Digital Security

# Критические уязвимости систем эквайринга

Глеб Чербов

Директор департамента аудита Digital Security

# Agenda

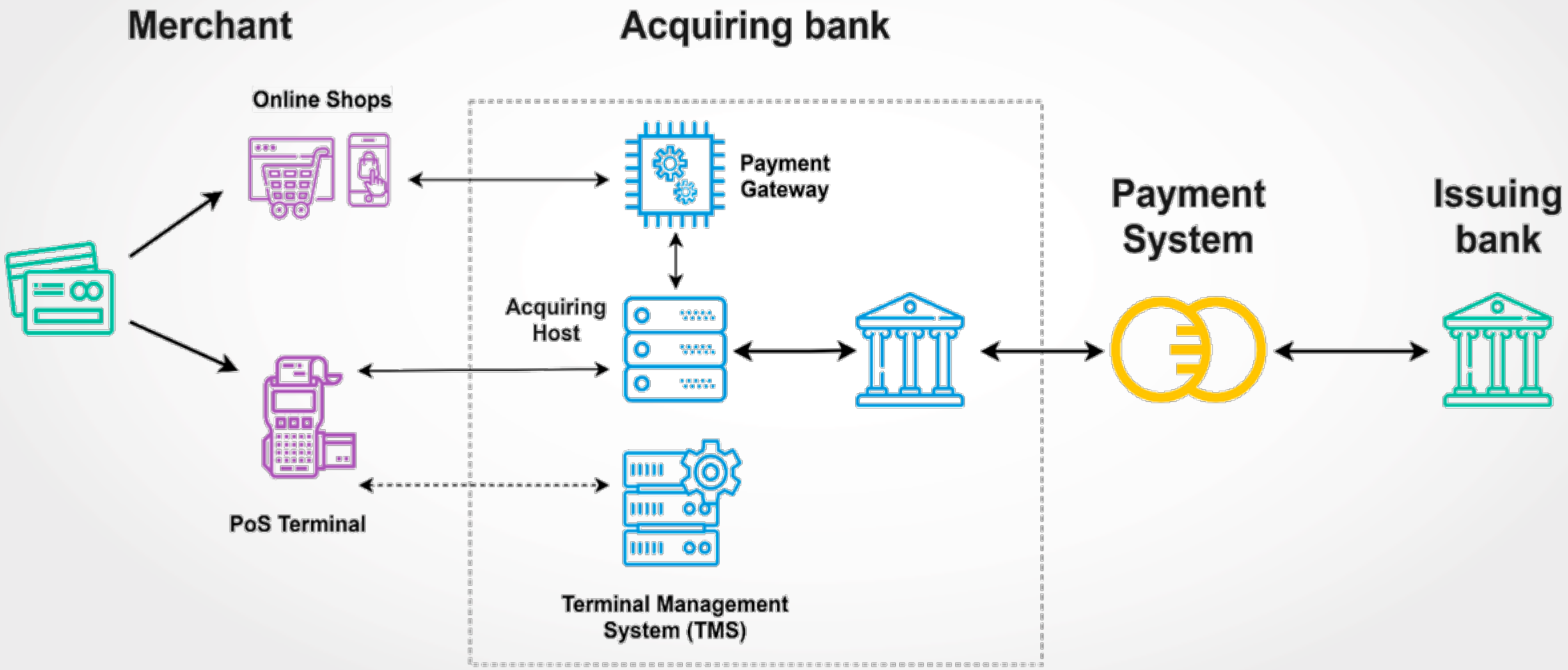
01 Инфраструктура эквайринга

02 Системы управления терминалами (PoS Terminal Management System – TMS)

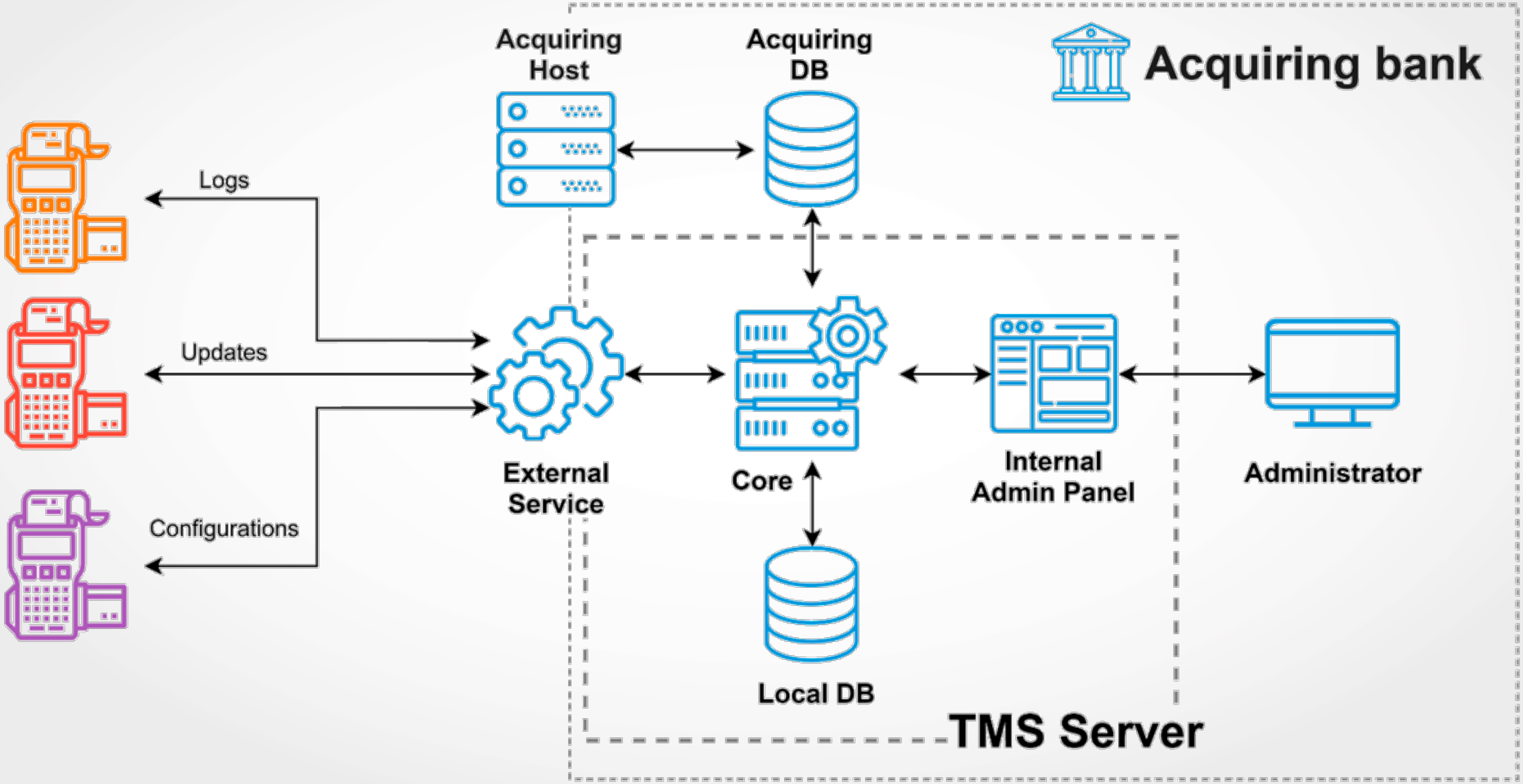
03 **Атаки на инфраструктуру эквайринга**

04 Выводы

# Инфраструктура Эквайринга



# Terminal Management System (TMS)



# TMS

## 3 кейса: различные реализации TMS

| Вендор | Чтение файлов | Запись файлов | SQL injection | Server Side Request Forgery | Исполнение произвольного кода |
|---|---|---|---|---|---|
| Alpha | + | | + | | + |
| Bravo | + | + | | + | + |
| Charlie | + | + | | | + |

Возможность некорректной конфигурации TLS – Alpha, Bravo, Charlie
Возможность компрометации сервера – Alpha, Bravo, Charlie

# TMS

## Ищем IP адрес TMS сервера

Отыскать IP адрес TMS сервера довольно сложно. Протоколы проприетарные, но:

> Сканировать AS банка, и обратить внимание на нестандартные TCP порты

> С помощью google dorks можно поискать специальную PDF/DOCX инструкцию на доменах банка для конфигурации PoS-терминалов

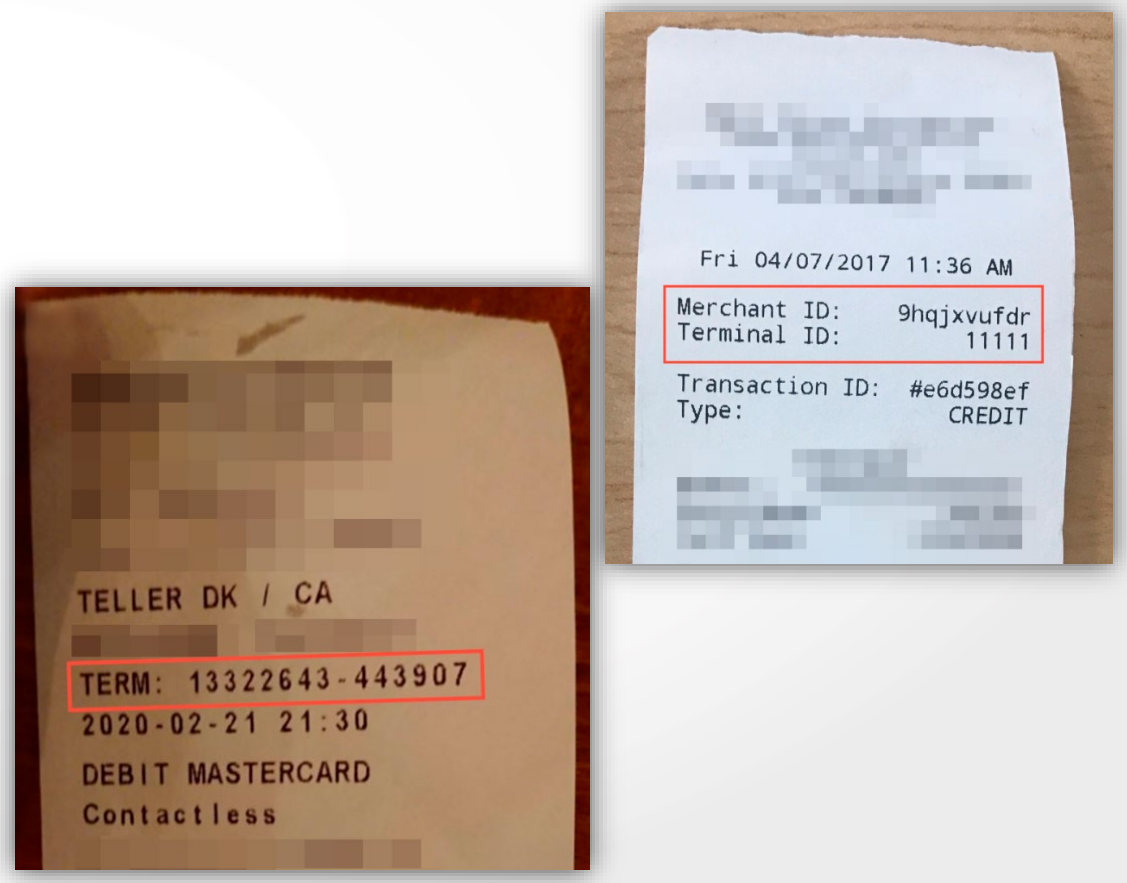
# TMS

## Terminal ID

Для эксплуатации TMS Vendor Bravo и Vendor Charlie, необходимо знать ID терминала.

Но как его узнать?

- ID терминала часто печатается на чеке
- Поискать фото реального человека в Google
- Bruteforce!



# Attack #1

## Атака на внутреннюю инфраструктуру

> TMS сервер обычно расположен в важном сетевом сегменте
> TMS сервер связан с другими эквайринг-системами
> В TMS сервере может быть админка с аутентификацией через LDAP
> TMS сервер часто развернут на Windows, что позволяет быстрее развить атаку на AD

TMS может стать входной точкой в банк для хакеров

# Attack #2

## Подделка транзакций

Для успешной атаки, нужно знать:

> ID терминала

> Физическое расположение PoS-терминалов

> Возможность изменять конфигурацию PoS-терминала (Взломав TMS или с помощью MiTM на PoS-терминал)

# Attack #2

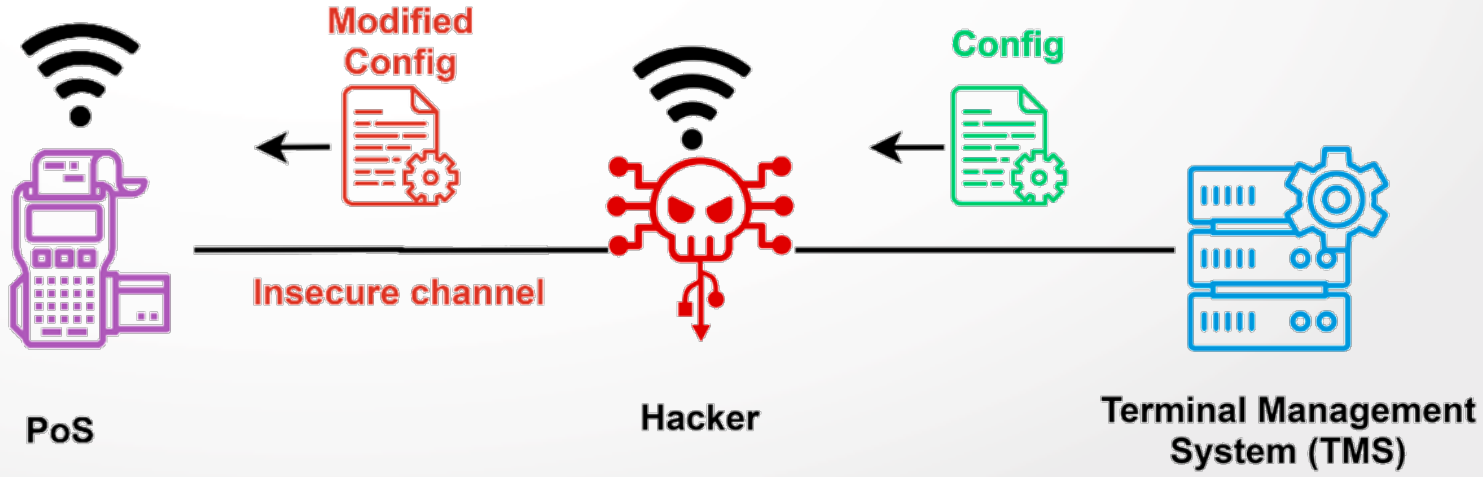
## Подделка транзакций

Шаг 1

> Получить контроль над TMS или осуществить MiTM атаку на POS

> Изменить конфигурацию для PoS-терминала:

- Изменить IP адрес Acquiring Host
- Включить поддержку Technical Fallback / MagStripe / Contactless
- Отключить проверку MAC



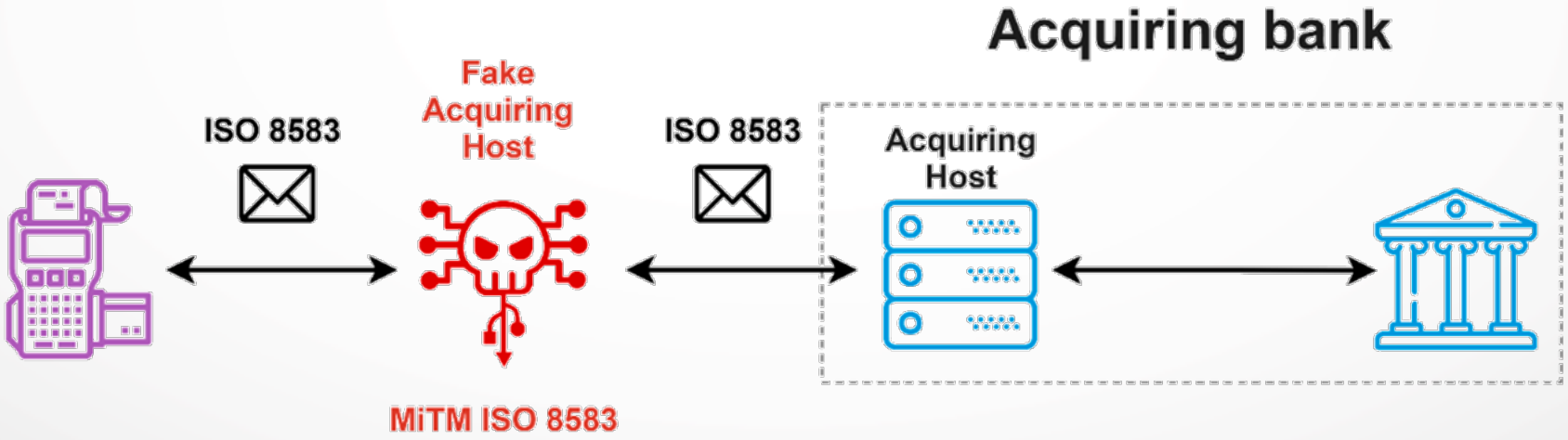
# Attack #2

## Подделка транзакций

Шаг 2

> Развернуть свой Acquiring Host, а точнее эмуляцию (примерно ~22 строчки на Python)

> Проксировать соединение между PoS и реальным Acquiring Host



# Attack #2

## Подделка транзакций

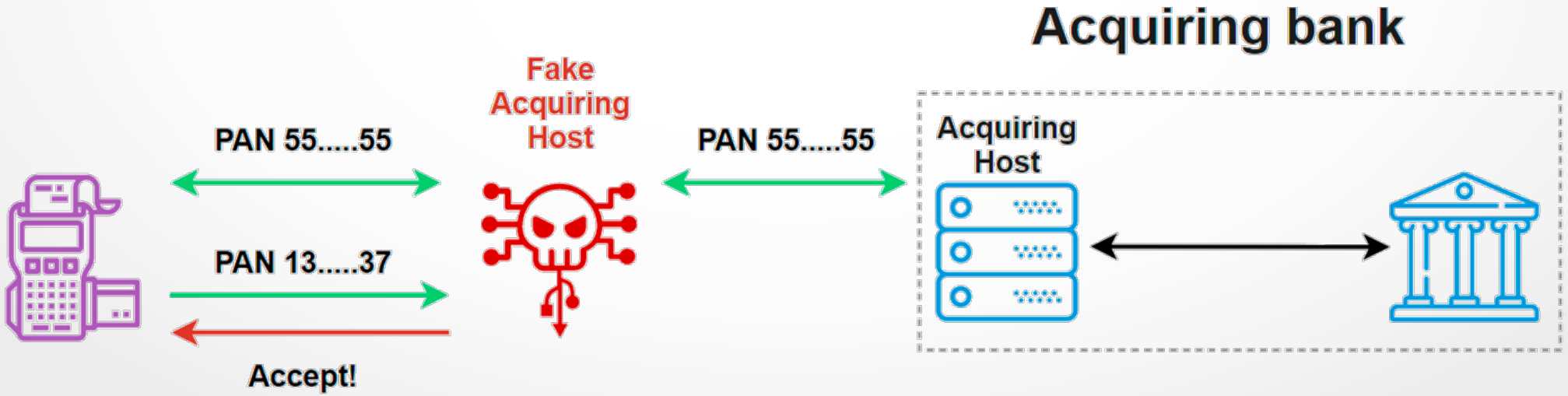
Шаг 3 – шоппинг!

> Отправляемся в магазин, где расположен PoS-терминал

> Проводим транзакцию через Technical Fallback или MagStripe или Contactless MChip

> На нашем Fake Acquiring Host отправляем поддельное подтверждение транзакции

> Забираем покупку!



# Future Attacks

## Атакуем транзакции по Chip

Вся безопасность строится на PKI и CA сертификате, хранящемся в PoS терминале.

PoS терминал проверяет сертификат карты => подписанный сертификатом банка => подписанный CA сертификатом платежной системы.

Но что если мы можем подменить CA сертификаты платёжных систем на PoS-терминале?

```
<CA_Key>
        <CA_Key RID="A000000004" checksum="5ADDF21D09278661141179CBEFF272EA384B13BB"
expireDate="291231" exponent="00000003" hashalg="01" index="03"
keyModulus="C2490747FE17EB0584C88D47B1602704150ADC88C5B998BD59CE043EDEBF0FFEE3093AC7956AD3B6AD4554C6DE1
9A178D6DA295BE15D5220645E3C8131666FA4BE5B84FE131EA44B039307638B9E74A8C42564F892A64DF1CB15712B736E3374F1
BBB6819371602D8970E97B900793C7C2A89A4A1649A59BE680574DD0B60145" sigalg="01"/>
        <CA_Key RID="A000000004" checksum="EBFA0D5D06D8CE702DA3EAE890701D45E274C845"
expireDate="291231" exponent="00000003" hashalg="01" index="05"
keyModulus="B8048ABC30C90D976336543E3FD7091C8FE4800DF820ED55E7E94813ED00555B573FECA3D84AF6131A651D66CFF
4284FB13B635EDD0EE40176D8BF04B7FD1C7BACF9AC7327DFAA8AA72D10DB3B8E70B2DDD811CB4196525EA386ACC33C0D9D4575
916469C4E4F53E8E1C912CC618CB22DDE7C3568E90022E6BBA770202E4522A2DD623D180E215BD1D1507FE3DC90CA310D27B3EF
CCD8F83DE3052CAD1E48938C68D095AAC91B5F37E28BB49EC7ED597" sigalg="01"/>
        <CA_Key RID="A000000003" checksum="D34A6A776011C7E7CE3AEC5F03AD2F8CFC5503CC"
expireDate="291231" exponent="00000003" hashalg="01" index="01"
keyModulus="C696034213D7D8546984579D1D0F0EA519CFF8DEFFC429354CF3A871A6F7183F1228DA5C7470C055387100CB935
A712C4E2864DF5D64BA93FE7E63E71F25B1E5F5298575EBE1C63AA617706917911DC2A75AC28B251C7EF40F2365912490B939BC
A2124A30A28F54402C34AECA331AB67E1E79B285DD5771B5D9FF79EA630B75" sigalg="01"/>
    </CA_Key>
```

# Future Attacks

## Атакуем транзакции по Chip

Что можно сделать:

- Создаем свой CA и изменяем CA сертификат в PoS-терминале
- Делаем специальную карту, эмитирующую реальную карту, но с сертификатом, подписанным нашим CA
- Шоппинг!

# Выводы

Похоже, безопасность эквайринг-инфраструктуры довольно сильно обделена вниманием. Возможно, сказывается отсутствие публичной информации о безопасности таких систем.

Исследуя несколько таких систем, мы нашли схожие критичные уязвимости и проблемы с конфигурацией, которые позволяют полностью скомпрометировать инфраструктуру банка эквайера.

Все эти уязвимости можно эксплуатировать удаленно, достаточно лишь вставить карту в PoS-терминал.

# Спасибо за внимание!

Это все, что мы успели рассказать вам за 15 минут. Однако далеко не все, что могли бы рассказать. Поэтому предлагаем посмотреть видеодоклад со всеми техническими деталями **здесь**.

Наши эксперты готовы проверить безопасность вашей инфраструктуры эквайринга, выявить уязвимости и повысить защищенность информационной системы банка.

О том, как мы это сделаем, подробно написано **здесь**.

inbox@dsec.ru +7 (495) 223-07-86

## Свяжитесь с нами