Who Are You? It Depends (On What You Ask Me!): Context-Dependent Dynamic User Authentication

Raghav V. Sampangi
Faculty of Computer Science, Dalhousie University
Halifax, NS, Canada
raghav@cs.dal.ca

Kirstie Hawkey
Faculty of Computer Science, Dalhousie University
Halifax, NS, Canada
hawkey@cs.dal.ca

1. WHO ARE YOU? AN INTRODUCTION

In this position paper, we present a new mechanism for context-dependent user authentication. We propose an approach in which the type of authentication (single/two factor, two-step, etc.) and the choice of the authentication mechanisms (algorithms/protocols used) vary dynamically, depending on contextual information.

Authenticating mechanisms in online and offline systems rely on three main factors related to the user [2]—user attributes (e.g. fingerprint), knowledge (e.g. password, PIN) and possession (e.g. devices, cards). With most of our daily transactions being online, the emphasis on multi-step verification and multi-factor authentication is more than ever now.

Traditionally, the approaches to user authentication have been more static, which have often proved to be less secure. More recently, some researchers [3] have explored allowing users to choose one of several available authentication schemes. In the recent past, researchers have also considered context-dependent attributes in user authentication. Context is information that allows a system to "characterize the situation of an entity, where an entity can be a person, place, or physical, or computational object" [4]. Using context-dependent attributes makes a system more dynamic and adaptive; it makes it possible for systems to associate levels of trust with user actions to grant access to requested resources [1] and to design adaptive systems to authenticate users based on their location and other attributes [5].

In our approach, we consider the possibility of making the authentication process itself dynamic, in that the type of authentication (whether the system uses single or multiple factors, and if the system uses two-step verification) and the choice of the mechanism used are determined dynamically. By doing so, the authentication remains dynamic—not known to either the user or the administrator, and we hope to make it difficult for an unauthorized entity to gain access to the system, if he/she has acquired user credentials and/or possessions (devices, cards, etc.).

Symposium on Usable Privacy and Security (SOUPS) 2016, June 22-24, 2016, Denver, Colorado.

2. IT DEPENDS: OUR APPROACH

In our work, we set out to explore the extent to which user authentication can be dynamic and adaptive. Having explored existing research (and having been at the receiving end of stolen credentials!), we considered ways to make the authentication unpredictable to an unauthorized entity.

We were inspired by the potential of context-aware systems and the promise shown by multi-factor authentication and two-step verification in being able to successfully (and increasingly reliably) authenticate users. The ability of contextual data to uniquely define a transaction motivated us to consider a combination of the two. We considered the feasibility of dynamically choosing mechanisms to authenticate users, which led us to design our system with a context-dependent choice of the authentication mechanism. For example, we could deploy *N* approaches to authenticate a user (such as password, PIN, fingerprint recognition, etc.) and choose one of them, as decided by the context signature. We define a context signature to be a hashed value of the contextual information that define the situation of a transaction. We then decided to add one more layer of unpredictability by making the type of authentication also context-dependent. Note that we consider two-step verification, two-factor authentication and a combination thereof as *types of authentication* in our work. However, in addition to the context of use, we also need to consider organizational policies around resource access and any role-based restrictions.

These factors led us to develop our context-dependent dynamic authentication system (illustrated in Figure 1) that works as follows:

Context acquisition: When the user requests to log in to access a resource, a user context profile is generated, which includes the devices in which the user has logged in, the location from where the request was received and other pertinent user data. The context acquisition process is based on the dynamic context-object model discussed in [6].

Context signature generation: Following context acquisition, a context signature is generated by computing a hash of the contextual information. This context signature is used with a pseudorandom number generator to choose (a) the type of authentication, and (b) the specific mechanisms to be used.

These two steps are followed by a *user authentication* step, where the user responds by entering appropriate credentials as expected by the mechanism, using a conventional challenge-response protocol.

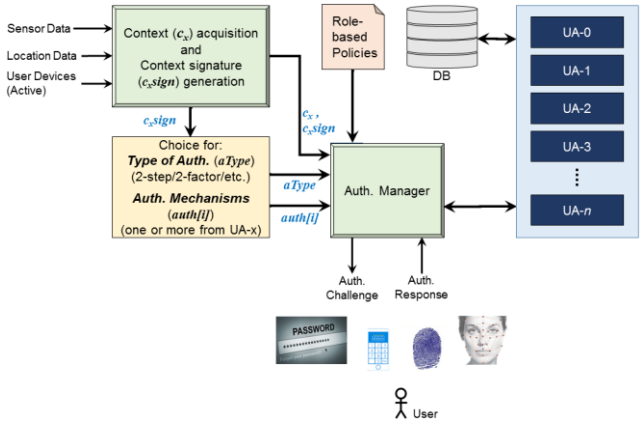

Figure 1. Modules in the proposed context-dependent authentication model (UA-x represents user authentication mechanisms such as password-based, PIN-based, etc.).

For example, if authentication type was determined to be two-step verification, and mechanisms were chosen to be face recognition and one-time password (OTP) token generation, then, the user would first have to record a live face and will be asked to enter a OTP sent to a registered device.

In deciding the type and mechanisms, the authentication manager considers both role-based and other organizational policies around resource access.

3. WHAT'S NEXT?

Our work considers the limitations of current industry practices in authentication and proposes a solution that is context-dependent, user role-dependent, and presents a dynamic way to combine and use several successful authentication paradigms. In doing so, we hope to introduce unpredictability in the manner in which a user is validated by the system. The changing conditions and expected responses to authentication challenges will make it harder for an unauthorized entity to be prepared in their attempt or to know what to expect. Of course, we understand that users of such a system could face longer (and complex) registration processes and may need to remember more than one password. However, since this system uses techniques such as biometric authentication that does not need users to remember anything, the burden on the user is minimal. We believe this is a starting point, and could one day lead to systems that do not require users to remember several credentials with its dynamic and adaptive choices.

In this workshop, we would like to discuss the viability of such a dynamic authentication system in real-life applications. We would also like to take this opportunity to discuss appropriate user study designs that will help us validate our work. We begin our work with the following set of initial research questions:

I. From an everyday user's perspective:

[U1] *Ease of use and willingness to adopt*: Are users willing to adopt such a system? How easy will the system be for people to use, given that there are many security mechanisms and each of them would require the user to do/submit something different?

[U2] From what is being shown to the users on the interface, is it clear to the user as to what action needs to be performed by them? Is it clear to them what the consequences will be of any action they take?

[U3] *Trust issues*: Are users willing to trust such a system with dynamic and context-aware choices for security? Will it make them feel that their data and/or their identities are safe? Will the users feel that the system is trustworthy if it were able to prove itself (mutual authentication)? If so, how would the users want the system/server to prove itself?

[U4] How frequently would users like to be notified (and required to perform further action) when a context change is observed and a re-authentication is necessary? Can the system automatically "infer" the users' validity through user interactions and other actions? Would such automatic inference lead to the system appearing more trustworthy or as prying?

[U5] In a single system/application, what is the number of different types of actions a user is willing to perform for authentication? Examples of actions include: drawing patterns, entering PIN/passwords, recording their face/fingerprint, etc.

II. From an administrator's perspective:

[A1] Do administrators believe that such a system is trustworthy to protect the organization's data, and keep their users safe?

[A2] Does this system pose infrastructure and maintenance expectations, in addition to what is already being used?

[A3] Is the contextual data being logged by the system sufficient to provide administrators enough information about potential unauthorized access attempts?

[A4] Would automating a part or the complete process of unauthorized access risk identification/mitigation be useful to administrators? Would the system inferred "insight" augment what the administrators already know?

4. REFERENCES

[1] Bhatti, R., Bertino, E., & Ghafoor, A. (2005). "A Trust-Based Context-Aware Access Control Model for Web-Services," *Distrib. and Parallel Dat.*, 18(1), 83-105.

[2] Federal Financial Institutions Examination Council. (2008). "Authentication in an Internet Banking Environment," http://www.ffiec.gov/pdf/authentication_guidance.pdf.

[3] Forget, A., Chiasson, S., & Biddle, R. Choose Your Own Authentication. In Proceedings of *2015 New Security Paradigms Workshop (NSPW)*, pages 1 – 15, 2015.

[4] Gellersen, H. -W (Ed.). (2001). "Towards a Better Understanding of Context and Context-Awareness," *Handheld and Ubiquitous Computing LNCS 1707*, 304-307.

[5] Lenzini, G., & Hulsebosch, B. (2007). "Context-Based Adaptive and Responsive Authentication," *In European Research Consortium for Informatics and Mathematics (ERCIM) News*, No. 71, 34-35, http://ercim-news.ercim.eu/images/stories/EN71/EN71-web.pdf

[6] Sampangi, R. V., & Hawkey, K. Secure Contexts: Context-Dependent, Dynamic, and Adaptive Security and Privacy. Poster presented at *Symposium on Usable Privacy and Security (SOUPS)*, 2016.