Suddivisione slide ATCNS

1 - Overview on PINs and context

PINs as the simplest type of authentication (memory, easiness)

Where are they used

Compromise between simplicity and enforcing something secure

2 - Where are PIN used

Classic usage inside ATMs

Modern usage inside mobile phones

Possible exploits given the habits of user

3 - Focus on ATMs and PoS PINs

Observation via video of keypress

Usage of audio channels to exploit user (inter-keystroke timing - which keys pressed and when)

Problem of information leakage in:

Non-acoustic Side-channels

Acoustic Side-channels

4 - How to track and study user habits

Non-acoustic - thermal residual over keys

Acoustic - sound of key

Usage of adversary models

5 - Adversary Model

Keystroke timing

Single or Multi-finger Typists

Information about the first or the last digit of the PIN

Which keys have been pressed

6 - Extraction over user data - Timing

Extraction of Keystroke Timings from Keypad Sound - more accurate time estimation than using video

PIN Inference from Keystroke Timing - a smaller decrease in guessing performance compared to timings extracted from video

7 - Extraction over user data - Distance and behavior

Extraction of inter-keystroke timings

Enter-key distance vector

Able to guess a substantially higher number of PINs for single-finger typists compared to multi-finger typists

8 - Extraction over user data - Knowledge of key presses

Usage of a thermal camera for checking which keys were touched

Combining two sources leads to higher recovery rate

Combining them all make you guess all of them

9 - Pin Guessing Probability and Paper 1 Conclusions

Knowing one digit do not affect the guessing over all pins

Choosing PINs at random is not the best strategy

Distance between keys and timings when typing with one more finger

Combining multiple sources works and reduce guess number attempts

10 - PINs: portable and secure

Problem of usability and security

Why PIN selection policies are so important

Frequency of keypad usage and presses

Users are annoyed by strict things

Compromise between users load and security

11 - How PINs are distributed in the real world

Occurrence frequency of the PINs - it's easier guessing the first digit

PINs generated from dates and years - many were designed like this

PINs generated through arithmetic operations - they are only a fraction

PINs with close proximity - pins with close numbers are more selected

12 - How PINs can be more effectively chosen (part 1)

Enforce PIN selection for stronger pins, practical and similar to everyday ones

Selecting PINs for mobile locking over 5 different policies

Explanation of different types of pins

13 - How PINs can be more effectively chosen (part 2)

Study of probability over average number of guesses and leaks and user feedback

Users want shorter policies (short/free over long - shorter pins and easier to remember)

Entropy is higher on longer ones and odd numbers are less frequent

14 - Future in PIN Selection

Percentual of participants who should change their pins

Users ofter ignore security requirements

Entropy increases in PIN length

Solution in the middle: making an easy length, impose more characters and avoid popolar words