Everything you always wanted to know about payment terminals * (*But were afraid to ask)

Pr Jean-Jacques Quisquater

David Samyde

Cardis 2023

Tuesday November 14th 2023

Apologies for remote presentation

- Wanted to be present at Cardis
- Planed delayed and would not have made it in time at connection
- Sincere apologies, but we shall adapt
- Apologies to any authors who are not mentioned for their contribution (picture, text, …) this is not intentional.
- This subject is very dense and could give a 12H talk
  - So we shall grab the most relevant parts for a very technical audience

Explanation about the title of this tutorial

Everything You Always Wanted to Know About Sex (*But Were Afraid to Ask)* (film)

For the book, see Everything You Always Wanted to Know About Sex (*But Were Afraid to Ask) (book).*

This article **needs additional citations for verification**. Please help improve this article by adding citations to reliable sources. Unsourced material may be challenged and removed.

Find sources: "Everything You Always Wanted to Know About Sex* (*But Were Afraid to Ask)" film – news · newspapers · books · scholar · JSTOR *(February 2015)* *(Learn how and when to remove this template message)*

Everything You Always Wanted to Know About Sex* (*But Were Afraid to Ask) is a 1972 American sex comedy anthology film directed by Woody Allen. It consists of a series of short sequences loosely inspired by David Reuben's 1969 book of the same name.

The film was an early success for Woody Allen, grossing over $18 million in North America alone against a $2 million budget, making it the 10th highest-grossing film of 1972.

- Payment terminals are everywhere nowadays
  - Everyone in this room has already used one multiple times.
  - How are they built ? What are the concepts behind them?
- Redde Wikipedia quae sunt Wikipedia (next few slides, until slide 15)

According to Wikipedia

Payment terminals … on the other side of the card

- Name : Payment terminal, Point of sale (P.O.S) terminal, credit card machine, PIN pad, EFTPOS Terminal, PDQ (Process Data Quickly) terminal
- Function : Device that interfaces with payments cards to make electronic funds transfers
- General architecture : Contains a secure keypad for entering PIN, a screen, a means of capturing information from payments cards and a network connection to access a payment network for authorization
- Function : A payment terminal allows a merchant to capture credit card and debit card information and to transmit this data to the merchant services provider or bank for authorization. Eventually the funds are transfered to the merchant.
- How: The terminal allows the merchant or their client to swipe, insert or hold a card near the device (NFC) to capture the information. Payment terminals are often connected to point of sale systems so that payment amounts and confirmation of payment can be transferred automatically to the merchant's retail management system.
- Stand alone mode : Terminals can also be used in stand alone mode, where the merchant keys the amount into the terminal before the customer present their card and PIN.
- Transmission : Majority of card terminals today transmit data over cellular network connections and Wifi. Legacy terminals communicate over standard telephone lines or Ethernet connections. Some also have the ability to cache transactional data to be transmitted to the gateway processor when a connection becomes available.
- Real time : Major drawback to this is that immediate authorization is not available at the time the card was processed, which can subsequently result in failed payments. Wireless terminals transmit card data using Bluetooth, Wifi, cellular or even satellite networks in remotes areas and onboard planes.

History of evolution

- Prior to the development of payment terminals, merchants would capture card information manually using ZipZap machines and carbon paper copies.
- Development of payment terminals was led by the advantage of efficiency by decreased transaction processing times and immediate authorization of payments.
- Terminals provide end to end card data encryption and auditing functions.
- There have been some cases of POS pin pad malware. There have also been incidence of skimming at card terminals and this led to the move away from using the magnetic strip to instead capturing information using EMV standards.

Old and recent payment terminals

Verifone

- Point of sale terminals emerged in 1979
- Visa introduced a bulky electronic data capturing terminal which was the first payment terminal.
- Same year magnetic stripes were added to credit cards for the first time. This allowed card information to be captured electronically and led to the development of payment terminals.
- One of the first companies to produce dedicated payment terminals was Verifone (Verification over the phone of credit card information). It started in 1981 in Hawaii as a small electronic company. In 1983 they introduced the ZON terminal series, which would become the standard for modern payment terminals.

Hypercom

- Hungarian-born George Wallner in Sydney, Australia, founded rival Hypercom in 1978.
- In 1982 started producing dedicated payment terminals. It went on to dominate the Australia pacific region.
- The company signed a deal with American Express to provide its terminals to them in the US.
- To consolidate the deal, Hypercom moved its head office from Australia to Arizona. It then faced head-to-head competition with Verifone on its home market.
- In 2010 Verifone acquired Hypercom.

Lipman electronic engineering

- In 1994, Lipman Electronic Engineering Ltd was established in Israel.
- Lipman manufactured the Nurit line of processing terminals.
- Lipman targeted an untapped niche in the processing industry. While, Lipman held about a 10% share in wired credit card terminals, they were the undisputed leader, with more than 95% share in wireless processing terminals in the late 1990s.
- Verifone acquired Lipman in 2006.

Ingenico

- In 1980, Jean-Jacques Poutrel and Michel Malhouitre established Ingenico in France and developed their first payment terminal in 1984.
- Its Barcelona-based R&D unit would lead the development of payment terminals for the next decade.
- Ingenico, through a number of acquisitions, would dominate the European market for payment terminals for a number of years.
- Ingenico acquired French based Bull and UK based De La Rue payment terminal activity as well as German Epos in 2001.

- Refer to : https://www.radiofrance.fr/franceinter/podcasts/rendez-vous-avec-x/l-affaire-gemplus-5987400 (Perfect case of economic spying and protection of crypto knowledge and crypto geeks by using payment terminals)

Smartcards vs magnetic stripe

- Information was captured from the magnetic strip on the back of the card, by swiping the card through the terminal.

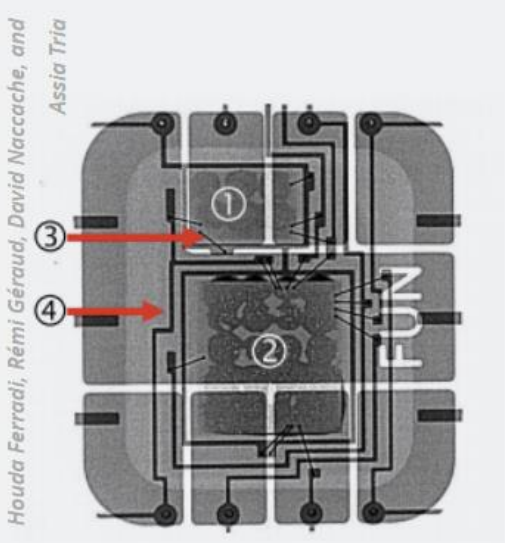
- In the late 1990s, this started to be replaced by smart cards. (Refer to https://arstechnica.com/tech-policy/2015/10/how-a-criminal-ring-defeated-the-secure-chip-and-pin-credit-cards/)

- Added security and required the card to be inserted into the credit card terminal.
- In early 2000s contactless payment systems were introduced and the payment terminals were updated to include the ability to read these cards using near field communication (NFC) technology.

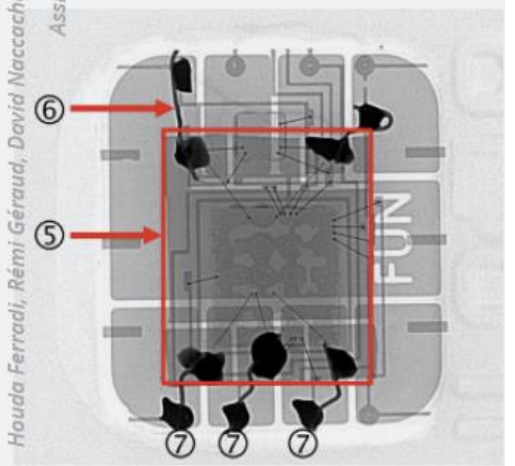
Man-in-the-Middle Attacks on EMV: What Happens When You Forget About the User

Steven Murdoch

work with Saar Drimer, Mike Bond, Omar Choudary, Ross Anderson



FUN card X-ray analysis. (1) External memory (AT24C64); (2) Microcontroller (AT90S8515A); (3) Connection wires; (4) Connection grid.



"Forgery X-ray analysis. (5) Stolen card's module; (6) Connection wires added by the fraudster; (7) Weldings by the fraudster (only three are pointed out here)."

Typical features according to Wikipedia

- Key entry (for customers not present mail and telephone order)
- Tips and/or gratuities
- Refunds and adjustments
- Settlement (including automatic)
- Pre-authorisation
- Payments using NFC enabled devices (Host Card Emulation mode)
- Remote initialisation and software update
- Point of sale (POS) integration
- Multi-merchant capabilities
- PIN authorization by the customer
- Surcharge function
- Secure password operation
- Additional PIN pad attachments
- Like automated teller machines, some payment terminals are also equipped with raised tactile buttons and an earphone jack which allow the people challenged with vision to audibly finish the payment process

Major manufacturers

- Ingenico
- Pax technology
- Verifone

- And many Asian manufacturers appeared with time
  - Managed to reduce cost and figured out the secret sauce

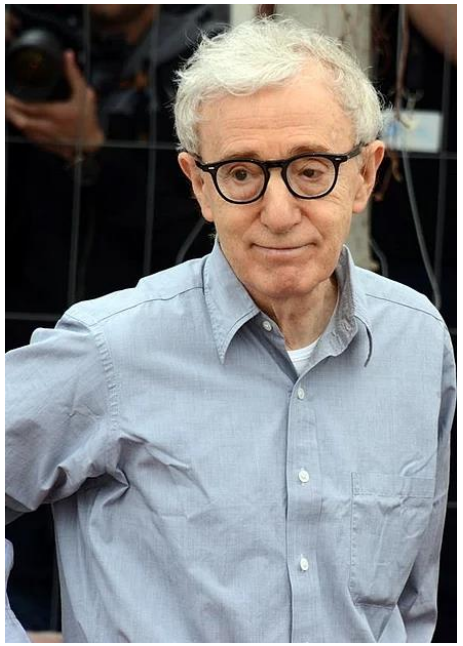
- Some manufacturers even copied/borrowed the PCB mistakes of some competitors ☺
  - Some terminals are almost duplicate of some others …

Evolution of things

- A merchant can replace the functionality of dedicated credit card terminal hardware using a terminal application running on a computer or mobile device such as a smart phone.
- Payment acceptance applications are also called tap on phone or software point of sale.
- They usually work with dedicated hardware readers or not that can transfer magnetic stripe data to the application, while there are also some that also work with smartcards (using technology such as EMV).
- In case the necessary hardware is unavailable, these applications usually support manual entry of the card number and other data.
- In addition, more and more devices are beginning to offer built-in NFC technology to accommodate contactless or mobile phone device payment methods, often without requiring additional external hardware.
- There exist payment processors that offer virtual terminals for processing payments without the card being present (when taking payments over the phone).
- In Asia more mobile payment systems are now based on QR code payments to bypass the need for payment terminals altogether, relying on smartphones and a printed QR code.

Payment Card Industry

7 parts to the referred movie



1. *Do payment terminals work?*
2. *What is PCI?*
3. *Why do some manufacturers have trouble making secure terminals?*
4. *Are mobile based payment transgressive?*
5. *What are attacks against terminals?*
6. *Are the findings of hackers and researchers accurate?*
7. *What happens during a hack?*

Let’s try to answer to all that ☺

History of smartcards

- ~1970 Japan / USA: Arimura, Ellingboe, Halpern, and others independently describe the “portable circuit” aka memory card, and potential applications (electronic payment scheme, unmanned gas station…).
- 1974 France : Moreno using memory chips modifies the form factor and patents the memory card.
- 1976 Germany: Dethloff replaced the memory chip by a microprocessor + memory.
- 1977 France: Ugon replaced the memory chip by a microcontroller + memory.
- …, Palladium, TPM, …
- TEE , Secure Element

A 4-digit code to prove the owner knows something is a natural evolution

Payment industry before 2004

- Each country/card brand/bank/acquirer wrote and enforced their own security standards
- Large variations of what needed to be certified for each organization
- Security of systems (data and hardware) was not well tested
- This meant that there was a high barrier to entry for new companies

Formation of PCI in 2004

PCI Structure and Core Components		
PCI DSS	PCI PTS	PCI PA-DSS
Data **S**ecurity **S**tandard *Protection of card data* • *track data / magnetic stripe* • *CVC / CVV*	**P**IN **T**ransaction **S**ecurity *Protection of PIN data on terminals* • *PIN entry devices* • *Encrypted PIN pads* • *etc.*	**P**ayment **A**pplication **D**ata **S**ecurity **S**tandard *Development of secure payment applications*

Liability shift

- Normally the card-issuer is liable for fraudulent transaction
- Implemented to drive shift to EMV technologies
- The liability for a fraudulent transaction shifts to the merchant if they do not have an EMV (Europay Mastercard Visa) capable terminal

USA and Europe a quick overview

- USA
  - All PIN acceptance terminals must be PCI PTS certified
  - Strong emphasis on PCI DSS compliance
  - Visa, Mastercard, American Express and Discover are implementing a liability shift for POS terminals since October 2015
  - Recently, big breaches in PCI DSS compliant orgs have renewed focus on compliance.

- Europe
  - Coordinated by European Payments Council
  - SEPA – Single Euro Payments Area – Mandatory from 31 March 2014
  - SEPA intends to start assessing payment terminals to a new “OSeC JTEMS” standard – based on Common Criteria.
  - Intended to replace the national standards around the European area
  - Again – PCI DSS compliance is mandated by large issuers.

PCI PTS (PIN Transaction Security)

- 2004
  - Version 1, Version 1.1
- 2005
  - Version 1.3
- 2007
  - Version 2
- 2009
  - Version 3
- 2011
  - Version 3.1
- 2013
  - Version 4
- 2005
  - Version 1.3
- 2007
  - Version 2
- 2009
  - Version 3
- 2011
  - Version 3.1
- 2018
  - Version 5
- 20202
  - Version 6

Former PCI modules

Module 1 **Core Requirements**

- A Core Physical
- B Core Logical
- C Online PIN
- D Offline PIN

Module 2 **Integration Requirements**

- E Integration Tests

Module 3 **Open Protocols**

- F Physical and Logical Interfaces
- G Vulnerability Assessment
- H Vendor Guidance
- I Operational Testing
- J Maintenance

Module 4 Secure Reading and Exchange of Data

- K Account data protection

DTR A1	Tamper-Detection Mechanisms
DTR A2	Independent Security Mechanisms
DTR A3	Robustness Under Changing Environmental and Operational Conditions
DTR A4	Protection of Sensitive Functions or Information
DTR A5	Monitoring During PIN Entry
DTR A6	Determining Keys Analysis
DTR A7	Physical Security of Display Prompts
DTR A8	Visual Observation Deterrents
DTR A9	Magnetic-Stripe Reader
DTR A10	Component Protections against Removal
DTR A11	Audible Tones During PIN Entry

DTR B1	Self-Test
DTR B2	Logical Anomalies
DTR B3	Firmware Certification
DTR B4	Firmware Updates
DTR B4.1	Software Authenticity
DTR B5	Differentiation of Entered PIN
DTR B6	Clearing of Internal Buffers
DTR B7	Protection of Sensitive Services
DTR B8	Sensitive Services Limits
DTR B9	Random Numbers

DTR B10	Exhaustive PIN Determination
DTR B11	Key Management
DTR B12	Encryption Algorithm Test
DTR B13	Encryption or Decryption of Arbitrary Data Within the Device
DTR B14	Clear-Text Key Security
DTR B15	Transaction Controls
DTR B16	Logical Management of Display Prompts
DTR B17	Application Separation
DTR B18	Minimal Configuration
DTR B19	Component Integration Documentation
DTR B20	Security Policy

DTR D1	Penetration Protection
DTR D2	ICC Reader Slot Visibility
DTR D3	ICC Reader Construction (Wires)
DTR D4	PIN Protection During Transmission Between Device and ICC Reader

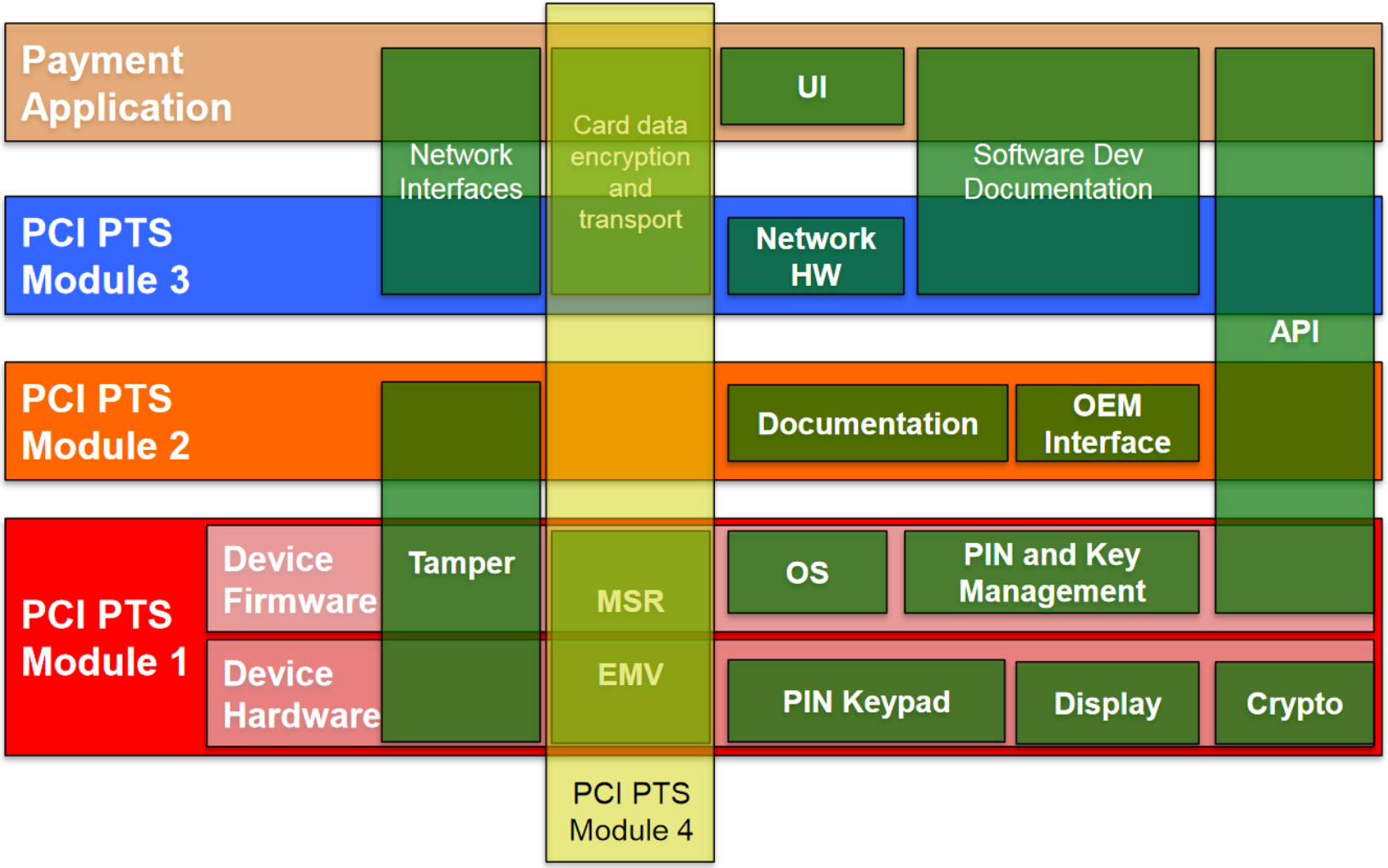
DTR E1	Target of Evaluation (TOE) Identification
DTR E2.1	Integration of PIN Entry Functions
DTR E2.2	Overlay Attack Protection
DTR E3.1	Integration Vulnerabilities
DTR E3.2	Protection Against Card Trapping
DTR E3.3	PIN Entry Interface Segregation
DTR E3.4	User Interface Consistency
DTR E3.5	Control of any Numeric Interface
DTR E4.1	Protection against Removal
DTR E4.2	Unauthorized Removal – Integration Documentation
DTR E4.3	Unauthorized Removal - Embedded Devices

F – Discovery and Definition of Physical and Logical Interfaces	
DTR F1	Identification of Interfaces
G - Vulnerability Assessment	
DTR G1	Vendor Vulnerability Assessment Procedures
DTR G2	Vulnerability Assessment of all Interfaces
DTR G3	Vulnerability Disclosure
H – Vendor Guidance	
DTR H1	Security Guidance for the Interfaces
DTR H2	Default Configuration of the Interfaces
DTR H3	Management Security Guidance

I – Operational Testing	
DTR I1	Use of Secure Protocols
DTR I2	Secure Protocols to Provide Data Confidentiality
DTR I3	Secure Protocols to Provide Data Integrity
DTR I4	Secure Protocols to Provide Server Authentication
DTR I5	Secure Protocols to Provide Exception Handling and Replay Detection
DTR I6	Session Management
J – Maintenance	
DTR J1	Vendor Vulnerability Assessment Procedures
DTR J2	Vulnerability Assessment of all Interfaces
DTR J3	Vulnerability Disclosure
DTR J4	Authentication of Configuration and Software Updates

DTR K1	Account Data Processing
DTR K1.1	Account Data Protection
DTR K1.2	Independent Security Mechanisms
DTR K2	Account Data Protection - Integration
DTR K3	Determining Keys Analysis
DTR K3.1	Public Key Protection
DTR K4	Encryption Mechanisms
DTR K5	Remote Key Distribution
DTR K6	Data Origin Authentication
DTR K7	Unique Secret and Private Keys Per Device
DTR K8	Encryption/Decryption of Arbitrary Data Within a Device
DTR K9	Remote Access

Modules and intersections



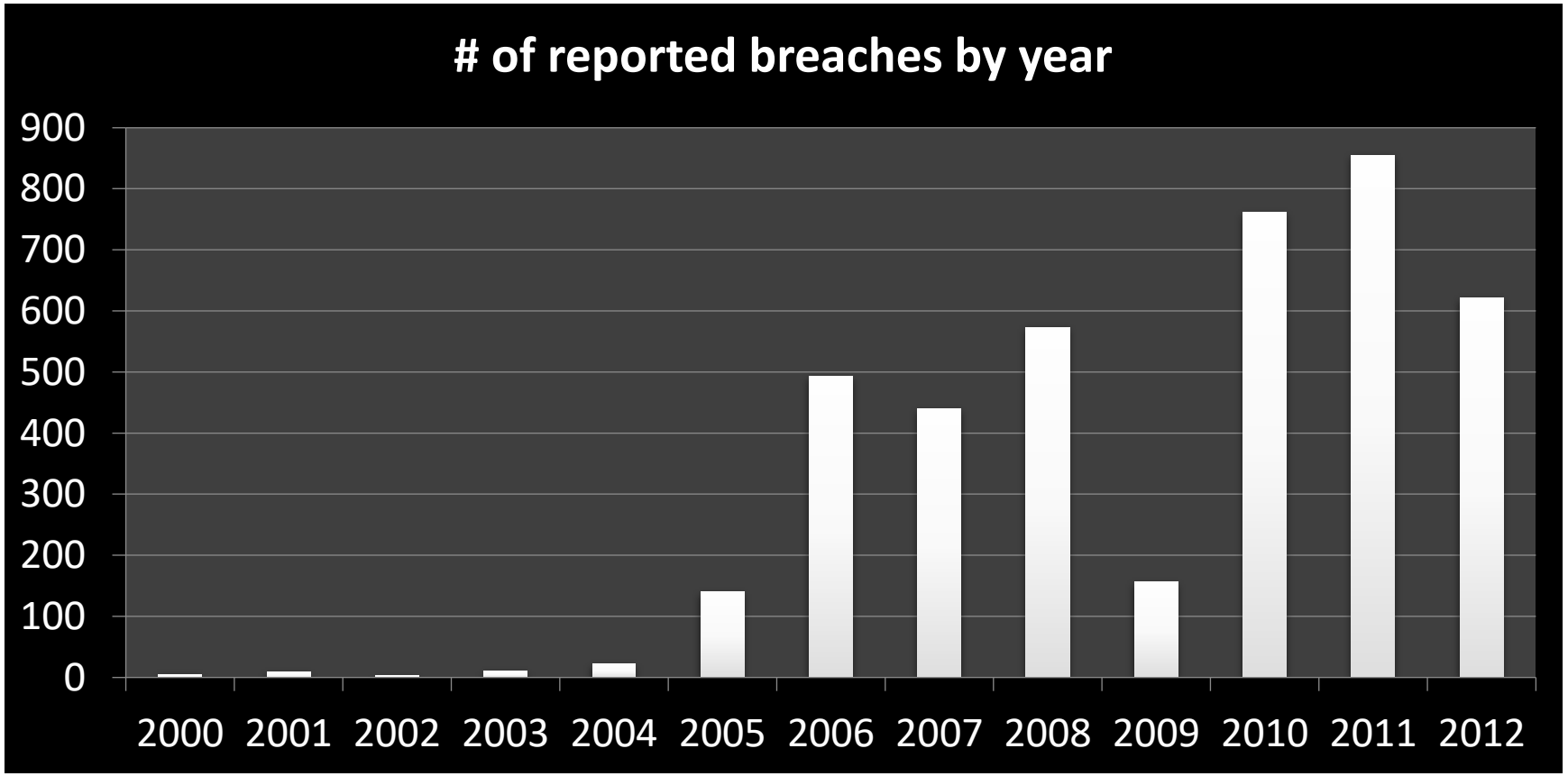
PCI evolution

- Started with hardware security focus
- Increased software focus with time
- Embraced software security best practices with time

- Now focusing on supply chain and more on operations at manufacturing and key loading
- Raised cryptographic level with time
  - ECC mandatory, better check of RNG

- Still some obscurity on some specific points (under sampling not seriously considered in side channel attacks, no answer to Windtalker attack -> https://dl.acm.org/doi/pdf/10.1145/2976749.2978397)

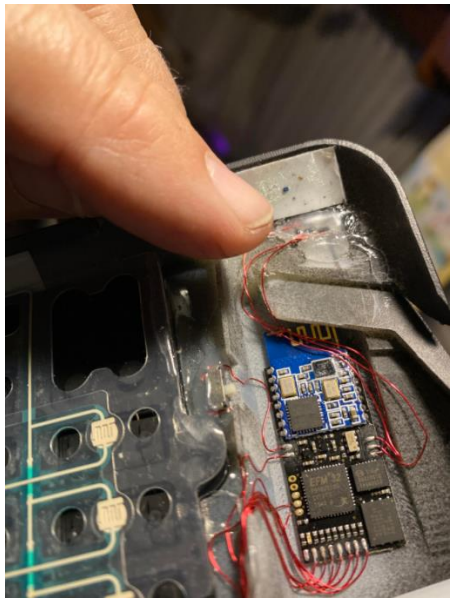
Data breaches



Outside a payment terminal

Simplest attack

- Duplicate payment terminal
  - Make a fake one
  - Like fake ATM at Black Hat https://www.theregister.com/2009/08/03/fake_atm_scam_busted_at_defcom/
- Use an overlay
  - (Refer to : https://krebsonsecurity.com/2021/02/bluetooth-overlay-skimmer-that-blocks-chip/)



Inside a payment terminal

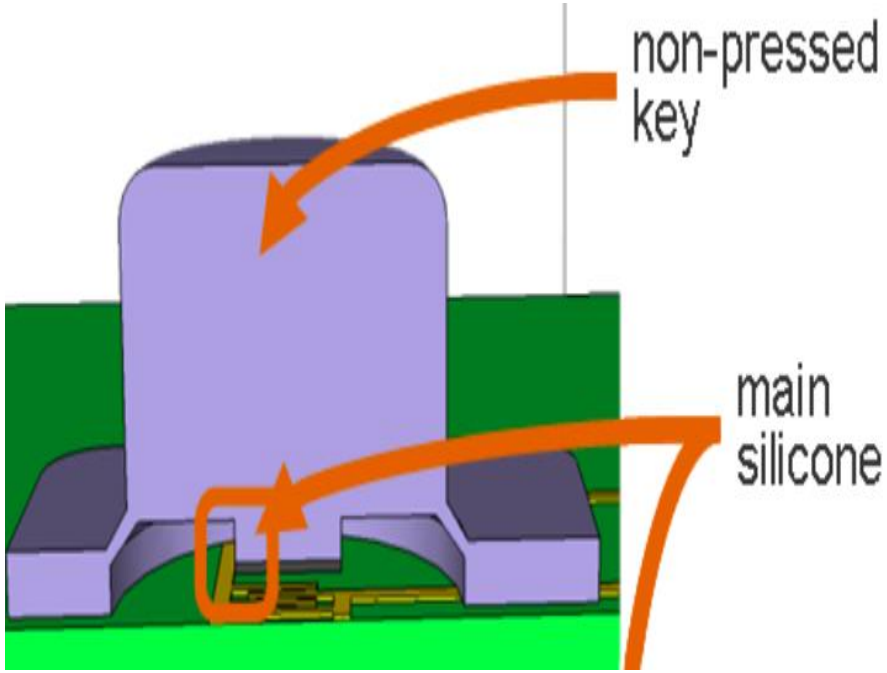
Payment terminal, few properties

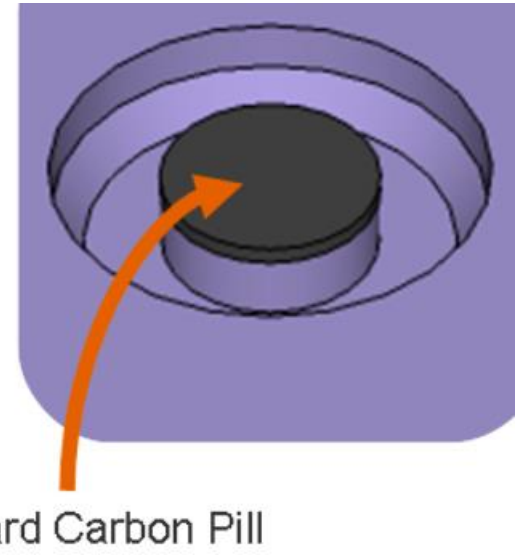
- Contains a secure processor
  - Ability to protect a secret
    - Protection means ability to delete this secret under attack
      - Tamper detection and tamper reaction
      - Presence of a source of energy to take action of erase the secret
    - Ability to detect attacks
      - Detection of opening of the terminal
      - Detection of probing on processor or buses
      - Detection of tampering with existing peripherals
    - Ability to react to prevent attacks
      - Bus encryption
      - Memory encryption
      - Encryption of data at MSR level
- Contains a secure storage
  - Ability to store data securely
    - Usage of cryptography
      - Will rely on secret protected above

Tamper detection

- Secure processor will use random signals routed in a single line to detect:
  - Cut/ Interruption of signal
  - Modification of signal
    - Short circuit
    - Replay
  - Constant value
    - Ground
    - Power
- Several tamper lines are routed inside the terminal
  - Around sensitive areas
  - Inside PCB to avoid abrasion

Tamper switches





Hardware of a payment terminal

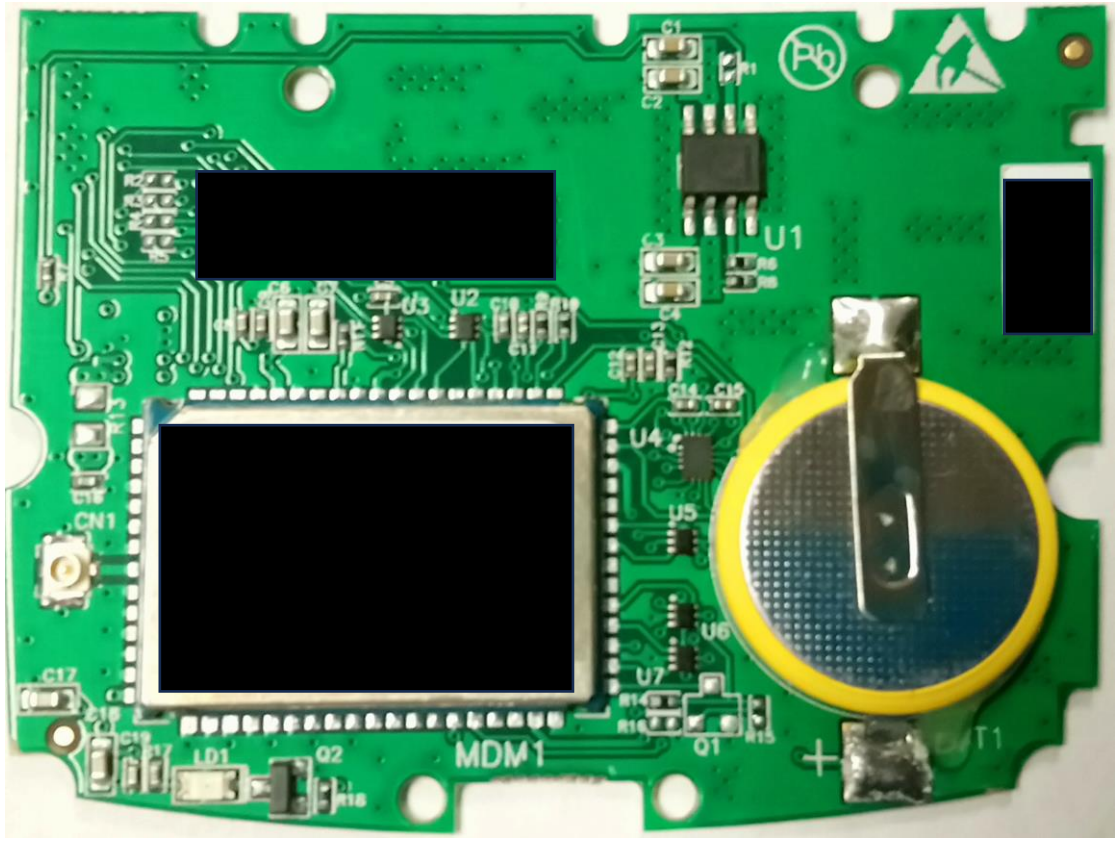
- Uses a cryptographic processor with tamper protections and dedicated key storage.
- Uses a combination of tamper mechanisms to protect sensitive areas
- Uses tamper mechanisms to cover weak areas of the other tamper mechanisms.
- Make sure to protect the whole path of sensitive signals, including vias and connectors used.
- Turn on all the security mechanisms provided by the processor.

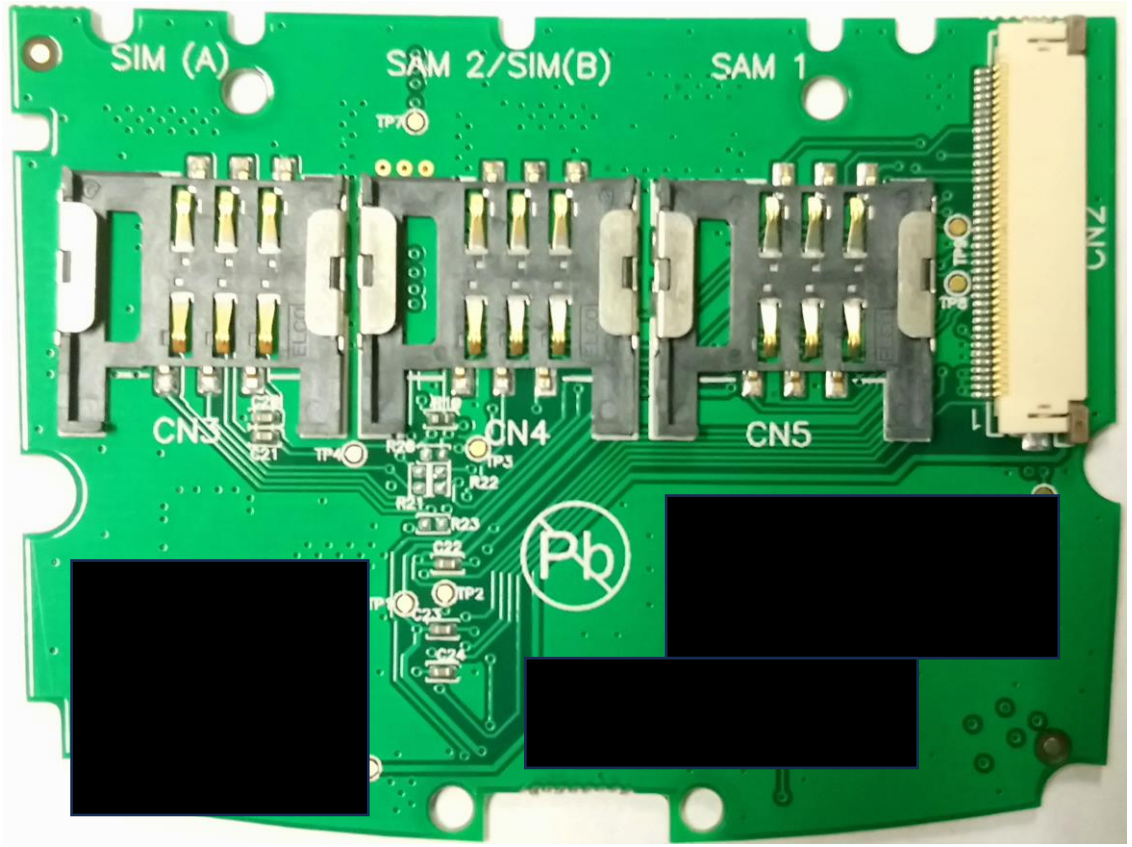
Device front, back and sides

PCB analysis

SIM, SAM, modem, backup battery PCB

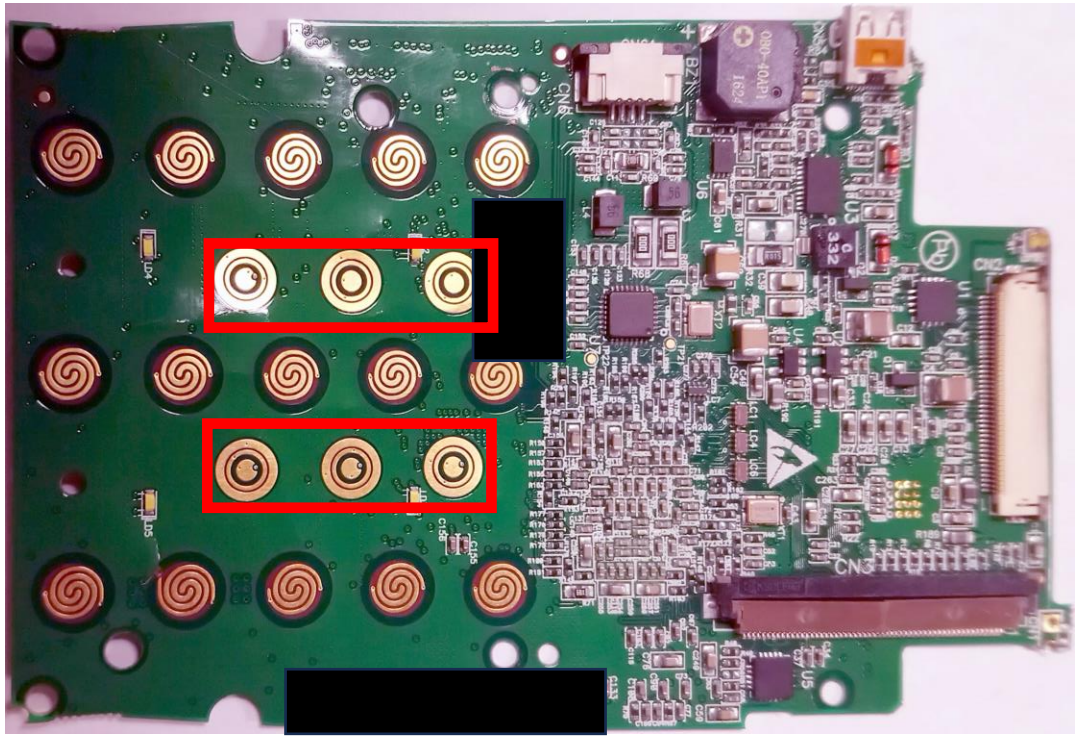
- Battery backing up security processor

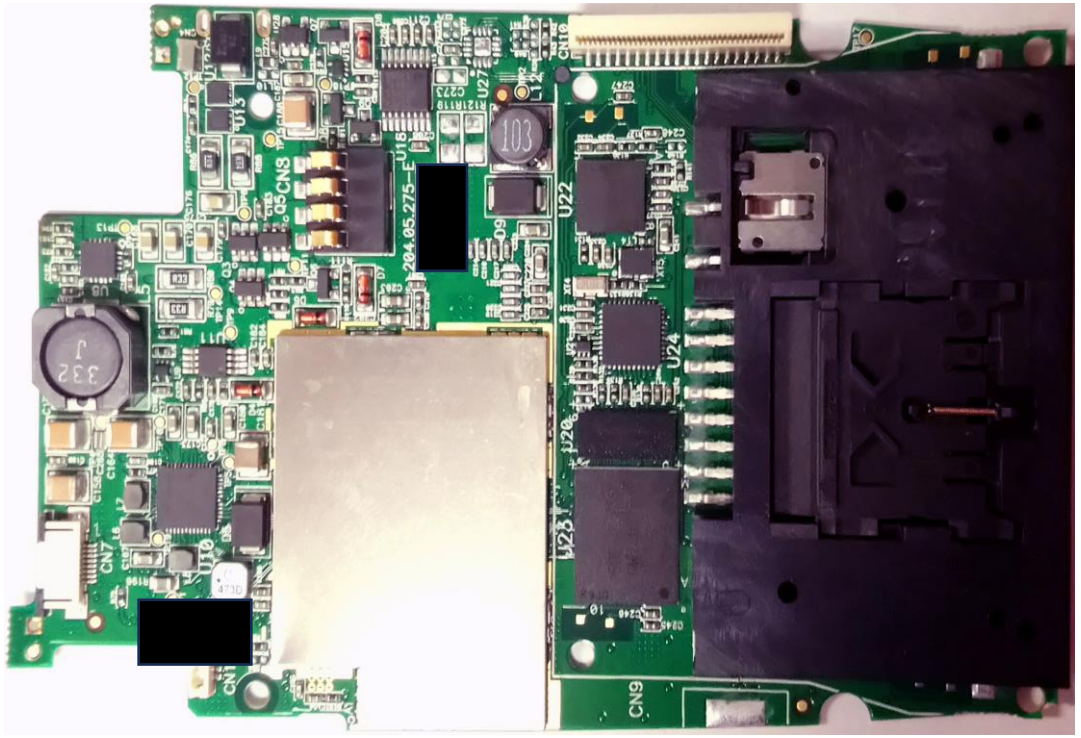




Main board

- Protection of keyboard against separation from casing
- Presence of tamper switches





Presence of internal wiremesh

Keypad analysis

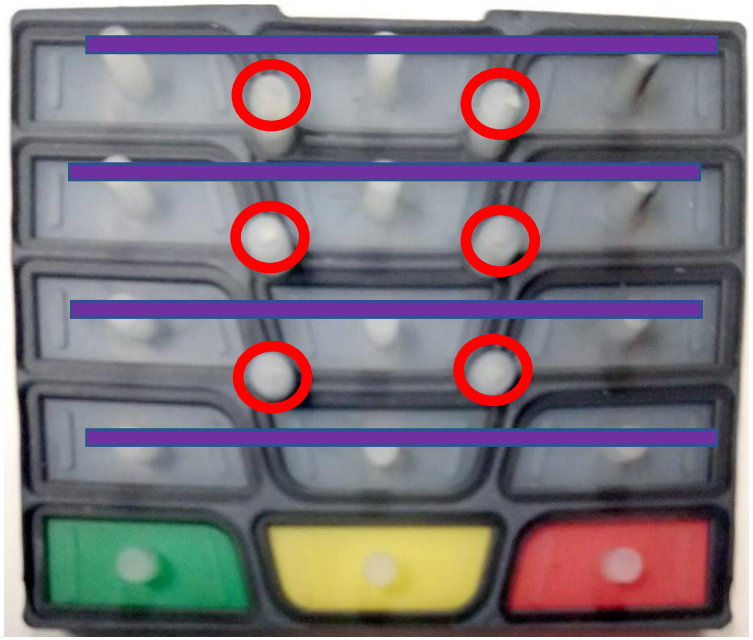
Keypad soft plastic

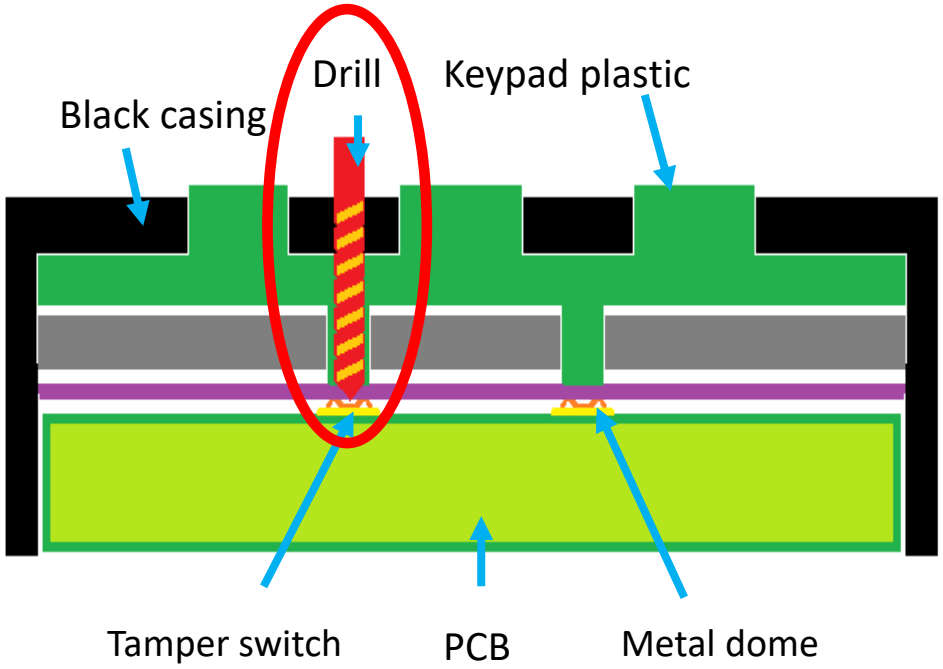
- Keypad is made of soft plastic
- Allows drilling without too much mechanical damage
- Can be drilled through vertical parts that are creating contact pressure on tamper switches under keypad area

The absence of mesh above the tamper switches allow to access the electrical signal directly and to create a bypass between switches

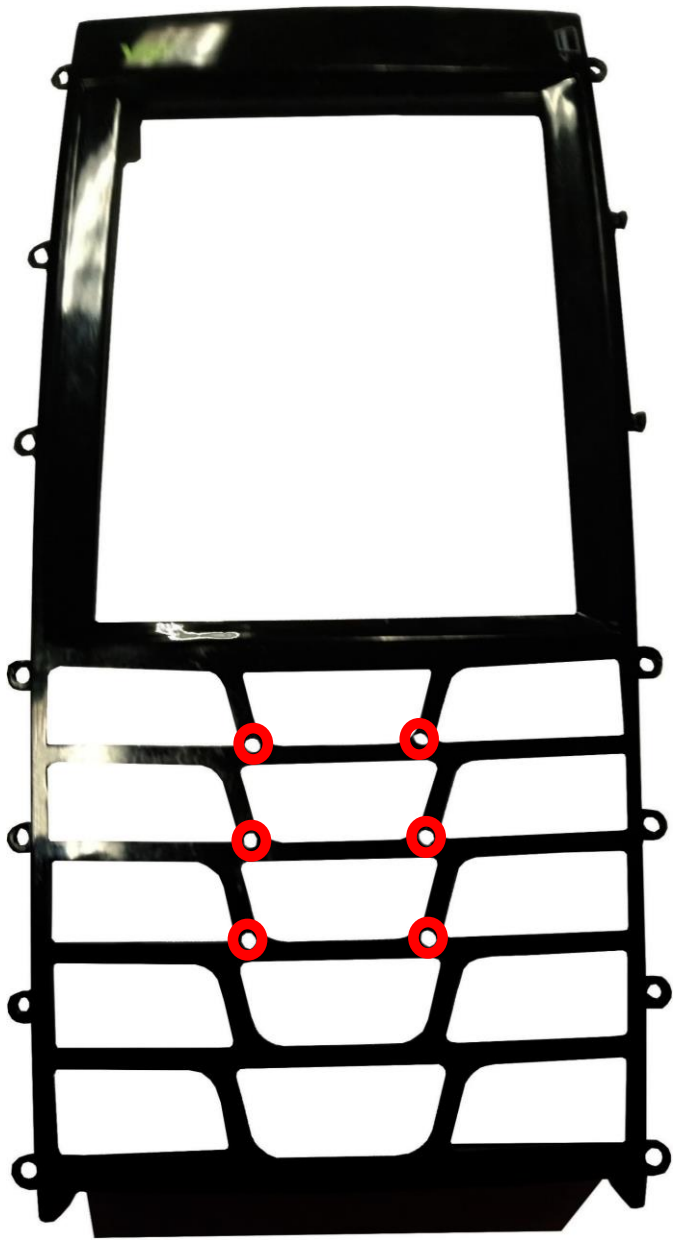
The position of the switches does not prevent the insertion of an underlay (based on rows)

Refer to purple lines below : none crosses a tamper switch

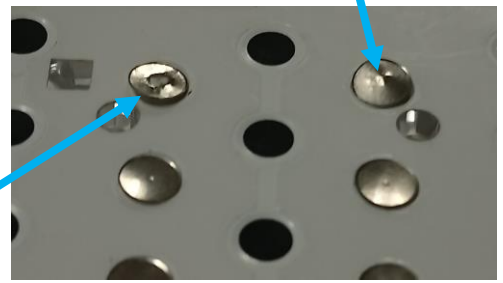




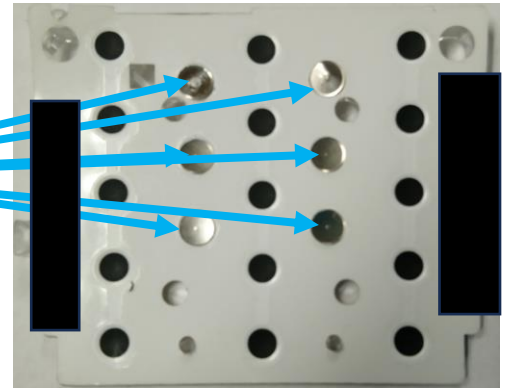
How to bypass keypad security



- Possible to drill upper plastic
- Drill through keypad plastic
  - Refer to previous slide
- Access tamper switch
  - Bump tamper switches using screw driver



  - Drill tamper switch carefully
  - Connect to tamper switch and create bypass to other switches



Yet another way to bypass keypad security

- A side attack is also possible and enables insertion of an underlay
- Attacker will soften the plastic
- Push the plastic away
- Drill the proper window in the side casing
- Remove transparent plastic locally to create a path for an underlay
- Insert underlay
- Connect to appropriate electronic
- Close and repair the device
- Put the device back in production

The device never tampered

Views to main steps to insert an underlay

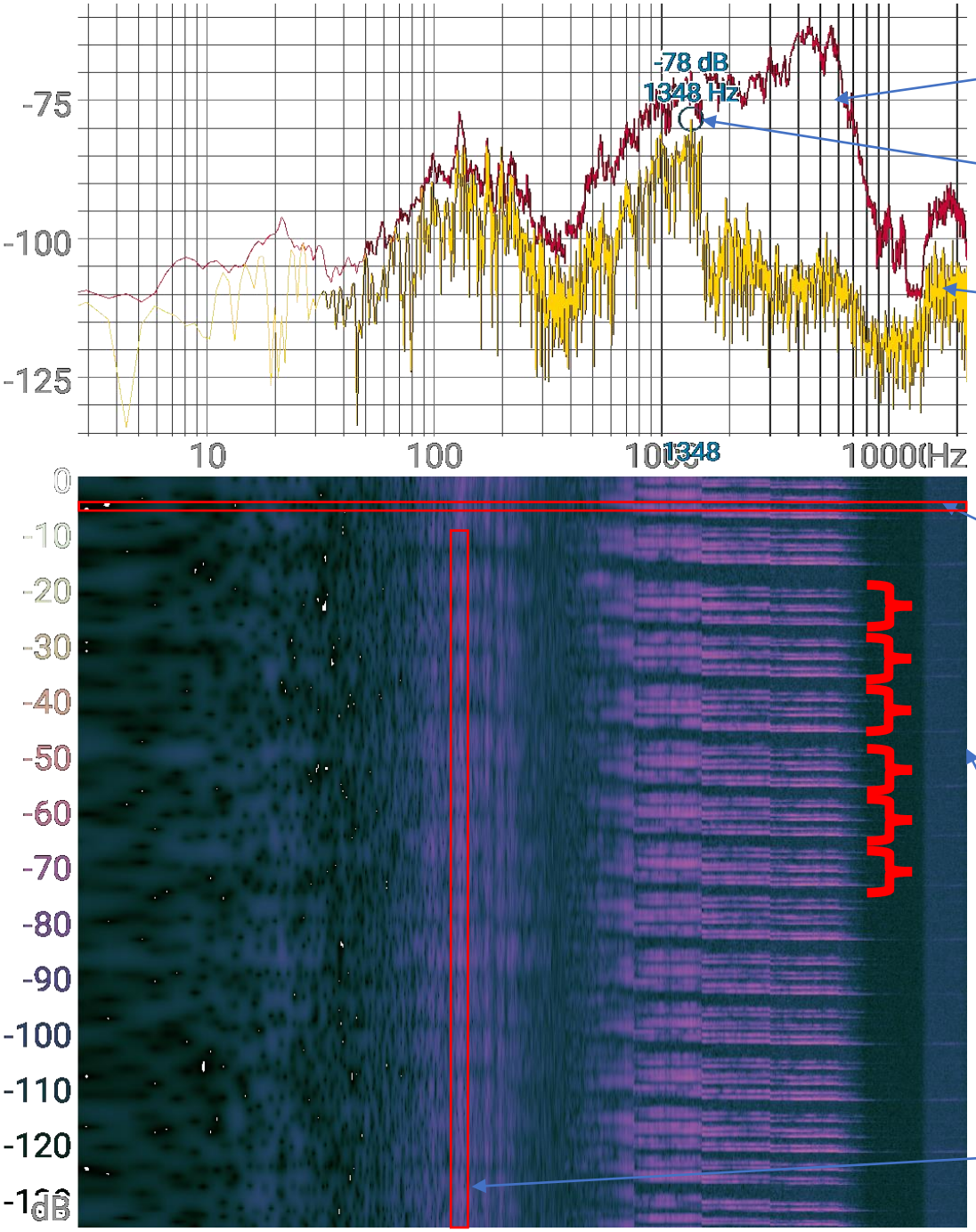
Review of keypad area

- By lack of time we inserted paper size equivalent pieces under the keypad area but did not insert an overlay
- The tamper switches are not well positioned
  - They do not prevent insertion of an underlay on columns and rows
- Absence of side protection using a mesh

Acoustic analysis

Audio and acoustic analysis

- It should not be possible to separate to recover a PIN from the contribution of the keypad at time of PIN entry
- We used our robot to obtain the best acoustic contribution of each key
- We then performed the same tests with a human and averaged the contribution of each key
- Using a frequential representation we can already identify some PINs
- Using non linear signal processing and segmentation the keypad turns out to be too noisy and to leak the PIN
- We also performed some tests using some accelerometers but did not have the time to analyze some very promising results
- The next slide detail what is obtained from a basic measurement and what representation is used



Maxhold : Maximum reached for all frequencies

Highest peak present in signal

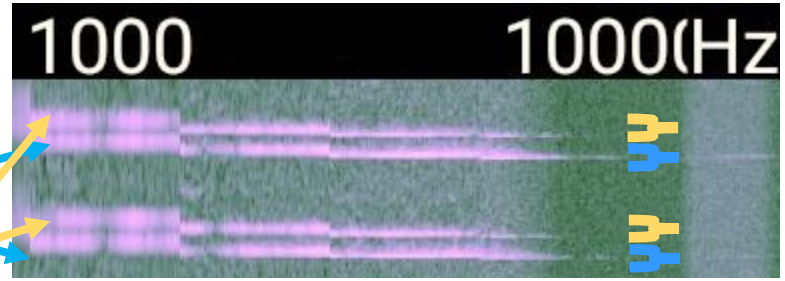
Spectral representation of current signal

Spectrogram : Sliding window in time made with the evolution of the spectral representation of the signal

Repetition of the same key or PIN several times to extract the real contribution and empirically remove some noise

Doubling of 50Hz from power line due to power supply of robot in vicinity (Diodes bridge)

Expectations



- The expectations are simple
  - The audio contribution of each key press will be due to two parts:
    - The metallic dome compression at time of key press will create a ‘click’
    - The metallic dome release at time of finger removal will also create a ‘click’
  - All contributions for all key press should be identical to prevent PIN recovery
    - The next slides shows some differences in the spectrum using colored circles and ellipses
    - Each difference can be used to recognize a key ‘signature’ if this contribution is atypical
- Results

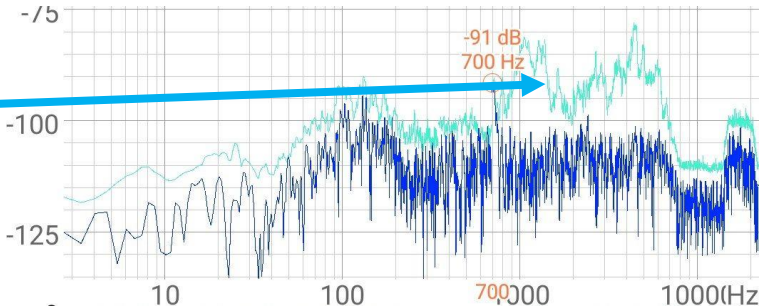
  The contribution of all keys **is not identical**

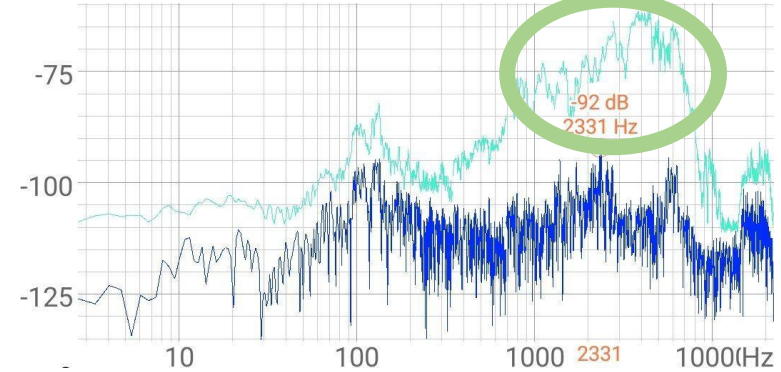
  Key 4 is more noisy than other keys
  - Even a human can find key 4 with a blind test using hear only

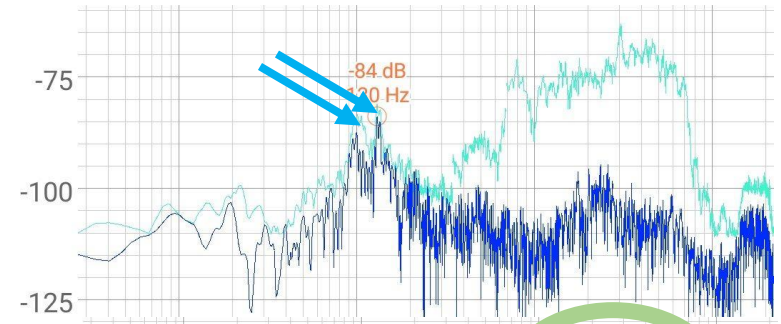
  Key 9 is more silent than other keys

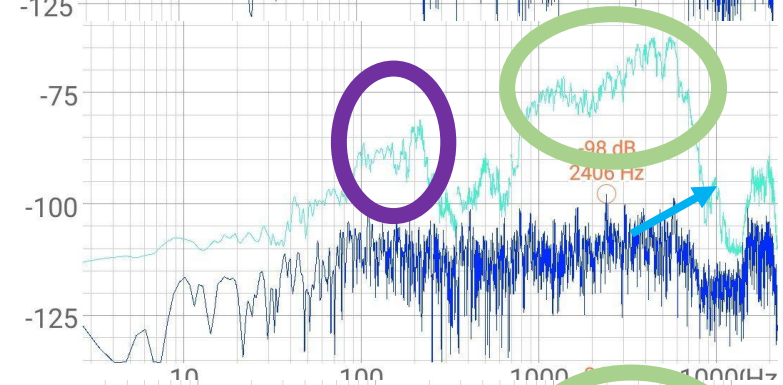
  Key 0 has a particular acoustic signature
  - Due to specific position 4th on row and 2nd column

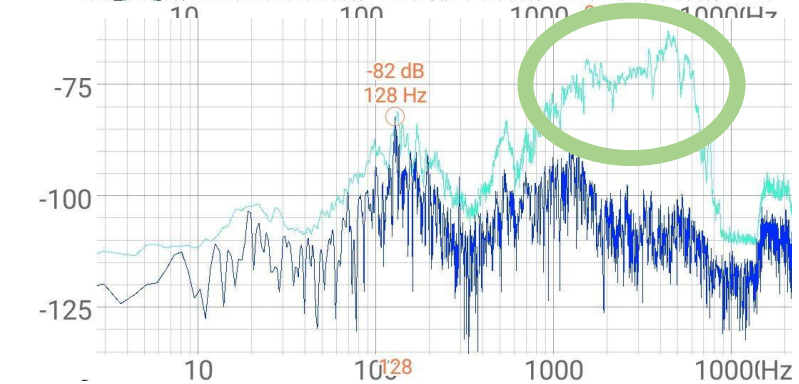
  Key 8 has a high level pitch signature that is almost like key 4 but can be separated
- As a reference we also included the absence of key press and background contribution as a spectral representation but also an average PIN entry
- Please refer to the Maxhold function in light green for each spectrum

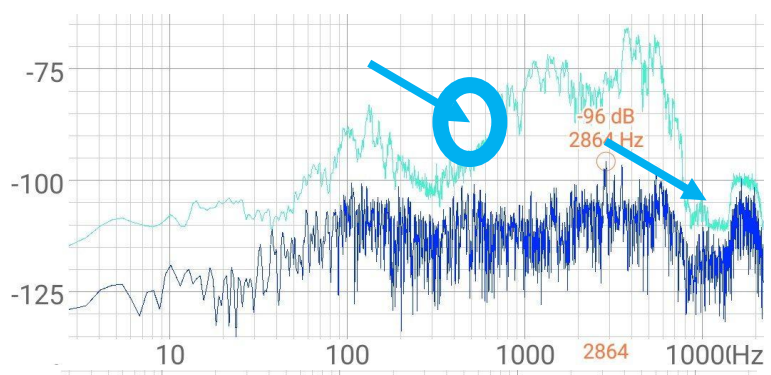


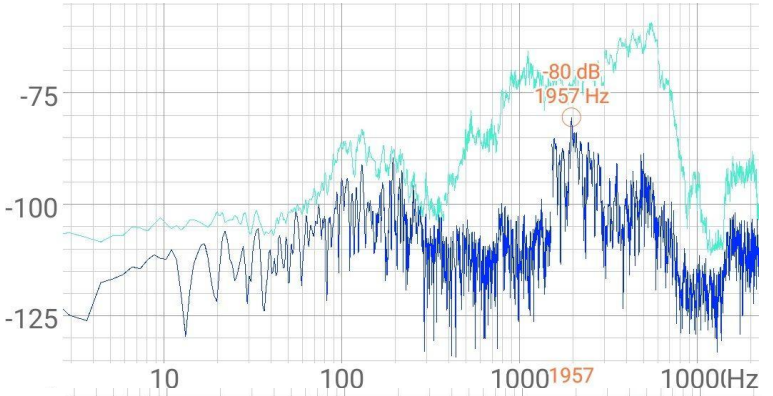

-75
-100
-125
-92 dB
2331 Hz
10
100
1000
2331
1000(Hz

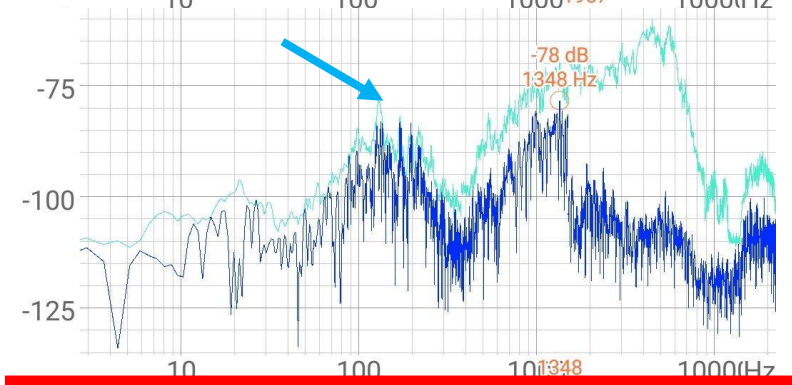

-75
-100
-125
-84 dB
Hz

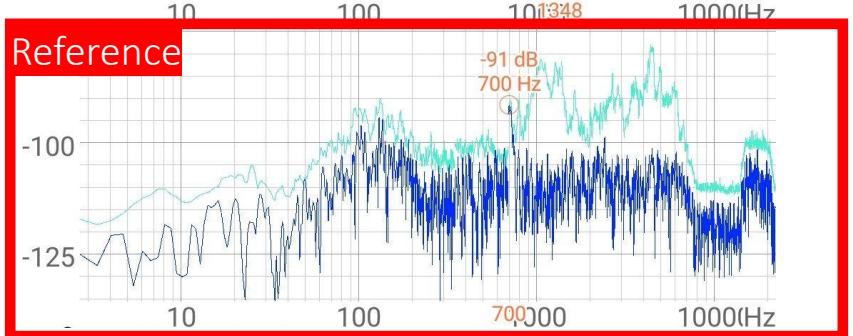

-75
-100
-125
-98 dB
2406 Hz

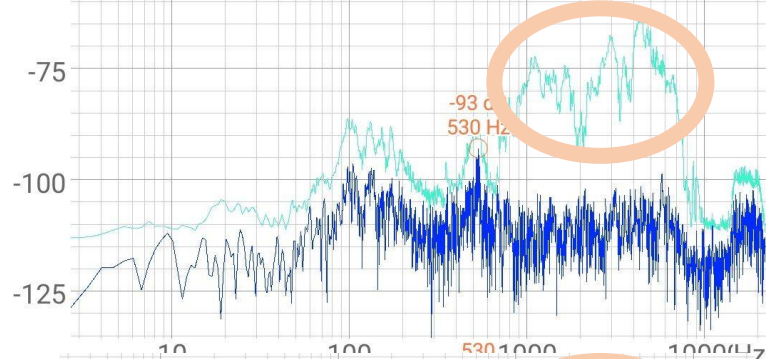

-75
-100
-125
-82 dB
128 Hz
10
128
1000
1000(Hz

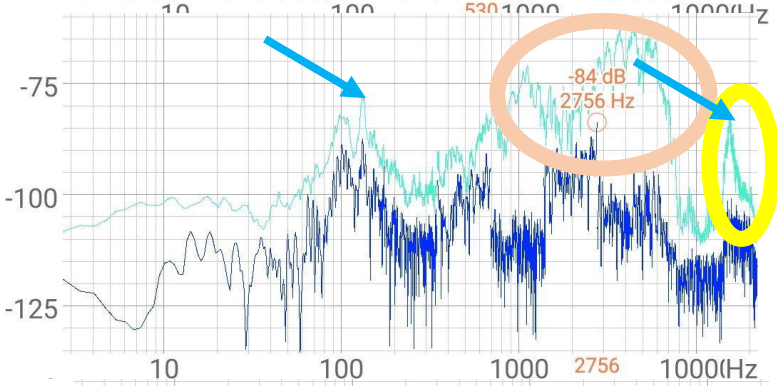

-75
-100
-125
-96 dB
2864 Hz
10
100
1000
2864
1000(Hz

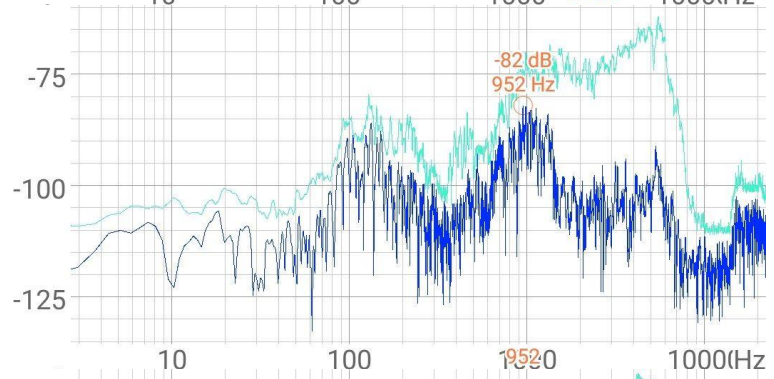

-75
-100
-125
-80 dB
1957 Hz
10
100
1000
1957
1000(Hz

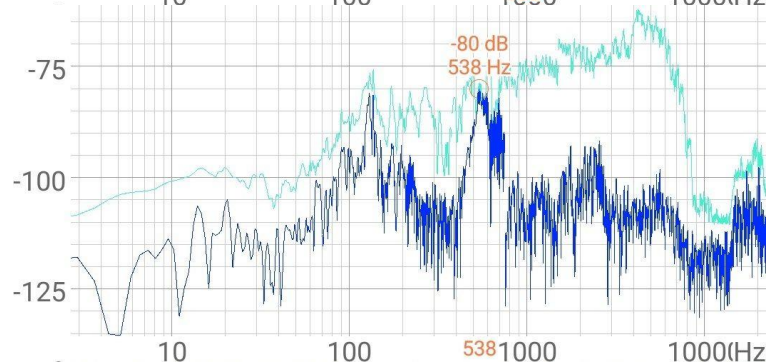

-75
-100
-125
-78 dB
1348 Hz
10
100
1348
1000(Hz


Reference
-100
-125
-91 dB
700 Hz
10
100
700
1000
1000(Hz


-75
-100
-125
-93 d
530 Hz
530
1000

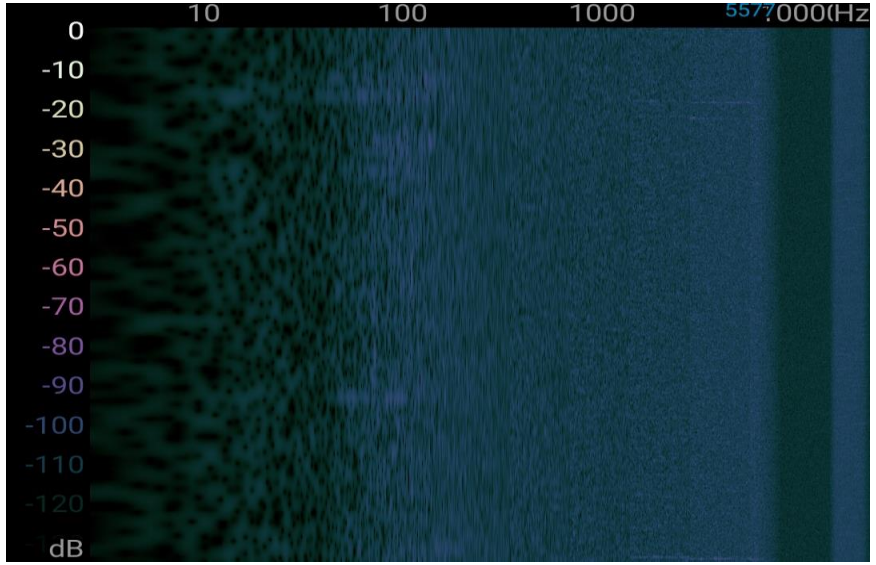

-75
-100
-125
-84 dB
2756 Hz
10
100
1000
2756
1000(Hz


-75
-100
-125
-82 dB
952 Hz
10
100
952
1000(Hz

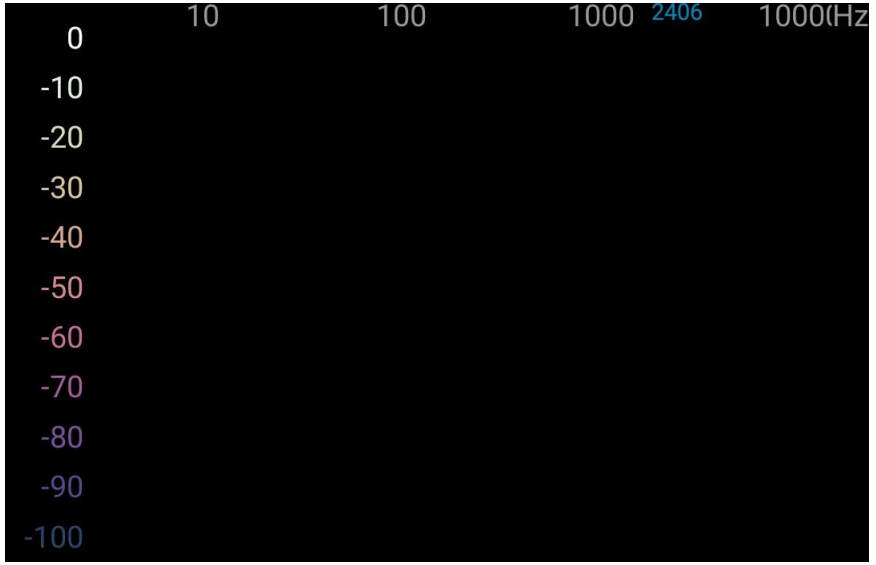

-75
-100
-125
-80 dB
538 Hz
10
100
538
1000
1000(Hz

Spectrograms

- Validate the contribution of each key press to a 4 digit PIN entry
- Requires a reference spectrogram of silence and ambient noise

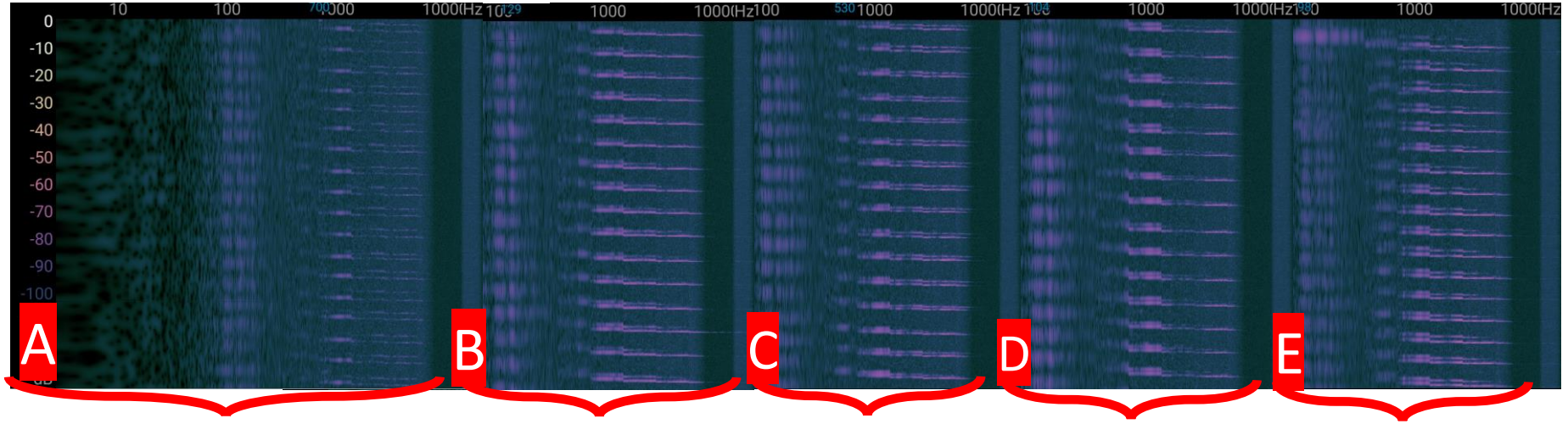


Ambient noise

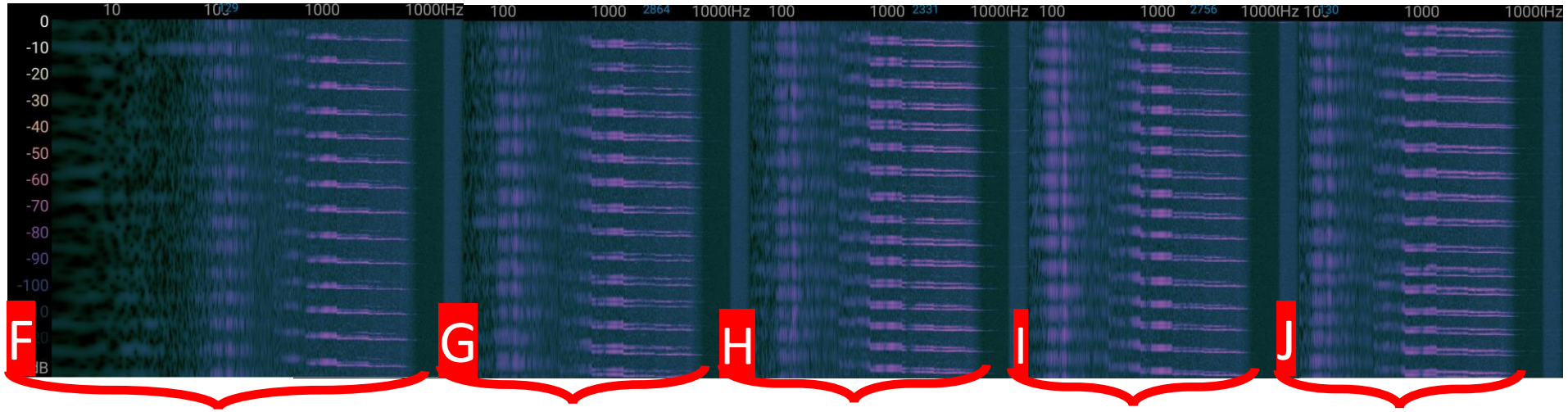


Silence (< 30 dB)

Key press X times in a row … ranking

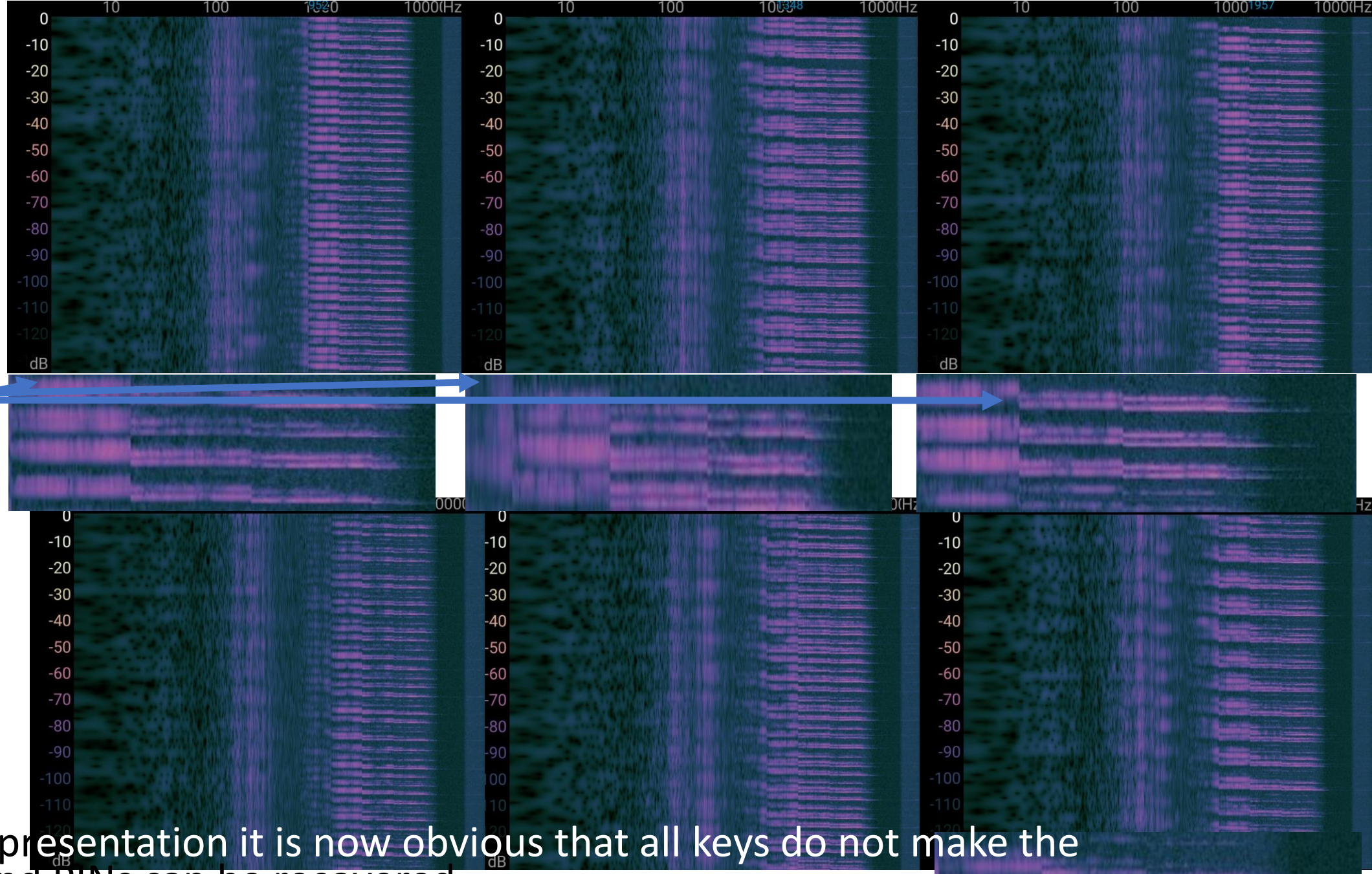


Most silent key | 2nd most silent key | Fastest dome action | Most average key | 2nd most average



Asymmetric result on key push | ‘Clickety’ key | Noisry key | Spurious key press | Most noisy

PIN entry



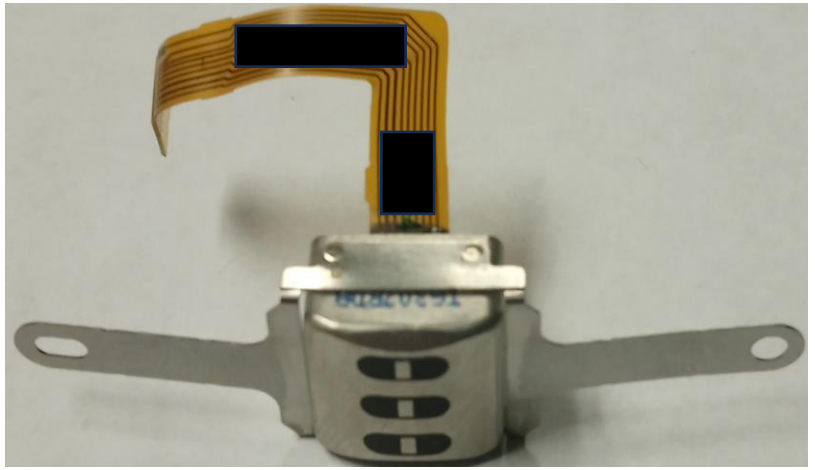
Those are not equal signatures !!!

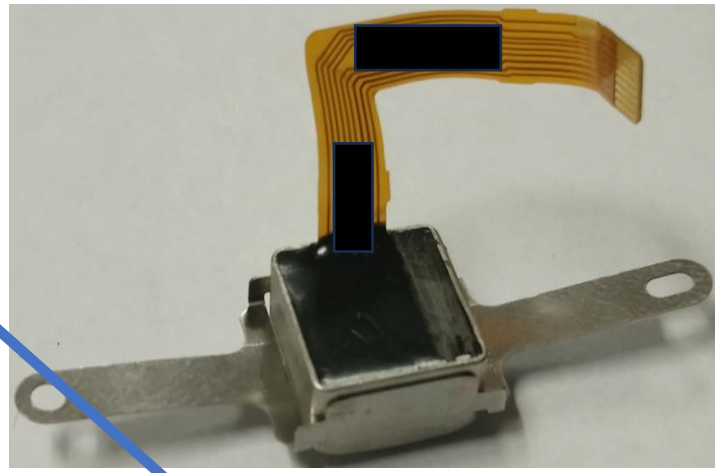
- Under this representation it is now obvious that all keys do not make the same noise and PINs can be recovered

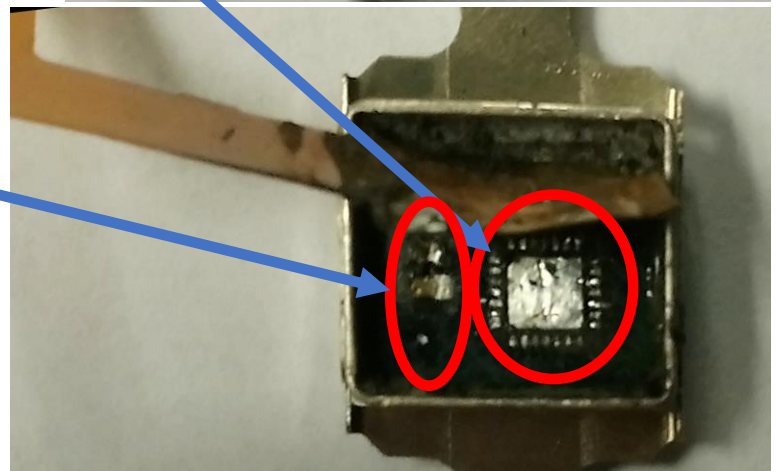
Magnetic Stripe Reader analysis

Security of MSR head

- MSR head uses an embedded encryption dedicated processor
- However it is possible to access the plaintext data before it enters in the encryption processor because of the design of the MSR internally
  - The soldering points of the coils are to prominent
  - An attacker could just create contact with coils ends at soldering level
- The presence of a flexible mesh above those parts would prevent such an attack

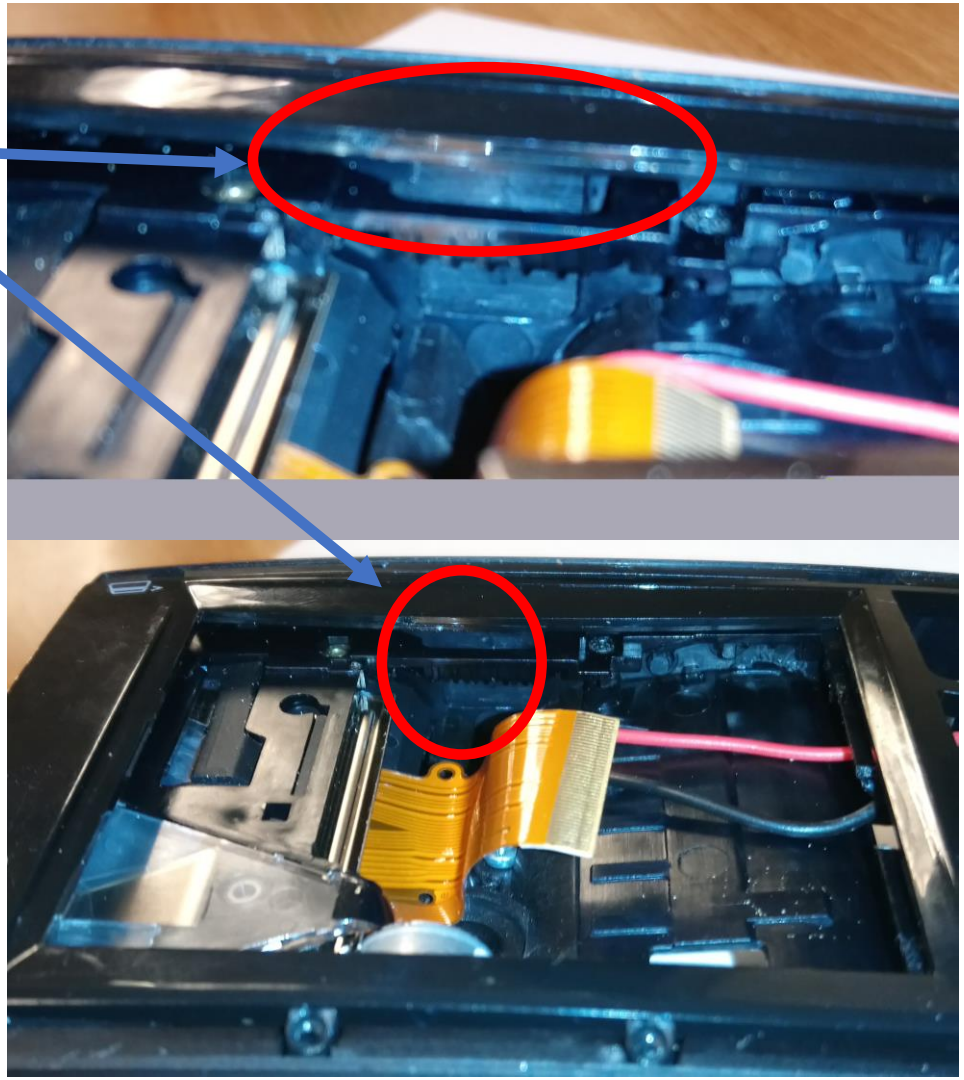


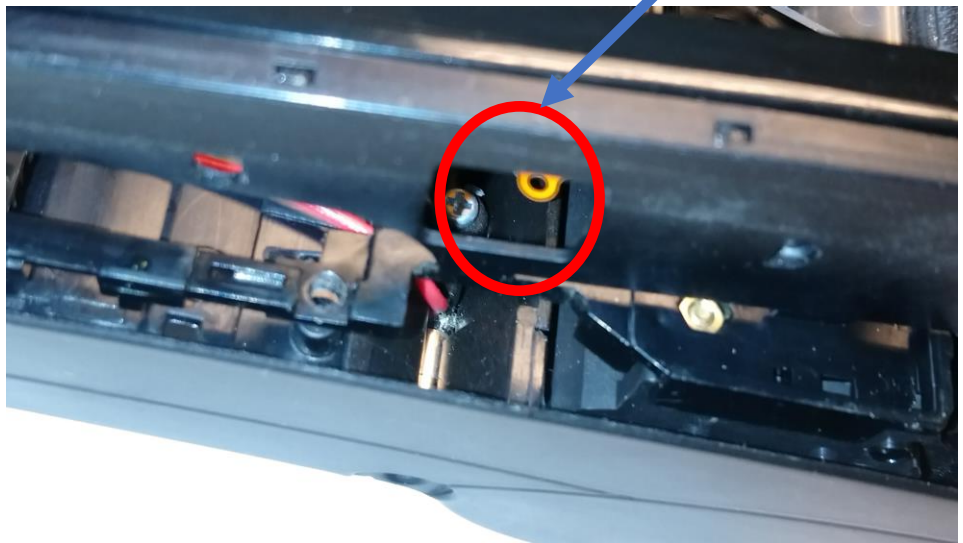




Good design : impossible to insert a 2nd MSR

- We tried and concluded it was too difficult !

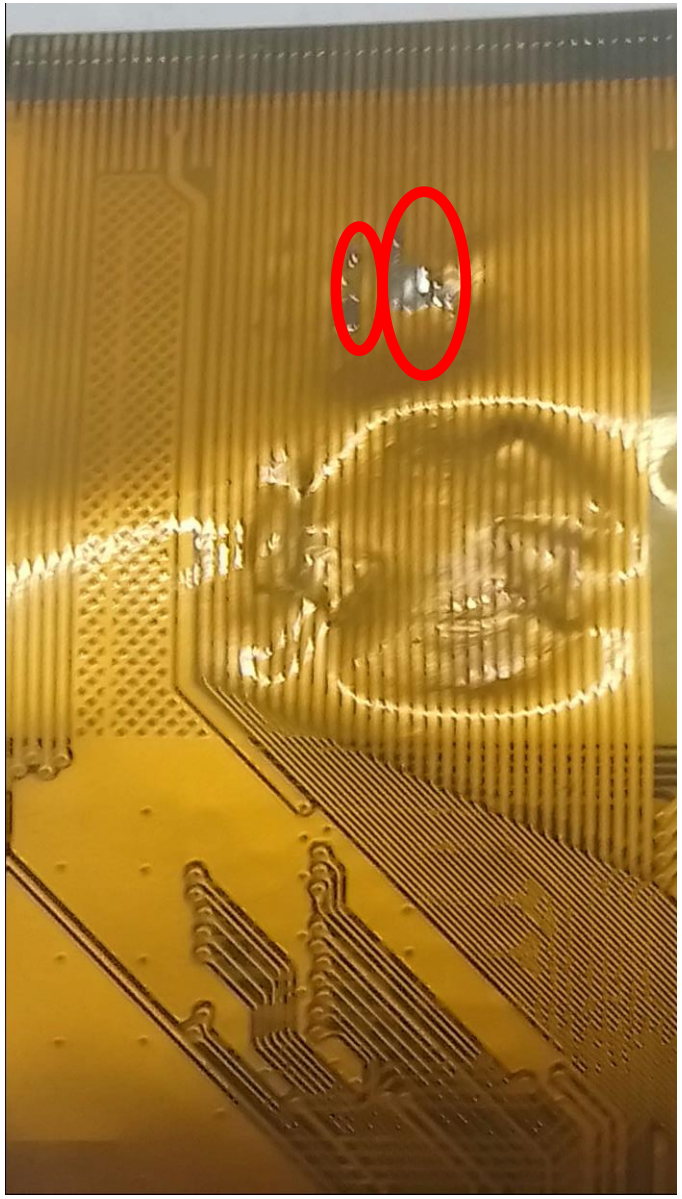




LCD analysis

Soldering on flexible ribbon

- We tested the flexible ribbon connecting the LCD to the main board
  - Resistance to abrasion is good
- We managed to solder on the flexible ribbon
  - We also managed to cut a unique line and solder on both ends
- We stopped there by lack of time
- We believe we could have taken control of LCD easily



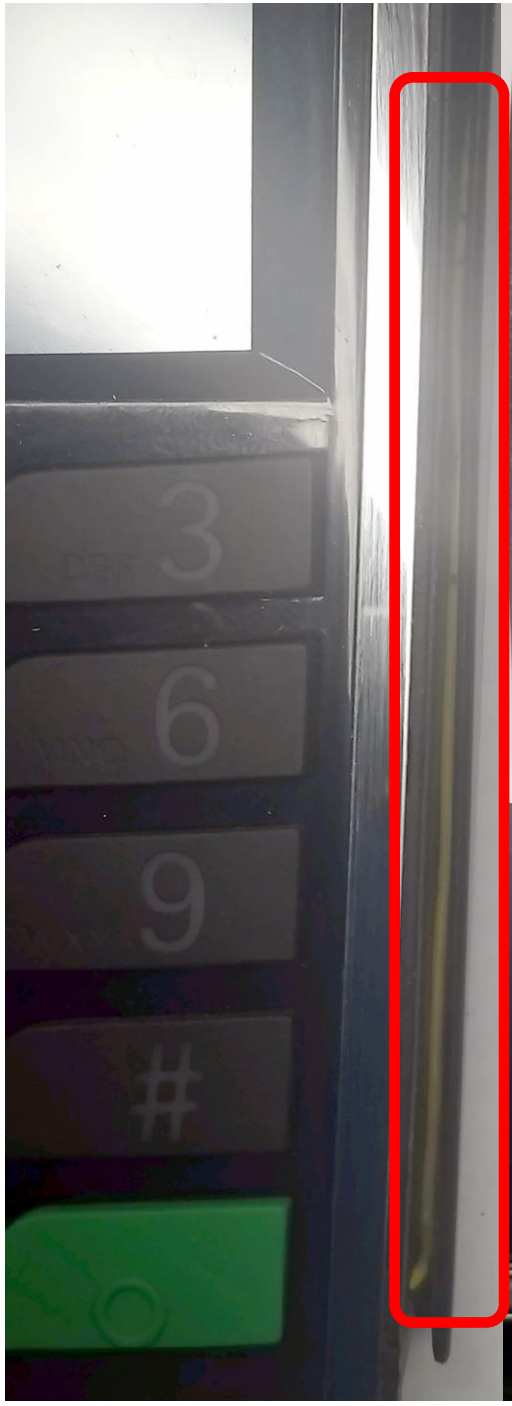
Smartcard connector area analysis

Accessing smartcard data for fun and profits

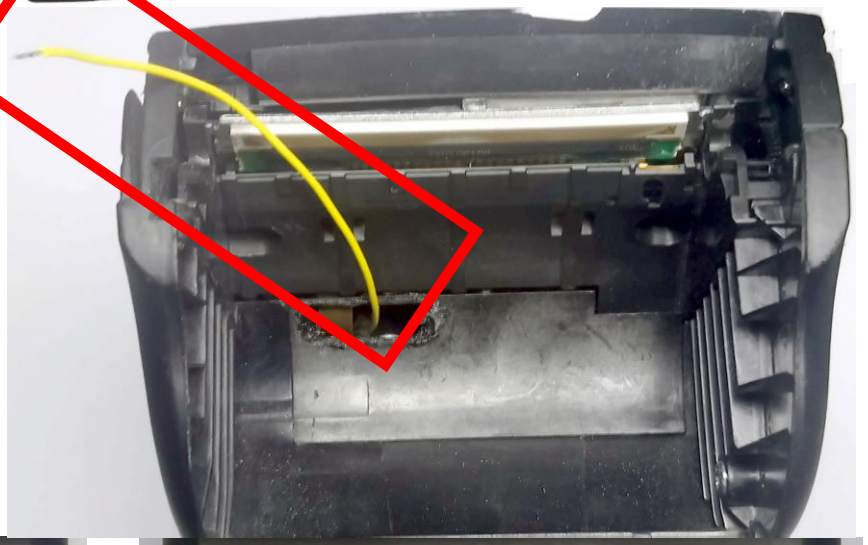
- An easy attack can be mounted on the smartcard area
  - The LDS protection does not come close enough to the opening of the plastic casing
- Attacker will sold a wire to data pin of smartcard connector
- Attacker will drill a small hole on the side of casing just after LDS protection
- Attacker will create exit hole inside sliding card area of MSR.
  - Black copper wire is fully hidden and not visible
- Attacker will drill holes to hide skimmer part by printer area in tiny hole
- Attacker routes wire and enables skimmer
- Attacker repairs plastic and hides traces

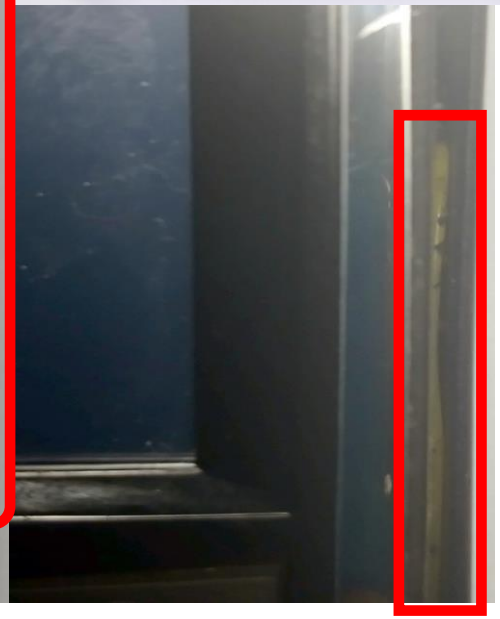
  The device never tampered

- To simplify the view for this tutoral we used a wide YELLOW wire instead of using a small black copper wire (refer to next slide)

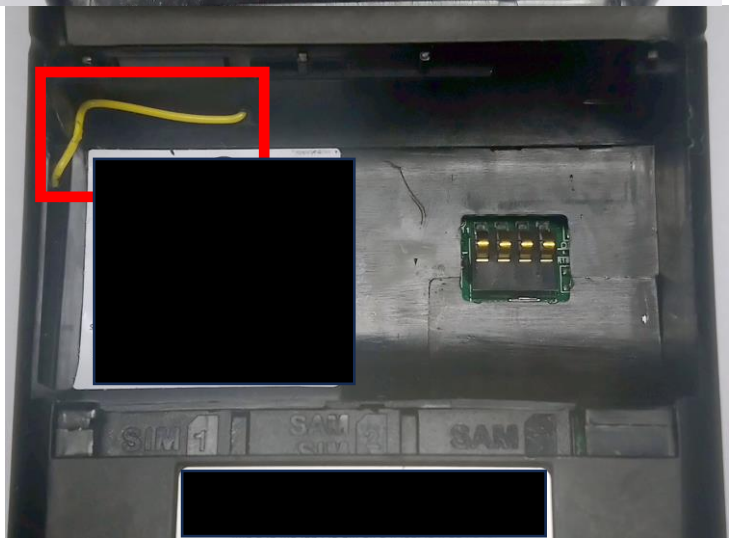

3
6
9
#


1
2
3
4
5
6
7
8
9
*
0
#





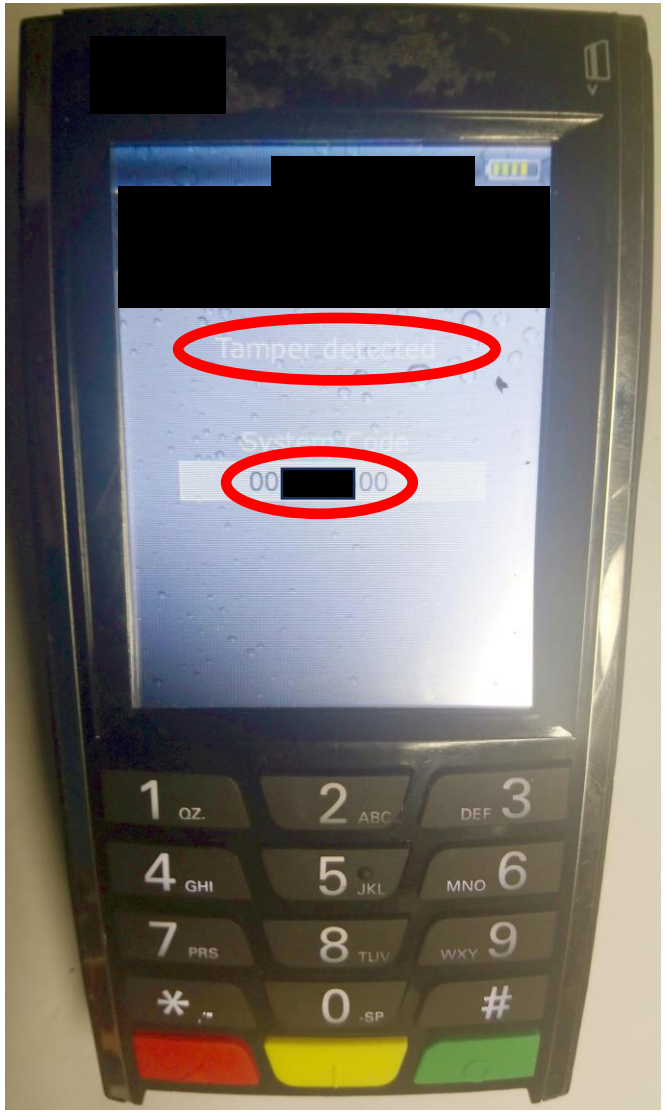

SIM 1
SAM 2
SIM
SAM 1


SIM 1
SAM 2
SIM
SAM

Tampering the device

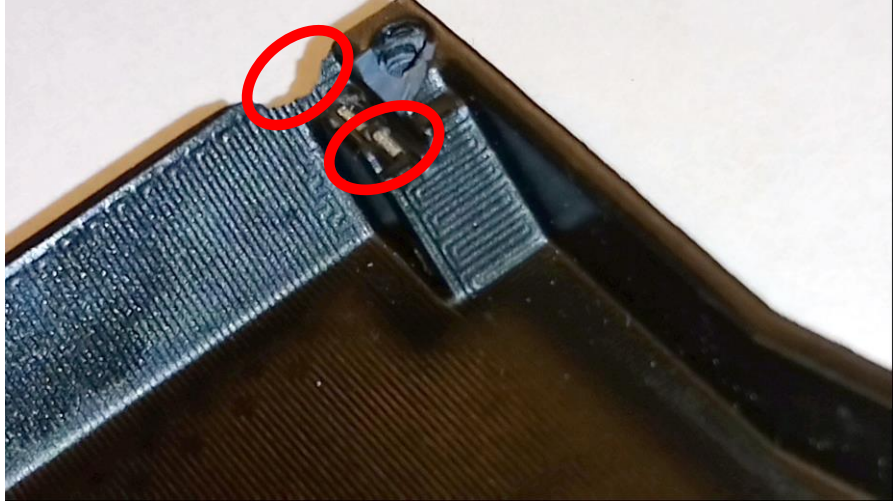
Was tamper enabled on this device?

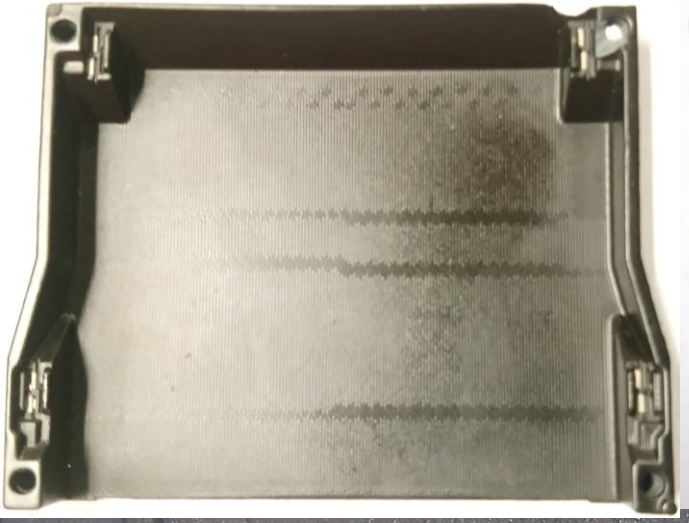
- We needed to be sure we received a fully functional device with tamper enabled
  - We made all our attacks with no tamper event
- So we lifted the keypad area to create a tamper event
- This is the proof that tamper was enabled !!!



LDS security

- We believe we found a way to abuse LDS
  - It initially defeated us
  - Excellent heat and mechanical resistance
- We could not validate our success by lack of time
  - We created electrical contact with mesh running inside LDS from outside





Attacking unsecured parts …

Connection to printer

- Printer is not considered important
  - Therefore it is not secure

- Example of an attack
  - Take two identical terminals
  - Reverse the printing mechanism of the first terminal
  - Program your own microcontroller replacing the required data sent to the printer
    - Change the logo and name of the shop
  - Insert your new toy in the second terminal
  - Go to a shop and replace your target by your terminal
    - People will buy things, receive a receipt but the money comes to your account !!!

Well documented attacks

Same player play again
https://vimeo.com/89924160

Aldi’s 2010, Michaels 2011, …

- Old pre-pci terminals
- Inserted a key capturing underlay to obtain PINs
- Additionally captured Magstripe information using another Magnetic head
- Used a small bluetooth board to transmit data to attacker
  - Quite common nowadays

Pin Pad Powner at Black Hat in 2012

- Research done by MWR Labs
- PCI PTS Version 1 device.
- Attacked was done through EMV, Ethernet and software update mechanism (failed)
- No opening of the device was required
- Device unfortunately printed internal debugging
- Attacker was able to control the application processer of the device, obtain card numbers etc.
- FROG, TETRIS, CAR … !!!

Common German Terminal – SR Labs

- Similar to PIN Pad Powned attack
- PCI PTS Version 1 device
- Targeted the applications processor
- Interfaces were not sufficiently tested again.
- Debugging interfaces not disabled
- JTAG left enabled !!!

More recently

FBI unexpected visit …

FBI Raids Chinese Point-of-Sale Giant PAX Technology

October 26, 2021 165 Comments

U.S. federal investigators today raided the Florida offices of **PAX Technology**, a Chinese provider of point-of-sale devices used by millions of businesses and retailers globally. KrebsOnSecurity has learned the raid is tied to reports that PAX's systems may have been involved in cyberattacks on U.S. and E.U. organizations.

FBI agents entering PAX Technology offices in Jacksonville today. Source: WOKV.com.

Headquartered in Shenzhen, China, PAX Technology Inc. has more than 60 million point-of-sale terminals in use throughout 120 countries. Earlier today, Jacksonville, Fla. based **WOKV.com** reported that agents with the FBI and **Department of Homeland Security** (DHS) had raided a local PAX Technology warehouse.

Mailing List

Subscribe here

Search KrebsOnSecurity

SEARCH

Recent Posts

It's Still Easy for Anyone to Become You at Experian

Who's Behind the SWAT USA Reshipping Service?

Russian Reshipping Service 'SWAT USA Drop' Exposed

.US Harbors Prolific Malicious Link Shortening Service

NJ Man Hired Online to Firebomb, Shoot at Homes Gets 13 Years in Prison

Story Categories

A Little Sunshine

All About Skimmers

Ashley Madison breach

Tried to find was FBI did not find

- Eight functional devices have been procured separately and by groups
  - Previous usage of devices can be guessed
    - Clear origin is unknown however
  - No specific applications installed on device(s)
    - Key loading, App Store, … are present

Device mandates connection to app store to be onboarded … by design

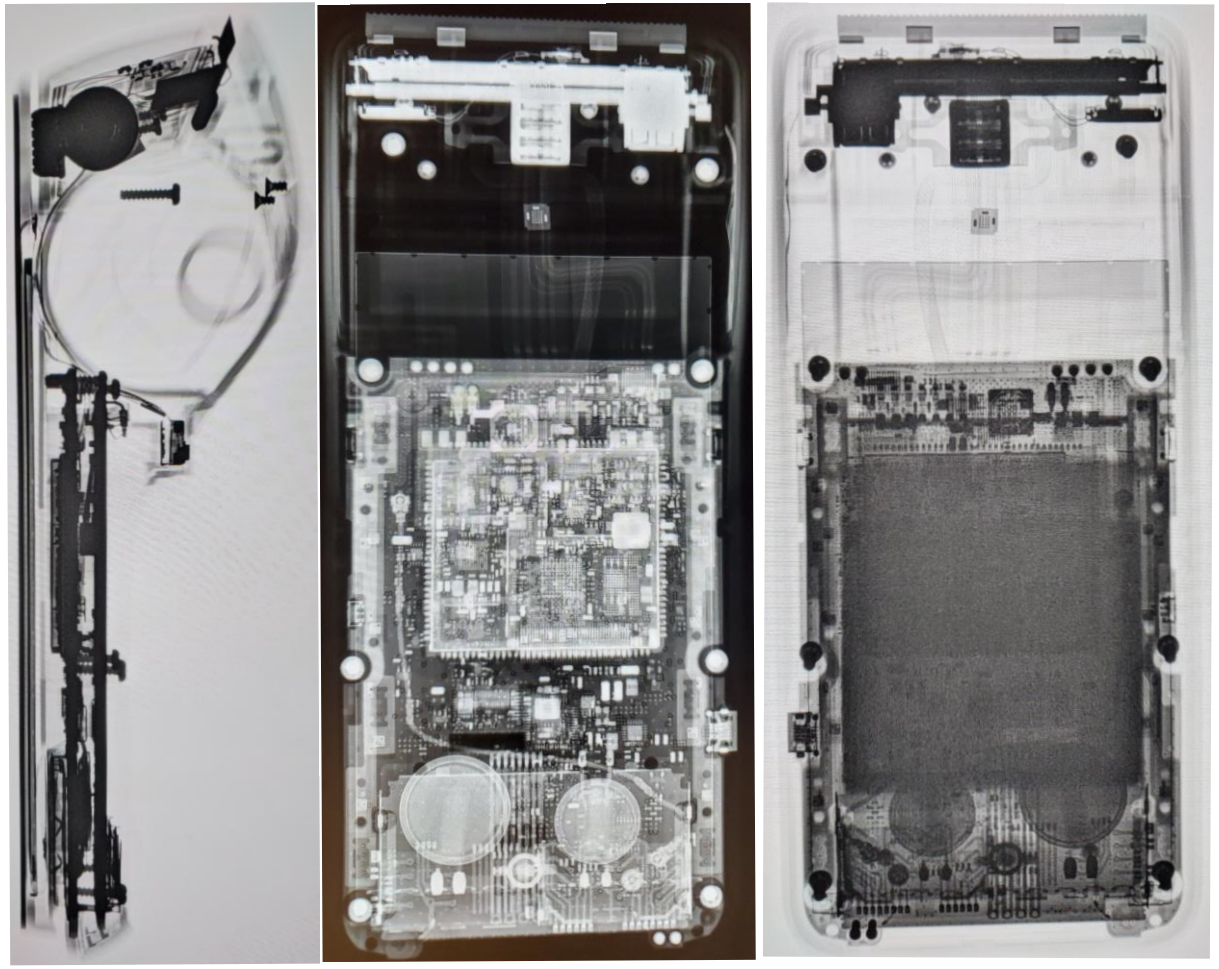
- Device runs Android operating system and is based on applications
- Device is suspected of having data exchanges with unexpected and undocumented sources
- Many traces on internet of people suspecting a strange behavior from those devices
- Manufacturer clearly claims that nothing is proven about connection to home country
- However a dedicated network is used with connection in Hong-Kong to receive data
- Approach is to invite other companies and manufacturer to bring their applications to app store

Work hypothesis

- Device is not tampered
  - Devices are tamper enabled
    - Tampering the device would erase keys and neutralize device
    - Requires to be skillful and cautious
  - Devices are PCI PTS certified and compliant
  - If nefarious behavior is present
    - Serious nefarious behavior would be covered as plausible deniability
      - Bugs, error, rogue engineer … (Think Weather balloon, … it unfortunately escaped :-)
    - Not serious behavior will be isolated and will not create chain of profitable events

A view from outside

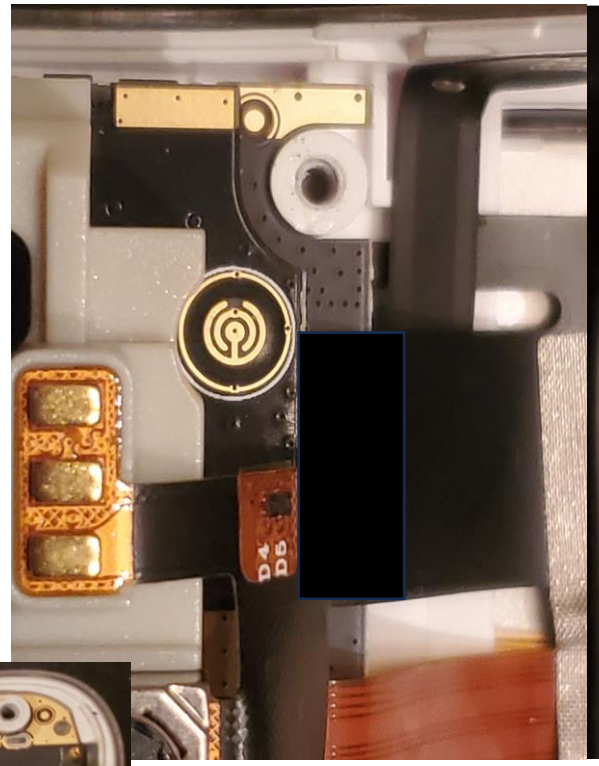
- Use Xrays and tomography
  - All devices are identical
    - Quectel module (like CM5)
  - Physical security model is average and devices could be abused by skilled attacker
  - MSR space management is poor
  - Suspicious film to deactivate tamper switch
    - Inserted at manufacturing, must have been done by an intern …☺

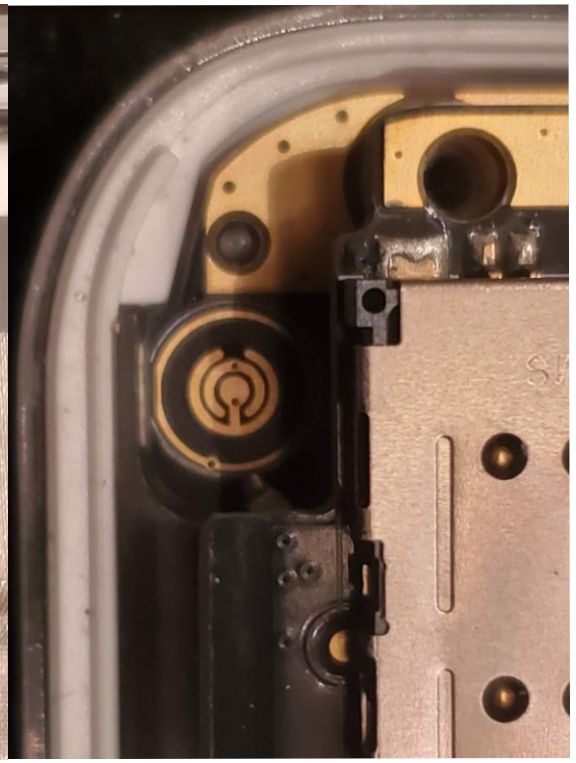


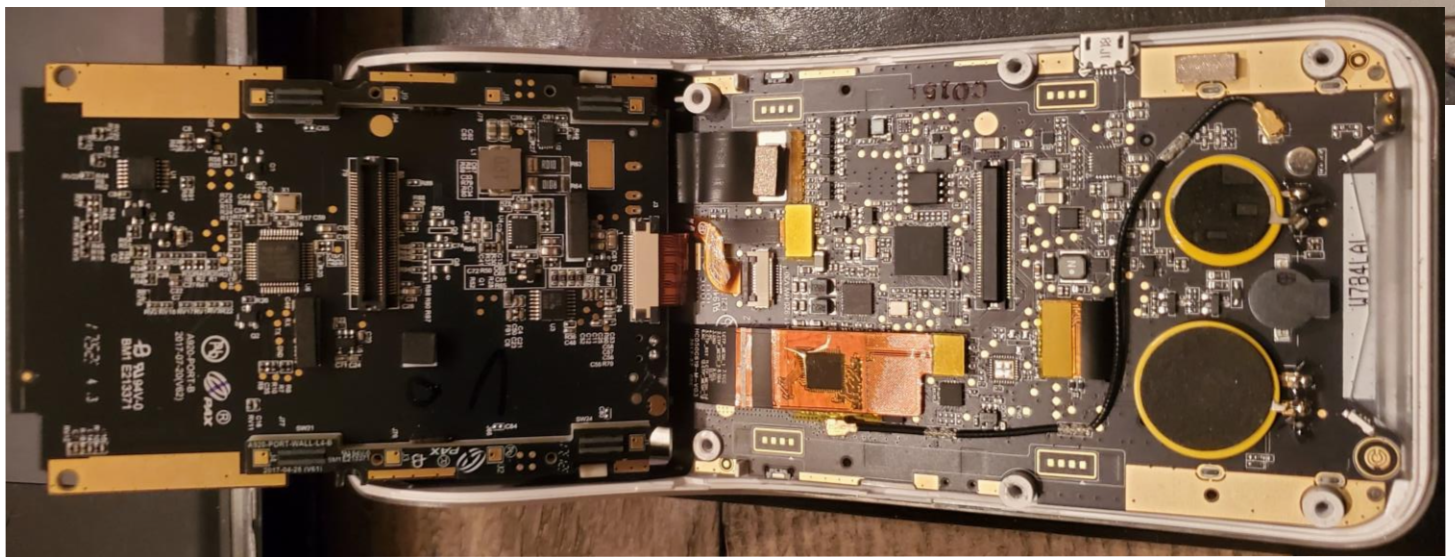
Tampered one device to check inside

- Possible modification of tamper confirmed in comparison to what is expected from PCI
- Guard rings can be defeated because of simple mistake

Maybe

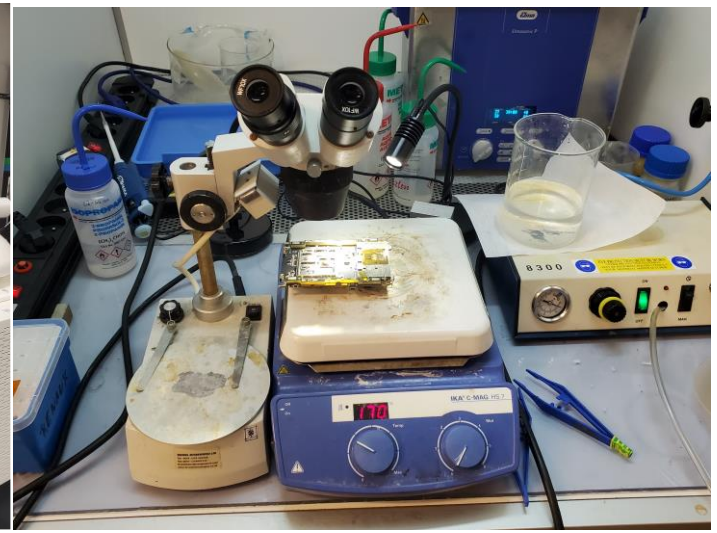


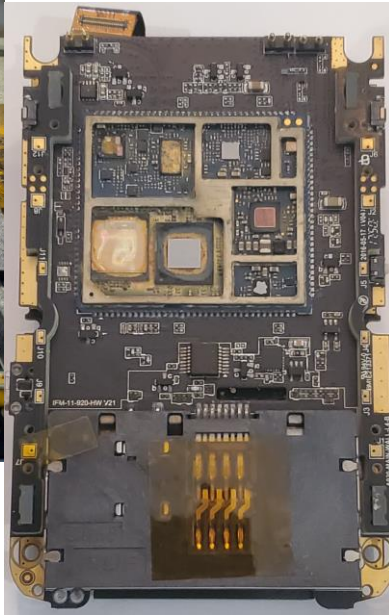




Checking the components

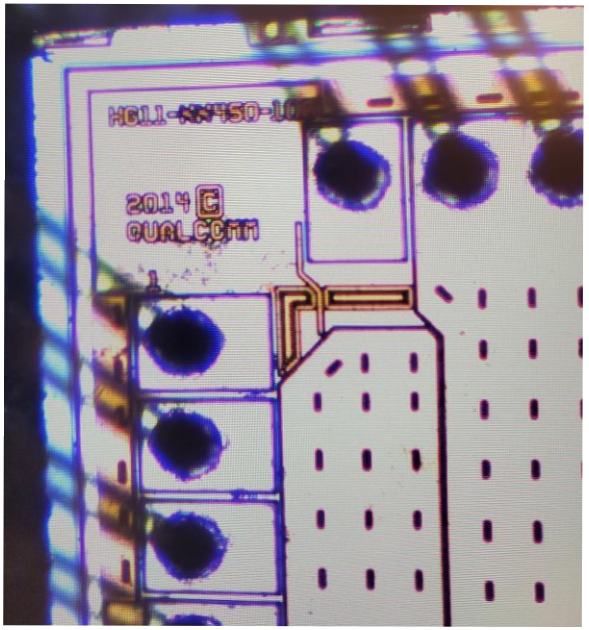
- Sacrificed one device for hardware analysis
- Used industrial equipment
  - Depackaging of ICs (Nitric acid,...)
  - Components are genuine

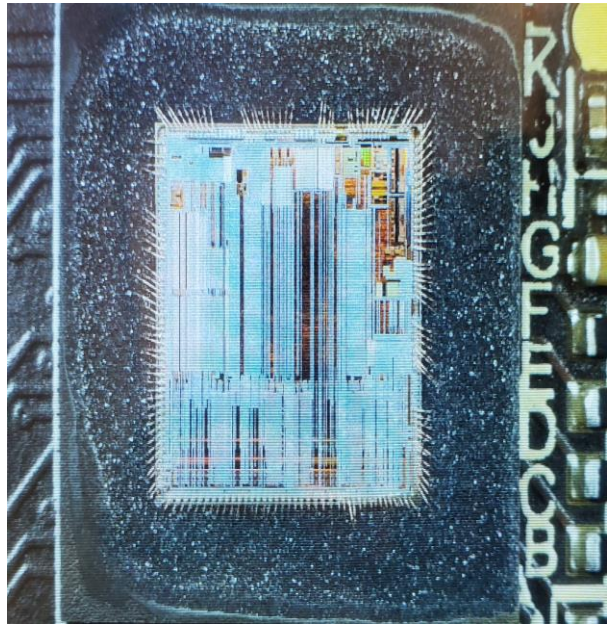
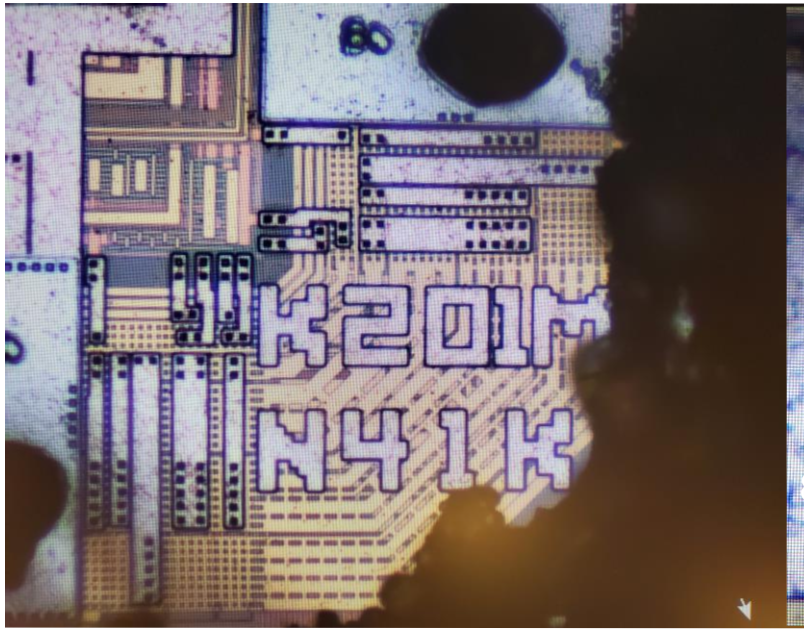


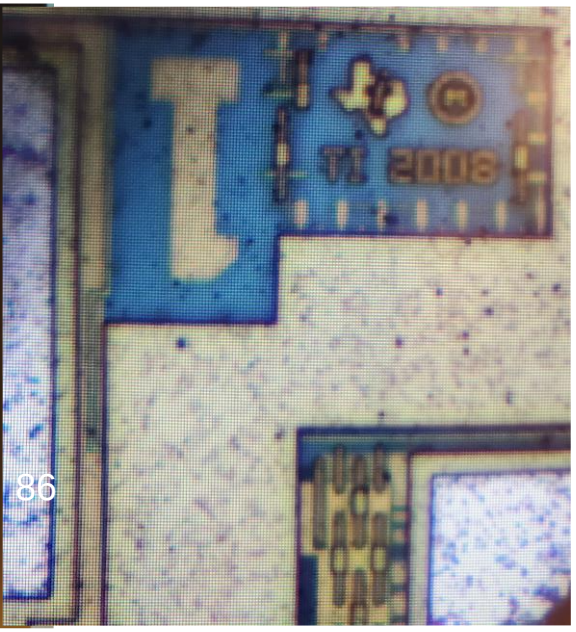


Components are genuine

- Origin of components seems ok and not suspicious
  - Manufacturers symbols, insigna and watermarks are present per expectations





Connection to network

- Created dedicated network
  - Installed device
    - Device tries to move around on network even when fixed to one place
  - Intercepted all in and out communications
  - Recorded communications
  - Performed first analysis of exchange

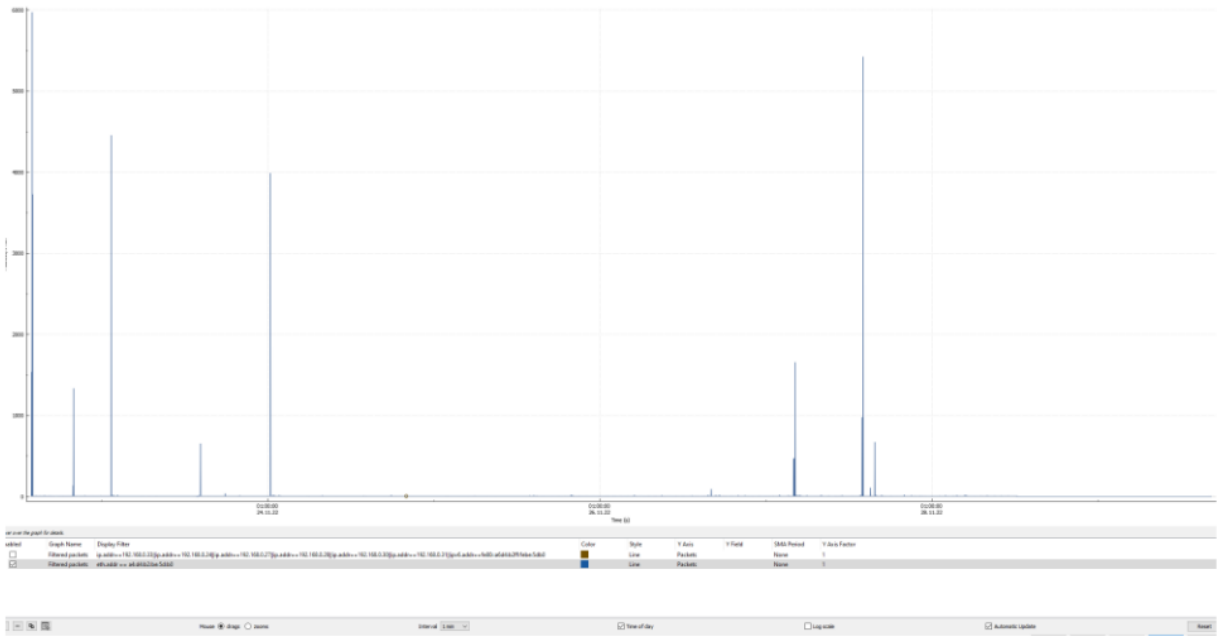
  - Note to the manufacturer
  - Your TLS 1.2 version might be a target of a timing attack ☺

Frame analysis

```
> Frame 11986: 185 bytes on wire (1480 bits), 185 bytes captured (1480 bits) on interface eth0, id 0
> Ethernet II, Src: Shenzhen_be:5d:b0 [redacted], Dst: PcsCompu_a2:cd:92 [redacted]
> Internet Protocol Version 4, Src: 192.168.0.33, Dst: 13.226.[redacted]
> Transmission Control Protocol, Src Port: 55878, Dst Port: 443, Seq: 1, Ack: 1, Len: 119
v Transport Layer Security
  v TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 114
      Encrypted Application Data: c3e33833696e607762430dab7029177f98ac55524f0012a298174d3e57108c2fb99916d3…
      [Application Data Protocol: http-over-tls]
```

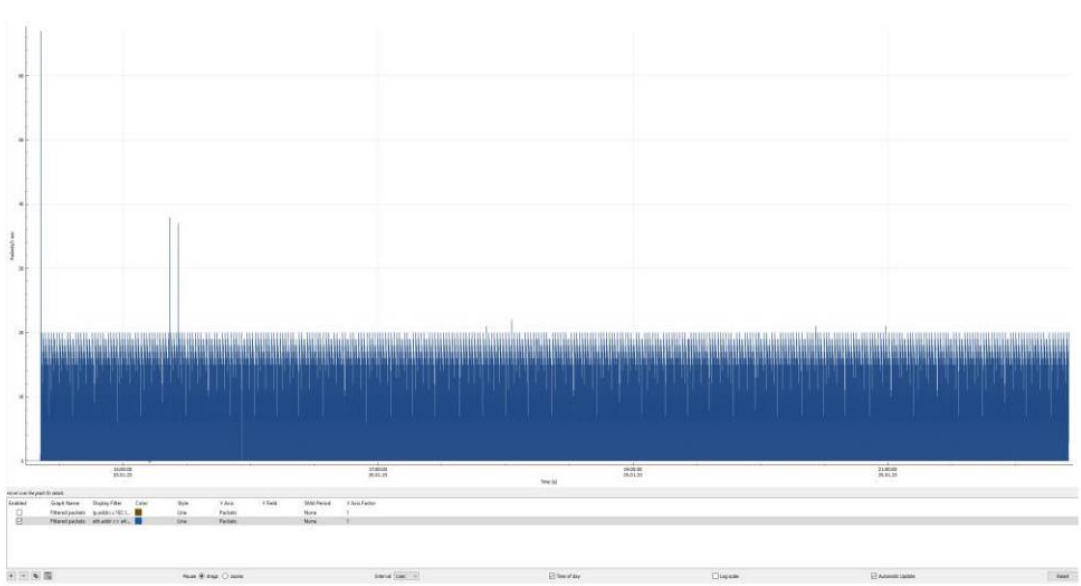
Massive peak of uploading data

- Communications peak at time
- 0.5 Giga exchanged with one end point
  - Not unique

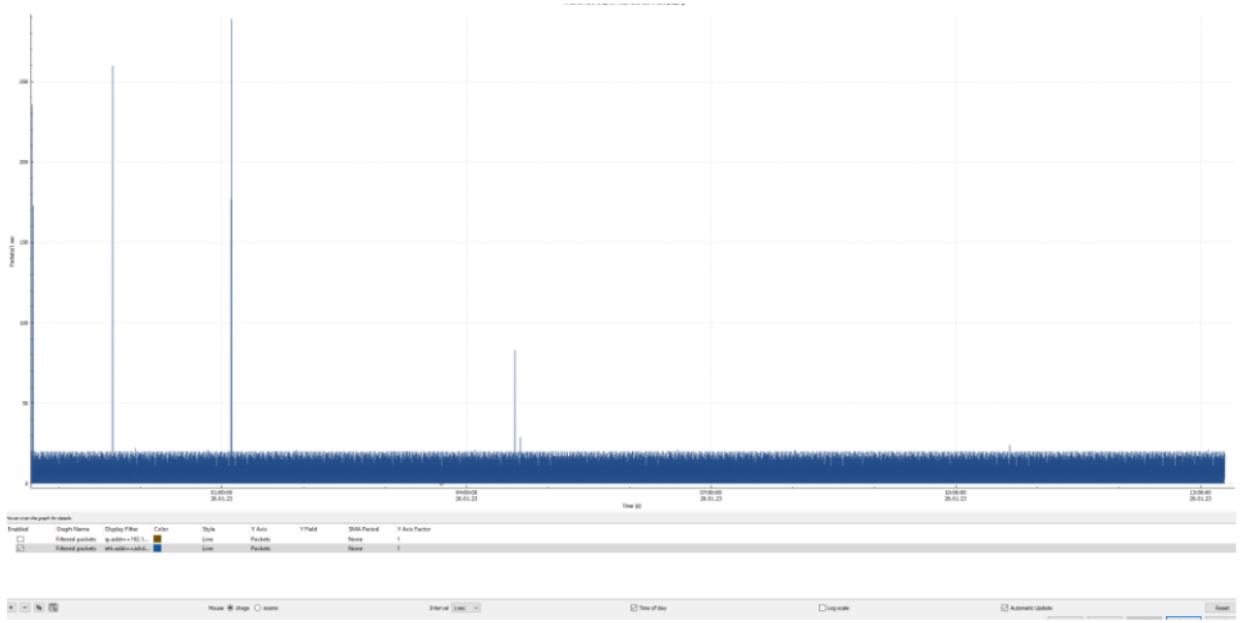


I/O Graph

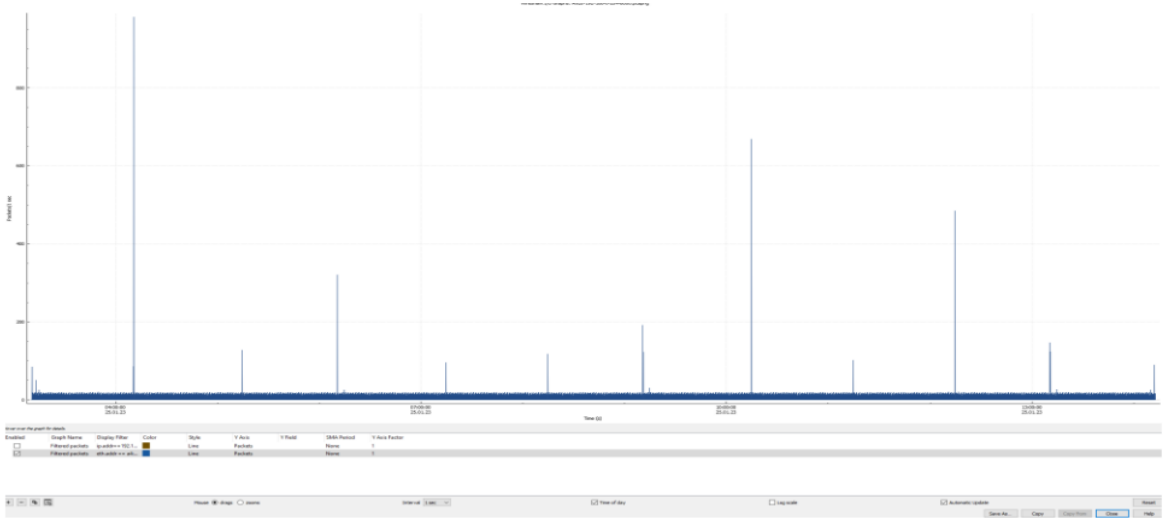
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
212.27.60.27	546,851	504 M	323,012	488 M	223,839	15 M
192.168.0.29	1,033,503	490 M	24,399	9194 k	1,009,104	481 M
192.168.0.22	512,371	440 M	214,193	15 M	298,178	425 M
192.168.0.26	1,020,639	428 M	107,308	48 M	913,331	380 M
192.168.0.25	218,439	221 M	69,831	4669 k	148,608	217 M
142.250.201.161	363,466	214 M	347,220	201 M	16,246	13 M
192.168.0.32	769,228	171 M	15,893	7189 k	753,335	164 M
151.101.122.132	151,972	149 M	101,228	145 M	50,744	3438 k
216.58.214.161	246,790	131 M	236,400	123 M	10,390	8088 k
142.250.179.65	236,014	131 M	227,508	124 M	8,506	6946 k
216.58.213.65	243,416	106 M	234,346	99 M	9,070	7315 k
142.250.179.97	150,222	103 M	143,078	97 M	7,144	5839 k
216.58.214.65	158,154	97 M	150,840	91 M	7,314	5858 k
216.58.215.33	200,896	96 M	193,804	90 M	7,092	5519 k
142.250.75.225	85,660	51 M	80,516	47 M	5,144	4283 k
142.250.178.129	72,388	46 M	68,876	44 M	3,512	2754 k
192.168.0.34	51,501	23 M	51,501	23 M	0	0
45.57.90.1	54,440	18 M	53,740	18 M	700	110 k
45.57.91.1	38,687	11 M	37,752	11 M	935	150 k



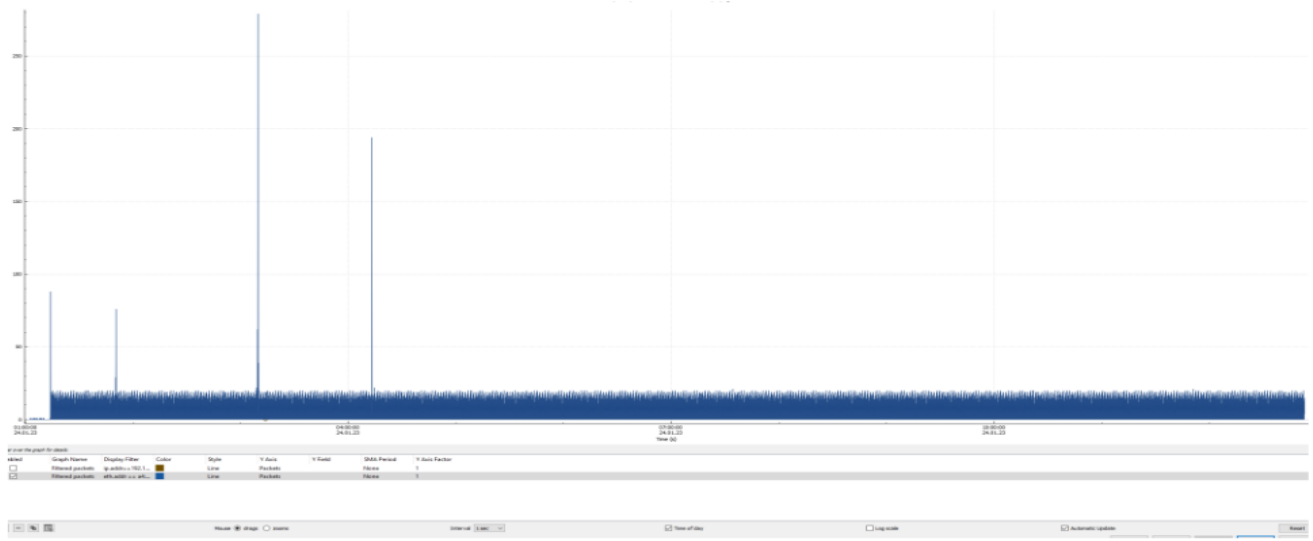
I/O Graphs



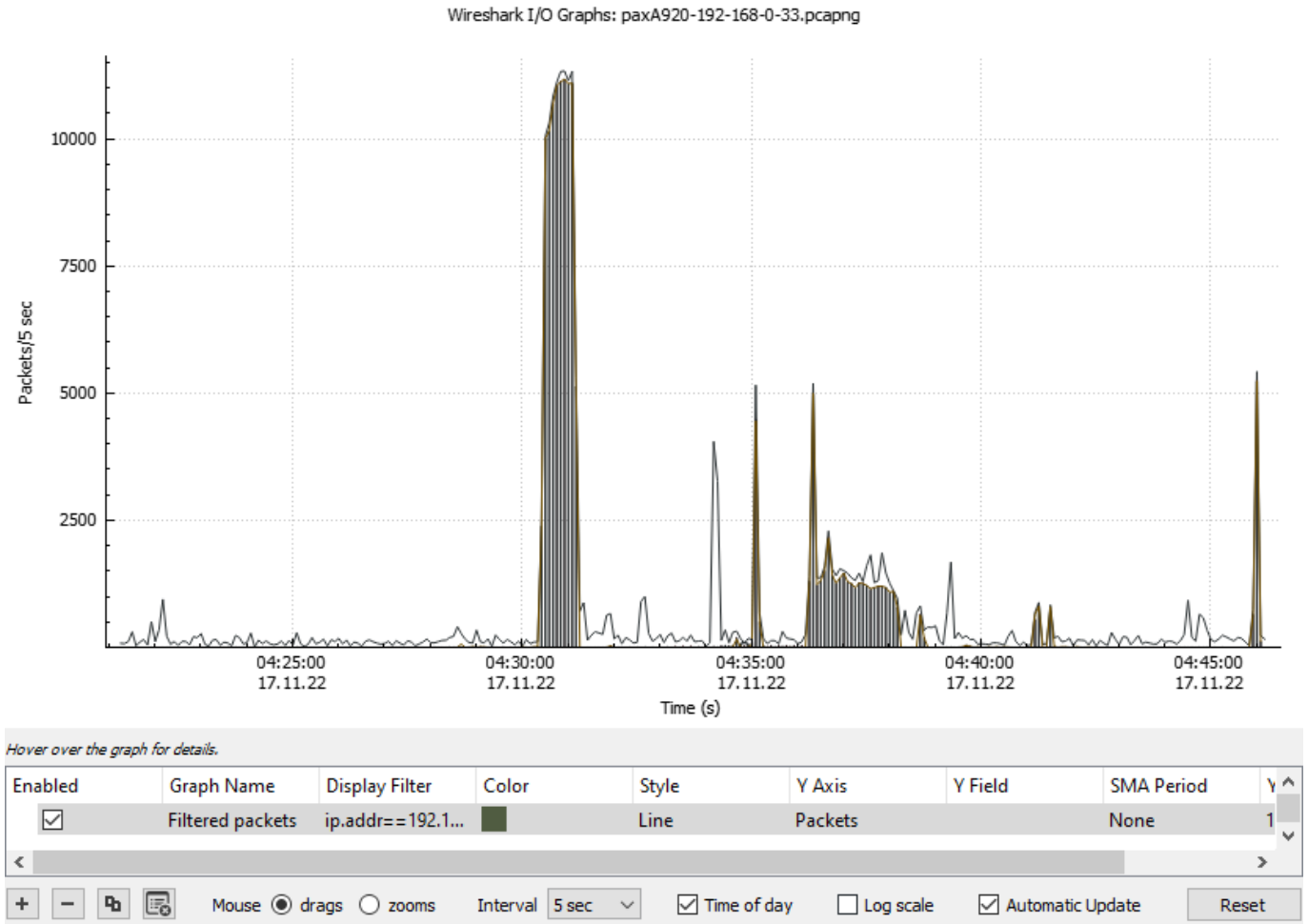
I/O Graphs



I/O Graphs



I/O Graph


Wireshark I/O Graphs: paxA920-192-168-0-33.pcapng
Packets/5 sec
10000
7500
5000
2500
04:25:00
17.11.22
04:30:00
17.11.22
04:35:00
17.11.22
04:40:00
17.11.22
04:45:00
17.11.22
Time (s)
Hover over the graph for details.
Enabled
Graph Name
Display Filter
Color
Style
Y Axis
Y Field
SMA Period
Filtered packets
ip.addr==192.1...
Line
Packets
None
Mouse
drags
zooms
Interval
5 sec
Time of day
Log scale
Automatic Update
Reset

13.224.34.94 : Subject: CN=*.paxstore.us

13.225.49.153 : Subject: CN=*.paxstore.us

99.84.111.16 : Subject: CN=*.paxstore.us

13.225.146.106 : Subject: CN=*.paxstore.us

99.81.73.231 : CN=paxsaas.com

52.37.253.181 : ec2-52-37-253-181.us-west-2.compute.amazonaws.com, probably pax

52.14.42.201 : ec2-52-14-42-201.us-east-2.compute.amazonaws.com, probably pax

3.23.55.207 : ec2-3-23-55-207.us-east-2.compute.amazonaws.com, probably pax

3.14.9.119 - > redirect to
https://info2.paxsz.com/#/login?redirect=0.7663211313603565&fromPath=%2Fhome

Non-Pax

35.181.16.16 : Subject: CN=www.worldenergy.fr

52.47.80.63 : CN=*.skyhookwireless.com

13.226.238.16 : Subject: CN=pp.s3.ringcentral.com

99.84.246.4 : Subject: CN=alexa.amazon.co.jp

143.204.128.177 : CN=*.svc.nhl.com [BAMTECH]

96.17.193.41 : No info

142.250.179.69 : redirect to google.com

13.107.136.254 : CN=*.msedge.net

13.107.237.254 : CN=*.msedge.net

13.107.253.254 : CN=*.msedge.net

13.107.42.254 : CN=*.msedge.net

20.194.51.173 : CN=*.footprintdns.com

43.135.106.241 : CN=*.nov04-2022-1.ias.tencent-cloud.net

13.226.238.16 : CN=Go Daddy Secure Certificate Authority - G2

52.45.98.208 : CN=receive-lp1.dg.srv.nintendo.net

52.223.198.2 : CN=*.cdg02.hls.live-video.net

54.85.191.60 : CN=receive-lp1.dg.srv.nintendo.net

142.250.75.228 : redirect to google.com

Suspect IPs compared with week-long analysis

Japan Alexa API

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
99.84.246.4	443	5,493	367 k	5,417	357 k	76	

367k bytes sent to this address

Ethernet · 2 | IPv4 · 80 | IPv6 · 1 | TCP · 165 | UDP · 153

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
192.168.0.24	45238	99.84.246.4	443	6	952	6	952	0	0
192.168.0.24	55989	99.84.246.4	443	10	1319	10	1319	0	0
192.168.0.27	60792	99.84.246.4	443	4	303	4	303	0	0
192.168.0.27	38529	99.84.246.4	443	7	1030	7	1030	0	0
192.168.0.27	55607	99.84.246.4	443	7	1030	7	1030	0	0
192.168.0.30	36730	99.84.246.4	443	7	1030	7	1030	0	0
192.168.0.30	56940	99.84.246.4	443	5,429	358 k	12	1048	5,417	357 k
192.168.0.30	43770	99.84.246.4	443	10	796	10	796	0	0
192.168.0.31	48619	99.84.246.4	443	6	964	6	964	0	0
192.168.0.31	54414	99.84.246.4	443	7	1030	7	1030	0	0

Line 7 shows 358k bytes sent to 99.84.246.4 and 357k received from this address

BAMTECH (NHL)

No evidence found in week-long analysis but found this in the first quick analysis of the first product analysed

Ethernet · 6 | IPv4 · 22 | IPv6 · 3 | TCP · 17 | UDP · 6

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
143.204.128.177	443	53,308	11 M	53,291	11 M	17	

11M sent to this address

Ethernet · 5 | IPv4 · 20 | IPv6 · 2 | TCP · 12 | UDP · 4

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
									20
									78
143.204.128.177	443	192.168.0.33	56563	15,707	2120 k	15,704	2120 k	3	180
143.204.128.177	443	192.168.0.33	46156	10,414	1405 k	10,412	1405 k	2	120
143.204.128.177	443	192.168.0.33	33846	10,412	1405 k	10,410	1405 k	2	120
143.204.128.177	443	192.168.0.33	40155	10,409	1405 k	10,407	1404 k	2	120
143.204.128.177	443	192.168.0.33	35705	8	562	6	442	2	120
									1 k
192.168.0.33	45905	143.204.128.177	443	6,358	4816 k	6	807	6,352	4815 k

Around 6.6M received from this address

Conclusion of quick analysis

- Cat and mouse game
  - :-) Device calibrates GPS with special file prior to TLS connection and download files from mothership in Asia.
- Device has suspicious communications with external end points
- Massive exchange of data proven
- Quantity of data correlate with network exchanges
- Command and control might be well placed
  - Chain of events is clearly suspicious here
- First conclusion is device is well suited to analyze network and Phone what was found back … “Home”

More software only attacks

Use embedded sensors against the terminal

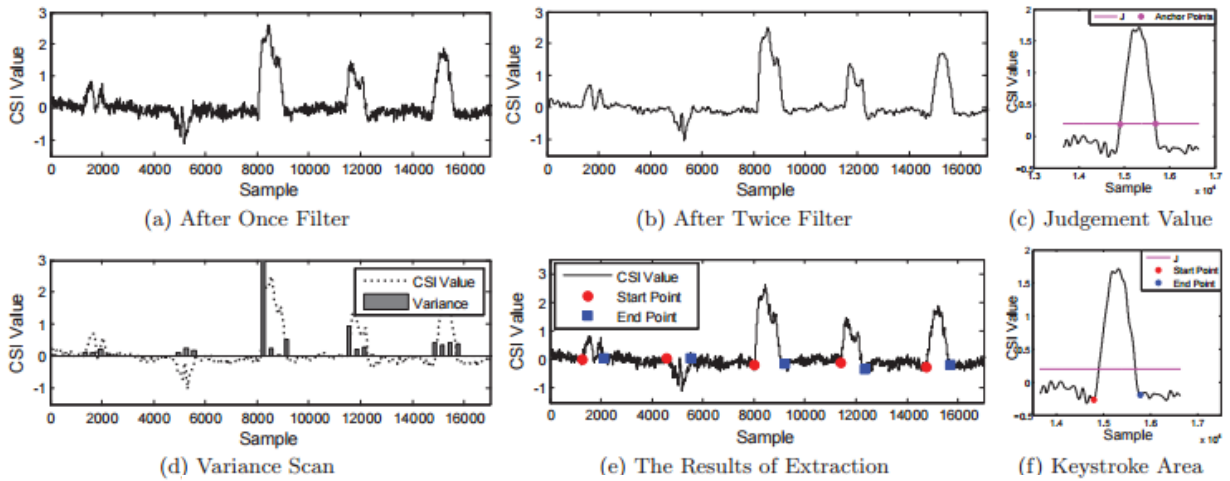
- Some devices include a tablet and a payment terminal
  - Device are mechanically joined
  - If manufacturer did not disable accelerometers then sensors can be used to record vibrations at PIN entry time
  - A bit a non linear separability and some learning with some neural networks and PIN can be compromised fast.

- Some manufacturers do the job properly !!!
  - But not all ☺

Windtalker attack

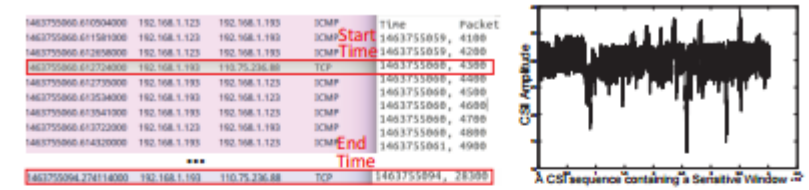
- Use 5GHz Wifi interference at router level to detect position of finger of user on screen
- Use neural network and infer PIN with high probability

- https://blog.acolyer.org/2016/11/10/when-csi-meets-public-wifi-inferring-your-mobile-phone-password-via-wifi-signals/

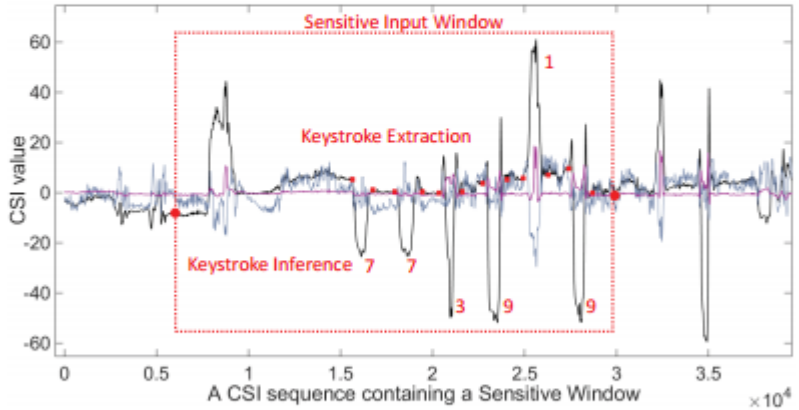


(a) After Once Filter (b) After Twice Filter (c) Judgement Value

(d) Variance Scan (e) The Results of Extraction (f) Keystroke Area



(a) Sensitive Input Windows Recognition Module (b) Original CSI



(c) Keystroke Inference Module

Figure 14: WindTalker in Case Study

Many more attacks to consider

- Use infrared contribution from user to infer PIN
- Refer to : https://news.softpedia.com/news/Card-PIN-Codes-Revealed-by-Finger-Heat-Signature-457315.shtml
- Infrared camera for less than 100 Euros on Alibaba

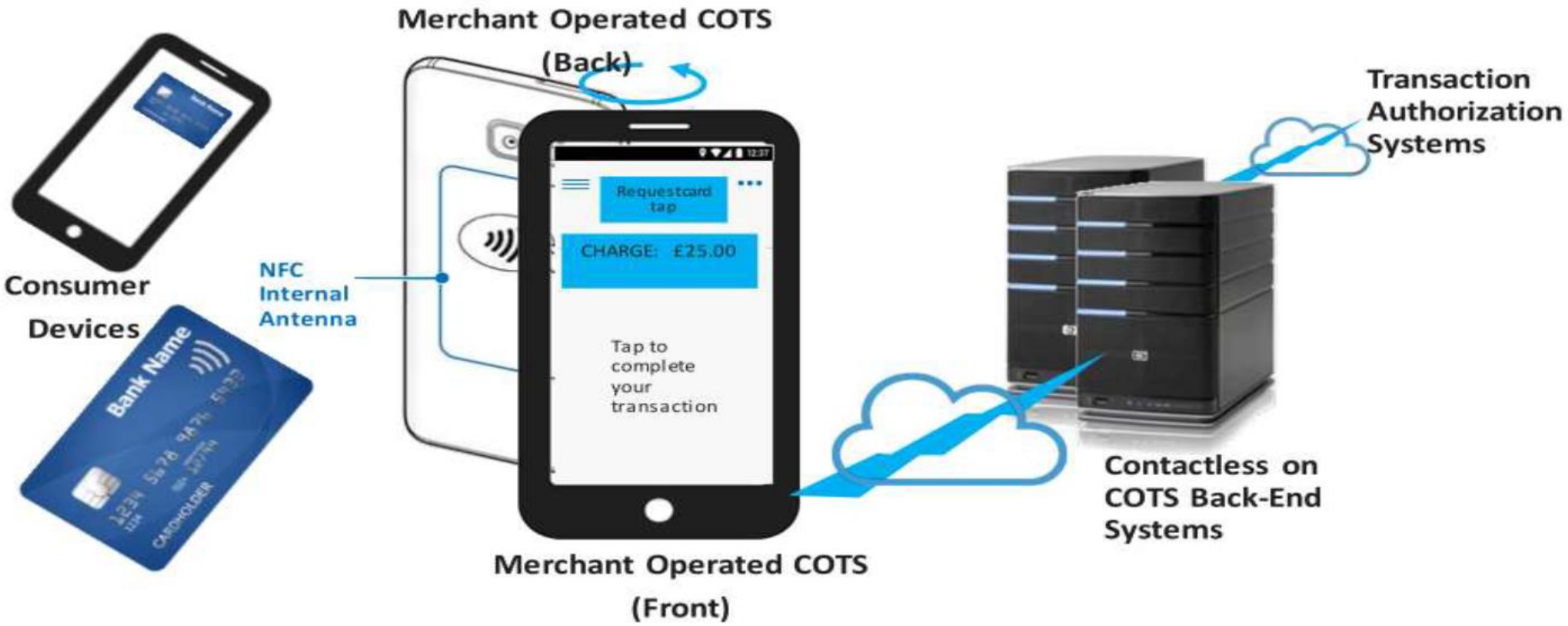
Manufacturer failed

- In case of APOS, in the past, the manufacturer failed and disable the validation of the signature of the application
- A hacker found it and revealed it years ago at a Chinese conference

- Would you like to play Candy Crush on your terminal ?
  - We found a terminal where the manufacturer gives the user the opportunity to load third party applications on the terminal and to void the PCI clause … but it continues to accept payments ☺

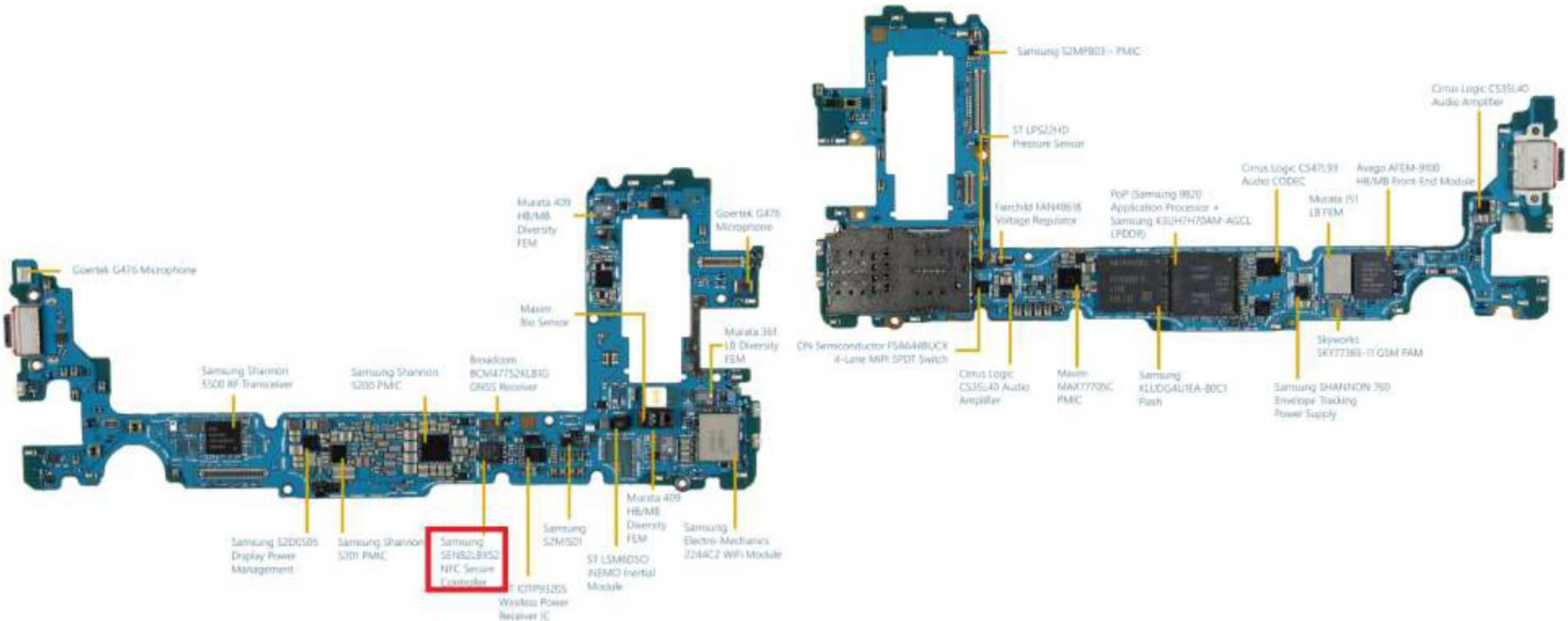
Most recent evolution

When the phone becomes a terminal



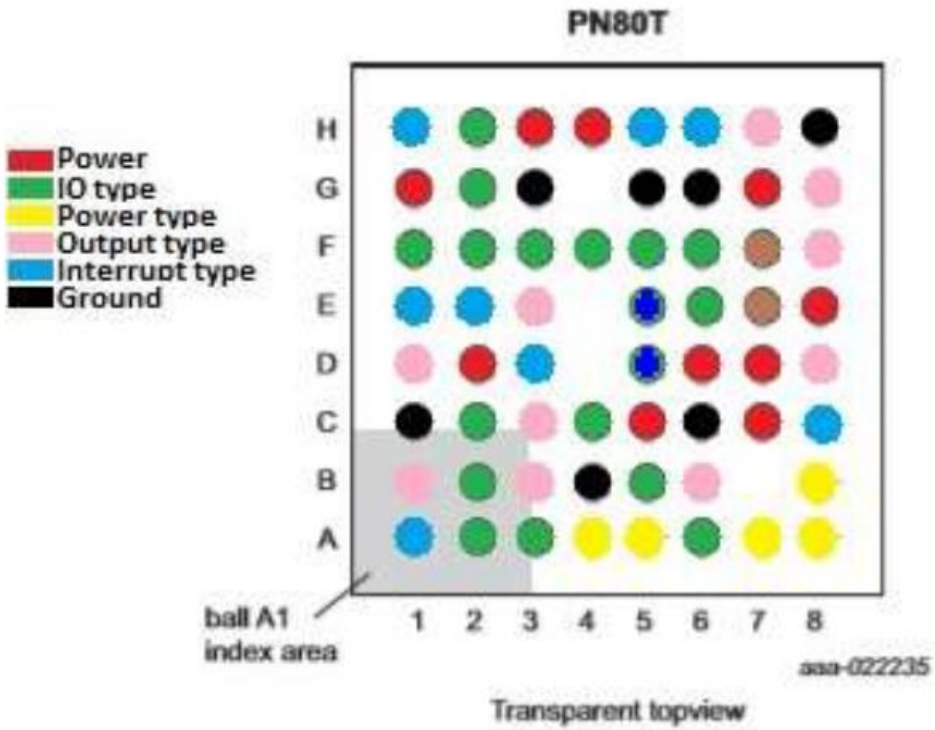
* Figure borrowed from PCI: ***Contactless Payments on COTS (CPoC™) Security and Test Requirementsv1.0 - Dec 2019***

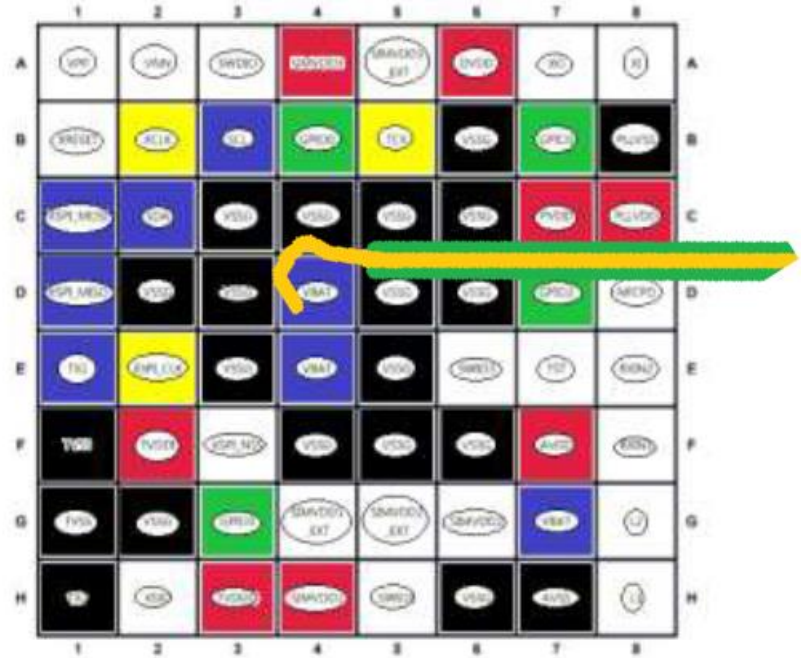
S10+ Tear down by TechInsight



- Historically aligned
  - Smartcards (microcontroller)
  - Trusted Personal Module
  - Secure Element
- System On Chip
- Required to perform:
  - Cryptography
  - Handle sensitive data
  - Ability to perform secure computation
    - Javacard

- EXAMPLE : POSITION OF PADS
- OBJECT : AVOID INSERTION OF A BENT MICROWIRE TO SNOOP ON SENSITIVE SIGNALS OR PREVENT UNSOLDERING





CPOC and MPOC

Core, Mobile and App security

- Objective of Security and assets
- Ecosystem protection
- Security mechanisms (RNG & Entropy, Cryptography and documentation, Authentication, Key management)
- Tampering and reverse engineering: attacks and counter-measures
- White-box crypto, agility and protection
- Crypto assets lifecycle
- App authenticity
- Internal buffers
- Attestation
- Code separation
- Sensors and security
- Special events detection mechanisms
- Documentation

Android & App management

- Android history
- Android architecture and design approach
- App separation and security
- Android tools and app store
- Android's requirements in CPoC
- Device attestation and device management
- App lifecycle (installation, update, revocation)
- Install and first use procedure and requirements
- Uninstall CPOC app procedure

Backend system and monitoring system

- Back end architecture and requirements
- Back end HSM and connection to payment system
- Back end for onboarding of mobile phone or tablet
- Back end monitoring systems
- Back end Front end interactions
- Main events to be detected and logged
- Communication types and security
- Reporting frequency, trigger events and format
- Attack detection
- What to expect from the back end

Backend system and monitoring system

- Back end architecture and requirements
- Back end HSM and connection to payment system
- Back end for onboarding of mobile phone or tablet
- Back end monitoring systems
- Back end Front end interactions
- Main events to be detected and logged
- Communication types and security
- Reporting frequency, trigger events and format
- Attack detection
- What to expect from the back end

The end

Let’s take it easy …

Thanks for your attention