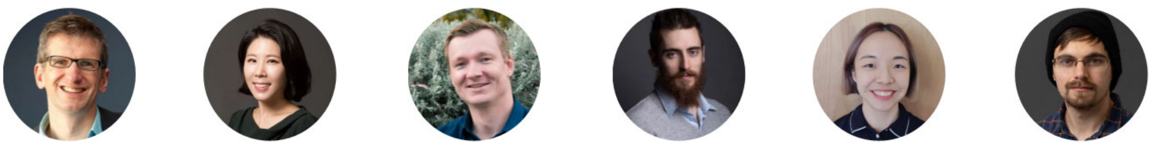


250+ Researchers
(currently around 80)

Mission: study and develop technical foundations and interdisciplinary aspects of security and privacy

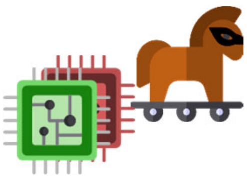
MPI-SP FACULTY

Gilles Barthe, Peter Schwabe, Asia Biega, Catalin Hritcu, Clara Schneidewind



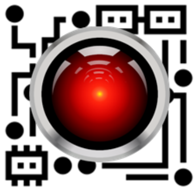
Christof Paar, Meeyoung Cha, Marcel Böhme, Giulio Malavolta, Yixin Zou, Abraham Mhaidli

EMBEDDED SECURITY GROUP



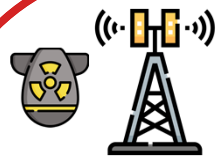
Hardware Security

- Hardware Trojans
- IP protection & infringement
- Circuit manipulation & countermeasures



Netlist Reverse Engineering

- Open-source framework HAL
- Automated netlist analysis
- Cognitive factors in hardware reverse engineering



Physical Layer Security

- New security primitives from radio-frequency channels
- Application: Nuclear disarmament control

AGENDA

1 Who We Are
2 Introduction to Wireless Sensing for Security and Privacy
3 Case Study I: Remote monitoring of nuclear warheads
4 Case Study II: Anti-Tamper Radio
5 Case Study III: IRShield
6 Conclusion

THE CYBERSECURITY ZOO

PKI
Trusted Execution
Certificates
Post-Quantum Cryptography
Formal Verificati
chitecture
Blockchain
ro Knowledge
omorphic Encryption
TLS
Fuzzing
Differential Privacy
RSA
Secure Multiparty Computation
Authentication
Threshold Signatures

Many well-established and proven methods

What about security problems in the physical domain?

DIGITAL-ONLY SECURITY PRIMITIVES HAVE LIMITS

In particular, in settings involving security for the physical environment

- Hardware attacks (e.g., side-channel, fault injection, rowhammer)
- Secure location / distance
- Tamper detection
- Wireless sensing privacy violation
- …

➔ Physical-layer methods bridge physical and digital domains

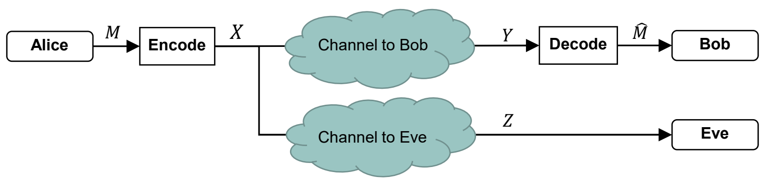
A BRIEF HISTORY: PHYSICAL-LAYER SECURITY

Strong focus on information-theoretic secure communication

- Shannon 1949 and Wyner 1975: Information theory, wiretap channel
- Maurer 1993, Ahlswede and Csiszár 1993: Key generation from public discussion
- Hershey 1995: First wireless key generation

Leverages physical-layer properties, signal processing, and channel coding

CLASSICAL PHYSICAL-LAYER SECURITY



Intuition: Leverage difference of channels to Bob and Eve for secrecy

Approach 1: Eve's channel is noisier than Bobs

→

Ap

→

Problem ... nel.

Paradigm: Use wireless physical-layer to address security services without digital counterparts

Competes with well established cryptographic primitives

AGENDA

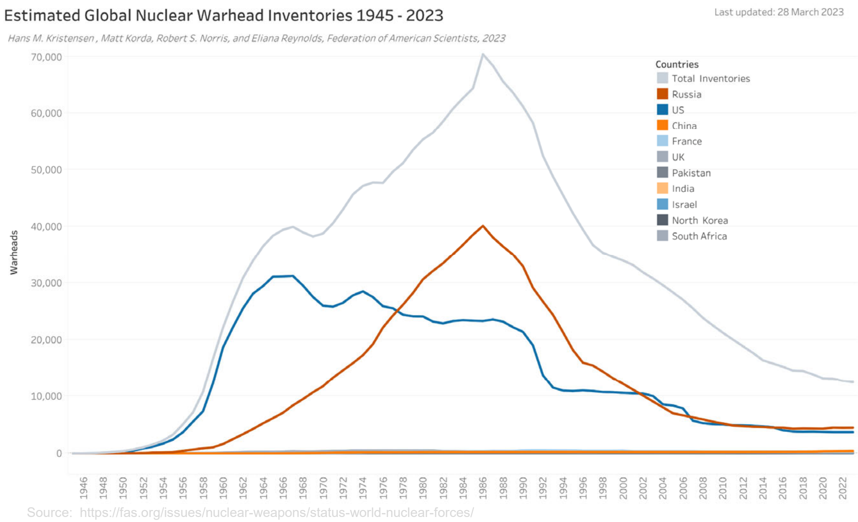
REMOTE INSPECTION OF ADVERSARY-CONTROLLED ENVIRONMENTS

in Nature Communications volume 14, 2023

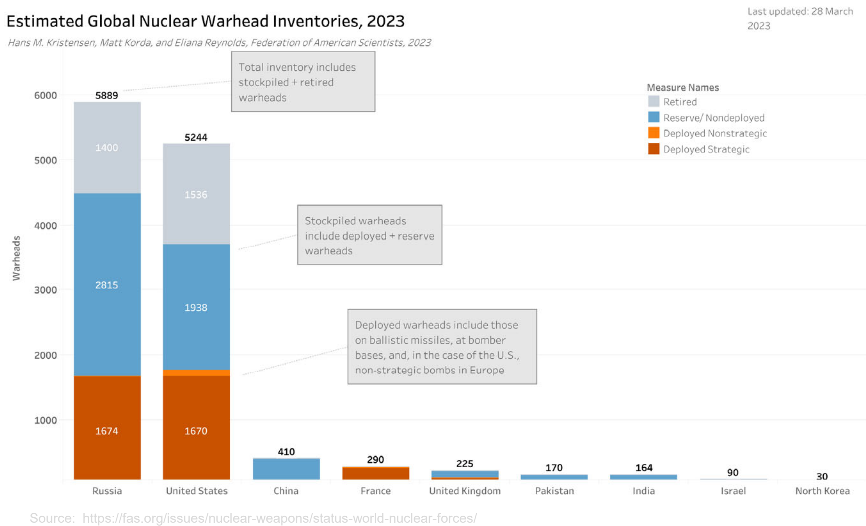
Johannes Tobisch[1], Sébastien Philippe[2], Boaz Barak[3], Gal Kaplun[3], Christian Zenger[4,5], Alexander Glaser[2], Christof Paar[1] & Ulrich Rührmair[6,7]

[1] Max Planck Institute for Security and Privacy, Bochum, Germany
[2] Program on Science and Global Security, Princeton University, Princeton, NJ, USA
[3] John A. Paulson School of Engineering and Applied Sciences, Harvard University, Boston, MA, USA
[4] PHYSEC GmbH, Bochum, Germany
[5] Secure Mobile Networking, Ruhr University Bochum, Bochum, Germany
[6] Electrical Engineering and Computer Science Department, TU Berlin, Berlin, Germany
[7] Secure Computation Laboratory, University of Connecticut, Storrs, Mansfield, CT, USA

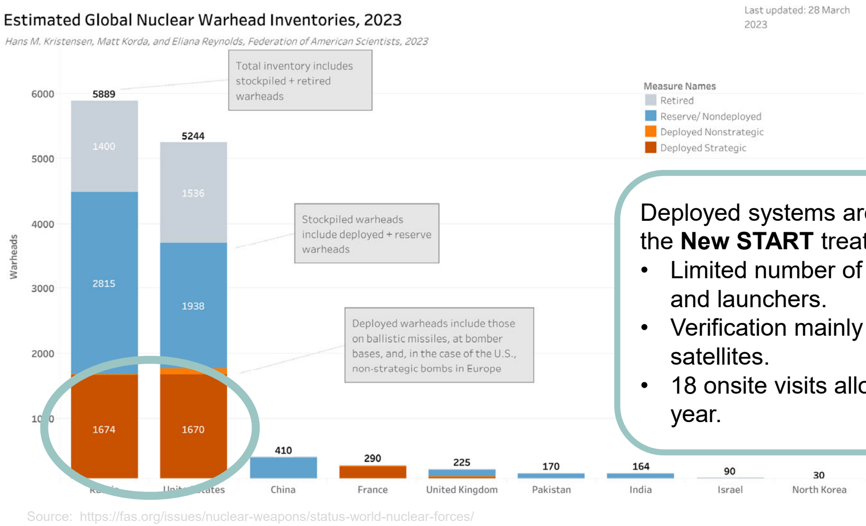
CHALLENGES IN NUCLEAR DISARMAMENT



CHALLENGES IN NUCLEAR DISARMAMENT



CHALLENGES IN NUCLEAR DISARMAMENT

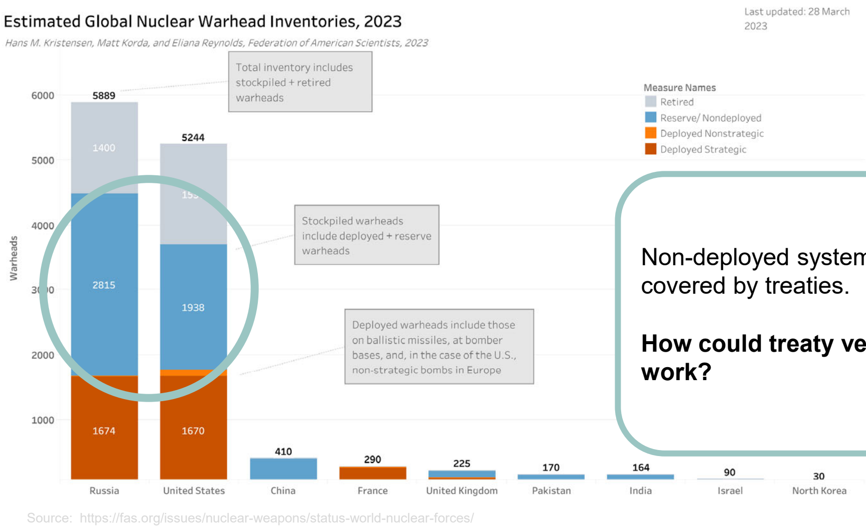


Source: https://fas.org/issues/nuclear-weapons/status-world-nuclear-forces/

Deployed systems are covered by the **New START** treaty:

- Limited number of warheads and launchers.
- Verification mainly done by satellites.
- 18 onsite visits allowed per year.

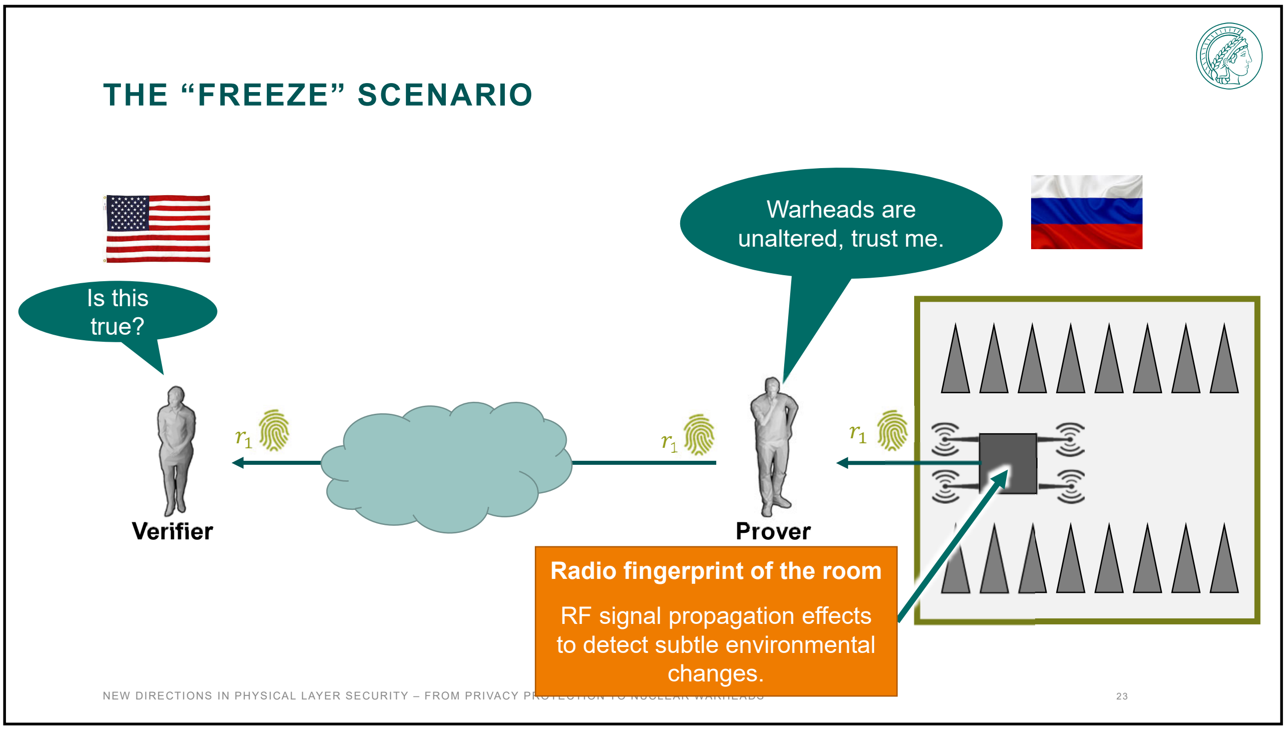
CHALLENGES IN NUCLEAR DISARMAMENT

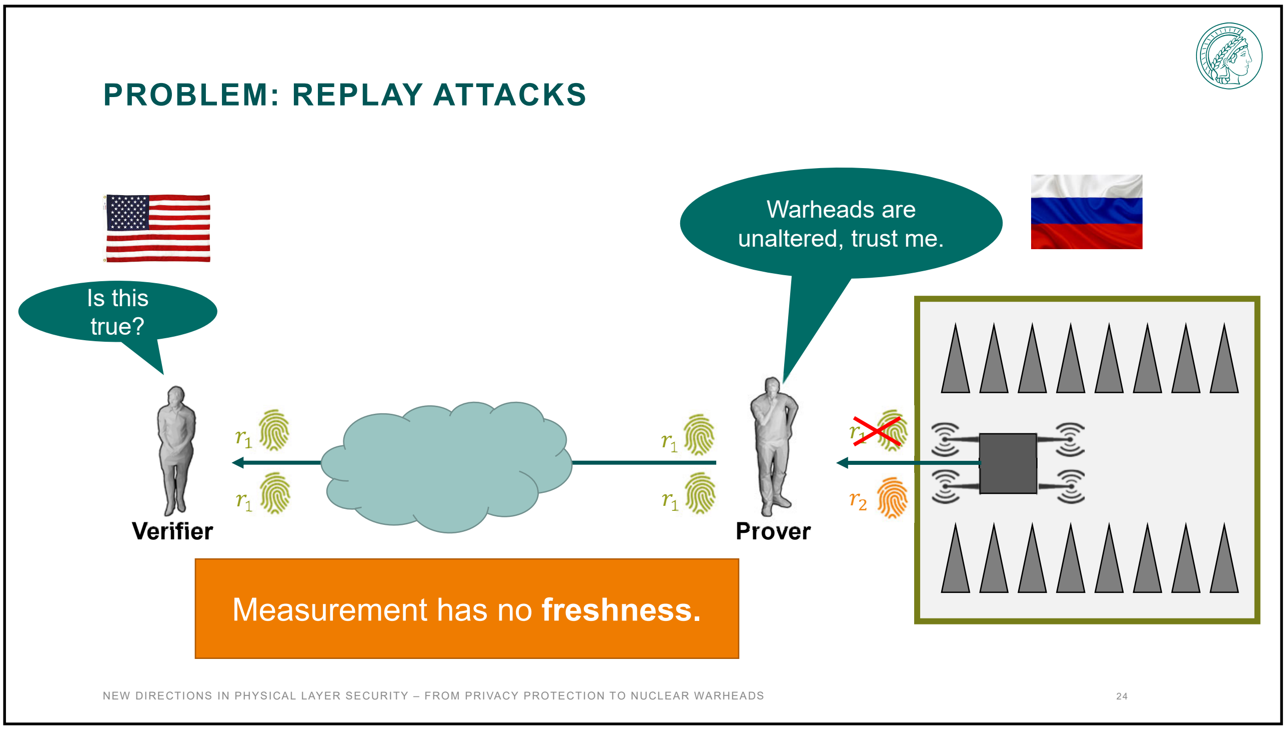


Source: https://fas.org/issues/nuclear-weapons/status-world-nuclear-forces/

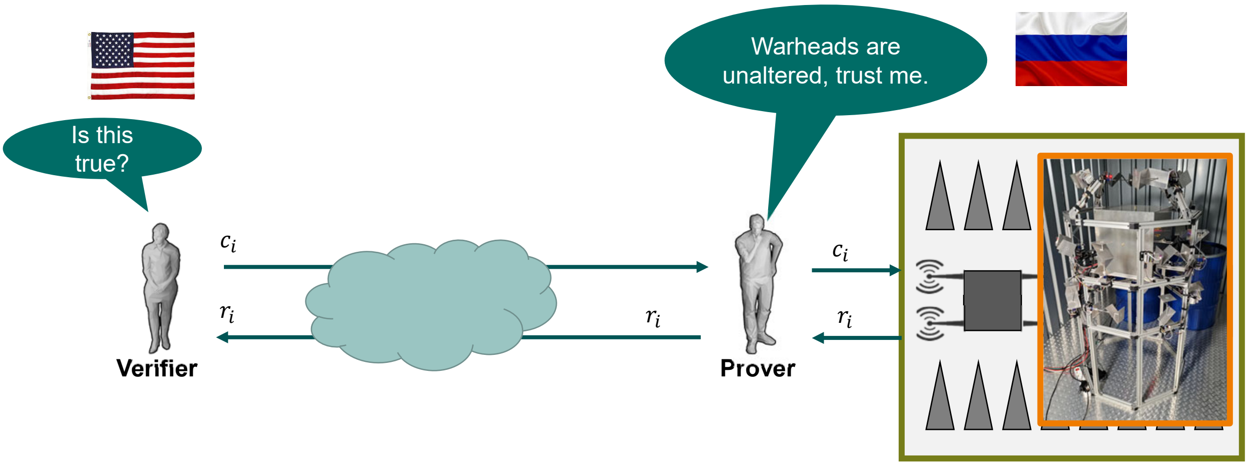
Non-deployed systems are not covered by treaties.

How could treaty verification work?

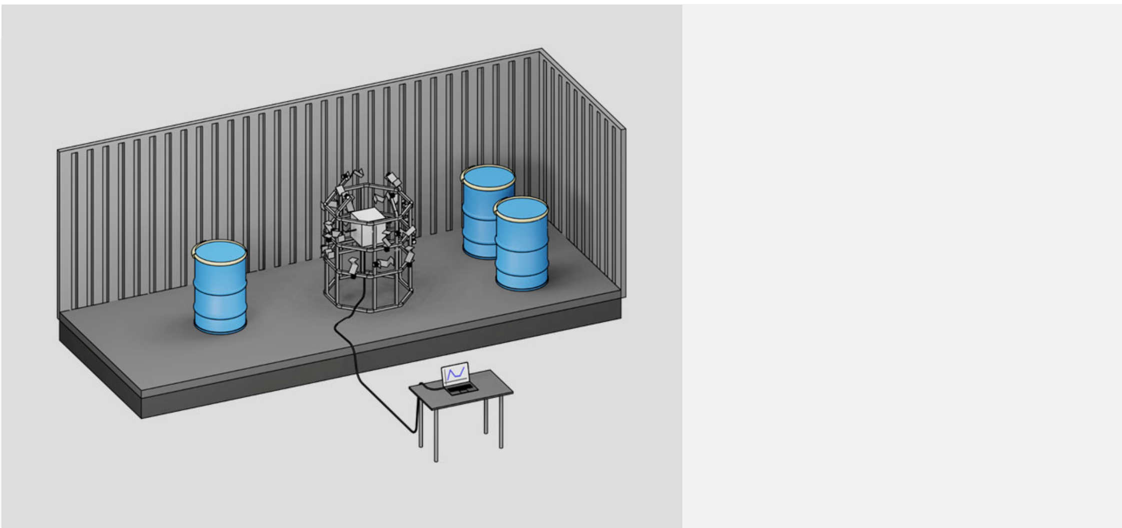

THE "FREEZE" SCENARIO
Warheads are unaltered, trust me.
Is this true?
r_1
r_1
r_1
Verifier
Prover
Radio fingerprint of the room
RF signal propagation effects to detect subtle environmental changes.
NEW DIRECTIONS IN PHYSICAL LAYER SECURITY – FROM PRIVACY P
23


PROBLEM: REPLAY ATTACKS
Warheads are unaltered, trust me.
Is this true?
r_1
r_1
r_1
r_1
r_2
Verifier
Prover
Measurement has no **freshness.**
NEW DIRECTIONS IN PHYSICAL LAYER SECURITY – FROM PRIVACY PROTECTION TO NUCLEAR WARHEADS
24

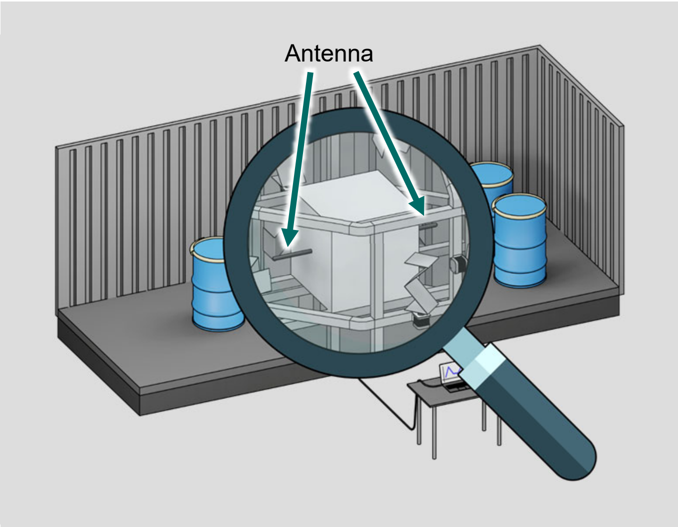
PHYSICAL CHALLENGE-RESPONSE AUTHENTICATION



REMOTE INSPECTIONS – EXPERIMENTAL REALIZATION

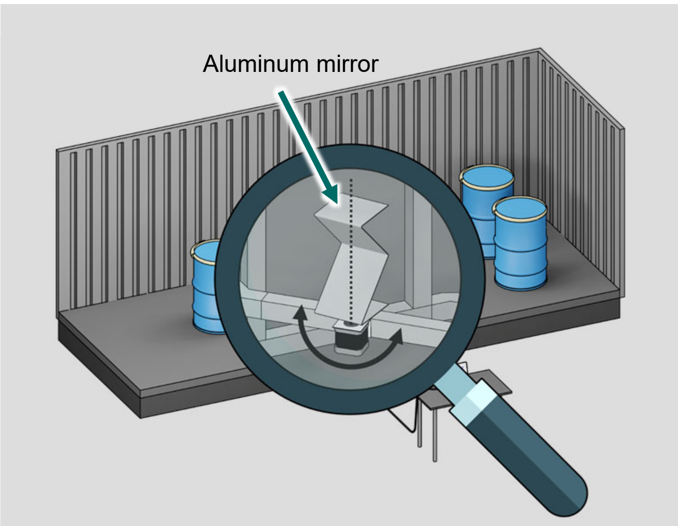


REMOTE INSPECTIONS – EXPERIMENTAL REALIZATION



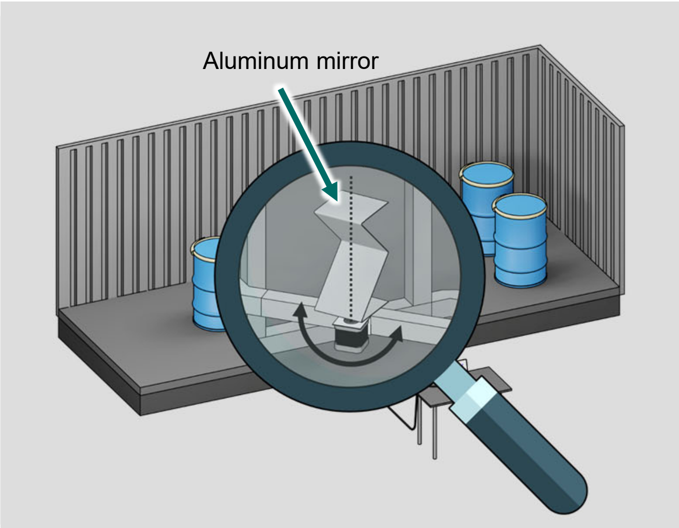
1. **Radio-frequency fingerprint:**
   Magnitude channel frequency response between antennas from 2 - 9 GHz.

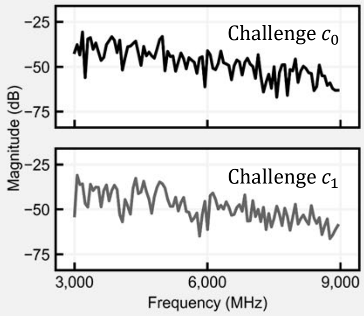
REMOTE INSPECTIONS – EXPERIMENTAL REALIZATION



2. **Freshness:**
   20 mirrors, 200 positions each
   $200^{20} \approx 10^{46} \approx 2^{152}$ configurations
   Each mirror configuration is a "challenge".

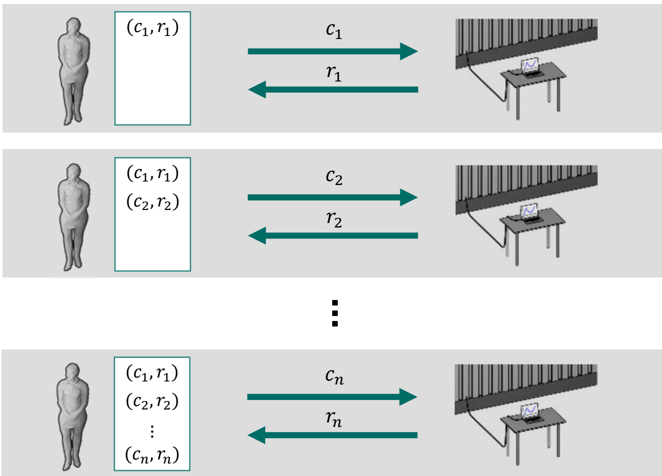
REMOTE INSPECTIONS – EXPERIMENTAL REALIZATION





We use Euclidean distance to quantify differences between responses.

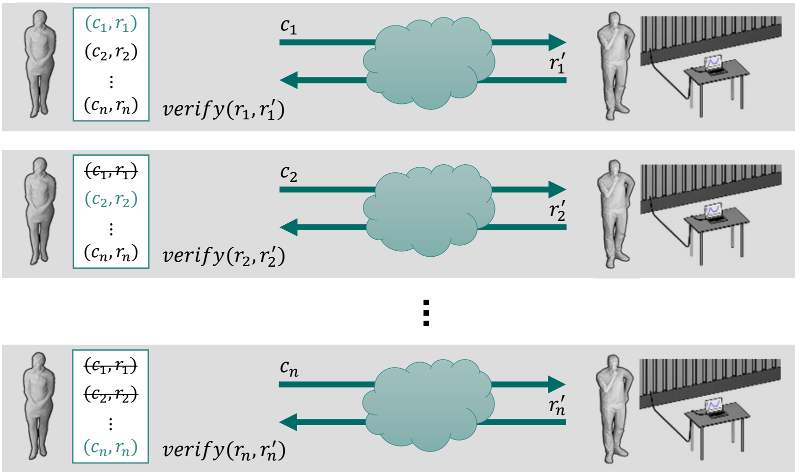
REMOTE INSPECTIONS – SETUP PHASE



Verifier onsite for short (~ 1 day) setup phase.

Prover must not spy.

REMOTE INSPECTIONS – PROOF PHASE



$verify(r_i, r_i')$

Accept $r_i' \approx r_i$

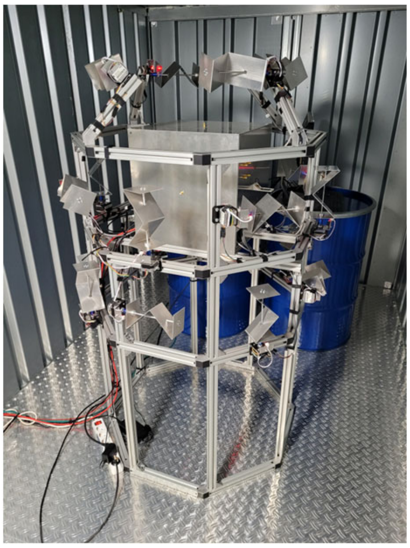
Reject $r_i' \not\approx r_i$

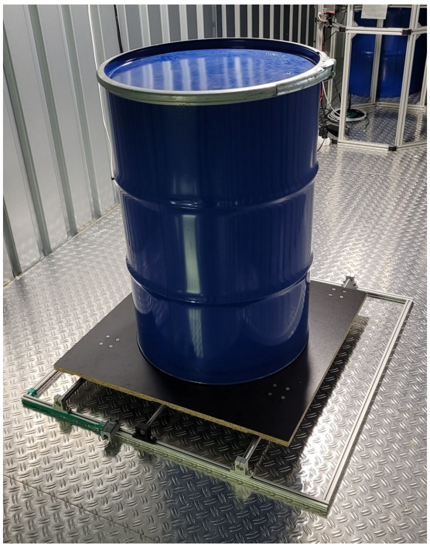
Long (~ 1 year) proof phase for remote verification.

Use each challenge only once. It must be impossible to predict responses.

EXPERIMENTAL REALIZATION

EXPERIMENTAL REALIZATION





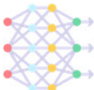
EXAMINED SYSTEM PROPERTIES

How well can tampering be detected?

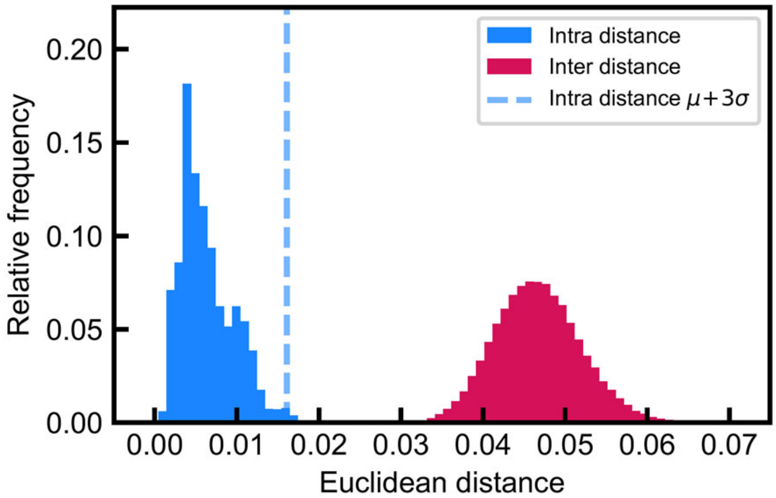
Are responses long-term stable?

How large is the effective challenge space?

How difficult are machine learning attacks?



DISTANCE NOMENCLATURE: CHALLENGES VS. "NOISE"

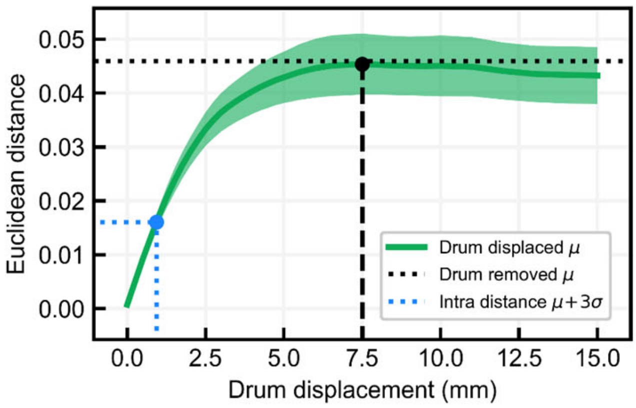


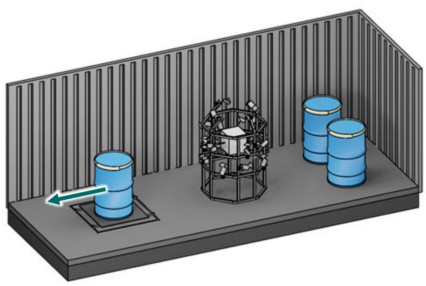
Intra Distance:
Legitimate variation of the response for a single challenge.

Decision Threshold ($\mu + 3\sigma$):
Border for the detection of illegitimate variation.

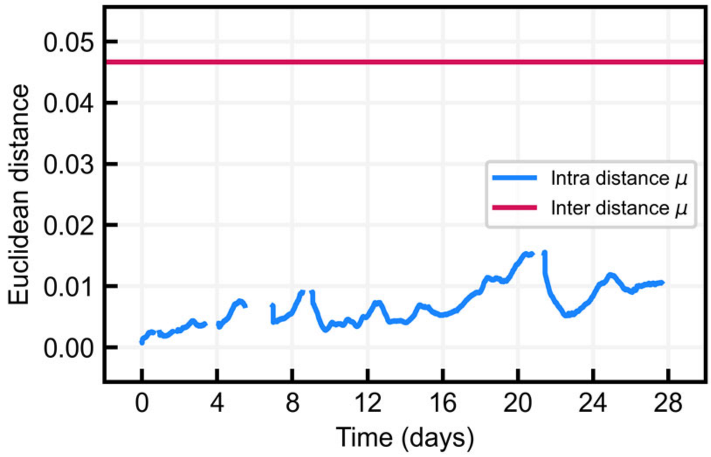
Inter Distance:
Variation of responses between random challenges.

SENSITIVITY AGAINST PHYSICAL MANIPULATION: TAMPER DETECTION



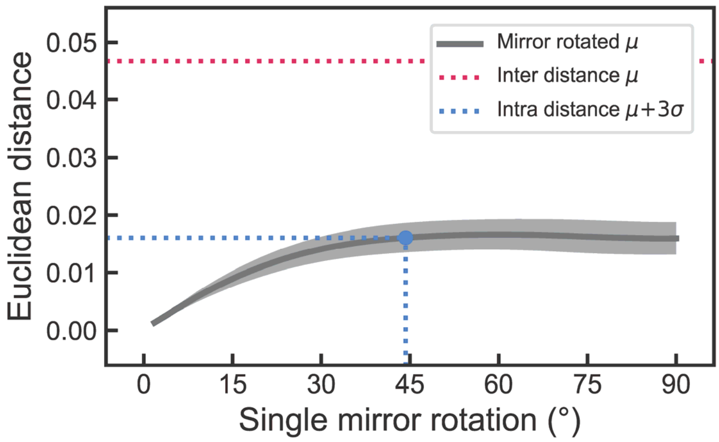


INTRA DISTANCE OVER TIME



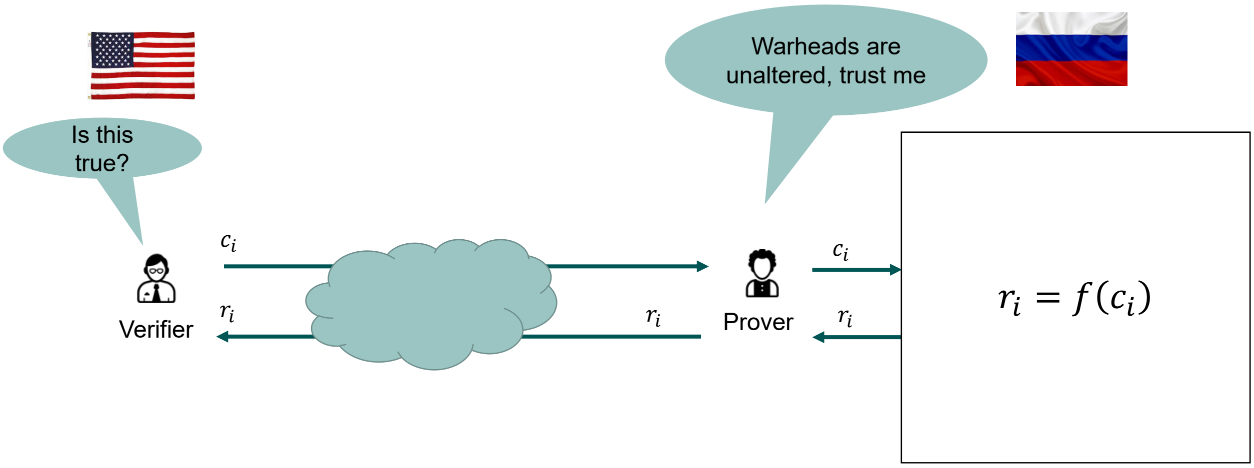
Environmental factors are the major drivers of intra distance drift.

EFFECTIVE CHALLENGE SPACE ESTIMATION



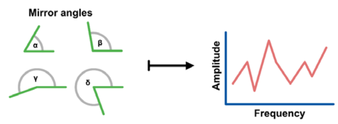
Assuming $360°/45° = 8$ independent mirror positions, there are $8^{20} \approx 2^{60}$ challenges.

MODELLING ATTACKS

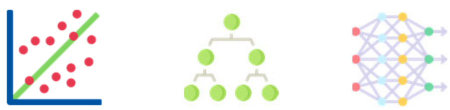


MACHINE LEARNING MODELING ATTACKS

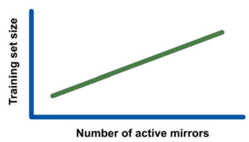
- **Learning problem:**
  Find a function f that maps challenges to responses.



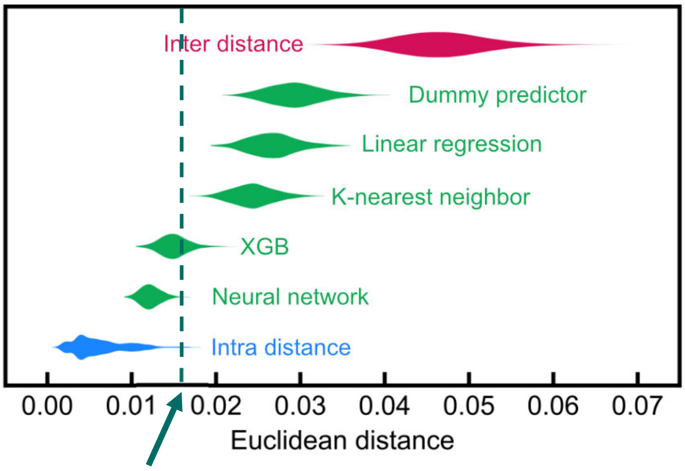
- **Which machine learning algorithms perform well?**



- **How does the learning difficulty scale?**



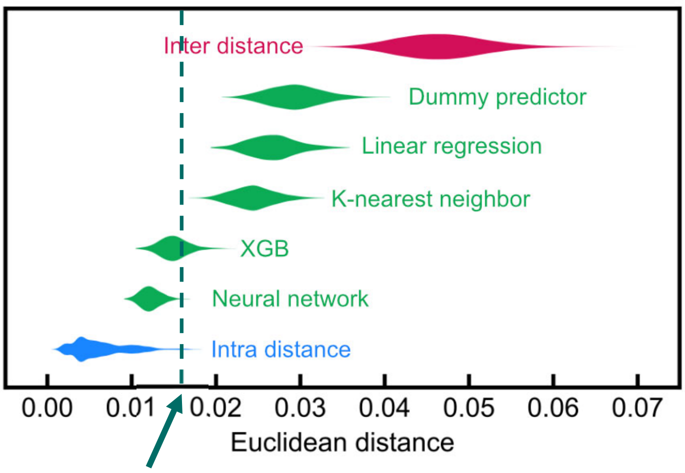
ALGORITHM COMPARISON FOR 12 ACTIVE MIRRORS



Threshold
intra distance $\mu + 3\sigma$

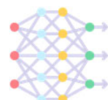
Algorithms trained with 1,280,000 data points. Depicted test error computed over 1,000 data points.

ALGORITHM COMPARISON FOR 12 ACTIVE MIRRORS



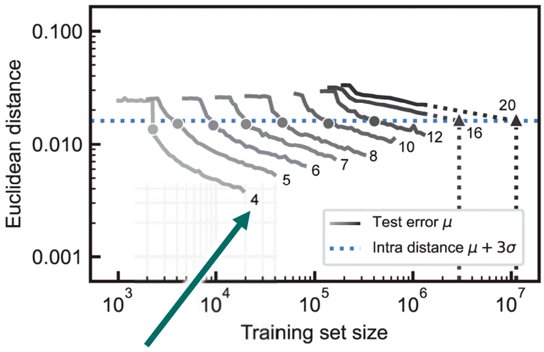
Threshold
intra distance $\mu + 3\sigma$

Neural Network
Simple architecture of 8 stacked dense layers, 3,072 neurons per layer, ReLU activation.

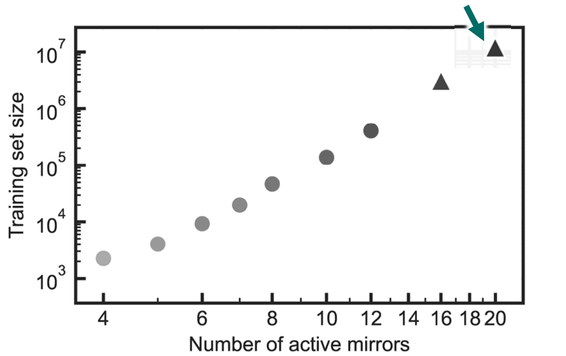


MODELING ATTACKS – NEURAL NETWORK PERFORMANCE

Takes 51 days to collect.



Number of mirrors scale challenge space size



Power law / polynomial scaling

→ Select number of mirrors to force adversary into unrealistically large training set size.

MORE INFORMATION IN OUR PAPER

nature communications

Article https://doi.org/10.1038/s41467-023-42314-2

Remote inspection of adversary-controlled environments

Received: 13 April 2023

Accepted: 6 October 2023

Published online: 17 October 2023

Check for updates

Johannes Tobisch[1], Sébastien Philippe[2], Boaz Barak[3], Gal Kaplun[3], Christian Zenger[4,5], Alexander Glaser[2], Christof Paar[1] & Ulrich Rührmair[6,7]

Remotely monitoring the location and enduring presence of valuable items in adversary-controlled environments presents significant challenges. In this article, we demonstrate a monitoring approach that leverages the gigahertz

ANTI-TAMPER RADIO: SYSTEM-LEVEL TAMPER DETECTION FOR COMPUTING SYSTEMS

Presented at S&P '22

Paul Staat[1], Johannes Tobisch[1], Christian Zenger[2], Christof Paar[1]

[1] Max Planck Institute for Security and Privacy
[2] PHYSEC GmbH

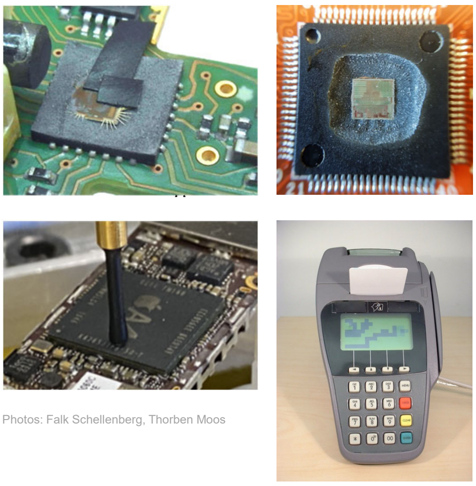
MAX PLANCK INSTITUTE FOR SECURITY AND PRIVACY
PHYSEC SECURITY FOR THINGS

PHYSICAL ATTACKS

Adversaries with **physical access** can extract information or implant malicious functionality

Side-channel analysis, bus probing, fault injection...

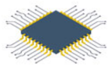
Countermeasure: **Tamper detection** and response



Photos: Falk Schellenberg, Thorben Moos

EXISTING APPROACHES TO TAMPER DETECTION

Chip-level [1, 2]



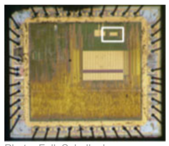


Photo: Falk Schellenberg

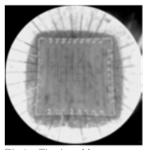
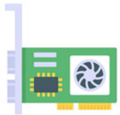
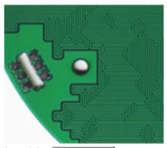


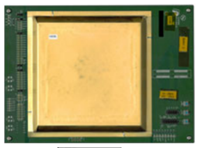
Photo: Thorben Moos

Module-level [3, 4, 5]



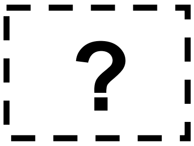


from [5],



from [4],

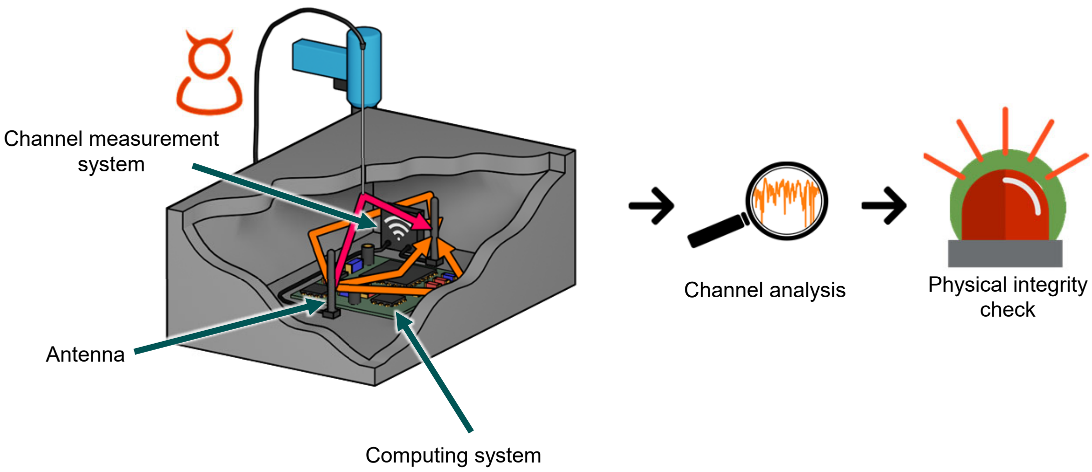
System-level



[1] Tuyls et al. "Read-proof hardware from protective coatings," CHES, Heidelberg, 2006
[2] Anderson et al., "Cryptographic processors – a survey," Technical Report Number 641, 2005
[3] Obermaier and Immler, "The Past, Present, and Future of Physical Security Enclosures: From Battery-Backed Monitoring to PUF-Based Inherent Security and Beyond," J. of Hardw. and Syst. Secur. vol. 2, no. 4, 2018.
[4] Immler et al., "Secure Physical Enclosures from Covers with Tamper-Resistance," CHES 2019
[5] Götte et al., "Can't Touch This: Inertial HSMs Thwart Advanced Physical Attacks," CHES 2022.

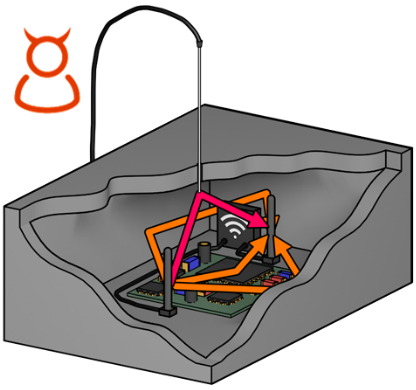
IDEA: ANTI-TAMPER RADIO (ATR)

Radio Wave-based Tamper Detection



IDEA: ANTI-TAMPER RADIO (ATR)

Radio Wave-based Tamper Detection

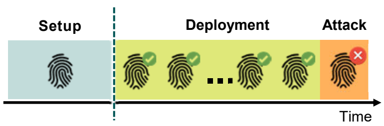


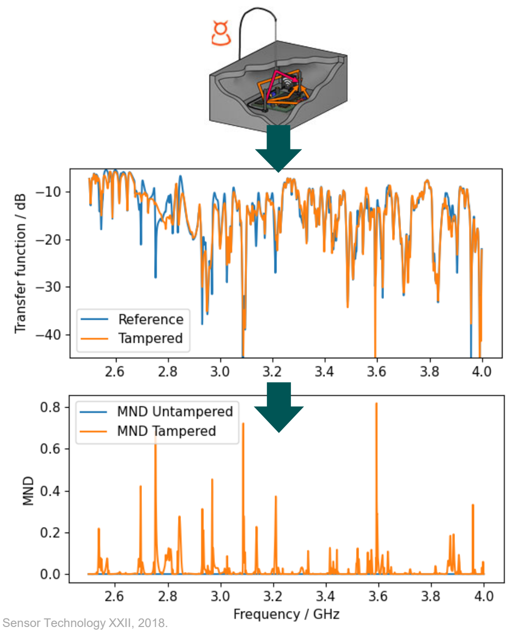
- **System-level detection**
- **High flexibility**
- **Retrofittable**
- **Re-initializable**

RADIO MEASUREMENTS

Channel magnitude frequency response as “fingerprint” of the environment

Mean normalized deviation (MND) [2] quantifies deviation from initial measurement





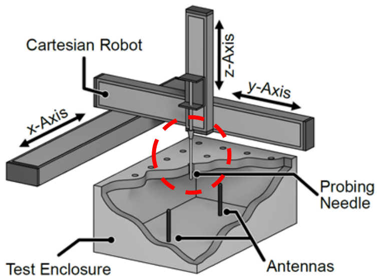
Channel response

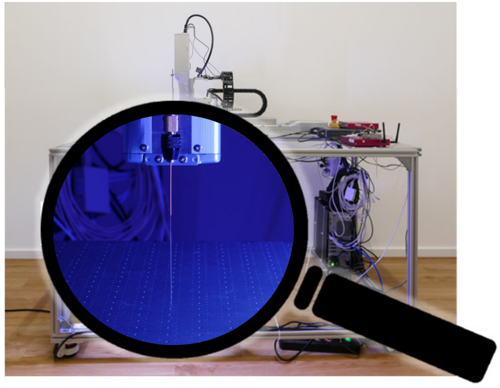
MND tampered: 0.02106506

MND untampered: 0.00000144

[2] Doerry and Bickel, "Measuring Channel Balance in Multi-Channel Radar Receivers," Radar Sensor Technology XXII, 2018.

SYSTEMATIC EXPERIMENTAL EVALUATION

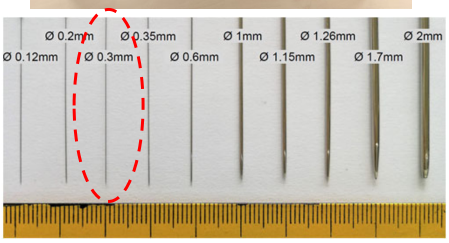


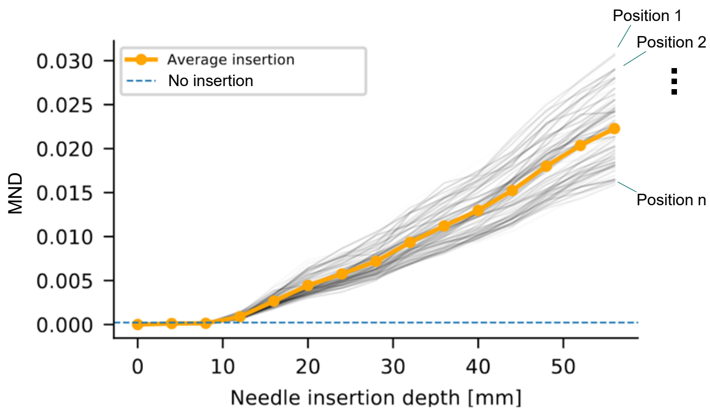


Degrees of freedom:

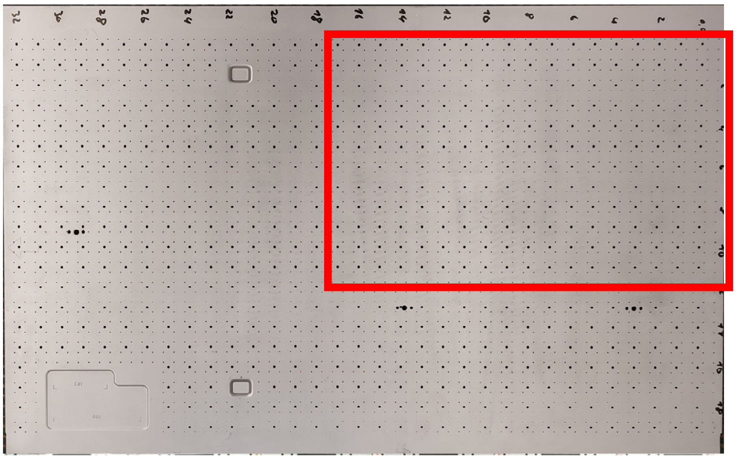
- Physical extent of attack (needle insertion depth, ...)
- Attack position
- Temporal behavior

SENSITIVITY AGAINST PHYSICAL MANIPULATION

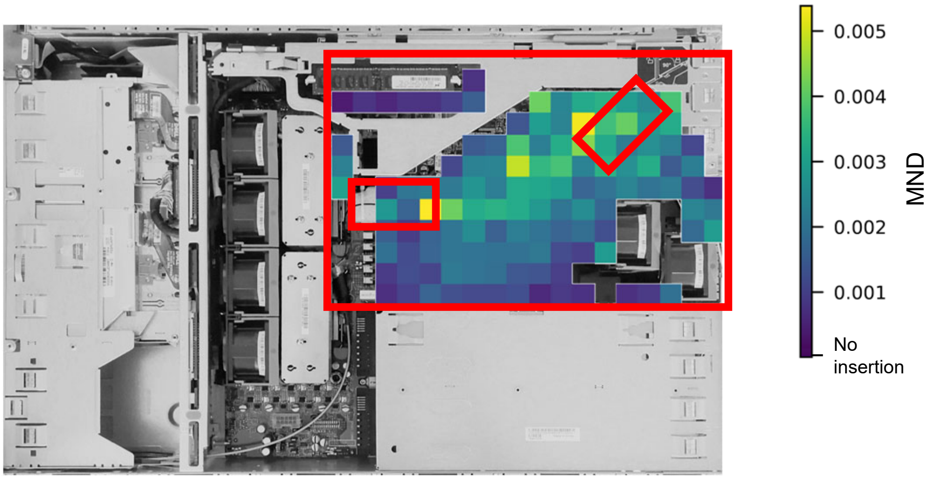




CASE STUDY: 19" SERVER



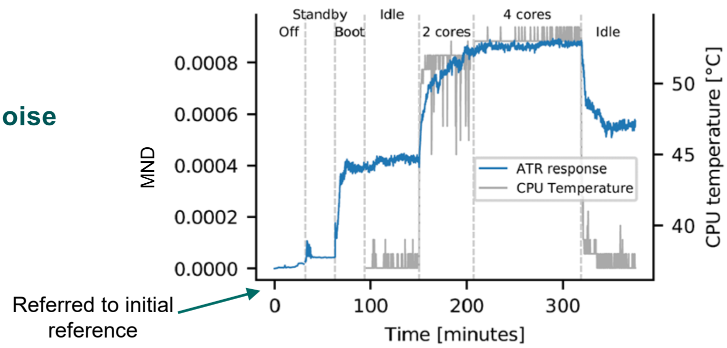
CASE STUDY: 19" SERVER – TURNED OFF



CASE STUDY: 19" SERVER – TURNED ON

Running the server introduces noise

- Vibration
- Temperature swings
- Air flow



Noise over time – without attack

CASE STUDY: 19" SERVER – TURNED ON

Server powered on with varying CPU loads

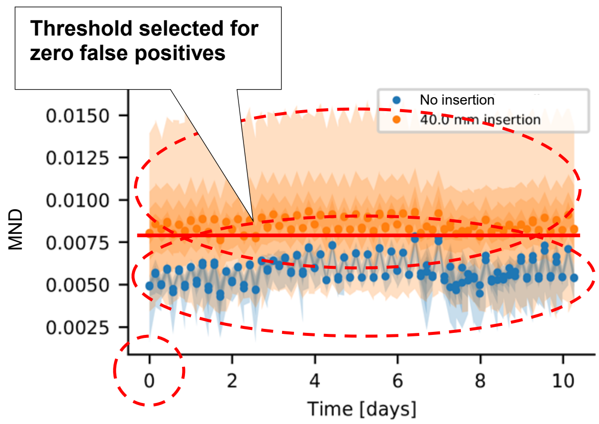
Measure initial reference

Repeatedly test all positions

- Needle outside
- Needle inside

→ **Reliable detection not possible for most positions**

How to improve detection?



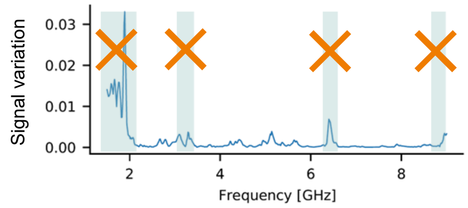
ENHANCE ROBUSTNESS – SPECTRAL SELECTION

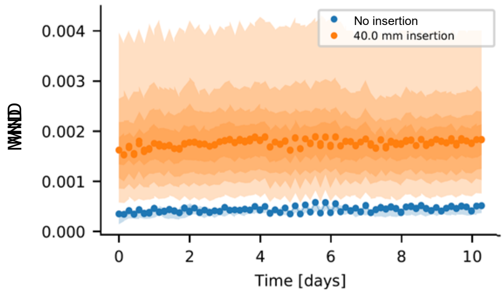
Solution: Initial setup phase

Monitor **untampered** environment

Detect parts of response with strong signal variation

Disregard during deployment

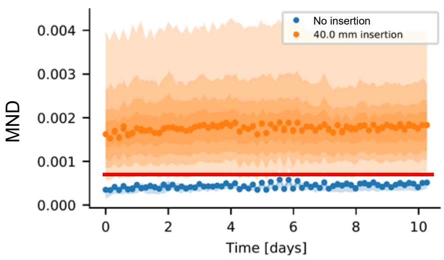




MEASUREMENT SYSTEMS

Vector network analyzer

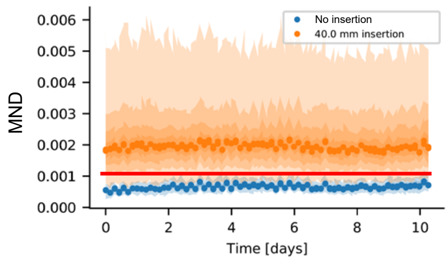
$12,000



Detects at least 114 / 117 positions

Single-chip UWB transceiver

2 x $5



Detects at least 90 / 117 positions

IRSHIELD: A COUNTERMEASURE AGAINST ADVERSARIAL PHYSICAL-LAYER WIRELESS SENSING

Presented at S&P '22

Paul Staat[1], Simon Mulzer[2], Stefan Roth[2], Veelasha Moonsamy[2], Markus Heinrichs[3], Rainer Kronberger[3], Aydin Sezgin[2], Christof Paar[1]

[1] Max Planck Institute for Security and Privacy
[2] Ruhr University Bochum
[3] TH Köln – University of Applied Sciences

MAX PLANCK INSTITUTE FOR SECURITY AND PRIVACY

RUB

Technology Arts Sciences TH Köln

WIRELESS DEVICES AT HOME

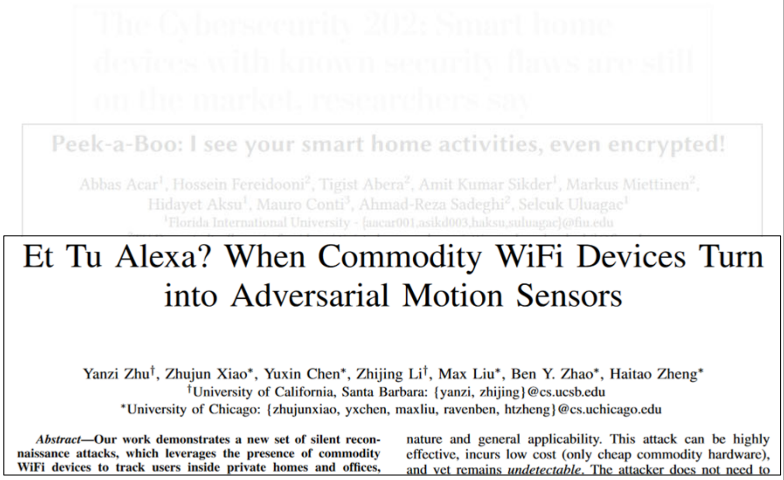
Photos: Noupload, luis2500gx, Muhammad Abdullah, haus_automation, USA-Reiseblogger, luis2500gx at pixabay.com; cottonbro, Fabian Hurnaus, Torsten Dettlaff, Pixabay at pexels.com

UBIQUITOUS WI-FI – PRIVACY THREATS

Application-Level Privacy

Network-Level Privacy

Physical-Layer Wireless Sensing


The Cybersecurity 202: Smart home devices with known security flaws are still on the market, researchers say

Peek-a-Boo: I see your smart home activities, even encrypted!

Abbas Acar[1], Hossein Fereidooni[2], Tigist Abera[2], Amit Kumar Sikder[1], Markus Miettinen[2], Hidayet Aksu[1], Mauro Conti[3], Ahmad-Reza Sadeghi[2], Selcuk Uluagac[1]

[1]Florida International University - {aacar001,asikd003,haksu,suluagac}@fiu.edu

Et Tu Alexa? When Commodity WiFi Devices Turn into Adversarial Motion Sensors

Yanzi Zhu[†], Zhujun Xiao[*], Yuxin Chen[*], Zhijing Li[†], Max Liu[*], Ben Y. Zhao[*], Haitao Zheng[*]

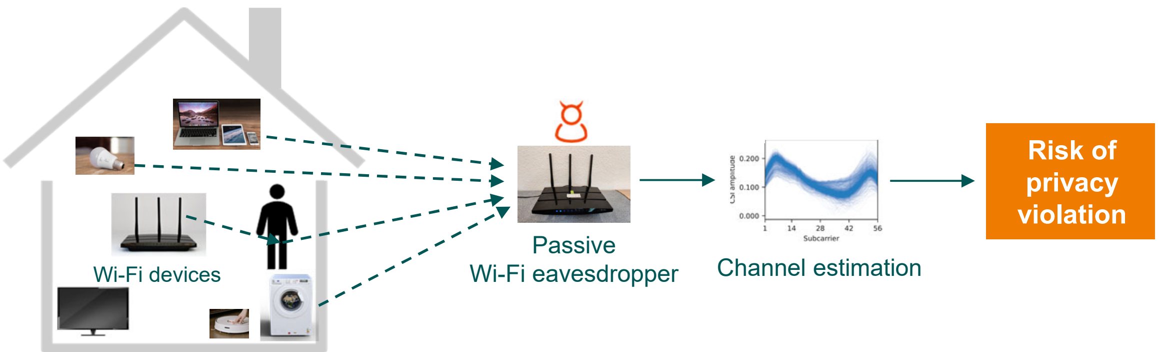
[†]University of California, Santa Barbara: {yanzi, zhijing}@cs.ucsb.edu

[*]University of Chicago: {zhujunxiao, yxchen, maxliu, ravenben, htzheng}@cs.uchicago.edu

Abstract—Our work demonstrates a new set of silent reconnaissance attacks, which leverages the presence of commodity WiFi devices to track users inside private homes and offices, nature and general applicability. This attack can be highly effective, incurs low cost (only cheap commodity hardware), and yet remains *undetectable*. The attacker does not need to

Zhu et al., "Et Tu Alexa? When Commodity WiFi Devices Turn into Adversarial Motion Sensors," **NDSS 2020**.

ADVERSARIAL WIRELESS SENSING



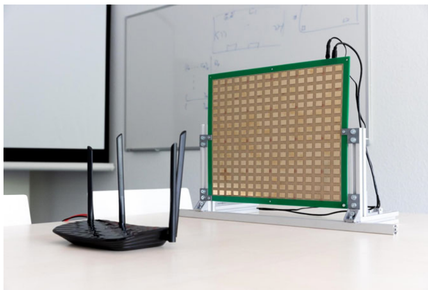
IDEA: NOVEL COUNTERMEASURE IRSHIELD

Thwart adversarial wireless sensing based on Intelligent Reflecting Surfaces (IRSs)

Partial randomization of wireless radio channels

- Fully device-agnostic
- Wireless quality-of-service not affected

Defeats state-of-the-art adversarial human motion detection



WIRELESS SENSING

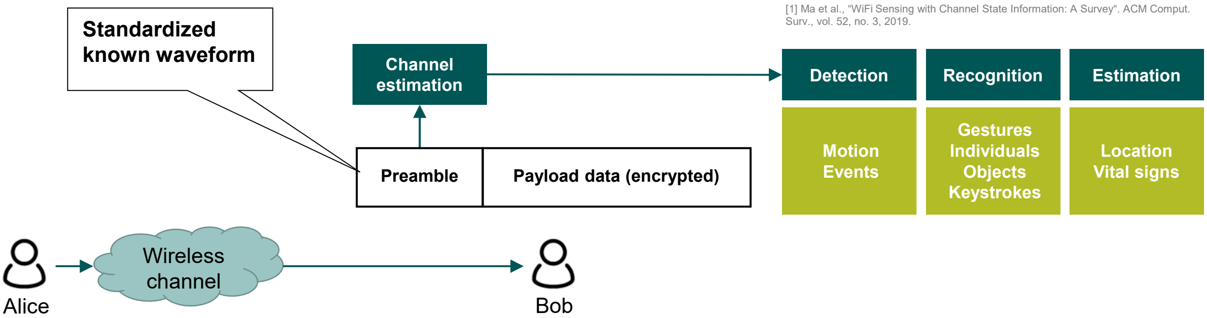
Extract information about the physical environment from communication signals

WiFi Sensing with Channel State Information: A Survey

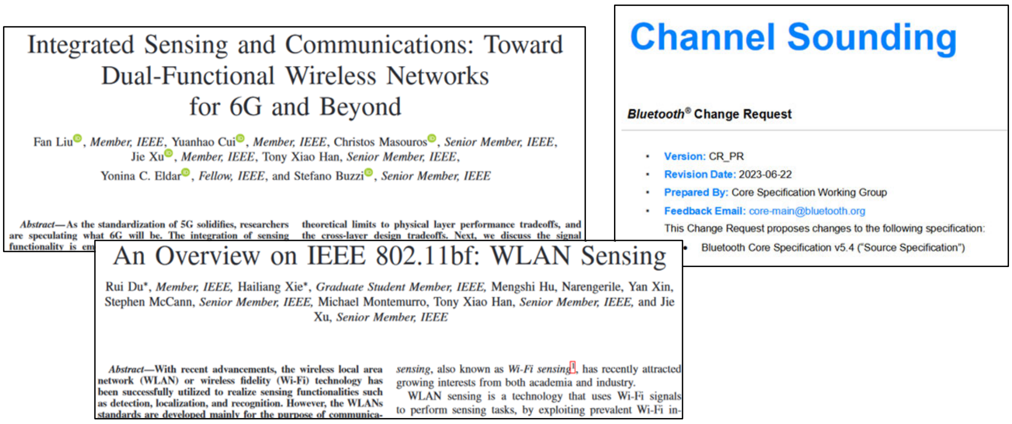
YONGSEN MA, GANG ZHOU, and SHUANGQUAN WANG, Computer Science Department, College of William & Mary, USA

With the high demand for wireless data traffic, WiFi networks have very rapid growth because they provide high throughput and are easy to deploy. Recently, Channel State Information (CSI) measured by WiFi networks is widely used for different sensing purposes. To get a better understanding of existing WiFi sensing technologies and future WiFi sensing trends, this survey gives a comprehensive review of the signal processing techniques, algorithms, applications, and performance results of WiFi sensing with CSI. Different WiFi sensing algorithms and signal processing techniques have their own advantages and limitations and are suitable for different WiFi sensing applications. The survey groups CSI-based WiFi sensing applications into three categories: detection, recognition, and estimation, depending on whether the outputs are binary/multi-class classifications or numerical values. With the development and deployment of new WiFi technologies, there will be more WiFi sensing opportunities wherein the targets may go beyond from humans to environments, animals, and objects. The survey highlights three challenges for WiFi sensing: robustness and generalization, privacy and security, and coexistence of WiFi sensing and networking. Finally, the survey presents three future WiFi sensing trends, i.e., integrating cross-layer network information, multi-device cooperation, and fusion of different sensors, for enhancing existing WiFi sensing capabilities and enabling new WiFi sensing opportunities.

[1] Ma et al., "WiFi Sensing with Channel State Information: A Survey". ACM Comput. Surv., vol. 52, no. 3, 2019.



STANDARDIZATION OF WIRELESS SENSING: COMING TO A WIRELESS NETWORK NEAR YOU


Integrated Sensing and Communications: Toward Dual-Functional Wireless Networks for 6G and Beyond

Fan Liu, *Member, IEEE*, Yuanhao Cui, *Member, IEEE*, Christos Masouros, *Senior Member, IEEE*, Jie Xu, *Member, IEEE*, Tony Xiao Han, *Senior Member, IEEE*, Yonina C. Eldar, *Fellow, IEEE*, and Stefano Buzzi, *Senior Member, IEEE*

Abstract—As the standardization of 5G solidifies, researchers are speculating what 6G will be. The integration of sensing functionality is em… theoretical limits to physical layer performance tradeoffs, and the cross-layer design tradeoffs. Next, we discuss the signal

Channel Sounding

Bluetooth® Change Request

- Version: CR_PR
- Revision Date: 2023-06-22
- Prepared By: Core Specification Working Group
- Feedback Email: core-main@bluetooth.org

This Change Request proposes changes to the following specification:

- Bluetooth Core Specification v5.4 ("Source Specification")

An Overview on IEEE 802.11bf: WLAN Sensing

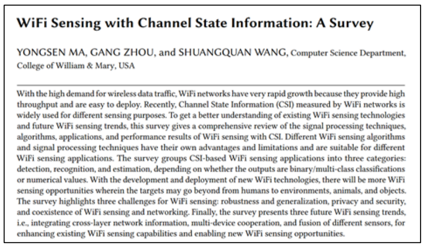
Rui Du*, *Member, IEEE*, Hailiang Xie*, *Graduate Student Member, IEEE*, Mengshi Hu, Narengerile, Yan Xin, Stephen McCann, *Senior Member, IEEE*, Michael Montemurro, Tony Xiao Han, *Senior Member, IEEE*, and Jie Xu, *Senior Member, IEEE*

Abstract—With recent advancements, the wireless local area network (WLAN) or wireless fidelity (Wi-Fi) technology has been successfully utilized to realize sensing functionalities such as detection, localization, and recognition. However, the WLANs standards are developed mainly for the purpose of communica- *sensing*, also known as *Wi-Fi sensing*[1], has recently attracted growing interests from both academia and industry.

WLAN sensing is a technology that uses Wi-Fi signals to perform sensing tasks, by exploiting prevalent Wi-Fi in-

WIRELESS SENSING

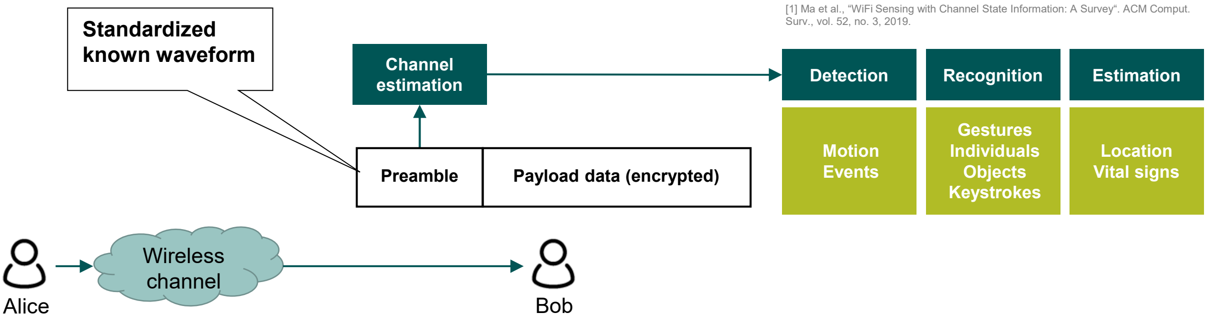
Extract information about the physical environment from communication signals


WiFi Sensing with Channel State Information: A Survey

YONGSEN MA, GANG ZHOU, and SHUANGQUAN WANG, Computer Science Department, College of William & Mary, USA

With the high demand for wireless data traffic, WiFi networks have very rapid growth because they provide high throughput and are easy to deploy. Recently, Channel State Information (CSI) measured by WiFi networks is widely used for different sensing purposes. To get a better understanding of existing WiFi sensing technologies and future WiFi sensing trends, this survey gives a comprehensive review of the signal processing techniques, algorithms, applications, and performance results of WiFi sensing with CSI. Different WiFi sensing algorithms and signal processing techniques have their own advantages and limitations and are suitable for different WiFi sensing applications. The survey groups CSI-based WiFi sensing applications into three categories: detection, recognition, and estimation, depending on whether the outputs are binary/multi-class classifications or numerical values. With the development and deployment of new WiFi technologies, there will be more WiFi sensing opportunities wherein the targets may go beyond from humans to environments, animals, and objects. The survey highlights three challenges for WiFi sensing: robustness and generalization, privacy and security, and coexistence of WiFi sensing and networking. Finally, the survey presents three future WiFi sensing trends, i.e., integrating cross-layer network information, multi-device cooperation, and fusion of different sensors, for enhancing existing WiFi sensing capabilities and enabling new WiFi sensing opportunities.

[1] Ma et al., "WiFi Sensing with Channel State Information: A Survey". ACM Comput. Surv., vol. 52, no. 3, 2019.



WIRELESS SENSING

WiFi Sensing with Channel State Information: A Survey

YONGSEN MA, GANG ZHOU, and SHUANGQUAN WANG, Computer Science Department, College of William & Mary, USA

With the high demand for wireless data traffic, WiFi networks have very rapid growth because they provide high throughput and are easy to deploy. Recently, Channel State Information (CSI) measured by WiFi networks is widely used for different sensing purposes. To get a better understanding of existing WiFi sensing technologies and future WiFi sensing trends, this survey gives a comprehensive review of the signal processing techniques, algorithms, applications, and performance results of WiFi sensing with CSI. Different WiFi sensing algorithms and signal processing techniques have their own advantages and limitations and are suitable for different WiFi sensing applications. The survey groups CSI-based WiFi sensing applications into three categories: detection, recognition, and estimation, depending on whether the outputs are binary/multi-class classifications or numerical values. With the development and deployment of new WiFi technologies, there will be more WiFi sensing opportunities wherein the targets may go beyond from humans to environments, animals, and objects. The survey highlights three challenges for WiFi sensing: robustness and generalization, privacy and security, and coexistence of WiFi sensing and networking. Finally, the survey presents three future WiFi sensing trends, i.e., integrating cross-layer network information, multi-device cooperation, and fusion of different sensors, for enhancing existing WiFi sensing capabilities and enabling new WiFi sensing opportunities.

[1] Ma et al., "WiFi Sensing with Channel State Information: A Survey". ACM Comput. Surv., vol. 52, no. 3, 2019.

Extract information about the physical environment from communication signals

Standardized known waveform

Channel estimation

Preamble | Payload data (encrypted)

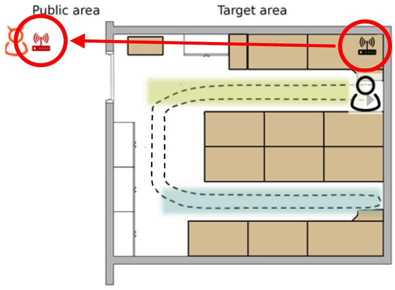
Detection | Recognition | Estimation

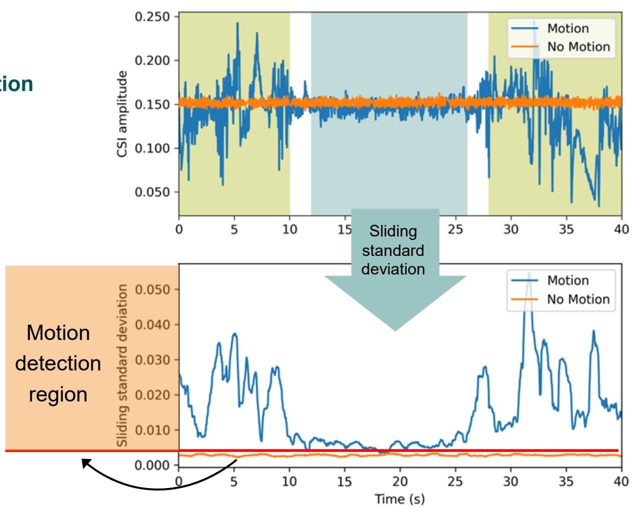
Privacy violation by rogue receiver

Alice → Wireless channel → Eve

STATE-OF-THE-ART: ADVERSARIAL MOTION DETECTION

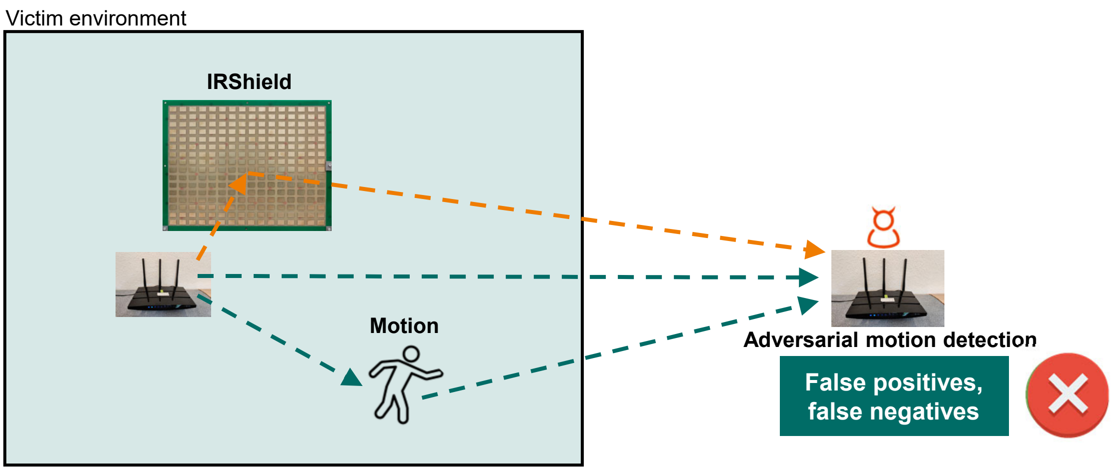
Zhu et al., NDSS '20 [3]:
Wi-Fi signals for adversarial motion detection





[3] Zhu et al., "Et Tu Alexa? When Commodity WiFi Devices Turn into Adversarial Motion Sensors," in 27th Annual Network and Distributed System Security Symposium, NDSS 2020.

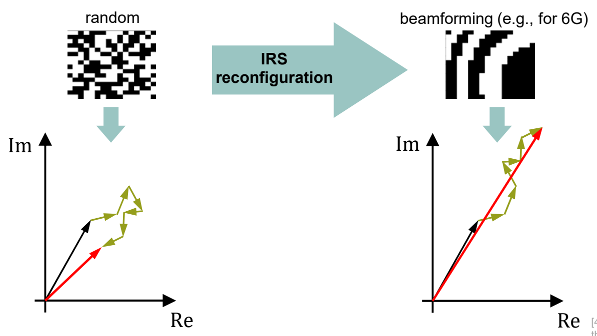
CHANNEL OBFUSCATION WITH AN INTELLIGENT REFLECTING SURFACE (IRS)

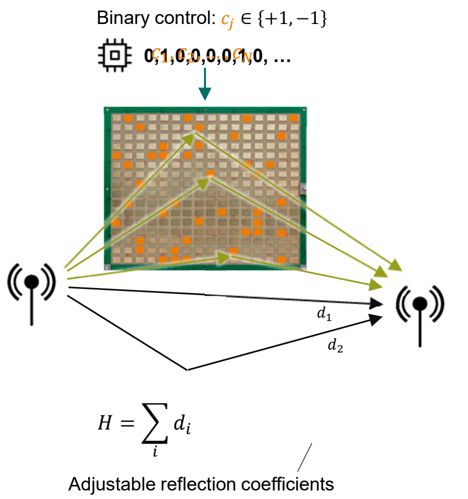


IRS OPERATION PRINCIPLE

Passive surface with digitally-controllable reflection

- Partially programmable wireless channel
- Prototype built by Heinrichs and Kronberger [4]





[4] Heinrichs and Kronberger, "Digitally Tunable Frequency Selective Surface for a Physical Layer Security System in the 5 GHz Wi-Fi Band," in 2020 International Symposium on Antennas and Propagation (ISAP), Osaka, Japan, 2021.

PS75

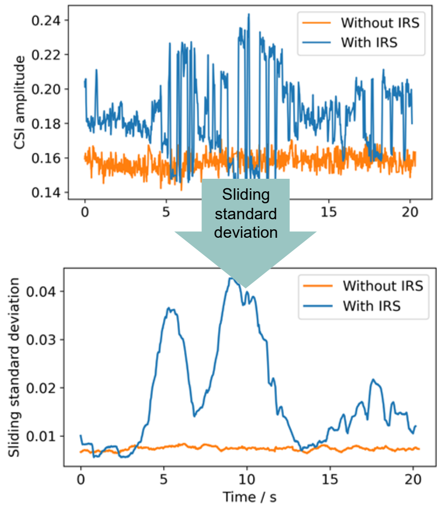
IRS-BASED CHANNEL VARIATION

Goal:
Use IRS to create artificial motion-like channel variation

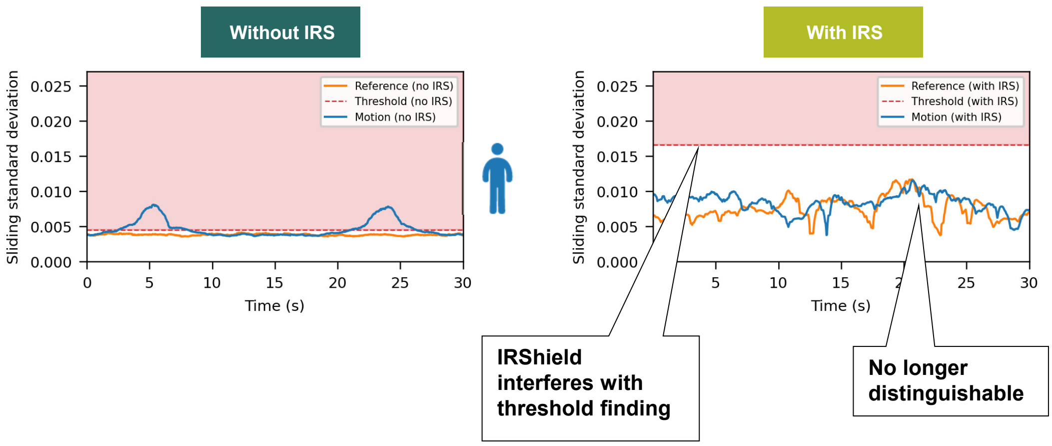
1. **Randomly select 5% out of all IRS elements to flip**
   ➔ Gradual random variation
2. **Interleave with flip of all IRS elements**
   ➔ Enhanced signal variation

IRS change: 5% | 100% | 5% | 100% | 5% | 100% | ...

Time



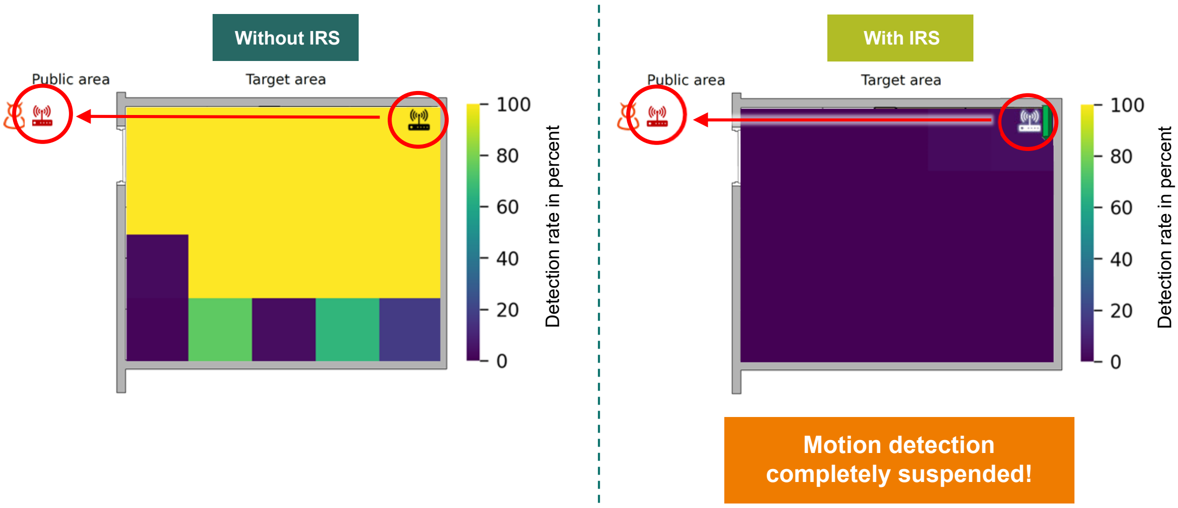
EFFECT OF IRSHIELD



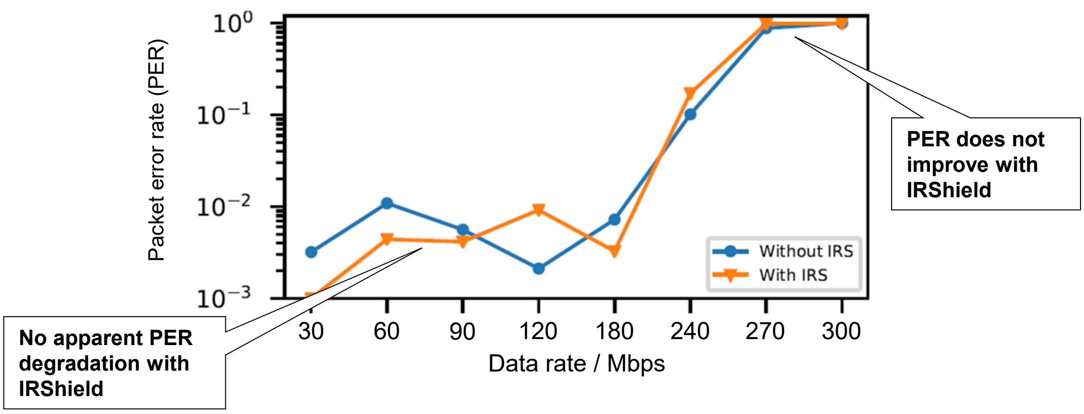
Folie 71

PS75 if possible add no motion
Paul Staat; 28.05.2024

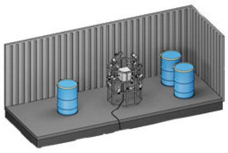
SPATIAL IMPACT OF IRSHIELD

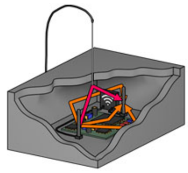


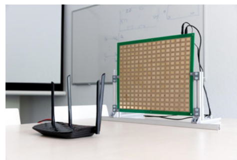
WIRELESS QUALITY OF SERVICE



TALK SUMMARY







Remote Inspections

Strong PUF authentication for entire rooms based on radio-wave propagation

→ Tackles an important problem in nuclear disarmament.

Anti-Tamper Radio (ATR)

Radio propagation effects to verify physical integrity

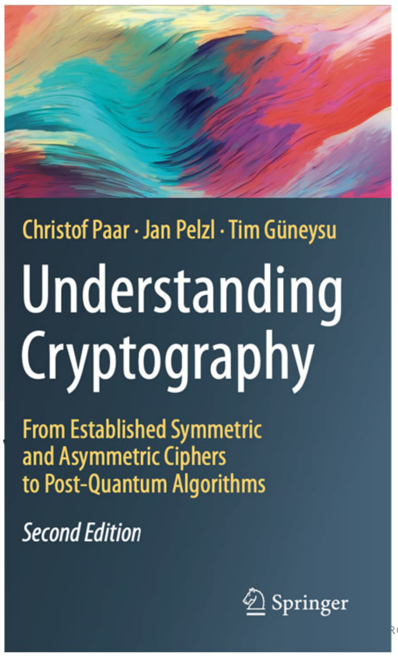
→ Wireless channel for distributed sensing solves system-level tamper detection.

IRShield

Novel means to thwart wireless sensing privacy violation

→ Programmable radio propagation environments can protect sensitive wireless sensing information.

LEARNING MORE ABOUT CRYPTOGRAPHY



- 2nd edition (14 years later, ahem ☺)
- 350 → 500+ pages
- much new material
  - PQC chapter: **Lattice, Code, Hash** (70+ pages)
  - **SHA-3, Salsa20, ChaCha**
  - **Authenticated encryption**
  - Heavily updated**: Security estimations, Discussion, Problem set, Key management**
- Foreword by Ron Rivest

THANKS FOR YOUR ATTENTION!

ANY QUESTIONS?

Contact: christof.paar@mpi-sp.org