Chapter 1: Introduction

In Chapter 1, the paper introduces the topic of password guessing based on timing attacks. It provides an overview of the state-of-the-art in timing attacks and discusses the significance of timing attacks in cracking passwords. The chapter also presents the goals and objectives of the paper, which is to quantify the amount of information leaked through video recordings of on-screen keystroke feedback.

It outlines the scenarios and adversary models considered in the paper, including a presenter entering a password into a computer connected to an external projector and a user entering a PIN at an ATM in a public location. The chapter concludes by highlighting the contributions of the paper, which include extensive data collection experiments involving 84 subjects and the analysis of inter-keystroke timings to infer keypairs.

Chapter 2: Related Work

In Chapter 2, the paper discusses the state-of-the-art in password guessing based on timing attacks. It mentions that there is a large body of prior work on timing attacks in the context of keyboard-based password entry. The paper specifically references a study by Song et al. that demonstrated a weakness in SSH sessions, where the adversary can extract information about passwords typed during the sessions by eavesdropping on inter-keystroke timing information transmitted in separate IP packets. The impact of this work is significant as it shows the power of timing attacks in cracking passwords.

The paper also mentions several studies on keystroke inference from video recordings, particularly in the context of shoulder-surfing scenarios. One such study by Balzarotti et al. addresses the typical shoulder-surfing scenario, where an adversary can infer keystrokes by analyzing video recordings. Overall, Chapter 2 provides an overview of the existing research on timing attacks and keystroke inference, setting the stage for the introduction of the PILOT system and adversary model in the subsequent sections.

Chapter 3: PILOT and the Adversary Model

In Chapter 3, the paper presents PILOT and the adversary model. PILOT is an attack that leverages timing information from video recordings of password or PIN entry sessions to reduce the search space for guessing passwords. The adversary model considers scenarios where the adversary has access to multiple video recordings of the same user or presenter entering passwords or PINs. The chapter provides details on how PILOT works and the assumptions made about the adversary's knowledge and capabilities.

**Timing Extraction from Video**

The researchers developed software that analyzes video recordings to detect the appearance of masking symbols and log corresponding timestamps. The software uses OpenCV to infer the number of symbols present in each image. By converting frames to grayscale and applying edge detection, the software captures the edges of the masking symbol. When a masking symbol is detected, the software logs the corresponding frame number, providing fairly accurate inter-keystroke timing information.

**Accuracy of Timing Extraction**

The experiments showed that the software's timing extraction technique had an average discrepancy of 8.7 ms (with a standard deviation of 26.6 ms) compared to the ground truth recorded by the ATM simulator. 75% of the extracted inter-keystroke timings had errors under 10 ms, and 97% had errors under 20 ms. Similar statistics were observed for data recorded on keyboards in the passwords setting.

**Percentage of PIN Guessed**

Table 3 shows the percentage of PINs guessed using different techniques. The researchers' technique had significantly higher success rates compared to random guessing and PIN guessing with exact distance. For example, with 640 attempts, their technique guessed 28.33% of the PINs, while random guessing only guessed 6.40% and PIN guessing with exact distance guessed 100.00%.

**Acknowledgements**

The researchers acknowledge the support they received from various sources, including the National Science Foundation and EU projects.

Chapter 4: Data Collection and Experiments

In Section 4 of the document, the authors discuss their data collection and experiments related to password guessing. They provide details on the methodology used to collect data and conduct experiments. Unfortunately, no specific information or findings from these experiments are mentioned in the given document content.

**Timing Extraction from Video**

The researchers developed software that analyzes video recordings to detect the appearance of masking symbols and log corresponding timestamps. The software uses OpenCV to infer the number of symbols present in each image. By analyzing the frames, the software can extract fairly accurate inter-keystroke timing information. The average discrepancy between the timings extracted from the video and the ground truth recorded by the ATM simulator was 8.7 ms, with 75% of the timings having errors under 10 ms and 97% having errors under 20 ms.

**Password Guessing**

The researchers treated the identification of digraphs from keystroke timings as a multi-class classification problem. They assumed that the user's password is a sequence of lowercase alphanumeric characters typed on a keyboard with a standard layout. They used a technique that involved analyzing inter-keystroke times to guess the user's PIN. The results showed that their technique had a higher success rate compared to random guessing and another technique called SILK-TV.

**Percentage of PIN Guessed**

Table 3 shows the percentage of PINs guessed using the researchers' technique, random guessing, exact distance guessing, and another technique called SILK-TV. The researchers' technique had a higher success rate compared to random guessing and SILK-TV. As the number of attempts increased, the success rate of the researchers' technique improved significantly compared to the other techniques.

Chapter 5: Results on Password Guessing using PILOT

In Section 5 of the paper, the authors present the results on password guessing using PILOT. They discuss the impact of timing attacks on cracking passwords and how accurate inter-keystroke timing information can be used to restrict the search space of passwords. The authors also mention the discrepancy in performance of PILOT on various passwords, which they attribute to the frequency of digraphs in each password appearing in the training data.

**State-of-the-art in password guessing based on timing attacks** Timing attacks in the context of keyboard-based password entry have been extensively studied. One notable work by Song et al. demonstrated a weakness in SSH sessions that allows the adversary to extract information about typed passwords by analyzing inter-keystroke timing. This information can be used to narrow down the search space of passwords, making timing attacks a powerful tool for cracking passwords.

**Keystroke inference from video recordings** There have been studies on inferring keystrokes from video recordings, particularly in shoulder-surfing scenarios. Balzarotti et al. addressed this scenario, where an adversary records a victim's screen to capture their keystrokes. By analyzing the video, the adversary can infer the timing and content of the keystrokes, potentially compromising the victim's passwords.

**PILOT and the adversary model** PILOT is a password guessing technique that leverages timing information from video recordings of on-screen keystroke feedback. The adversary model assumes that the adversary has access to video recordings of password entry sessions, either through a dedicated camera or a compromised camera. The goal is to reduce the search time for guessing passwords by training PILOT with population data.

**Data collection and experiments** To evaluate the effectiveness of PILOT, extensive data collection experiments were conducted. Videos were recorded using a Sony FDR-AX53 camera, capturing keystroke timings at a resolution of 1,920×1,080 pixels and 120 frames per second. The experiments involved 84 subjects, who were asked to type alphanumerical passwords multiple times. The ground-truth keystroke timings were recorded for analysis.

**Results on password guessing using PILOT** PILOT was evaluated on the RockYou password dataset, specifically focusing on 8-character passwords. The results showed that PILOT outperformed random choice in reducing search time. The success rate of PILOT varied depending on the frequency of digraphs in the training data. Passwords with more frequent digraphs in the training data had higher success rates.

**Conclusion and future work** The paper concludes by summarizing the findings and discussing future directions. The research aimed to quantify the amount of information leaked through video recordings of on-screen keystroke feedback. The results highlight the effectiveness of timing attacks in password guessing and provide insights for improving the success rate of PILOT.

Chapter 6: PIN Guessing

In Chapter 6, the paper discusses PIN guessing in the context of timing attacks. It presents the system and adversary model used in the study. The goal is to learn the user's secret PIN by analyzing inter-keystroke timings and inferring corresponding keypairs. The paper also describes the data collection process, which involved video-recording the screen of a simulated ATM to capture PIN entry. The results of the study are presented in Section 6 of the paper.

**Timing Extraction from Video**

The researchers developed software that analyzes video recordings to detect the appearance of masking symbols and log corresponding timestamps. The software uses OpenCV to infer the number of symbols present in each image. By converting frames to grayscale, applying a bilateral filter to reduce noise, and using Canny Edge detection to capture the edges of the masking symbol, the software is able to accurately extract inter-keystroke timing information from the videos.

**Accuracy of Timing Extraction**

The experiments showed that the timing extraction technique led to fairly accurate results. On average, there was a discrepancy of 8.7 ms between the inter-keystroke timings extracted from the video and the ground truth recorded by the ATM simulator. 75% of the extracted timings had errors under 10 ms, and 97% had errors under 20 ms. The distribution of error discrepancies is shown in Figure 6.

**Percentage of PIN Guessed**

Table 3 provides the percentage of PINs guessed using different techniques. The researchers' technique had significantly higher success rates compared to random guessing and PIN guessing with exact distance. For example, with 640 attempts, their technique guessed 28.33% of the PINs, while random guessing only guessed 6.40% and PIN guessing with exact distance guessed 100.00%.

**Acknowledgements**

The researchers were supported by the National Science Foundation under Grant No. CNS-1619023 and Grant No. CNS-1559652. They also received partial support from the EU TagItSmart! Project and the EU-India REACH Project.

**References**

The researchers referenced various sources, including the RockYou password leak, the LinkedIn password leak, and previous works on keyboard acoustic emanations and secret information leakage from keystroke timing videos.

Chapter 7 - Conclusion

In Chapter 7, the paper concludes by summarizing the findings and discussing future directions. The authors have demonstrated that inter-key timing information can be effectively used to reduce the cost of password guessing attacks. They have shown the impact of this side channel and its potential to restrict the search space of passwords. The technique significantly improves on random guessing and previous methods, with the ability to guess about 3% of PINs within 10 attempts.

This corresponds to a 26-fold improvement compared to random guessing. The authors believe that inter-keystroke timings contain considerable information about the physical distance between consecutive keys in a PIN, and thus can substantially reduce the number of attempts required to guess a PIN. Future work directions are discussed, indicating potential areas for further research and improvement in password guessing based on timing attacks.