COTS AND ERTMS VULNERABILITIES

Chris McMahon Stone,
Richard Thomas,
Joeri De Ruiter,
Mihai Ordean
Flavio Garcia
Tom Chothia
Plus many others….

University of Birmingham

Who Am I?

- Tom Chothia
- Research at the University of Birmingham
- Research on a wide range of cyber security topics.
  - Protocols
  - Analysis methods
  - “TRAKS” design for rail key management.
    - http://www.cs.bham.ac.uk/~
  - Two ICS projects, which

Trigger warning: This talk will contain low-level technical details and math

Cyber Security

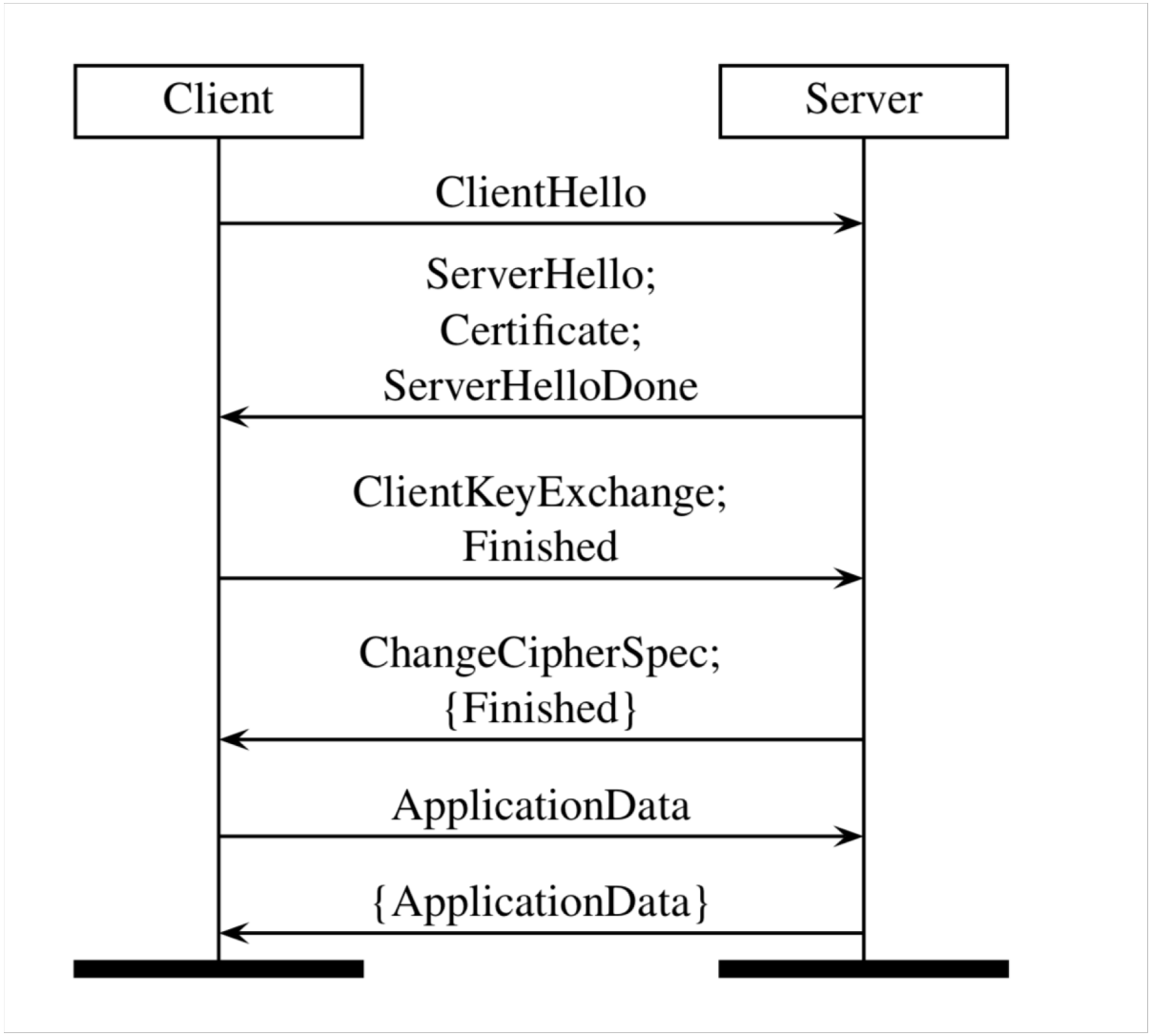
1. We can build unbreakable systems.

2. Pen. testers are very useful to show that there are no vulnerabilities.

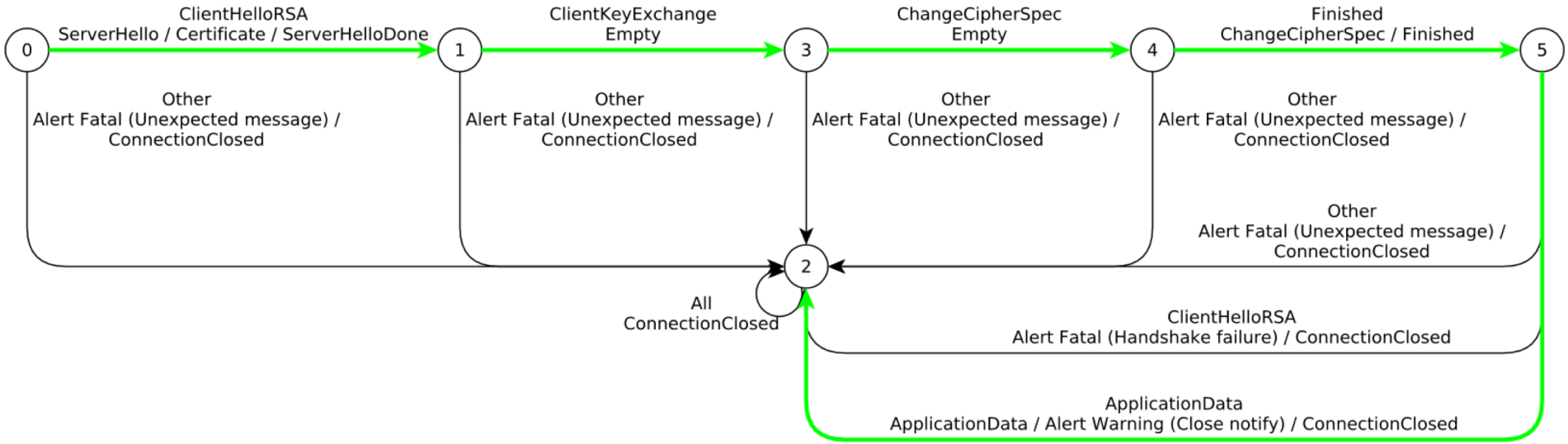
3. Secret systems are secure systems.

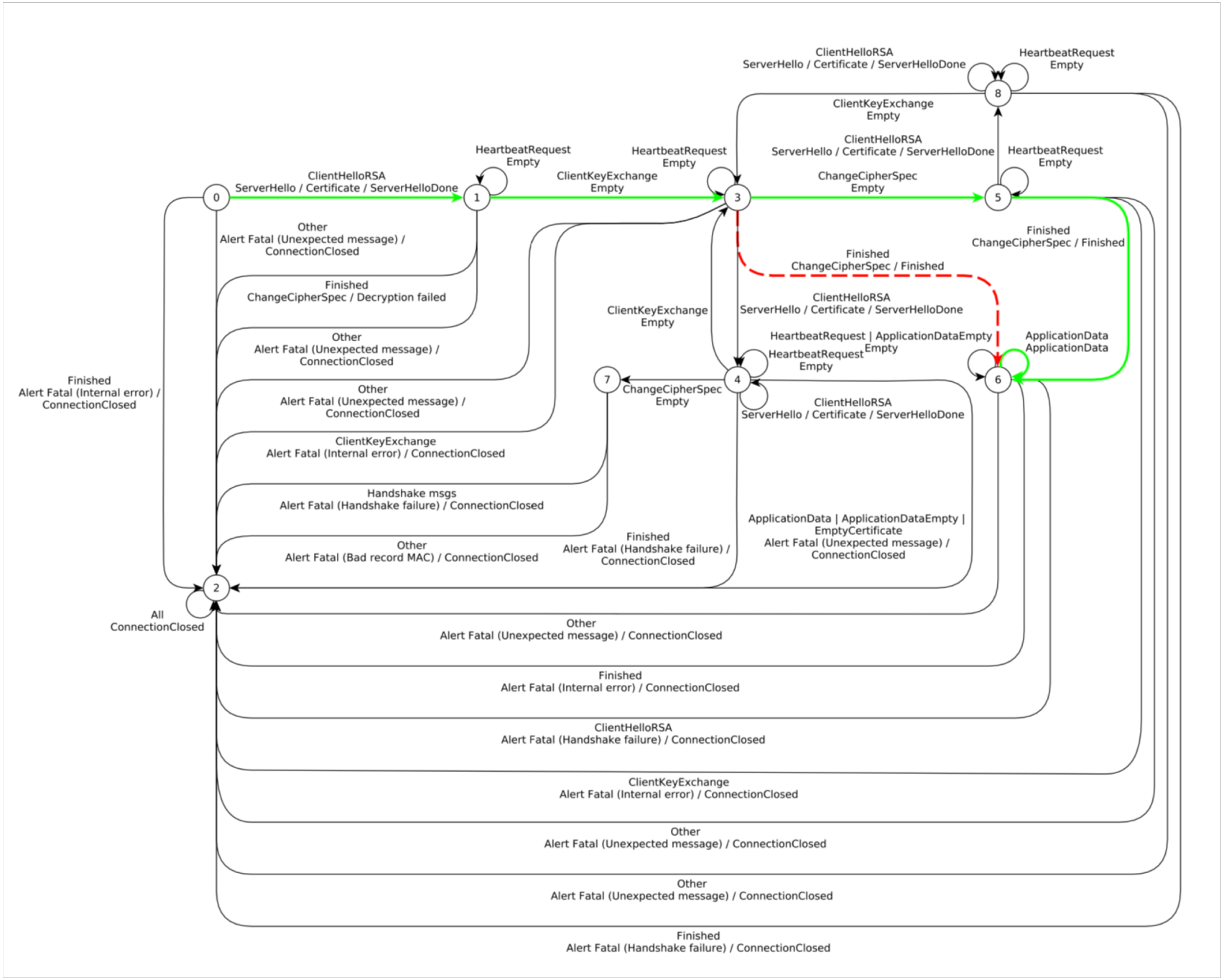
Everything on this slide is COMPLETE false

Transport Layer Security

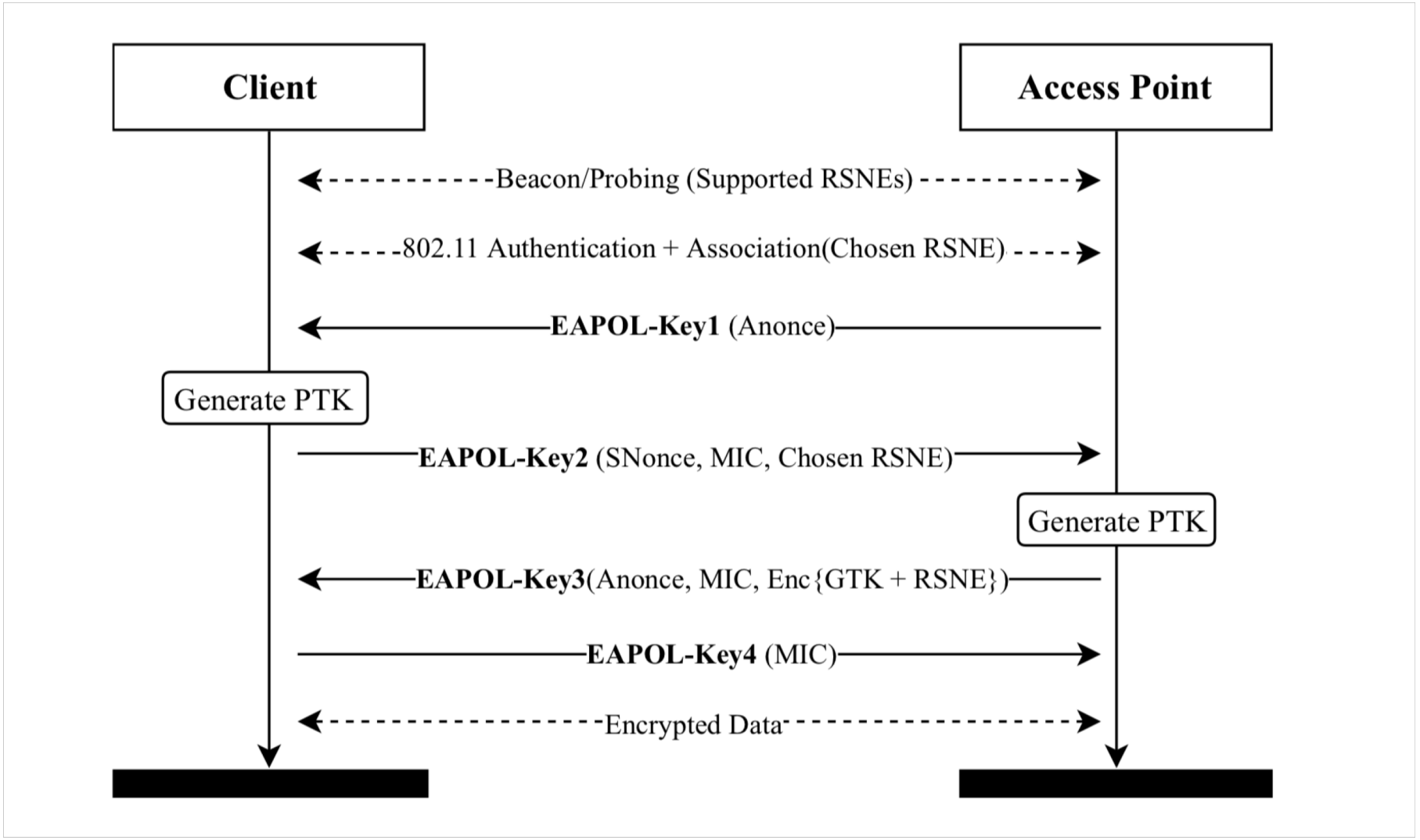


Transport Layer Security

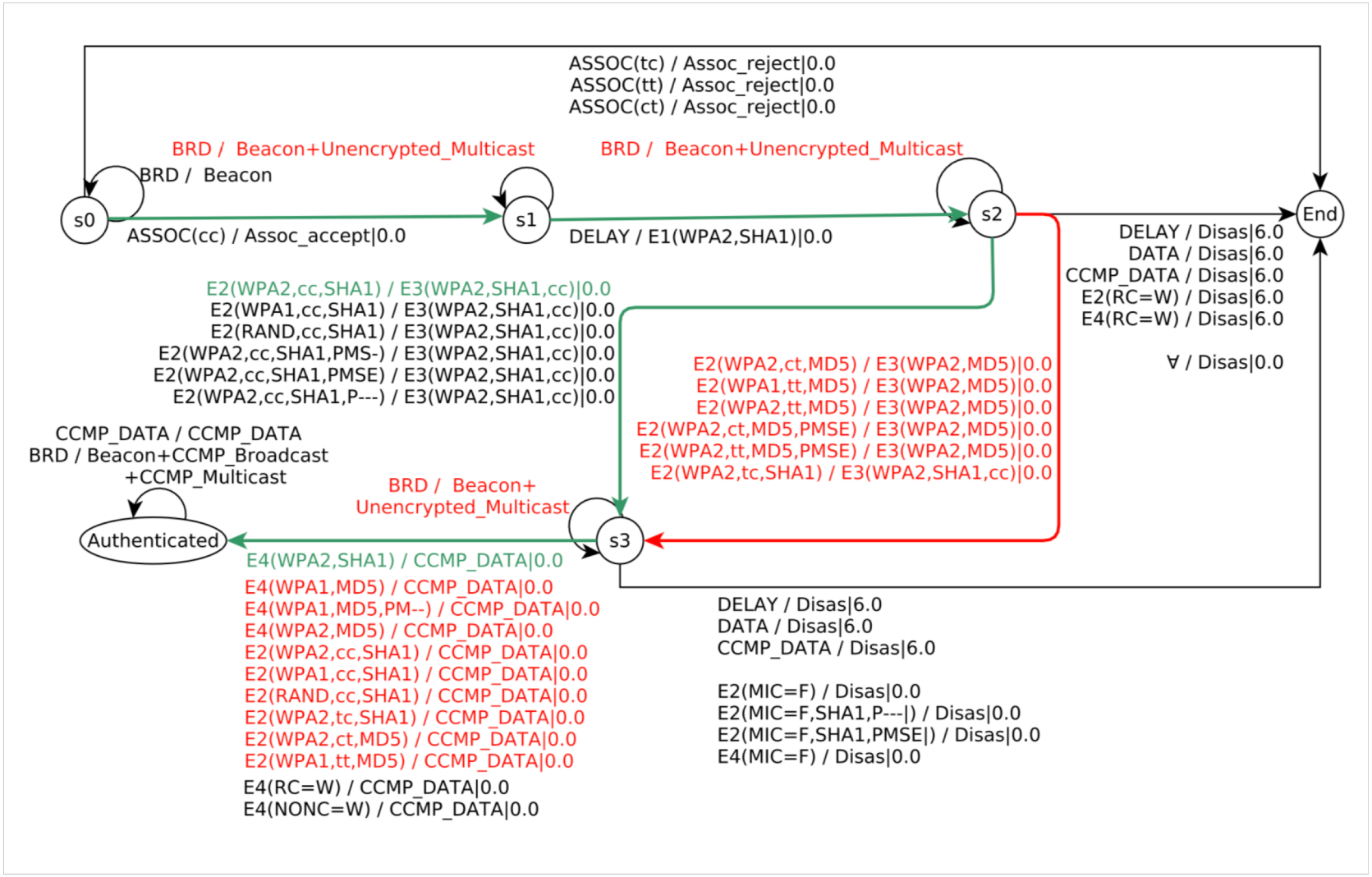



0
1
2
3
4
5
6
7
8
ClientHelloRSA
ServerHello / Certificate / ServerHelloDone
HeartbeatRequest
Empty
ClientKeyExchange
Empty
ChangeCipherSpec
Empty
Other
Alert Fatal (Unexpected message) /
ConnectionClosed
Finished
ChangeCipherSpec / Decryption failed
Finished
ChangeCipherSpec / Finished
HeartbeatRequest | ApplicationDataEmpty
ApplicationData
ApplicationData
Finished
Alert Fatal (Internal error) /
ConnectionClosed
ClientKeyExchange
Alert Fatal (Internal error) / ConnectionClosed
Handshake msgs
Alert Fatal (Handshake failure) / ConnectionClosed
Other
Alert Fatal (Bad record MAC) / ConnectionClosed
Finished
Alert Fatal (Handshake failure) /
ConnectionClosed
ApplicationData | ApplicationDataEmpty |
EmptyCertificate
Alert Fatal (Unexpected message) /
ConnectionClosed
All
ConnectionClosed
Other
Alert Fatal (Unexpected message) / ConnectionClosed
Finished
Alert Fatal (Internal error) / ConnectionClosed
ClientHelloRSA
Alert Fatal (Handshake failure) / ConnectionClosed
ClientKeyExchange
Alert Fatal (Internal error) / ConnectionClosed
Other
Alert Fatal (Unexpected message) / ConnectionClosed
Other
Alert Fatal (Unexpected message) / ConnectionClosed
Finished
Alert Fatal (Handshake failure) / ConnectionClosed

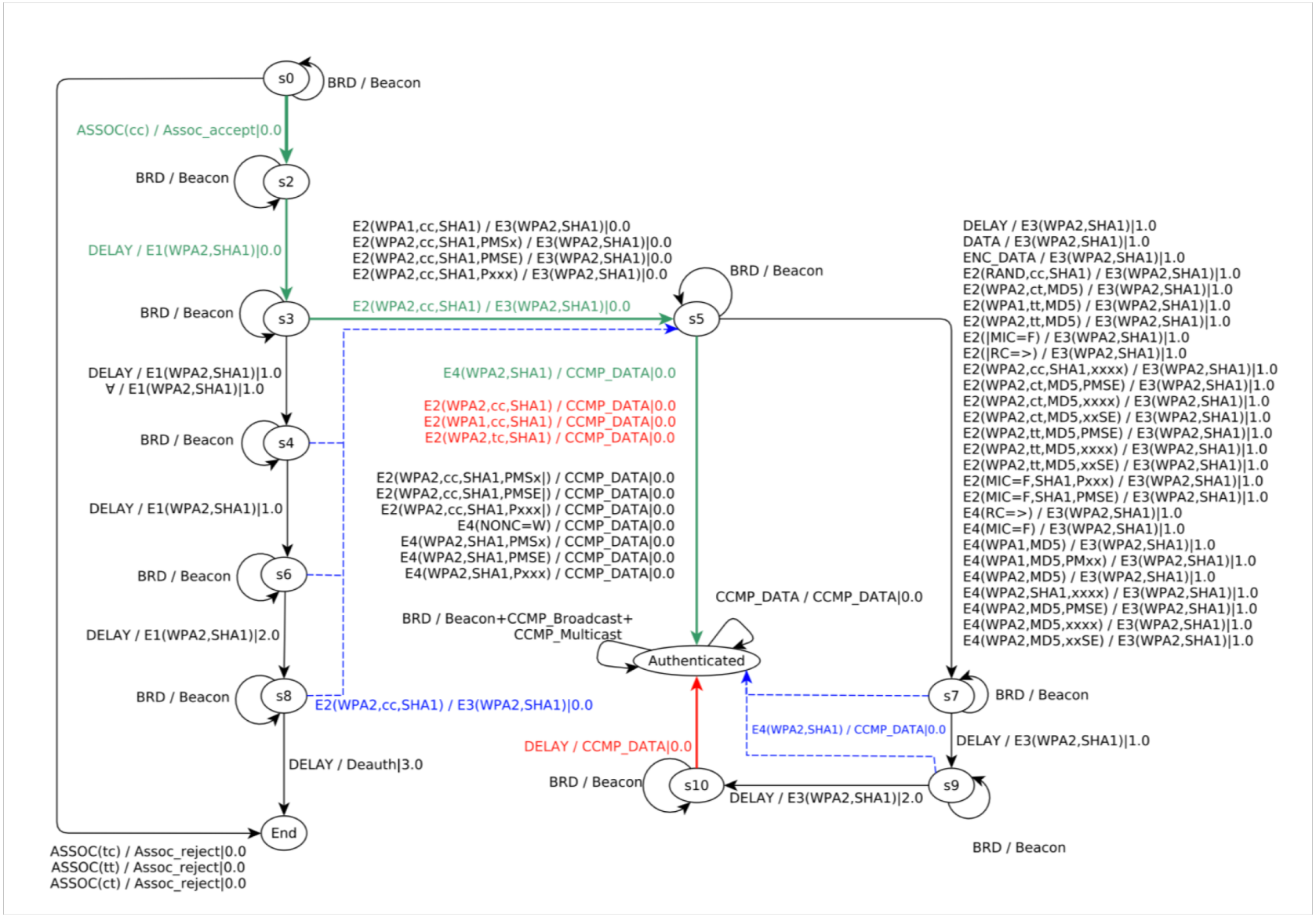
WPA


Client
Access Point
Beacon/Probing (Supported RSNEs)
802.11 Authentication + Association(Chosen RSNE)
EAPOL-Key1 (Anonce)
Generate PTK
EAPOL-Key2 (SNonce, MIC, Chosen RSNE)
Generate PTK
EAPOL-Key3(Anonce, MIC, Enc{GTK + RSNE})
EAPOL-Key4 (MIC)
Encrypted Data

TP-link routers



Cisco routers



Certificate pinning with no hostname verification


NatWest


HSBC

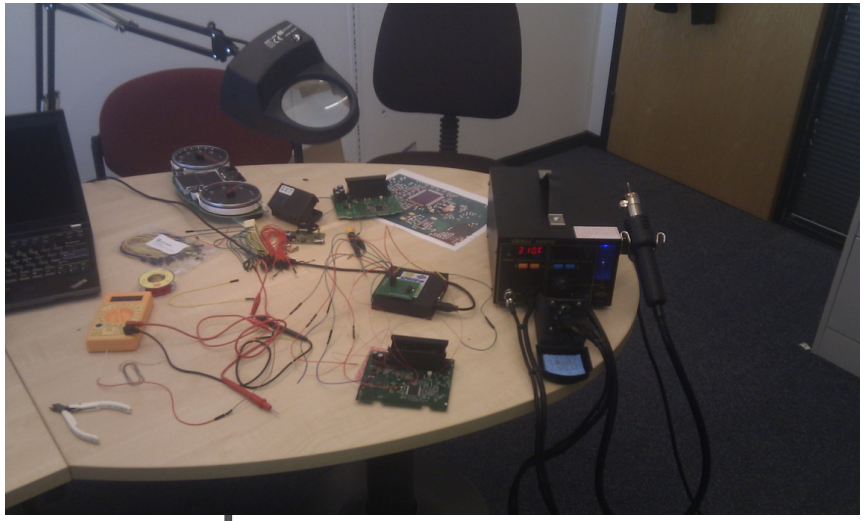

Royal Bank
of Scotland

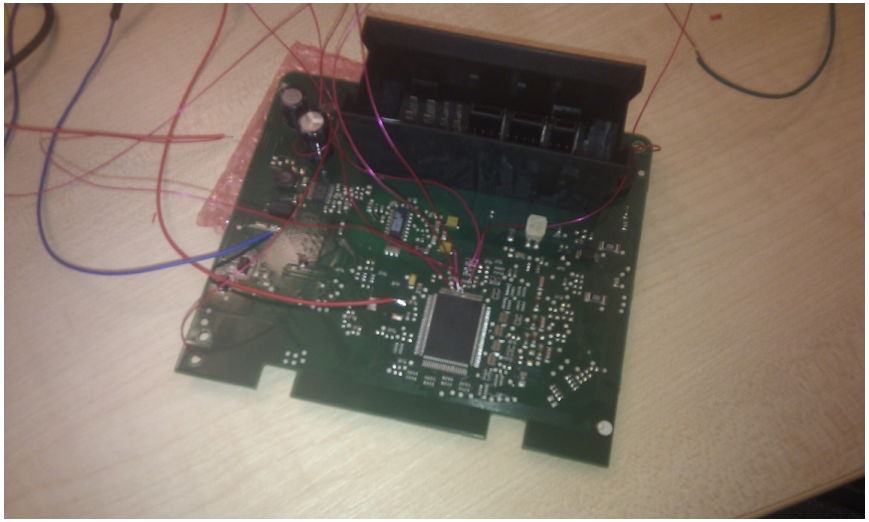

SM
Bank of America

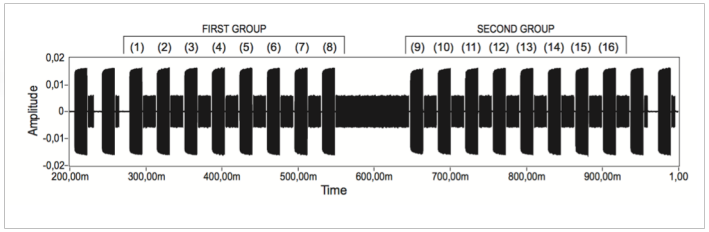

Santander

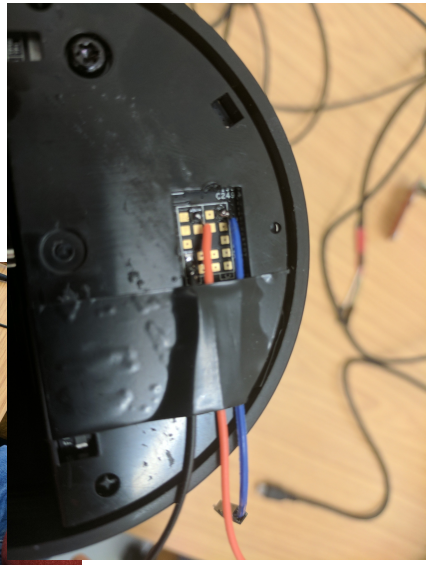

AIB
Allied Irish Bank

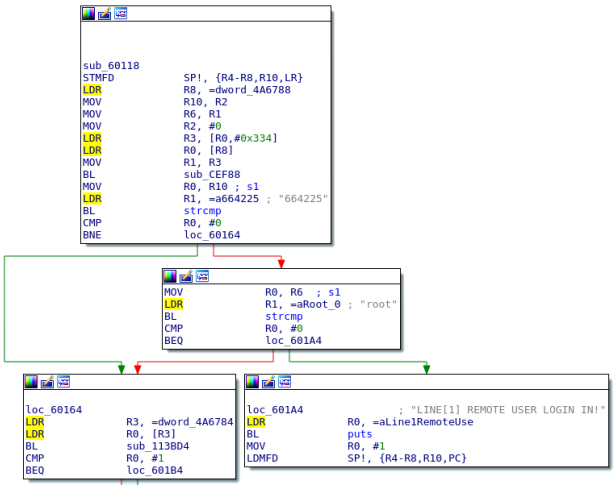
If these systems are vulnerable why not keep the design secret?



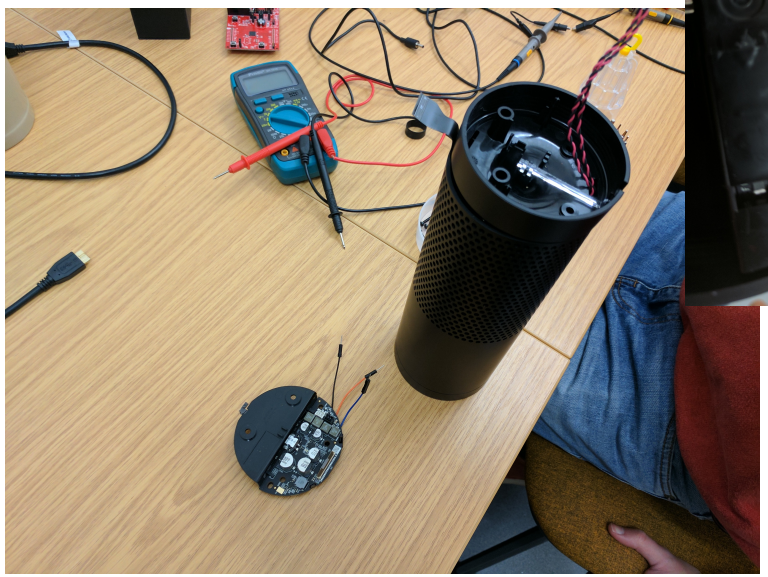








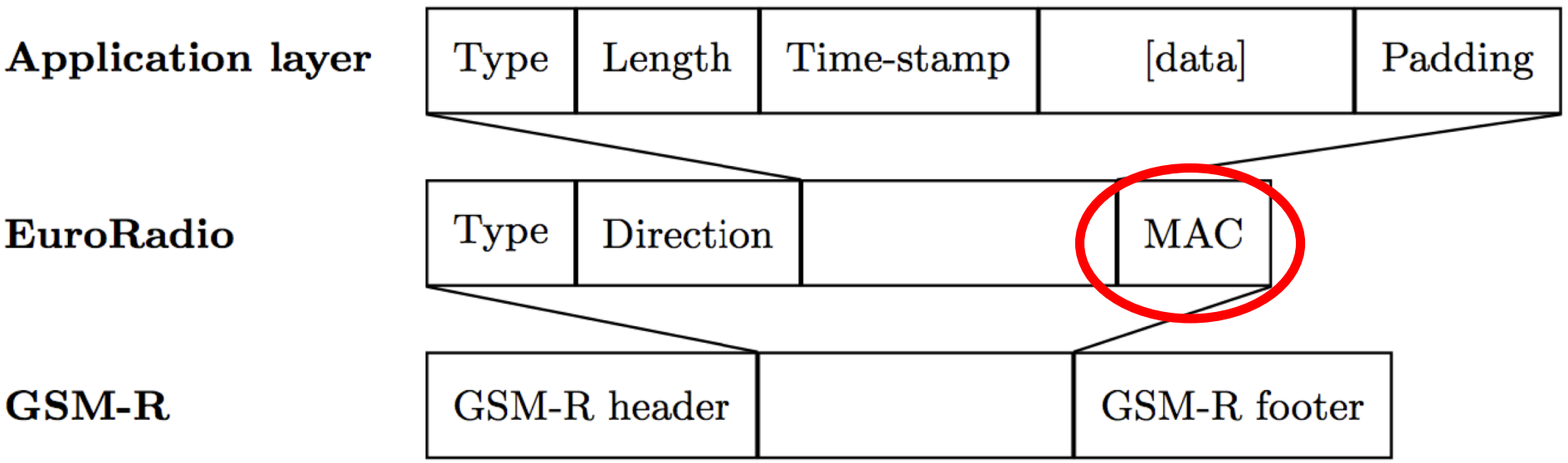
```
sub_60118
STMFD           SP!, {R4-R8,R10,LR}
LDR             R8, =dword_4A6788
MOV             R10, R2
MOV             R6, R1
MOV             R2, #0
LDR             R3, [R0,#0x334]
LDR             R0, [R8]
MOV             R1, R3
BL              sub_CEF88
MOV             R0, R10 ; s1
LDR             R1, =a664225 ; "664225"
BL              strcmp
CMP             R0, #0
BNE             loc_60164

MOV             R0, R6  ; s1
LDR             R1, =aRoot_0 ; "root"
BL              strcmp
CMP             R0, #0
BEQ             loc_601A4

loc_60164
LDR             R3, =dword_4A6784
LDR             R0, [R3]
BL              sub_113BD4
CMP             R0, #1
BEQ             loc_601B4

loc_601A4               ; "LINE[1] REMOTE USER LOGIN IN!"
LDR             R0, =aLine1RemoteUse
BL              puts
MOV             R0, #1
LDMFD           SP!, {R4-R8,R10,PC}
```



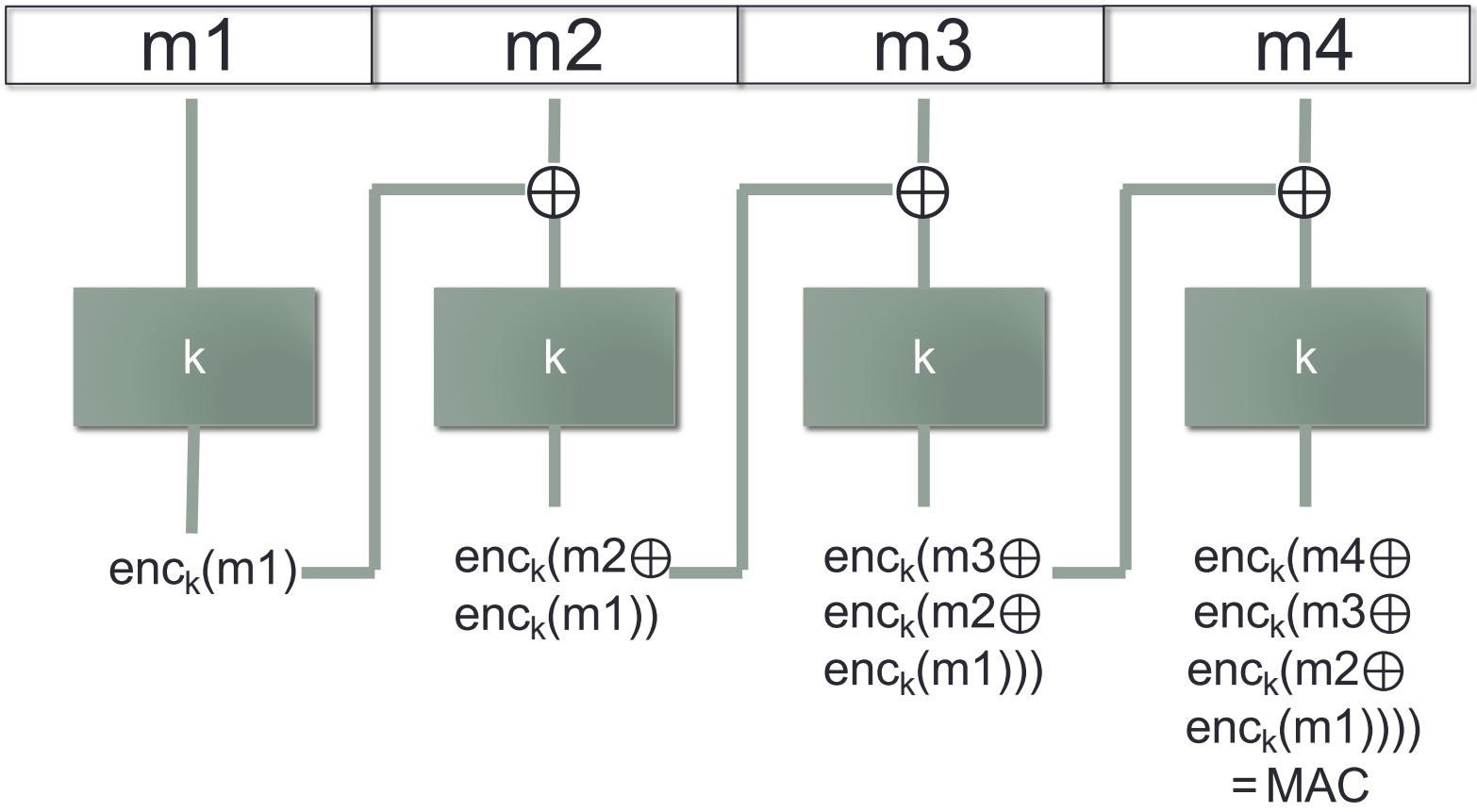
If the crypto. spec. and protocols are not public you must assume they are insecure.

Keeping the design secret just slows down patching.

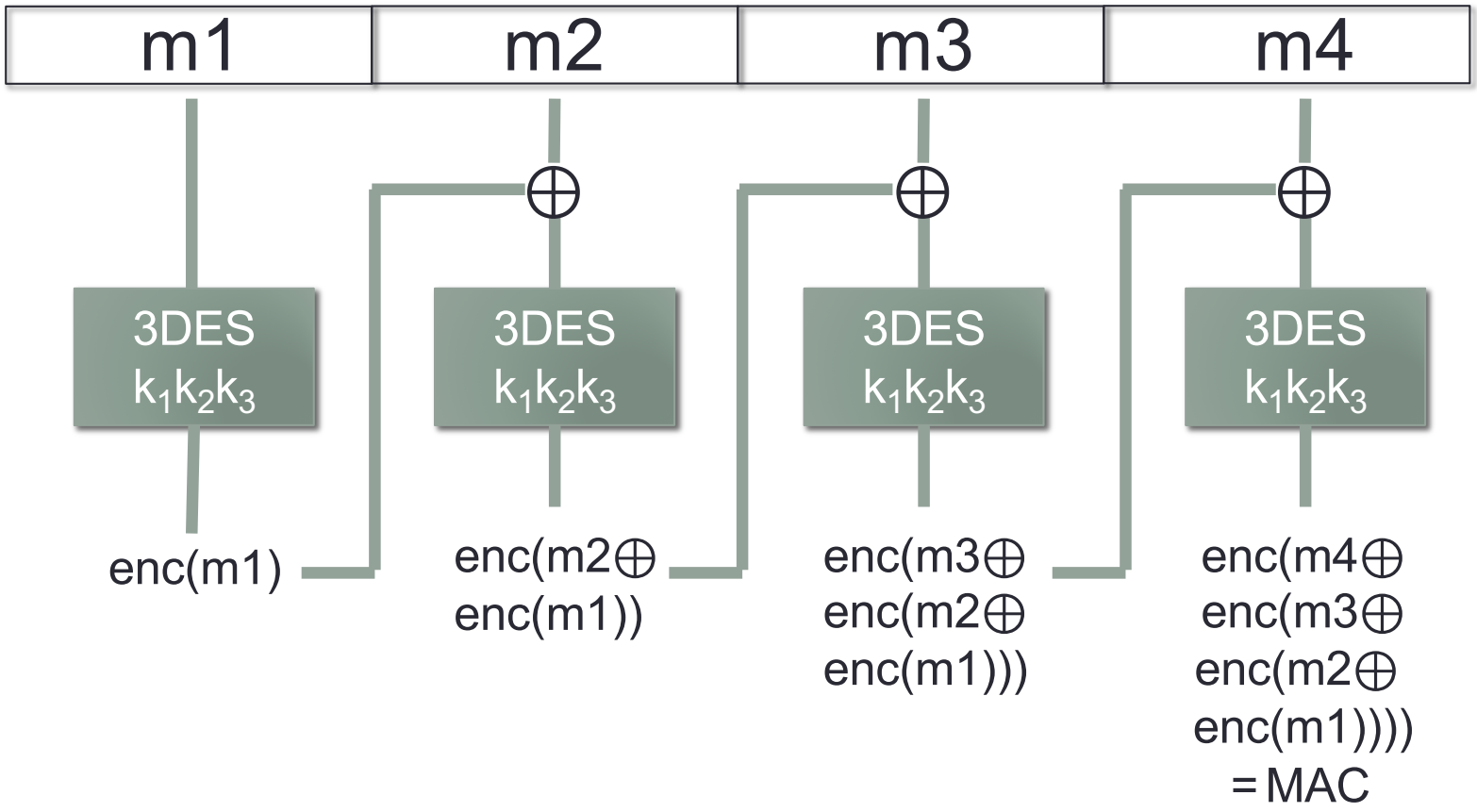
ERTMS Protocol Stack



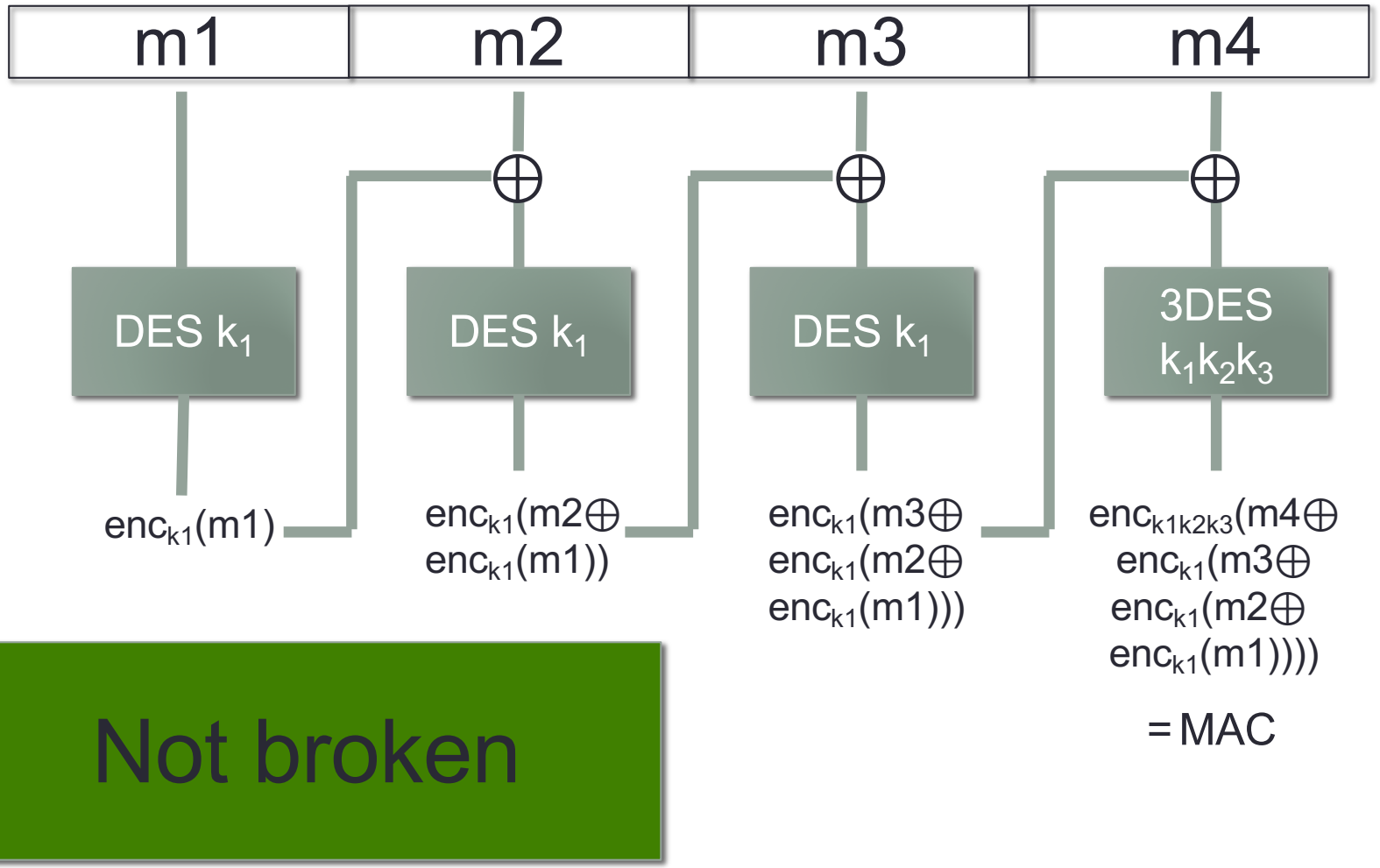
CBC-MAC


m1
m2
m3
m4
k
k
k
k
$enc_k(m1)$
$enc_k(m2 \oplus enc_k(m1))$
$enc_k(m3 \oplus enc_k(m2 \oplus enc_k(m1)))$
$enc_k(m4 \oplus enc_k(m3 \oplus enc_k(m2 \oplus enc_k(m1))))$
= MAC

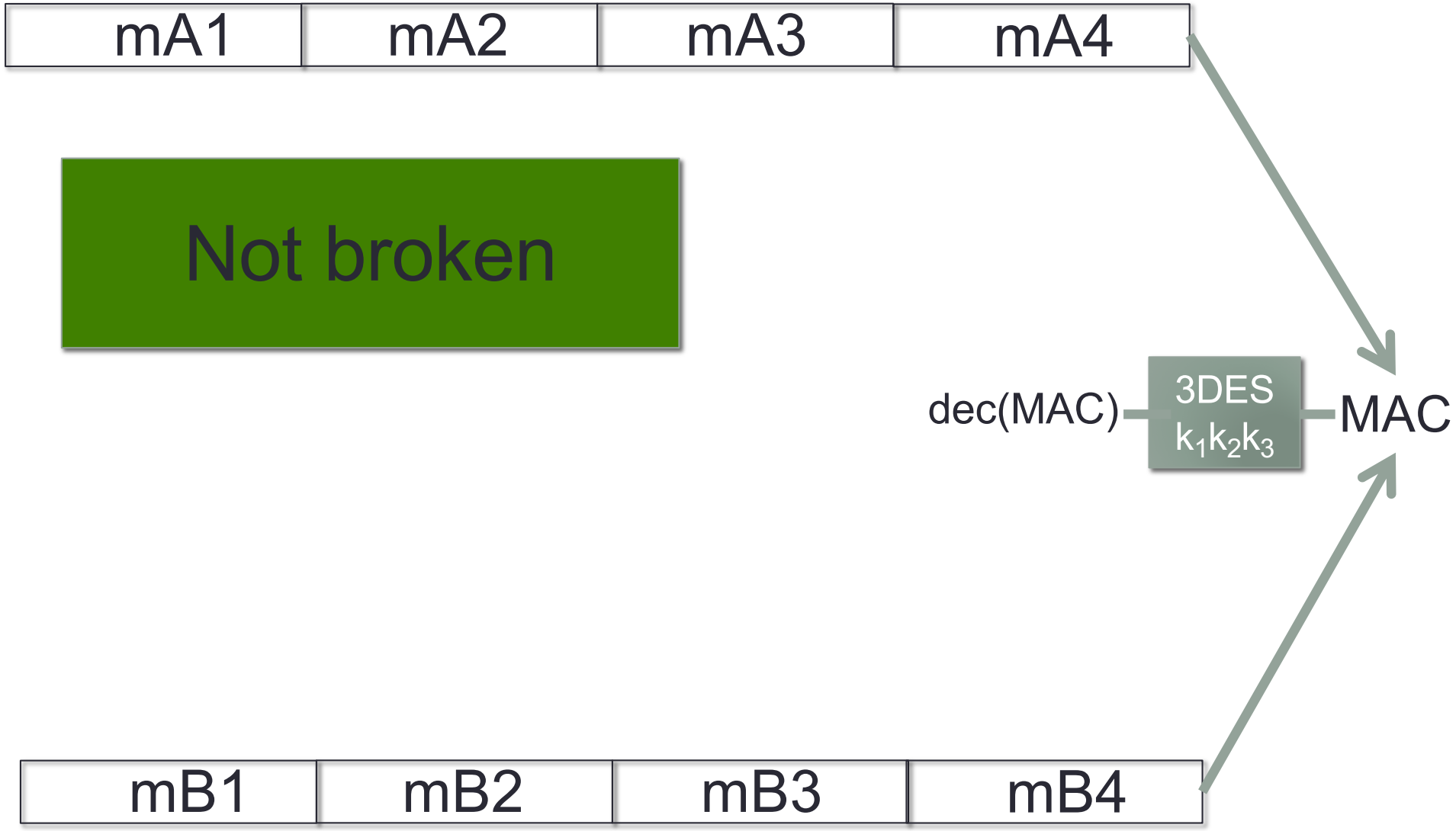
3DES-CBC-MAC


m1
m2
m3
m4
3DES
$k_1k_2k_3$
3DES
$k_1k_2k_3$
3DES
$k_1k_2k_3$
3DES
$k_1k_2k_3$
enc(m1)
enc(m2⊕
enc(m1))
enc(m3⊕
enc(m2⊕
enc(m1)))
enc(m4⊕
enc(m3⊕
enc(m2⊕
enc(m1))))
= MAC

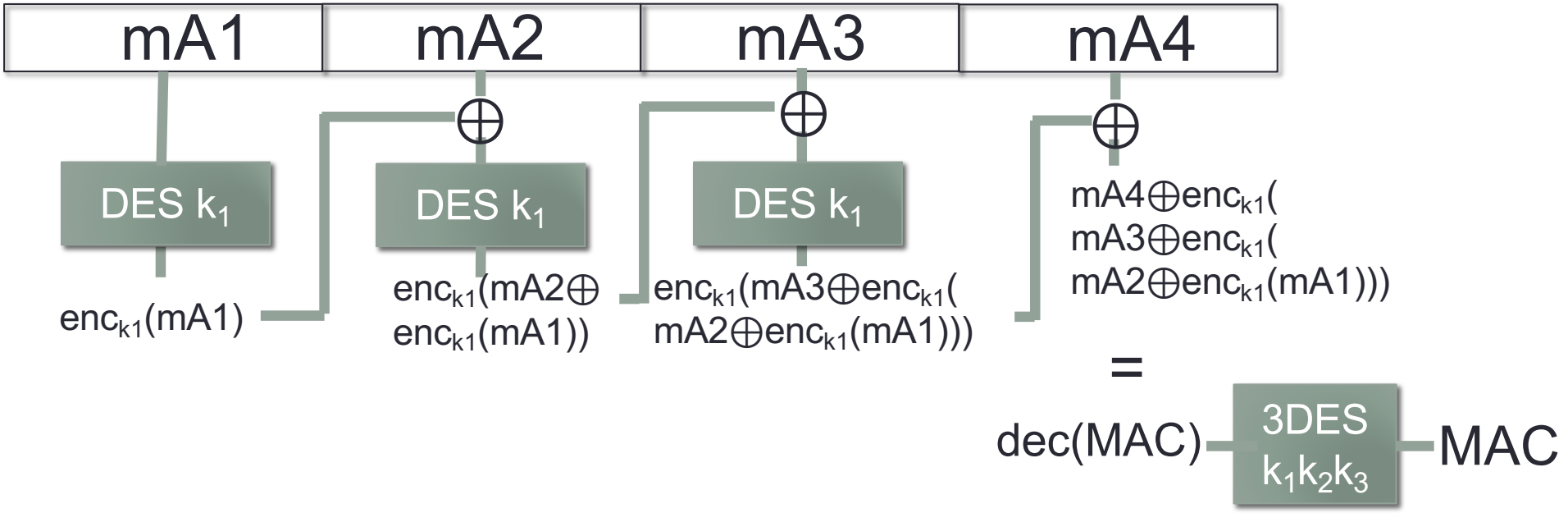
The EuroRadio MAC



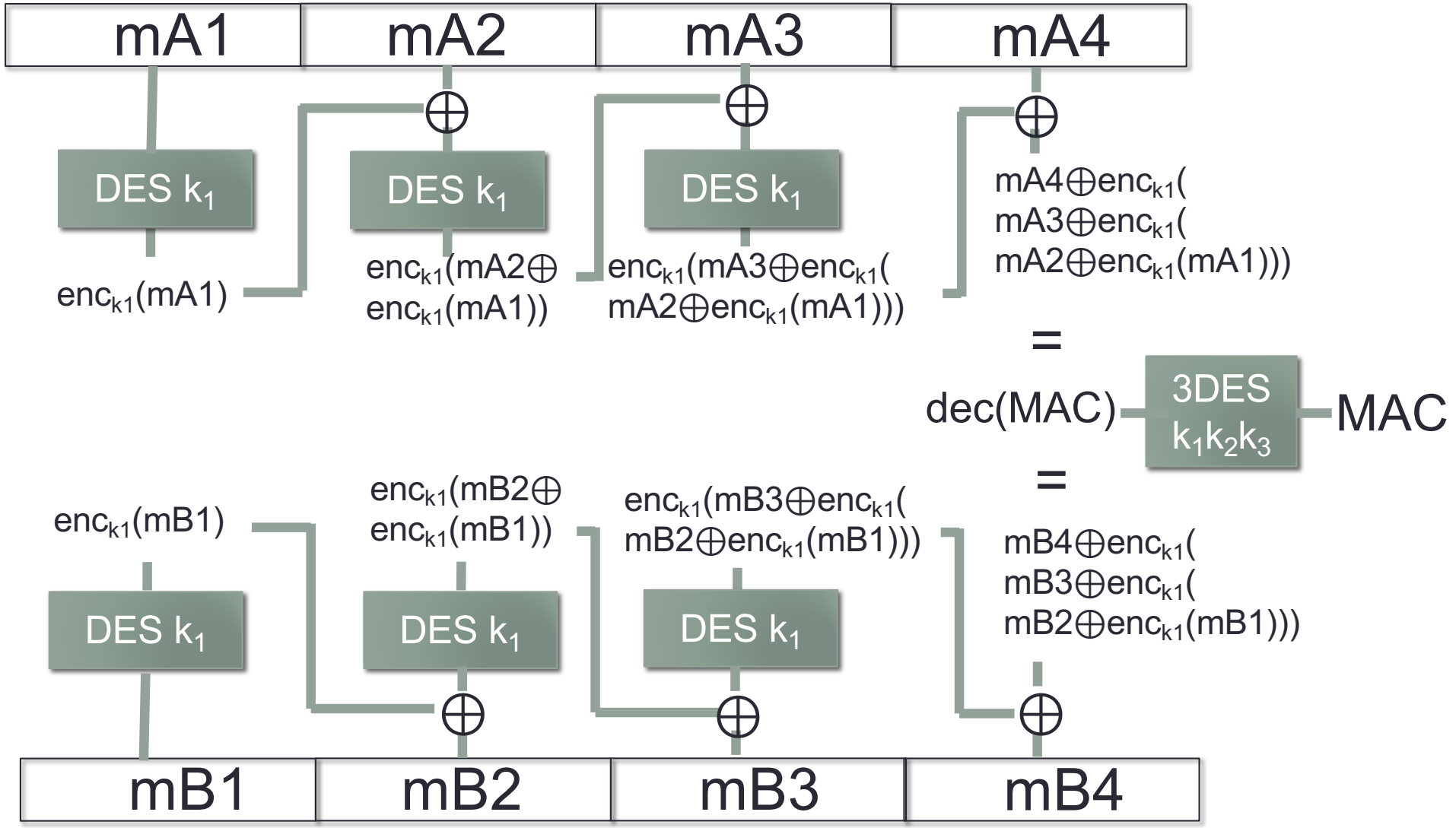
The EuroRadio MAC



The EuroRadio MAC



The EuroRadio MAC



The EuroRadio MAC

$mA4 \oplus enc_{k1}($
$mA3 \oplus enc_{k1}($
$mA2 \oplus enc_{k1}(mA1)))$

=

$dec(MAC)$ — 3DES $k_1 k_2 k_3$ — MAC

=

$mB4 \oplus enc_{k1}($
$mB3 \oplus enc_{k1}($
$mB2 \oplus enc_{k1}(mB1)))$

The EuroRadio MAC

$$mA4 \oplus enc_{k1}(\, mA3 \oplus enc_{k1}(\, mA2 \oplus enc_{k1}(mA1)))$$

$$=$$

$$mB4 \oplus enc_{k1}(mB3 \oplus enc_{k1}(\, mB2 \oplus enc_{k1}(mB1)))$$

The EuroRadio MAC

mA1	mA2	mA3	mA4

Still not broken

$mA4 \oplus enc_{k1}(mA3 \oplus enc_{k1}(mA2 \oplus enc_{k1}(mA1)))$

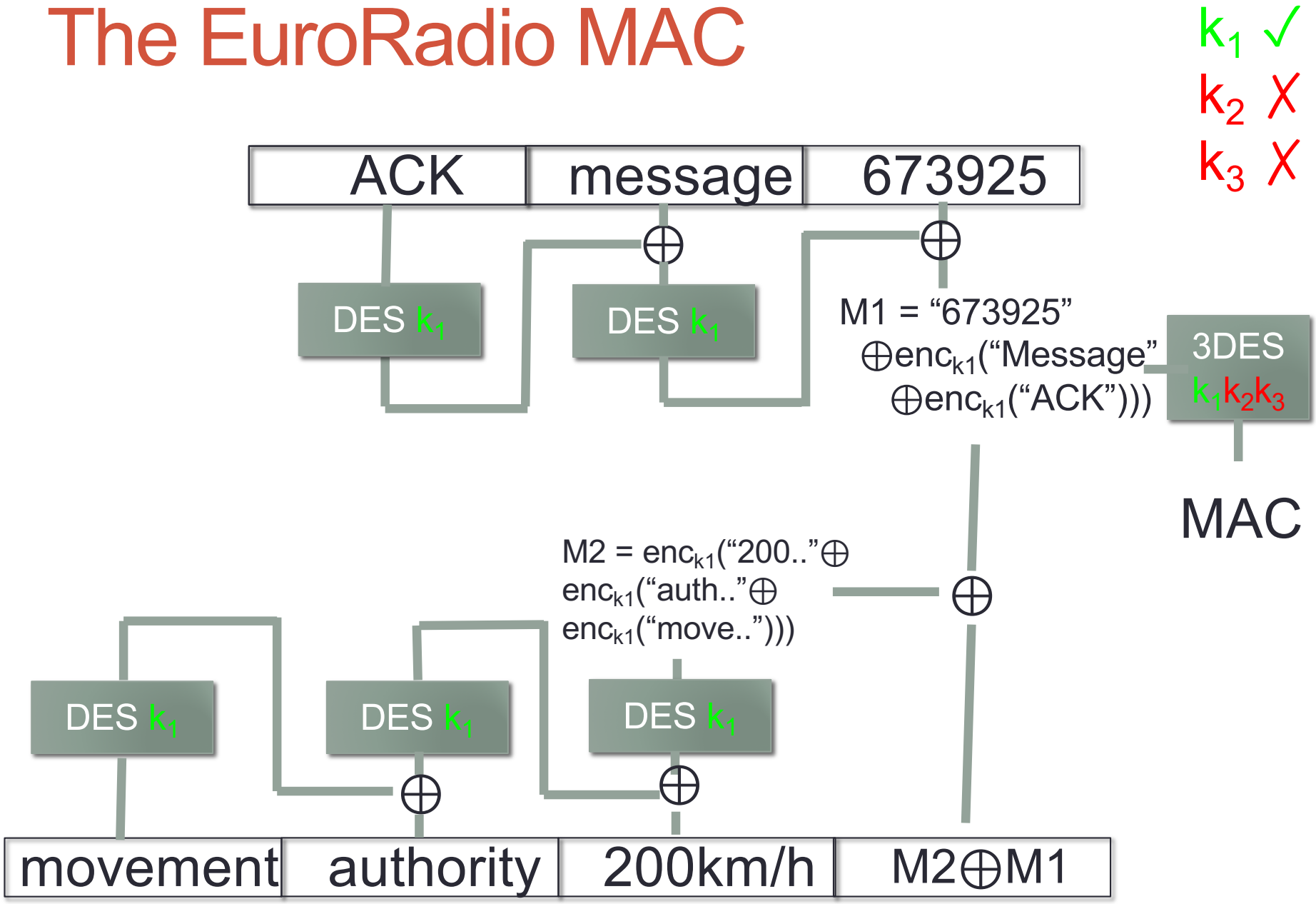
=

$mB4 \oplus enc_{k1}(mB3 \oplus enc_{k1}(mB2 \oplus enc_{k1}(mB1)))$

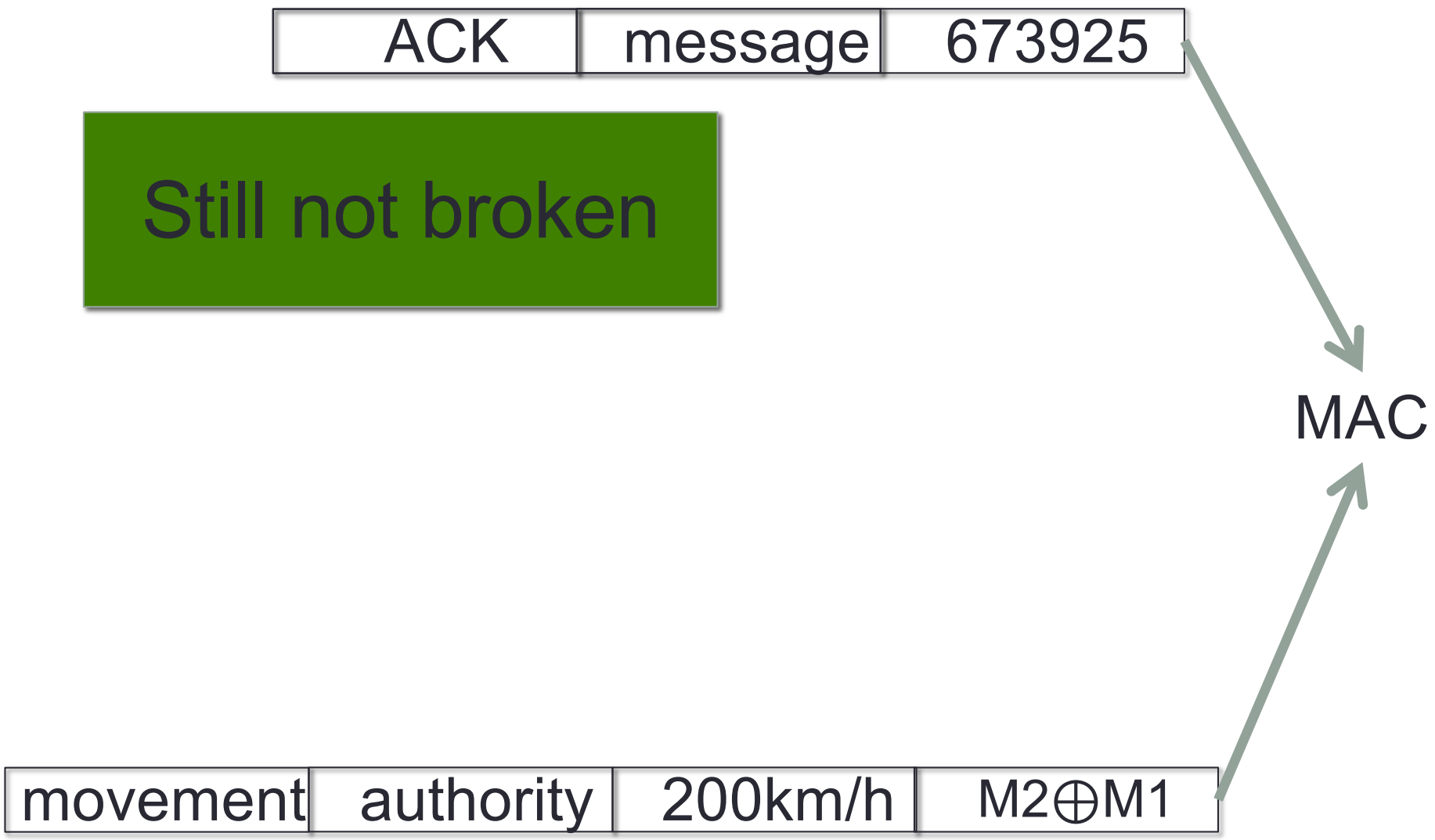
$38,246 to break k_1
in 30 mins using Amazon

mB1	mB2	mB3	mB4

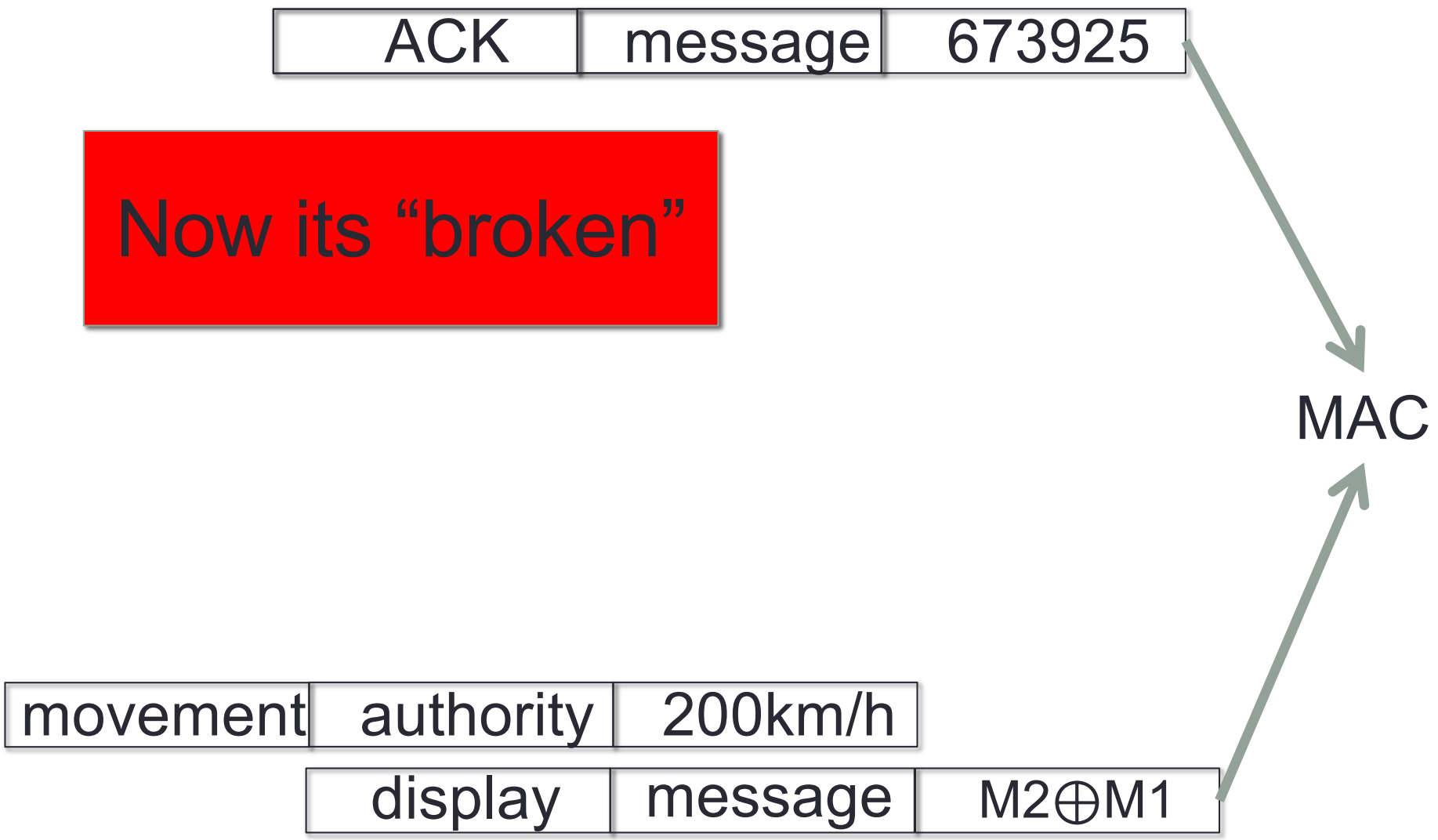
The EuroRadio MAC



The EuroRadio MAC



The EuroRadio MAC



Examples

Two acknowledgement messages:

00120000020A9203A2105E0480000062105DFD0000000000

MAC: 80B7557F31566DBB

00120000020A9203AAE360078000006AE360000000000000

MAC: 80B7557F31566DBB

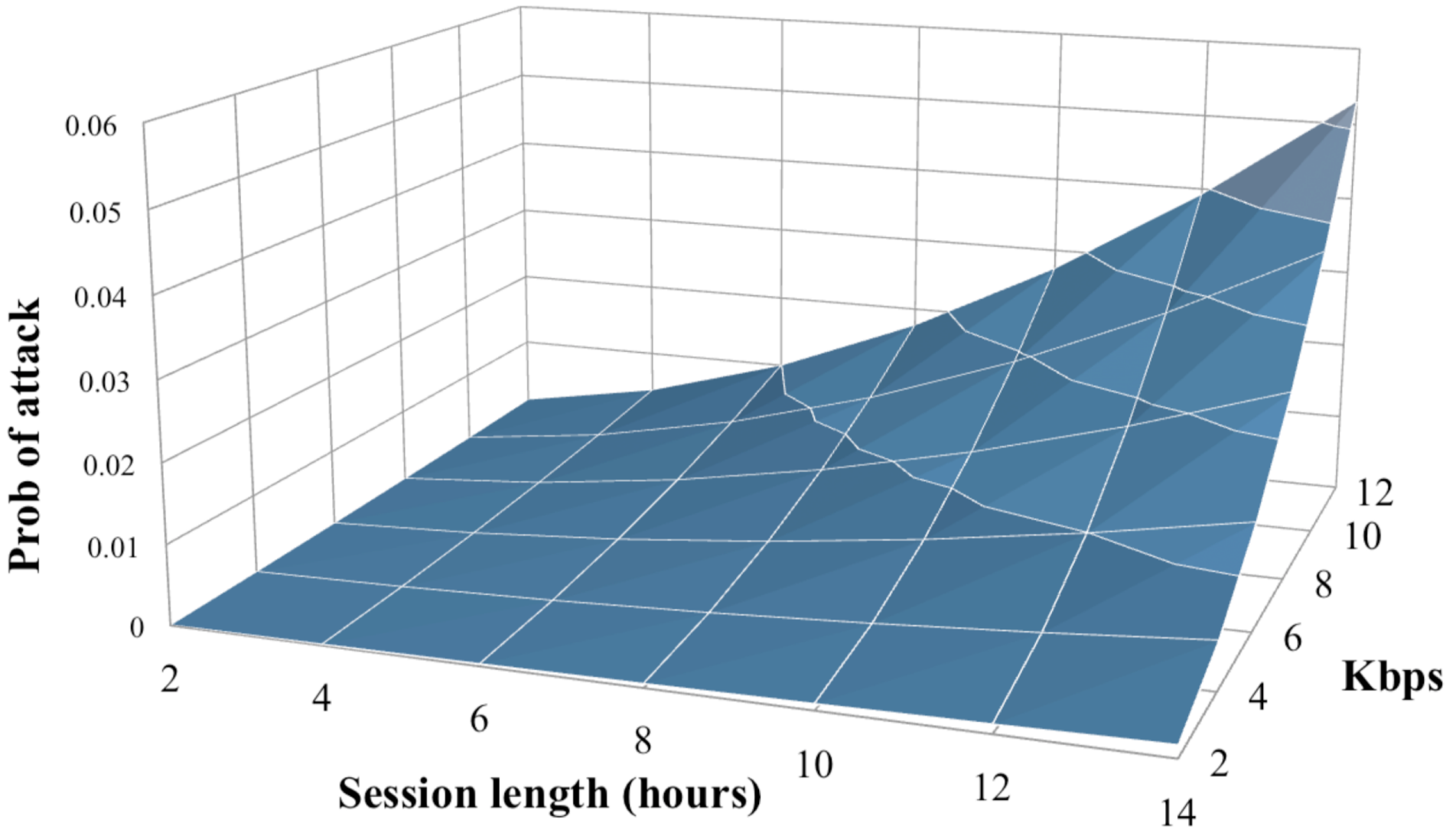
Examples

Two acknowledgement messages:

00120000020A9203A2105E0480000062105DFD0000000000
MAC: 80B7557F31566DBB
00120000020A9203AAE360078000006AE360000000000000
MAC: 80B7557F31566DBB

Continue at 300km/h; display “uWP3=k0d<CbKQn9{”:

003600000203OCD3C677A100000021F01C651FF809C408000
0000007E4801B90FFFD2000000120107557503330d6b30643c4
3624b516e397b
MAC: 80B7557F31566DBB


Prob of attack
0.06
0.05
0.04
0.03
0.02
0.01
0
2
4
6
8
10
12
14
Session length (hours)
2
4
6
8
10
12
Kbps

Must do list

- Every company must have a very clear place to report vulnerabilities.
- They must have a clear owner for all reported vulnerabilities.
- They must have a way to patch all devices in the field.

If your company doesn’t have this you cannot claim a good level of security.

Do not buy products from companies without this.

Why should you believe me?

I’ve shown you major breaks from my group on:

- TLS
- WPA
- Many of the worlds leading banks
- Almost all models of cars

And a very near miss against EuroRadio.

Conclusion

- You must accept your devices have cyber security vulnerabilities.
- A key measure of cyber security is how quickly you can receive and respond to new vulnerability reports.
- The rail industry is a long way behind the IT industry on this.

You Retweeted

kennyog @kennyog · 7 Dec 2018

I want to share a thought about cryptography and business. It's something I've hit upon a lot lately, in consulting, research, and responsible disclosure contexts: if you are a company and crypto is core to your business, then you need to hire some damn cryptographers.

3 23 74