Treat ’Em Like Other Devices: User Authentication of Multiple Personal RFID Tags

Nitesh Saxena
Polytechnic Institute of NYU
Six MetroTech Center
Brooklyn, NY 11201
nsaxena@poly.edu

Md. Borhan Uddin
Polytechnic Institute of NYU
Six MetroTech Center
Brooklyn, NY 11201
borhan@cis.poly.edu

Jonathan Voris
Polytechnic Institute of NYU
Six MetroTech Center
Brooklyn, NY 11201
jvoris@isis.poly.edu

ABSTRACT

User-to-tag authentication can prevent a variety of potential attacks on personal RFID tags. In this poster, a new RFID authentication scheme is presented that allows a user to control when a tag responds to queries by leveraging a mobile phone. The design and implementation of this approach is presented along with a study of its usability.

1. INTRODUCTION

RFID tags respond promiscuously to all queries issued by any reader. This leads to security and privacy concerns for personal tags, such as those used in access cards. Since a malicious entity can easily read a tag without the authorization or knowledge of the tag’s owner, a variety of attacks are possible on this class of devices. These include clandestine eavesdropping and relaying [2, 3]. It is therefore necessary to authenticate users to their RFID tags to address this issue. Fundamental difficulties exist in developing viable user-to-tag authentication methods, however. Since RFID devices are designed to be transparent to their users, they lack any user interfaces. Moreover, RFID usage is atypical compared to that of other devices in that most users prefer to keep their tags stored in their wallet or pocket during authentication [1]. This means that any user-to-tag authentication system must be careful not to inadvertently unlock all stored tags when a user attempts to unlock a single tag, as this would allow attacks to be mounted on the other devices. The problem of RFID authentication becomes quite challenging in light of these issues. This poster proposes a novel means of authentication between a human and her personal RFID tags. This approach, called PIN-Vibra, allows a user to control when and where her RFID tags can be accessed.

Mobile phones have become an integral and indispensable part of users’ lives and are consistently available. Such a device can therefore be effectively exploited to achieve strong RFID authentication. In the PIN-Vibra approach presented in this poster, a mobile phone acts as a token which can be used to authenticate to an accelerometer-equipped RFID tag. Authentication is achieved by simply touching a vibrating phone with a wallet or other object carrying a user’s RFID tags. This technique has several advantages which are explored throughout this work. The design and implementation of PIN-Vibra on Intel’s WISP tags [4, 5] is discussed. Furthermore, a usability evaluation of the proposed method is presented along with its results, which indicate that the mechanism is reasonably efficient, robust, and user friendly, despite the usage constraints imposed by RFID technology.

2. RELATED WORK

A recent approach called “Secret Handshakes” [1] is closely related to this proposal. In order to authenticate to an accelerometer equipped RFID device [4, 5] using Secret Handshakes, a user must move or shake the wallet containing the device in a specific pattern. While the Secret Handshakes approach is desirable for not requiring any reader-side changes, it also has some shortcomings. When a user shakes a wallet in a particular manner in order to unlock a desired RFID tag, *all* devices in the wallet get unlocked, enabling relay attacks on other devices. To prevent this, each device must be associated with a *unique* pattern which a user must remember. This might become cumbersome as the number of devices increases. Moreover, there might only exist a limited number of “robust” movement patterns. Also, this scheme does not provide any protection against the loss or theft of a user’s wallet containing the RFID devices. Finally, since Secret Handshake authentication requires users to make a visible motion, this authentication method is vulnerable to visual observation attacks such as shoulder surfing.

3. RFID AUTHENTICATION USING A MOBILE PHONE

PIN-Vibra uses a mobile phone, M, as an authentication token for a user to authenticate to a RFID device, D. The crux of the idea is to authenticate the user to D via M. Mobile phones are not as constrained in terms of memory and computational capabilities in comparison to a human user and thus can form the basis of strong authentication to multiple RFID devices. Given a tag equipped with an onboard accelerometer, and given that almost all current mobile phones have vibrational capability, PIN-Vibra builds a novel out-of-band (OOB) channel between M and D which can be used to authenticate the former to the latter. This communication channel is assumed to be secret as well as authenticated. Authentication can therefore be achieved by simply transmitting a PIN or secret key shared between M and D over this OOB channel.

Consider an adversary who attempts to launch a user impersonation or relay attack on a tag that is using PIN-Vibra. Assume that the PIN shared between the phone and each RFID device is p bits. Additionally, consider a user who is restricted to q authentication attempts to the RFID device. Once an adversary has physical access to a user’s RFID device, the probability of success of the adversary attempting to impersonate a user and access the RFID service is at most $q/2^p$. Clearly, if the adversary has physical access to both the phone and RFID, she can succeed in accessing the RFID service. Having physical access to only the phone would not be sufficient, however.

4. DESIGN AND IMPLEMENTATION

To test PIN-Vibra, a prototype implementation was developed using Intel’s WISP tags [4, 5]. As WISP tags, like typical RFID tags, have low computational, memory and power capabilities, its onboard accelerometer is not able to detect different vibration intensities. Thus, for encoding a PIN using vibration, a simple time interval based ON-OFF encoding scheme was employed. A four-digit PIN is used in this prototype, which is equivalent to 14 bits of binary data. Three additional bits ('110') are used as a "start" sequence to indicate the beginning of the transmission. Each '1' bit is converted into a vibration of 200ms and each '0' bit is converted to a 200ms interval of stillness. Thus for transmitting 4-digit PIN a total of 17 bits of transmission are needed, resulting in a total transmission time of $17 \times 200\ ms = 3.4\ seconds$. After booting up, the tag's onboard accelerometer starts sensing the vibration sequence (i.e., the encoded PIN). If the decoded vibration sequence matches the stored PIN on the tag it transmits its ID to the reader; otherwise the tag does not transmit.

5. EXPERIMENTATION AND EVALUATION

A usability study was conducted to investigate the viability of the PIN-Vibra prototype. Tests were administered in which 20 subjects utilized PIN-Vibra to authenticate themselves to a RFID reader as per a normal access card usage scenario. These interactions were logged to measure the speed and reliability of the prototype. Additionally, test subjects were polled using pre- and post-condition questionnaires to determine their view of the proposed system, particularly as compared to a typical access card setup.

No errors caused by mistakes made by users while manipulating the mobile device were observed. This result indicates that users are capable of authenticating themselves via a vibratory channel. The only errors observed were due to problems caused by capturing and processing the OOB vibration transmission between the WISP tag and mobile device. While carrying out the 80 test cases, 21.25% were transmitted completely correctly, 42.50% were off by a single bit, and 27.50% were off by two bits. The remaining 8.75% were incorrect in more than two of the bits transmitted. The average time taken to complete the authentication process was 7.122 seconds with a standard deviation of 0.929 seconds. Out of the approximately 7 seconds taken to authenticate, 3.4 seconds were taken up by the vibration transmission and 3.6 seconds were caused by user manipulation.

These results suggest that the vibrational authentication scheme is a promising solution for RFID access card insecurity. The lack of user-induced errors demonstrates the scheme's usability. Although hardware based errors were observed, these are less cause for concern as they can be assuaged through hardware optimizations. While the new scheme takes slightly longer than normal access card usage, this is a necessary tradeoff for the stronger security provided by PIN-Vibra. No average user study responses were negative for positive questions or vice versa. Test subjects indicated agreement with statements that PIN-Vibra was easy to use, intuitive, and enjoyable. Conversely, they felt that the scheme did not seem lengthy or challenging.

6. DISCUSSION

These usability study results show that PIN-Vibra takes approximately 7 seconds to complete on average. The underlying vibration channel results in a fairly high amount of 1 bit (42.5%) and 2 bit errors (27.50%), but a low rate of errors in 3 or more bits (8.75%). Since transmission on the vibration channel accounts for 3.4 seconds, these results also show that the user induced delays accounted for $(7 - 3.4) = 3.6$ seconds on average. Because these user actions were more or less independent of PIN-Vibra, it can be argued that RFID access card usage can not be faster than few seconds in practice, even without any authentication mechanism in place.

A vibration-based OOB channel was used in this authentication method due to its inherent secrecy properties. Traditional PIN or password-based authentication methods, or other setups that utilize a visual channel, are vulnerable to visual eavesdropping techniques such as shoulder surfing. Similarly, there exist different possibilities for eavesdropping on a vibration channel. Specialized equipment could be designed that utilize radar, lasers, or electromagnetic emanations to detect vibration. Example of such a devices can be found in [7, 6]. However, these need sophisticated pieces of equipment that would require a great deal of expertise to create and operate. While plausible, this type of technique has challenges that must be overcome with a combination of technical expertise and custom built equipment. This is in contrast to traditional authentication techniques, which can be defeated through casual observation by an unassisted human with little technical knowledge.

7. CONCLUSIONS AND FUTURE WORK

In this poster, a novel approach for authentication of multiple RFID tags, PIN-Vibra, was introduced. This approach leverages a pervasive device such as a mobile phone, which has become an inseparable part of many users' lives. In PIN-Vibra, this phone acts as an authentication token, forming a unidirectional communication channel between a user and her RFID tags. Authenticating to a RFID tag using PIN-Vibra involves simply touching a vibrating phone to the wallet or object carrying the tag. The design and implementation of the new authentication method on Intel's WISP tags was discussed. A usability evaluation of PIN-Vibra was also reported, the results of which indicate the method to be reasonably efficient, robust, and user friendly, despite several design constraints in the context of RFID authentication. Future work includes improving the speed and robustness of the proposed vibration channel, looking for efficient ways to perform RFID fallback authentication, and further usability studies with a broader, more diverse user pool.

8. REFERENCES

[1] A. Czeskis, K. Koscher, J. R. Smith, and T. Kohno. RFIDs and Secret Handshakes: Defending Against Ghost-and-Leech Attacks and Unauthorized Reads with Context-Aware Communications. In *CCS*, 2008.

[2] A. Juels. RFID Security and Privacy: a Research Survey. *IEEE Journal on Selected Areas in Communications*, 24(2):381–394, 2006.

[3] Z. Kfir and A. Wool. Picking Virtual Pockets using Relay Attacks on Contactless Smartcard. In *Security and Privacy for Emerging Areas in Communications Networks (Securecomm)*, 2005.

[4] A. Sample, D. Yeager, P. Powledge, and J. Smith. Design of a Passively-Powered, Programmable Sensing Platform for UHF RFID Systems. In *IEEE International Conference on RFID*, 2007.

[5] J. Smith, A. Sample, P. Powledge, A. Mamishev, and S. Roy. A Wirelessly-Powered Platform for Sensing and Computation. In *UBICOMP*, 2006.

[6] W. van Eck. Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? *Computers and Security*, 1985.

[7] G. Williamson. Laser Microphone. Available at `http://www.williamson-labs.com/laser-mic.htm`, 2006.