Research at Google

Attacking encrypted USB keys the hard(ware) way

Jean-Michel Picod, Rémi Audebert, Sven Blumenstein, Elie Bursztein
with the help of many Googlers

13.6%

Of USB drives storing company data are lost or stolen

Are encrypted USB drives really hacker proof?

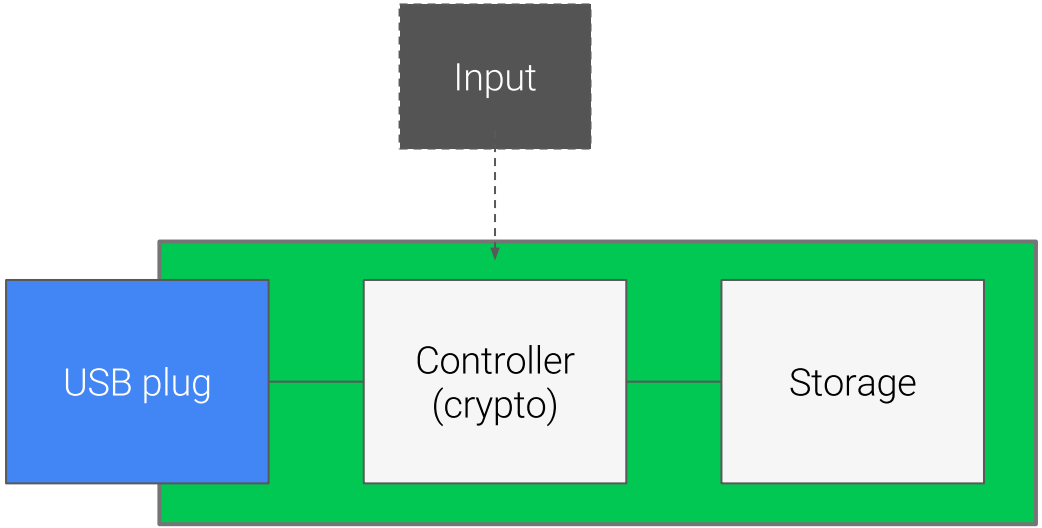
How to audit encrypted drives

Show-case real attacks found while auditing

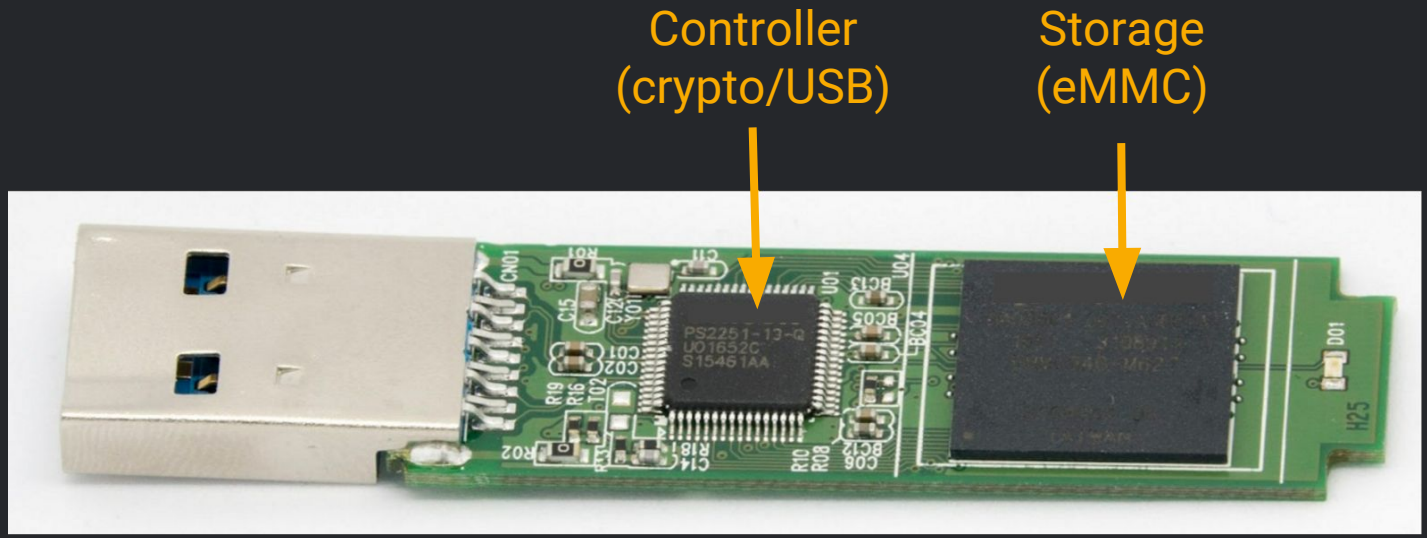
On-going research ahead

Encrypted USB key inner working

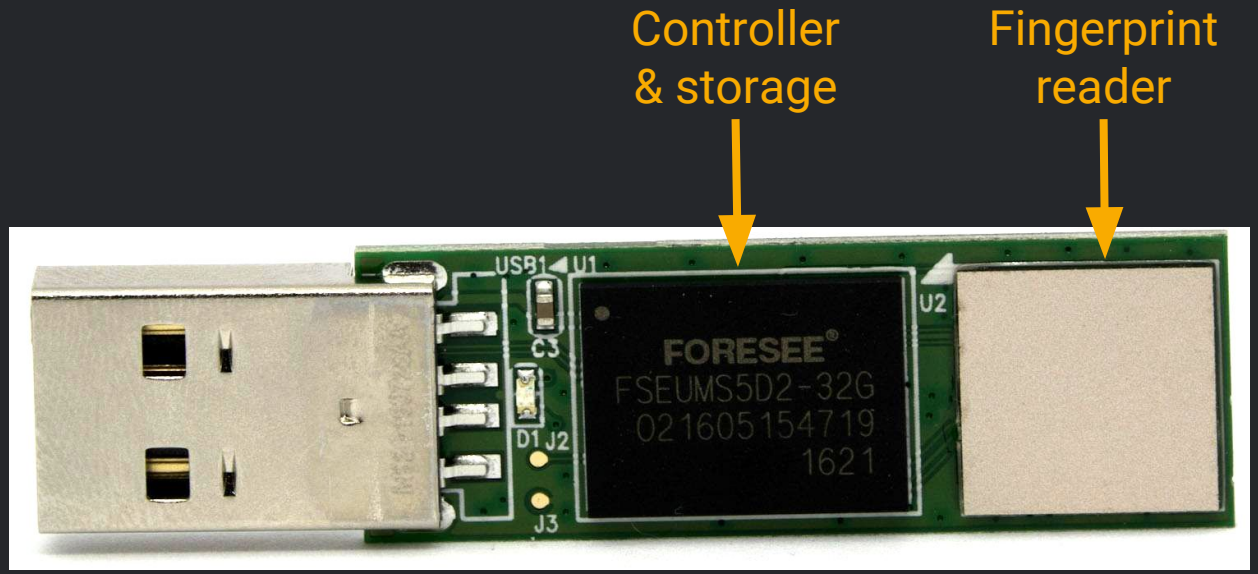
Logical view of a secure USB key

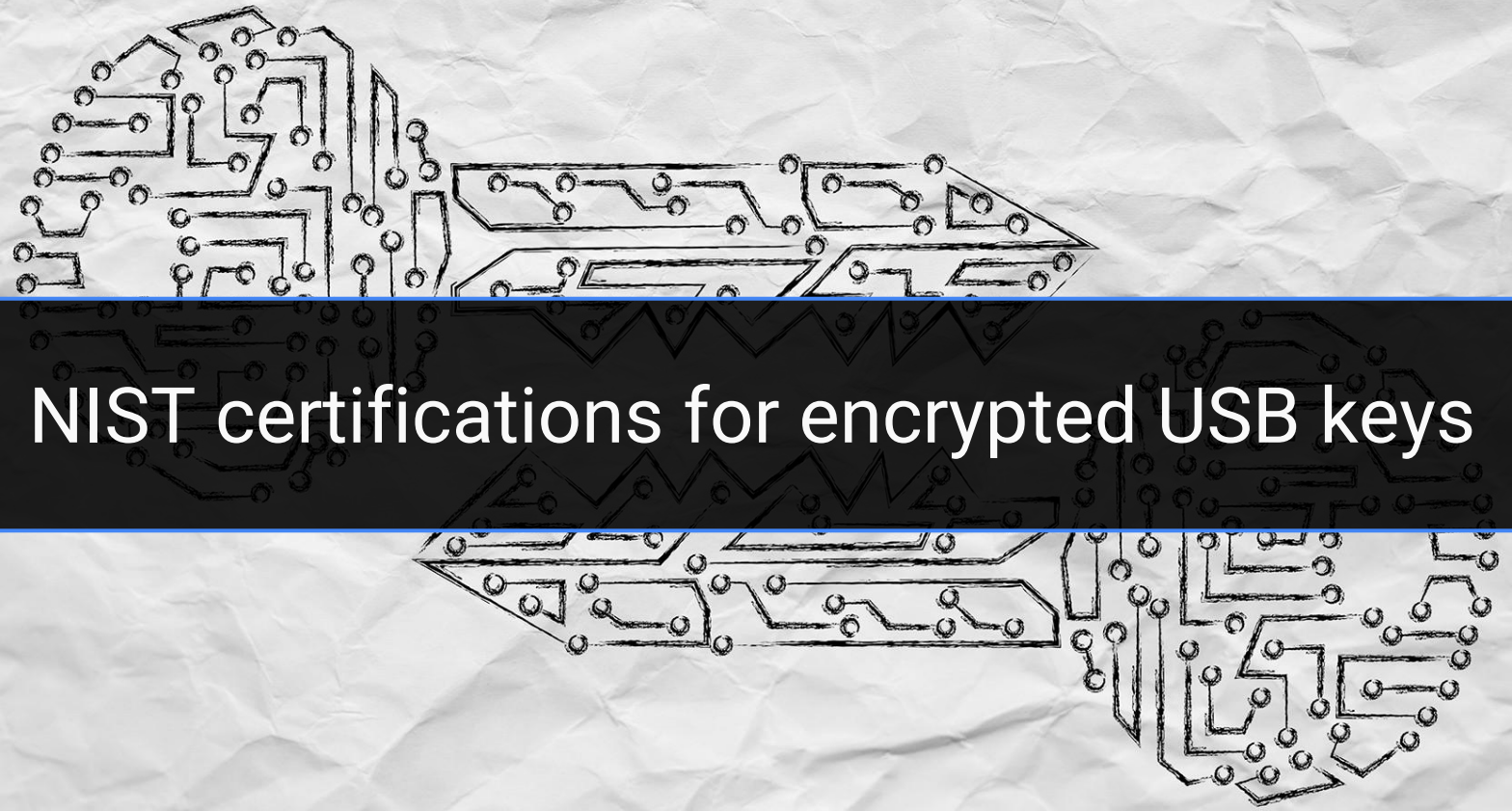


Key with controller and memory separated



Integrated key





NIST certifications for encrypted USB keys

FIPS certifications

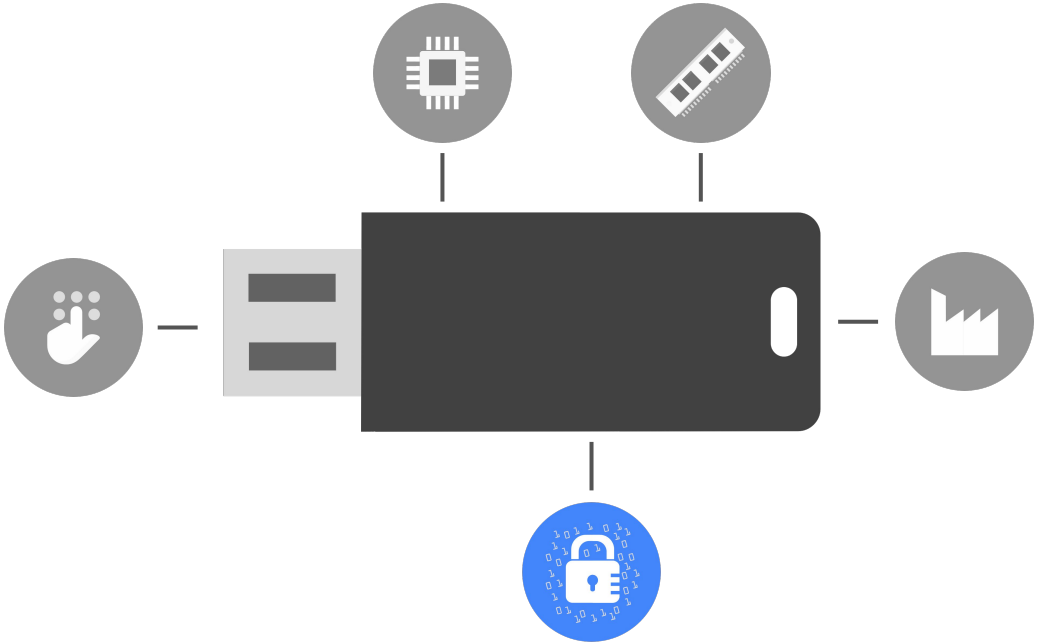
FIPS 140

Cryptographical security disclosure & validation process

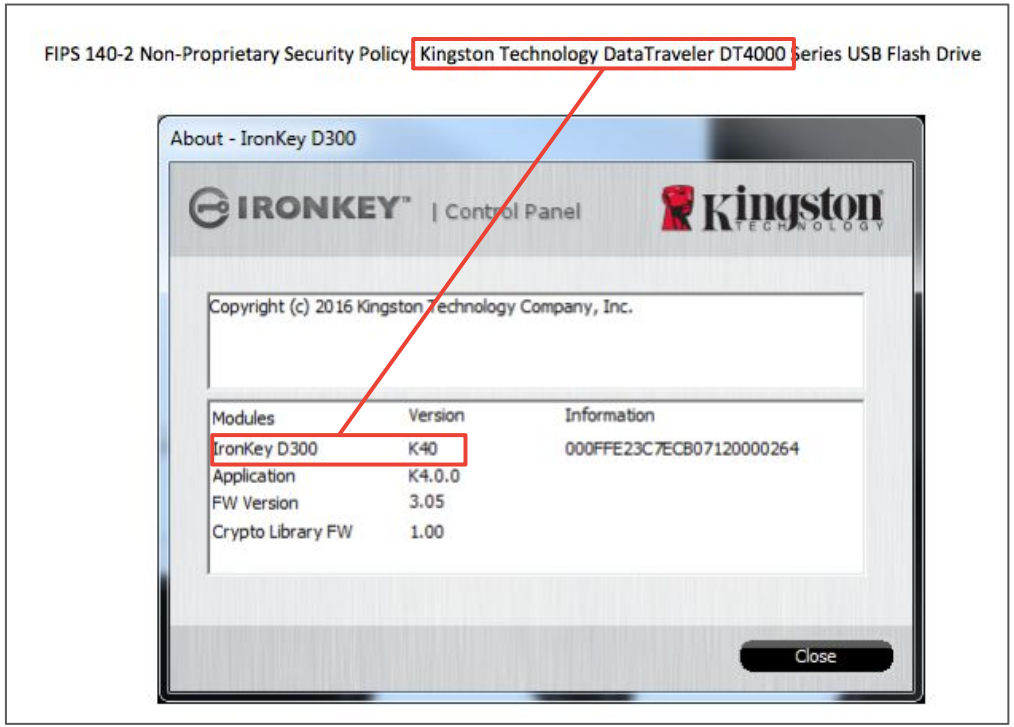
FIPS 197

Fancy way to write AES ;)

FIPS 140 scope in a nutshell



One of the many FIPS certification fails



Audit methodology

Attacker type

Serendipitous

Opportunistic attacker with minimal resources

Professional

Attacker with resources, albeit limited

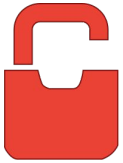
State sponsored

After specific data/keys that are worth a large investment

Attack impact

Weaken security

Makes carrying attack easier

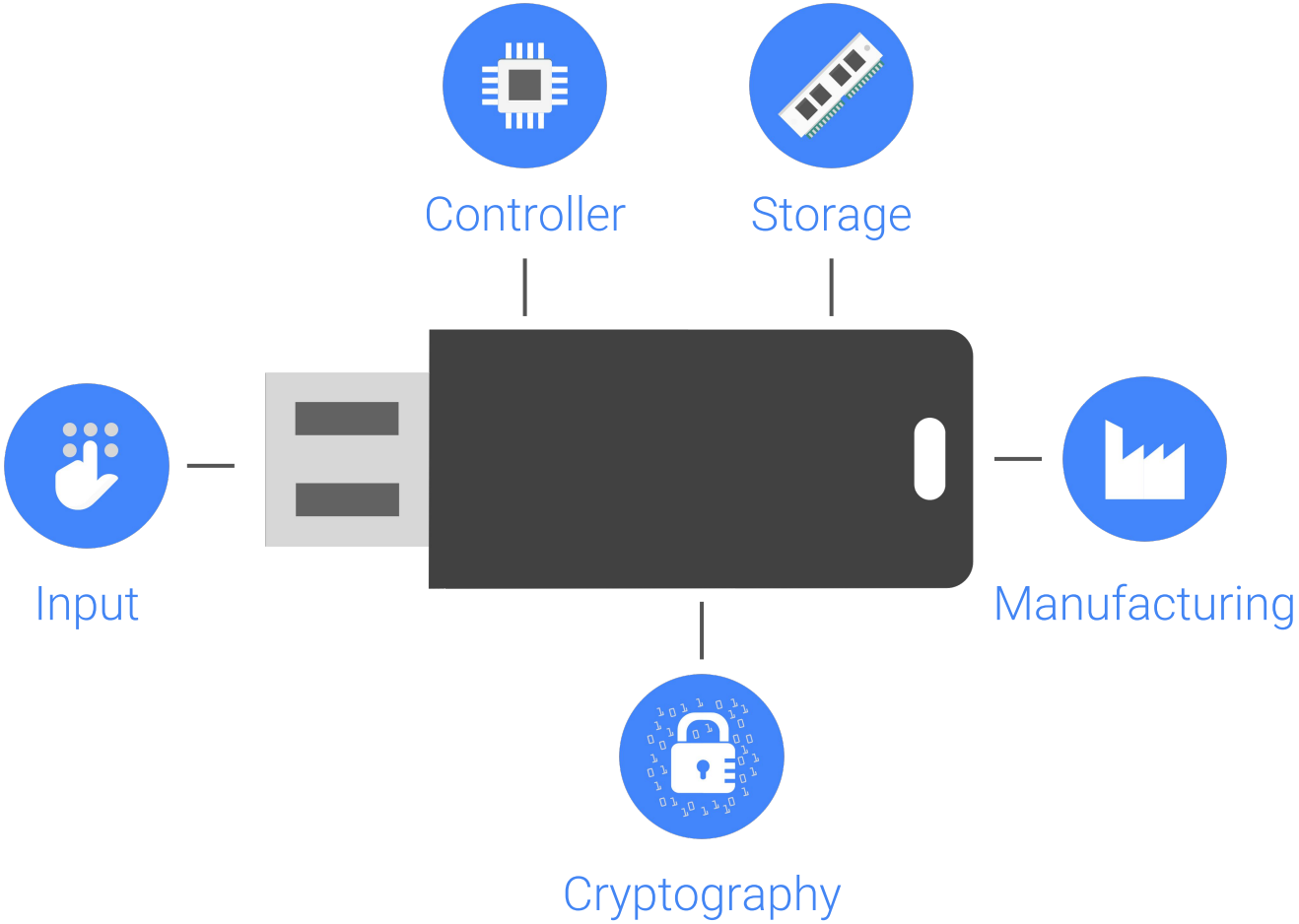


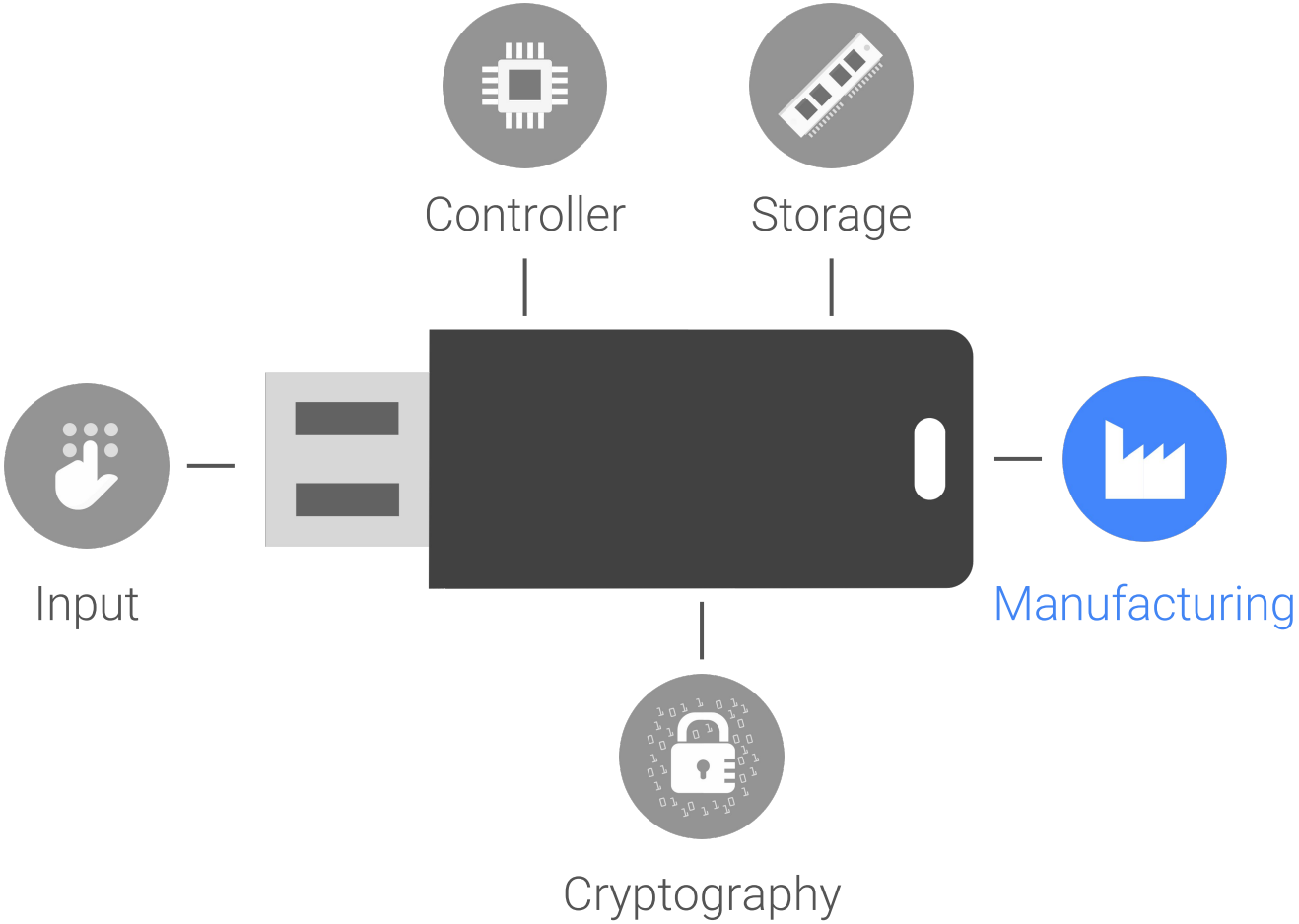
Single drive break

“Only” allowed to recover a single drive data

Full break

Recovery attack that affects all drives


Controller
Storage
Input
Manufacturing
Cryptography


Controller
Storage
Input
Manufacturing
Cryptography

Defensive manufacturing key goals

Mitigating hardware attacks

Slowdown initial analysis and prevent physical tampering & counterfeit

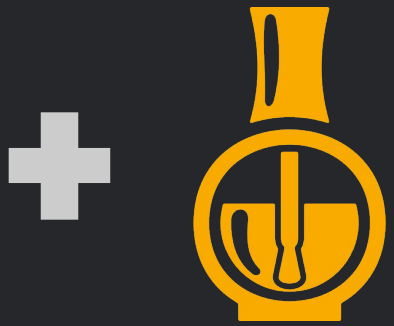
Preventing advanced attacks

Defend against very targeted attack: e.g TEMPEST, EVIL MAID

TEMPEST prevention via copper shielding

Mitigate component extraction with epoxy

Fake epoxy insecurity



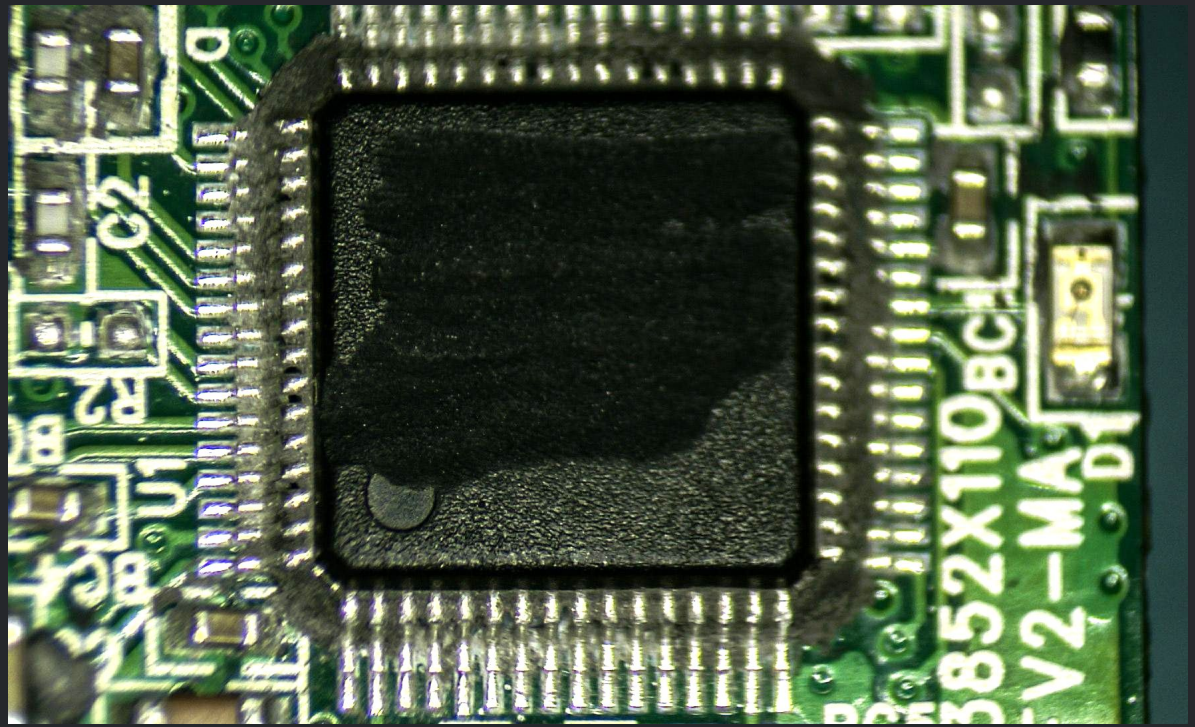
NIST evaluation fail

[redacted] PLC. - [redacted] (Underlying Steel Chassis) and [redacted] Plus (Underlying Steel Chassis)

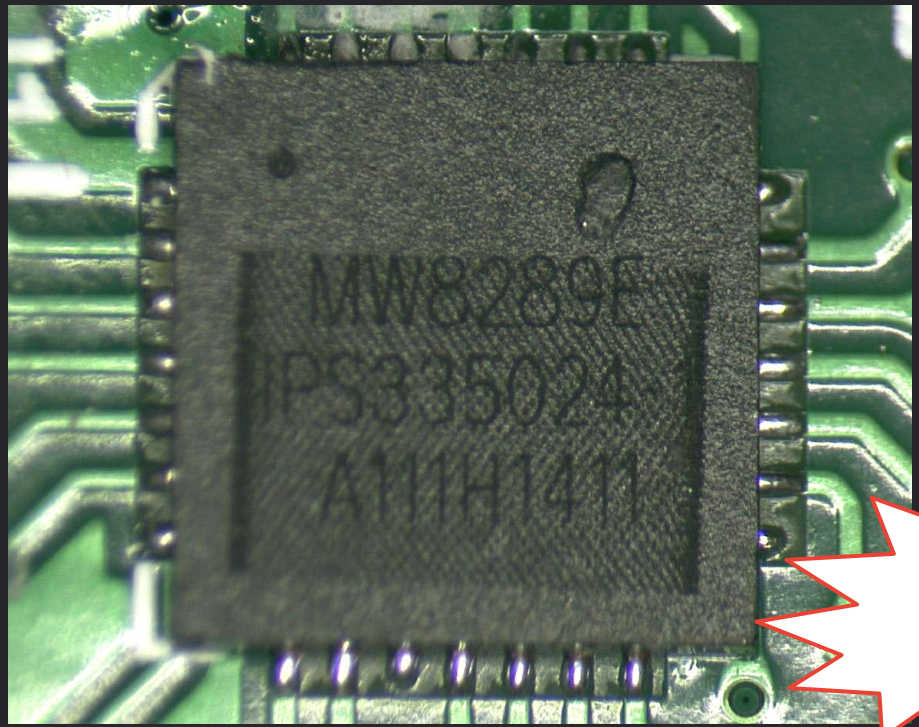
5 PHYSICAL SECURITY

The cryptographic boundary for the modules is defined as all components within the steel chassis only. All components are coated in epoxy and encased in the steel chassis. The rubber sleeve material which surrounds the steel chassis is not considered part of the cryptographic boundary, and has been excluded from the FIPS 140-2 requirements on the basis that it contributes nothing to the module's security. The modules do not have removable doors or cover[redacted] They [redacted] components with integrated circuit packaging that is production grade using standard passivation within the visible spectrum.

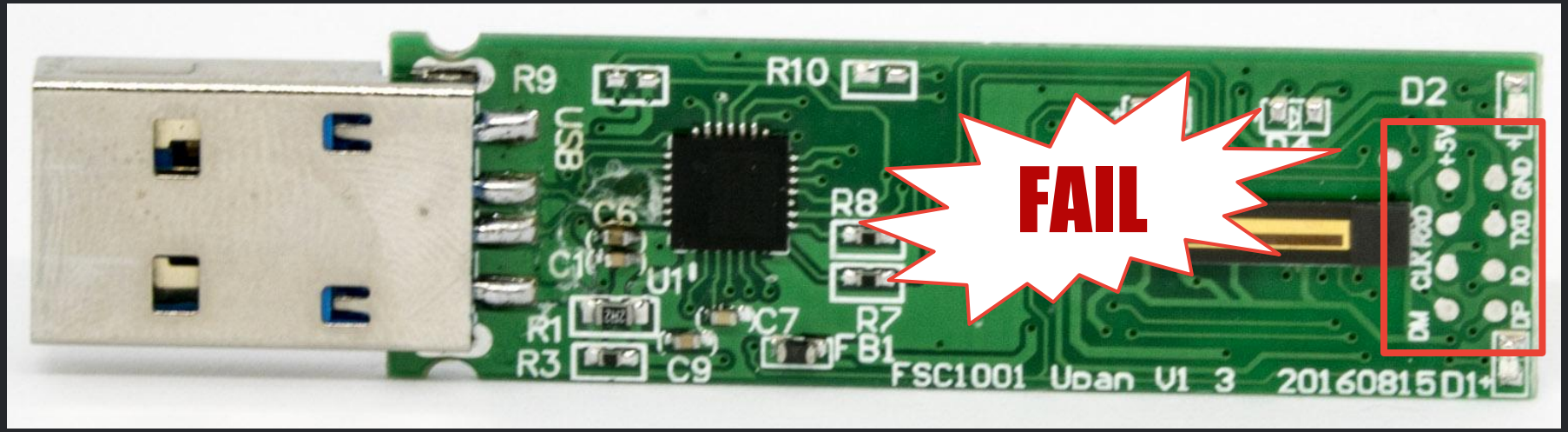
Etching



Etching failed



Leaving debug ports active



Defensive manufacturing criteria

Device is tamper evident		
PCB is dipped in epoxy to make extraction harder		
Hardware components marking & serial numbers are erased		
Firmware must be properly signed or read-only		
PCB is shielded in copper to prevent TEMPEST attack		
Device is counterfeiting resistant		
Encryption key is wiped out upon tampering		

 Serendipitous

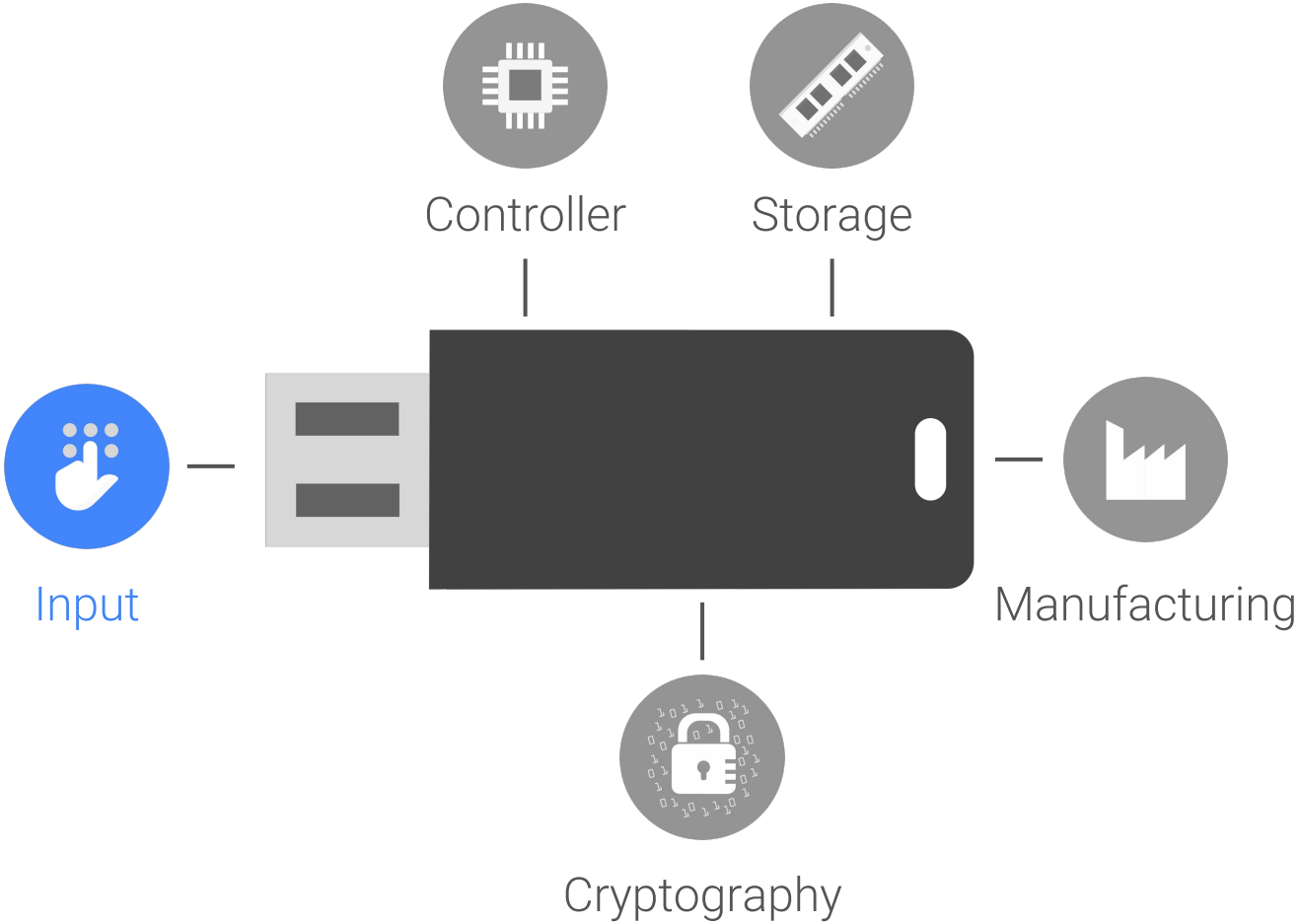
 Professional

 State sponsored

 Weakness

 Single drive break

 Full break


Controller
Storage
Input
Manufacturing
Cryptography

Input mechanism key security goals

Identifying users accurately

Only valid users should be recognized

Securing credential enrollment

Prevent rogue identifiers (fingerprint/badges) to be enrolled

Pinpad

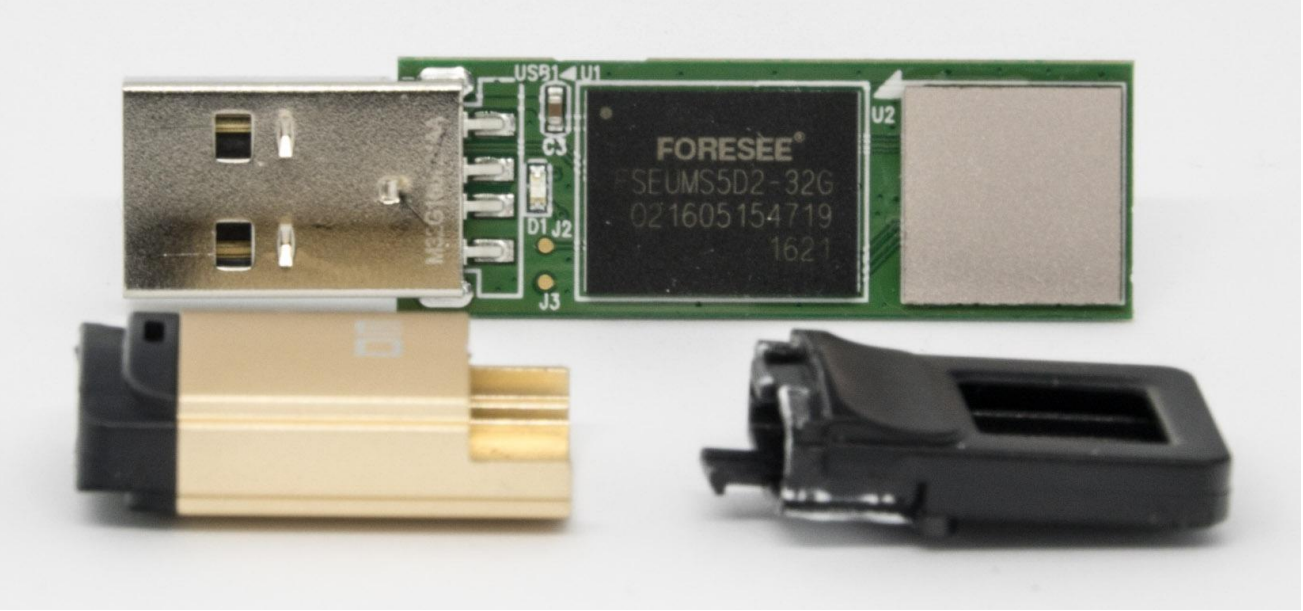
Pinpad

Badge

Badge
(RFID/NFC)

Fingerprint

Fingerprint reader



Software

Software

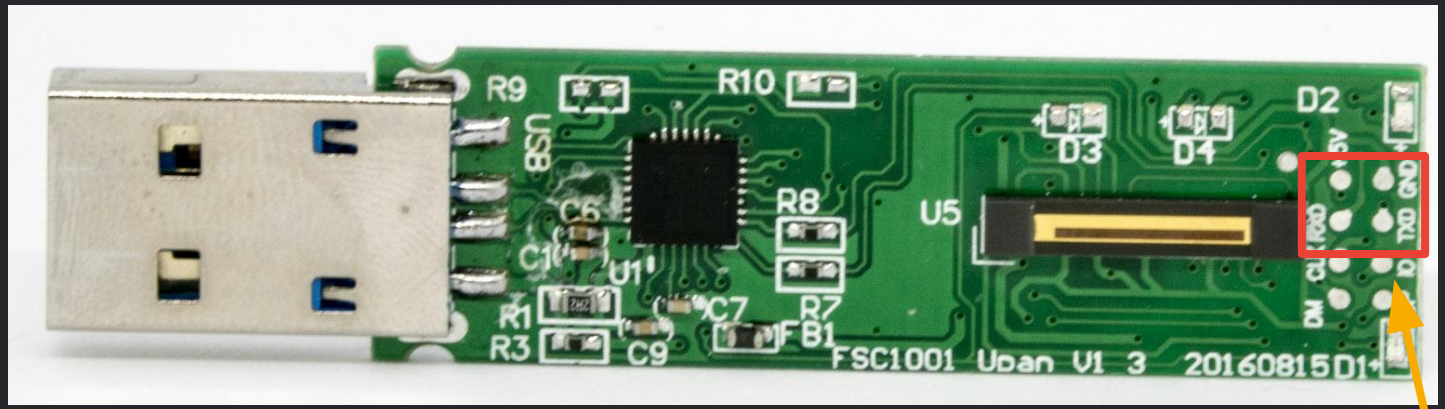
Unlock command can be replayed

Target		Fingerprint key 1
Impact		Full break
Attacker		Professional

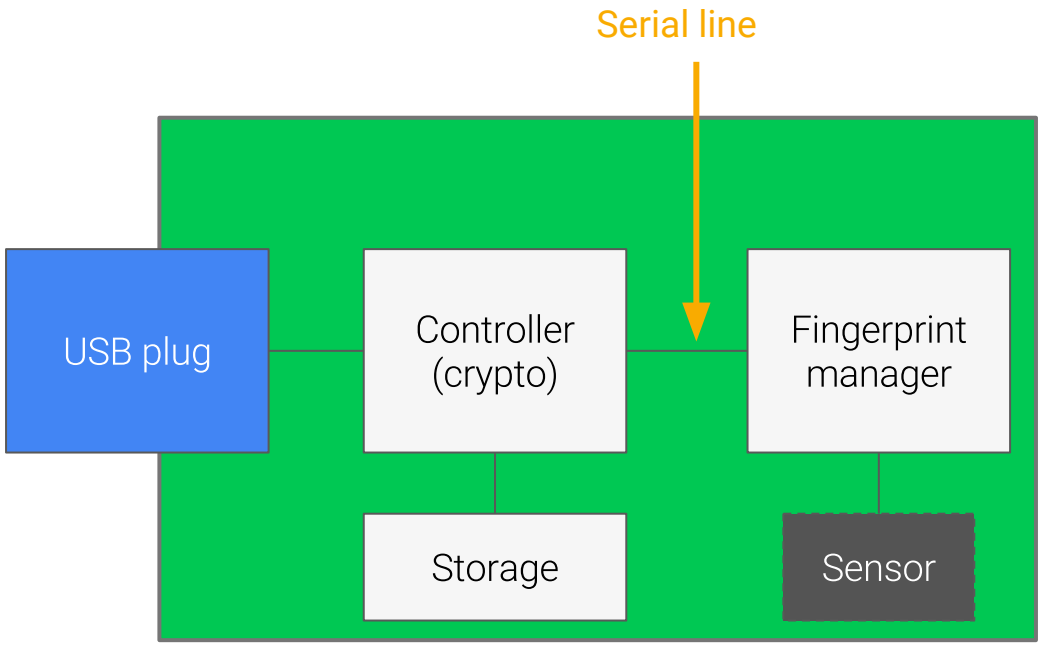
Unlock command replay attack against software based key found in 2010

Vulnerable key

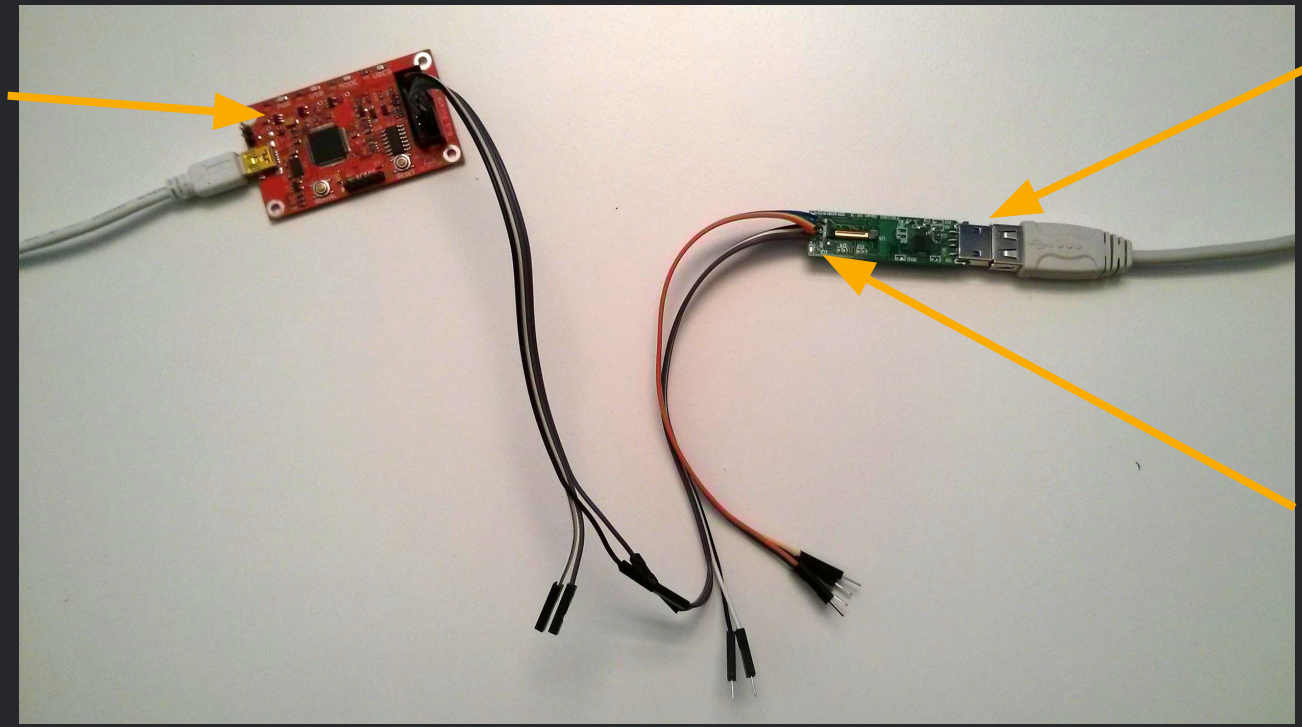
Vulnerable key internal



Identification command flow through serial line



Attack setup



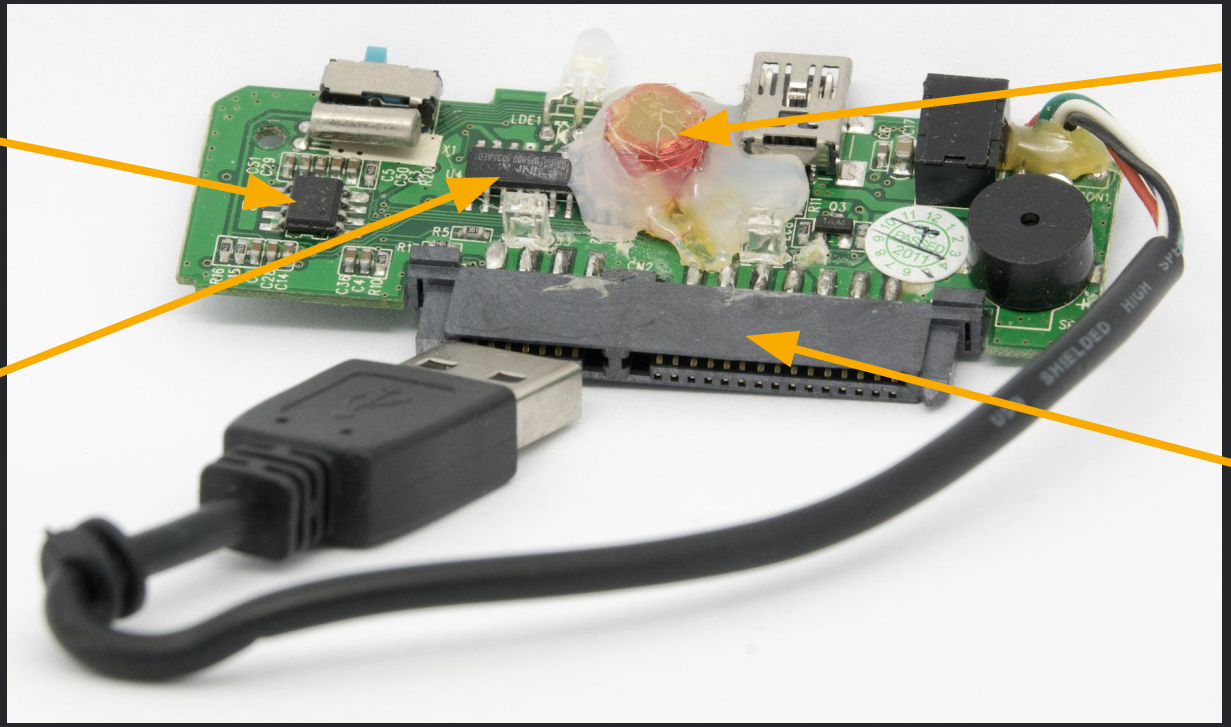

UART>0x3a 0x04 0x00 0x00 0x00 0x02 0x3c 0x00 0x00 0x8

Input can be cloned

Target		HDD with badge
Impact		Single drive break
Attacker		Professional

Vulnerable device

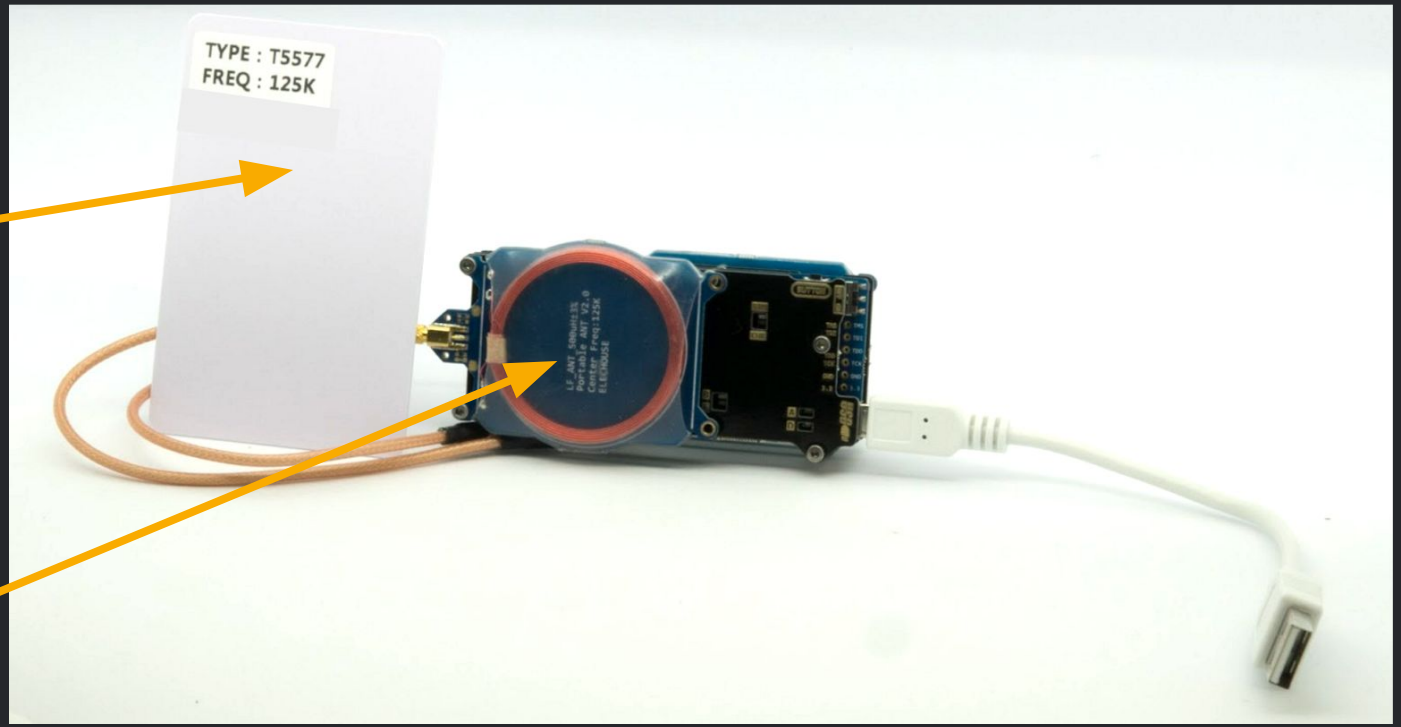
Vulnerable device internal



Cloning equipment

Reprogrammable RFID tag

Proxmark3




U#1
Badge is dumped
Using standard 125KHz reader

Input audit criteria

Pin is not stored in software		
Unlock command can't be replayed		
Keypad don't show obvious sign of wear and tear		
Input (e.g tag, fingerprint) can't be cloned		
Debug ports are disabled		

 Serendipitous

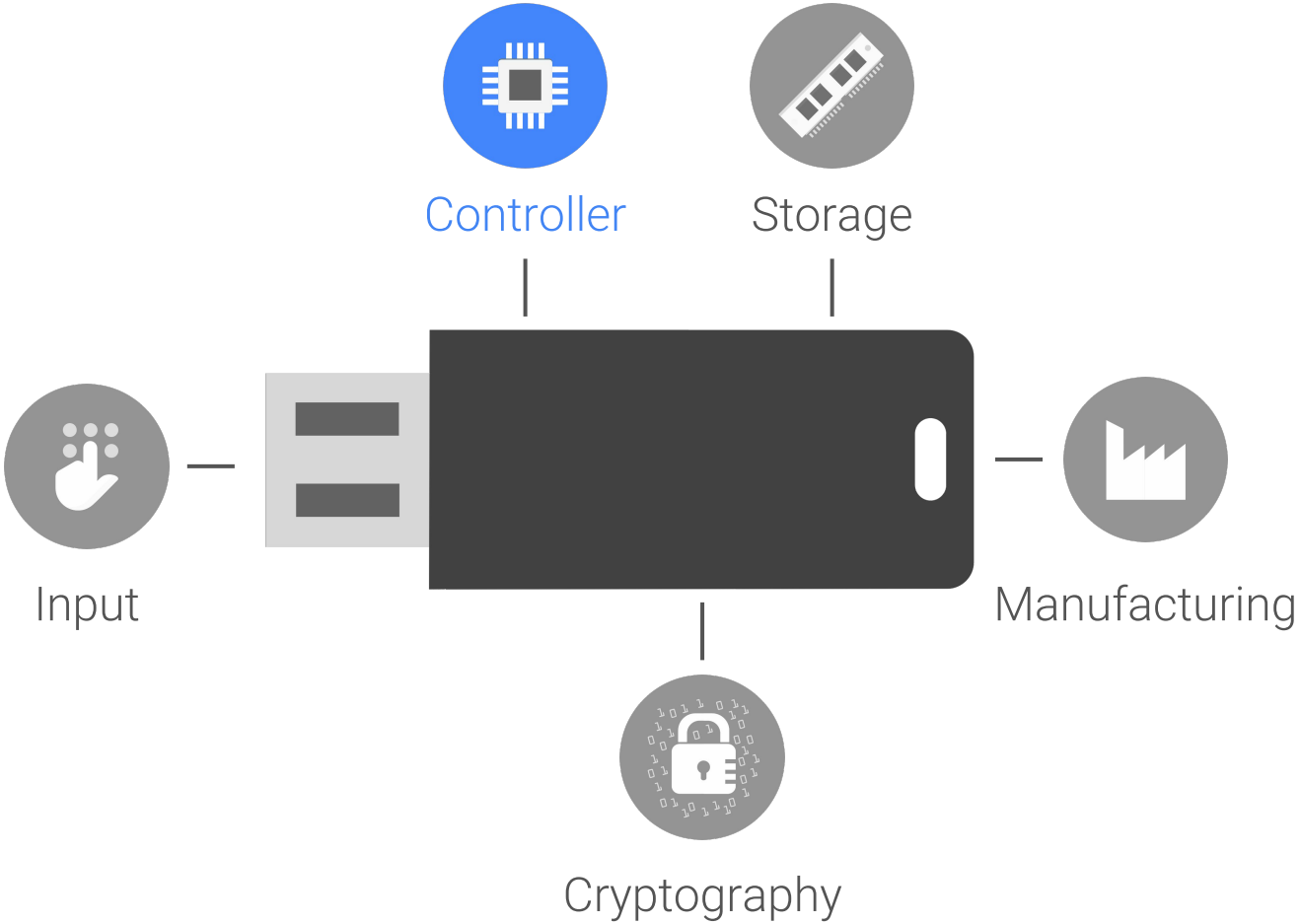
 Professional

 State sponsored

 Weakness

 Single drive break

 Full break


Controller
Storage
Input
Manufacturing
Cryptography

Controller security key goals

Protect secrets

Pin hash and AES key must be non recoverable

Lock the drive when needed

Ensure that data is only accessed in safe circumstances

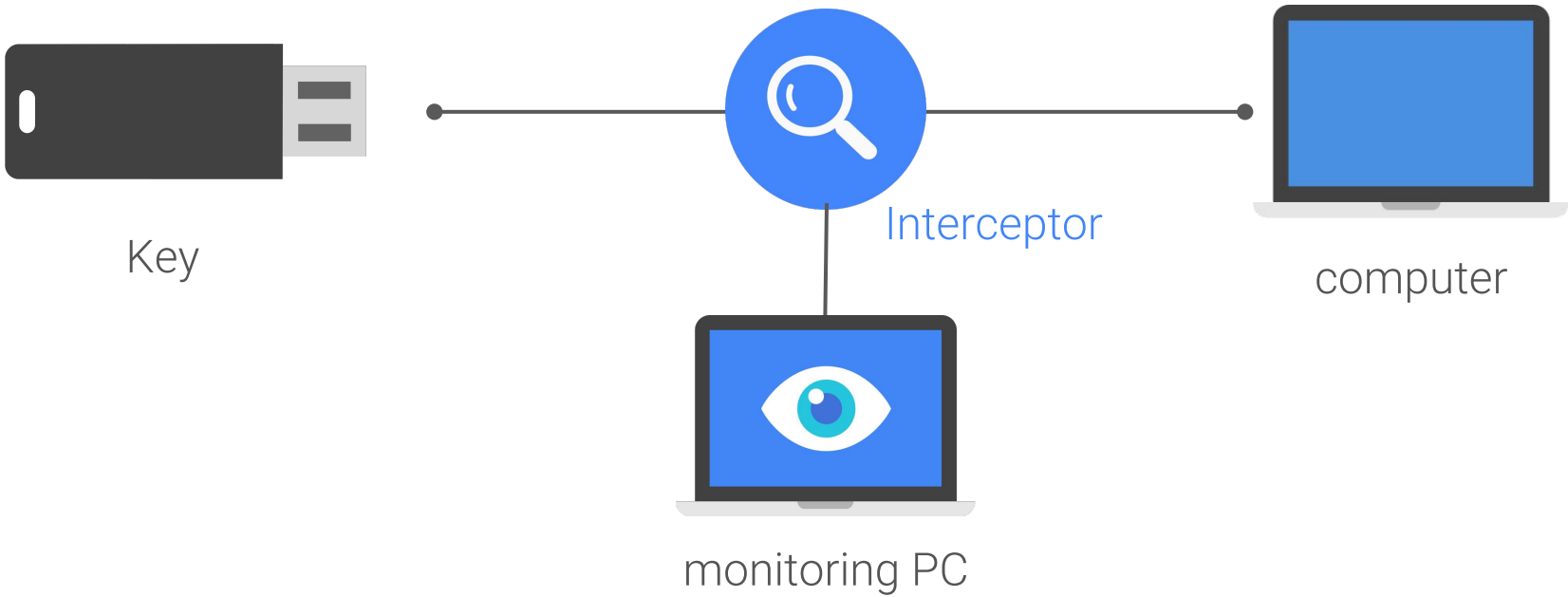
Destroy secrets when attacked

Make the drive unusable in case too many attempts are made

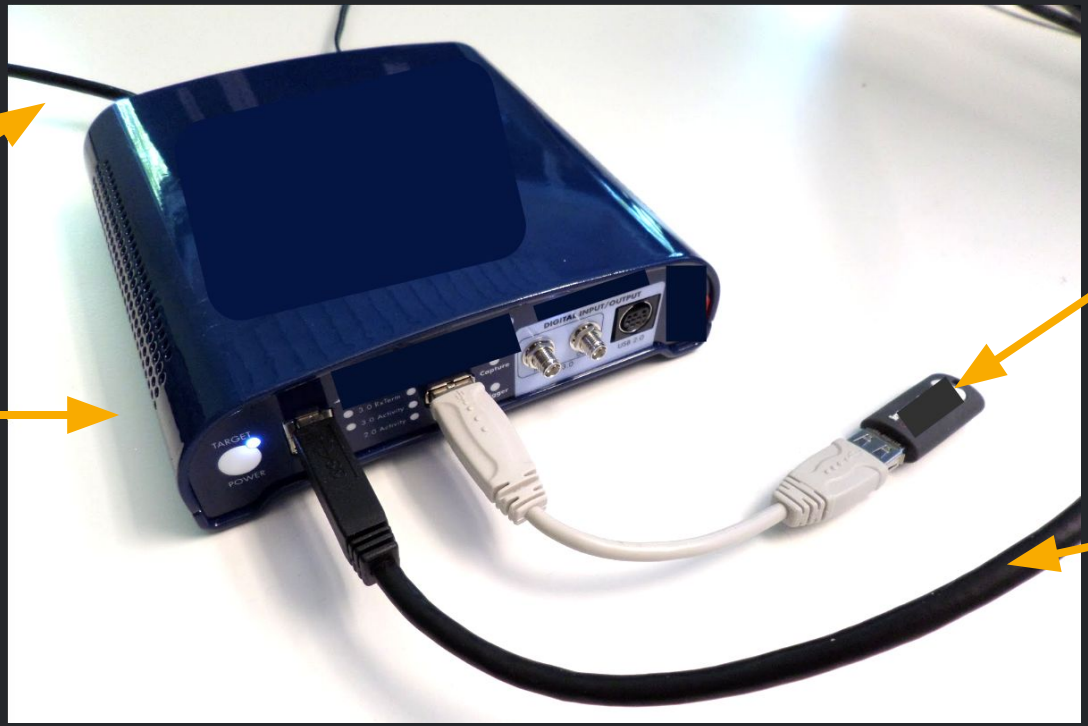
Firmware attestation

Ensure that the firmware used is really the one disclosed

USB communication interception



Interception in practice

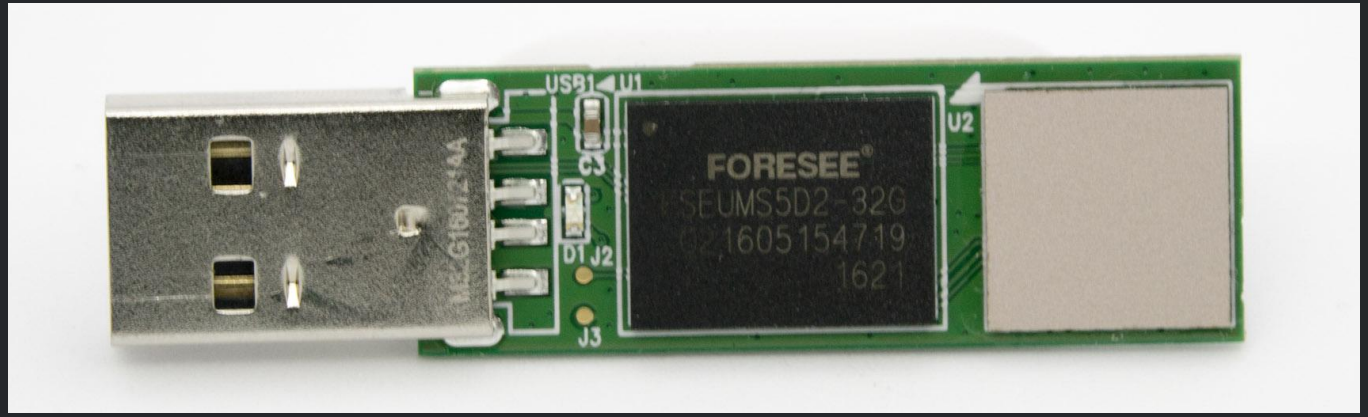


Password can be extracted

Target		Fingerprint key 2
Impact		Full break
Attacker		Serendipitous

Vulnerable key

Key internals



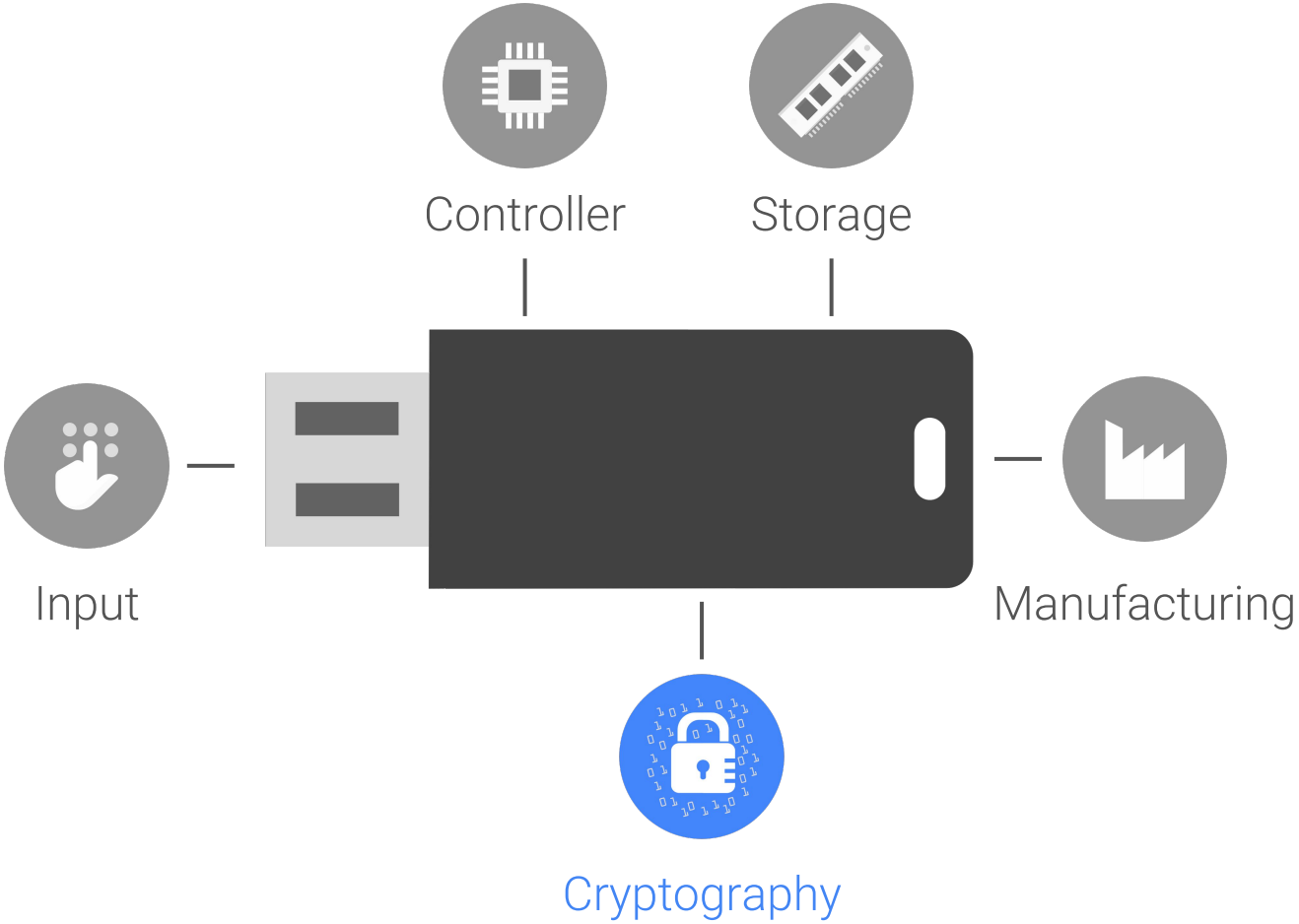
Input can be brute-forced

Target		HDD with badge
Impact		Full break
Attacker		Serendipitous

Vulnerable badge

Controller audit criteria

Device is burned out after nth unsuccessful attempts		
Password & AES key can't be requested		
AES Key is regenerated upon drive reset		
Device immediately lock itself when removed from USB port		
Device lock itself after inactivity period		
Device immediately lock itself after a USB reset		
Encryption key is zeroed when the device is burnt		
Data is zeroed out when the device is burnt		


Controller
Storage
Input
Manufacturing
Cryptography

Cryptography key goals

Data is properly encrypted (duh!)

State of the art encryption with proper initialization and settings

Encryption keys are truly random

Each drive have a unique key that is not predictable

Cryptography audit on hardware complexity

Black box (literally!)

Algorithms are baked in the silicon

Most tests are too expensive in current setting

Audit can only catch the most blatant errors

Use outdated crypto

Target		Password protected key
Impact		Single drive break
Attacker		State sponsored

A few examples we came across

RSA-512 used to communicate on USB port

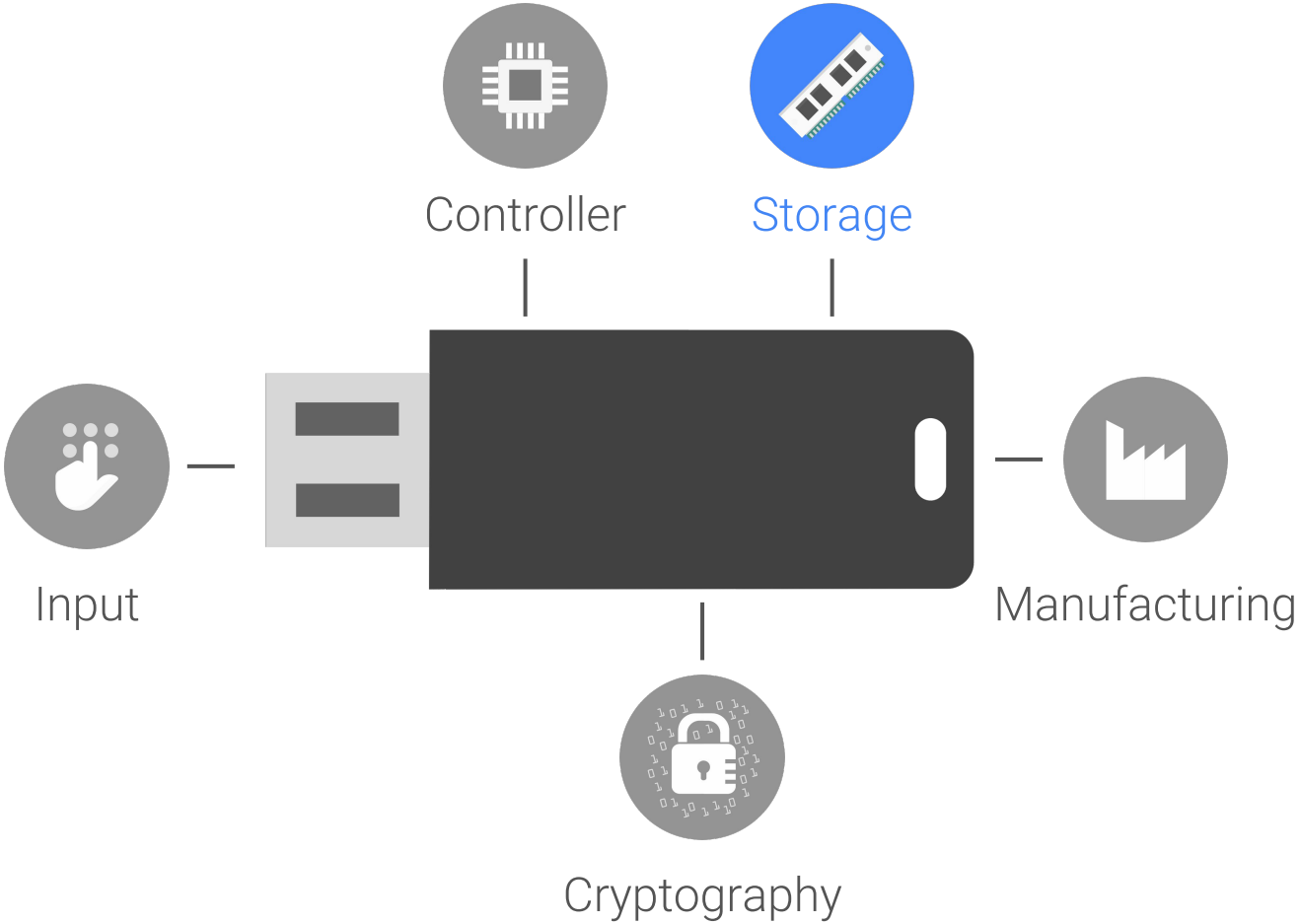
Open the door to factoring attacks

RC4 to encrypt files

Broken cipher

Encryption audit criteria

Encryption key is unique per device		
There is no recovery/master key		
Encryption key derivation use PBKDF2 algorithm with enough round		
Encryption key is randomly generated		
A secure random generator is used		
Data is encrypted with AES or newer standard		
IV are properly randomized		
Encryption chaining algorithm is secure		


Controller
Storage
Input
Manufacturing
Cryptography

Storage goals

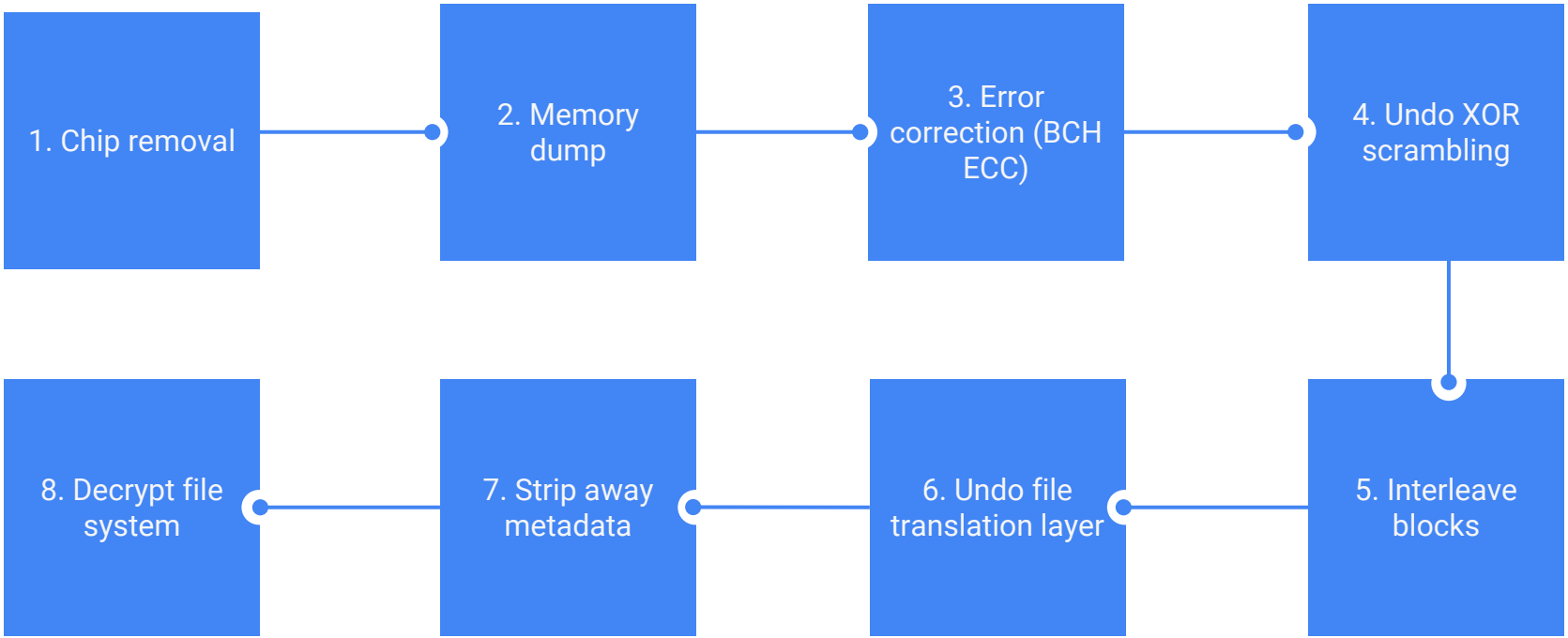
Full encryption

Everything including data, configuration, software should be encrypted

Integrity

Storage tampering should be detected

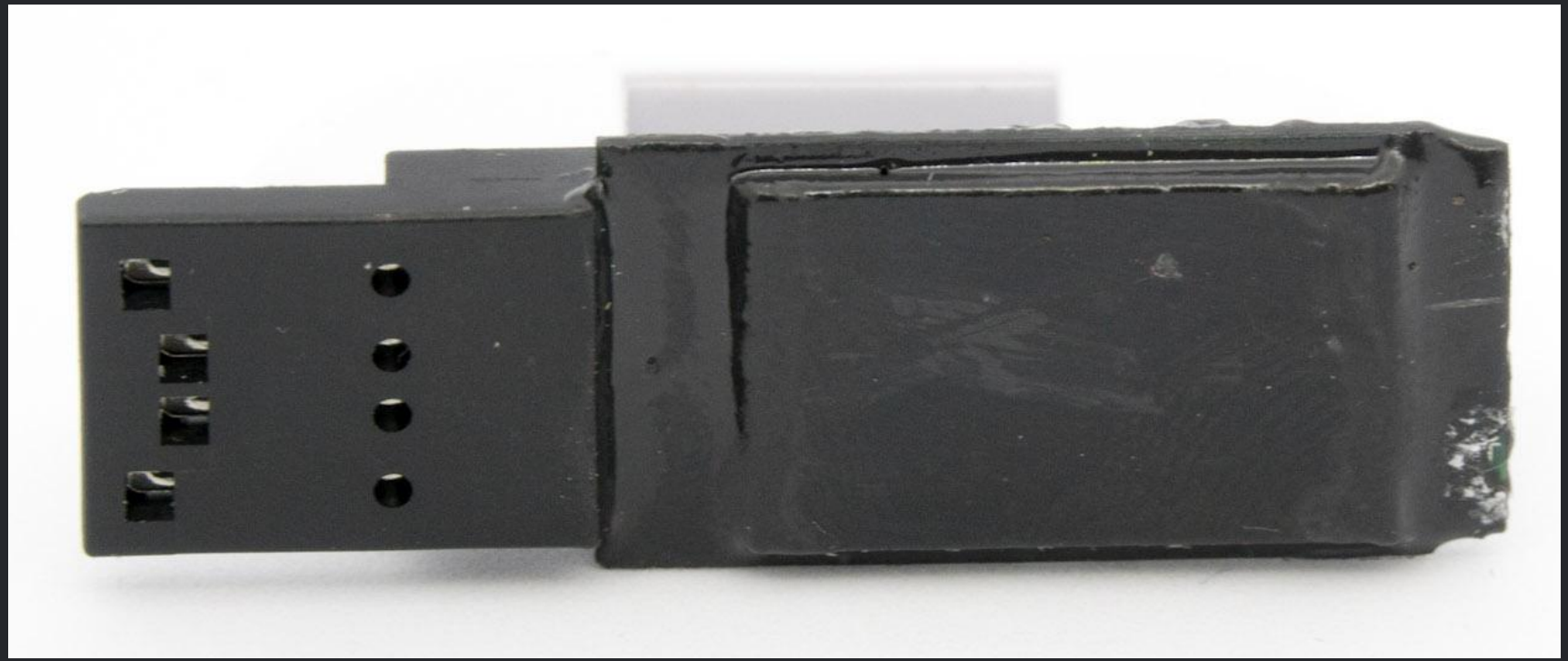
Extracting memory content - not that easy ^^



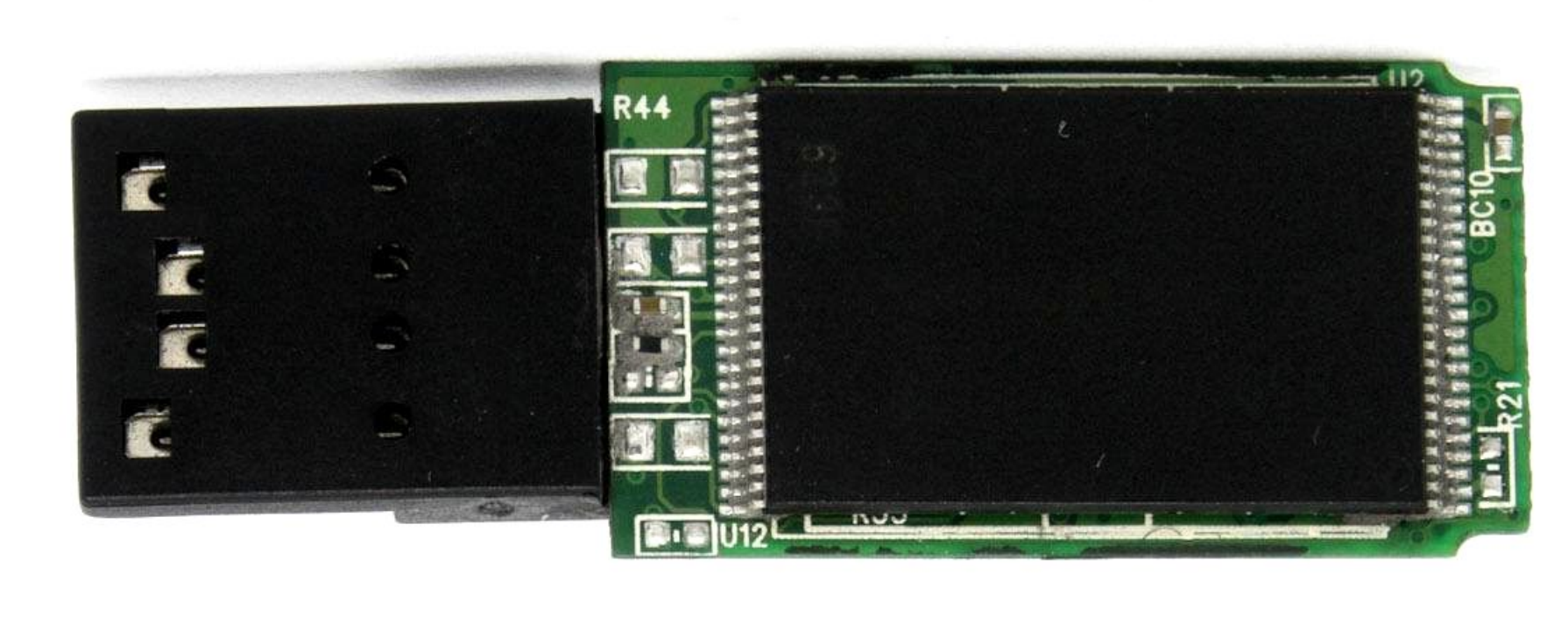
CD-ROM partition can be backdoored

Target		Password protected key
Impact		Single drive break
Attacker		State sponsored

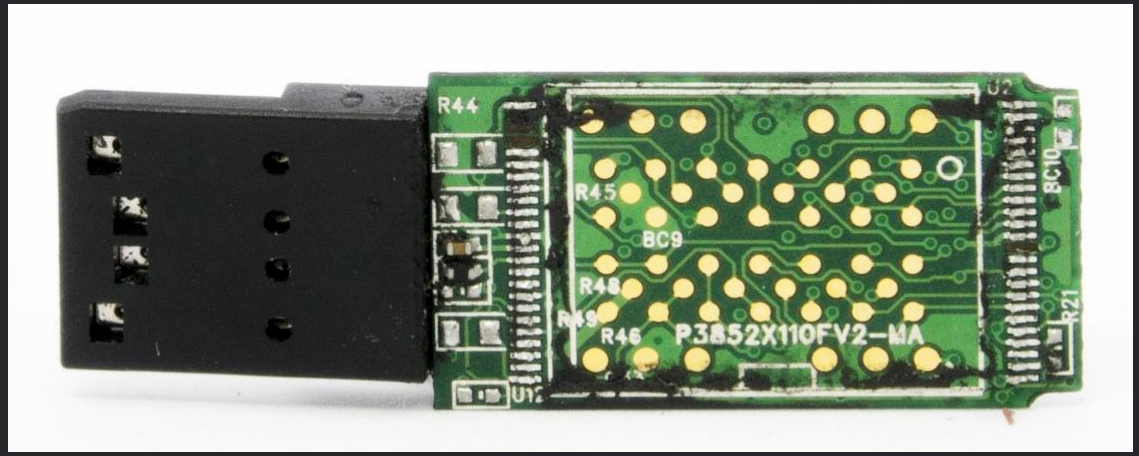
After removing the metal enclosure



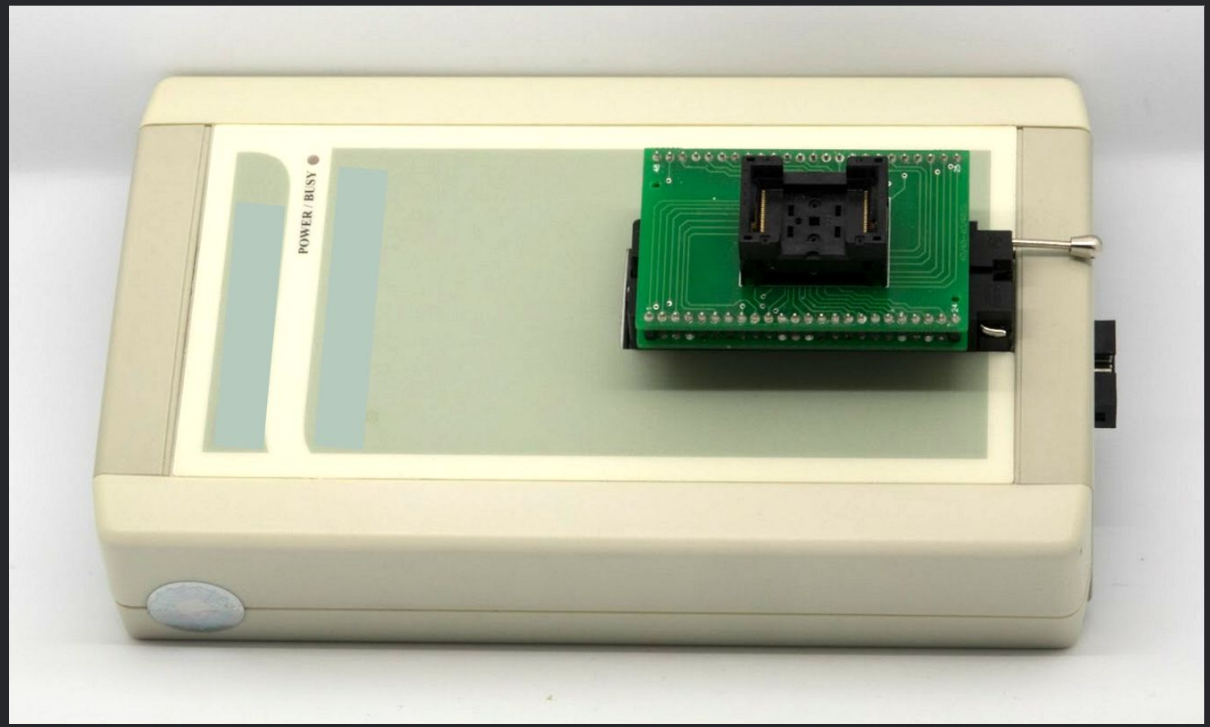
Epoxy removed



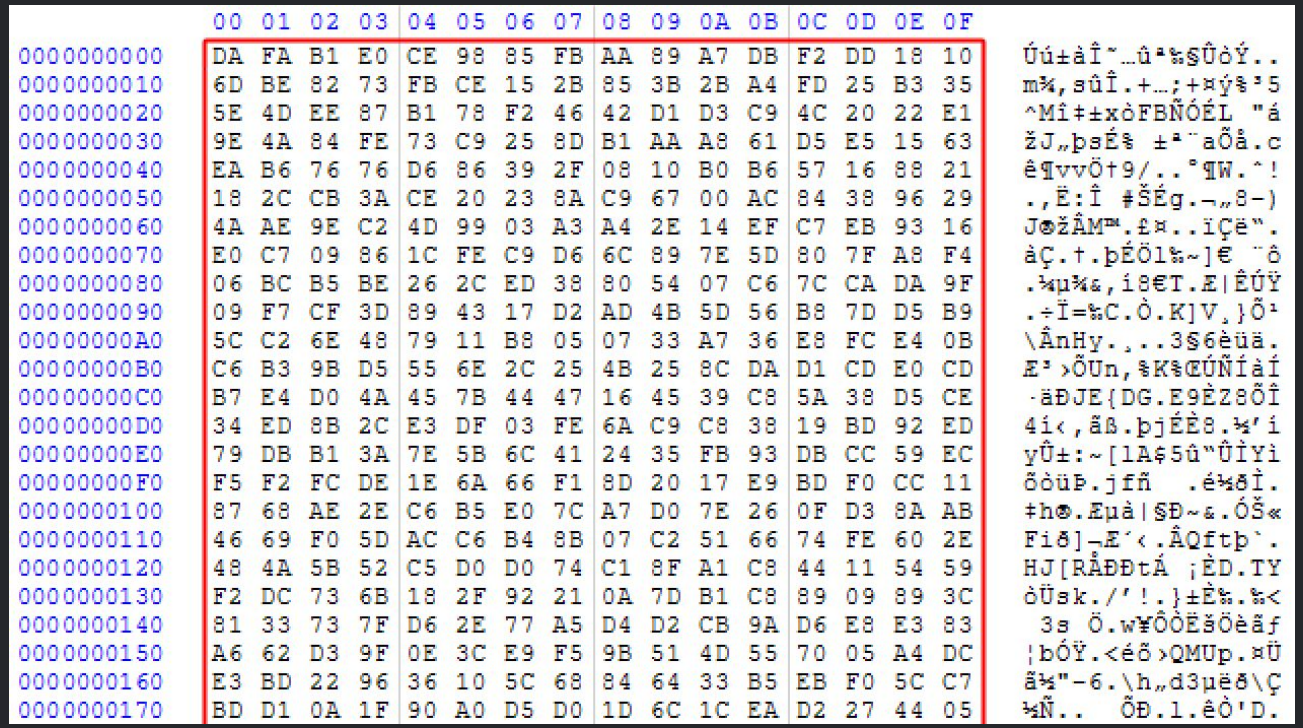
Chip-off



Memory dump

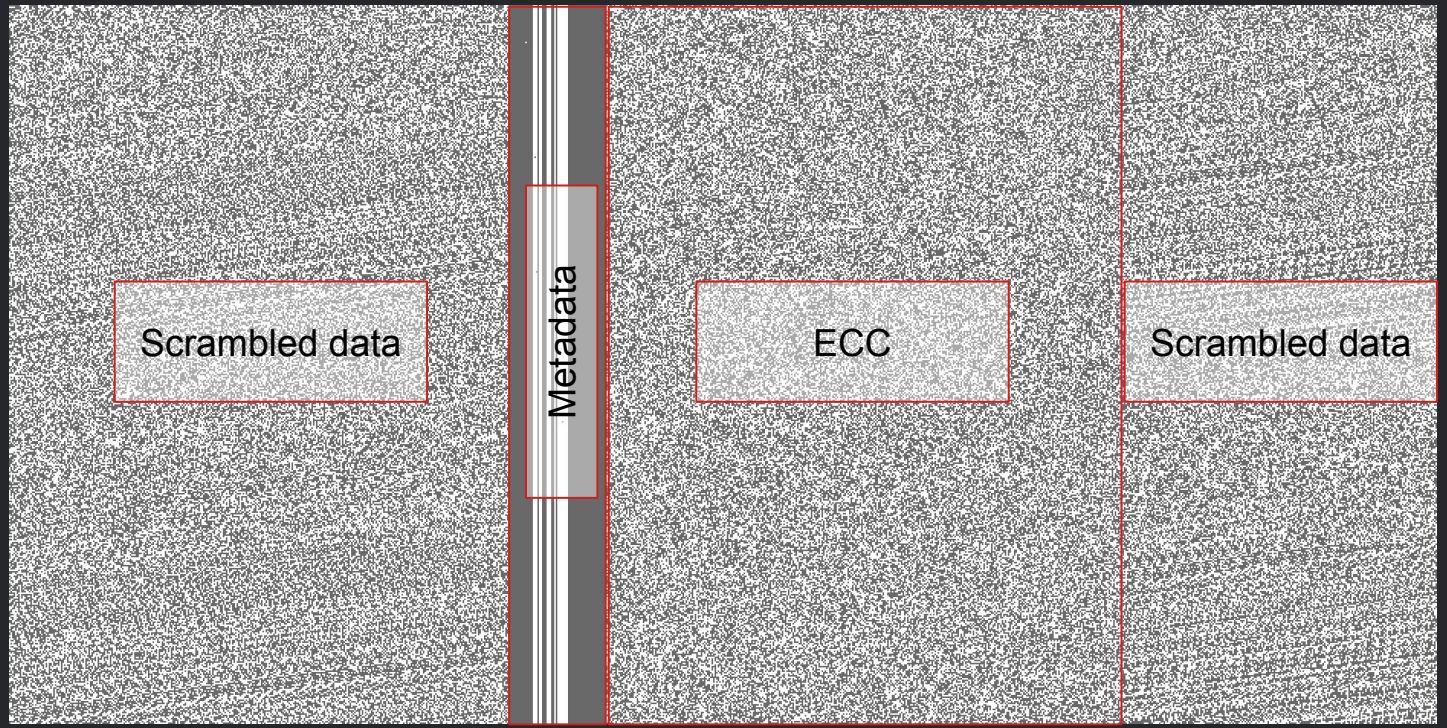


Hexdump of the raw dump

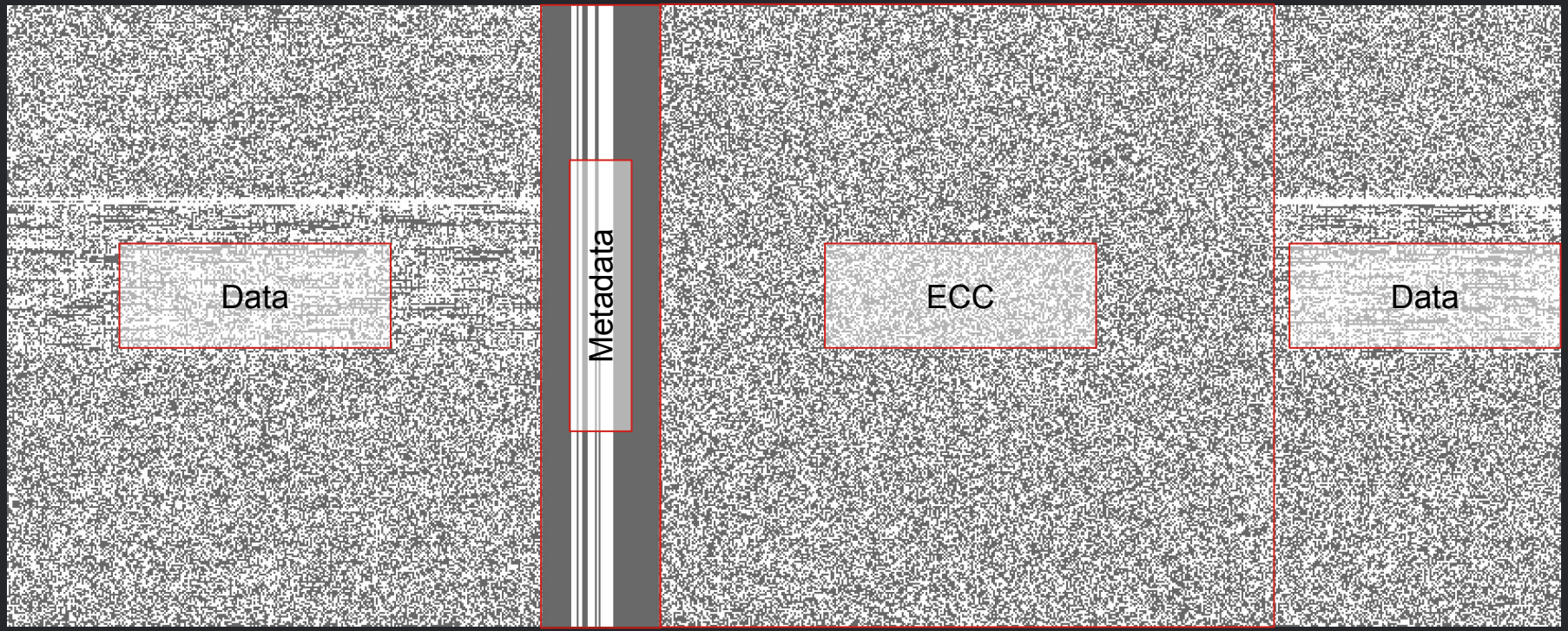


	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
0000000000	DA	FA	B1	E0	CE	98	85	FB	AA	89	A7	DB	F2	DD	18	10	Úú±àÎ˜…û ª‰§ÛòÝ..
0000000010	6D	BE	82	73	FB	CE	15	2B	85	3B	2B	A4	FD	25	B3	35	m¾‚sûÎ.+…;+¤ý%³5
0000000020	5E	4D	EE	87	B1	78	F2	46	42	D1	D3	C9	4C	20	22	E1	^Mî‡±xòFBÑÓÉL "á
0000000030	9E	4A	84	FE	73	C9	25	8D	B1	AA	A8	61	D5	E5	15	63	žJ„þsÉ% ±ª¨aÕå.c
0000000040	EA	B6	76	76	D6	86	39	2F	08	10	B0	B6	57	16	88	21	ê¶vvÖ†9/..°¶W.ˆ!
0000000050	18	2C	CB	3A	CE	20	23	8A	C9	67	00	AC	84	38	96	29	.,Ë:Î #ŠÉg.¬„8–)
0000000060	4A	AE	9E	C2	4D	99	03	A3	A4	2E	14	EF	C7	EB	93	16	J®žÂM™.£¤..ïÇë“.
0000000070	E0	C7	09	86	1C	FE	C9	D6	6C	89	7E	5D	80	7F	A8	F4	àÇ.†.þÉÖl‰~]€ ¨ô
0000000080	06	BC	B5	BE	26	2C	ED	38	80	54	07	C6	7C	CA	DA	9F	.¼µ¾&,í8€T.Æ|ÊÚŸ
0000000090	09	F7	CF	3D	89	43	17	D2	AD	4B	5D	56	B8	7D	D5	B9	.÷Ï=‰C.Ò.K]V¸}Õ¹
00000000A0	5C	C2	6E	48	79	11	B8	05	07	33	A7	36	E8	FC	E4	0B	\ÂnHy.¸..3§6èüä.
00000000B0	C6	B3	9B	D5	55	6E	2C	25	4B	25	8C	DA	D1	CD	E0	CD	Æ³›ÕUn,%K%ŒÚÑÍàÍ
00000000C0	B7	E4	D0	4A	45	7B	44	47	16	45	39	C8	5A	38	D5	CE	·äÐJE{DG.E9ÈZ8ÕÎ
00000000D0	34	ED	8B	2C	E3	DF	03	FE	6A	C9	C8	38	19	BD	92	ED	4í‹,ãß.þjÉÈ8.½'í
00000000E0	79	DB	B1	3A	7E	5B	6C	41	24	35	FB	93	DB	CC	59	EC	yÛ±:~[lA$5û“ÛÌYì
00000000F0	F5	F2	FC	DE	1E	6A	66	F1	8D	20	17	E9	BD	F0	CC	11	õòüÞ.jfñ .é½ðÌ.
0000000100	87	68	AE	2E	C6	B5	E0	7C	A7	D0	7E	26	0F	D3	8A	AB	‡h®.Æµà|§Ð~&.ÓŠ«
0000000110	46	69	F0	5D	AC	C6	B4	8B	07	C2	51	66	74	FE	60	2E	Fið]¬Æ´‹.ÂQftþ`.
0000000120	48	4A	5B	52	C5	D0	D0	74	C1	8F	A1	C8	44	11	54	59	HJ[RÅÐÐtÁ ¡ÈD.TY
0000000130	F2	DC	73	6B	18	2F	92	21	0A	7D	B1	C8	89	09	89	3C	òÜsk./'!.}±È‰.‰<
0000000140	81	33	73	7F	D6	2E	77	A5	D4	D2	CB	9A	D6	E8	E3	83	3s Ö.w¥ÔÒËšÖèãƒ
0000000150	A6	62	D3	9F	0E	3C	E9	F5	9B	51	4D	55	70	05	A4	DC	¦bÓŸ.<éõ›QMUp.¤Ü
0000000160	E3	BD	22	96	36	10	5C	68	84	64	33	B5	EB	F0	5C	C7	ã½"–6.\h„d3µëð\Ç
0000000170	BD	D1	0A	1F	90	A0	D5	D0	1D	6C	1C	EA	D2	27	44	05	½Ñ.. ÕÐ.l.êÒ'D.

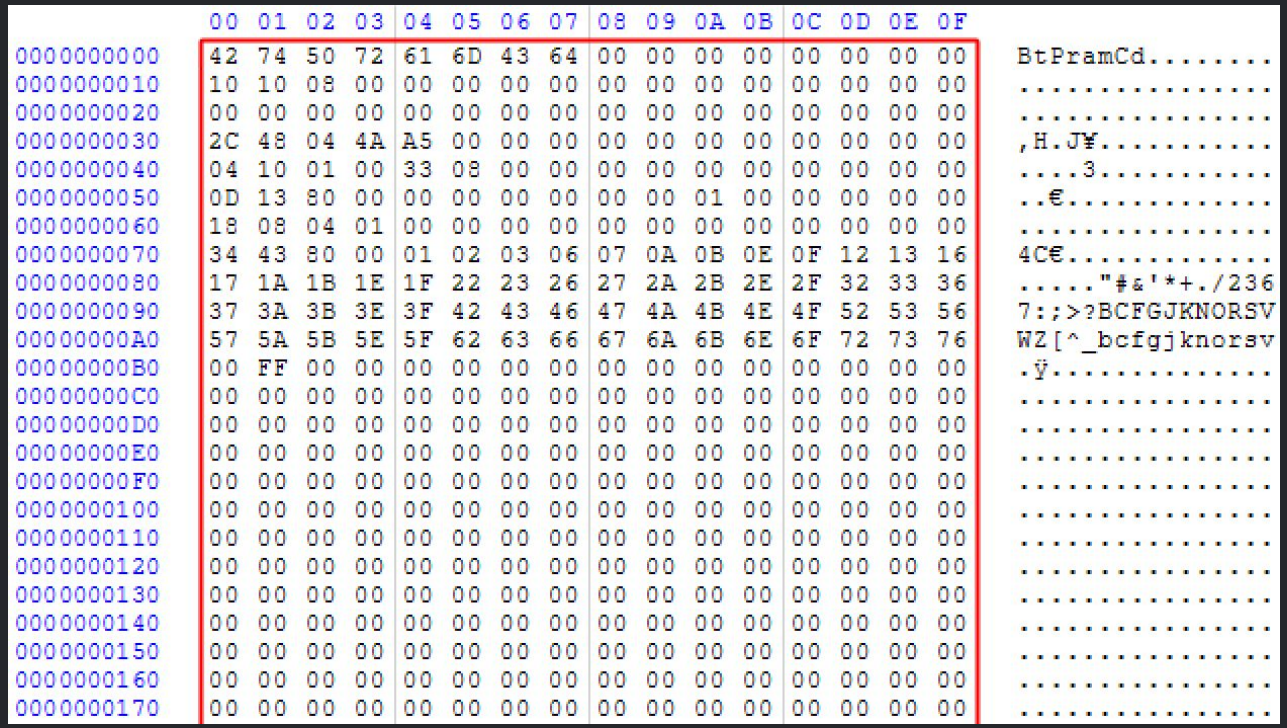
Splitting areas based on visual patterns



Patterns after unscrambling



After XOR unscrambling

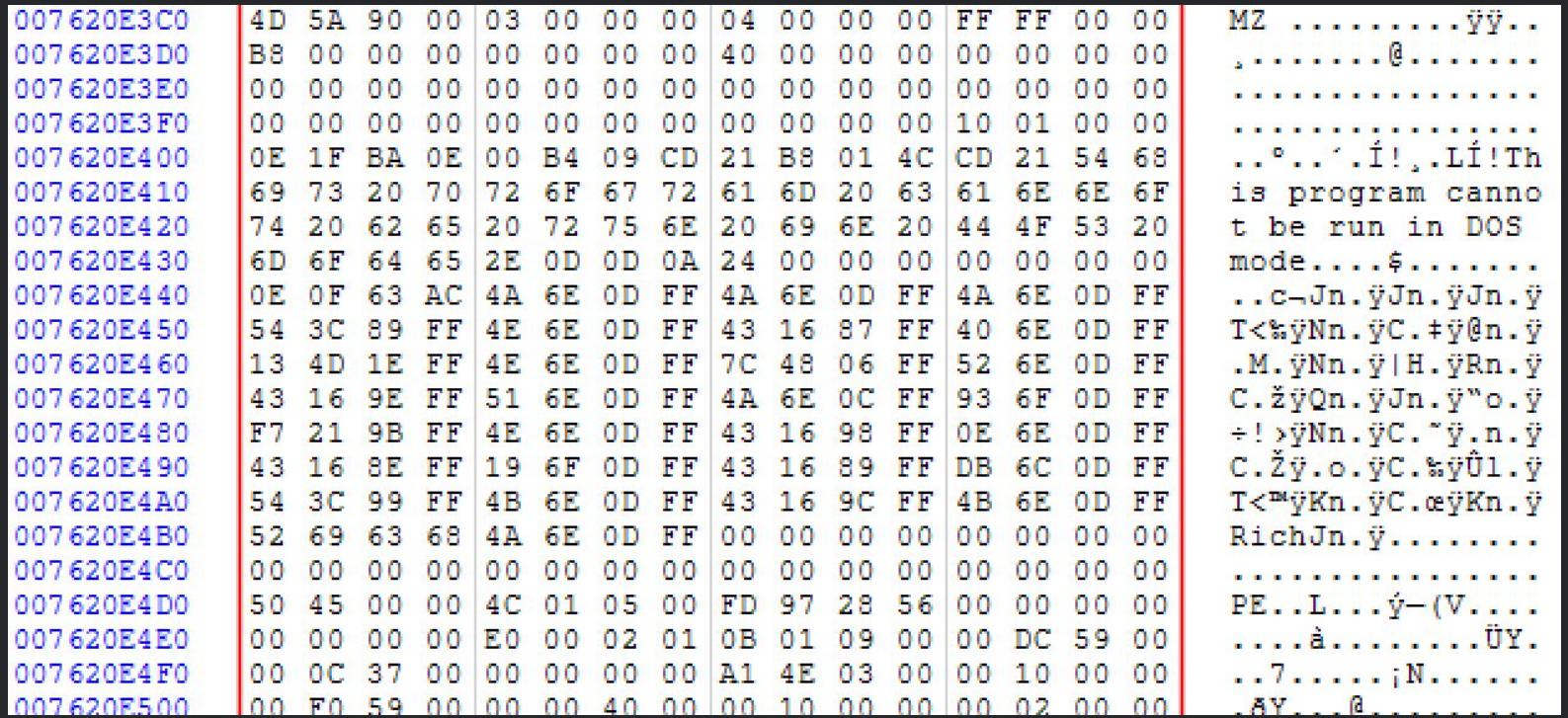


	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
0000000000	42	74	50	72	61	6D	43	64	00	00	00	00	00	00	00	00	BtPramCd........
0000000010	10	10	08	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000030	2C	48	04	4A	A5	00	00	00	00	00	00	00	00	00	00	00	,H.J¥...........
0000000040	04	10	01	00	33	08	00	00	00	00	00	00	00	00	00	00	....3...........
0000000050	0D	13	80	00	00	00	00	00	00	00	01	00	00	00	00	00	..€.............
0000000060	18	08	04	01	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000070	34	43	80	00	01	02	03	06	07	0A	0B	0E	0F	12	13	16	4C€.............
0000000080	17	1A	1B	1E	1F	22	23	26	27	2A	2B	2E	2F	32	33	36	....."#&'*+./236
0000000090	37	3A	3B	3E	3F	42	43	46	47	4A	4B	4E	4F	52	53	56	7:;>?BCFGJKNORSV
00000000A0	57	5A	5B	5E	5F	62	63	66	67	6A	6B	6E	6F	72	73	76	WZ[^_bcfgjknorsv
00000000B0	00	FF	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.ÿ..............
00000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0000000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....

ISO9660 partition

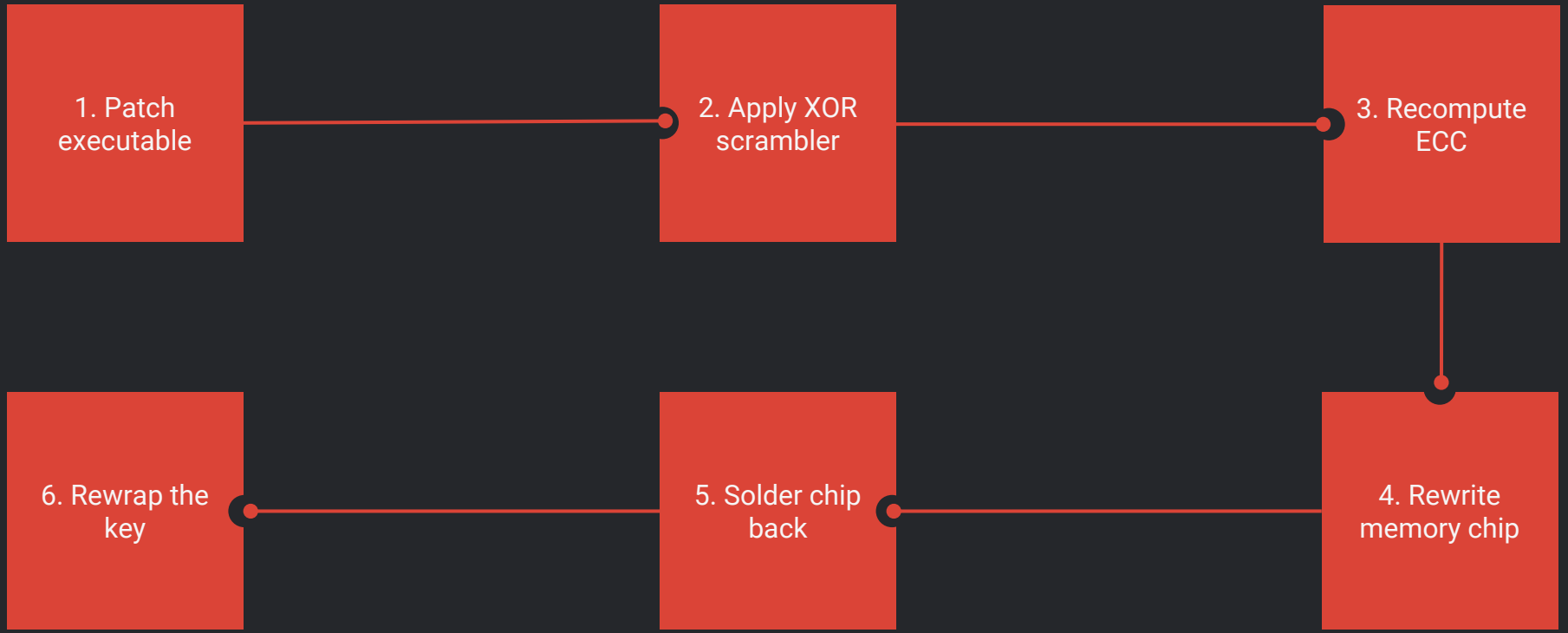
0070008A30	20	20	20	20	20	20	20	20	20	20	20	20	20	20	4D	4B	MK
0070008A40	49	53	4F	46	53	20	49	53	4F	39	36	36	30	2F	48	46	ISOFS ISO9660/HF
0070008A50	53	2F	55	44	46	20	46	49	4C	45	53	59	53	54	45	4D	S/UDF FILESYSTEM
0070008A60	20	42	55	49	4C	44	45	52	20	26	20	43	44	52	45	43	BUILDER & CDREC
0070008A70	4F	52	44	20	43	44	2F	44	56	44	2F	42	6C	75	52	61	ORD CD/DVD/BluRa
0070008A80	79	20	43	52	45	41	54	4F	52	20	28	43	29	20	31	39	y CREATOR (C) 19
0070008A90	39	33	20	45	2E	59	4F	55	4E	47	44	41	4C	45	20	28	93 E.YOUNGDALE (
0070008AA0	43	29	20	31	39	39	37	20	4A	2E	50	45	41	52	53	4F	C) 1997 J.PEARSO
0070008AB0	4E	2F	4A	2E	53	43	48	49	4C	4C	49	4E	47	20	20	20	N/J.SCHILLING
0070008AC0	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
0070008AD0	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
0070008AE0	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
0070008AF0	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
0070008B00	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
0070008B10	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
0070008B20	20	20	20	20	20	20	20	20	20	20	20	20	20	32	30	31	201
0070008B30	35	31	30	32	32	31	31	31	33	30	39	31	39	0C	32	30	5102211130919.20
0070008B40	31	35	31	30	32	32	31	31	31	33	30	39	31	39	0C	30	15102211130919.0
0070008B50	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	00	000000000000000.
0070008B60	32	30	31	35	31	30	32	32	31	31	31	33	30	39	31	39	2015102211130919

Main binary to unlock the key

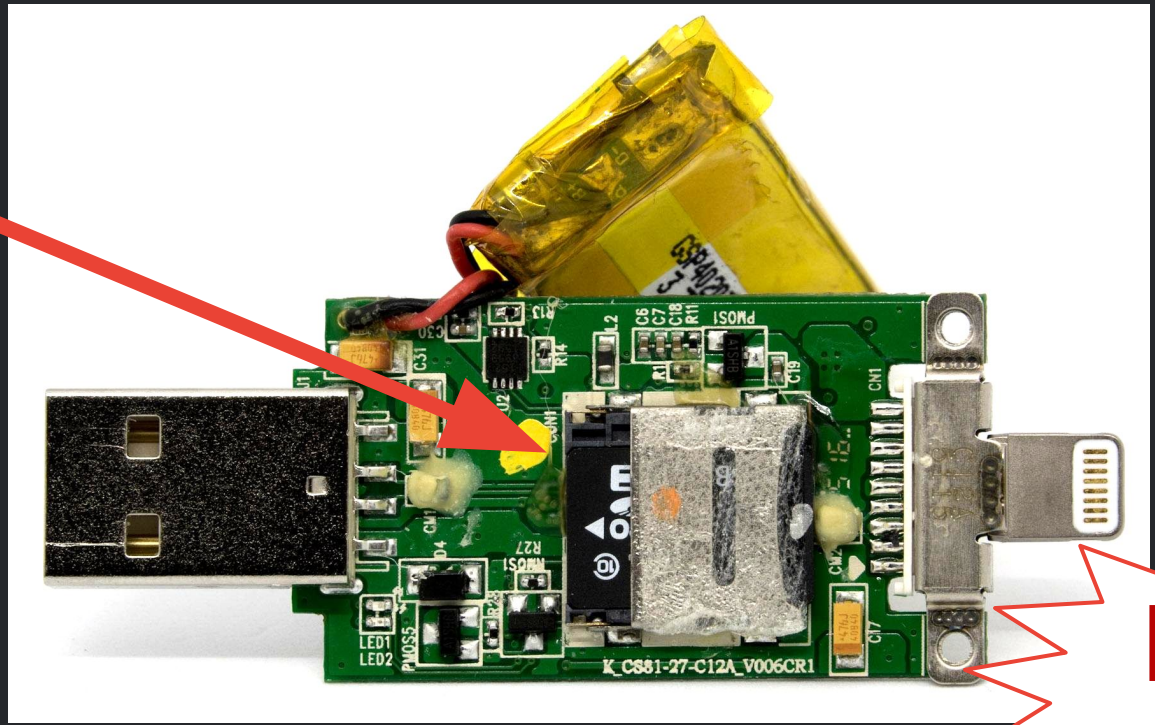


```
007620E3C0  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ .....ÿÿ..
007620E3D0  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
007620E3E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
007620E3F0  00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00  ................
007620E400  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
007620E410  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
007620E420  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS
007620E430  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
007620E440  0E 0F 63 AC 4A 6E 0D FF 4A 6E 0D FF 4A 6E 0D FF  ..c¬Jn.ÿJn.ÿJn.ÿ
007620E450  54 3C 89 FF 4E 6E 0D FF 43 16 87 FF 40 6E 0D FF  T<‰ÿNn.ÿC.‡ÿ@n.ÿ
007620E460  13 4D 1E FF 4E 6E 0D FF 7C 48 06 FF 52 6E 0D FF  .M.ÿNn.ÿ|H.ÿRn.ÿ
007620E470  43 16 9E FF 51 6E 0D FF 4A 6E 0C FF 93 6F 0D FF  C.žÿQn.ÿJn.ÿ"o.ÿ
007620E480  F7 21 9B FF 4E 6E 0D FF 43 16 98 FF 0E 6E 0D FF  ÷!›ÿNn.ÿC.˜ÿ.n.ÿ
007620E490  43 16 8E FF 19 6F 0D FF 43 16 89 FF DB 6C 0D FF  C.Žÿ.o.ÿC.‰ÿÛl.ÿ
007620E4A0  54 3C 99 FF 4B 6E 0D FF 43 16 9C FF 4B 6E 0D FF  T<™ÿKn.ÿC.œÿKn.ÿ
007620E4B0  52 69 63 68 4A 6E 0D FF 00 00 00 00 00 00 00 00  RichJn.ÿ........
007620E4C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
007620E4D0  50 45 00 00 4C 01 05 00 FD 97 28 56 00 00 00 00  PE..L...ý—(V....
007620E4E0  00 00 00 00 E0 00 02 01 0B 01 09 00 00 DC 59 00  ....à........ÜY.
007620E4F0  00 0C 37 00 00 00 00 00 A1 4E 03 00 00 10 00 00  ..7.....¡N......
007620E500  00 F0 59 00 00 00 40 00 00 10 00 00 00 02 00 00  .ðY...@.........
```

Backdooring

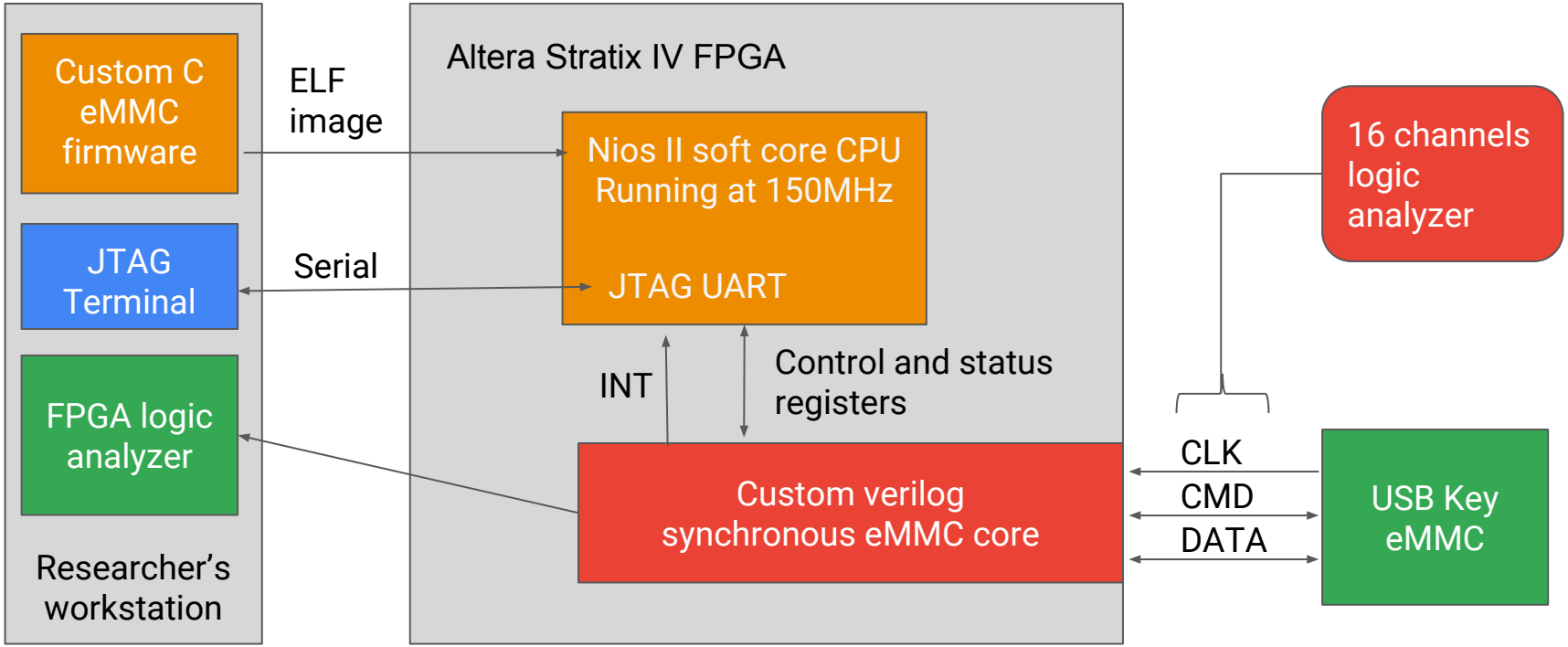


Sometime a SDcard reader will do

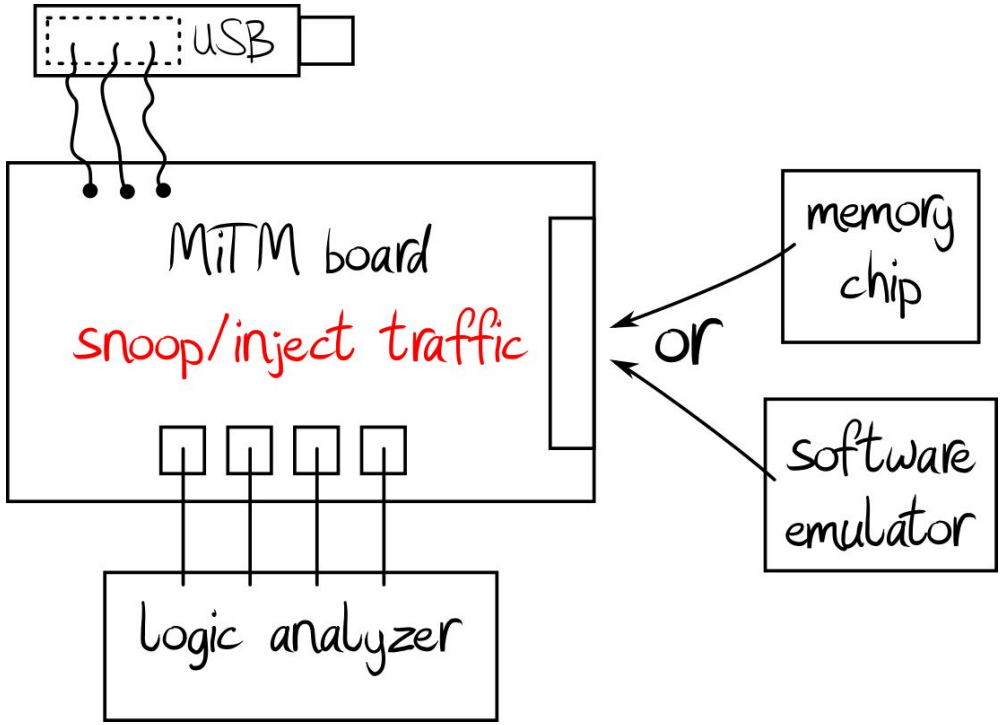



Where are the secret stored?

Interception platform overview

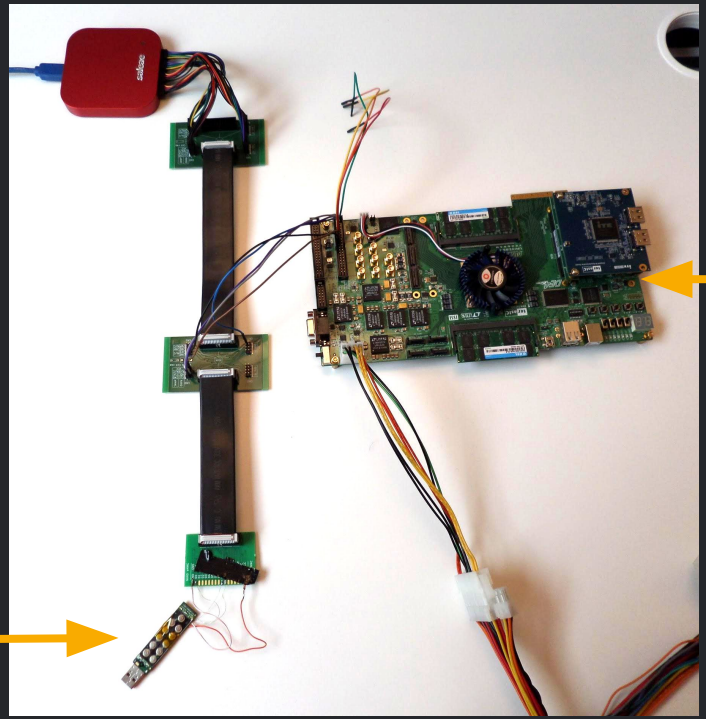


Interception platform simplified overview :)



Interception platform

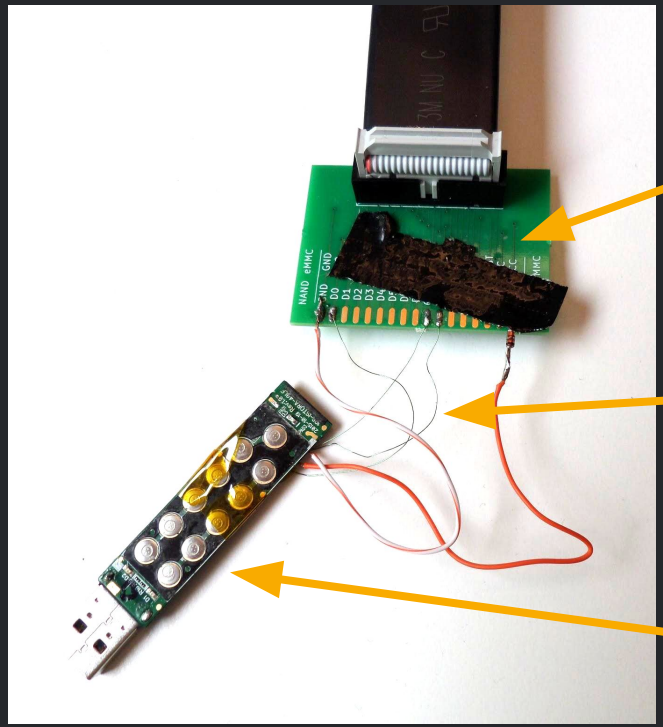
Logic analyzer



FPGA emulating memory

Key without memory

Key wiring details



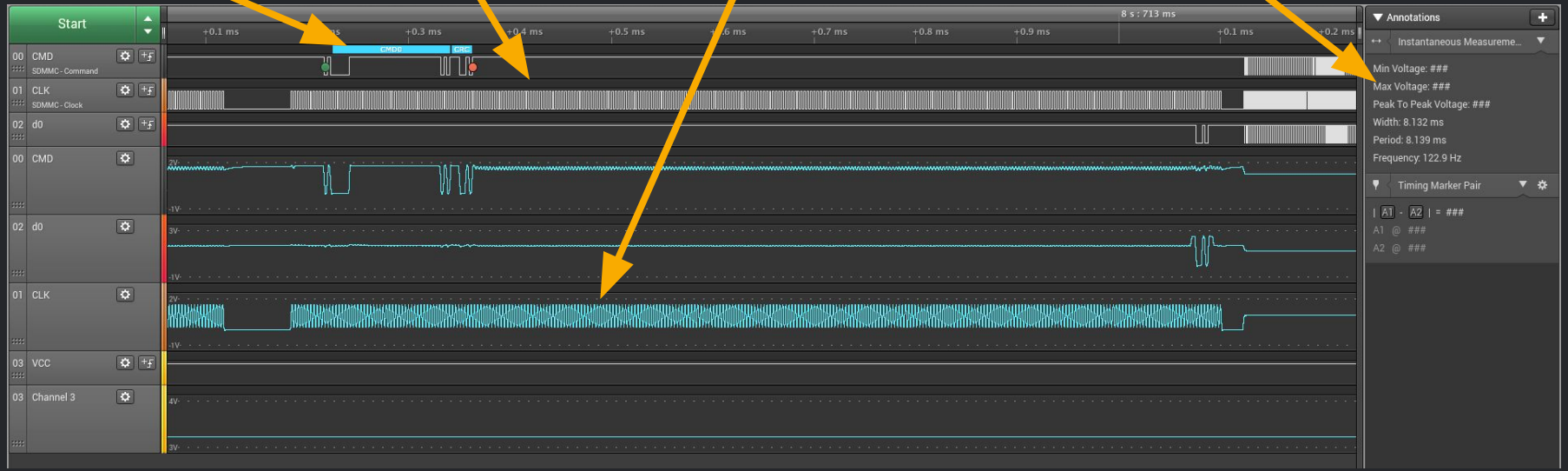
Analysing eMMC at the logic level

Decoded overlay

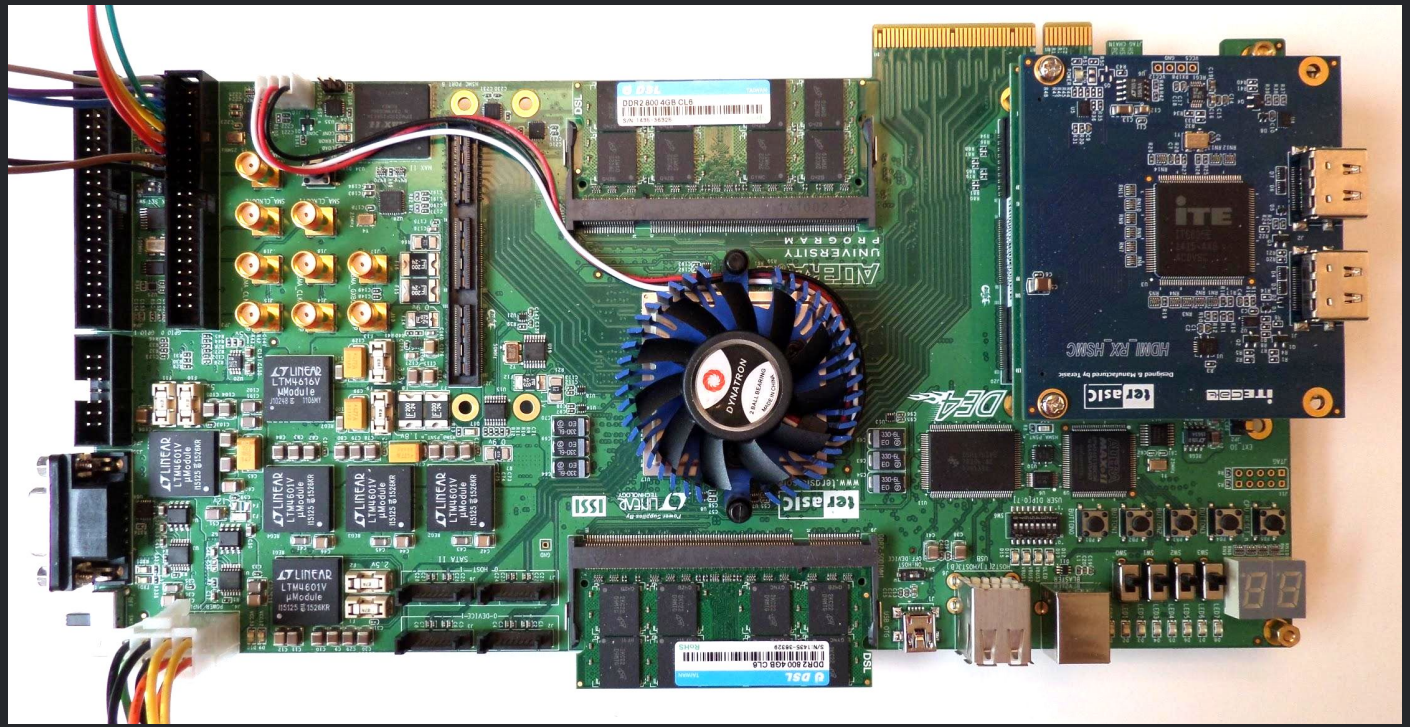
Digital channels

Analog channels

Measurement panel



Emulating an eMMC chip with a FPGA



Analyzer output

```
[+] eMMC firmware started
[+] eMMC system ready for commands!
[+] CMD  0, H2D, verdict: ACCEPT, arg: 0xfffffffa, ctr: 0
[+] CMD  0, H2D, verdict: ACCEPT, arg: 0xfffffffa, ctr: 1
[+] CMD  0, H2D, verdict: ACCEPT, arg: 0xf0f0f0f0, ctr: 2
[+] CMD  0, H2D, verdict: ACCEPT, arg: 0x0, ctr: 3
[+] CMD  1, H2D, verdict: ACCEPT, arg: 0x401c0000, ctr: 4
[+] CMD  2, H2D, verdict: ACCEPT, arg: 0x0, ctr: 5
[+] CMD  3, H2D, verdict: ACCEPT, arg: 0x10000, ctr: 6
[+] CMD  7, H2D, verdict: ACCEPT, arg: 0x10000, ctr: 7
[+] CMD 13, H2D, verdict: ACCEPT, arg: 0x10000, ctr: 8
```

AES key can be recovered?

Target		?
Impact		?
Attacker		?

Looking forward to collaborate on this

Storage audit criteria

Data is encrypted :)		
Should not be stored in memory chip		
- Pin in clear		
- AES key		
- User pin in hashed form		
- Firmware signing key		
Tool (CD) partition integrity must be verified		

 Serendipitous

 Professional

 State sponsored

 Weakness

 Single drive break

 Full break

Takeaways

Certification is important (e.g FIPS-140)

Ensure cryptographic info are (somewhat) disclosed - helps with audit

Current certification is not enough!

Many areas are not covered by current certification as demonstrated

The security of various drives greatly varies

Not all manufacturers or models for a given manufacturers provide the same level of security

Next steps

Use secure encrypted keys

Don’t get breached because sensitive data was on a lost USB key

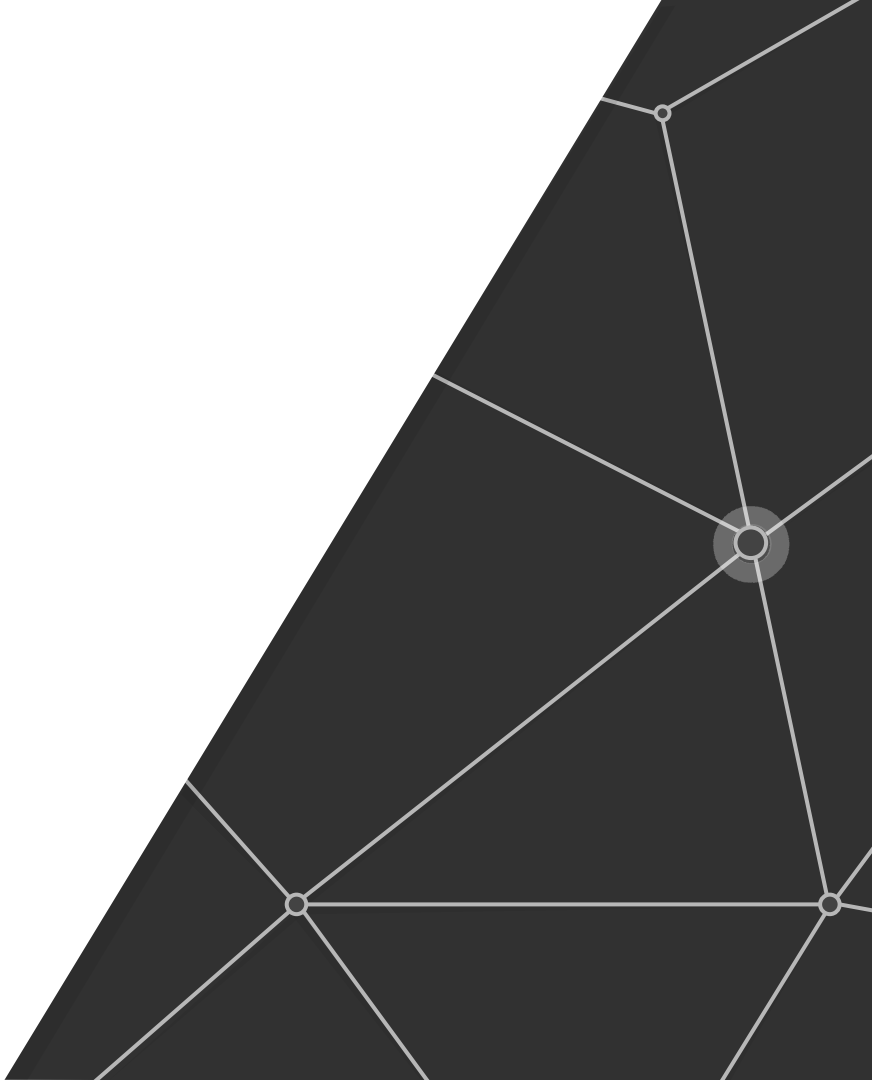
Demand transparency from manufacturers

Key security audit shouldn’t be hard - full spec must be disclosed

Let’s build a better audit and certification process

It is our community responsibility to create a sound methodology

Questions?



Research at Google

Thank you

g.co/research/protect