ETH zürich

PURE:
Payments with UWB RElay-protection

D. Coppola

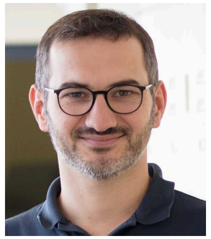
G. Camurati

C. Anliker

X. Hofmeier

P. Schaller

D. Basin


S. Capkun

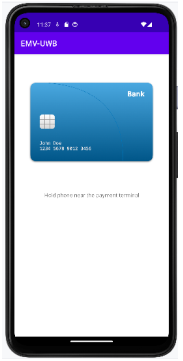
Relay Attacks on Contactless Payments

* A Practical Relay Attack on ISO 14443 Proximity Cards, G.Hancke

Relay Attacks on Contactless Payments

* A Practical Relay Attack on ISO 14443 Proximity Cards, G.Hancke

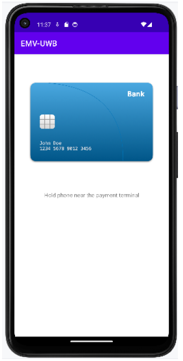
Relay Attacks on Contactless Payments



Hold phone near the payment terminal

* A Practical Relay Attack on ISO 14443 Proximity Cards, G.Hancke

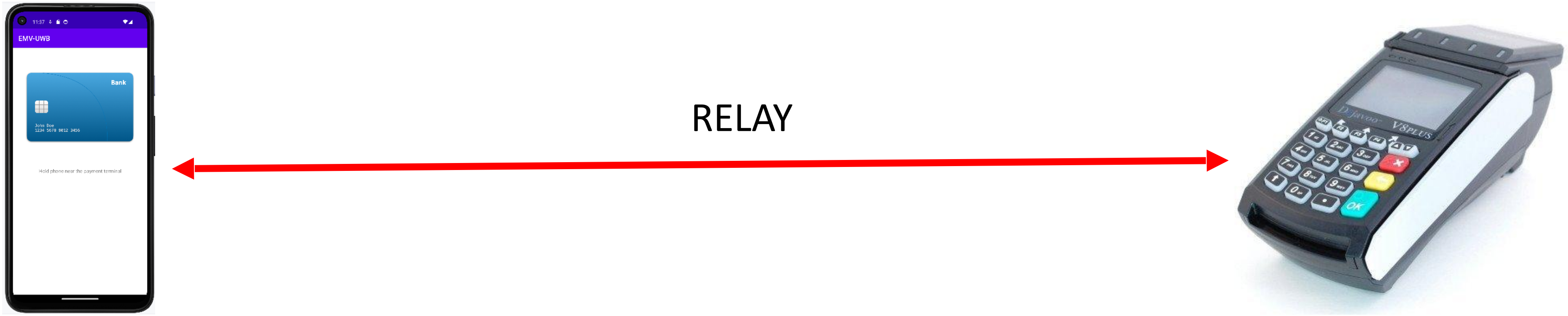
Relay Attacks on Contactless Payments



Hold phone near the payment terminal

* A Practical Relay Attack on ISO 14443 Proximity Cards, G.Hancke

Relay Attacks on Contactless Payments



EMV-UWB

Bank

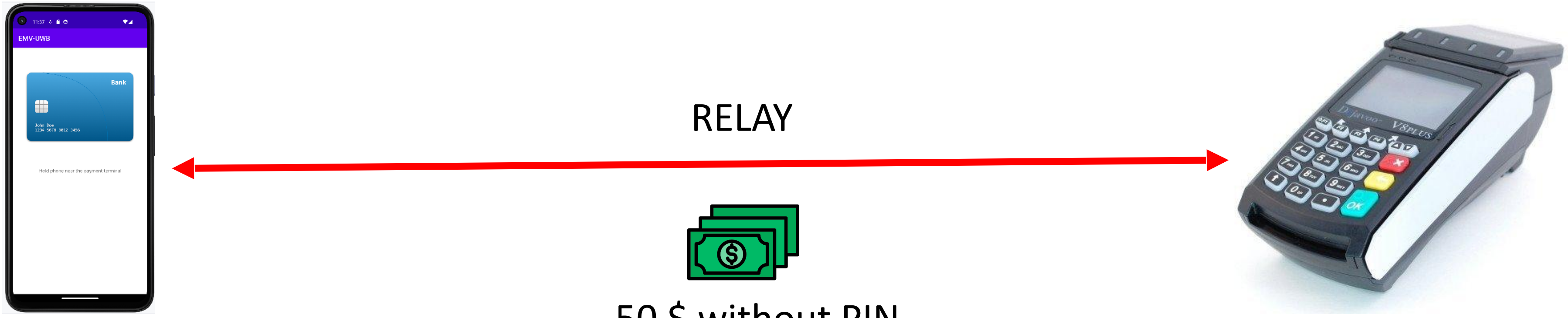
John Doe
1234 5678 9012 3456

Hold phone near the payment terminal

RELAY

* A Practical Relay Attack on ISO 14443 Proximity Cards, G.Hancke

Relay Attacks on Contactless Payments

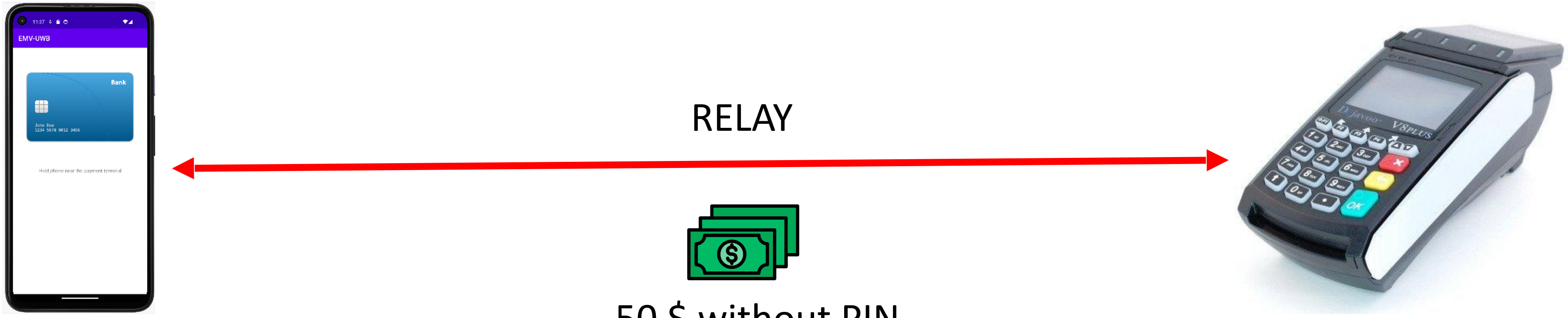


RELAY

~50 $ without PIN
Up to card limit with an unlocked phone

* A Practical Relay Attack on ISO 14443 Proximity Cards, G.Hancke

Relay Attacks on Contactless Payments

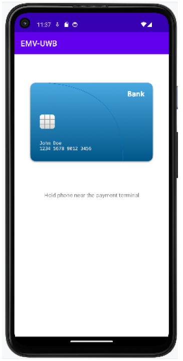


~50 $ without PIN
Up to card limit with an unlocked phone

Logical layer relays

* A Practical Relay Attack on ISO 14443 Proximity Cards, G.Hancke

Relay Attacks on Contactless Payments



11:37

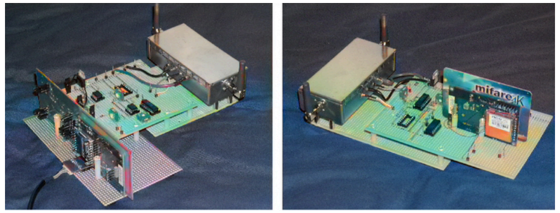
EMV-UWB

Hold phone near the payment terminal

RELAY

~50 $ without PIN
Up to card limit with an unlocked phone

Logical layer relays

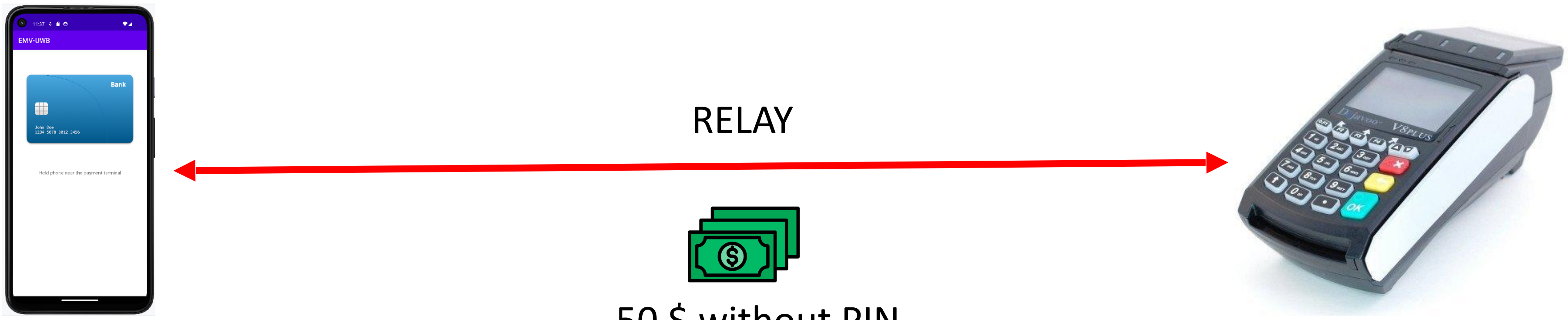


*

Physical layer relays

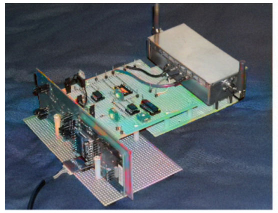
* A Practical Relay Attack on ISO 14443 Proximity Cards, G.Hancke

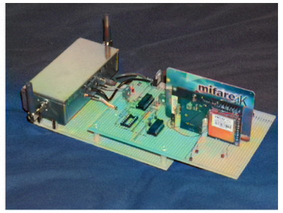
Relay Attacks on Contactless Payments



~50 $ without PIN
Up to card limit with an unlocked phone

Logical layer relays



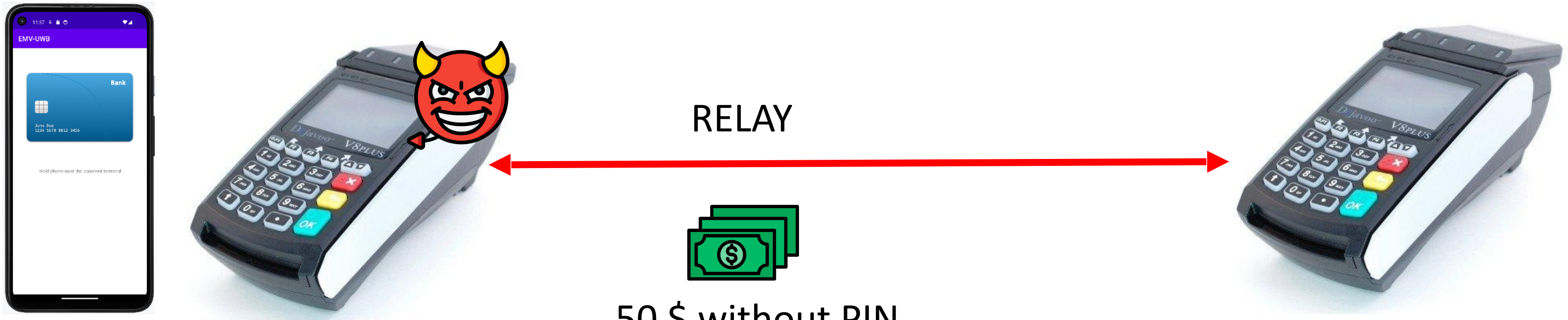


*

Physical layer relays

* A Practical Relay Attack on ISO 14443 Proximity Cards, G.Hancke

Relay Attacks on Contactless Payments

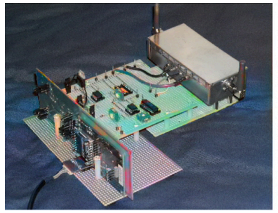


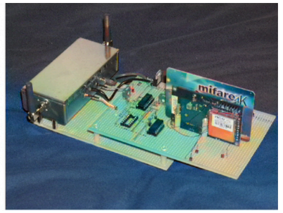
RELAY

Fake terminal

~50 $ without PIN
Up to card limit with an unlocked phone

Logical layer relays



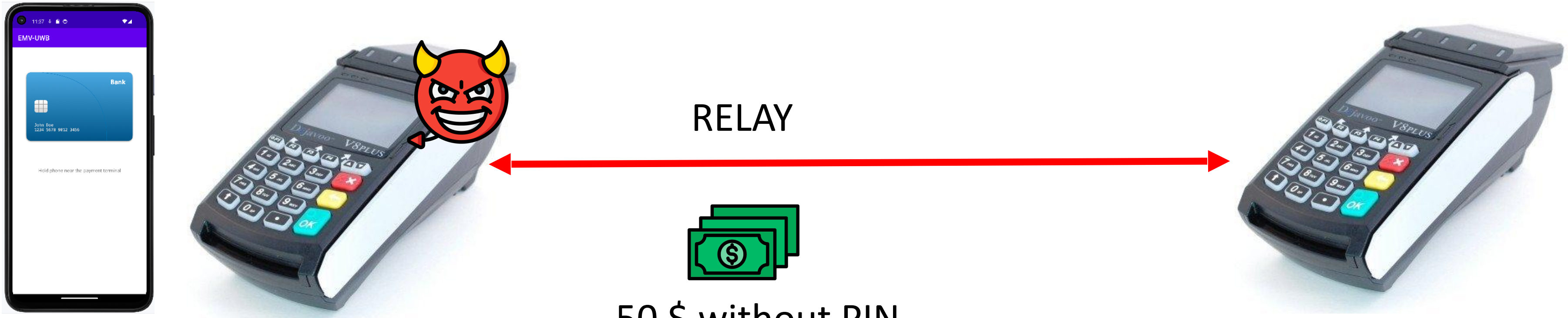


*

Physical layer relays

* A Practical Relay Attack on ISO 14443 Proximity Cards, G.Hancke

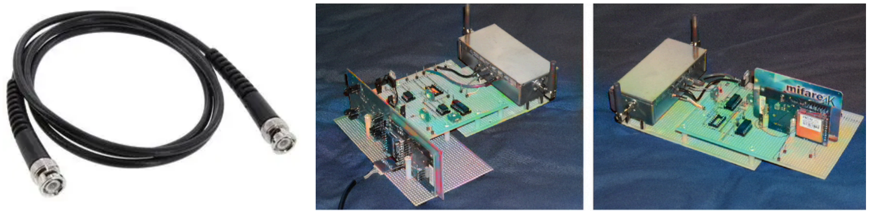
Relay Attacks on Contactless Payments



Fake terminal

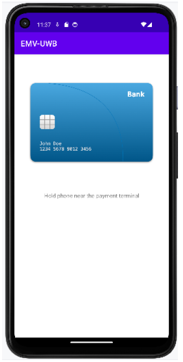
~50 $ without PIN
Up to card limit with an unlocked phone

	Existing countermeasures
Logical layer relays	✓
Physical layer relays	✗ ~ km

 *

* A Practical Relay Attack on ISO 14443 Proximity Cards, G.Hancke

Relay Attacks on Contactless Payments


11:37

EMV-UWB

Bank

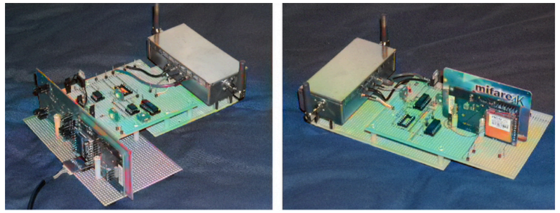
John Doe
1234 5678 9012 3456

Hold phone near the payment terminal

Fake terminal

RELAY

~50 $ without PIN
Up to card limit with an unlocked phone

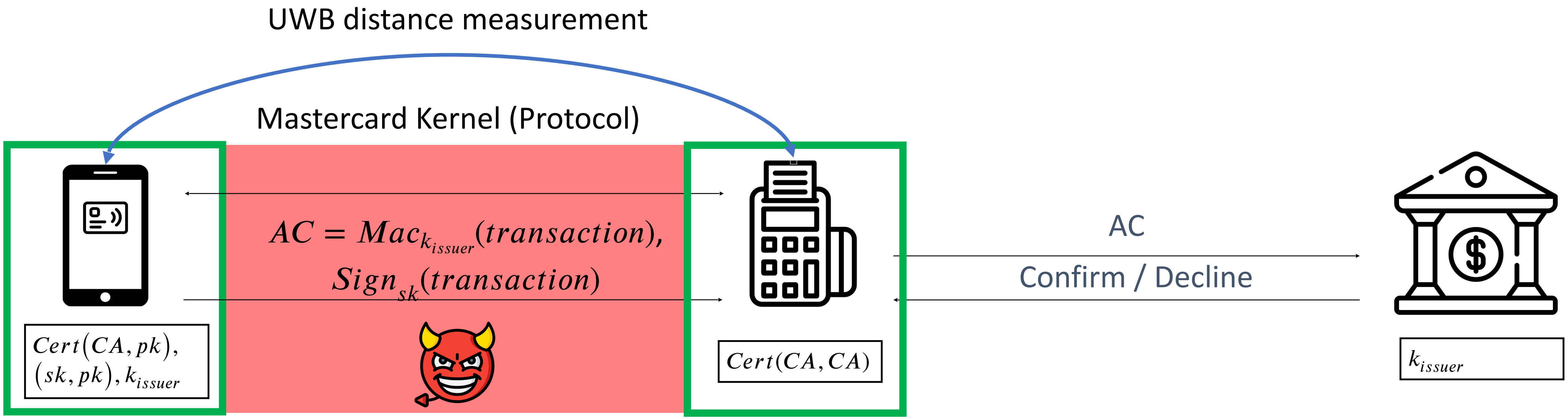


*

	Existing countermeasures	PURE
Logical layer relays	✓	✓
Physical layer relays	✗ ~ km	✓ ~ 50 cm

* A Practical Relay Attack on ISO 14443 Proximity Cards, G.Hancke

PURE in the Payment Ecosystem



UWB distance measurement

Mastercard Kernel (Protocol)

$AC = Mac_{k_{issuer}}(transaction),$

$Sign_{sk}(transaction)$

$Cert(CA, pk),$
$(sk, pk), k_{issuer}$

$Cert(CA, CA)$

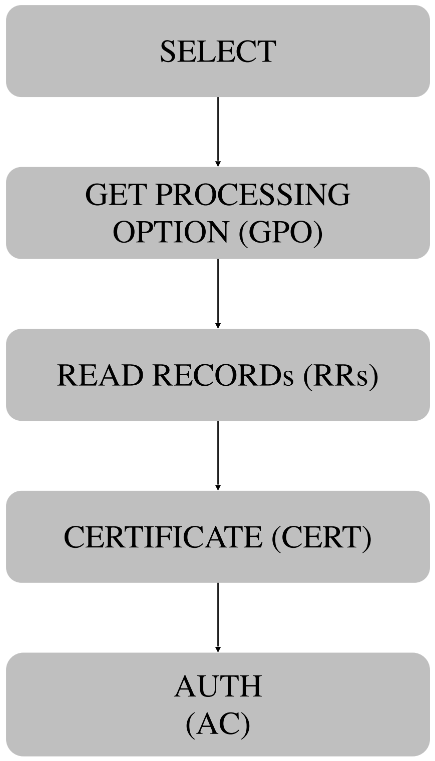
AC

Confirm / Decline

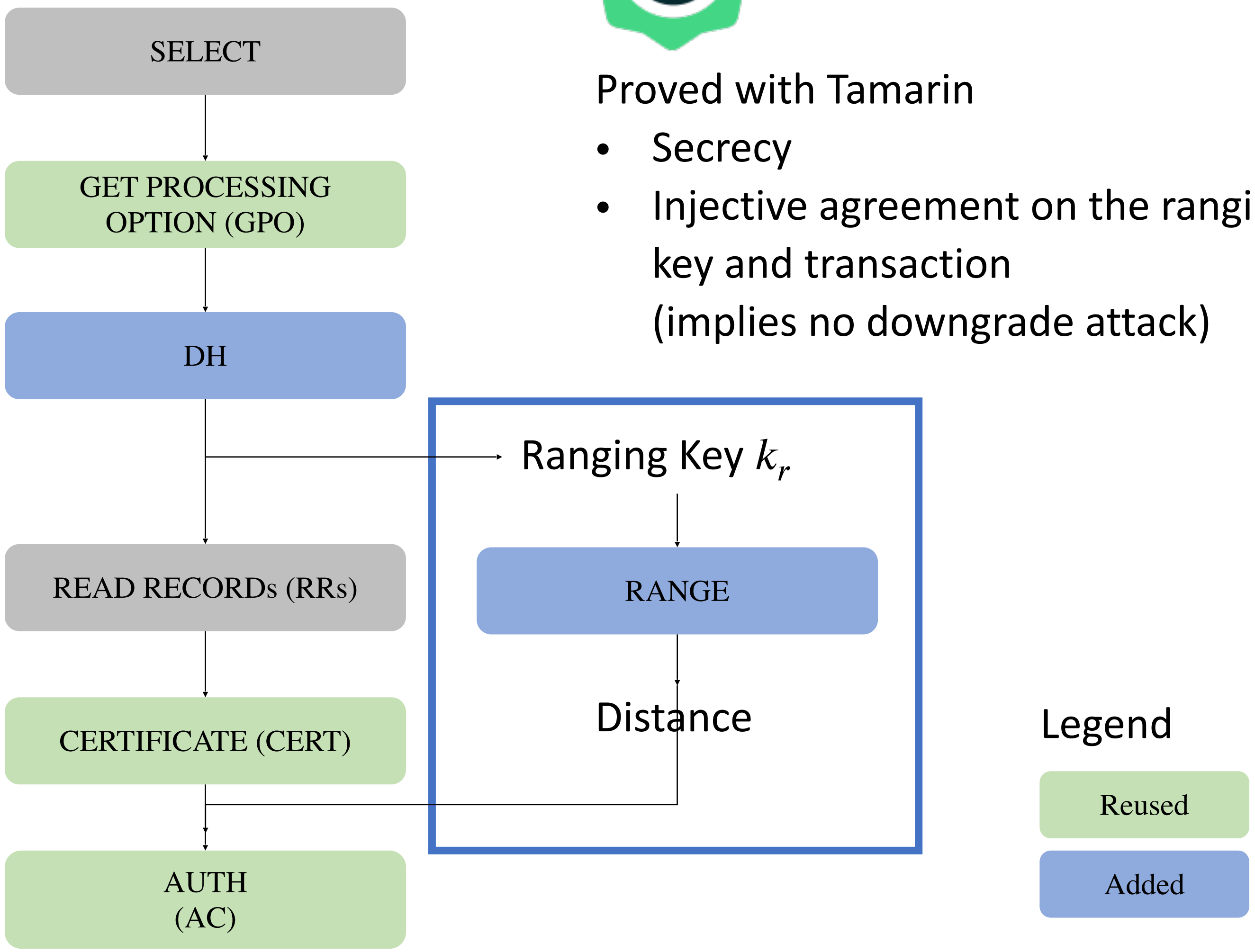
k_{issuer}

PURE specifically target
smartphone payments

PURE Protocol Extension



1. Mastercard Kernel

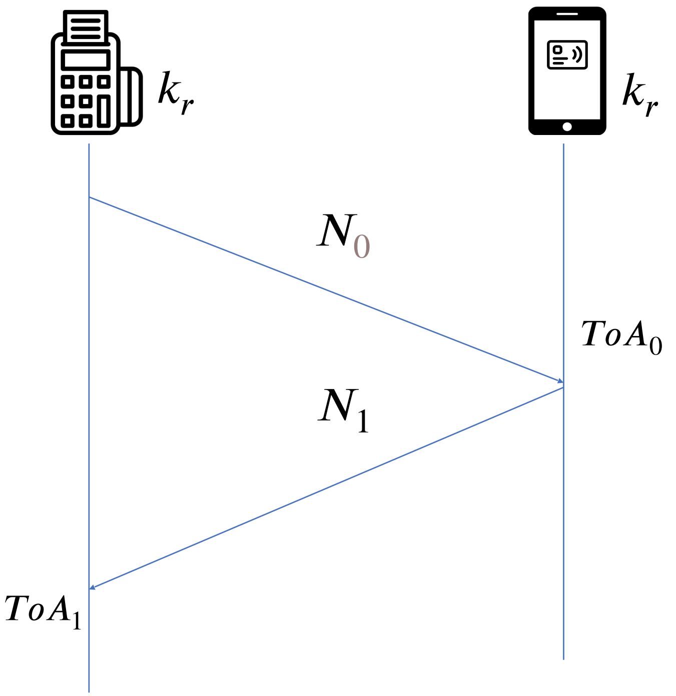


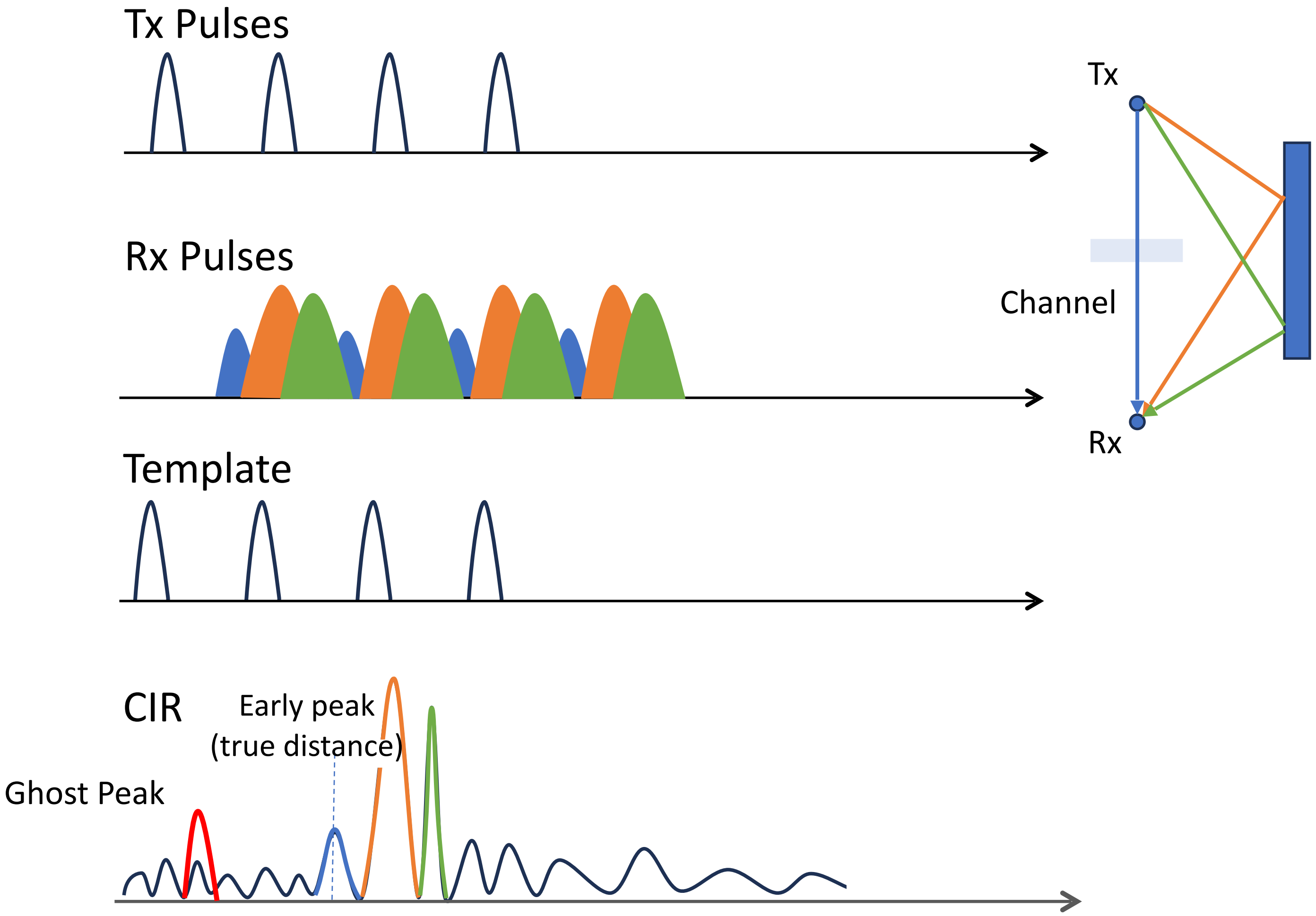
2. Mastercard Kernel + PURE

Proved with Tamarin

- Secrecy
- Injective agreement on the ranging key and transaction (implies no downgrade attack)

UWB Ranging



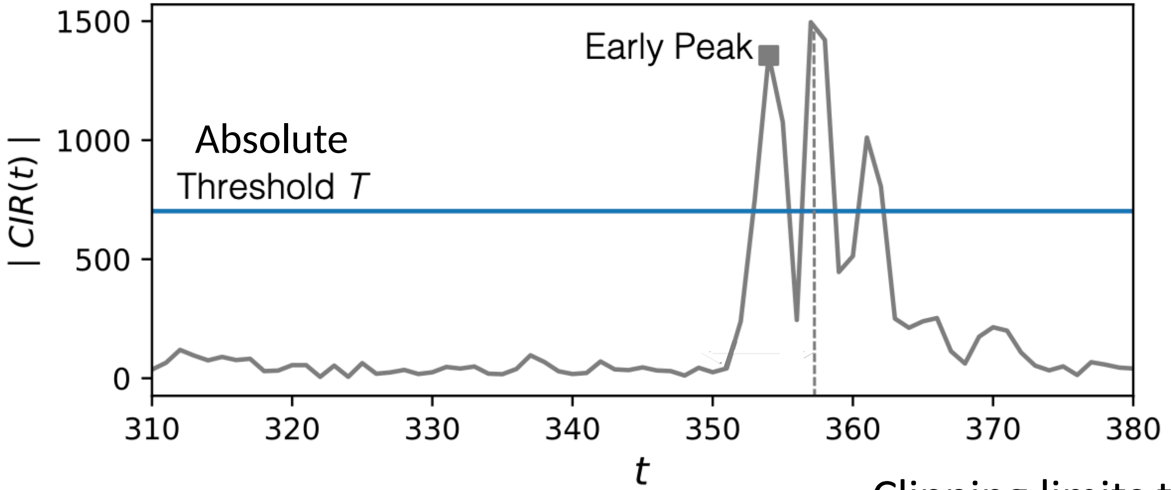


ToF = Time of Flight

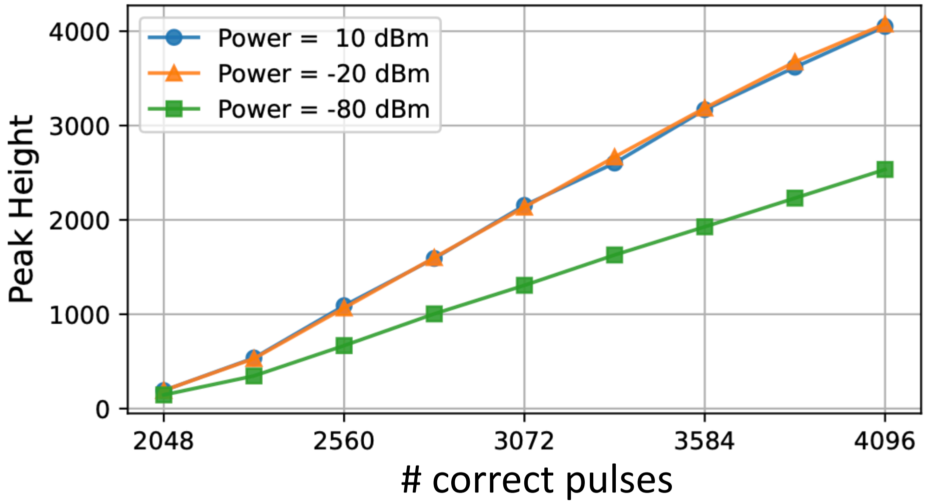
ToA = Time of Arrival

CIR = Channel Impulse Response

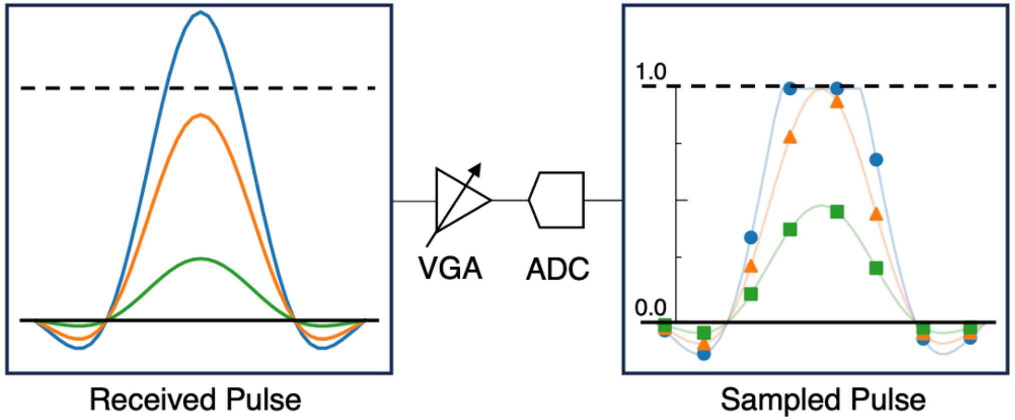
Security of the Time of Arrival Verification



More power⇏Higher peaks



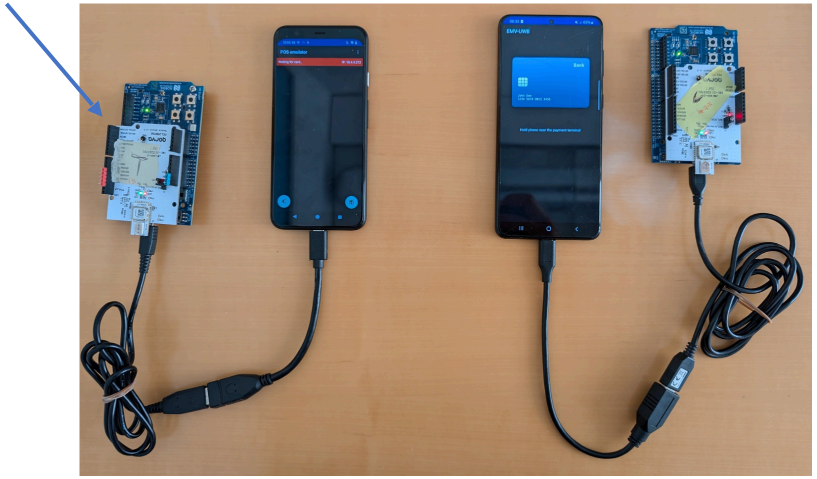
Clipping limits the contribution of each pulse



- A fixed threshold forces the adversary to correctly guess a certain amount of pulses
- We fix out threshold to limit the probability of a Ghost Peak attack to 2^{-48}

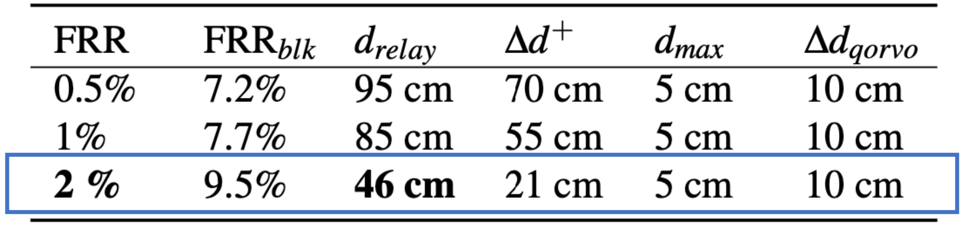
Putting it all together

External UWB chip for richer API

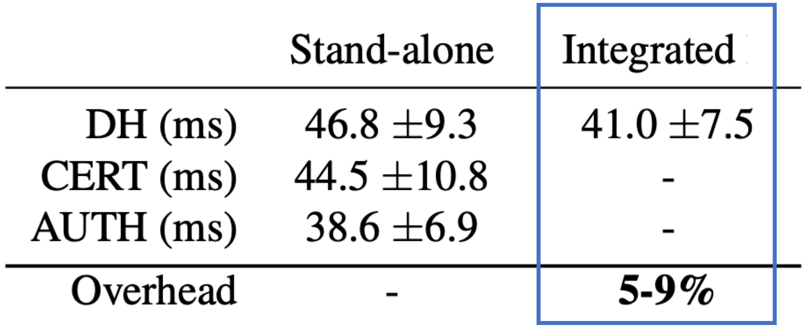


PURE terminal

PURE card



FRR	FRR$_{blk}$	d_{relay}	Δd^{+}	d_{max}	Δd_{qorvo}
0.5%	7.2%	95 cm	70 cm	5 cm	10 cm
1%	7.7%	85 cm	55 cm	5 cm	10 cm
2 %	9.5%	**46 cm**	21 cm	5 cm	10 cm



	Stand-alone	Integrated
DH (ms)	46.8 ±9.3	41.0 ±7.5
CERT (ms)	44.5 ±10.8	-
AUTH (ms)	38.6 ±6.9	-
Overhead	-	**5-9%**

Conclusion

Limitations

- PURE is not applicable to physical cards because not equipped with UWB chips
- PURE backward compatibility requires large deployments on terminals

Main contributions

- PURE protects mobile contactless transactions from relays greater than 50 cm
- The protocol extension was proven secure in Tamarin
- The ToA verification function protects against Ghost Peak attack
- The payment channels characterization shows PURE achieves high reliability (2% FRR)

Artifacts at
https://github.com/pure-uwb