Contacts

Edit Rubóczki PhD Student
Óbuda University - Doctoral School on Safety and Security Sciences
Budapest - Hungary

References

[1] *David Kolb – The Learning Cycle, available: 26 November 2016* *http://www.businessballs.com/kolblearningstyles.htm*

[2] *Péter Tóth - The Role of Individual Differences in Learning, Acta Polytechnica Hungarica, Vol. 11, No. 4, 2014, pp. 184-197,* *https://uni-obuda.hu/journal/Toth_50.pdf* *, available: 26 November 2016*

[3] *Racskó Réka - Alternatívák az elektronikus tanulási környezetek kialakítására, Tudományos és Műszaki Tájékoztatás, Könyvtár- és információtudományi szakfolyóirat, 59. évfolyam (2012) 2. Szám* *http://tmt.omikk.bme.hu/print.html?id=5588&issue_id=534* *; available: 26 November 2016*

[4] *Rubóczki Edit - How to develop cloud security awareness Applied Computational Intelligence and Informatics (SACI), 2015 IEEE 10th Jubilee International Symposium on pp. 323-326, 2015.*

[5] *E-Learning,* *https://en.wikipedia.org/wiki/Educational_technology*; *available: 26 November 2016*

[6] *Webinars:* *https://en.wikipedia.org/wiki/Web_conferencing*; *available: 26 November 2016* *http://www.oktatas-informatika.hu/2011/12/papp-danka-adrienn-az-online-tanulasi-kornyezet-fogalmanak-ertelmezesi-lehetosegei/* *Malcolm Gladwel: Outliars Carnegie Hall Melon University*

[7] *Jane McGonigal – TED Speaking, 2010. május 17, elérhető: 2016. november 26.* *https://www.ted.com/talks/jane_mcgonigal_gaming_can_make_a_better_world?language=hu#t-1100901*

[8] *Daphne Bavelier – TED Speaking, 2012. november 19, elérhető: 2016. november 26.* *https://www.youtube.com/watch?v=FktsFcooIG8*

[9] *Rubóczki Edit - Serious Games Experience in Teaching Cloud Security; ICERI 2016., ISBN: 978-84-617-5895-1*

[10] *Gyula Mester, Distance Learning in Robotics, Proceedings of The Third International Conference on Informatics, Educational Technology and New Media in Education, pp. 239-245, ISBN 86-83097-51-X, Sombor, Serbia and Montenegro, 01-02.04.2006.*

TOKENIZATION AS AN EFFECTIVE TOOL FOR SECURE PAYMENTS

Peter Schmidt

Summary

Tokenization in practice means that during the contactless payments, these payments do not carry credit card information, but only the security token created especially for a particular device, merchant and purpose of payment. Thanks to the tokenization service access to other electronic devices will be simplified in the near future. Besides "wearables", i.e. devices worn on body, these devices can be automobiles, televisions, game consoles, refrigerators and washing machines. Tokenization allows easy connection with a digital credit card payment service, and at the same time it ensures sufficient credit data when paying on the Internet or in a shop.

Key words

Authentication, Multifactor authentication, Token, Tokenization

Introduction

Although people rarely pay by phones in shops, it does not mean that after years of focusing at this topic banks had forgotten mobiles. On the contrary, payment companies, financial start-ups and banks are looking for solutions to convince people to exchange cards - which can be stolen, copied and misused – with a phone that can be safer and in addition offers a variety of additional functions. Last but not least is the probability that you forget phone at home, is lower than forgetting to put card in the wallet. The basis of each payment is the authentication process to verify and establish the identity of the person with the required degree of assurance, that the person making any claim about his identity is really the person for which they are issued.

Authentication

Validation is a process consisting of several stages. In general, the user must subscribe to a particular service and then prove its eligibility. Demonstration of eligibility is performed in one of the following three ways:

1. demonstrate knowledge (password, PIN)
2. proof of ownership (hardware token)
3. demonstration of biometric features (fingerprint, voice, retina)

At the present, the absolute majority of people use one-factor authentication. This means that the user proves his identity by one of three types of evidence - evidence of knowledge, proof of ownership, proof of a personal characteristic. Most often it is a password that is linked to the identifier such as a user name or login ID. At present, however, should be oriented more authentication parameter, which is a solution based on a combination of two or three authentication parameters.

Multifactor authentication

Multi-Factor Authentication (MFA) is a security mechanism in which individuals are authenticated through more than one required security and validation procedure. MFA is built from a combination of physical, logical and biometric validation techniques used to secure a facility, product or service. MFA is implemented in an environment where an individual's authentication and validation is the highest priority. To gain access to a secured location or system, MFA typically requires three different security mechanism layers and formats, as follows: Physical security: Validates and authenticates a user based on an employee card or other type of physical token; Logical/knowledge base security: Validates and authenticates a user based on a required password or personal identification number (PIN), which is memorized by the user; Biometric security: Validates and authenticates based on a user's fingerprints, retinal scan and/or voice. Frequently used authentification method - Two-factor authentication (2FA) - is a method of confirming a user's claimed identity by utilizing a combination of two different components.

Multifactor Authentication (MFA) software tool that adds additional security measures (via smartphones and biometrics) to standard user name/password logins for a number of services and servers. By doing so, it prevents unauthorized logins, even when passwords have been compromised and were shared among many different services.

Many of number of MFA products are especially suitable for those organizations that want to make use of a variety of external software as a service (SaaS) products, such as Google Docs, Salesforce.com and Outlook Web App.

Multifactor authentication products can provide significant benefits to an enterprise, but the technology is complex and the tools themselves can vary greatly from vendor to vendor. A feature on MFA is looked at three primary use cases for MFA, which are:

1. Augmenting Active Directory or similar user logins to local network resources such as file servers or VPNs/remote access controllers.
2. Providing strong identity verification to third-party Web services, such as Salesforce.com or Google Docs, using the Security Assertion Markup Language (SAML) standards,
3. Augmenting Web server logins directly, such as a website or web-enabled applications such as Outlook Web App or Microsoft SharePoint.

Most vendors provides a solid MFA tools that have been around for years and can handle a wide variety of situations, token types and applications; and all come in both cloud and on-premises versions.

Tokens

In general, a token is an object that represents something else, such as another object (either physical or virtual), or an abstract concept as, for example, a gift is sometimes referred to as a token of the giver's esteem for the recipient. In computers, there are a number of types of tokens.

1, In a token ring network, the presence of a token (which is simply a particular bit setting) in a continually circulating transmission stream allows a device to change the bit setting (thus taking the token) and put a message in its place. The receiver of the message elsewhere in the token ring network removes the message and resets the bit setting (this putting the token back) so that someone else in the ring of devices will be able to have a turn at using that message space.

2, A programming token is the basic component of source code. Characters are categorized as one of five classes of tokens that describe their functions (constants, identifiers, operators, reserved words, and separators) in accordance with the rules of the programming language.

3, A security token (sometimes called an authentication token) is a physical device, that the owner carries to authorize access to a network service. The device may be in the form of a smart card or may be embedded in a commonly used object such as a key fob. Security tokens provide an extra level of assurance through a method known as two-factor authentication: the user has a personal identification number (PIN), which authorizes them as the owner of that particular device; the device then displays a number which uniquely identifies the user to the service, allowing him to log in. The identification number for each user is changed frequently, usually every five minutes or so. Unlike a password, a security token is a physical object. A key fob, for example, is practical and easy to carry, and thus, easy for the user to protect. Even if the key fob falls into the wrong hands, however, it cannott be used to gain access because the PIN (which only the rightful user knows) is also needed.

One-time password tokens

The recent phishing attack on Citibank's one-time password (OTP) authentication has questioned the viability of OTP tokens as a secure method for two-factor authentication. That concern is even greater among banks who had pinned their hopes on using tokens to meet the Federal Financial Institutions Examination Council (FFIEC) recommendation that they implement two-factor authentication to protect their Internet banking Web sites from malicious access. One-time password tokens can still be effective for two-factor authentication depending on how and where they're implemented.

OTP tokens generate new PIN numbers every 30 to 60 seconds and can be used in addition to static user IDs and passwords to log on to a Web site. The idea is that if the static credentials are stolen, say, in a phishing attack, the malicious user would still have to guess the PIN to gain access. But since the time window is short to guess the PIN, it would be nearly impossible to break in.

Information security professionals have known for a while that OTP tokens are susceptible to man-in-the-middle (MITM) attacks. However, as scary as a real-time phishing attack may be, it requires that the hacker be at his keyboard at the right moment and act very quickly (like in 30 seconds) to gain access to the victim's online bank account. So unless it can be automated, it doesn't make a lot of sense for the serious criminal. Remember, phishing attacks are committed by organized criminal groups interested in making a fast buck. This means constant monitoring of the victim online. Traditional phishing sites can harvest more prey, more efficiently, and make more money through passively harvesting credentials than the occasional one-off real-time attack, which depends mostly on luck. Of course, with the right combination of automated scripts and botnets, this could all change.

There are two strategies for successfully and securely implementing OTP tokens: architecture of the token implementation and physical security of the tokens themselves.

In terms of architecture, the first consideration is placement of the token in your system. The most secure use of OTP tokens is for logging in to workstations locally or for accessing an internal network behind a firewall. In an internal network, unlike the open Internet, where all servers are not monitored an MITM attack is not as likely. Therefore, a good approach for Web sites is to use Secure Sockets Layer (SSL) for the login page, where the OTP value is entered only for the following transaction pages. This encrypts all credentials – both the user ID and password, and the OTP's PIN – from the beginning. Login pages of some Web sites that use plain HTTP may pass credentials openly unencrypted over the Internet, where they can be sniffed. Unfortunately, SSL cannot stop a man-in-the-middle attack. SSL with mutual authentication enabled can provide some protection since both the server and client exchange certificates, preventing the type of server spoofing needed for MITM attacks. Is important design website with the latest version of SSL that has mutual authentication.

Tokenization

What is tokenization? Tokens itself means nothing. It is a unique cluster of characters, often disposable, which is the system processor card payments linked to the client. Dealer for payment by phone gets available only token through which implements payment card information never seen before. The token is not a cipher, one can not even break and can not be traced back to him from the card details. That is because credit card's data do not enter into the token making process. Sensitive card data remains in the strong security system of the bank or card company. In the case that the trader is hacked, attackers receive only useless tokens.

Tokenization, when applied to data security, is the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token, that has no extrinsic or exploitable meaning or value. The token is a reference (i.e. identifier) that maps back to the sensitive data through a tokenization system. The mapping from original data to a token uses methods which render tokens infeasible to reverse in the absence of the tokenization system, for example using tokens created from random numbers. The tokenization system must be secured and validated using security best practices applicable to sensitive data protection, secure storage, audit, authentication and authorization. The tokenization system provides data processing applications with the authority and interfaces to request tokens, or detokenize back to sensitive data. When tokens replace live data in systems, the result is minimized exposure of sensitive data to those applications, stores, people and processes, reducing risk of compromise or accidental exposure and unauthorized access to sensitive data. Applications can operate using tokens instead of live data, with the exception of a small number of trusted applications explicitly permitted to detokenize when strictly necessary for an approved business purpose. Tokenization systems may be operated in-house within a secure isolated segment of the data center, or as a service from a secure service provider. Tokenization may be used to safeguard sensitive data involving, for example, bank accounts, financial statements, medical records, criminal records, etc.

However, the client does not know anything about what is tokenization and how it works. He just knows that it is a secure system. The fear of abuse is still a major obstacle to the use of mobile payments. However, the advantages outweigh the drawbacks and shopping in e-shops through mobile devices are significantly growing year by year.

Token authentication vs. biometric authentication systems

Biometric systems have been around for a significant period of time, and they have successfully made the leap from science fiction and movies to the real world. Early issues such as revocation and replay have largely been resolved, though compromise of the biometric storage system still remains an issue. Consider what happens if your biometrics are compromised where they're stored. What do you do if your fingerprints or retina scans are pinched? You cannot very well go and get a new set!

Unlike swipe cards, tokens and passwords, it's hard to forget your fingers at home. The problem with biometric authentication is that some vendors are promoting them as a substitute for conventional authentication processes, but they're not. Biometric systems make an excellent addition to security, and could be considered a substitute for token-based authentication, but they will never be a substitute for a username/password/PIN. If you haven't implemented a second factor of authentication, then review both biometrics and tokens. Either would significantly complement your current security setup.

Conclusion

Tokenization greatly simplifies the use of payment applications for mobile phones. HCE solution (host card emulation) in mobile phones creates a space that was previously only found on the SIM card and was under the control of the operators. The exclusion of operator, as a necessary third-party, payment options opened up a greater number of candidates. Some banks offer mobile apps, which after downloading and activating, allow pay by pressing a single icon. No need to visit either the operator or a bank. Bank through the application connects mobile devices with a card of the client. Then, the mobile phone starts to behave like a contactless payment card, while not necessary to have the running application, but must be turned on NFC mode. These applications allow the generation of replacement data from which cannot clone a plastic card, but allows payment on websites which are unknown to customer, . Shopping on the Internet will become safer and without establishing a PayPal account.

Contacts

Ing. Mgr. Peter Schmidt, PhD.
Department of Applied informatics,
Faculty of Economic Informatics,
University of Economics in Bratislava
peter.schmidt@euba.sk

Bibliography

1. *Cárachová, Magdaléna. Aspekty informačnej bezpečnosti v podnikovom prostredí. In Dnešní trendy inovací 4 / Ved. editori: Ladislav Várkoly, Jaromír Bogr, Ladislav Mareček ; Recenzenti: Josef Filípek, Jozef Hvorecký ... [et al.]. - Brno : B&M InterNets, 2014. - ISBN 978-80-260-6151-9. - S. 204-211.*

2. *DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dát. Brno: Computer Press, 2004. ISBN 80-251-0106-1.*

3. *JELÍNEK, M. Autentizační tokeny v praxi. Systemonline.cz [online]. 2008 [cit. 2013-05-05]. Dostupný z: http://www.systemonline.cz/it-security/autentizacnitokeny-v-praxi.htm*

4. *Szivósová, Mária. E-business in European small and medium sized enterprises, In Ekonomika a informatika : vedecký časopis FHI EU v Bratislave a SSHI. - Bratislava : Fakulta hospodárskej informatiky : Slovenská spoločnosť pre hospodársku informatiku, 2013. - ISSN 1336-3514. - Roč. 11, č. 1 (2013), s. 156-167.*

5. *Rakovská, Eva. E-business - the technologies behind. In Trends and Innovation in E-business, Education and Security : Proceedings, dňa 19.11.2014 / recenzenti: Miroslav Hudec, Jaroslav Kultán. - Bratislava : Ekonomická univerzita v Bratislave, 2014. - ISBN 978-80-225-3987-6. - pp. 68-75 [CD-ROM].*

6. *Záborský, Ján. Nové zaklínadlo mobilných platieb: tokenizácia. In Trend, News and Media Holding, Bratislava 2016, roč. XXVI, číslo 47, ISSN: 1335-0684*

7. *Website technopedia [online 4.11.2016] < https://www.techopedia.com/definition/13657 /multi-factor-authentication-mfa>*

8. *Website TechTarget [online 3.11.2016] < http://searchsecurity.techtarget.com>*