Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2015 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-13-2015

A New Approach to Mobile Device Authentication

Jordan Shropshire
University of South Alabama

Philip Menard
University of South Alabama

A New Approach to Mobile Device Authentication

Jordan Shropshire
Associate Professor
University of South Alabama
jshropshire@southalabama.edu

Philip Menard
Assistant Professor
University of South Alabama
pmenard@southalabama.edu

ABSTRACT

The effectiveness of primary and secondary authentication systems on mobile devices leaves room for improvement. Device manufacturers provide security features which require users to memorize long, complex passwords and/or provide biometric information. These approaches have drawbacks which make their continued usage untenable. Users are already inundated with passwords and regularly forget answers to security challenges. People are growing resistant to sharing their biometrics with device manufacturers. An authentication solution which overcome these limitations are essential. This research addresses this need by proposing a new method for mobile device authentication. First, it reviews past and current approaches to authentication. It then identifies design goals for future mobile device authentication systems. Finally, it describes a new model for backup mobile device authentication. The proposed model integrates video with social authentication for asynchronous secondary verification.

Keywords: Authentication, mobile, user-friendly, video, user interface

INTRODUCTION

Given the prevalence of smartphone theft and the sensitivity of onboard data, manufacturers have begun incorporating features which provide last-resort defenses against local attacks (Williams 2014). Most mobile devices are equipped with lock codes – PIN or character sequences which prevent data thieves from accessing information. Password complexity requirements are often enforced in order to slow brute force attacks (Hamblen 2013). This makes them difficult to remember. Some devices have backup authentication systems which use biometrics. However, a major risk to biometrics is privacy. Users are increasingly resistant to using biometrics because they do not want these records available to device manufacturers (Munday 2013). At least one survey shows that educated users are more concerned about their privacy than the potential security benefits (Pons et al. 2008).

There is a need for primary and backup means of mobile device authentication which are more manageable for users than passwords and are not as risky as biometrics. The purpose of this research is to (1) review traditional and contemporary authentication approaches for mobile computing, (2) provide guidelines for designing authentication techniques which are robust, scalable, and user-friendly, and (3) propose a new model for secondary mobile device authentication. In this model, a person's trusted contacts are entrusted to confirm his or her identity. This decision is used to programmatically unlock the mobile device. Specifically, a locked-out user records a video of himself or herself reading a time-sensitive CAPTCHA. The video is distributed to select members of the user's social network. These individuals watch the video to confirm the identity of the user. They also view the CAPTCHA text and compare it against the user's reading of the CAPTCHA to ensure that the video was recently recorded and the device is not in the hands of thieves. If the user's identity and the timestamp are authenticated, then the

device is unlocked. This method differs from other contemporary approaches in that it supports asynchronous communication. Trusted contacts can provide authentication at their convenience and are not required to be on video to complete the process.

Given the ubiquity of complex passwords and the risks associated with biometrics, new approaches to authentication are essential. There is a need for robust, user friendly authentication procedures which do not sacrifice security. The authentication model proposed in this manuscript could be of significant value to businesses and end users. The remainder of this paper is organized as follows: Section Two describes traditional approaches to authentication. Section Three describes contemporary and emerging developments in mobile device authentication. Section Four considers the requirements of user-friendly authentication. Section Five presents the proposed model for secondary authentication and describes its implementation. Finally, Section Six provides conclusions and discusses future directions.

TRADITIONAL APPROACHES

Given their susceptibility to physical theft, mobile devices warrant increased security features. Often, the last line of defense is the lock code which prevents unauthorized users from pilfering data. Authentication is therefore paramount. Traditionally, authentication techniques are based on one or more of the following three approaches: Something the user knows, something the user has, and something the user is (Furnell et al. 2008). The first approach relies on secret knowledge such as PINs and passwords. Passwords are complex, long, hard to remember, must be regularly changed, cannot be dictionary-based, and cannot be written down (Stajano 2011). These added complexities are meant to reduce the likelihood of an effective brute force attack or dictionary attack on account credentials. However, mobile device users already have to keep track of many complex passwords and user names.

The second authentication approach relies on something a user has. This approach generally involves a separate hardware device called a security token. The token provides a cryptographic value on demand. The authenticating user enters the token string to electronically prove his or her identity. If the string supplied by the user matches the value expected by the authentication system, then the user is authenticated. The primary weakness of separate, hardware-based tokens it that they are also susceptible to theft (Nieva 2014). If an independent hardware token is required for authentication, then it should be assumed that the hardware token will be kept near the mobile device (O'Gorman 2003). This increases the risk that both components will be stolen. Not only would the thief have the stolen device, he or she could also have the means to log into the system.

The third authentication approach involves biometrics. Biometric authentication classifies users according to a physical attribute such as a fingerprints, facial features, or iris patterns. During enrollment, one or more physical traits is observed by the device sensors and is associated with the user's account. For authentication, the device takes a measurement of the same biological feature (e.g. fingerprint). If the observed values match the saved values, then it is assumed the user is verified. However, this authentication approach is not without limitations (Clarke et al. 2007). Many users are becoming leery of sharing their biometric properties with device manufacturers and software companies (Munday 2013).

Although the triad of passwords, tokens, and biometrics has worked in the past, it does not meet the scalability, robustness, and user-friendliness requirements which must be incorporated into future designs (O'Gorman 2003). Some researchers have recognized these requirements and are exploring solutions which move beyond the traditional authentication approaches.

RECENT DEVELOPMENTS

An emerging trend in authentication is to pass the responsibility for authentication onto other systems or people who can confirm the user's identity. This type of approach is called transitive authentication (Reeder, 2011). Transitive authentication approaches are generally proposed as secondary or fallback methods which are used if password or PIN authentication is unsuccessful (Javed et al. 2014). They typically incorporate email, phone, or trusted contacts. For email based authentication, locked-out users request to have their password reset or account otherwise unlocked. An access code is then sent to the email address associated with the account. The code or password is entered into the system or service's user interface in order to unlock the account. This process is based on the assumption that only the authorized user will be able to access the secret code sent to the associated email account (Garfinkel 2003). This is a reasonable assumption, given that email service providers implement robust authentication systems and users generally value the privacy of their email accounts. However, there are some limitations to email-based authentication. For instance, if addresses are not updated regularly then the code may be sent to an inactive email account. Further, users who are locked out of their mobile device will need access to another computer in order to retrieve the access code. This could be problematic for persons who are traveling or are away from the office.

The second type of transitive authentication is phone-based authentication. This procedure works like email authentication with the exception that text or SMS messages are sent instead of emails (Jakobsson et al. 2008). During account enrollment, the user provides his or her mobile phone number. To unlock the device, the user receives an access code on his or her phone. As with email addresses, users may change mobile phone numbers without remembering to update the settings in all of their accounts (Georgea et al. 2011). Further, this method assumes that the user

has access to the text message on the designated mobile device. The assumption is problematic if the user is locked out of the device.

The third type of transitive authentication is social authentication. It is based on the assumption that people are good at recognizing their friends, family members, and co-workers (Schechter et al. 2009). The sensors on mobile devices are used to convey the physical appearance, voice, or speech mannerisms of locked out users. There are several variations of this technique. Some social media websites authenticate users by asking them to identify someone they know from a line of images (Sharmila et al. 2013). The user is then instructed to correctly name the individual by selecting his or her name from a list. The displayed images are from the user's social network (e.g. friends or contacts). Another variation of trusted contact authentication is based on the principal of email or text authentication. The locked out user one of contacts his or her trusted contacts and asks them to initiate the account unlock process. The trusted contact then requests an unlock code be sent to their email address. When the trusted contact receives the code, he or she relays it to the locked out user. This approach can be challenging for users to manage. The user must not only remember who is a designated trustee but also be able to contact that person without using his or her mobile device (Javed et al. 2014). Another approach is based on software which grants locked out users limited access in order to initiate a video conference with a trusted contact (Libonati et al. 2014). This approach is quite promising but it is limited in that relies on synchronous communication. The locked out user must wait until one or more of his or her trusted contacts is available to confirm his identity and initiate device unlock procedures.

NEW REQUIREMENTS

Any time a new tool is introduced in existing information systems, the impact of changes to human-computer interaction (HCI) must be considered. System usage and adoption is a core

research area in IS, and one of the most critical factors that influences adoption is the user's perception of performance expectancy of the system (Davis 1989; Venkatesh et al. 2003). Performance expectancy is the degree to which an end user believes that using the system will help achieve gains in performance (Venkatesh et al. 2003). For adoption of our proposed tool to be successful, users must perceive that the tool is successful in helping to further protect their mobile devices, thus achieving gains in overall device security. Thorough testing of our proposed solution will be necessary to determine if the usefulness of the system meets users' standards.

One of the most obvious factors that should be examined is effort expectancy, which through a multitude of IS studies has demonstrated a strong influence on both intention to use a system and actual system usage (Venkatesh et al. 2003). At face value, the proposed authentication mechanism should seem to minimize effort for smartphone users, as the user would not be required to perform a large number or difficult set of steps to achieve authentication (see Section five for a detailed discussion of the proposed authentication model). As the mechanism is examined further, however, effort expectancy will certainly be assessed.

Similarly, the confidence that a user possesses related to his or her ability to perform a task in an information system may impact the user's ultimate usage of the system. Behavioral information security researchers have widely adapted Protection Motivation Theory (PMT) as a means to understand users' adoption behaviors regarding information security protocols or software solutions (Crossler et al. 2013). With PMT, self-efficacy is one of the key elements that influences a user's performance of secure behaviors (Floyd et al. 2000; Maddux et al. 1983). The extent to which the system is easy to use and does not require tasks that are drastically different than what a user is accustomed to will influence the user's perception of self-efficacy for that task.

This should result in a user feeling confident in his or her ability to use the proposed authentication mechanism.

Another important factor included in the PMT model is response cost, which may be manifested in several ways, including the monetary cost of the solution, the effort involved in performing the secure behavior, or the amount of time required to perform the recommended response (Ifinedo 2012). If the response cost of a particular security solution is too high, the user's performance of the secure behavior could be negatively affected (Herath et al. 2009; Vance et al. 2012; Workman et al. 2008). Our proposed authentication mechanism would not require a great deal of time or effort on the user's part, and if bundled in the mobile device's operating system, the new authentication method would not introduce a monetary burden to the user.

Response cost also highlights another important factor in developing new tools in information systems – cognitive load, which refers to the mental burden associated with performing a particular task (Browne et al. 2007; Gallupe et al. 1988; Zigurs et al. 1998). Developers must be mindful of not substantially increasing a user's cognitive load while he or she is performing a task in a system. Because our proposed solution will only require a user to record a short video for SMS transmission, the cognitive load required for this task should be minimized.

MODEL FOR SOCIAL AUTHENTICATION

Overview

Having reviewed past and present approaches to authentication and elicited the requirements for future verification mechanisms, this section describes a new process for mobile device authentication (see Figure 1). Based on the concept of transitive authority, it incorporates elements of social authentication and video communication. It differs from current video-based approaches in that it is asynchronous. A person's trusted contacts can provide authentication at

their convenience. Further, they are not required to be on video in order to complete the process. The proposed model is designed to be used as a back-up means of authentication, in instances in which a user cannot remember his or her password or PIN but requires device access.

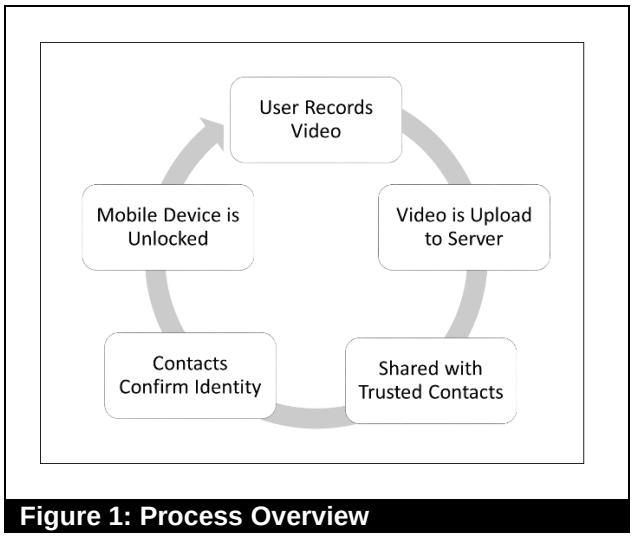

Figure 1: Process Overview

It is designed to be implemented as an extension to a mobile operating system and requires that the mobile device have onboard video and audio recording hardware. For account setup, the user identifies contacts who will serve as his or her trustees. These contacts are selected or deselected via the standard device contacts menu. During lockout, the user activates a feature which prompts him or her to record a short video in which he or she reads a time-sensitive CAPTCHA message. The video is then distributed to the trusted contacts via text message.

The Trustees would watch the video to confirm the identity of the user. They would also compare the embedded string which the user is reading against an identical copy of the CAPTCHA which is displayed to them. The purpose of the time-sensitive CAPTCHA is to ascertain that the video was recorded recently and that it is likely that the person in the video is still in possession of the hardware. If the string does not match the string which is displayed to the trustee, then it is assumed that the video is not recent enough to confirm possession of the device. If the person in

the video is appears to be the legitimate device owner and the CAPTCHA strings match, then the user is considered to be authenticated.

Although the request will be distributed to multiple trustees, the device state (LOCK or UNLOCK) will be based on the first response received from a trustee. Once this message is received, a "nevermind" message will be sent to the other trustees. A slightly more advanced process could incorporate a polling algorithm that waits for either a quorum or a time period before tallying votes. But this would force the user to wait longer and include the possibility that not enough trustees respond before the authentication window expires. The proposed time period of 20 minutes was selected because it seemed to be a reasonable balance between convenience and the likelihood of losing one's phone. However, it is not based on any empirical evidence and is therefore subject to change.

A benefit of this approach is that it is asynchronous. It is not necessary for users to interact with their trusted contacts in real time. Trustees can verify the user's identity at their convenience. They do not need to appear on video. This approach also eliminates the hassle of finding alternative means of communication. Further, it reduces the likelihood of beating the authentication system, since people are generally good at recognizing their friends and close colleagues. In addition, it supports communication between dissimilar operating systems because communications are transmitted via SMS message. Although the system is synchronous, it does incorporate windowing in order to ensure that the requesting user still has possession of the device. Some users could be forced to record multiple videos if none of their trustees respond in time. This problem would be more significant during late night/ early morning hours. This inconvenience could be overcome by incorporating trusted contacts from other time zones.

Implementation

The proposed model is designed to be implemented in two components: a mobile device software module and an authentication server. The mobile device software could be implemented as a JAVA extension for mobile device operating systems such as Android and iOS. The extension is activated by the user on lockout. A "forgot password" button is added to the login screen. Selecting this option launches a graphic user interface which first prompts the user to create a video of himself or herself reading CAPTCHA text. Once the user presses the record button, the CAPTCHA text is downloaded from the server and displayed onscreen. After the user finishes recording the video, he or she presses the submit button. At this point, the video is uploaded to the server for distribution to trusted contacts. The mobile device software deletes the video file after it receives a confirmation of a successful upload. The role of the server is to distribute and manage time-sensitive CAPTCHA files and facilitate sharing of the video file. The server is conceived as a Linux operating system with SSL and TLS modules for secure communication between endpoints. It uses a combination of newly-developed JAVA code and open-source software to provide support functionality. These processes are depicted in Figures 2 and 3 (below).

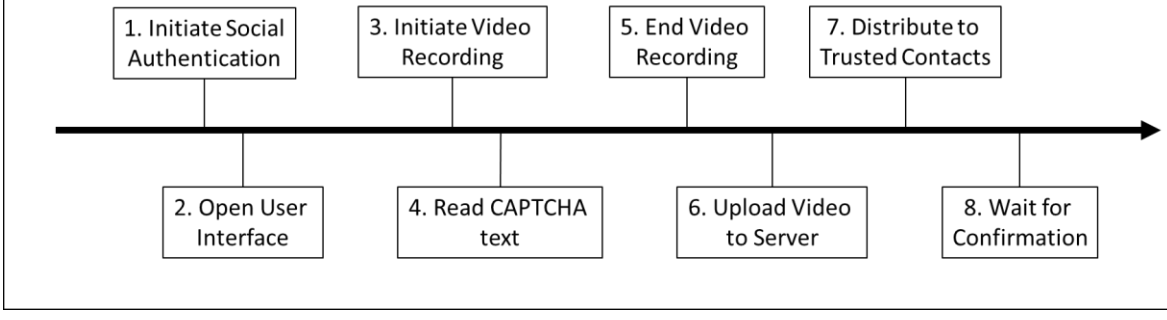

Figure 2: Overview of Locked-Out User's Role

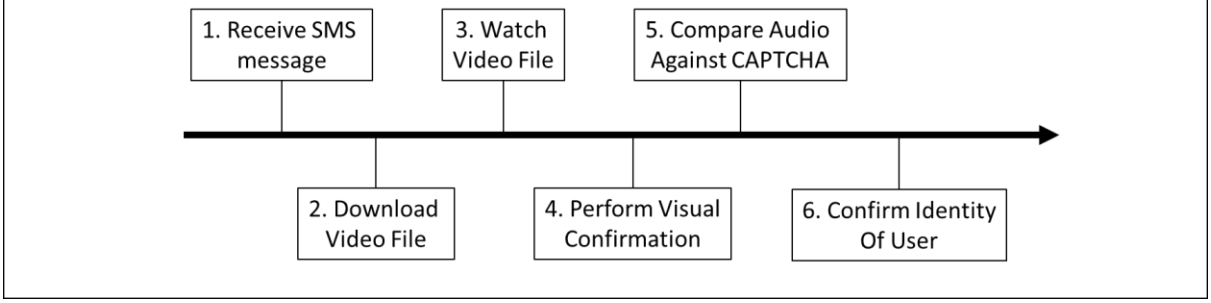

Figure 3: Overview trusted Contact's Role

Future Research

This research provides the outline of a new method for social authentication on mobile devices. Although it has been proposed as a solution for overcoming mobile device lockout, it could also be used for other applications. For instance, numerous banks, credit card companies, cloud platforms, and social media platforms require strong authentication to verify users. This same concept could be used authenticate users in cases in which passwords are forgotten or additional security challenges are required (e.g. location, time, or amount attributes are uncharacteristic of the associated account).

The next step is to develop and test the proposed solution. This process is currently underway. An early proof-of-concept has been created and implemented on the Android platform. User testing is expected to begin shortly (before WISP 2015). For testing, a sample of approximately 30 users will be provided smartphones which are equipped with the software extension. The smartphones will be modified so that the login PINs are six numbers long, significantly increasing the likelihood that users will forget their PIN. They will then be forced to activate and test the secondary authentication system. Statistics will be collected for each use of

the proposed authentication system. Finally, a survey of the users will be conducted at the end of the study in order to gauge their sentiments and identify improvements.

CONCLUSION

In the past, the authentication triad of "something you know, something you have, or something you are" has been the standard means for user authentication. However, the susceptibility of mobile devices to theft, the sensitive nature of their data, and the increased complexity of passwords call for advances in mobile device authentication. This research contributes toward this goal by reviewing past and present authentication methods. It also considers behavioral implications and future end user requirements. For illustration, this manuscript describes a conceptual model for secondary mobile device authentication. The model is based on the principle of transitive authentication. Users' trusted contacts are responsible for verifying their identity by watching a recent video recording. The proposed model goes beyond existing approaches in that it supports asynchronous video-based authentication. If properly implemented, it would provide strong authentication while relieving users of many of the burdens associated with current authentication methods. In future research, a working prototype of the authentication model should be evaluated across a number of realistic testing scenarios involving non-technical users. The results will have significant implications for researchers and end users.

REFERENCES

Browne, G., Pitts, M., and Wetherbe, J. 2007. "Cognitive stopping rules for terminating information search in online tasks," *MIS Quarterly*), pp 89-104.

Clarke, N., and Furnell, S. 2007. "Advanced user authentication for mobile devices," *Computers & Security* (26:2), pp 109-119.

Crossler, R., Johnston, A., Lowry, P., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future directions for behavioral information security research," *Computers & Security* (32), pp 90-101.

Davis, F. 1989. "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly*), pp 319-340.

Floyd, D., Prentice-Dunn, S., and Rogers, R. 2000. "A meta-analysis of research on protection motivation theory," *Journal of applied social psychology* (30:2), pp 407-429.

Furnell, S., Clarke, N., and Karatzouni 2008. "Beyond the PIN: Enhancing user authentication for mobile devices," *Computer Fraud & Security* (2008:8), pp 12-17.

Gallupe, R., DeSanctis, G., and Dickson, G. 1988. "Computer-based support for group problem-finding: An experimental investigation," *MIS Quarterly*), pp 277-296.

Garfinkel, S. 2003. "Email-based identification and authentication: an alternative to PKI? ," *IEEE Security & Privacy* (1:6), pp 20-26.

Georgea, B., Valevaa, A., and Mangalaraja, G. 2011. "Usable authentication in Ebusiness: challenges and opportunities," *Journal of Information Privacy and Security* (7:2), pp 28-64.

Hamblen, M. 2013. "Mobile phone security no-brainer: Use a device passcode," http://www.computerworld.com/article/2497183/mobile-security/mobile-phone-security-no-brainer--use-a-device-passcode.html, ComputerWorld.

Herath, T., and Rao, H. 2009. "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems* (18:2), pp 106-125.

Ifinedo, P. 2012. "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Computers & Security* (31:1), pp 83-95.

Jakobsson, M., Stolterman, E., Wetzel, S., and Yang, L. 2008. "Love and Authentication," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '08)*: Florence, IT.

Javed, A., Bletgen, D., Kohlar, F., Durmuth, M., and Schwenk, J. Year. "Secure fallback authentication and the trusted friend attack," IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW), Madrid, SP, 2014.

Libonati, A., Caine, K., kapadia, A., and Reiter, M. 2014. "Defending against device theft with human notarization," in *International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*: Miami, FL.

Maddux, J., and Rogers, R. 1983. "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *Journal of Experimental Social Psychology* (91:1), pp 93-114.

Munday, O. 2013. "Biometric Security Poses Huge Privacy Risks," http://www.scientificamerican.com/article/biometric-security-poses-huge-privacy-risks/, Scientific American.

Nieva, R. 2014. "Confessions of a smartphone thief," http://www.cnet.com/news/smartphone-thief/, CNET.

O'Gorman, L. 2003. "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE* (91:12), pp 2021-2040.

Pons, A., and Polak, P. 2008. "Understanding user perspectives on biometric technology," *Communications of the ACM* (51:9), pp 115-118.

Schechter, S., Egelman, S., and Reeder, R. 2009. "It's not what you know, but who you know: a social approach to last-resort authentication," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09)*: Boston, MA.

Sharmila, K., Janaki, V., and Nagaraju, A. Year. "Enhanced user authentication techniques using the fourth factor "some body the user knows" " International Conference on Advances in Computer Sciences (AETACS), NCR, IN, 2013.

Stajano, F. Year. "Pico: No more passwords!," 19th International Workshop on Security Protocols, Cambridge, UK, 2011.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating IS security compliance: Insights from habit and protection motivation theory," *Information & Management* (49:3), pp 190-198.

Venkatesh, V., Morris, M., Davis, G., and Davis, F. 2003. "User acceptance of information technology: Toward a unified view," *MIS Quarterly*), pp 425-478.

Williams, M. 2014. "10 things to know about the smartphone kill switch," http://www.pcworld.com/article/2367480/10-things-to-know-about-the-smartphone-kill-switch.html, PCWorld.

Workman, M., Bommer, W., and Straub, D. 2008. "Security lapses and the omission of information security measures: A threat control model and empirical test," *Computers in Human Behavior* (24:6), pp 2799-2816.

Zigurs, I., and Buckland, B. 1998. "A theory of task/technology fit and group support systems effectiveness," *MIS Quarterly*), pp 313-334.