SafeNet

Time versus Event Based One-Time Passwords

Andrew Y. Lindell

SafeNet

Contents

Abstract

In this document we compare the two main approaches to one-time passwords (OTP): time-based OTP and event-based OTP. Our main conclusion is that they are very similar from both a security and usability perspective (with each having slight advantages of a different nature).

Introduction

It is a well known fact that plain password-based authentication is highly problematic. Beyond the fact that many users are not aware of the adversarial threats that exist and therefore engage in insecure behavior, it is often impossible for a user to remember all of her passwords. Users often have to handle ten or more passwords to various applications, and it is not feasible for most human beings to remember even five long random passwords. Thus, even if users are well educated as to the risks, the plain password solution just doesn't work. In addition to frustrating users, security is often compromised.

A number of different authentication mechanisms are used today in order to alleviate this problem. One-time-password authentication (or OTP) is just one of these mechanisms.[1] In this method, login is performed using a different, essentially random password each time. The passwords are generated by a device, most commonly a hardware token associated with the user, and so the password is not based on the user's memory. This greatly increases security. Furthermore, by adding a personal secret PIN or password that the user needs to provide in order to authenticate, strong two-factor authentication is achieved.

There are two main approaches to OTP. In the first approach, called time-based OTP, the one-time password changes at frequent intervals (say, every two minutes). In the second approach, called event-based OTP, the one-time password is generated by pressing a button on the OTP device.[2] The cryptographic mechanism underlying both approaches is the same. Each one-time password is generated by applying a random-looking cryptographic function to a unique series value. In the time-based case, the value is the current time. In the event-based case, the value is a sequence number that is incremented with each button click. We stress that each device is initialized with a secret key that makes prediction of the one-time passwords infeasible to an outside attacker. We also stress that the current time and sequence numbers are not secret and the security rests on the inability to predict the output of the cryptographic function on the current number due to the secret key.

[1] In this paper we assume that the reader is familiar with the basic OTP mechanisms and with the concepts of authentication and two-factor authentication.

[2] A third approach, called *challenge-response-based* OTP, is not addressed here.

A Security Comparison

As we have mentioned, the underlying mechanism is the same for both time-based and event-based OTP. Of course, the security of the scheme depends heavily on the quality of the cryptographic algorithm that is chosen to generate the one-time password values. In order to achieve the effect of a fresh random password each time, the algorithm should be a pseudorandom function (meaning that to anyone not knowing the secret key, the output looks just like a random string). Examples of the algorithms used are AES and HMAC-SHA1, which both have very strong pseudorandom properties. We remark that both of these algorithms are industry standards and constitute excellent choices.

Given that the underlying cryptography is essentially the same in both approaches, we consider secondary issues that can have some security ramifications. These issues have to do with how the hardware devices typically work for these approaches.

An important observation regarding event-based OTP is that the OTP value does not automatically expire after a given amount of time (say, two minutes). This implies that if a one-time password is somehow maliciously obtained by an attacker, it can be used later to break into the user's account. Note, however, that the stolen OTP value is only valid until the legitimate user next carries out an authentication procedure. This is due to the fact that once the legitimate user authenticates, the current sequence number is updated to the one on the device, making all previous sequence numbers (and their associated OTP values) invalid. In addition to the above, unnoticed physical access to the OTP device is required for carrying out this attack. We remark that if an attacker does obtain physical access to the device, then she can actually extract multiple OTP values by pressing the button a number of times. However, there is not much difference between this and obtaining a single one-time password and remaining logged on (some sophistication is needed to ensure that the session opened using the single stolen password will not be closed, but this is possible).

In time-based OTP, each OTP value is only valid for a short amount of time. Furthermore, only a single one-time password appears on the screen at any one time and so it is not possible to obtain future OTP values. Thus, the aforementioned attack on event-based OTP is not applicable here. Nevertheless, time-based OTP has its own threats. For example, in most time-based OTP devices, the one-time password appears continually on the device and can be viewed by someone who "innocently" passes by. This same bystander can then run to another machine and use that one-time password in order to logon. (More realistically, she can call an accomplice on her cell phone who then logs on immediately before the password expires.)

We view the above attacks as incomparable. On the one hand, in event-based OTP there is no need to use the password immediately, as in the case for time-based OTP. On the other hand, in event-based OTP undetected physical access to the device is required, whereas in time-based OTP it can be much easier to obtain a valid one-time password. In either case, the danger posed by these attacks is not as significant as it may seem. This is due to the fact that OTP systems typically rely on two-factor authentication and so the user has a short 4-digit PIN (or longer password) that is also needed. Thus, obtaining the one-time password value is not enough. Notice that the window of opportunity for an attacker is limited in both cases. In addition, OTP systems typically lock the user after a number of unsuccessful logon attempts. Therefore, extensive password guessing attacks are not possible.

A Usability Comparison

As with security, each approach has a different disadvantage with respect to usability. In event-based OTP the user must press a button, whereas in time-based OTP the password can just be read off the screen. In time-based OTP, however, there is a problem that arises when the one-time password changes exactly when it is being entered. Since the passwords change frequently (for example, every two minutes), this happens quite often and can be disruptive to the user. We view the usability of event-based OTP as preferable to time-based OTP. However, once again, we stress that in both cases any annoyances incurred are far outweighed by the advantages.

Conclusion

We conclude that both OTP approaches greatly enhance security beyond password-based authentication. From both a security and usability perspective, time-based and event-based OTP mechanisms have distinct relative advantages and ultimately we regard them as being equally effective. In both cases, we emphasize the importance of user behavior in the security of the solution. We recommend that organizations implementing OTP authentication educate their users to keep their personal device passwords (or PINs) secret, and to keep their device physically secure. This will ensure a high level of security, whichever OTP approach is used.

Summary Comparison of Time-Based vs. Event-Based OTP

	Security	Convenience
Time-based OTP	Pro: OTP values are valid for a short period of time Con: OTP values can be obtained easily by a by-stander	Pro: The OTP value can be simply read off the screen Con: The OTP value may change while it is being entered
Event-based OTP	Pro: An attacker would need undetected physical access to the device Con: An OTP value is valid until a new OTP value is used	Pro: The OTP value is generated at the user's request; no value change after a short amount of time Con: The user must press a button to generate the OTP value

Short biography of the author

Andrew Lindell is a cryptography expert and an Assistant Professor at Bar-Ilan University in Israel. Andrew attained a Ph.D. at the Weizmann Institute of Science in 2002 and spent two years at the IBM T.J.Watson research lab as a Postdoctoral fellow in the cryptography research group. Andrew has carried out extensive research in cryptography, and has published more than 40 conference and journal publications, as well as a book detailing secure protocols. Andrew has presented at numerous international conferences, workshops and university seminars, and has served on program committees for top international conferences in cryptography. In addition to Andrew's notable academic experience, he joined Aladdin Knowledge Systems in 2004. In his position as Chief Cryptographer, he has worked on the cryptographic and security issues that arise in the design and construction of authentication schemes, smartcard applications, software protection schemes and more. Offering a unique combination of academic and industry experience, Andrew brings a fresh and insightful perspective on many of the crucial security issues that arise today.

To find out more about SafeNet authentication solutions go to:
http://www.safenet-inc.com/authentication