Sommario

[Slide 1 – Title 2](#_Toc151470968)

[Slide 2 - PIN sounds good… but is it? 2](#_Toc151470969)

[Slide 3 - Where are PINs used? 2](#_Toc151470970)

[Slide 4 - How are ATM PINs exploited? 2](#_Toc151470971)

[Slide 5 - How to track and study PINs (Non-acoustic)? 2](#_Toc151470972)

[Slide 6 - How to track and study PINs (Acoustic)? 3](#_Toc151470973)

[Slide 7 - Keystroke Timing (part 1) 3](#_Toc151470974)

[Slide 8 - Keystroke Timing (part 2) 3](#_Toc151470975)

# 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 most importantly, uncovering potential solutions. 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: they 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.