PIN Inference at ATMs by Side-Channel Attacks

REU fellows: Tristan Gurtler[1], Charissa Miller[2], Kendall Molas[3], and Lynn Wu[4]
Faculty Mentors: Drs. Paolo Gasti[3] and Kiran Balagani[3]
Affiliation: [1]College of Engineering, University of Illinois at Urbana-Champaign, [2]College of Computing and Information Sciences, Rochester Institute of Technology, [3]School of Engineering and Computing Science, New York Institute of Technology, [4]Department of Computer Science, Bryn Mawr College

BACKGROUND

- Automated Teller Machines (ATMs) require an ATM card and a Personal Identification Number (PIN) to access an account.
- ATMs typically display symbols (i.e. dots or asterisks) to track the number of PIN digits a user has entered while protecting against low-effort attempts to steal their PIN.
- Displaying symbols does not immediately leak the PIN, but unintentionally leaks information about the inter-key press timings.

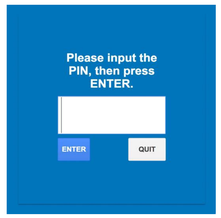

Figure 1. A typical PIN entry display prompt

HYPOTHESES

We test two different hypotheses on what features predict inter-key timing effectively for potential use in PIN inference.

Figure 2. PIN Distance on a model keypad

Distance Hypothesis
Inter-key timing correlates with physical distance – that is, a pair of keys with greater physical distance from one another will also have a correspondingly longer inter-key latency than a pair of keys closer together.

Figure 3. PIN Direction on a model keypad

Direction Hypothesis
Inter-key timing varies with physical orientation – that is, a pair of keys that are equal distances from one another but lie in different directions from one another will have different inter-key latencies. This may be limited to horizontal vs. vertical directions (e.g., 1 to 3 vs. 1 to 7), or may be any direction (e.g. left vs. right, as in 2 to 1 vs. 2 to 3)

EXPERIMENT & RESULTS

Figure 4. The experiment setup

In order to observe keystroke timings, we designed and executed an experiment featuring:
- An ATM simulation with a real ATM keypad
- A camcorder recording the screen from a fixed location
- 22 users, with a total of 61 sessions and over 40,000 data points collected

The PINs used were generated specifically to test our hypotheses. Each session had:
- A total of fifteen 4-digit PINs
- 4 fifteen second breaks throughout the session
- Each PIN presented 3 separate times
- Each PIN typed correctly a total of 12 times
- No PIN repeated across different sessions per user

Analysis of inter-key timings:
- Discarded outliers ranging within the top 5 percent
- Isolated inter-key timings by distance and direction
- Aggregated data
- Compared varying distance timings
- Compared varying direction timings

Figure 5. The PIN 6305 is chosen to test the distance hypothesis.

Figure 6. The PIN 9317 is chosen to test the direction hypothesis.

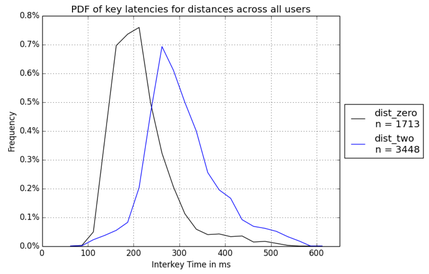

Figure 7. The distribution of keypress timings for keys distances 0 and 2 keys apart from one another

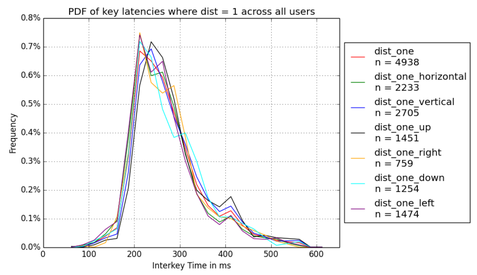

Figure 8. The distribution of keypress timings for keys distance 1 apart from one another in differing directions

TIMING DETECTION

We designed a system to automatically detect, from videos of the ATM screen, the appearance of symbols and log the times that were observed. The system:
- Scans each frame for dots using OpenCV.
- Logs the frame and timestamp when a new dot is discovered.
- Logs the frame and timestamp when multiple dots disappear as when an Enter was pressed.

From this, all inter-key latencies are then derived.

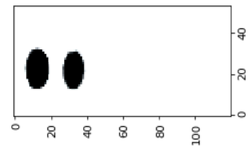

Figure 10. Sample output from our timing detection system

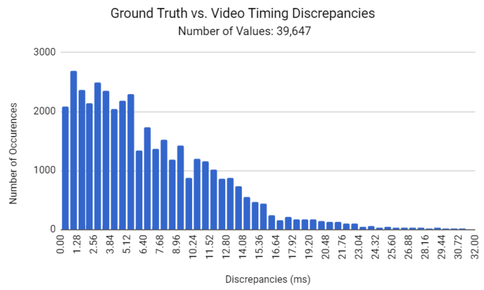

Figure 9. The distribution of error by our video timing detecting system

PIN INFERENCE

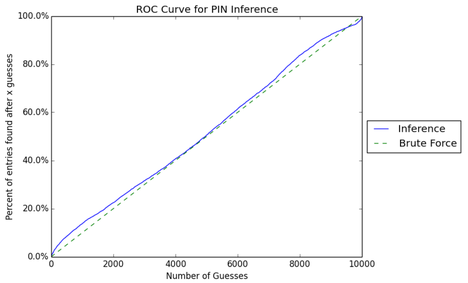

Figure 11. Effectiveness of first-stab approach to PIN Inference

- Preliminary measures have been tested, but only look at key pairs.
- Further work may look at triplets and beyond.

CONCLUSION

- Symbols appearing on the ATM screen leak information about inter-key timings.
- Varying distances between key presses produces different inter-key press timings.
- This leakage might be sufficient to restrict the number of PIN guesses in an attack.

FUTURE WORK

Further work is needed in evaluating alternative measures of the timing data available and in identifying what other features may be used in conjunction with timing features to improve PIN inference.

ACKNOWLEDGEMENTS

The project is funded by National Science Foundation Grants No. CNS-1559652, CNS-1712149, and CNS-1619023 and New York Institute of Technology.