MAY THE FORCE BE WITH YOU: FORCE-BASED RELAY ATTACK DETECTION

Iakovos Gurulian[1], Gerhard P. Hancke[2], Konstantinos Markantonakis[1], and Raja Naeem Akram[1]
iakovos.gurulian.2014@live.rhul.ac.uk, gp.hancke@cityu.edu.hk, {k.markantonakis, r.n.akram}@rhul.ac.uk

November 14, 2017

[1] Information Security Group, Smart Card and IoT Security Centre
Royal Holloway, University of London

[2] Department of Computer Science
City University of Hong Kong, 83 Tat Chee Avenue, Kowloon, Hong Kong

RELAY ATTACKS

RELAY ATTACKS

Definition

A relay attack is a passive man-in-the-middle attack during which an attacker is extending the communication distance of two legitimate devices by relaying each communication message between them, without the legitimate user's consent.

RELAY ATTACKS

Definition

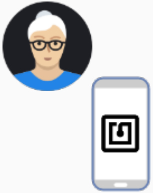
A relay attack is a passive man-in-the-middle attack during which an attacker is extending the communication distance of two legitimate devices by relaying each communication message between them, without the legitimate user’s consent.

Potential attack vectors:

- Unauthorised payments
- Unauthorised access to buildings and facilities
- User impersonation

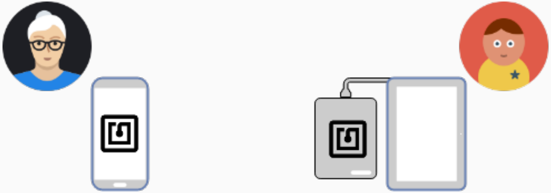
ANATOMY OF A RELAY ATTACK

Use Case: Contactless Payment



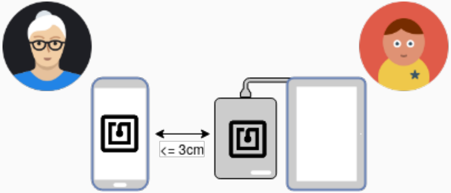
ANATOMY OF A RELAY ATTACK

Use Case: Contactless Payment



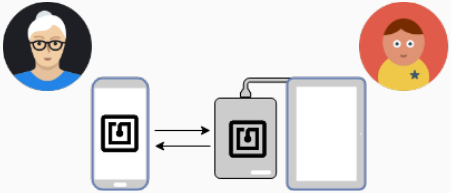
ANATOMY OF A RELAY ATTACK

Use Case: Contactless Payment



ANATOMY OF A RELAY ATTACK

Use Case: Contactless Payment



ANATOMY OF A RELAY ATTACK

Use Case: Contactless Payment

ANATOMY OF A RELAY ATTACK

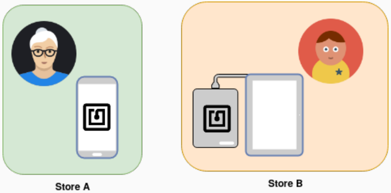
Use Case: Contactless Payment

ANATOMY OF A RELAY ATTACK

Use Case: Contactless Payment

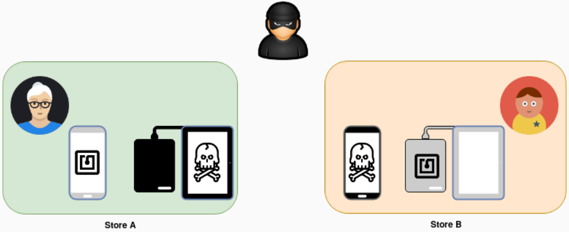
ANATOMY OF A RELAY ATTACK

Use Case: Contactless Payment



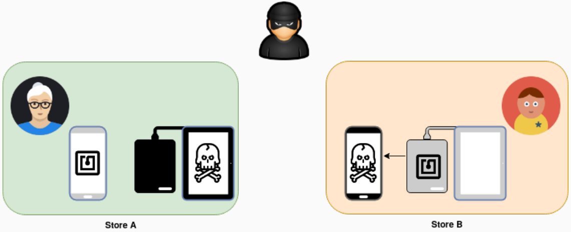
ANATOMY OF A RELAY ATTACK

Use Case: Contactless Payment

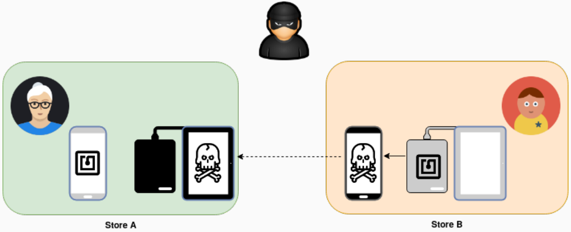


ANATOMY OF A RELAY ATTACK

Use Case: Contactless Payment

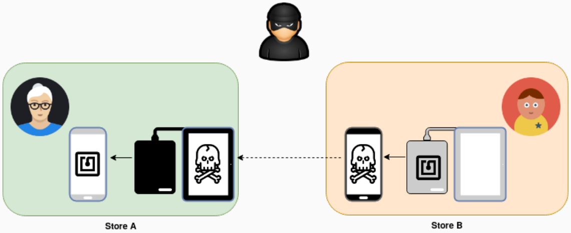


Use Case: Contactless Payment



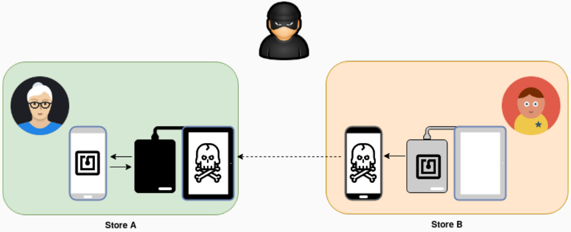
ANATOMY OF A RELAY ATTACK

Use Case: Contactless Payment



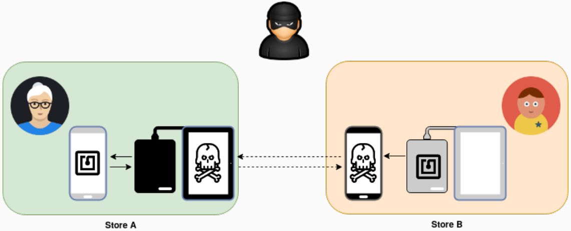
ANATOMY OF A RELAY ATTACK

Use Case: Contactless Payment



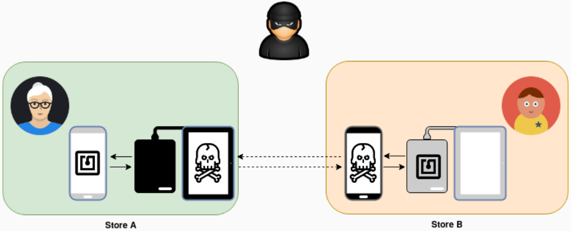
ANATOMY OF A RELAY ATTACK

Use Case: Contactless Payment



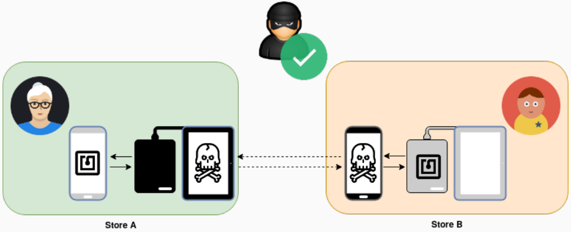
ANATOMY OF A RELAY ATTACK

Use Case: Contactless Payment



ANATOMY OF A RELAY ATTACK

Use Case: Contactless Payment



RELAY ATTACK DETECTION

(Contactless) Smart Cards

Distance bounding protocols have been proposed.

RELAY ATTACK DETECTION

(Contactless) Smart Cards

Distance bounding protocols have been proposed.

Smartphones

- Distance bounding protocols may not be applicable:
  - Multitude of hardware
  - Multiple processes running
- Sensing the ambient environment has been proposed instead (more on the next slide)

RELAY ATTACK DETECTION USING THE NATURAL AMBIENT ENVIRONMENT

NATURAL AMBIENT ENVIRONMENT-BASED RELAY ATTACK DETECTION

NATURAL AMBIENT ENVIRONMENT-BASED RELAY ATTACK DETECTION

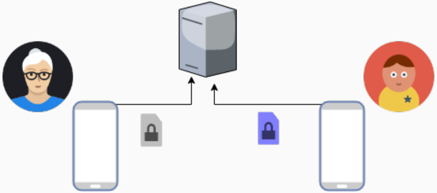
- Both devices measure the ambient environment using some sensor(s) for some pre-defined time
  - Temperature
  - Accelerometer
  - GPS
  - ...
- Transfer the captured values to one of the devices, or a trusted third party
- Compare the captured values
- Return decision based on the similarity of the captured values

NATURAL AMBIENT ENVIRONMENT-BASED RELAY ATTACK DETECTION

- Both devices measure the ambient environment using some sensor(s) for some pre-defined time
  - Temperature
  - Accelerometer
  - GPS
  - ...
- Transfer the captured values to one of the devices, or a trusted third party
- Compare the captured values
- Return decision based on the similarity of the captured values

NATURAL AMBIENT ENVIRONMENT-BASED RELAY ATTACK DETECTION

- Both devices measure the ambient environment using some sensor(s) for some pre-defined time
  - Temperature
  - Accelerometer
  - GPS
  - ...
- Transfer the captured values to one of the devices, or a trusted third party
- Compare the captured values
- Return decision based on the similarity of the captured values

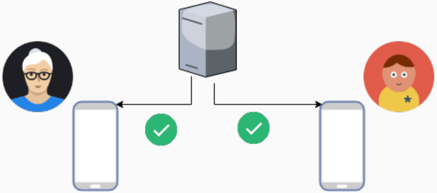


NATURAL AMBIENT ENVIRONMENT-BASED RELAY ATTACK DETECTION

- Both devices measure the ambient environment using some sensor(s) for some pre-defined time
  - Temperature
  - Accelerometer
  - GPS
  - ...
- Transfer the captured values to one of the devices, or a trusted third party
- Compare the captured values
- Return decision based on the similarity of the captured values

NATURAL AMBIENT ENVIRONMENT-BASED RELAY ATTACK DETECTION

- Both devices measure the ambient environment using some sensor(s) for some pre-defined time
  - Temperature
  - Accelerometer
  - GPS
  - ...
- Transfer the captured values to one of the devices, or a trusted third party
- Compare the captured values
- Return decision based on the similarity of the captured values



NATURAL AMBIENT ENVIRONMENTS EFFECTIVENESS

Previously proposed solutions:

- $\sim$9% Equal Error Rate (EER) at best
  - Probably not sufficient for tasks like contactless payments
- Timing restrictions in many contactless transactions $\leq$ 500ms
  - Current solutions require more time

NATURAL AMBIENT ENVIRONMENTS EFFECTIVENESS

Previously proposed solutions:

- $\sim$9% Equal Error Rate (EER) at best
  - Probably not sufficient for tasks like contactless payments
- Timing restrictions in many contactless transactions $\leq$ 500ms
  - Current solutions require more time

Paper	Sensor(s) Used	Sample Duration	Contactless Suitability
Ma et al. [2]	GPS	10 seconds	Unlikely
Halevi et al. [1]	Audio	30 seconds	Unlikely
	Light	2 seconds	More Likely
Varshavsky et al. [8]	Wi-Fi (Radio Waves)	1 second	More Likely
Urien et al. [7]	Temperature	N/A	-
Mehrnezhad et al. [3]	Accelerometer	0.6 to 1.5 Seconds	More Likely
Truong et al. [6]	GPS Raw Data	120 seconds	Unlikely
	Wi-Fi	30 seconds	Unlikely
	Ambient Audio	10 seconds	Unlikely
	Bluetooth	12 seconds	Unlikely
Shrestha et al. [5]	Temperature (T)	Few seconds	Unlikely
	Precision Gas (G)	Few seconds	Unlikely
	Humidity (H)	Few seconds	Unlikely
	Altitude (A)	Few seconds	Unlikely
	HA	Few seconds	Unlikely
	HGA	Few seconds	Unlikely
	THGA	Few seconds	Unlikely

NATURAL AMBIENT ENVIRONMENTS EFFECTIVENESS

Previously proposed solutions:

- $\sim$9% Equal Error Rate (EER) at best
  - Probably not sufficient for tasks like contactless payments
- Timing restrictions in many contactless transactions $\leq$ 500ms
  - Current solutions require more time

Problem

In previous work we questioned the suitability of using the natural ambient environment for proximity detection [4]:

- 17 widely available sensors were tested in 500ms transactions
- Best performance: Pressure sensor
- Still: $\sim$10% False acceptance rate

RELAY ATTACK DETECTION BY GENERATION OF AN ARTIFICIAL AMBIENT ENVIRONMENT

ARTIFICIAL AMBIENT ENVIRONMENTS

We proposed the generation of an Artificial Ambient Environment (AAE), using peripherals of the transaction devices (terminal and instrument)

- Based on randomly generated streams or sequences
- Easy for the genuine devices to establish proximity assurances
- Hard for an attacker to timely reproduce at a distance location

ARTIFICIAL AMBIENT ENVIRONMENTS

We proposed the use of the following peripherals:

- Infrared light
    - Tested against 6 attack test-beds using off-the-shelf equipment
    - All relay attacks were successfully detected
    - 98% True Accept Rate
    - But:
        - Infrared emitters not available on most modern smartphones
        - Might be vulnerable to more sophisticated attacks
- Vibration
    - Tested against 15 attack scenarios
    - $\sim$0% EER (using various popular machine learning classifiers)
    - But might be vulnerable when a more sophisticated attacker is involved

FORCE SENSING-BASED RELAY ATTACK DETECTION

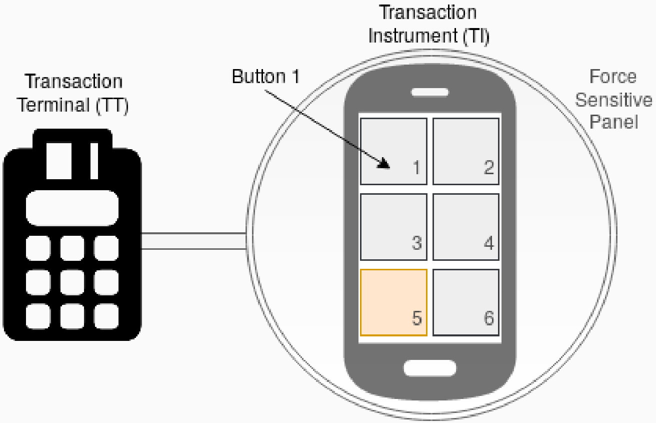
FORCE SENSING-BASED RELAY ATTACK DETECTION

- Different approach (not relying on environmental measurements)
- Part of the transaction (similar to PIN entry)
- Requires user interaction
- Based on the duration of subsequent presses/releases of virtual buttons that appear on the smartphone's screen

FORCE SENSING-BASED RELAY ATTACK DETECTION (CONTINUED)

- The user is called to position the device on a force-sensitive ‘plate’
- A randomly selected button (out of 6 buttons) is displayed on the device’s display that the user is called to press
- Both devices (payment terminal and payment instrument) record the id of the pressed button, as well as the time of the press (in ms)
- Upon pressing the button, another button is randomly chosen and displayed
- The time between subsequent button presses is also recorded
- Four buttons are displayed in total
- The captured timings and entered PIN from the two devices are compared — if within a certain threshold, we assume that the devices are in proximity (no relay attack)

FORCE SENSING-BASED RELAY ATTACK DETECTION (CONTINUED)



The Basic Framework Architecture

FORCE SENSING-BASED RELAY ATTACK DETECTION FRAMEWORK

Transaction Instrument (TI):

- Standard Android libraries

Transaction Terminal (TT):

- Four force sensitive resistors
- Algorithm to detect which of the 6 buttons is being pressed, based on the pressure that the resistors measure

FORCE SENSING-BASED RELAY ATTACK DETECTION FRAMEWORK

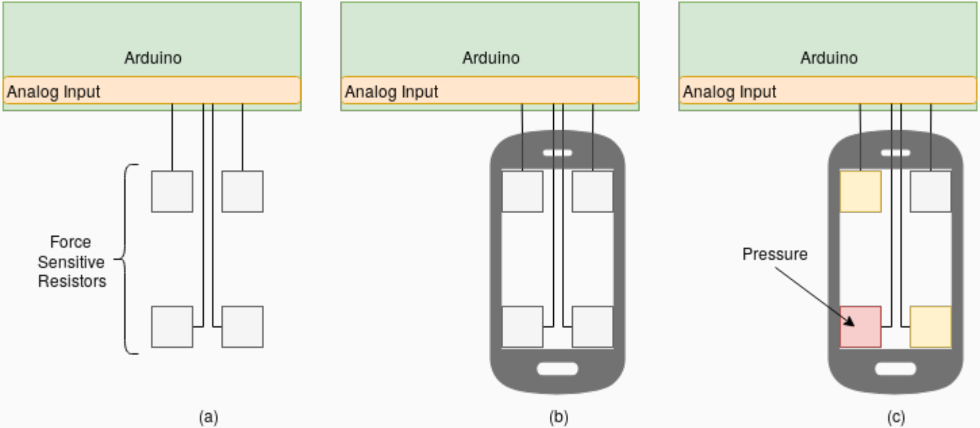
Transaction Instrument (TI):

- Standard Android libraries

Transaction Terminal (TT):

- Four force sensitive resistors
- Algorithm to detect which of the 6 buttons is being pressed, based on the pressure that the resistors measure

FORCE SENSING-BASED RELAY ATTACK DETECTION FRAMEWORK



Detection of Presses by the transaction terminal

BUTTON PRESS DETECTION ALGORITHM

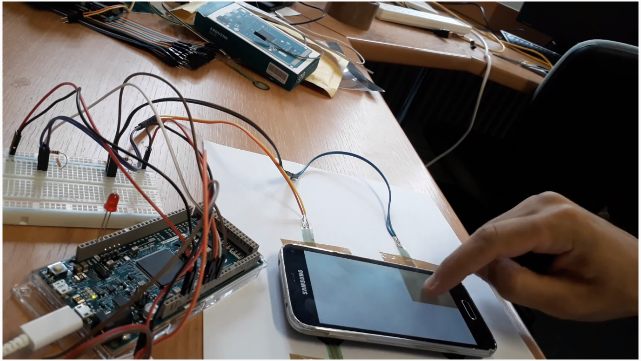
Algorithm 1: Detection of Pressed Button

```
Input   : int sensor1, int sensor2, int sensor3, int sensor4
Output: int pressedButtonID
leftSide $\leftarrow$ sensor1 + sensor2;
rightSide $\leftarrow$ sensor3 + sensor4;
if leftSide $>$ rightSide then
    force $\leftarrow$ sensor1 / leftSide;
    if force $\geq$ 0 and force $<$ 0.33 then
        return 5
    else if force $\geq$ 0.33 and force $<$ 0.66 then
        return 3
    return 1
end
force $\leftarrow$ sensor3 / rightSide;
if force $\geq$ 0 and force $<$ 0.33 then
    return 6
else if force $\geq$ 0.33 and force $<$ 0.66 then
    return 4
return 2
```

PARTS

- Part 1: Set thresholds
- Part 2: Experimental evaluation

PART 1: SET THRESHOLD



<video demonstration>

PART 1: SET THRESHOLD

Captured PIN, Timings, and Difference Between the Captured Timings (in ms) from the Two Devices

	Terminal (TT)	Genuine User (TI’)	Difference
PIN	6315	6315	—
Press 1	113	129	-16
Release 1	1120	1081	39
Press 2	244	262	-18
Release 2	1168	1136	32
Press 3	201	214	-13
Release 3	1263	1232	31
Press 4	177	190	-13

PART 1: SET THRESHOLD

- Based on 100 measurements we set acceptance thresholds for presses and releases
- We repeated the experiment using another 2 devices (heavier and larger), without readjusting the terminal's setup
- Devices used:
  - Samsung Galaxy S5 mini (SGS5 mini) — 4.5" display, 120g
  - Samsung Galaxy S4 (SGS 4) — 5" display, 130g
  - Nexus 9 tablet — 8.9" display, 425g

PART 1: SET THRESHOLD

Proximity Detection Results – in ms (negative results indicate that TI's measurement durations were larger than TT's)

	Minimum		Maximum		Span		Average	
	Press	Release	Press	Release	Press	Release	Press	Release
SGS5 mini	-46	11	-11	48	35	37	-29.09	28.71

PART 1: SET THRESHOLD

Proximity Detection Results – in ms (negative results indicate that TI’s measurement durations were larger than TT’s)

	Minimum		Maximum		Span		Average	
	Press	Release	Press	Release	Press	Release	Press	Release
SGS5 mini	-46	11	-11	48	35	37	-29.09	28.71
SGS 4	-28	-8	9	30	37	38	-5.32	5.26
Nexus 9	-18	-8	12	23	30	31	-2.16	2.83
Total	-46	-8	12	48	58	56	-12.19	12.27

PART 2: EXPERIMENTAL EVALUATION

Two phases:

- 10 users were shown 10 videos and tried to attack them by replicating the user's movement on the device, while the video was playing or afterwards (up to them)
  - The users were familiar with the definition of a relay attack
  - The videos were presented on a 24” computer screen and the users could choose the orientation that suited them best
  - 4 of the users were musicians
- The same users were shown a single video 10 times and called to attack it each time (very powerful attacker)

Two analyses:

- Threshold-based analysis
- Machine learning-based analysis

USER STUDY

Performance of 5 Users

	Genuine User	Genuine Terminal	Attacker 1	Attacker 2	Attacker 3	Attacker 4	Attacker 5
PIN	6315	6315	6315	6315	6315	6315	6315
Press 1	129	113	91	61	195	102	87
Release 1	1081	1120	804	847	985	2068	1151
Press 2	262	244	75	287	86	158	44
Release 2	1136	1168	1486	1360	1774	930	1454
Press 3	214	201	262	79	37	105	188
Release 3	1232	1263	1052	1094	939	1479	1198
Press 4	190	177	386	197	88	113	173

USER STUDY

Performance of 5 Users

	Genuine User	Genuine Terminal	Attacker 1	Attacker 2	Attacker 3	Attacker 4	Attacker 5
PIN	6315	6315	6315	6315	6315	6315	6315
Press 1	129	113	91	61	195	102	87
Release 1	1081	1120	804	847	985	2068	1151
Press 2	262	244	75	287	86	158	44
Release 2	1136	1168	1486	1360	1774	930	1454
Press 3	214	201	262	79	37	105	188
Release 3	1232	1263	1052	1094	939	1479	1198
Press 4	190	177	386	197	88	113	173

USER STUDY

Performance of 5 Users

	Genuine User	Genuine Terminal	Attacker 1	Attacker 2	Attacker 3	Attacker 4	Attacker 5
PIN	6315	6315	6315	6315	6315	6315	6315
Press 1	129	113	91	61	195	102	87
Release 1	1081	1120	804	847	985	2068	1151
Press 2	262	244	75	287	86	158	44
Release 2	1136	1168	1486	1360	1774	930	1454
Press 3	214	201	262	79	37	105	188
Release 3	1232	1263	1052	1094	939	1479	1198
Press 4	190	177	386	197	88	113	173

USER STUDY

Performance of 5 Users

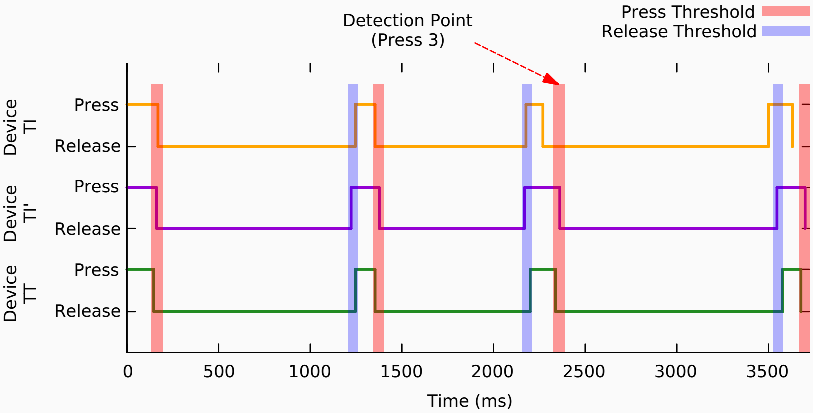
	Genuine User	Genuine Terminal	Attacker 1	Attacker 2	Attacker 3	Attacker 4	Attacker 5
PIN	6315	6315	6315	6315	6315	6315	6315
Press 1	129	113	91	61	195	102	87
Release 1	1081	1120	804	847	985	2068	1151
Press 2	262	244	75	287	86	158	44
Release 2	1136	1168	1486	1360	1774	930	1454
Press 3	214	201	262	79	37	105	188
Release 3	1232	1263	1052	1094	939	1479	1198
Press 4	190	177	386	197	88	113	173

USER STUDY — DATA ANALYSIS: THRESHOLD-BASED

Threshold-Based Relay Attack Detection Results (out of 100 attempts)

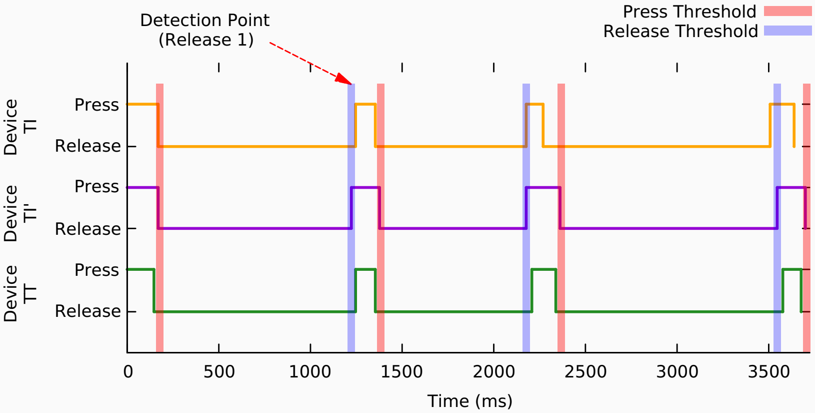
	Press 1	Release 1	Press 2	Release 2	Press 3	Release 3	Press 4	False Accept
General Threshold – Phase 1								
Detected	73	24	0	2	1	0	0	0
Correct	27	10	37	10	24	5	31	—
Device Specific Threshold – Phase 1								
Detected	84	16	0	0	0	0	0	0
Correct	16	7	25	9	9	4	23	—
General Threshold – Phase 2								
Detected	57	37	5	1	0	0	0	0
Correct	43	11	29	24	26	9	20	—
Device Specific Threshold – Phase 2								
Detected	65	33	2	0	0	0	0	0
Correct	35	6	21	22	20	6	9	—

USER STUDY — DATA ANALYSIS: THRESHOLD-BASED



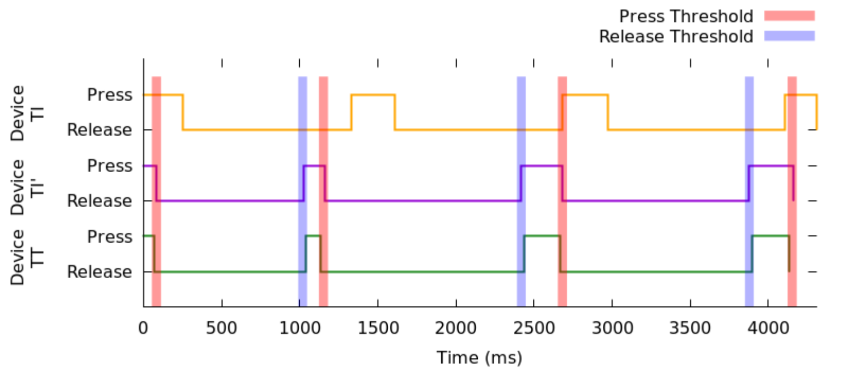
Graphical Representation of the Best Attack Attempt (TT – TI) Versus the Corresponding Genuine Transaction (TT – TI’)

USER STUDY — DATA ANALYSIS: THRESHOLD-BASED



Graphical Representation of the Best Attack Attempt (TT – TI) Versus the Corresponding Genuine Transaction (TT – TI') using device specific threshold

USER STUDY — DATA ANALYSIS: THRESHOLD-BASED

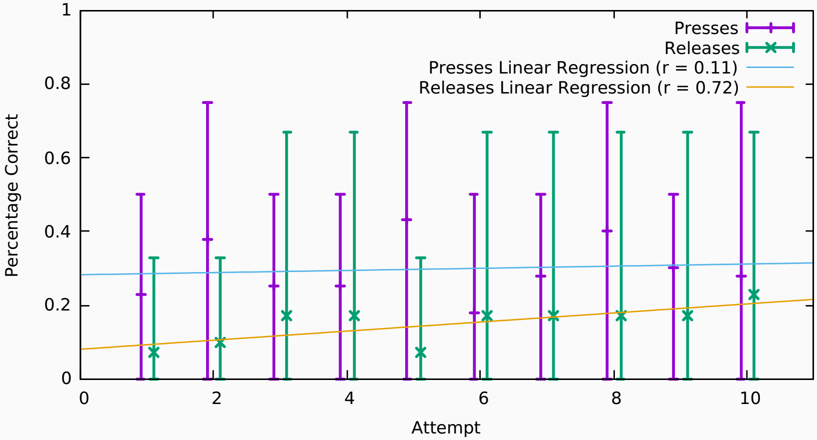


Graphical Representation of a Typical Attack Attempt (TT – TI) Versus the Corresponding Genuine Transaction (TT – TI')

MULTIPLE ATTACKS AGAINST THE SAME VIDEO

- The same video was presented 10 times to each participant
- The participant was asked to attack it after each time

MULTIPLE ATTACKS AGAINST THE SAME VIDEO



Performance Variation of Each of the 10 Attempts in the Second Phase

MULTIPLE ATTACKS AGAINST THE SAME VIDEO

- Result: Minor performance improvement over time
- This scenario is not likely to occur

USER STUDY — DATA ANALYSIS: MACHINE LEARNING-BASED

Machine Learning Classification Results Obtained by Repeating 10-Fold Cross-Validation 10 Times

	Random Forest	Naïve Bayes	Logistic Regression	Decision Tree	Support Vector Machine
Accuracy (%)	99.62	99.80	86.58	98.78	100.00
AUC	0.9999	0.9996	0.8163	0.9873	1.0
F1-score	0.9969	0.9984	0.90	0.9901	1.0
EER	0.0022	0.0047	0.1993	0.104	0.0

DISCUSSION

- Both threshold-based and machine learning-based approaches could detect all relay attack attempts
- Even when the device was not position perfectly the accuracy of the terminal was very high
- Tried with 8 buttons instead of 6 with good results (not as good)
- (Musicians did not perform better than the rest of the users)

Potential concerns:

- A robotic arm might be more accurate — but will easily be spotted by the terminal's operator
- Not very user friendly (compared to just tapping the devices)
- Requires extra HW
- Phone cases might obstruct

FUTURE DIRECTIONS

- Extend user study
- Find new approaches to more accurately measure the force (e.g. in case the placement is not good)
- Add more features, like the amount of pressure (most smartphones do not support this or the accuracy is very low)

CONCLUSION

- Proposed a novel approach to relay attack detection on smartphones
- Experimental evaluation of the approach showed promising results
- 100% relay attack detection rate was achieved, using threshold- and machine learning-based analyses

REFERENCES

[1] T. Halevi, D. Ma, N. Saxena, and T. Xiang.
Secure Proximity Detection for NFC Devices Based on Ambient Sensor Data.
In S. Foresti, M. Yung, and F. Martinelli, editors, Computer Security – ESORICS 2012, LNCS, pages 379–396. Springer, 2012.

[2] D. Ma, N. Saxena, T. Xiang, and Y. Zhu.
Location-Aware and Safer Cards: Enhancing RFID Security and Privacy via Location Sensing.
IEEE TDSC, 10(2):57–69, March 2013.

[3] M. Mehrnezhad, F. Hao, and S. F. Shahandashti.
Tap-Tap and Pay (TTP): Preventing Man-In-The-Middle Attacks in NFC Payment Using Mobile Sensors.
In 2nd International Conference on Research in Security Standardisation (SSR'15), October 2014.

[4] C. Shepherd, I. Gurulian, E. Frank, K. Markantonakis, R. N. Akram, E. Panaousis, and K. Mayes.
The Applicability of Ambient Sensors as Proximity Evidence for NFC Transactions.
In Mobile Security Technologies (MoST) 2017, 2017.

[5] B. Shrestha, N. Saxena, H. T. T. Truong, and N. Asokan.
Drone to the Rescue: Relay-Resilient Authentication using Ambient Multi-sensing.
In Financial Cryptography and Data Security, pages 349–364. Springer, 2014.

[6] H. T. T. Truong, X. Gao, B. Shrestha, N. Saxena, N. Asokan, and P. Nurmi.
Comparing and Fusing Different Sensor Modalities for Relay Attack Resistance in Zero-Interaction Authentication.
In Pervasive Computing and Communications (PerCom), 2014 IEEE International Conference on, pages 163–171. IEEE, 2014.

[7] P. Urien and S. Piramuthu.
Elliptic curve-based RFID/NFC authentication with temperature sensor input for relay attacks.
Decision Support Systems, 59:28 – 36, 2014.

[8] A. Varshavsky, A. Scannell, A. LaMarca, and E. de Lara.
Amigo: Proximity-Based Authentication of Mobile Devices.
In J. Krumm, G. Abowd, A. Seneviratne, and T. Strang, editors, UbiComp 2007, LNCS, pages 253–270. Springer, 2007.

Thank you!

Any questions or suggestions?