TimeTrust: Robust Timing via Hareware Roots of Trust

University of Birmingham:

Andreea-Ina Radu
a.i.radu@bham.ac.uk

Tom Chothia
t.p.chothia@bham.ac.uk

University of Surrey:

Christopher J.P. Newton
c.newton@surrey.ac.uk

Ioana Boureanu
i.boureanu@surrey.ac.uk

Liqun Chen
liqun.chen@surrey.ac.uk

UNIVERSITY OF BIRMINGHAM

UNIVERSITY OF SURREY

The TimeTrust Project part of UK RISE (Research Institute in Secure Hardware and Embedded Systems)

Robust Timing via Hardware Roots of Trust and Non-standard Hardware -with Application to EMV Contactless Payments- (04/2019 – 11/2022)

UNIVERSITY OF SURREY

PI - Ioana Boureanu
Professor in Secure Systems

UNIVERSITY OF SURREY

Professor in Secure Systems

UNIVERSITY OF BIRMINGHAM

Anna Clee, PhD Student

UNIVERSITY OF SURREY

Chris Newton
Research Associate

UNIVERSITY OF BIRMINGHAM

Andreea-Ina Radu
Research Associate

Mike Ward
Director, Product Development and Innovation, EMV & Digital Devices

Charles Chen
Senior Director – EMV Solutions

Fraser Dickin
Senior Research Engineer

Steve Pannifer
Director

2

TimeTrust Research:

- The Closer You Look, The More You Learn: A Grey-box Approach to Protocol State
- Practical EMV Relay Protect
- Security Analysis and Implementation o Contactless Payment, CCS2020

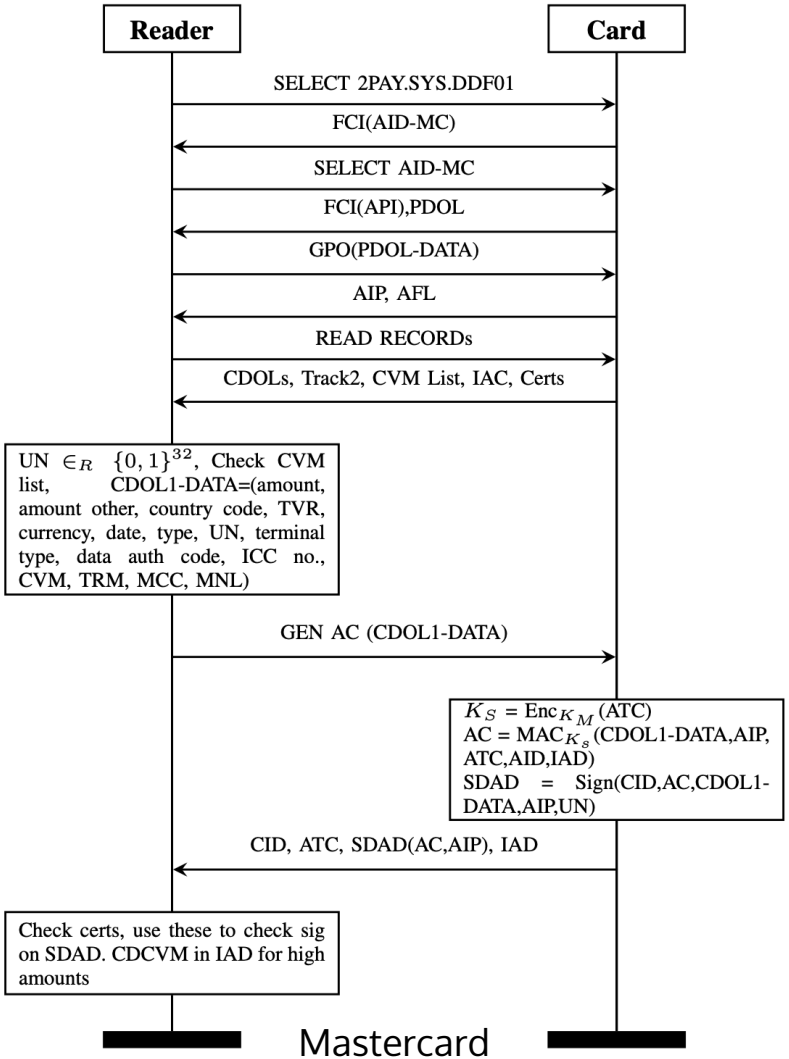
Protection for EMV from Malicious Shop Readers Using Tru

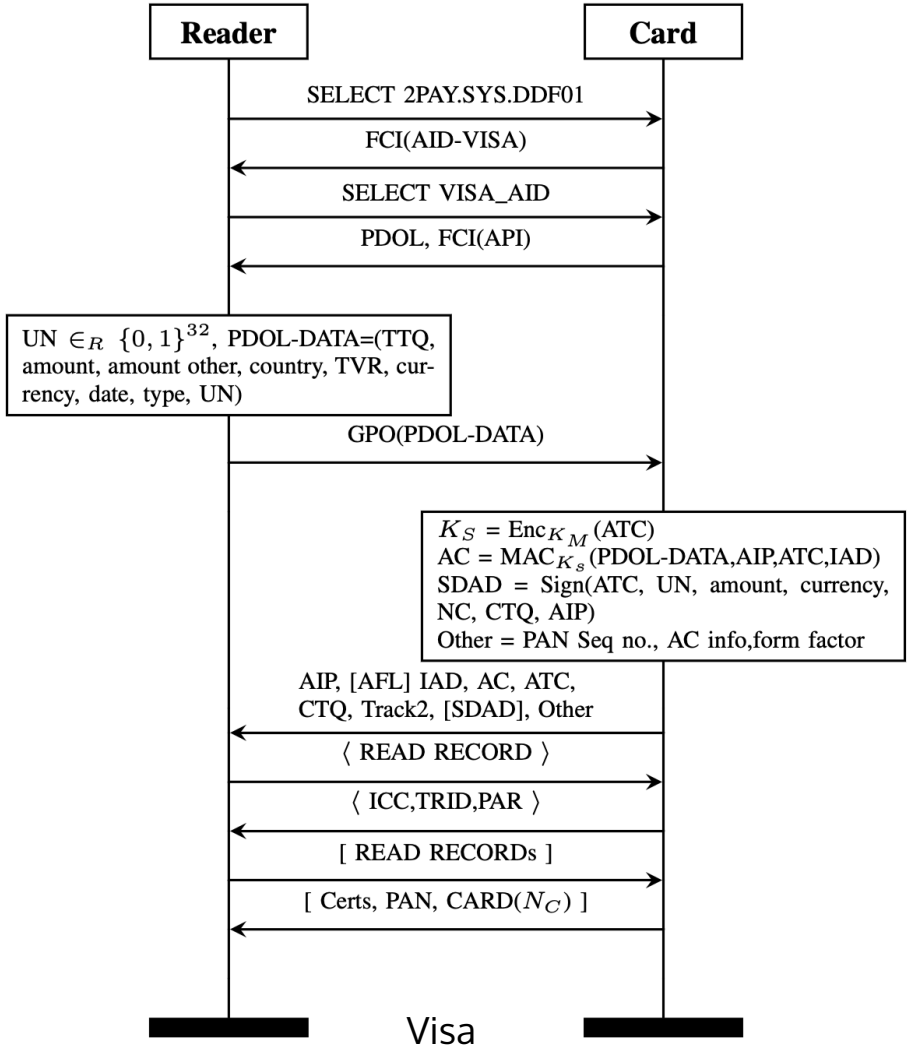
Fuzzing Methods to find logical flaws

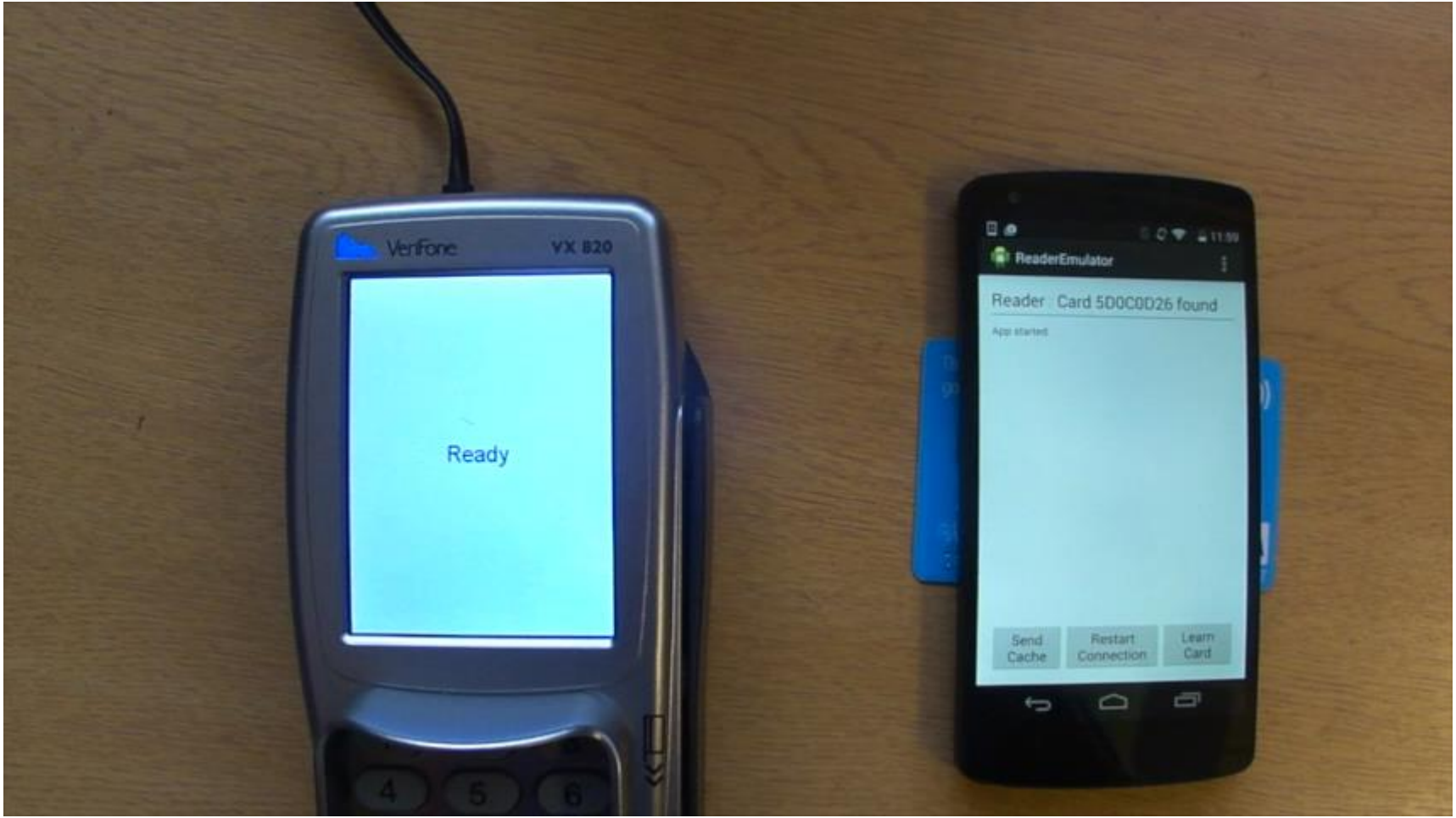
- plus papers on side channel resistance for sel4, ICS hardware vulnerabilities, theory of distance bounding, attack on Knox v2

UNIVERSITY OF BIRMINGHAM

UNIVERSITY OF SURREY


Reader
Card
SELECT 2PAY.SYS.DDF01
FCI(AID-MC)
SELECT AID-MC
FCI(API),PDOL
GPO(PDOL-DATA)
AIP, AFL
READ RECORDs
CDOLs, Track2, CVM List, IAC, Certs
UN $\in_R \{0,1\}^{32}$, Check CVM list, CDOL1-DATA=(amount, amount other, country code, TVR, currency, date, type, UN, terminal type, data auth code, ICC no., CVM, TRM, MCC, MNL)
GEN AC (CDOL1-DATA)
K_S = Enc$_{K_M}$(ATC)
AC = MAC$_{K_s}$(CDOL1-DATA,AIP, ATC,AID,IAD)
SDAD = Sign(CID,AC,CDOL1-DATA,AIP,UN)
CID, ATC, SDAD(AC,AIP), IAD
Check certs, use these to check sig on SDAD. CDCVM in IAD for high amounts
Mastercard


Reader
Card
SELECT 2PAY.SYS.DDF01
FCI(AID-VISA)
SELECT VISA_AID
PDOL, FCI(API)
UN $\in_R \{0,1\}^{32}$, PDOL-DATA=(TTQ, amount, amount other, country, TVR, currency, date, type, UN)
GPO(PDOL-DATA)
K_S = Enc$_{K_M}$(ATC)
AC = MAC$_{K_s}$(PDOL-DATA,AIP,ATC,IAD)
SDAD = Sign(ATC, UN, amount, currency, NC, CTQ, AIP)
Other = PAN Seq no., AC info,form factor
AIP, [AFL] IAD, AC, ATC, CTQ, Track2, [SDAD], Other
⟨ READ RECORD ⟩
⟨ ICC,TRID,PAR ⟩
[READ RECORDs]
[Certs, PAN, CARD(N_C)]
Visa


VeriFone
VX 820
Ready
4
5
6
ReaderEmulator
Reader : Card 5D0C0D26 found
App started
Send Cache
Restart Connection
Learn Card

Relay protections

relay resistant protocol

relay protection

vs

Samsung Pay

vs

Life was good in 2015

- The world stops a deadly virus (Ebola) by taking swift science-based measure.
- 195 countries sign the the Paris Climate Agreement.
- Global poverty at record low.
- Mr. Robot was released.
- There was finally a good Star Wars film

UNIVERSITY OF BIRMINGHAM

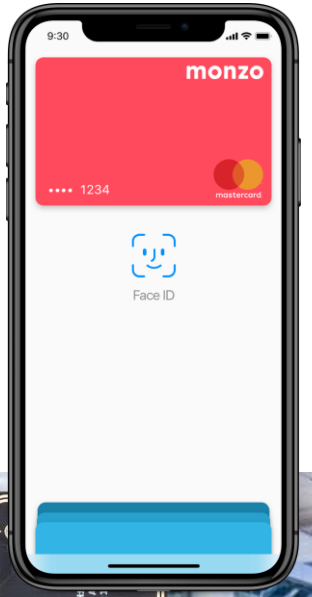
UNIVERSITY OF SURREY

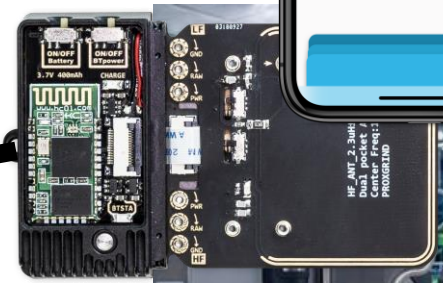
Apple Pay Express Travel

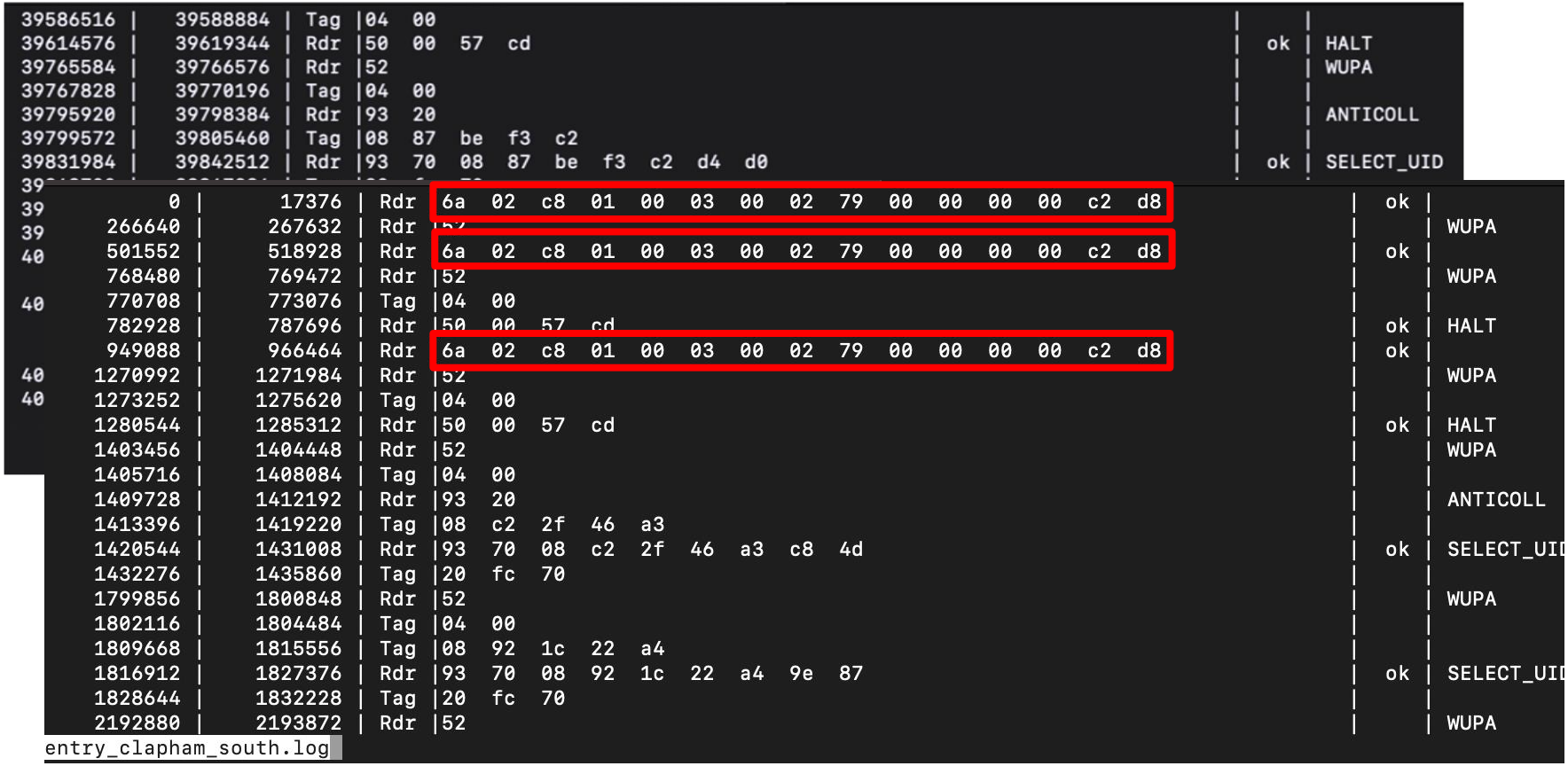
Pay |

Streamlined for London

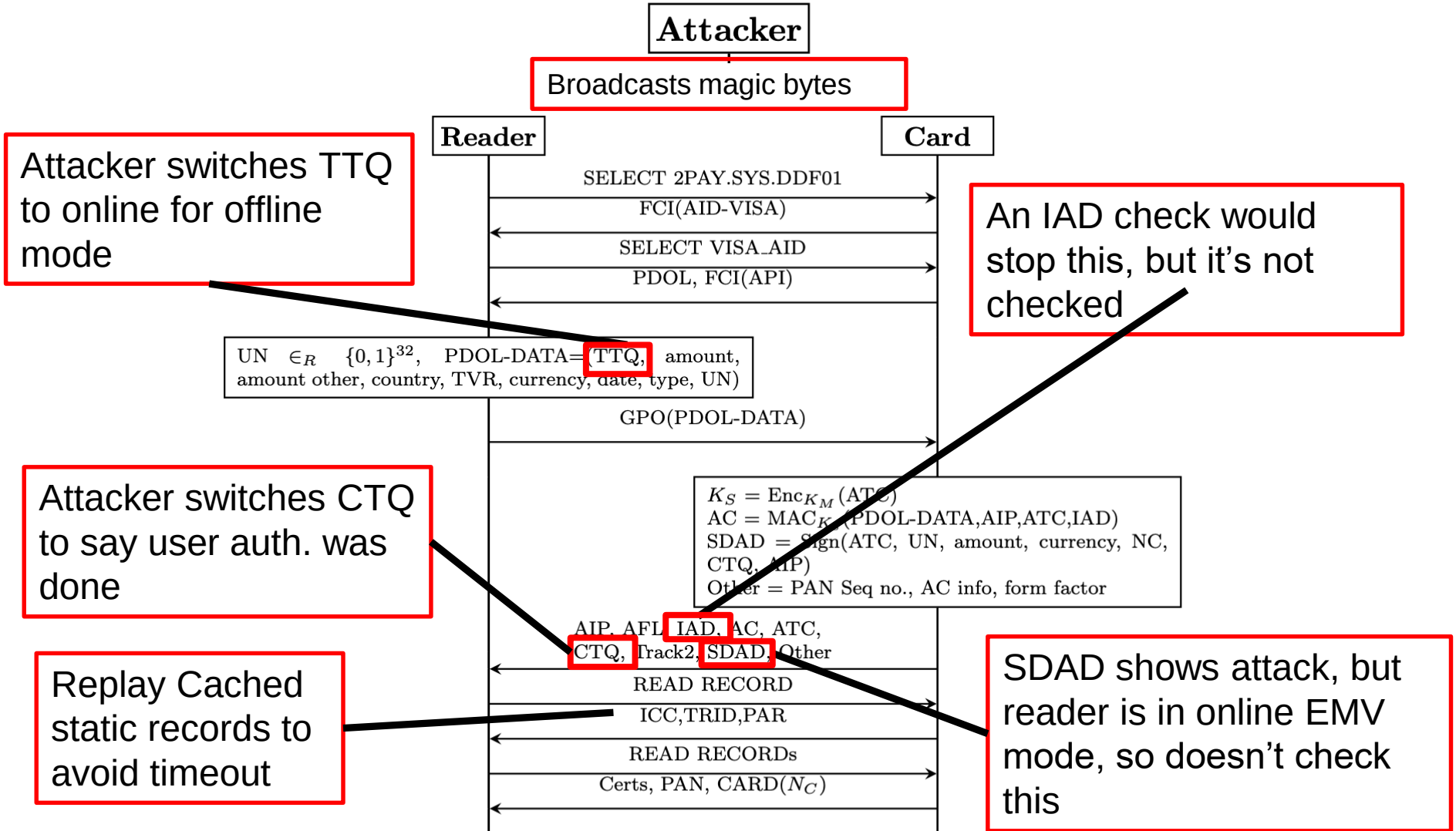
Paying for journeys on Transport for London is easier with Express Mode for Apple Pay. You no longer need to authenticate your payment with Face ID or Touch ID. Simply select a card for travel in Wallet. Then just tap your iPhone or Apple Watch on the yellow card reader and go.

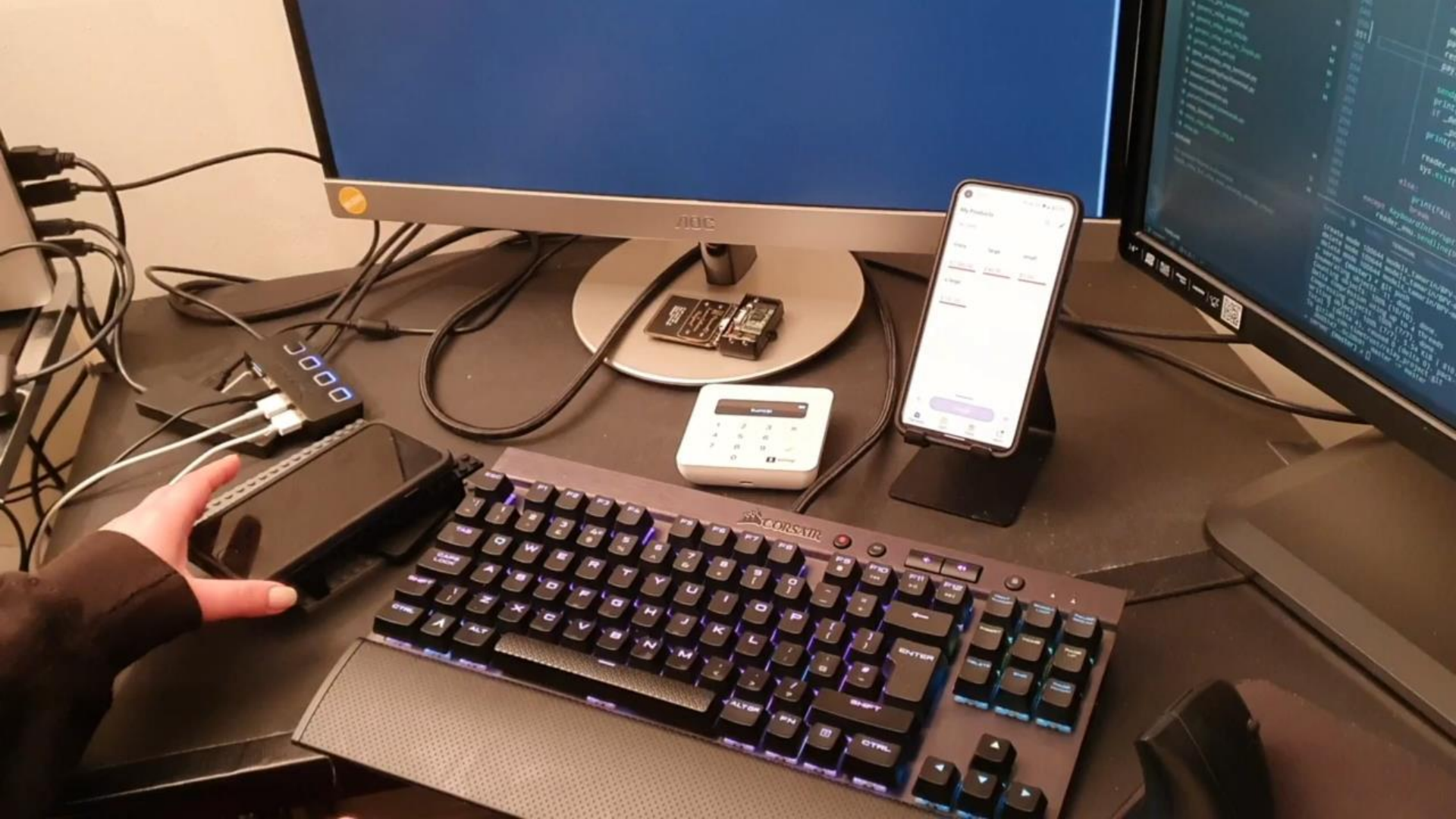

9:30
monzo
•••• 1234
mastercard
Face ID


ON/OFF
Battery
ON/OFF
BTpower
3.7V 400mAh
CHARGE
LF
HF

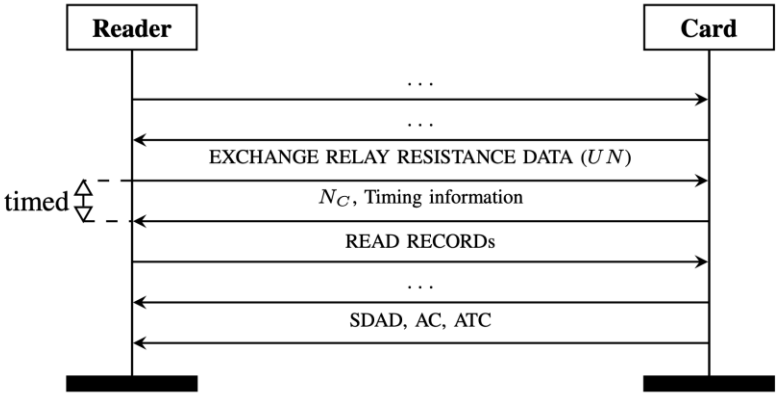


```
39586516 |   39588884 | Tag |04  00                                                                 |    |
39614576 |   39619344 | Rdr |50  00  57  cd                                                         |  ok | HALT
39765584 |   39766576 | Rdr |52                                                                     |    | WUPA
39767828 |   39770196 | Tag |04  00                                                                 |    |
39795920 |   39798384 | Rdr |93  20                                                                 |    | ANTICOLL
39799572 |   39805460 | Tag |08  87  be  f3  c2                                                     |    |
39831984 |   39842512 | Rdr |93  70  08  87  be  f3  c2  d4  d0                                     |  ok | SELECT_UID
39
39             0 |      17376 | Rdr |6a  02  c8  01  00  03  00  02  79  00  00  00  00  c2  d8                 |  ok |
39        266640 |     267632 | Rdr |                                                                       |    | WUPA
40        501552 |     518928 | Rdr |6a  02  c8  01  00  03  00  02  79  00  00  00  00  c2  d8                 |  ok |
          768480 |     769472 | Rdr |52                                                                     |    | WUPA
40        770708 |     773076 | Tag |04  00                                                                 |    |
          782928 |     787696 | Rdr |50  00  57  cd                                                         |  ok | HALT
          949088 |     966464 | Rdr |6a  02  c8  01  00  03  00  02  79  00  00  00  00  c2  d8                 |  ok |
40       1270992 |    1271984 | Rdr |52                                                                     |    | WUPA
40       1273252 |    1275620 | Tag |04  00                                                                 |    |
         1280544 |    1285312 | Rdr |50  00  57  cd                                                         |  ok | HALT
         1403456 |    1404448 | Rdr |52                                                                     |    | WUPA
         1405716 |    1408084 | Tag |04  00                                                                 |    |
         1409728 |    1412192 | Rdr |93  20                                                                 |    | ANTICOLL
         1413396 |    1419220 | Tag |08  c2  2f  46  a3                                                     |    |
         1420544 |    1431008 | Rdr |93  70  08  c2  2f  46  a3  c8  4d                                     |  ok | SELECT_UID
         1432276 |    1435860 | Tag |20  fc  70                                                             |    |
         1799856 |    1800848 | Rdr |52                                                                     |    | WUPA
         1802116 |    1804484 | Tag |04  00                                                                 |    |
         1809668 |    1815556 | Tag |08  92  1c  22  a4                                                     |    |
         1816912 |    1827376 | Rdr |93  70  08  92  1c  22  a4  9e  87                                     |  ok | SELECT_UID
         1828644 |    1832228 | Tag |20  fc  70                                                             |    |
         2192880 |    2193872 | Rdr |52                                                                     |    | WUPA
entry_clapham_south.log
```


Attacker
Broadcasts magic bytes
Reader
Card
Attacker switches TTQ to online for offline mode
An IAD check would stop this, but it's not checked
SELECT 2PAY.SYS.DDF01
FCI(AID-VISA)
SELECT VISA_AID
PDOL, FCI(API)
UN $\in_R$ $\{0,1\}^{32}$, PDOL-DATA=(TTQ, amount, amount other, country, TVR, currency, date, type, UN)
GPO(PDOL-DATA)
Attacker switches CTQ to say user auth. was done
$K_S = \text{Enc}_{K_M}(\text{ATC})$
AC = MAC_{K_S}(PDOL-DATA,AIP,ATC,IAD)
SDAD = Sign(ATC, UN, amount, currency, NC, CTQ, AIP)
Other = PAN Seq no., AC info, form factor
AIP, AFL, IAD, AC, ATC, CTQ, Track2, SDAD, Other
READ RECORD
Replay Cached static records to avoid timeout
ICC,TRID,PAR
READ RECORDs
Certs, PAN, CARD(N_C)
SDAD shows attack, but reader is in online EMV mode, so doesn't check this


AOC
CORSAIR
ENTER
SHIFT
CTRL

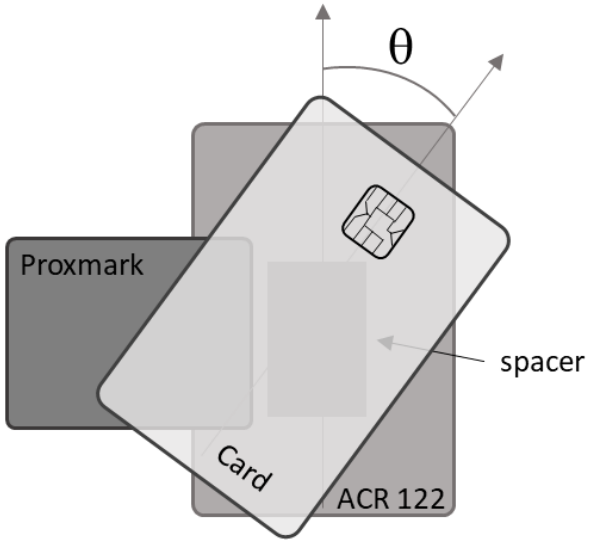
Mastercard Relay Resistant Protocol

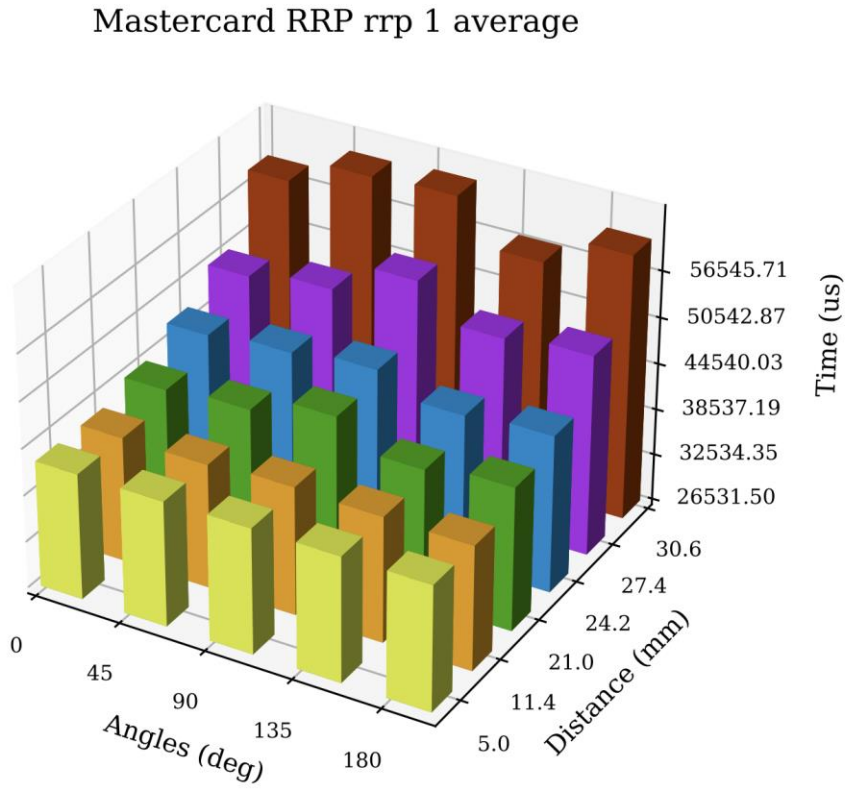


VS

ERSITY OF
RREY

Mastercard Relay Resistant Protocol





Visa's Relay Protection Protocol

- Works at ISO 14443 Level 1, so really good timing!
- Broken due to rookie protocol mistakes.
- They aimed to only protect against attacks using COTS mobile phones but failed to do that.
- Models in Tamarin and ProVerif, but not really needed.

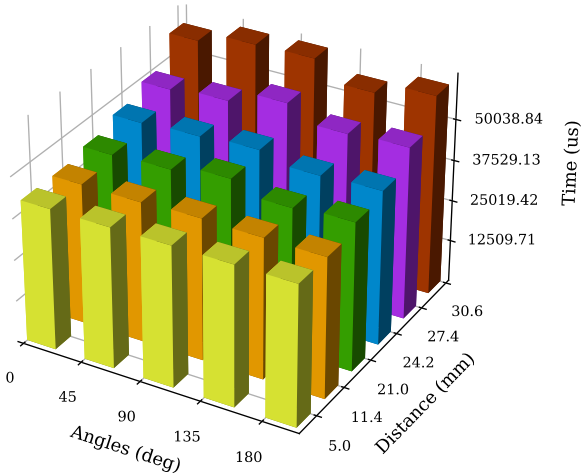
UNIVERSITY OF BIRMINGHAM

UNIVERSITY OF SURREY

How do we solve all this?

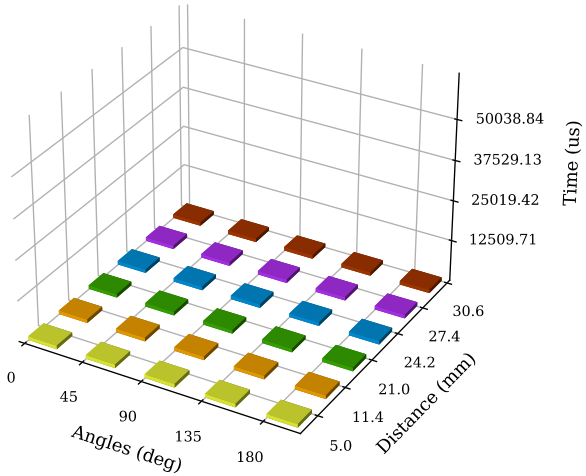
Application level

Mastercard RRP rrp 1 average

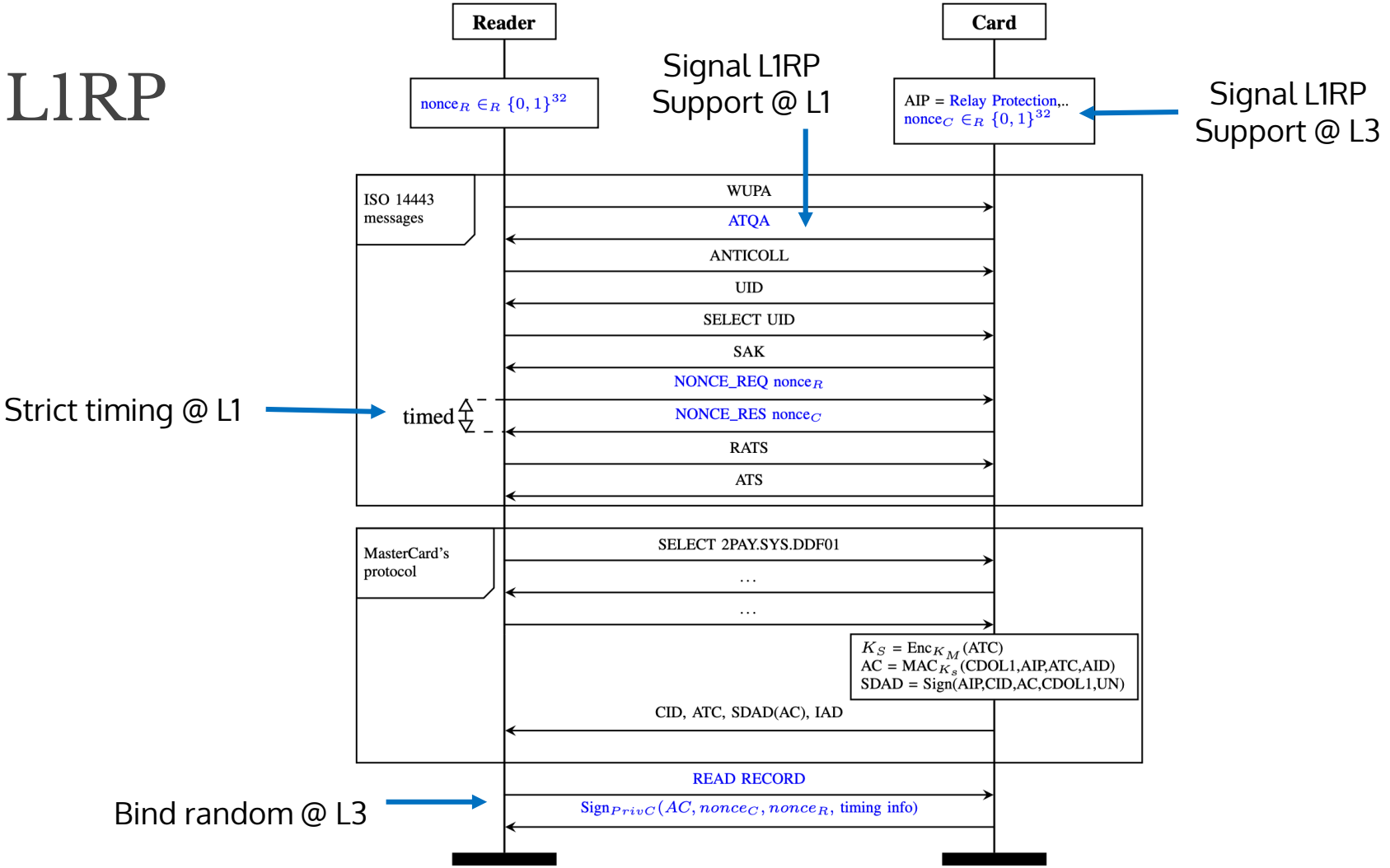


Anticollision level

Mastercard RRP select uid average



L1RP


Reader
Card
nonce$_R$ $\in_R$ $\{0,1\}^{32}$
AIP = Relay Protection,..
nonce$_C$ $\in_R$ $\{0,1\}^{32}$
Signal L1RP Support @ L1
Signal L1RP Support @ L3
ISO 14443 messages
WUPA
ATQA
ANTICOLL
UID
SELECT UID
SAK
NONCE_REQ nonce$_R$
NONCE_RES nonce$_C$
RATS
ATS
Strict timing @ L1
timed
MasterCard's protocol
SELECT 2PAY.SYS.DDF01
...
...
K_S = Enc$_{K_M}$(ATC)
AC = MAC$_{K_s}$(CDOL1,AIP,ATC,AID)
SDAD = Sign(AIP,CID,AC,CDOL1,UN)
CID, ATC, SDAD(AC), IAD
READ RECORD
Sign$_{PrivC}$($AC, nonce_C, nonce_R$, timing info)
Bind random @ L3

Adding our Protocol to the ISO 14443 Standard

- March: Reach out to the ISO/ IEC 14443 BSI UK mirror group
- July: Present the proposal to them in person and get their approval.
- August: get support of EMV Co. and NXP
- Oct: They took it to ISO smart card security working group ISO/IEC JTC 1/SC 17/WG 8, Berlin, who have approved the addition in principle.
- Next, we write a full draft to by voted on by all ISO countries (usually follows the working group)

UNIVERSITY OF BIRMINGHAM

UNIVERSITY OF SURREY

Question?