


# Preparing for Tomorrow's Fraud:

## Offensive Security Research on Merchant Payment Hardware

# Niels Vonk

## Team Lead – Offensive Security

## @ Adyen





# Aleksei Stennikov

**Head of Software Composition Analysis Unit**
**@ PCA Cyber Security**





# Introduction
# Adyen & PCA



# Adyen

Global Payment Service Provider for E-commerce, In-Person Payments and Platforms

IPO in 2018 - Bank license in Europe, UK Banking Authorization, Branch license in US

**99.9999%**
Uptime during Black Friday and Cyber Monday

Wide range of terminals vendors and models supported

GLOBAL PROCESSED VOLUME
**€1.39TN**
Financial Year 2025

All technology developed in-house, weekly release cycles

**1.5 Million**
terminals in the field

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

# PCA Cyber Security

PCA | CYBER SECURITY

PCI Security Standards Council
ASSOCIATE PARTICIPATING ORGANIZATION

TISAX ENX ASSOCIATION RESULT AVAILABLE
Level 3 Assessment with Protection of Prototype

| | |
|---|---|
| Established: | 2019 |
| Locations: | Hungary, Germany, Spain & USA |
| Team: | 3-10+ years of experience |
| Successful projects: | 100+ in various sectors |
| On-site centers of expertise: | CyberLab & CyberGarage |



Penetration Testing



Device-centric Threat Intelligence Platform



Vulnerability Intelligence



Software Composition Analysis & Patch verification



Security Assessment

*We are a team of White Hat Hackers & Threat Intelligence Analysts*

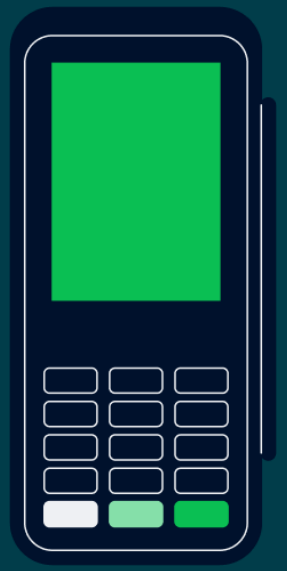
20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

# Our payment offering

## In-Person Payments



# POS Ecosystem



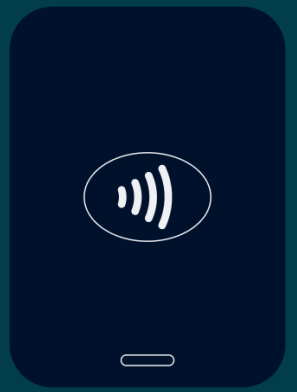
**Countertop & Customer facing**

Compact, stationary devices on the counter



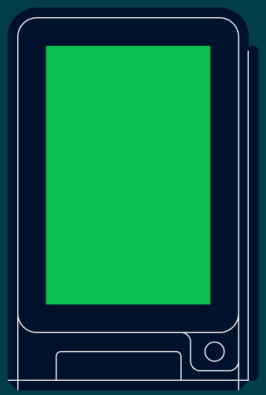
**Mobile terminals**

Standalone and portable systems



**Card reader/ Tap to Pay**

Accept payments on your mobile devices



**Unattended**

Self-service devices

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

# The Compliance Baseline

PCI 5/6/7 flow and timelines

| Assessment Area | PCI PTS v5 (2017-2021) | PCI PTS v6 (2020-2026) | PCI PTS v7 (2025-TBD) |
|---|---|---|---|
| **Testing Structure** | Generic, monolithic requirements. | Four distinct evaluation modules. | Heavily focused on software segregation and component isolation. |
| **Cryptography Minimums** | Acceptable legacy support (RSA, TDES). | ECC hardware support mandated. | Strict 128-bit minimum for all device security functions; |
| **Network Protocols** | Older TLS versions accepted. | Modern protocols standard. | TLS 1.3 mandated; TLS 1.2 cipher limited. |
| **Firmware Lifecycle** | Assessed once at certification. | Lab re-validation required every 3 years. | Continuous secure update validation. |
| **Application Logic** | Basic payment app isolation. | SPoC (Software PIN on COTS) support integrated. | Strict sandboxing and zero cleartext routing to non-payment apps. |

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

# The Offensive Reality



# The Offensive Reality

Hackers do not care about the compliance

Forbes

EDITORS' PICK | INNOVATION > CYBERSECURITY

'Millions' Of Payment Terminals Are Vulnerable To Credit Card Theft Hacks

By Thomas Brewster, Forbes Staff. Senior writer at Forbes covering cybercrim... Follow Author

Published Dec 10, 2020, 06:16am EST, Updated Dec 10, 2020, 11:16am EST

This article is more than 5 years old.



Vulnerable Verifone payment terminals can be hac...

JEFF GREENBERG/UNIVERSAL IMAGES GROUP VIA GETTY I...

New Android malware steals your credit cards for NFC relay attacks

By Bill Toulas

April 19, 2025 11:17 AM 4



kaspersky

Home > About > Press Releases > Tap-to-pay, insert-to-rob: cybercriminals can now block contactless payments

**Tap-to-pay, insert-to-rob: cybercriminals can now block contactless payments**

January 31, 2023

**Kaspersky uncovered three new variants of Prilex malware, made by a group of cybercriminals, that was named after the most advanced Point-of-Sales (PoS) malware back in 2022. The discovered Prilex modifications can now block contactless near-field communication (NFC) transactions on infected devices, forcing customers to use their physical credit cards, enabling cybercriminals to steal money.**

USENIX

THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

**More is Less: Extra Features in Contactless Payments Break Security**

George Pavlides, *Surrey Centre for Cyber Security, University of Surrey;* Anna Clee, *University of Birmingham;* Ioana Boureanu, *Surrey Centre for Cyber Security, University of Surrey;* Tom Chothia, *University of Birmingham*

https://www.usenix.org/conference/usenixsecurity25/presentation/pavlides

IMPACT FACTOR 2.9 CITESCORE 7.0

Systematic Review Editor's Choice

Advanced Hardware Security on Embedded Processors: A 2026 Systematic Review

Ali Kia, Aaron W. Storey and Masudul Imtiaz

USENIX

THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

**Zombie Cards Back Online: Reviving Expired Credit Cards for Contactless Payments**

Raja Hasnain Anwar, Gerard DeCunha, and Muhammad Taqi Raza, *University of Massachusetts Amherst*

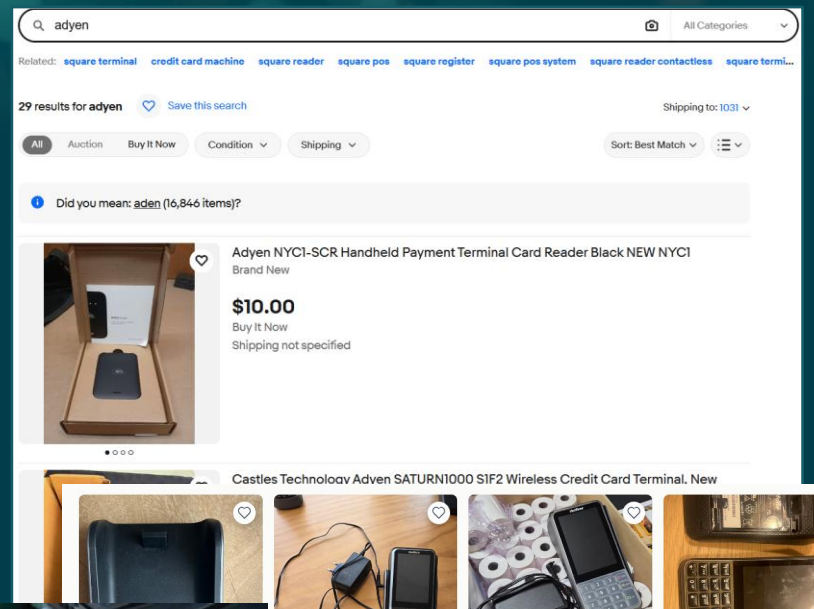
https://www.usenix.org/conference/usenixsecurity26/presentation/anwar

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

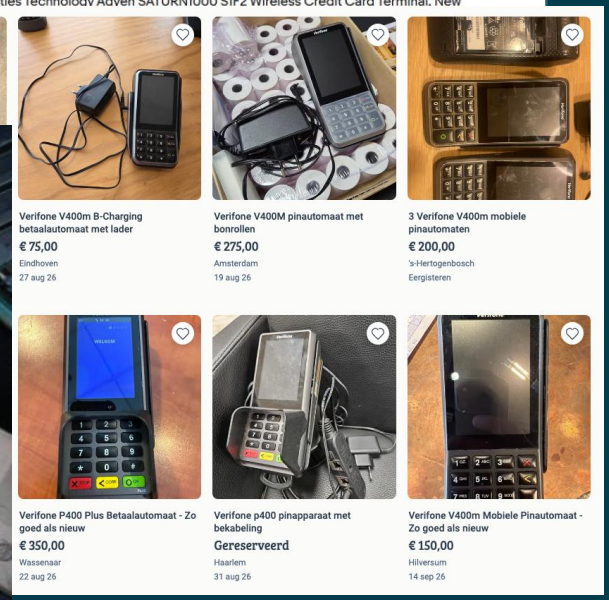
# The Offensive Reality

How do hackers obtain terminals?

- You don’t need to steal a terminal for a store
- Disposed terminals
- 2nd hand web shops
  - Tampered
  - Onboarded



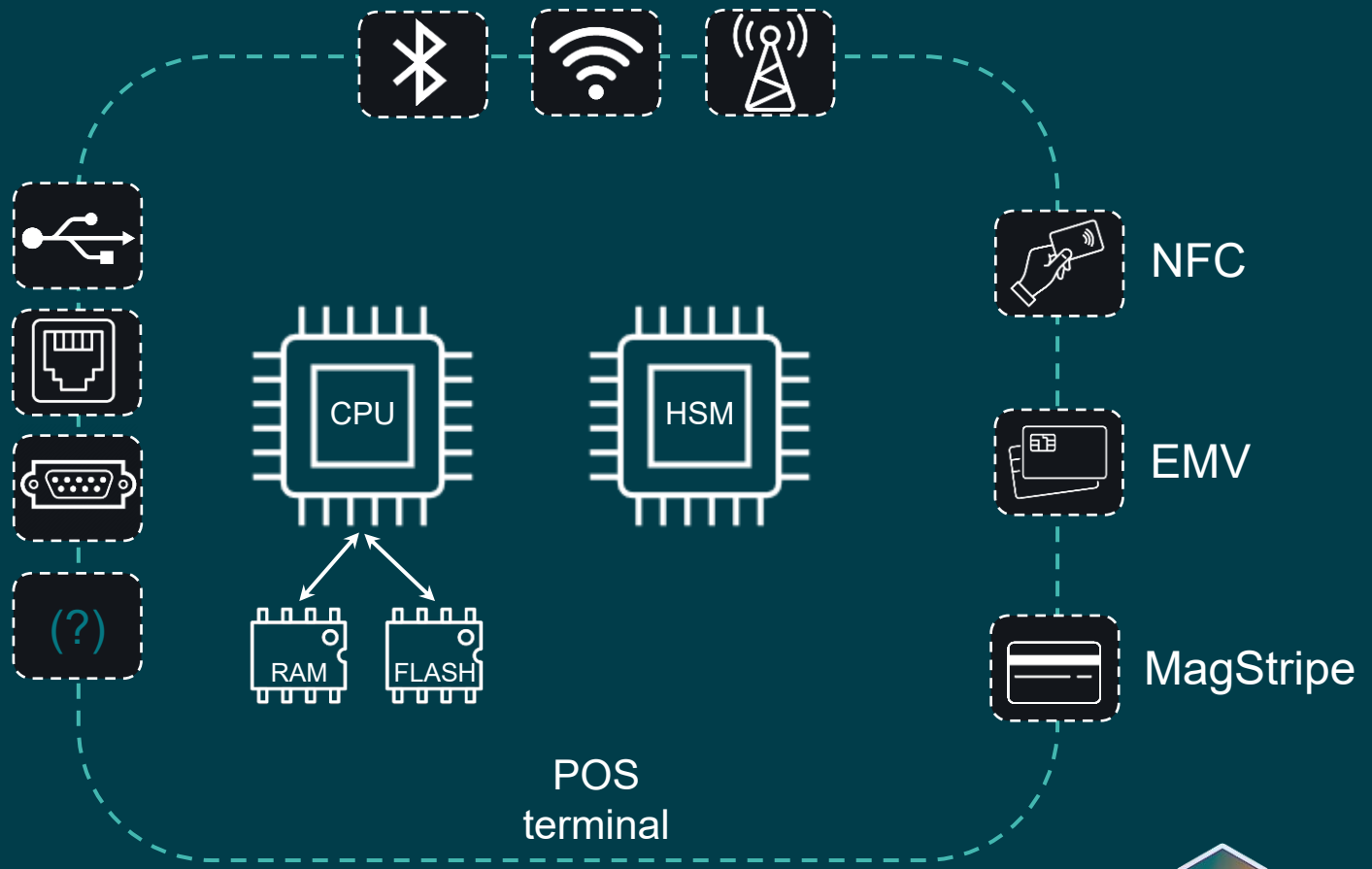



20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

# Architectural overview payment terminal

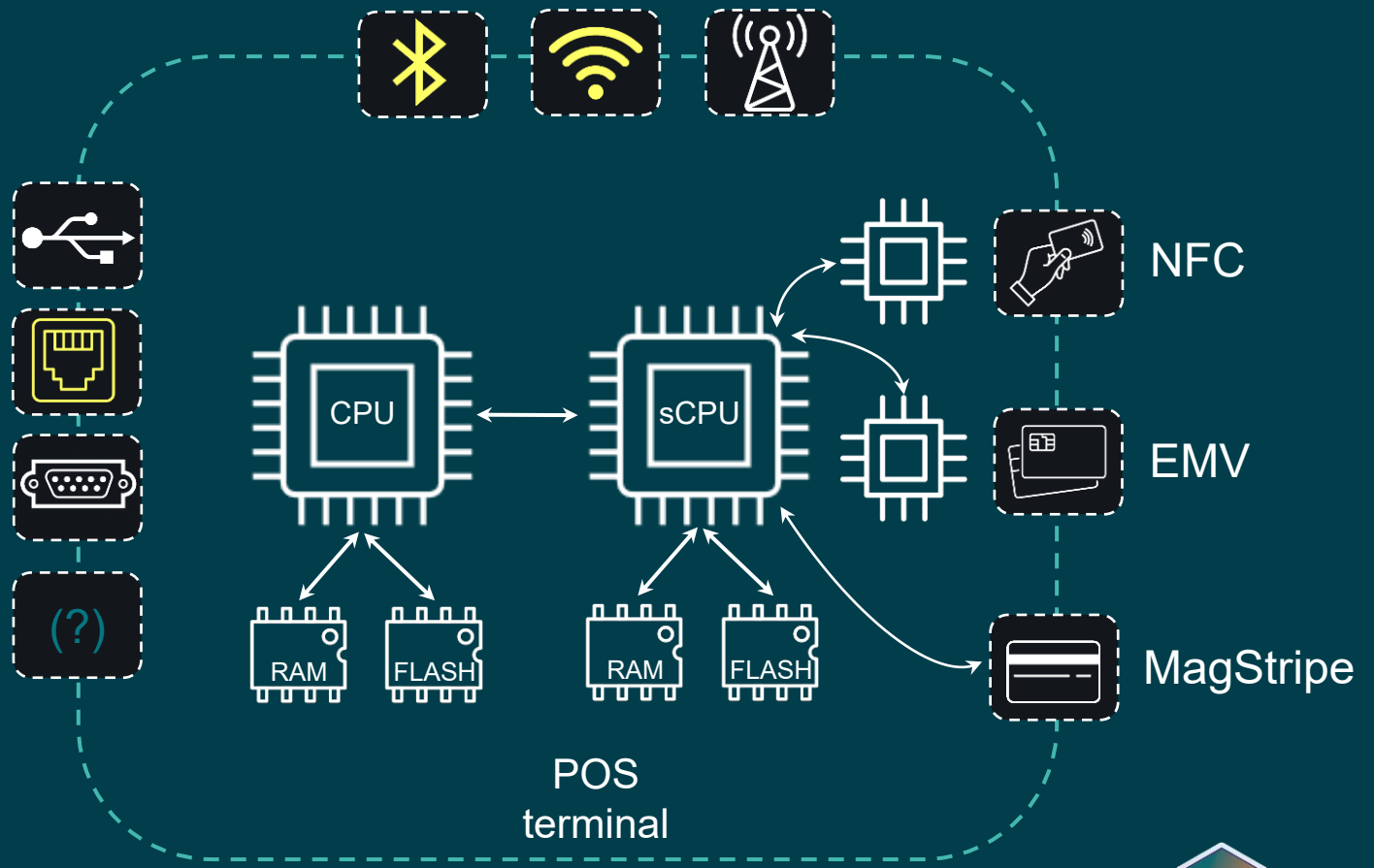
Generic view




20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

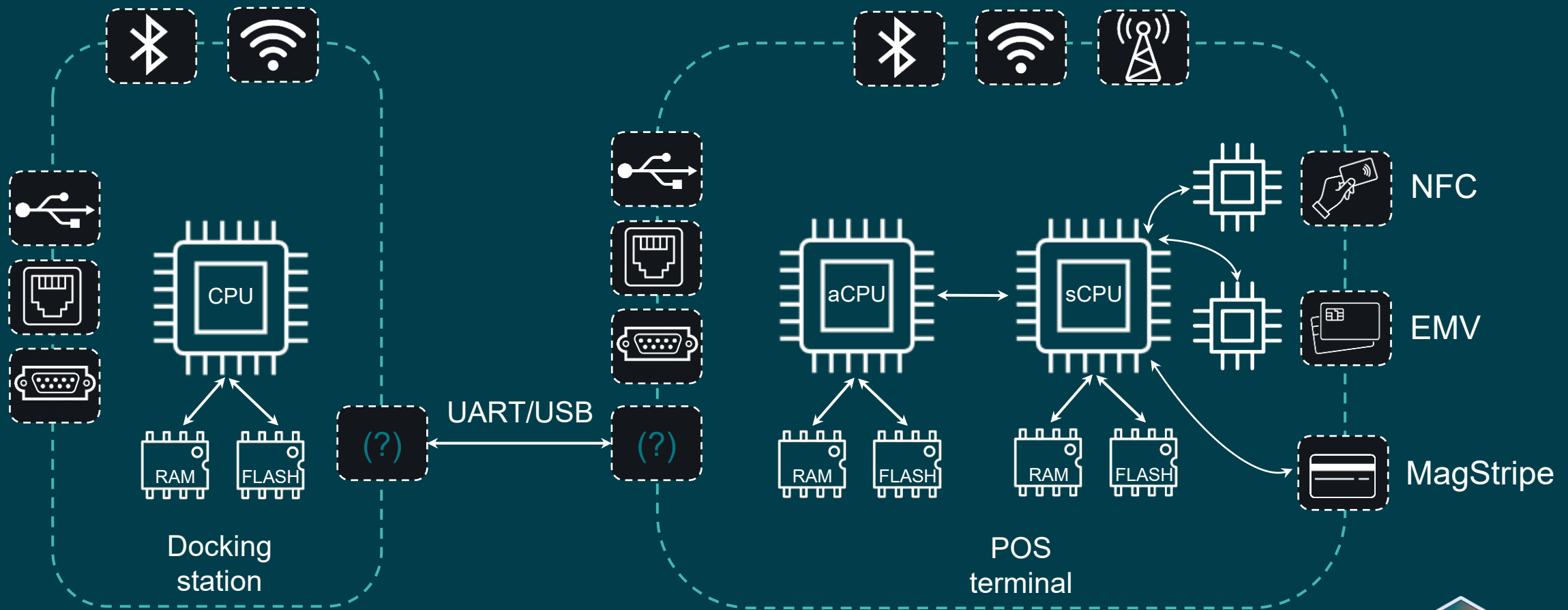
# Architectural overview payment terminal

Generic view ++



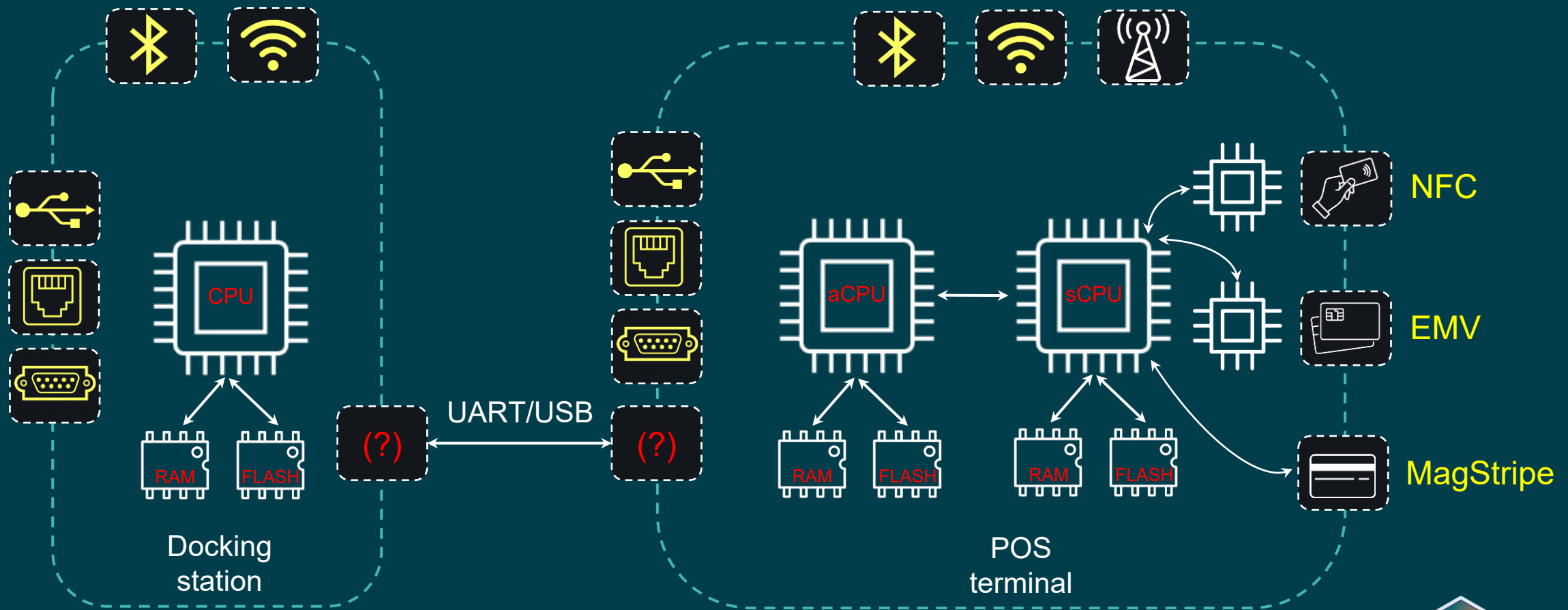

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

# Architectural overview payment terminal




20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

# Architectural overview payment terminal




20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

# Proactive defense

## The power of collaboration



# Collaboration

- Adyen works with various vendors to provide its merchants with a wide range of payment terminals and integrations

- We actively collaborate with PCA Cyber Security to:
  - Threat Model
  - Plan and Prioritize
  - Execute and Support
  - Communicate and Validate

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

# Collaboration flow diagram

PCA | CYBER SECURITY

Threat Model

Vulnerability research

Security retest

New terminals

Security Reports

New versions

Retest Reports

Final Reports

adyen

Threat Model

Internal analysis

Testing functionality

Security Reports

New versions

**Terminal OEMs**

Fixing software & hardware

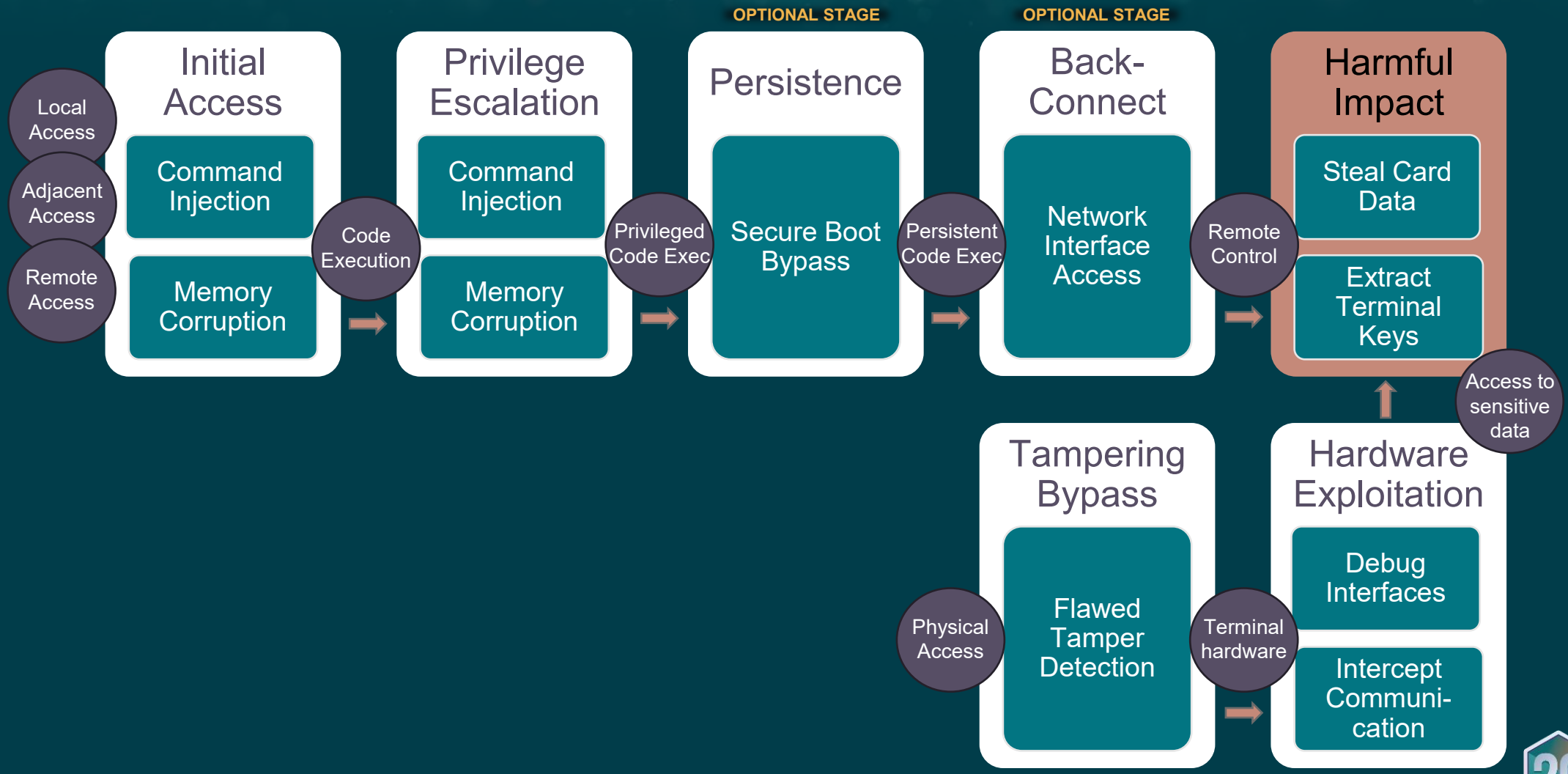
20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

# Realistic Attack Paths

## Beyond the Checklist



# Attack Stages



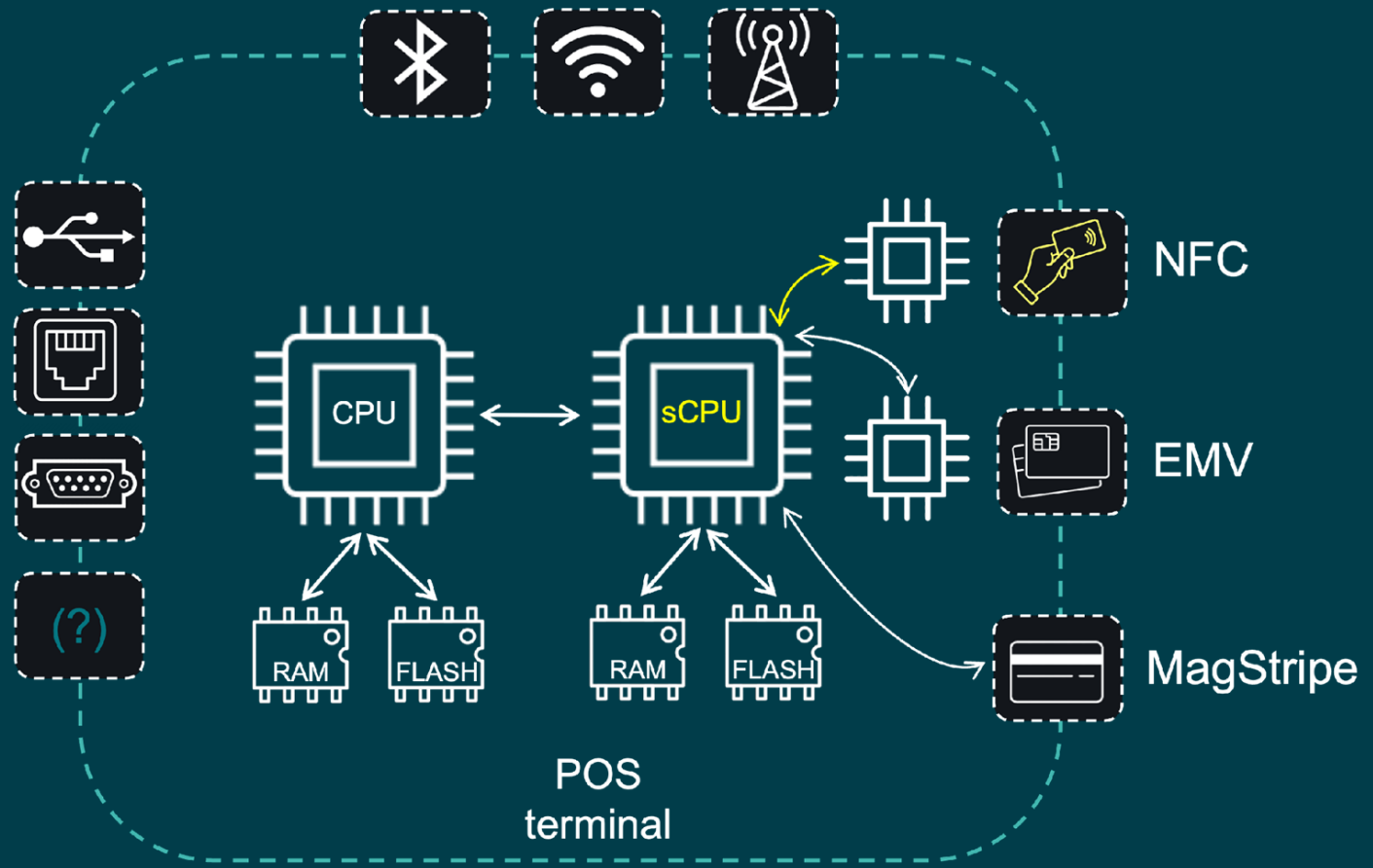

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

# Disclaimer

**The attacks, exploits and firms depicted are fictitious. Any similarity to actual devices or to actual firms, is purely coincidental.**

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

# Full Attack Chain – Step 1

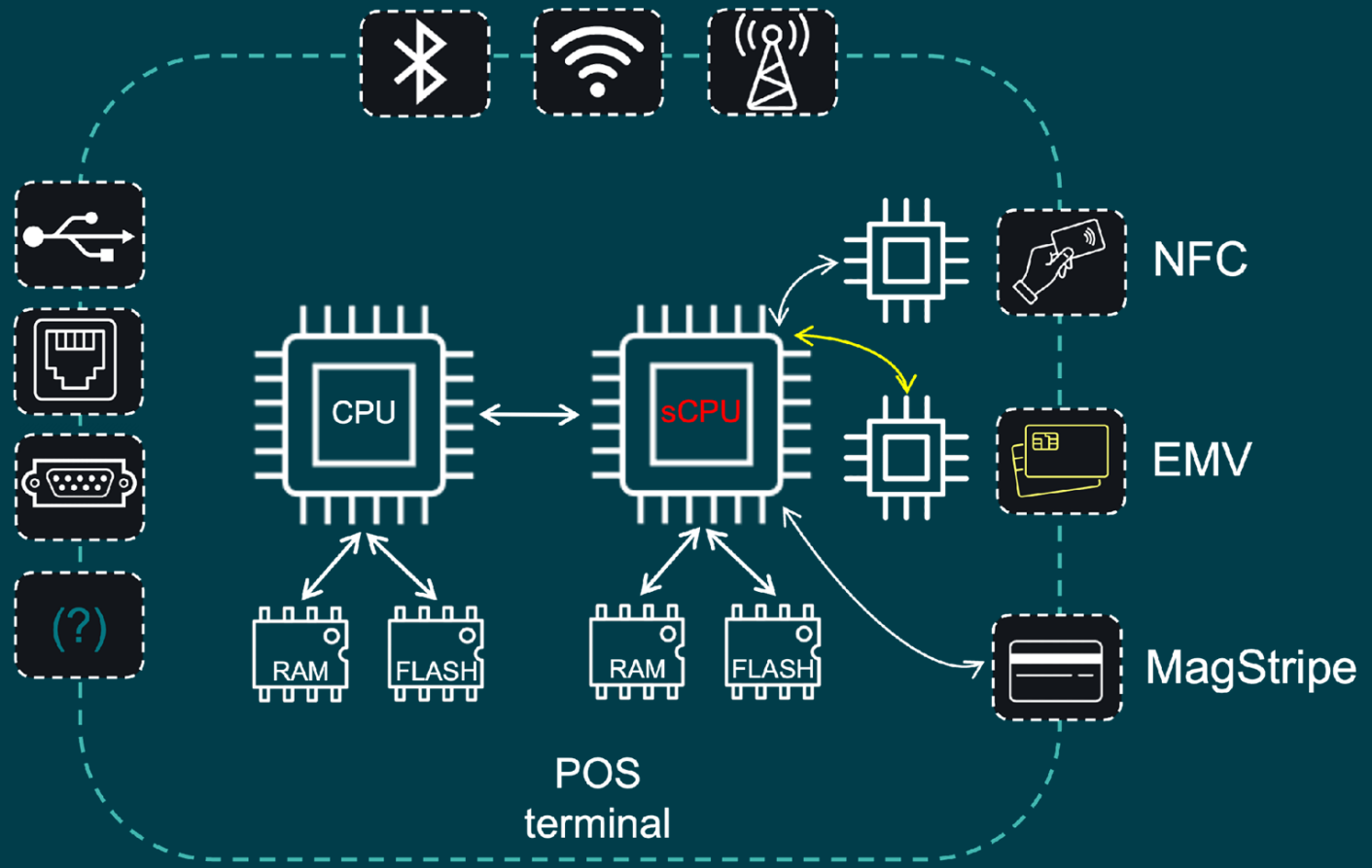



Step 1:

Exploit vulnerability in the NFC handling to gain unprivileged code execution on the sCPU to deploy first payload

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

# Full Attack Chain – Step 2

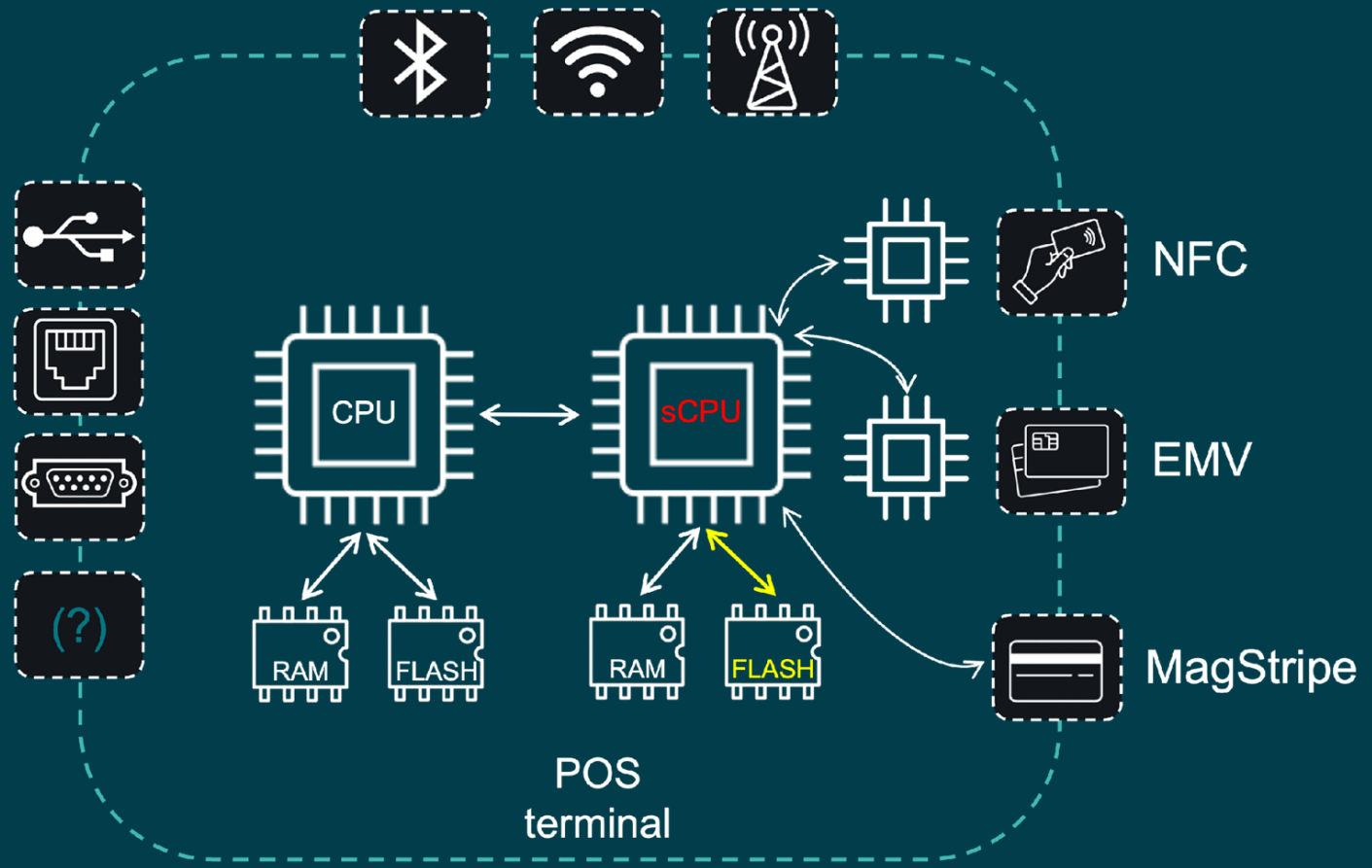



Step 2:

Trigger payload of step 1 by exploiting vulnerability in the EMV interface to gain privilege escalation and code execution on sCPU

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

# Full Attack Chain – Step 3

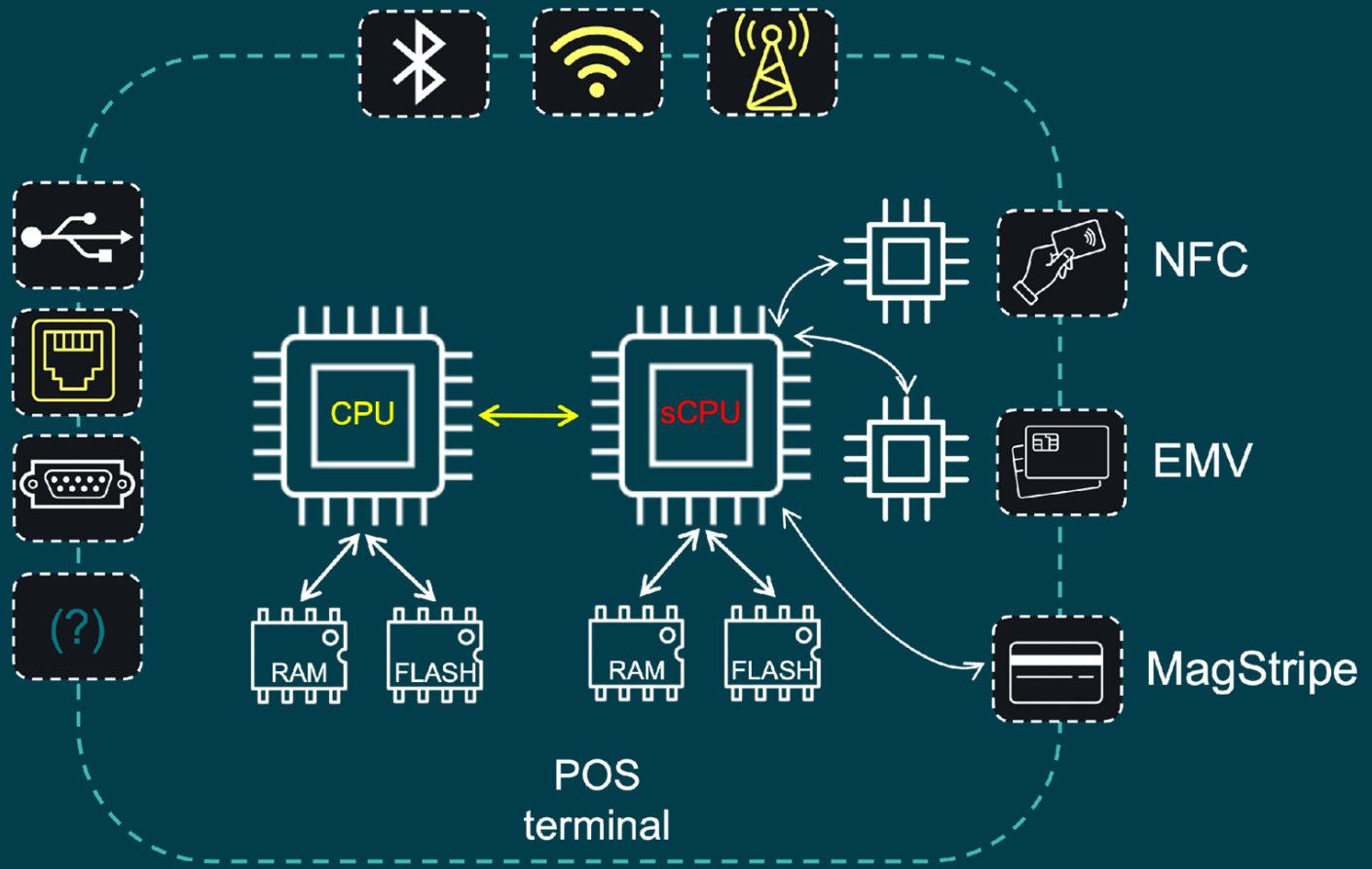



Step 3:

The payload from step 2 is then used to extract the cryptographic keys from the protected disposable memory of the sCPU that are used to encrypt the PAN and PIN

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

# Full Attack Chain – Step 4




Step 4:

By hooking into the supervisory call sensitive data such as cleartext PAN and PIN can be extracted to external servers via the exposed network interfaces

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

# Vulnerabilities summary

| Type | Sub-type | Component | CVSS 3.1 score (highest) | Interface | Count |
|---|---|---|---|---|---|
| **Hardware** | Tamper bypass | aCPU | 4.8 | Physical | 1 |
| **Broken security controls** | Secure boot failure | aCPU, sCPU | 7.5 | Physical | 2 |
| | Insecure MMU configuration | sCPU | 0 (Info) | - | 1 |
| **Memory corruptions** | Stack overflow | sCPU | 8.8 | NFC, EMV | 3 |
| | BSS overflow | sCPU | 7.9 | EMV | 1 |
| | Integer overflow | aCPU | 7.8 | local | 1 |
| | | | | **Overall** | **9** |

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

# Vulnerabilities summary

**21+ VULNS PER DEVICE COULD BE INHERITED**

| Type | Sub-type | Component | CVSS 3.1 score (highest) | Interface | Count |
|---|---|---|---|---|---|
| **Broken security controls** | Insecure MMU configuration | _CPU | 0 (Info) | - | 1 |
| **Memory corruptions** | Heap overflow | _CPU | 6.8 | NFC, cmd | 9+ |
| | Stack overflow | _CPU | 6.8 | NFC, cmd | 7 |
| | BSS overflow | _CPU | 8.8 | EMV, cmd | 3 |
| | Null pointer deref | _CPU | 3.5 | cmd | 1 |
| | | | | **Overall** | **21+** |

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council



```
[raspberrypi32:poc:0]
```

```
[raspberrypi32:poc:130] python poc_server.py
```

```
[raspberrypi32:poc:0] cat card_data_readme.txt
There is demo for card data saving attack. The attack has the following steps:
  1) The vulnerability in the NFC interface is used to get remote unpriviliged code execution on the Secure Modu
le.
  2) The payload from the step 1 is used to trigger another vulnerability (in the EMV chip interface) to elevate
 privileges and get execution of an arbitrary code on the privileged level.
  3) The payload from step 2 is used to setup custom hooks on the supervisor call's level. They is used to steal
 card data and send it to the remote server via [redacted] SDK from the Android part of the terminal.

This demo send key storage from the terminal to remote server.

Also, privileged code execution can be used to extract firmware and OTP memory data.
[raspberrypi32:poc:0]
```

```
@ 11 0:*                                                    2! 1h19m 0.02 4x1.8GHz 3.7G6% 29G43% 2024-08-22 13:58:03
```

ADYEN - PCA DEMO

# Defense-in-Depth

Hardening of the terminal

- Terminals require various defense-in-depth principles

- Safeguard the integrity of the payment terminals
  - Protecting the boot process and firmware integrity
  - Fault handling and memory protection
  - Least privileged configuration for sensitive (system) functions
  - Disabling extensive logging and debug functionalities
  - Pinning of secure version used within the terminal

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

# Closing the Loop

Continuous testing and validation

- Early iterations on design and new functionalities
- Transparency of the SBOM and validation of security posture
- Establish monitoring for N-day vulnerabilities
- Active threat intelligence focused on payment ecosystem
- Periodical assessment after (major) changes or new features

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

# Defending the Ecosystem

Lessons Learned

- Testing beyond the standards
- Threat modelling based on the (bad) use-cases for merchants
- Ever changing threat landscape, techniques and tools
- Extend scope of assessment to all peripherals

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

# Special thanks!

Who made this possible

**Artem Ivachev**

**Danila Parnishchev**

**Polina Smirnova**

**Radu Motspan**

**Mikhail Evdokimov**

**Abdellah Benotsmane**

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

# Thank You !



https://www.linkedin.com/in/nvonk



https://www.linkedin.com/in/aleksei-stennikov

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council