

Technology Exploration Project – M591

Secure Passwords? Patented One-Time Password Technologies and their Effect on Privacy

In information technology passwords are widely used to authenticate users. But password authentication in its basic form has many weaknesses. Therefore attemps exist to increase the security of password based authentication. A commen approach is the usage of one-time passwords. RSA SecureID and Grid Data Security's GridOne are such one-time password systems which are both based on patented technologies. GridOne is a fairly new product and still under development, SecureID is already established on the market and is widely used. While increasing the security of password authentication, how does this additional security affect the privacy of the user data?

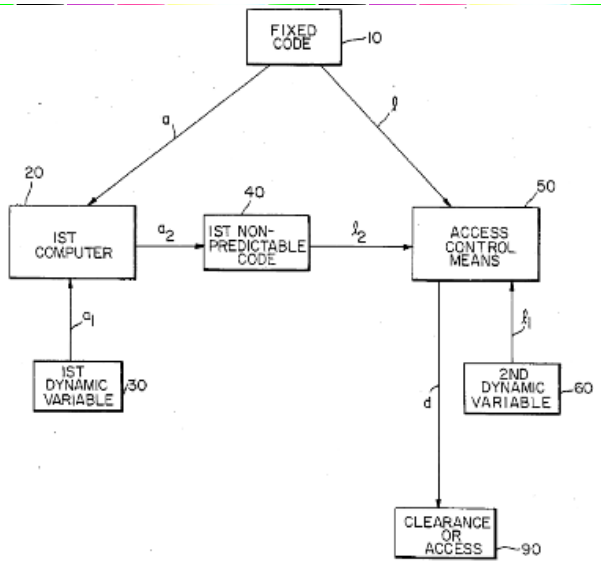
Introduction

Although the authentication with username and password is not very secure, it is still widely used and popular, because of its simplicity in implementing and using it. It is usually a one factor authentication using the method of "something you know". The problem is that users tend to choose passwords which are easy to remember and are therefore easy to guess. There are several attempts to enhance the security of password based authentication systems, e.g. introducing policies about the password's structure, like a minimum length, mandatory usage of numbers and special characters, expiry dates etc. These policies lead to "better" passwords which are usually not easy to remember and are therefore often written down by the users. Another weakness of conventional passwords is that they are static and therefore susceptible to eavesdropping. One-time passwords (OTPs) are another approach to make passwords more secure. As the name says, these passwords are only valid for a single authentication process. OTPs mainly focus on eliminating the effects of passive attacks like eavesdropping through wire-tapping or keyloggers. Although an attacker can get hold of the users password by eavsdropping, it is useless because it is invalid after its first usage.
The differences between one-time password systems usually lie in the generation process of an OTP. Leslie Lamport, for example, introduced in his article "Password Authentication with insecure Communication" a way of generating OPTs by applying a hash function multiple times on a secret only known to the user (Lamport, 1981). This method led to the open source systems S/Key and OPIE (Jonkmann, 2007).
The two methods discussed below use shared secrets as part of the OTP generation process. In SecurID this secret is a predefined and hardcoded 128-bit key stored in a hardware token (or its software implementation). GridOne is based on a user defined secret which will be converted to an OTP by a simple substitution and does not need additional hardware or software.

Technology and Patents for each System

SecurID

In 1984 Kenneth P. Weiss filed a patent application describing the basics of the SecurID system. The patent was granted in 1988 by the United States Patent Office as well as two more related patents in 1989 (RSA, n.d. a, Weiss, 1988 1989a 1989b) Because these patents were filed in 1984 and 1985, they are already expired and now free to use. The patents describe a way of generating a non-predictable code based on a fixed code and a dynamic variable. This should be done seperately on a handheld device and at the authenticating host. The non-predictable codes of both systems are then compared and if they match, access is granted.

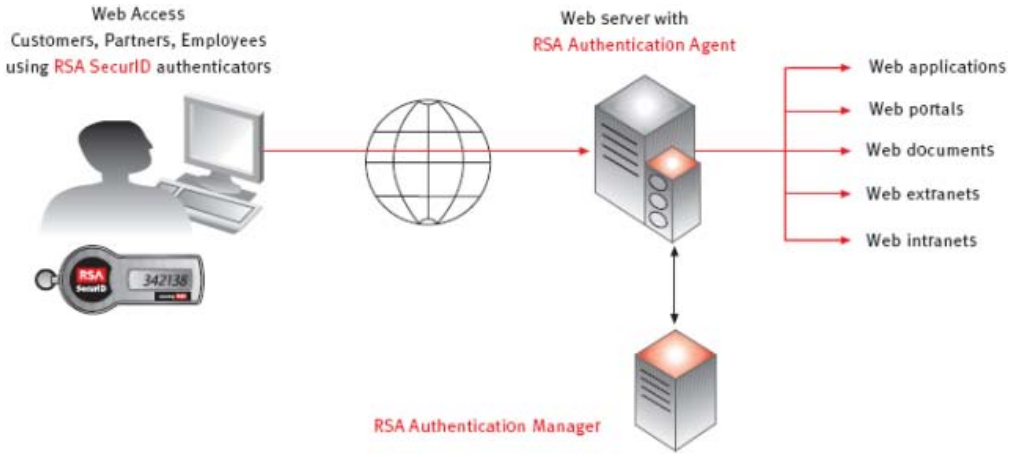


The patent describes the handheld device named SecurID as a token which contains a microcontroller, a display and an algorithm for the generation of a non-predictable code. All the informatin contained in this token should be stored in volatile memory in a tamper-proof manner so that the secrets can not be extracted. It also suggests the use of an algorithm not known to the user.

Until 2003 this was indeed the case with SecurID. The hashing algorithm used in the tokens was proprietary and only available to certain companies under a non-disclosure agreement. Nowadays SecurID uses AES to generate the non-predictable code.

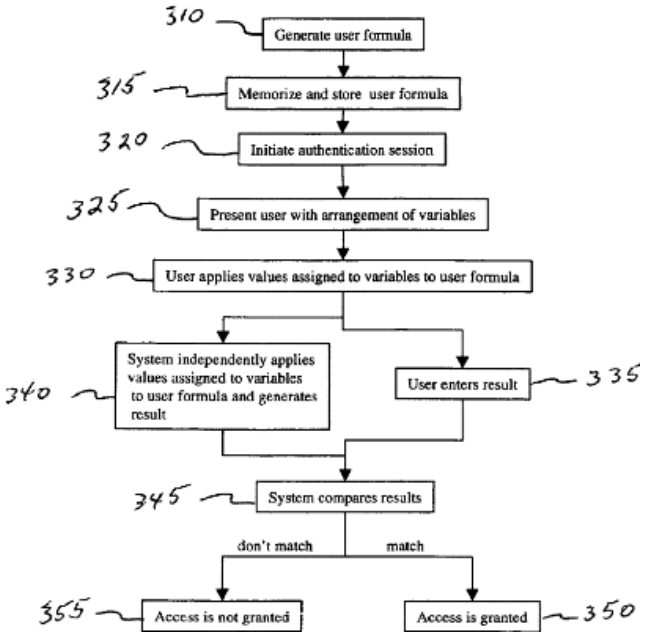
The dynamic variable used in this implementation is the time. The SecurID token generate every one minute (or 30 seconds) a new number which is based on a predefined 128-bit key and the current time. The token and the authenticating host has to be synchronized for the system to work. One of the related patents mentioned above addresses this problem which will not be discussed further in this article (Weiss, 1989b). SecurID uses two factor authentication. When asked the user has to enter the PASSCODE which consists of the non-predictable number generated by the token concatenated to the users PIN. The application the user wants to authenticate to forwards the PASSCODE to the RSA Authentication Manager where the PIN and the secret key for this user/token are stored. This server does the same calculation and compares the results, as it can be seen in the figure below. Therefore "something you have" is needed (the token) as well as "something you know" (the PIN).

If an attacker gets hold of the PIN, it is still almost impossible to guess the non-predictable number. For example if a delay of 3 seconds after a false login, it leaves the attacker up to 20 guesses for the 6 digit number, which leads to a probability of 1/50000. With 8 digits, the probability is 1/5000000. The probability can be reduced further by increasing the delay. The minimum probability is 10^{-n}, with *n* representing the number of digits. But first, the attacker has to get hold of the PIN.

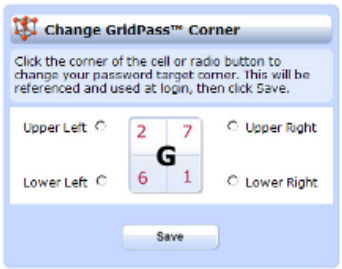


GridOne

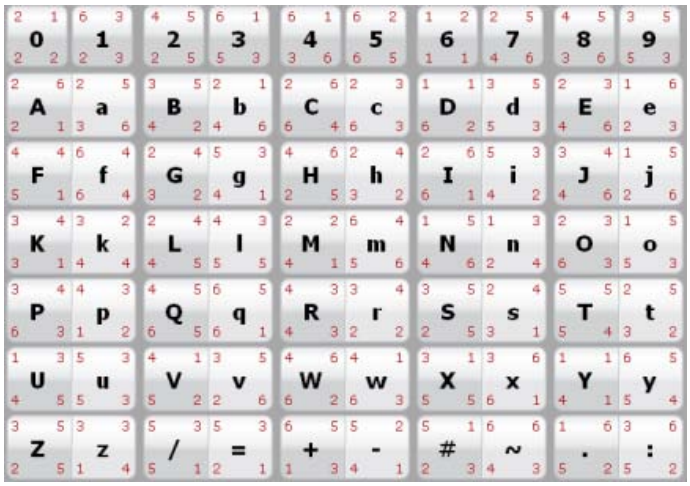
As mentioned above the technology used by GridOne is fairly new and was only patented a year ago under the United States Patent no 7143440 (Ginzburg, 2006). It describes the generation of an OTP by converting the normal password into a number with the help of a user defined formula. On initialization the user has to set up a formula for calculating the OTP (e.g. `(A+B)`). When the user tries to login, he is presented with a set of characters with a value assigned to each character. Now the user puts the assigned values into the formula and calculates his OTP. (e.g. `A=32, B=13 => OTP=45`).



The product GridOne is a web-based authentication system and uses a varied version of this technology. It does not yet allow the user to choose the formula. At the moment the formula used is a simple substitution of the single password characters by another value. Instead of only assigning one value to each character, four values used. On initialization the user has to choose a password and one of the four corners as shown in the figure below.



Each time the user wants to log in he is presented with a list of the allowed password characters. To each character four values are assigned. To authenticate himself the user has to enter his username and the converted password (e.g. `password -> 13336525` *using the lower left corner*)



Because the values assigned to the characters are different each time, an OTP is generated. The values used for the replacement can be chosen freely by the administrator. While SecurID has a time limit for each password, GridOne offers the possibility to limit the number of possible guesses to overcome the threat of

brute force and wordlist attacks.

There is always a tradeoff to be made between the number of possible OTPs and the possibility of getting the password by simply a limited number of authentication processes, as it is shown in a security analysis provided by Grid Data Security. The following table shows the probabilities of guessing the password or an OTP (GridCode) for an 8 digit password with 70 possible characters which are substituted by the numbers 0-9. having 3 guesses. (Speirs, n.d.)

Table 1: A summary of the probabilities for the different attack scenarios between a standard password authentication scheme and the Grid Data Security authentication scheme with and without DecoyDigits™.

Attack Scenario	Standard Password	Grid w/o Decoys	Grid with Decoys
Guess of the Password	$\frac{1}{192,160,033,333,334}$	$\frac{1}{768,640,133,333,334}$	$\frac{1}{768,640,133,333,334}$
Guess of a GridCode™	$\frac{1}{192,160,033,333,334}$	$\frac{1}{100,000,000}$	$\frac{1}{2,222,222}$
Observing an Auth.	$\frac{1}{1}$	$\frac{1}{10,821,830}$	$\frac{1}{598,084,451}$

.

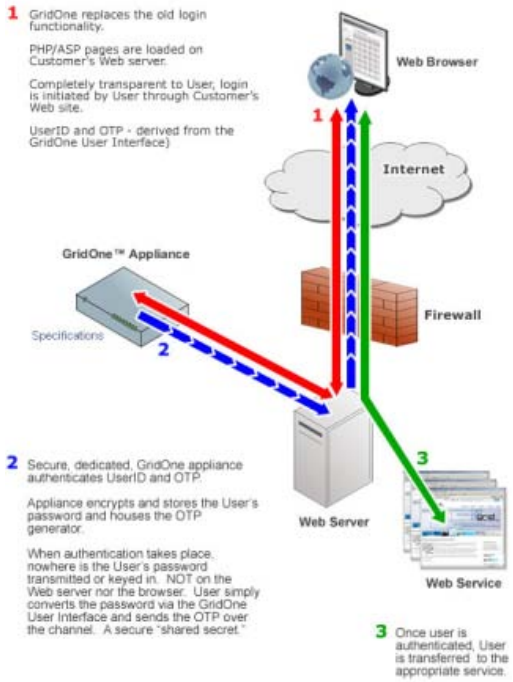
One optional enhancement (user formula) is used in this example, called DecoyDigits. These decoys can be added by the user to disguise the actual password length and to make it harder to extract the password after several observations of the authentication process. In this case, 1 DecoyDigit is allowed per 3 password digits. This means the user can add 0 - 2 additional digits somewhere between the substituted characters of his password.

As the numbers show, GridOne makes guessing of the password a bit easier, because less characters are used than in the original password (row 2), but it makes it almost impossible to get the password by simple eavesdropping, compared to the static password.

Compared to the probabilities calculated for SecurID in case the PIN is known, these numbers seem to be better. But only because of the chosen number of allowed guesses. SecurID does not need the method of locking an account after a certain amount of false guesses. This method reduces the usability and the effort for maintainance.

According to Paul Sitar there are other possible user formulas, like adding two corners together, adding an offset to the assigned values and so on. Basically anything a user or a company wants it to be and is feasible (Sitar, 2007). How these formulas affect the security has to be further evaluated.

While GridOne is web based, Grid Data Security has other products under development which will address other situation where authentication is needed like GridLock (desktop login), GridCert (certified mail), GridPro (enterprise wide user management) etc. For more details see the companies product page.



While very different on the user side and in generating the OTP, both systems use a centralized approach to authenticate the users. SecurID uses the RSA Authentication Manager to manage and authenticate the users and GridOne uses a GridOne appliance for the same purpose as shown in the figures above. With this centralized authentication both systems are able to communicate with different applications and to manage the authentication process for these application. Both systems are scalable which is a major issue for companies.

Effects on Privacy

One-time password systems in general enhance the security of password authentication. Therefore they have a good effect on the protection of the users data. Nevertheless, one-time passwords address only the weaknesses of the password system. Therefore they need to be used in combination with other technologies for securing communication channels and providing data integrity. RSA and its partners provide a range of solutions where SecurID is combined with those other

technologies. Grid Data Security has not been long on the market. Hence, no such a variety for their technology exists. This might be overcome in the future by introducing new products and setting up partnerships with other companies, like they have already done with Citrix.

But what data does the user have to provide in order to use one of these systems? On their website Grid Data Security emphasises that there is "no need to divulge information that once compromised can not be replaced", that there is "no need to offer personal biometric traits" and that users are "relieved of privacy concerns and fears" (Grid, 2007). Theses statements are also valid for SecurID, while SecurID is more concerned about the security of the data of the companies than of the individual users.

On first glance, GridOne looks like the user has only to provide as much information as the issuer of the identifier (e.g. owner of the webpage) wants to have on registration. In the best case no additional information apart from a username and password are needed, but usually webservice require nowadays at least a valid email address.

As said above, GirdOne tries to overcome the threat of guessing a password or the corresponding OTP by limiting the amount of false logins to a certain number k. Although, according to Paul Sitar, the implementation of this method is subject to the business rules of the company using this system (Sitar, 2007), there must be a similar method otherwise the system would become vulnerable to brute force and dictionary attacks. In case an account is locked due to k false logins, there must be a way of unlocking the account, which leads to the need of some additional information about the user. Hence, the authentication process itself needs as many private information as it does in other password systems and has no specific improvements.

Many webservices like email show only the last time the user tried to log in to the service (successfully or unsuccessfully). One approach of Grid Data Security of making the information gathered more transparent, is a login history. There the user can see the exact time and date of the last logins as well as the IP-Addresses. This can help the user to detect malicious behaviour.

Recent Account Activity

Status	Date - Time	IP Address
Logged In	7/20/2007 3:49:40 PM	10.1.1.22
GridPass Changed	7/20/2007 3:48:02 PM	10.1.1.22
Logged In	7/20/2007 3:47:44 PM	10.1.1.22
Logged In	7/20/2007 2:53:32 PM	10.1.1.22
Logged In	7/20/2007 1:23:06 PM	10.1.1.22
Logged In	7/20/2007 1:21:47 PM	10.1.1.22
Logged In	7/19/2007 1:57:34 PM	10.1.1.22
Logged In	7/19/2007 1:55:52 PM	10.1.1.22
Logged In	7/19/2007 8:58:23 AM	64.252.160.145
Logged In	7/19/2007 8:56:56 AM	64.252.160.145
Logged In	7/19/2007 8:36:24 AM	64.252.160.145
Login Failed	7/19/2007 8:35:44 AM	64.252.160.145
Logged In	7/19/2007 8:33:30 AM	64.252.160.145
Logged In	7/17/2007 3:23:51 PM	10.1.1.22

Because RSA SecurID is not cheap, it is usually only used by companies, their employees and customers. The employees and customers are already "registered" with the company, therefore no additional information is needed. For example, banks issues SecurID tokens to its customers for securing online banking. In this case as well, no addition information is needed for the already registered customer who was using online banking before (e.g. with PIN/TAN).

Marketing and Selling Strategies

The benefit of making a new idea or invention public through patents is the protection of this idea. By issuing a patent for a certain idea, the governments grants the inventor a monopoly over this idea for a limited period of time (US: 20 years from the date of application).

Companies often use patents in their marketing strategies. A patent is something official and gives the product some credibility. It also gives the impression that the solution a company offers can only be offered by them, because it is protected by a patent.

RSA does not use its patents on SecurID in its current marketing strategy but that is probably due to the fact that the patents are expired and that they do not need to anymore. The product SecurID is widely known and RSA Security has a very good reputation for its security solutions. It can be assumed that RSA used the patents on SecurID to protect its ideas and to establish its good position on the market for security applications. Through its partnerships the SecurID authentication solution is available for more than 350 non RSA products from other leading security companies (RSA, n.d. b). Through this partnership alone RSA reaches a much broader range of customers than through conventional marketing strategies like advertising in magazines and talking directly to potential customers, which is done as well.

Because Grid Data Security is a young company which products are all based on the patented technology, the patent will probably play a major part in their marketing strategy as it can be seen on their homepage griddatasecurity.com Almost every page of their website has at least a comment about the patent as well as each document received from Grid Data Security has. The Grid technology is not commercially available yet. According to Paul Sitar, Grid Data Security first wants to evaluate the strength and weaknesses of their technology in order to improve it before putting it on the market. Therefore it is still in its development phase and projects with different companies in piloting stage exist (Sitar, 2007). This piloting stage can also be seen as a kind of "getting a name" before actually going on the market. As stated on the website, other products apart from the webbased GridOne are under development to address the needs of future customers.

Conclusion

Both technologies improve the privacy of the data by improving the security of the authentication processes implemented to restrict access to these data. They both overcome the main weaknesses of password based security which are eavesdropping and weak, easy to guess passwords (hence susceptible to brute force and dictionary attacks). The systems themself do not provide any data integrity or security and are meant to be part of a bigger security solution, where other parts will address these issues. Because of its age and the reputation of RSA, there are many application and devices available supporting the SecurID authentication solution. The public has also been able to analyse the system in depth to find out it strengths and weaknesses. If there were significant weaknesses, not so many other security products would support the technology.

The advantage of the new Grid technology on the other side, are lower costs and the possibility to replace an existing password authentication without the need of having all users change their passwords or even registering again. Because no extra software or device is needed on the client side and its scalability on the server side, the costs to implement and maintain the system will probably be significantly lower than with the SecurID System. If the piloting stage is successful and future, independent security analysis verify the strength of the system and the companies claims about it, the Grid technology might become a cheap alternative to token based systems like SecurID.

While adding more protection to the data from attacks from the outside, both systems do not provide the user with much more control (if any) about the data used for registration and authentication and the data recorded during each authentication process. GridOne introduces some trancparency about the some data recorded with its activity record, but the user still has no control about it.

The patents protecting these technologies do not affect the privacy directly. The openess provided through the patents helps to analyse the technologies regarding their strength and weaknesses and therefore to make it easier to find possible threats on privacy.

References

- Ginzburg, Lev (2006). *US Patent 7143440 B2*. [Electronic version] http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=7143440.PN.&OS=PN/7143440&RS=PN/7143440
- Grid Data Security (2007). Companies website. Retrieved Nov 25 from http://www.syferlock.com
- Jonkmann, Ralf (2007). *Keeping Passwords Secret*. Retrieved from http://mosaic.cnfolio.com/M591CW2007B102
- Lamport, Leslie (1981). Password Authentication with Insecure Communication [Electronic version]. *Communications of the ACM 24.11* November 1981, 770-772
- RSA (n.d. a). *RSA SecurID Patents*. Retrieved Nov 20, 2007 from http://www.rsa.com/node.aspx?id=2777
- RSA (n.d. b). *RSA Secured Partner Solutions Directory*. Retrieved Nov 26, 2007 from http://www.rsa.com/rsasecured
- Sitar, Paul (2007). Personal communication with Paul Sitar, CEO of Grid Data Security. Nov 26, 2007
- Speirs, William R. II (n.d.). *Grid Data Security Authentication System and Methodology - A Security Analysis*. not published
- Weiss, Kenneth P. (1988). *US Patent No. 4720860*. [Electronic version] http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=4,720,860.PN.&OS=PN/4,720,860&RS=PN/4,720,860
- Weiss, Kenneth P. (1989a). *US Patent No. 4856062*. [Electronic version] http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=4,856,062.PN.&OS=PN/4,856,062&RS=PN/4,856,062
- Weiss, Kenneth P. (1989b). *US Patent No. 4885778*. [Electronic version] http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=4,885,778.PN.&OS=PN/4,885,778&RS=PN/4,885,778
