



PHYSEC
SECURITY FOR THINGS

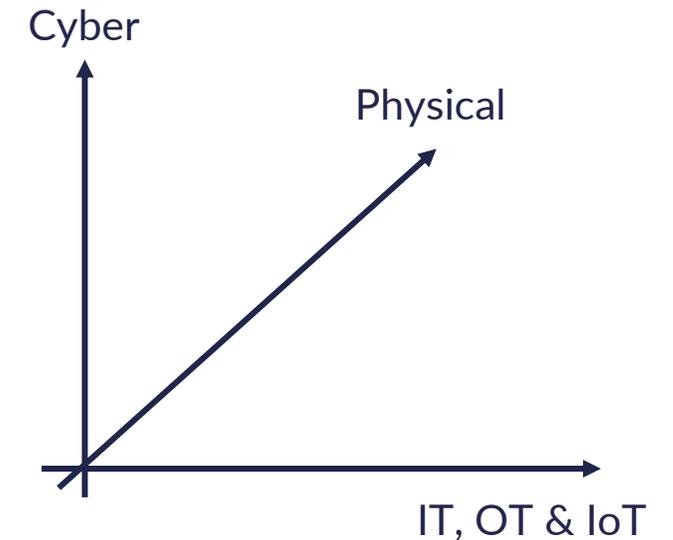
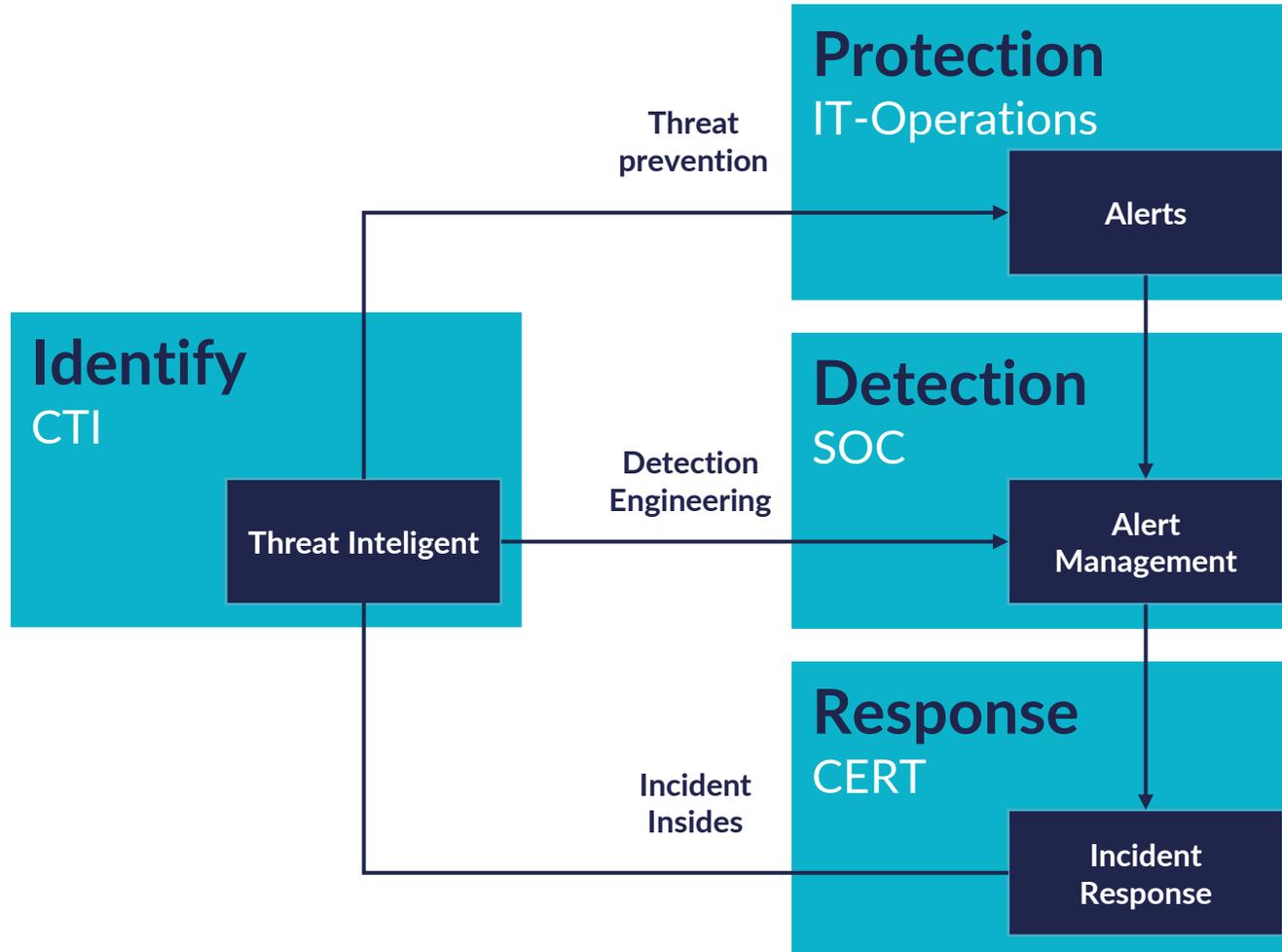
Übergang von der Cyber- zur Cyber- Physischen Sicherheit

Prof. Dr. Christian Zenger (CEO)

www.physec.de

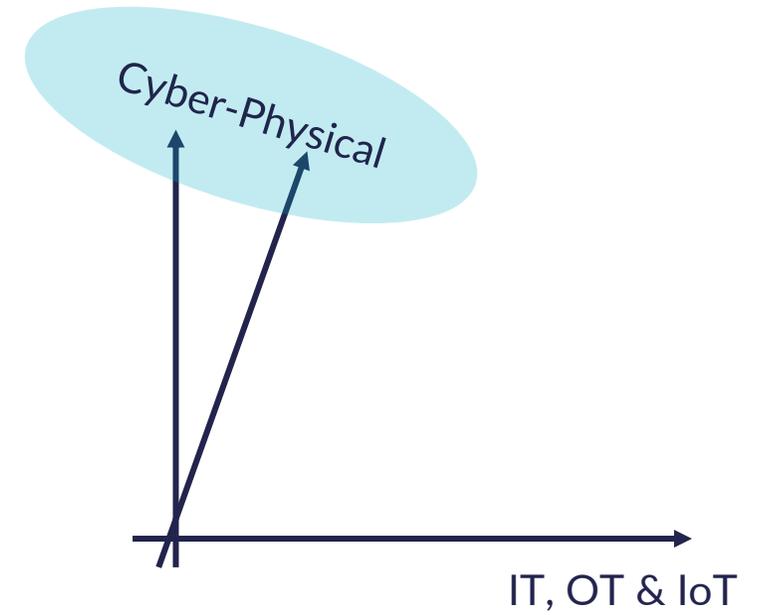
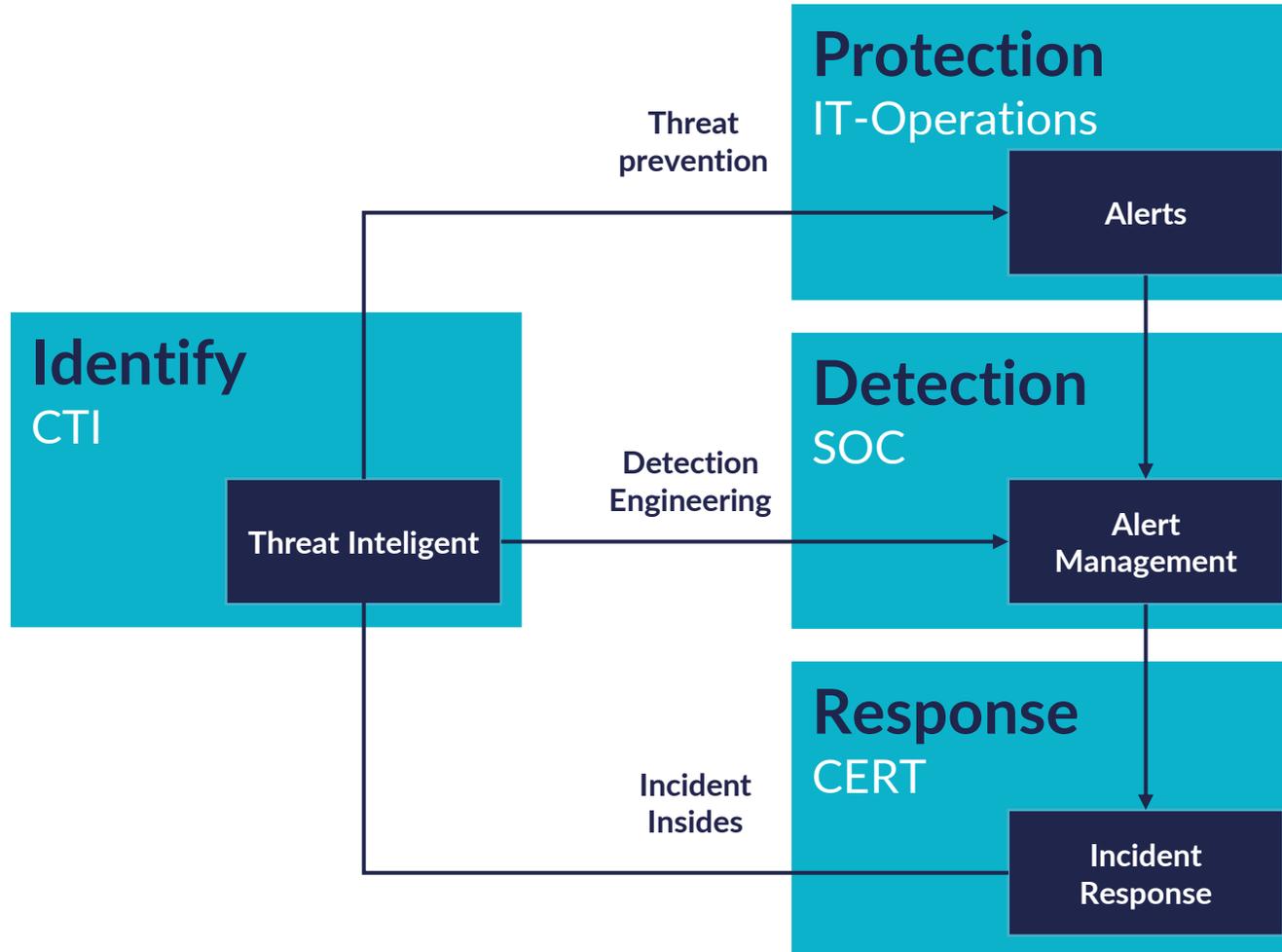
Information Security Process

Technical approaches to improving security



Information Security Process

Technical approaches to improving security



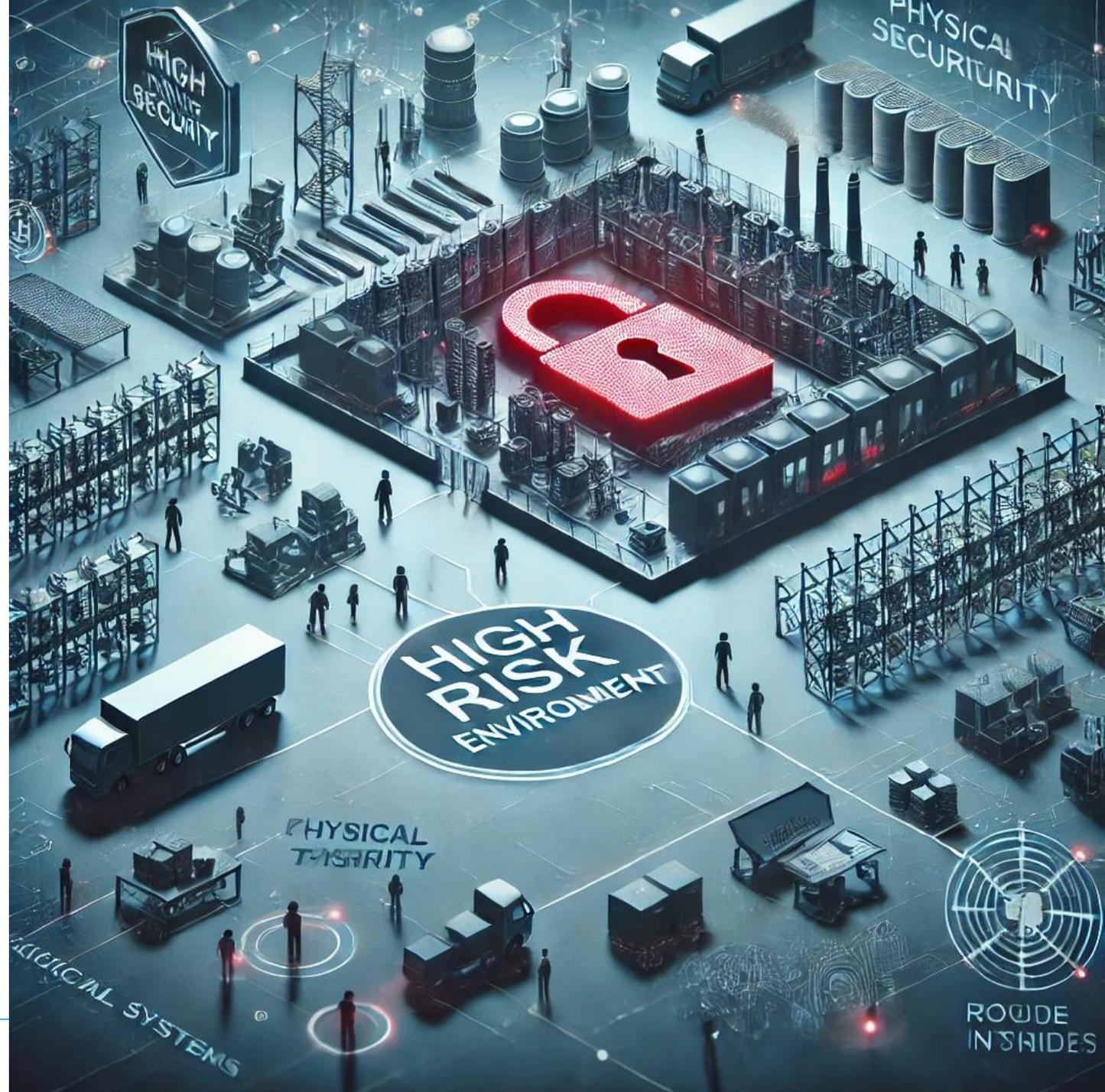
IoT in Public Zones

- Increasing digitization means increasing the deployment of IoT and OT systems in public zones. This **exposes the attack surface** especially for hardware and cyber-physical attacks.
- Isolated incidents of cyber-physical attacks on critical infrastructures are only the tip of the iceberg.



High Risk Environment

- The physical and digital integrity of critical systems is at a high risk, particularly in the supply chain where **perimeter security and access control measures cannot be reasonably expected.**
- Further, the threat of **rogue insiders** is omnipresent.

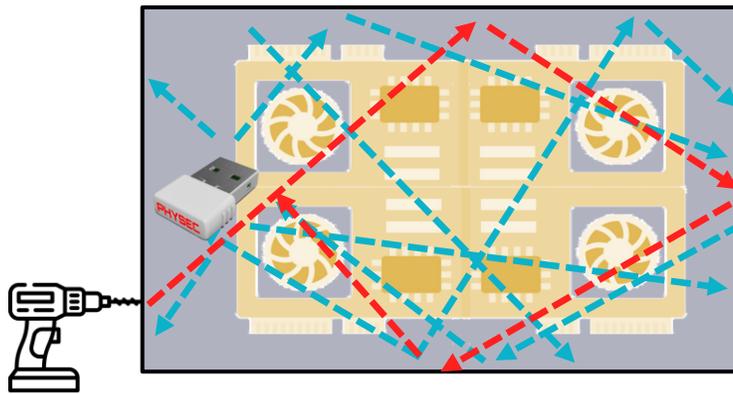


Change Detection

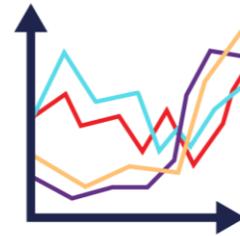
- In contrast to **continuous monitoring systems** or **tamper proofs**, our approach provides alerts upon detecting any changes to assets at only 10% the cost of other solutions on the market.



PHYSEC Wirkprinzip



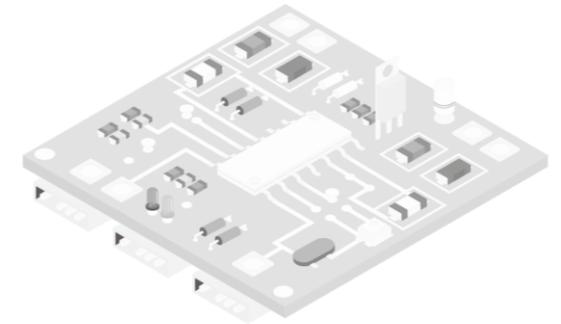
Zu schützendes Gerät



Radiometric
Device Signature



Fingerprint



Digital Shadow



PHYSEC R&D Activities



2013
Research
equipment
250.000€



2015
PHYSEC
evaluation kit
8.000€



PHYSEC v1: ~1.000€

2019



PHYSEC v2: ~200€

2020



Fully integrated:

PHYSEC v3: ~5€

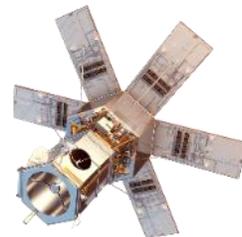
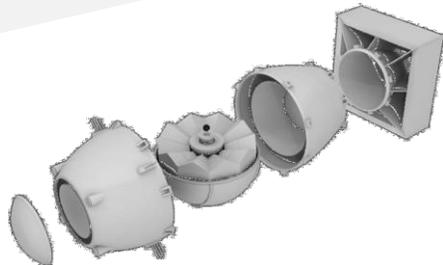
2022

Retrofit:



PHYSEC v3.1: ~50€

2024



PHYSEC SEAL[®]

- Miniatur-RADAR zur Change Detection
- Bis zu 120 μm^3 Auflösung
- Einfach und überall einsetzbar



PHYSEC SEAL[®]

- Miniatur-RADAR zur Change Detection
- Bis zu 120 μm^3 Auflösung
- Einfach und überall einsetzbar



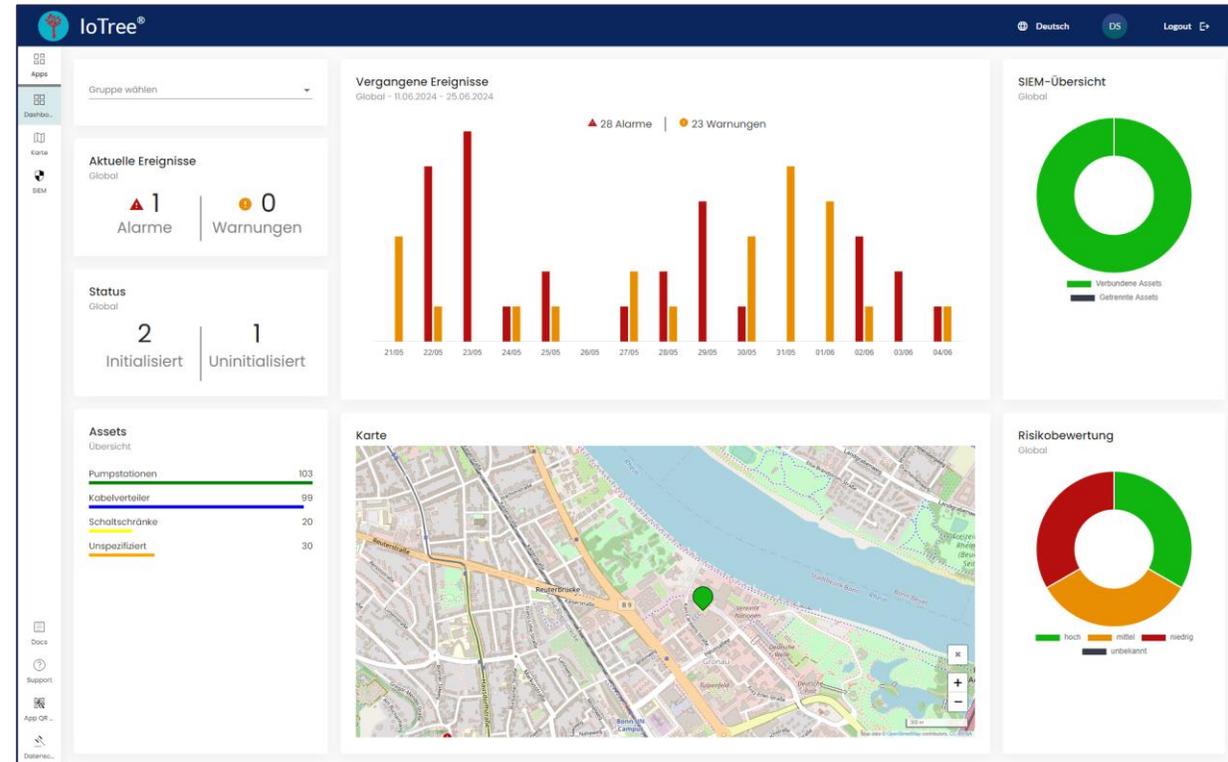
PHYSEC SEAL[®]

- Miniatur-RADAR zur Change Detection
- Bis zu 120 μm^3 Auflösung
- Einfach und überall einsetzbar



PHYSEC SEAL[®]

- Miniatur-RADAR zur Change Detection
- Bis zu 120 μm^3 Auflösung
- Einfach und überall einsetzbar





PHYSEC
SECURITY FOR THINGS

PHYSEC SEAL[®]

Entstanden aus Excellence Cluster

CASA
CYBER SECURITY IN THE AGE
OF LARGE-SCALE ADVERSARIES

- Miniatur RADAR zur Change Detection
- IoT für Hochsicherheitssysteme
- Einfach und überall einsetzbar
- Lösung gegen Insider-Threats

nature communications

Article <https://doi.org/10.1038/s41467-023-4234-2>

Remote inspection of adversary-controlled environments

Received: 13 April 2023
Accepted: 6 October 2023
Published online: 17 October 2023

Check for updates

Johannes Talsch¹, Sebastian Philipp², Ross Bark³, O'ul Kaplan⁴, Christian Zenger^{5,6}, Alexander Glaser⁷, Christof Faer⁸ & Maximilian Groll^{9,10}

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 glint-radar, radio-wave scattering and absorption of a room and its contents, including a set of mirrors with random orientations placed inside, to remotely verify the absence of any disturbance over time. Our technique extends to large physical systems the application of physical unclonable functions for integrity protection. Its main applications are scenarios where parties are mutually distrustful and have privacy and security constraints. Examples range from the verification of nuclear arms-control treaties to the securing of currency, artwork, or data centers.

Remotely monitoring valuable items in adversary-controlled environments constrains an intruder problem. Traditional inspection and surveillance methods are not always possible to implement or may fall short of meeting stringent security and privacy requirements. It may be difficult and perhaps impossible to generate optical fingerprints or glint-radar CCTV cameras in such secure environments to offer some level of confidence in the integrity of stored items. Agreed mutual access inspections have open the possibility of inspecting gathering information. Providing confidence that the surveillance data are originating from the correct location and have not been processed could prove challenging, when the environment is controlled by an adversary party¹. In this context, specific-level surveillance hardware and cryptographic tools are at risk of being hacked and spoofed.

An example for this problem can be found in the monitoring of non-depleted strategic and tactical nuclear warheads as part of an arms-control agreement. These warheads represent 95% of the global nuclear arms stockpile and remain outside of existing agreements because of the difficulties in monitoring them. They are kept in dedicated locations in certain military or civilian sites². In general, a small number of such warheads at a given site cannot be verified easily via satellite imagery or other external technical means that are unable to see into the storage vaults. To insulate them in future arms control treaties, there is a need to develop technologies and protocols to reliably assess if warheads declared as being in storage are not fake but authentic and perhaps impossible to generate optical fingerprints or glint-radar CCTV cameras in such secure environments to offer some level of confidence in the integrity of stored items.

Here we propose and demonstrate a new remote monitoring approach based on a radio-wave measurement system to generate fingerprints of a room and its contents using an array of randomly oriented mirrors to verify the monitoring status over time. This approach only requires a single on-site visit to initiate the monitoring process to initialize the mirrors and take an initial register of the room. Our approach builds on the concept of physical unclonable functions^{3–5} (PUFs) and novel proofs of reality⁶ for which data authenticity, confidentiality and integrity does not rely on digital keys and algorithms but on the information-theoretic complexity of physical systems to achieve privacy and security objectives. Our work shows that glint-radar can be implemented as a secure room and its content certificate for large-scale monitoring in an adversary room and its content certificate for large-scale monitoring in an adversary room.

The main idea for monitoring is to generate a fingerprint by combining a glint-radar with a random mirror. The glint-radar is a radar that is used to monitor the location of a mirror in a room and a nearby environment. Here, the power loss of a mirror

Anti-Tamper Radio: System-Level Tamper Detection for Computing Systems

Paul Saar¹, Johannes Talsch², Christian Zenger³ and Christof Faer⁴

¹Max Planck Institute for Security and Privacy, Bochum, Germany
²PHYSEC GmbH, Bochum, Germany

Always—A whole range of attacks becomes possible when adversaries gain physical access to computing systems that process or contain sensitive data. Examples include side-channel attacks, non-probing, device cloning, or implanting hardware Trojans. Including against these kinds of attacks is considered a challenging endeavor, requiring anti-tamper solutions to monitor the physical environment of the system. Current solutions range from simple tamper switches, which detect if a case is opened, to more sophisticated methods that provide more fine-grained detection of tamper. In addition, the use of tamper switches from an attacker that differs from a physical security on the site and reliability, cost, and difficulty to manufacture on the site.

In this work, we demonstrate that radio-wave propagation in an enclosed system of complex geometry is sensitive against adversarial physical manipulation. We present an anti-tamper radio (ATR) solution as a method for tamper detection, which combines high detection sensitivity and stability with low cost. ATR constantly monitors the wireless signal propagation behavior within the boundaries of a target case. Tamper attempts such as insertion of foreign objects, will alter the observed radio signal response, subsequently raising an alarm.

The ATR principle is applicable to most computing systems that require physical security such as servers, ATMs, and smart meters. As a case study, we use 10⁷ mirrors and iteratively investigate capabilities and limits of the ATR. Using a comprehensive automated testing system, we simulate probing attacks by inserting needles with high precision into protected environments. Our experimental results show that our ATR implementation can detect 100% insertion of needles of diameter as low as 100 μ m under ideal conditions. In the more realistic environment of a room, the detection sensitivity is reduced to 100% for needles of diameter of 1 mm for a period of 10 days.

1. INTRODUCTION

A. Motivation

Today, almost all parts of our digital society require security mechanisms. These usually rely on cryptographic primitives and protocols which have been subjected to intensive scrutiny in the past decades. As a result, mathematical attacks are not largely infeasible and attackers often focus on other weaker, but still break a system. It is especially concerning when adversaries gain physical access to devices which opens a broad attack surface. Depending on the attacker's motivation, their goal might be to extract secret information, plant malicious hardware, or theft of intellectual property (IP).

There are a number of prominent examples for invasive attacks. For instance, the extraction of trusted platform module (TPM) stored firmware keys via bus sniffing has been shown^{7,8} (Fig. 1). In this case, physical access completely

unlocks the device⁹. As another example, the manipulation of PIN entry devices for electronic payments allows attackers to copy card data and PIN codes¹⁰. In another case, it was possible to circumvent the encryption of PIVCA hardware¹¹, allowing for theft and injection of malicious circuit alterations. A real world example with far-reaching consequences can be found in the Snowden documents. The NSA¹² is apparently able to intercept and hackback hardware in transit in a manner that makes it virtually impossible for the recipient to detect tampering. This could, for example, result in tampered routers and firewalls which give persistent access to otherwise secure networks.

In defense against these kinds of attacks, a system designer can add tamper-detection solutions that monitor the physical state of the system. Any detected attack raises an alarm and the system usually has to resort to "self-destruction", which includes the wiping of any sensitive information such as secret keys material before the attacker has a chance of extraction. While anti-tamper techniques do not provide the same level of security as expected by standards of modern cryptography, they are still an important building block for the protection of real-world devices. In practice, computer solutions range from simple switches, that detect if a case has been opened, to complex hardware security modules (HSM). These use sophisticated methods made of conducting material to shielded devices of physical integrity and environmental monitoring¹³— devices to demonstrate reliable detection of physical tampering.

The most important certification standards for devices that require physical security are FIPS 140-2¹⁴, its recent successor FIPS 140-3, and Common Criteria (CC). In the case of FIPS, four levels of security are defined. Starting from the third level, compliant devices are expected to detect physical attacks and to react to them by termination of critical security parameters (CSPs). As a derivative of devices certified in the NIST's cryptographic module validation program is publicly available¹⁵. As an example, the Advanced Access Key Management Service HSM provides three levels physical security. Its description defines "the cryptographic boundary (i.e., in the scope domain of the appearance) and says that "all key materials are maintained exclusively in volatile memory in the appliance and are created immediately upon detection of physical tampering"¹⁶. Further documentation¹⁷ only

¹Max Planck Institute for Security and Privacy, Bochum, Germany; ²Project: cyber resilience and IT-Security, Fraunhofer IPA, Karlsruhe, 80, USA; ³Faculty of Engineering and Applied Sciences, Harvard University, Boston, MA, USA; ⁴PHYSEC GmbH, Bochum, Germany; ⁵Max-Planck-Wellbeing, Ruhr-University Bochum, Bochum, Germany; ⁶Research Engineering and Cognitive Systems Department, TU Berlin, Berlin, Germany; ⁷Secure Computation Laboratory, University of Connecticut, Storrs, Mansfield, CT, USA; ⁸email: johannes.talsch@mpispi.rwth-aachen.de; sebastian.philipp@mpispi.rwth-aachen.de

Nature Communications | (2023) 14:6666



60+

Mitarbeiter

8+

Jahre auf dem Markt

60+

Gerätetypen
von 30+
Herstellern

50+

IoT[®] -
Plattformen



PHYSEC
SECURITY FOR THINGS



130.000+

Connected Devices

50+

Kunden

LinkedIn



PHYSEC GmbH

Prof. Dr. Christian Zenger

Gründer und CEO

christian.zenger@physec.de

