SURFING ATTACK DETECTION THOUGH VOICE RECOGNITION

[1]E.Ganesh, [2]M.Prabu

[1]Research Scholar, [2]Assistant Professor
[1]Saveetha Engineering College, Chennai, India.
[2]Department of ECE, Misrmal Navajee Munoth Jain Engineering College, Chennai -97

Abstract : Speech recognition (SR) systems like Siri or Google Now have become a popular way for humans to interact with computers, turning many systems into voice-controllable systems (VCS). However, prior research has shown that VCS can be attacked using hidden voice commands that are not understandable to humans but can still control the system. These hidden commands are audible, but we have developed a new attack called the Surfing attack, which modulates voice commands on ultrasonic frequencies, making them completely inaudible to humans. By exploiting the nonlinearity of microphone circuits, we can successfully demodulate the low-frequency audio commands, record them, and most importantly, interpret them using speech recognition systems. The Surfing attack on popular speech recognition systems was tested on Siri, Google, and Alexa. We demonstrated proof-of-concept attacks by injecting a sequence of inaudible voice commands, including activating Siri to initiate a FaceTime call on an iPhone and activating Google Now to switch the phone to airplane mode. It is also possible to detect the Surfing attack by classifying the audio using a supported vector machine (SVM) and recommend that voice-controllable systems be redesigned to be resilient to inaudible voice commands.

Index Terms **- Surfing attack, inaudible sound, human speech, recognition.**

I. INTRODUCTION

The goal of our work is to investigate the threats posed by inaudible signal injection using ultrasound propagation hidden communication with AI-based voice assistants. Our proposed attack, Surfing Attack, allows for the delivery of various inaudible voice commands in ultrasound to a wide range of target devices from different manufacturers through different solid media . Due to the unique properties of guided wave propagation, Surfing Attack enables long-distance attacks with a lower power requirement and eliminates the need for line-of-sight for inaudible command injection attacks. Additionally, Surfing Attack allows for inaudible multi-rounds of interactions between the attacker and the target device without alerting users in physical proximity by controlling feedback mechanisms via the initial injected command .

One potential application scenario of Surfing Attack involves a malicious device hidden beneath a table to converse with the target device on top. Attackers can inject voice commands stealthily to instruct the voice assistants to leak various secrets, such as an authentication code for money transfer sent via an SMS message. The leaked secret can then be picked up by a malicious device hidden away and relayed back to the remote attacker. By leveraging the unique guided wave propagation properties in solid media, Surfing Attack presents a new genre of inaudible attack on voice-activated systems that enables not only non-interactive attacks but also interactive attacks that require multiple rounds of conversations with the target device.

To demonstrate the practicality of Surfing Attack, we built a prototype of the attack device using a commercial-off-the-shelf PZT transducer that costs around $5 per piece. We conducted two attacks as a demonstration: hacking an SMS passcode and conducting phone fraud using the synthetic voice of the victim. We evaluated Surfing Attack on Google Assistant of 11 popular smartphones and Siri of 4 iPhones and found it to be effective and resilient against verbal conversations. We also evaluated Surfing Attack on 4 representative types of table materials and found it to be most effective through aluminium/steel, glass, and medium-density fibreboard (MDF) tables, achieving a long-range attack of 30ft distance through a metal table.

We also explored the possibility of pairing command injection with a hidden microphone to enable hidden conversations between the attacker and the victim voice assistant. We demonstrated several practical attacks using the prototype we built, including hacking an SMS passcode and making a ghost fraud phone call without the owners' knowledge. We discussed potential defense mechanisms, including using the high-frequency components of guided waves as an indication of intrusion. In conclusion, Surfing Attack is the first exploration of attack leveraging unique characteristics of ultrasound propagation in solid medium and non-linearity of the microphone circuits to inject inaudible command on voice assistants.

SYSTEM ANALYSIS

A. Existing System

Surfing Attack is a new form of attack that exploits the vulnerability of home digital voice assistants like Amazon Alexa, Google Siri, and others. By using ultrasound propagation and a waveform generator, this attack can inject inaudible voice commands through guided waves, enabling the attacker to hack into the device from a significant distance.

B. Proposed System

A potential solution to protect home digital voice assistants like Amazon Alexa, Google Siri, etc. from the Surfing attack is to implement a hardware-based defense mechanism by redesigning the microphone layout to suppress any vibration with ultrasonic frequencies. Additionally, a software-based defense approach can be employed to identify and reject received voice commands. Another simple interlayer-based defense mechanism involves placing the device on a woven fabric to increase the impedance mismatch, while placing the device on a table with water or turning off the voice recognition and restricting device access can also provide protection. However, it should be noted that the attack may still work on plastic tables but with lower reliability. Users can also consider removing the headphones from their device or creating custom launch words to improve their security.

II. LITERATURE SURVEY

Presently, password authentication is a common method of securing personal accounts. However, it has become apparent that users tend to choose easily remembered passwords, which they may even write down on their screens. Consequently, this approach to authentication is vulnerable to brute-force, guessing, replay, and shoulder surfing attacks. Despite attempts to develop authentication methods that balance usability and security, the shoulder surfing attack remains a significant threat. To address this issue, we propose a new pattern-based authentication system that can withstand shoulder surfing attacks. Our research involves an analysis of the usability, deployability, and security of the proposed authentication method, compared to other authentication methods utilized in smart devices [1]. The use of financial technologies and their corresponding mobile services has surged in recent times. However, mobile security case studies indicate that security threats have also increased in this area. As a result, security departments in companies and banking institutions continuously research and develop solutions to ensure the safety of their services. Despite these efforts, recent studies of security threats have reported an increase in various new types of social engineering attacks on mobile services. This paper aims to compare several user authentication schemes with a focus on social engineering attacks, particularly shoulder surfing attacks. Through our experimental results, we discovered that existing schemes each have slightly different weaknesses. Based on the comparative analysis, we suggest some considerations for developing an anti-shoulder surfing security solution [2].

The use of public computer infrastructure or accessing password-protected accounts in public spaces, the risk of password disclosure is high. This can occur through keylogger spyware or a malicious observer who watches the user input their password. Virtual keyboards provide protection against keyloggers but are still vulnerable to shoulder surfing attacks. Some recent attempts to improve virtual keyboards involve dynamically loading and changing the keyboard layout to confuse any potential onlookers. Others have introduced graphical passwords that require the user to draw a specific pattern to authenticate. However, these methods are still susceptible to screenshot capture and are not easily integrated with existing systems and services. Additionally, they may have usability issues, such as longer authentication times and difficulty in understanding. PassBoard is a new approach that aims to address these challenges [3]. The classical PIN entry mechanism is a popular authentication scheme due to its balance of usability and security. However, when used in public systems, this scheme is vulnerable to shoulder surfing attacks. In this type of attack, an unauthorized user can observe the login session, record the session activities, and potentially gain access to the actual PIN. To address this issue, we propose a new intelligent user interface called Color Pass, designed to resist shoulder surfing attacks and allow genuine users to enter the session PIN without disclosing the actual PIN. The Color Pass interface is based on a partially observable attacker model and is shown to be safe and easy to use even for novice users through experimental analysis [4].

PINs and passwords are widely used authentication methods in various devices such as ATMs, smartphones, and electronic locks. However, traditional PIN-entry methods are vulnerable to shoulder-surfing attacks. Previous security examinations have relied on experiments and testing, rather than solely on quantitative analysis, to support proposed systems. In this paper, we propose a new theoretical and experimental technique for quantitative security investigation of PIN-entry methods. We introduce a new security concept, Grid Based Authentication System, and examine current methods under this new framework to establish rules for secure PIN-entry. Using these rules, we develop a new PIN-entry method that significantly increases the required calculations complexity, thereby preventing human shoulder-surfing attacks [5].

III. METHODOLOGY

This system overview as in figure 1 illustrates how the Surfing Attack works. The attacker places the device in the victim's physical environment, while the controller providing the main functionality is remotely connected off-site. The Surfing Attack device comprises three primary components: a signal processing module, an ultrasonic transducer, and a tapping device. Its primary function is to collect voice device output and deliver malicious commands via inaudible ultrasound. The workflow starts with the generation of voice commands or dialogues using a speech synthesis and text-to-speech (TTS) module. The controller produces the baseband signals of the voice commands, then sends them wirelessly to the attack device. The signal processor modulates the baseband signal into an excitation signal, which is transformed by the ultrasonic transducer into ultrasonic guided waves that propagate through the materials. The tapping device records the responses, which are transferred back to the controller in real-time. Based on the responses, the attacker can create follow-up commands. It is worth noting that the signal processor must maintain a high sampling rate to avoid signal aliasing. While the controller can be included in the Surfing Attack device, doing so can increase computation requirements and the form factor of the device.

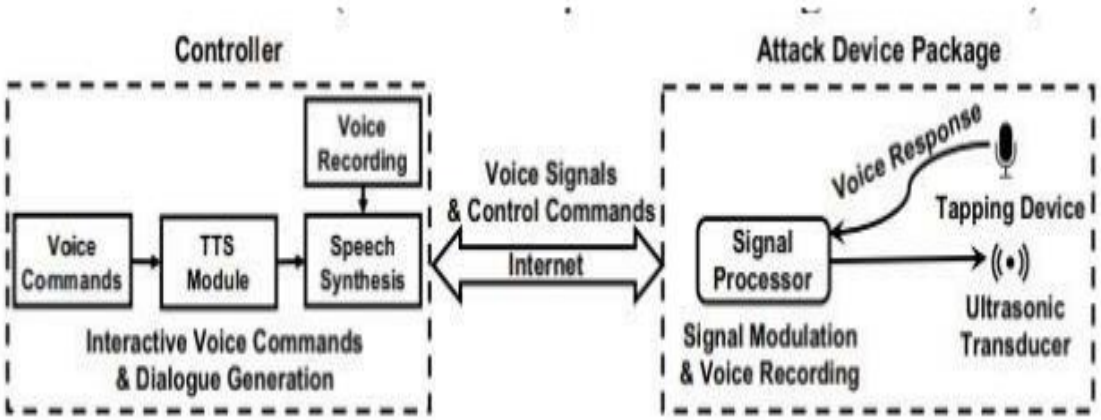

Figure 1 : Overview of surfing attack.

FRAUDULENT CALL

Phone calls are a prevalent method of communication these days, but there has been a significant rise in phone scams over the past few years, resulting in billions of dollars in financial losses for individuals and businesses. Typically, we tend to ignore calls from unknown numbers, but when we receive a call from someone we know, we let our guard down subconsciously. Advanced phone scams rely on caller ID spoofing to trick victims into thinking that the call is from a "trusted" source. Effective defense mechanisms have been proposed, but with Surfing Attack, attackers can bypass caller authentication frameworks and place fraudulent calls by directly controlling the victim's device. In this case study, we demonstrate how Surfing Attack can be used to initiate a fraudulent call via the victim's device placed on a tabletop without physical contact. Attackers can control the victim's device and engage in multi-round conversations with the hidden ultrasonic transducer and tapping device, as shown in a fraud call example where Alice's device is controlled to call her friend Sam and deceive him into revealing the access code.

IMPACT OF ATTACK DISTANCE

This section presents the evaluation of recognition rates for an activation command ("Hey Siri" or "Hi Galaxy") and a control command ("Call 1234567890") at varying distances. The recognition rates of these commands are tested on an Apple Watch and a Galaxy S6 Edge. Generally, the recognition rates for the activation command are higher than those for the control command due to the smaller number of words in the activation command. The Apple Watch achieves a 100% success rate in recognizing the activation command from a distance of 100 cm, while the Galaxy S6 Edge achieves the same success rate from a distance of 25 cm. This difference in distance may be due to the fact that Apple Watches are designed to accept voice commands from a longer distance than smartphones, as they are worn on the wrist.

IMPACT OF SOUND PRESSURE LEVELS

To improve the quality of recorded voices and recognition rates, a higher sound pressure level (SPL) is preferred for both audible and inaudible sounds. This is because a higher SPL provides a larger signal-to-noise ratio (SNR) for given noise levels. We conduct experiments to investigate the impact of SPLs on the recognition rates of the control command (“Call 1234567890”) on both the Apple Watch and the Galaxy S6 Edge smartphone using a mini sound meter to measure the environmental noise. The speaker is placed 10 cm from the target device in all experiments. We measure the impact of SPLs using two levels of granularity: sentence recognition rates and word recognition rates. The former calculates the percentage of successfully recognized commands, considering only if every word in the command is recognized correctly. The latter measures the percentage of words that are correctly interpreted. For instance, if the command “call 1234567890” is recognized as “call 1234567”, the word recognition rate is 63.6%.

TESTING THE DATASET

The dimensions of new features are stored in a numpy array called ‘n’. We want to use the predict method to predict the species of these features. The predict method takes the ‘n’ array as input and produces the predicted target value as output, which in this case is 0. To calculate the test score, we divide the number of correct predictions by the total number of predictions made. The accuracy score method is used to compare the actual values of the test set with the predicted values.

IV. CONCLUSION

This paper introduces Surfing Attack, an inaudible method for attacking SR systems. This attack utilizes the AM (amplitude modulation) technique to embed audible voice commands on ultrasonic carriers, which are not perceptible to human hearing. With Surfing Attack, an attacker can target popular SR systems such as Siri, Google Now, and Alexa. To prevent potential misuse of Surfing Attack, we propose two defense solutions that address both hardware and software aspects.

REFERENCES

[1] H. Shin, D. Kim and J. Hur, 2015 "Secure pattern-based authentication against shoulder surfing attack in smart devices," 2015 Seventh International Conference on Ubiquitous and Future Networks, Sapporo, Japan, pp. 13-18.

[2] Choi, C. Choi and X. Su, 2016 "Invisible Secure Keypad Solution Resilient against Shoulder Surfing Attacks," 2016 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Fukuoka, Japan, pp. 514-517.

[3] P. Nand, P. K. Singh, J. Aneja and Y. Dhingra, 2015 "Prevention of shoulder surfing attack using randomized square matrix virtual keyboard," 2015 International Conference on Advances in Computer Engineering and Applications, Ghaziabad, India, pp. 916-920.

[4] N. Chakraborty and S. Mondal, 2014 "Color Pass: An intelligent user interface to resist shoulder surfing attack," Proceedings of the 2014 IEEE Students' Technology Symposium, Kharagpur, India, pp. 13-18.

[5] Y. K. Mali and A. Mohanpurkar, 2015 "Advanced pin entry method by resisting shoulder surfing attacks," 2015 International Conference on Information Processing (ICIP), Pune, India, pp. 37-42.