АРХИТЕКТУРА НА POS АТАКИТЕ

Hardware • Protocols • Attacks • Defenses

OWASP Bulgaria | 2026

Здравко Здравков

Физическа структура на POS терминала

EMV CARD
Chip + NFC

CARD READER
MSR / ICC / NFC

SECURE CPU
control plane

ACQUIRE
R
HOST

PIN PAD / EPP
PIN + anti-tamper

SECURE
ELEMENT
HSM / SAM

PCI PTS

PCI DSS

P2PE

SRED

EMV стандарт — 4-те книги на EMVCo

1 ICC to Terminal Interface

Физически и електрически интерфейс, ATR, T=0/T=1

- ISO 7816 контакти
- ATR parsing
- Protocol negotiation

2 Security & Key Management

Криптография, PKI, offline/online authentication

- RSA / SHA
- SDA / DDA / CDA
- Certificate chains

3 Application Specification

Transaction flow, CVM и terminal risk management

- AID selection
- GPO + AFL
- Cryptogram generation

4 Cardholder & Acquirer Interface

UI, PIN entry, receipts и host communications

- Display management
- PIN pad interface
- Acquirer protocols

EMV Contact — Transaction Flow

ISO 7816 контактна линия: C1(VCC) • C2(RST) • C3(CLK) • C7(I/O) — half-duplex обмен между терминал и ICC

NFC / Contactless комуникация

CARD / PHONE
NFC antenna

RF FIELD
13.56 MHz

POS TERMINAL
Reader coil

ISO 14443-A/B

< 4 cm range

< 500ms tap-and-go

Kernels C1–C8

1 POLLING

2 ACTIVATION ATQA/ATS

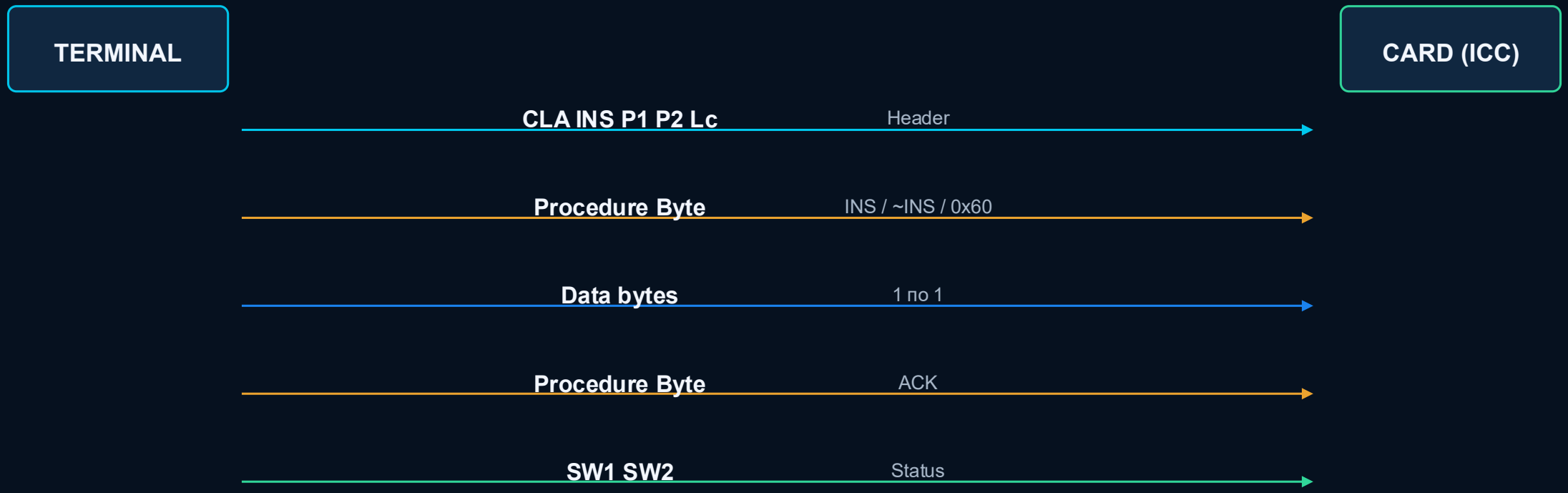
3 SELECT PPSE

4 GPO

5 READ RECORD

6 GENERATE AC

T=0 — Character-Oriented протокол



H — **Half-Duplex**
една I/O линия C7

P — **Procedure Byte**
ACK / NAK / wait

E — **Error Detection**
parity per byte

B — **Byte-by-Byte**
символ по символ

T=1 — Block-Oriented протокол

NAD	PCB	LEN	INF (Data)	EDC
Node Address	Protocol Control	Length	Information Field	Error Check
1 byte	1 byte	1 byte	0–254 bytes	LRC / CRC

I

I-Block

Information + APDU data
Chaining support (M-bit)

R

R-Block

Receive-ready ACK/NAK
Sequence number sync

S

S-Block

RESYNCH / IFS / ABORT
WTX wait extension

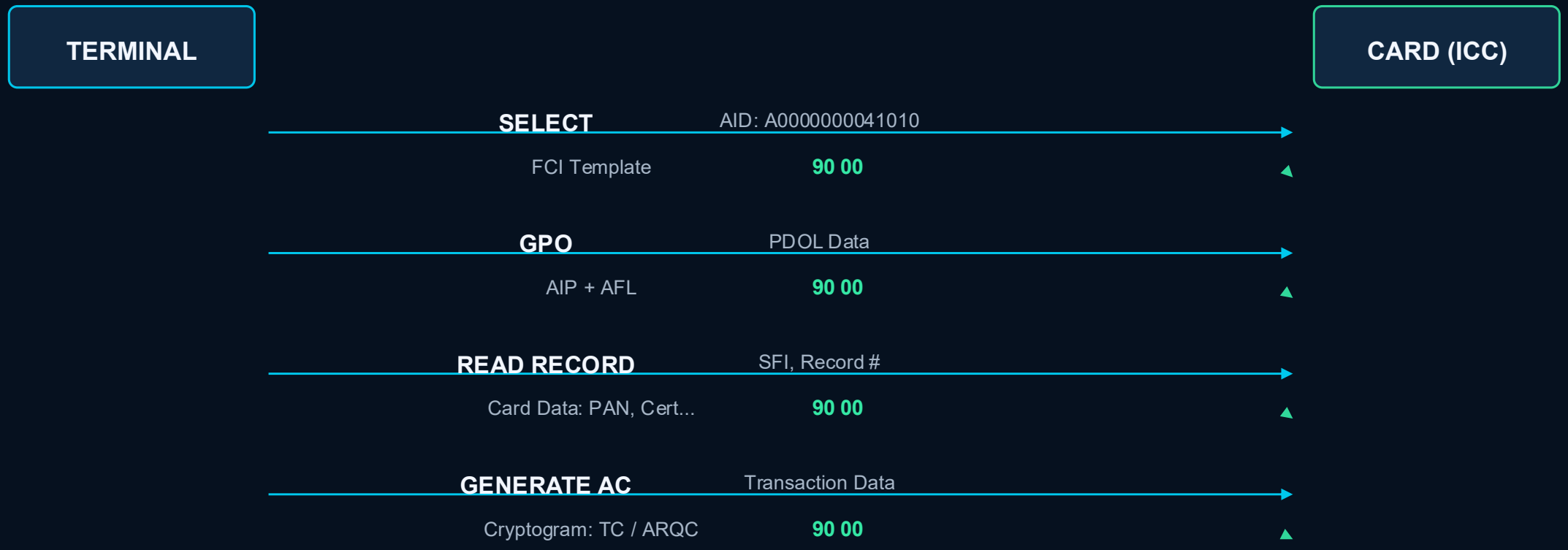
APDU — Application Protocol Data Unit

Command APDU (C-APDU)

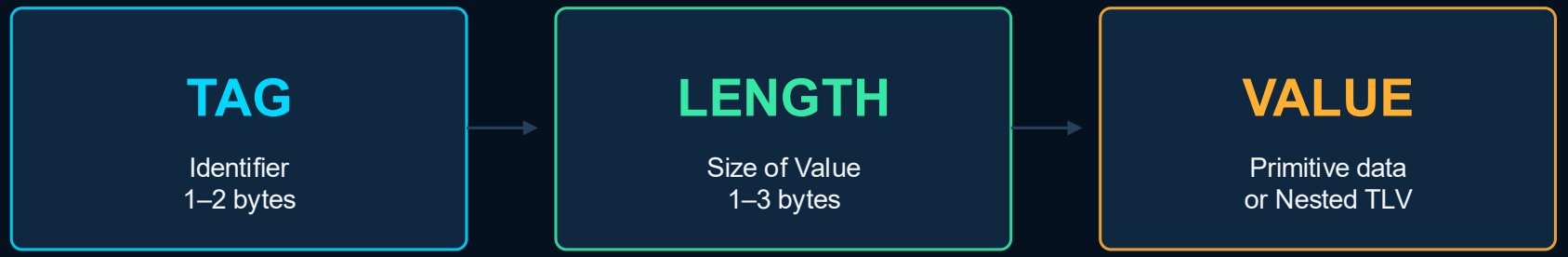
Response APDU (R-APDU)

90 00	SUCCESS
6A 82	FILE NOT FOUND
69 85	CONDITIONS NOT SATISFIED
63 00	AUTH FAILED

APDU — Transaction Sequence



Обмяна на данни — TLV формат



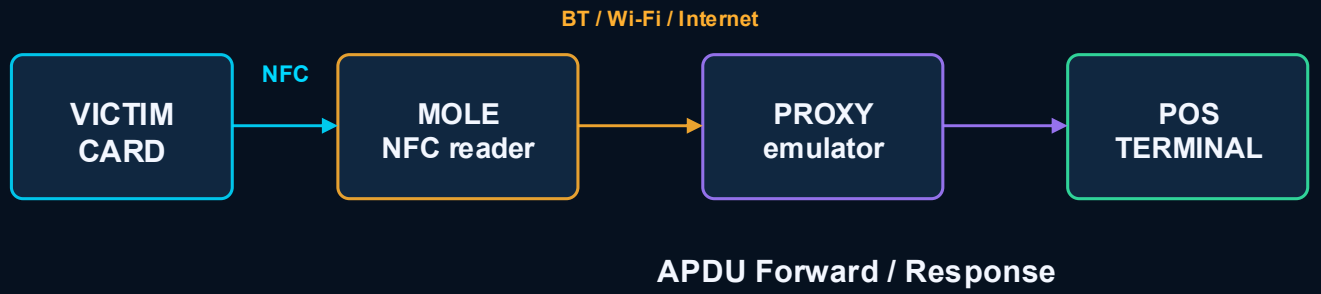
CARD DATA

5A	**Application PAN**	номер на картата
5F24	**Expiration Date**	срок на валидност
9F26	**App Cryptogram**	TC / ARQC / AAC
9F27	**Cryptogram Info**	тип криптограма

TERMINAL DATA

9F33	**Terminal Capabilities**	какво поддържа
9F1A	**Country Code**	код на държавата
9F02	**Amount Authorized**	сума
9F37	**Unpredictable Number**	anti-replay random

Relay Attack — архитектурен модел



Защити срещу Relay Attack

1 Distance Bounding

измерване на response time и физически лимит

2 Timing Analysis

latency anomaly спрямо нормален tap

3 Location Verification

съпоставка на терминал, карта и context

Replay и Downgrade атаки

REPLAY ATTACK

1 RECORD
Sniff APDU exchange от легитимна транзакция

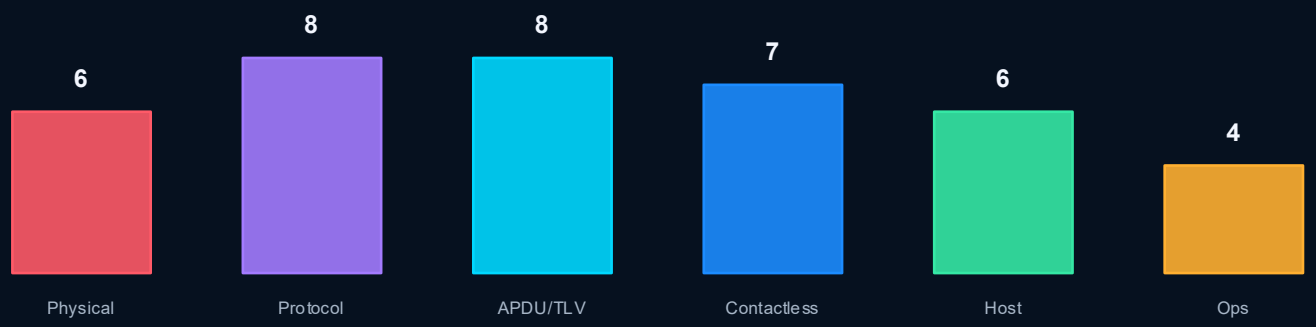
→

2 EMULATE
емулиране на карта със записани responses

→

3 REPLAY
изпращане към нов терминал

EMV защита: Unpredictable Number (9F37) + Application Transaction Counter (ATC) → всяка транзакция е уникална



Други категории

D DOWNGRADE
форсиране на слаб CVM/Auth

S SHIMMING
физически MitM между чип и ICC слот

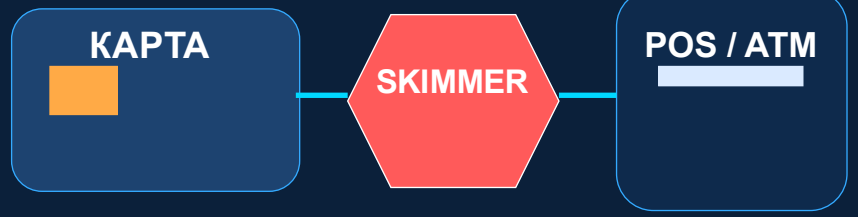
P PRE-PLAY
predictable UN → pre-computed crypto

M MAN-IN-THE-MIDDLE
real-time APDU modification

Skimmers, Deep-Insert Skimmers и sniffing на трафика

Високо ниво: какво представляват, какъв риск носят и какви са основните защити.

1) Какво са skimmer и deep-insert skimmer



Skimmer: неоторизирано устройство, което прихваща данни от магнитна лента или от интерфейса reader ↔ карта.

Deep-insert skimmer: поставя се дълбоко в ATM/POS слота и е по-труден за визуално откриване.

При EMV чип атакуващият често се стреми да наблюдава или препраща обмена, а не просто да „копира чипа“.

Рискът е по-голям при fallback към magnetic stripe и при слаби физически проверки.

2) Как се „sniff-ва“ трафикът между карта и терминал?

Magstripe — Track 1 / Track 2 данни се четат от допълнителна глава или skimmer модул.

ICC / Chip — Възможен е физически interposer / shimmer, който наблюдава APDU обмена между reader-а и чипа.

NFC / Contactless — При близост може да се наблюдава RF обменът или да се проксира комуникацията.

Какво е важно да кажем

Целта е прихващане, наблюдение или препращане на данни — не непременно разбиване на EMV криптографията.

Защити: anti-tamper reader-и, инспекция на слотове, disable/floor-limit на magstripe fallback, EMV/CDA, terminal monitoring и обучение на персонала.

Заключение

EMV Security
по-сигурен от magnetic stripe, но с attack surface на всеки слой

APDU Protocol
основният канал за анализ, MitM и defensive monitoring

Contactless Risk
удобство плюс wireless exposure: relay, timing и proximity risk

Best Defense
CDA + dynamic data + online authorization + monitoring

Благодаря за вниманието!

Здравко Здравков | www.vigilisdefense.com | zzdravkov@vigilisdefense.com