Sommario

[Slide 1 – Title 2](#_Toc151642784)

[Slide 2 - PIN sounds good… but is it? 2](#_Toc151642785)

[Slide 3 - Where are PINs used? 2](#_Toc151642786)

[Slide 4 - How are ATM PINs exploited? 2](#_Toc151642787)

[Slide 5 - How to track and study PINs (Non-acoustic)? 2](#_Toc151642788)

[Slide 6 - How to track and study PINs (Acoustic)? 3](#_Toc151642789)

[Slide 7 - Keystroke Timing (part 1) 3](#_Toc151642790)

[Slide 8 - Keystroke Timing (part 2) 3](#_Toc151642791)

[Slide 9 – Typing behavior 3](#_Toc151642792)

[Slide 10 - Typing Behavior + Keystroke Timing 4](#_Toc151642793)

[Slide 11 - Knowledge of which keys have been pressed 4](#_Toc151642794)

[Slide 12 - How much time to get the keys pressed? 4](#_Toc151642795)

[Slide 13 - Analysis of PINs Guessing Probability 4](#_Toc151642796)

# Slide 1 – Title

Good morning everybody, I’m Gabriel and today me and Michael will present and discuss a topic that touches each one of us in our daily lives — the security of our personal information. How often do you find yourself entering a PIN or password? We will discuss the vulnerability of PINs, understanding how they can be exploited and covering different scenarios of attack, making us understand more of the context and becoming aware of the possible tactics used to retrieve our data. I will handle the first part on the possible exploits, while Michael will handle the part covering the PIN policies.

# Slide 2 - PIN sounds good… but is it?

Our everyday experiences remind us that a PIN is more than just a combination of numbers; it's a fundamental aspect of authentication designed to strike a delicate balance. On one hand, it's crafted to be easily memorable, ensuring accessibility for users. On the other hand, it aspires to be complex enough to instill a sense of security. In reality, we should be careful over PINs creation, given they are a cornerstone of authentication in various realms, particularly in handling sensitive data, given they are the primary access method to get to those.

# Slide 3 - Where are PINs used?

Picture this – at the heart of financial transactions, PINs stand guard at ATMs and Points of Sale (PoS), ensuring the secure exchange of sensitive information. These numeric sentinels play a crucial role in our financial security, forming a key part of our interactions with automated systems. But that's not all. Extend this scenario to the device in your pocket. Your smartphone, a treasure trove of personal data, is often safeguarded by the simple nature of a PIN.

Attackers may be particularly interested in getting access to this information and there can be many sources of information related to these devices which lead to leakage and possible knowledge of PINs context, making an adversary able to guess one.

# Slide 4 - How are ATM PINs exploited?

In the context of PINs, many ways can be used to try to acquire maliciously information, which rely on different methods. First, let’s examine the non-acoustic ones: their keys and their movements, called keystrokes, can be analyzed electromagnetically, monitoring the motion and exploiting the user while he’s typing the password; for instance, this can be done via video or thermal observation of inputs.

Another type of exploit can be with the acoustic channels, in which attackers leverage the unique acoustic signatures of each key, which emits a characteristic sound; this can be the object of attacks based on the specific timing or the typing habits, tracking the distance between the single keys.

# Slide 5 - How to track and study PINs (Non-acoustic)?

As a user inputs their PIN, electromagnetic emanations from the keypad can be analyzed to recover each keystroke, via electronic components or motion detection, for example leaving thermal residues which have different dissipation rates according to the keypad material used, as shown here. Consider this as part of a broader strategy, where non-acoustic methods are intelligently combined with other sources of observation. This synergy not only enhances the precision of PIN recovery but also reduces the search space for potential PINs when integrated with alternative sources of possible leakage, as analyzed in this study.

# Slide 6 - How to track and study PINs (Acoustic)?

An exceptionally effective method in PIN retrieval involves the utilization of audio feedback. This study delves into the depth of acoustic channels, emphasizing their ease of collection and reduced risk of exposure in attacks.

As introduced, each key emits a specific sound when measured in frequency and this can be the object of eavesdropping or dictionary attacks of all kinds. The characteristic frequency progression in time becomes a crucial factor, characterizing the intervals between pressed keys. This information aids in triangulation via sound microphones, facilitating the guessing of key positions during entry, considering the timing between presses is a really effective source of attack.

Given the timing and latency between keystrokes, some other sources of attacks can be the snooping over SSH traffic, where the timing and appearance of symbols as dots on the screen device can be effectively reconstructed.

# Slide 7 - Keystroke Timing (part 1)

Now, let's shine a spotlight on a crucial aspect of PIN analysis — Keystroke Timing. This is the precise observation of the temporal space between consecutive keystrokes of subsequent keys, commonly defined as distance. This allows to get information over the possible PINs which are being typed by user without tampering the ATM/the device effectively using audio frequencies.

Here, the adversary filters timestamps of keys pressed from the keypad sound, normalizing the samples to isolate the distinctive keystroke timings. The timing information measured the specific user rhythm in action and is based on observation, often facilitated by video recording in conjunction with audio.

# Slide 8 - Keystroke Timing (part 2)

In our pursuit of understanding Keystroke Timing, we introduce a meticulous measurement—evaluating the distance between consecutive timestamps within a window. This method proves more accurate than relying solely on video analysis, where audio proved to be more effective in practice.

This distance measurement relies on the Euclidean distance, offering a numerical gauge of the dissimilarity between timing patterns of subsequent keys in each PIN. It's not merely a count of keys but a nuanced evaluation of how many can be input in a window of time, conveniently encapsulated in a vector.

For instance, let's dissect the distance vector associated with the PIN 5566: [0, 1, 0]. In this representation, the first '0' signifies the distance between the keystrokes of '5' and '5,' the '1' represents the distance between '5' and '6,' and the final '0' indicates the distance between '6' and '6.'

This vectorized approach allows us to quantify the rhythm and timing intricacies of PIN entry, providing a robust foundation for ranking and analysis.

# Slide 9 – Typing behavior

When evaluated with other sources of information leakage, the typing behavior of users is important; it’s revealed that is quite common to use different numbers of fingers to type a PIN, may it be via a single one (called single typists, slower typing speed, but more precise and careful) or multiple (called multi-finger typists, with interval between key presses more varied thanks to more speed achieved as imaginable) at a time. Usually, what happens is typing with one finger, or multiple fingers of one hand or multiple with both hands.

This pattern is yet again based on observation, so combining this knowledge with unique thermal signature or unique sound pattern can reveal quite effective in information extraction.

# Slide 10 - Typing Behavior + Keystroke Timing

By leveraging knowledge of whether the user is a single- or multi-finger typist, an adversary can better contextualize the timings between consecutive keys. For single-finger typists, the corresponding inter-keystroke timing tends to be the largest. However, when multiple fingers are involved in PIN input, the Euclidean distance in how many keys are input becomes less representative.

In such cases, leveraging audio feedback can significantly enhance the adversary's ability to infer PINs, especially when the rhythm becomes more random. According to the study, the percentage of PINs recovered within 5 attempts was twice as high for PINs entered with one finger compared to PINs entered with multiple fingers. This highlights the substantial impact of typing behavior on the security implications of PIN inference.

# Slide 11 - Knowledge of which keys have been pressed

The adversary's tactics extend beyond mere keystroke timing, as they may gain visibility of the keypad through a thermal camera, capturing the user's hand movements (in some cases even UV powder, quite borderline) and understanding more and more things.

When armed with knowledge of a single digit, the adversary significantly reduces the search space for the PIN. According to the findings from the paper, knowing just one digit cuts down the possibilities by a linear factor—whether it's the first or last digit. In essence, this reduces the guessing complexity, requiring the adversary to focus only on the remaining three digits.

To quantify the impact, the expected number of attempts to guess a random PIN, with no additional information, is reduced to 500. The paper's experiments reveal that knowledge of the first or last digit, coupled with keystroke timings, substantially boosts the guessing performance.

# Slide 12 - How much time to get the keys pressed?

The images present on this slide, analyzing in rows qualify the thermal traces left after 2/7/10/15 seconds after key press. These thermal images serve as a critical tool for the adversary. By employing thermal imaging, the adversary gains the ability to discern precisely which keys were pressed. This becomes a formidable asset when combined with other methods, especially those exploiting the user's typing behavior, the time intervals between key presses, and the distances between keys.

The synergy of these multiple information sources works wonders, strategically narrowing down the probabilistic combinations of pressed keys. It's a powerful technique that significantly restricts the search space, adding an extra layer of complexity to the adversary's task.

# Slide 13 - Analysis of PINs Guessing Probability

In this slide, we give a summary of the results analyzed until now. Given to different PINs combinations correspond different PIN vectors, choosing PINs at random is not the best strategy (say, 0000 is 1111/2222, while vector 1111 means 4 different keys with lot more combos, etc.).

This way, knowing a single digit of PIN does not help the retrieval of a single PIN; infact, the timing between keystrokes and audio works better on audio feedback over multiple analysis, effectively increasing accuracy in both knowledge of keys and typing habits, which allow an adversary to know how many fingers are used and reduce the distance between the keys. Combining audio and timings actually makes an adversary guess almost all PINs.

(I will now turn the floor over to my colleague Michael, who will present the next part of slides)