



Robust and Secure Access Schema using Dual Factor Authentication and OTP using Android Interface

Channappa Gowda D V

Assistant Professor, Dept. of ISE, The Oxford College of Engineering, Bangalore, Karnataka, India

ABSTRACT: The proposed system highlights one premium web services authentication system using dual factor in order to assure enhanced protection. As internet is flooded with illegal and malware application which are almost invisible to the generic user, hence there is a huge need to safe guard the clients who are actually paying for the services in order to maintain confidentiality and privacy. The proposed system provides a better score of authentication guarantee, which is very prominent for implementation purpose. A test bed is creating using windows OS and Android Mobile Interface (AMI), considering IMEI and IMSI information of a real time cellular phone. The proposed system highlights a novel dual-factor authentication scheme whereby a user's device produces multiples OTPs from an initial seed using the proposed production scheme.

KEYWORDS: One Time Password, Dual Factor Authentication, Android mobile interface

I. INTRODUCTION

Two-factor authentication is commonly found in electronic computer authentication, where basic authentication is the process of a requesting entity presenting some evidence of its identity to a second entity. Two-factor authentication seeks to decrease the probability that the requestor is presenting false evidence of its identity. The number of factors is important as it implies a higher probability that the bearer of the identity evidence indeed holds that identity in another realm (i.e.: computer system vs. real life). In reality there are more variables to consider when establishing the relative assurance of truthfulness in an identity assertion, than simply how many "factors" are used. Two-factor authentication is often confused with other forms of authentication. Two factor authentications require the use of two of the three regulatory-approved authentication factors. These factors are: Something the user knows (e.g., password, PIN); something the user has (e.g., ATM card, smart card); and something the user is (e.g., biometric characteristic, such as a fingerprint). According to proponents, TFA could drastically reduce the incidence of online identity theft, and other online fraud, because the victim's password would no longer be enough to give a thief permanent access to their information. However, many TFA approaches remain vulnerable to Trojan controlled websites and man in the middle attacks.[3] In addition to such direct attacks, three aspects must be considered for each of the 2 (or more) factors in order to fully realize the potential increase in confidence of authentication:

- The inherent strength of the mechanism, i.e. the entropy of a secret, the resistance of a token to cloning, or the uniqueness and reliability of a biometric.
- Quality of provision and management. This has many aspects, such as the confidence you can have that a token or password has been securely delivered to the correct user and not an imposter, or that the correct individual has presented himself for enrollment of his biometric, as well as secure storage and transmission of shared secrets, procedures for password reset, disabling a lost token, re-enrollment of a biometric, and prompt withdrawal of credentials when access is no longer required.
- Proactive fraud detection, e.g. monitoring of failed authentication attempts or unusual patterns of behavior which may indicate that an attack is under way, and suitable follow-up action.

Another solution suggests the utilization of signature chains to address the chain length restriction by involving public key techniques. This technique, however, also increases computation costs. Moreover, time-synchronized OTP



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 6, June 2017

systems, which are typically based on an internal clock synchronized with a main server, are not applicable for mobile phones. In addition, due to the general nature of mobile phones (e.g., out of network, etc.); such synchronization cannot typically be guaranteed. To overcome the restrictions discussed above, this proposed system will discuss OTP production in the forward direction. This production will completely eliminate the mentioned limitations. Our idea is to produce multiple OTPs from an initial seed in a parallel process with the service provider itself, e.g., an online bank, by utilizing two different types of hash functions, which come with a nested chain. The resulting chain provides forwardness and infiniteness.

II. RELATED WORK

D.Parameswari and L.Jose [1] describes a method of implementing two factor authentication using SMS OTP - One Time Password to Secure an E-Transaction (SET). D.Parameswari and L.Jose provides the reader with an overview of the various parts of the system and the capabilities of the system. Generated One Time Password is valid for only a short user defined period of time and it is generated and verified using Secured Cryptographic Algorithm. FadiAloul, Syed Zahidi, Wassim El-Hajj [2] describes a method of implementing two factor authentication using mobile phones. They generated One Time Password is valid for only a short userdefined period of time and is generated by factors that are unique to both, the user and the mobile device itself. Additionally, an SMS-based mechanism is implemented as both a backup mechanism for retrieving the password and as a possible mean of synchronization. FadiAloul proposes and develops a complete two factor authentication system using mobile phones instead of tokens or cards.

Bogdan Groza, DorinaPetrica [3] Leslie Lamport in his paper Password Authentication with Insecure Communication proposed the use of one-way functions in order to obtain one time passwords. Because of their simplicity cryptographic hash functions are commonly used for such purpose. HavardRaddum, Lars Hopland Nest^oas, and KjellJ^orgen Hole [4] suggested two minor changes to Encap's protocol designs, one to bring the activation protocol's key generation in line with "best practice," and one to simplify the designs without reducing the security. The seriousness of the attacks shows how important a system-level analysis and testing can be to determine the level of security provided by protocols in a real system.

Stephen Chan, Stephen Lau, Jay Srinivasan, Adrian Wong [5] presented a prioritization of the work that needs to be done. OTP has very broad ranging effects and it is important that the most pressing issues be dealt with first. In addition, there is technology that needs to be developed and deployed-identified the work that we feel needs to be done, and prioritized it based on current observations. Chunhua Chen, Chris J. Mitchell, Shaohua Tang [6] show how Trusted Computing can be extended in a GAA-like framework to offer new security services. They then propose a general scheme that converts a simple static password authentication mechanism into a one-time password (OTP) system using the GAA key establishment service. Vipul Goyal, Ajith Abraham, SugataSanyal and Sang Yong Han [7] device a novel construction of hash chains. The basic idea here is to repeatedly require the insertion of user password after a fixed distance in the hash chain. The links at which the insertion of the password is required may be made public and stored at the host (server).

Kenneth G. Paterson and Douglas Stebila [8] consider the use of onetime passwords in the context of password-authenticated key exchange (PAKE), which allows for mutual authentication, session key agreement, and resistance to phishing attacks. Author describe a security model for the use of one-time passwords, explicitly considering the compromise of past (and future) one time passwords, and show a general technique for building a secure one-time-PAKE protocol from any secure PAKE protocol. Our techniques also allow for the secure use of pseudo randomly generated and time-dependent passwords.

Dinei Florencio and Cormac Herley [9] describe a service that allows users one-time password access to any web account, without any change to the server, without changing anything on the client, and without storing user credentials in-the-cloud. Employ a simple mapping of the arbitrary input password to restricted character set OTP's: thus every OTP is readable without ambiguity no matter what display or font is used, can be transmitted over SMS, and can be entered even on unfamiliar keyboards without the use of meta keys.

Anders Moen Hagalisletto and Arne Riiber [10] present a commercial protocol, developed by a Norwegian start-up copmany, for using a mobile terminal as a password calculator that could potentially be used towards any service provider on the internet. They report theirr experiences by specification, validation, and analysis of the protocol in particular the threat of phishing attacks is investigated.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 6, June 2017

Ryoichi Isawa and MasakatuMorii [11] propose a new one-time password scheme against the Hybrid Theft attack*1. The proposed scheme has three advantages: 1) secure against all the existing attacks, 2) based on only one-way hash function, and 3) a mutual authentication scheme. Compared with SAS-X (2), the proposed scheme is more secure because of the advantage 1, and can compute faster because of the advantage 2. SAS-X (2) is a one-way authentication scheme

Andrew Tillman [12] presents Many MLSs and associations are looking to implement improved security measures such as two factor authentication. Existing solutions are problematic in either cost and/or practicalityA solutions that use SMS would be a cost-effective and practical way in which to provide this functionality and as a result greatly increase the security of these important online resources. Alberto BenaventeMartínez, Spain [13] designs an authentication model that uses a onetime password (OTP) mechanism.

Password-authenticated key exchange was first introduced by Bellovin and Merritt in 1992 [14] as a protocol in which the client and server share a plaintext password and exchange encrypted information to allow them to derive a shared session key. A later variant [15], often called verifier-based, removed the requirement that the server have the plaintext password, instead having a one-way transformation of the password. The most extensively used model for the security of PAKE protocols is the Bellare-Pointcheval-Rogaway (BPR) model [16] and its extension [17] for verifier-based protocols. This model is the starting point of our model for the security of one-time-PAKE protocols. One particular such protocol is the PAK protocol [18, 19], which is the basis of our construction in the full version of this paper. Various authors have noted the value of using one-time passwords in authenticated key exchange protocols [20, 21, 22]. Abdalla et al. [23] (see also [24]) describe the OPKeyX protocol, a verifier-based one-time-PAKE protocol. It uses a hash chain to derive subsequent one-time passwords from a seed such that the server can verify but not compute the next password.

III. PROBLEM DESCRIPTION

This dual-factor authentication system suffers from the following shortcomings:

- SMS Cost: During every login request or transaction process, it is necessary to send an SMS-OTP from the bank to the user. This, in turn, will be costly to the bank with the consideration of statistics of bank's transactions
- SMS Lateness: The SMS transmission delay represents one of the major limitations of the traditional system.
- International Roaming: Travelling overseas creates restrictions on the SMS services. Turning off the roaming service will prevent the bank from sending the SMS-OTP, which in turn, stops the user from resuming any further processes.
- SMS Security: It can be said that while designing the GSM system, it had all security measures in mind, but as time passed and algorithms were cracked by the hackers, SMS-OTP based systems were not kept secure.

IV. PROPOSED SYSTEM

The main aim of the paper is to develop an architectural framework for dual factor authentication system, where the system will produce one time password (OTP) in the forward direction. The prime idea is to generate multiple OTPs from an initial seed in a parallel process with the service provider itself, e.g., an online bank, student file management, financial services etc. by utilizing two different types of hash functions, which come with a nested chain. The resulting chain provides forwardness and infiniteness and it should run on multiple systems of wired or wireless network. The cumulative architecture of the proposed system is as shown in Figure 1. The Lamport's idea has been extended with some modifications in order to generate infiniteness and forwardness, avoiding the use of public key cryptography. The shortcoming of those two parameters, infiniteness and forwardness, cause the several vulnerabilities shown with respect to the related work. A one-time password is valid for only one login session or transaction. OTP avoid a number of shortcomings which are associated with traditional (static) passwords. Dual-factor authentication is an approach to authenticate which requires the presentation of two different kinds of evidence that someone is who they say they are. It is a part of the broader family of multi-factor authentication, which is a defense in depth approach to security. Authentication is the act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person, tracing the origins of an artifact, ensuring that a product is what it's packaging and labeling claims to

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 6, June 2017

be, or assuring that a computer program is a trusted one. The proposed work mainly constitutes of two modules e.g. administrator (or service provider) and student. The administrator basically supervises the application by assisting in creation of account as well as relaying the services based on the digital content used by the student user. As the application will consist of a privilege access for the student, so an efficient and robust authentication as well as authorization is highly required.

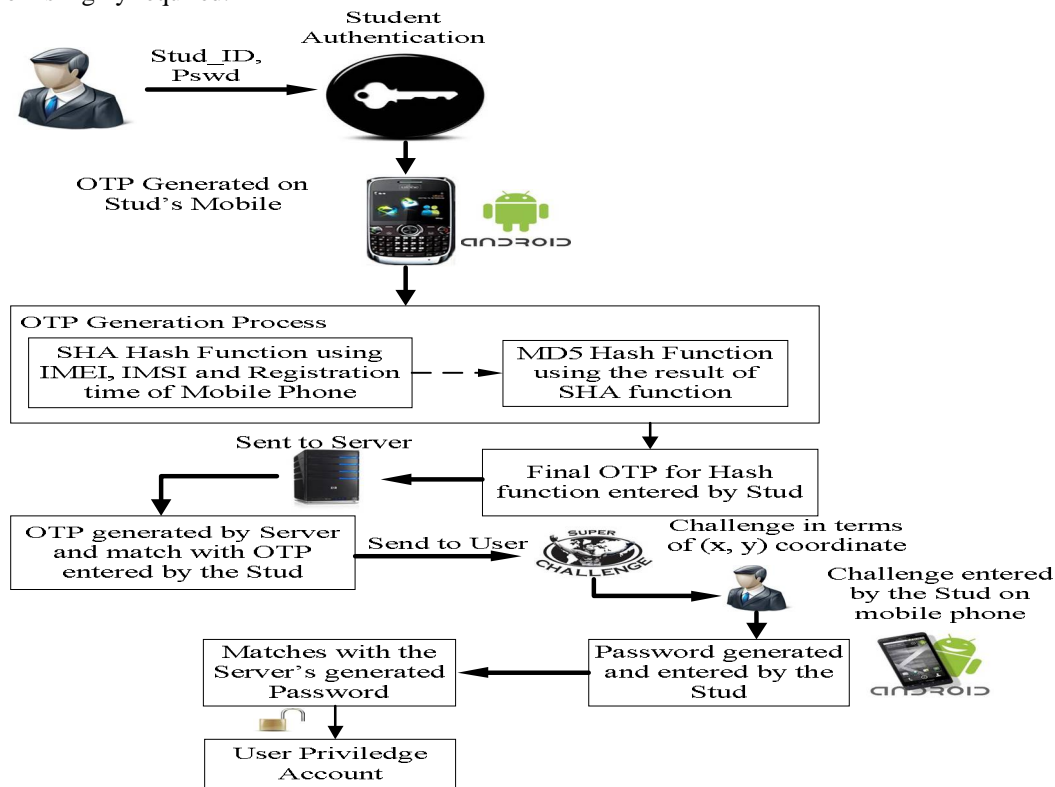


Figure 1: Proposed Architecture

The proposed system is mainly partitioned in three phases:

- **Enrollment Phase:** The student gets the two different hash functions, and an initial seed, established on their Android enabled mobile phone. To ensure that the information is completely shared with the service provider, the seed is produced by the shared and unique parameters of the host and user, e.g., the International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI), and enrollment date.
- **Login and Authentication Phase:** The steps of the login and authentication process between the user and service provider are like this; the student logs in to the service provider's website, requesting access. As a response to this access request, a secure session is established, allowing the student to enter their authentication privileges, i.e., student's name and password, the first factor of authentication, what the student knows. Also the student provides the server with their OTP's current status. The current status allows the server to synchronize the generated seed with the student's current seed to get the same seed value on both sides before sending a challenge. The server randomly challenges the student with new indexes. The student enters those indexes, in their OTPgenerator to get the corresponding OTP. The student responds with this corresponding OTP. The server compares the received OTP with the calculated one. According to the server check, done in the previous step, the server will transfer an authorization execution or a communication termination.
- **Mathematical Illustration:** Through the enrollment process, the student gets two different hash functions, which could be SHA-1, and $h_B(.)$, which could be MD5, along with an initial seed, " S_{int} ," as the concatenation of the IMEI,



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 6, June 2017

IMSI, and registration time, which could be “1234567891234561234567891234507012010200259” assuming IMEI is “123456789123456,” IMSI is “12345678912345,” and the registration time is “7/1/2012 20:02:59.” After logging into the service provider’s website using a different and static username and password, the first factor of authentication, the server asks the user for the OTP’s current status. If the student has generated numerous OTPs without using them, he might have reached an OTP status of, for example, “17.” The user will submit his current status to the server to allow the server to calculate the current seed $S_{\text{crt}}=H_A^{17}(S_{\text{int}})$ 1220848648030773785924867285680707842195071405780, which means that the server has calculated seventeen cascaded hashes of its initial seed “ S_{int} ,” using the SHA-1 algorithm, to be synchronized with the client. After that the server sends a random challenge value of new indexes, e.g., $x, y = 3, 4$, which means the user has to calculate his session OTP using this formula: $\text{OTP}=h_B^4(H_A^3(S_{\text{crt}}))= 68606061177919188523363813602016333158$. The server has to calculate the same value in a parallel process, and as soon as the client responds, the server will match the two values to give either a yes or no.

Static password has been long acknowledged as a big security and management headache to IT administrators of enterprises. Usually, a simple password was used repeatedly by a user or written down carelessly on a piece of paper. Unlike the traditional single-factor static password, one time password changes each time the user logs in. Thus, on one side, the users are forever freed from remembering static password by simply using a detached OTP generator or token; on the other side, sensitive personal information in the IT systems is better protected against unauthorized access since relay attacks are effectively prevented. To face the increasing security demands on IT systems nowadays, it is highly advised that enterprises introduce two-factor authentication methods into their IT infrastructure. The OTP solution, as the most adaptable and flexible scheme, is becoming the most popular information security solution in the field with cost-effective user OTP tokens and advanced security.

The proposed scheme can resist an off-line guessing attack because it uses strong passwords produced from strong hash functions. Moreover, replaying reusable passwords is restricted by encoding passwords to be used one time. However, it is necessary to prevent another token from becoming an OTP generator for the same user. A manual process should handle this situation.

V. SIMULATION RESULTS

The proposed system is designed on Windows 32-bit OS with 1.84 GHz processor with broadband connectivity of 100 Mbps. The programming is done on MyEclipse IDE. The experiment for the proposed system is done on real time Samsung Galaxy Smartphone with Android 2.2. Hence Android Development Tools (ADT) is used as it is a plug-in for the MyEclipse IDE that is designed to give a powerful, integrated environment in which to build Android applications. The proposed system will be experimented with active wireless connectivity between the system and Android enable device.

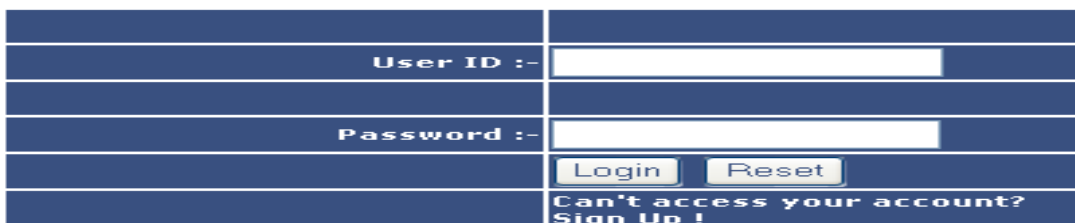


Figure 2: Student Login Options

THE ABOVE FIGURE 2 HIGHLIGHTS THE INITIAL AUTHENTICATION LOGIN FOR STUDENT. INITIALLY THE STUDENT HAS TO SIGN UP A NEW ACCOUNT WHERE THEY HAVE TO FURNISH ALL THE DETAILS AS SHOWN IN FIGURE 3.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirce.com

Vol. 5, Issue 6, June 2017

Name :-	<input type="text" value="Ravi"/>
College id :-	<input type="text" value="520923885"/>
Password :-	<input type="password" value="••••"/>
Confirm Password :-	<input type="password" value="••••"/>
Mobile No :-	<input type="text" value="7411666205"/>
Email :-	<input type="text" value="ravi.cbkinfotech@gmail.com"/>
Address :-	<input type="text" value="Mathikere
Bangaluru
Karnataka-560054"/>
IMEI No :-	<input type="text" value="0000000000000000"/>
IMSI No :-	<input type="text" value="3102600000000000"/>
Timestamps	<input type="text" value="1277931480000"/>
Your Question :-	<input type="text" value="How RU?"/>
Answer :-	<input type="text" value="I M GooD....."/>
	<input type="button" value="Submit"/> <input type="button" value="Reset"/>

Figure 3: Sign-up Information feeding.

After the successful sign-up, the student can log in to their privilege account using the similar College ID as user ID and password, which was successfully fed at the time of sign up process

Are you human?
If yes.
Type the characters you see in the picture below




Figure 4: Captcha Authentication.

Once the student logs and their initial user ID and password is accepted, then they will be prompted to feed the random digital information displayed by Captcha application as shown in Figure 4. Now, after the successful sign up, the student can now perform initial login authentication for which they will be asked to feed OTP and Current status, both of which is generated at the Mobile interface as shown in Figure 5 and 6.

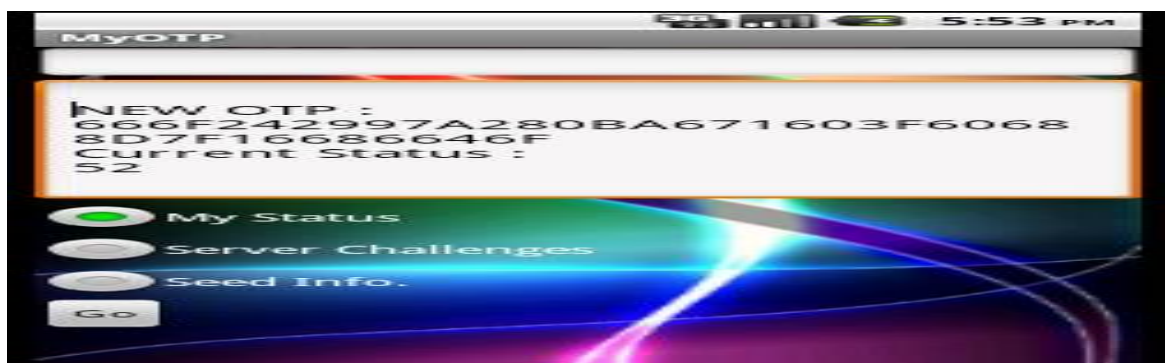


Figure 5: OTP & Current Status generation in Mobile interface

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirce.com

Vol. 5, Issue 6, June 2017

One Time Password :-	13F60688D7F16686646F
Current Status :-	52
<input type="button" value="Login"/>	<input type="button" value="Reset"/>

Figure 6: Feeding OTP and Current Status from mobile interface to web interface.

Once the OTP and current status is authenticated, the new index will be generated automatically in web interface as shown in Figure 7.

New Index :-	108, 104
<input type="button" value="Next"/>	

Figure 7: Generation of new Index



Figure 8: Generation of OTP in Mobile Interface.

Once the new index value is authenticated in the mobile interface, the next sequence, it will generate a new OTP, in same mobile interface as shown in Figure 9. The student needs to take the newly generated OTP and feed in to their web-interface for final authentication as shown in Figure 10.

Enter Your New OTP :-	3E38C29021E7CC54F93
<input type="button" value="Next"/>	

Figure 9: Feeding newly generated OTP in web interface.

VI. CONCLUSION AND FUTURE WORK

A new two-factor OTP-based authentication scheme has been proposed using Android mobile phones as they are becoming more and more powerful devices. This new authentication protocol provides forward and infinite OTP generation using two nested hash functions. The proposed approach has been illustrated to an online authentication process. This scheme achieves better characteristics than the other schemes discussed above. The proposed system is not limited to a certain number of authentications, unlike the previously-mentioned OTP hashing-based schemes and does not involve computationally expensive techniques to provide the infiniteness. The protocol doesn't require a token embedded server synchronized clock like. The approach eliminates the problems with utilizing OTPs with an SMS, consisting of the SMS cost and delay, along with international roaming restrictions. A detailed security analysis was also performed that covered many of the common types of attacks. The two factor authentication property has been achieved without restrictions.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 6, June 2017

REFERENCES

- [1] D.Parneswari a*, L.Jose "SET with SMS OTP using Two Factor Authentication" Journal of Computer Applications (JCA) ISSN: 0974-1925, Volume IV, Issue 4, 2011.
- [2] Fadi Aloul, Syed Zahidi, Wassim El-Hajj "Two Factor Authentication Using Mobile Phones" Conference Location: Las Vegas, NV E-ISBN: 978-0-7695-4367-3 Print ISBN: 978-1-61284-427-5, 11 July 2011
- [3] Bogdan Groza, Dorina Petrica "ONE TIME PASSWORDS FOR UNCERTAIN NUMBER OF AUTHENTICATIONS" "Politehnica" University of Timisoara Department of Automation and Applied Informatics Bd. Vasile Parvan nr. 2, 302223 Timisoara, Romania
- [4] Håvard Raddum, Lars Hopland Nestås, and Kjell Jørgen Hole "Security Analysis of Mobile Phones Used as OTP Generators" P. Samarati et al. (Eds.): WISTP 2010, LNCS 6033, pp. 324–331, 2010. C. IFIP International Federation for Information Processing 2010.
- [5] Stephen Chan, Stephen Lau, Jay Srinivasan, Adrian Wong "One Time Password Authentication for Open High Performance Computing Environments" April 26, 2004
- [6] Chunhua Chen, Chris J. Mitchell, Shaohua Tang, "Ubiquitous One-Time Password Service using the Generic Authentication Architecture" China (No. 9351064101000003).
- [7] Vipul Goyal, Ajith Abraham, Sugata Sanyal and Sang Yong Han "The N/R One Time Password System" RFC 1321, April 1992.
- [8] Kenneth G. Paterson, Douglas Stebila "One-time-password-authenticated key exchange" September 4, 2009, p. 264-281 (Lecture Notes in Computer Science).
- [9] Dinei Florêncio and Cormac Herley "One-Time Password Access to any Server without Changing the Server" Proc. ISC '08, Taipei
- [10] Anders Moen Hagalisletto Arne Riiber "Using the mobile phone in two-factor authentication" The basic authentication mechanism is covered by the patent application document (PCT WO/2007/039806).
- [11] Alberto Benavente Martínez, Spain "One-Time Password Authentication Scheme to Solve Stolen Verifier Problem" L-022, back to the Intelligence Science and Technology.
- [12] Andrew Tillman "Two Factor Authentication Using SMS" Center for REALTOR® Technology Version 1.0
- [13] Alberto Benavente Martínez, Spain "Authentication model that uses One Time Passwords" Global Information Assurance Certification Paper 1 December 2003
- [14] Steven M. Bellovin and Michael Merritt. Encrypted key exchange: Password-based protocols secure against dictionary attacks. In Proceedings of the 1992 IEEE Computer Society Conference on Research in Security and Privacy. IEEE, May 1992. DOI:10.1109/RISP.1992.213269.
- [15] Steven M. Bellovin and Michael Merritt. Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password file compromise. In Proc. 1st ACM Conference on Computer and Communications Security (CCS), pp. 244–250. ACM, 1993. DOI:10.1145/168588.168618.
- [16] Mihir Bellare, David Pointcheval, and Phillip Rogaway. Authenticated key exchange secure against dictionary attacks. In Preneel [Pre00], pp. 139–155. DOI:10.1007/3-540-45539-6_11.
- [17] Craig Gentry, Philip MacKenzie, and Zulfikar Ramzan. PAK-Z+, August 2005. URL <http://grouper.ieee.org/groups/1363/WorkingGroup/presentations/pakzplusv2.pdf>. Contribution to the IEEE P1363-2000 study group for Future PKC Standards.
- [18] Victor Boyko, Philip MacKenzie, and Sarvar Patel. Provably secure Password-Authenticated Key exchange using Diffie-Hellman. In Preneel [Pre00], pp. 156–171. DOI:10.1007/3-540-45539-6_12. Full version available as [BMP00b].
- [19] Philip MacKenzie. The PAK suite: Protocols for password-authenticated key exchange. Technical Report 2002- 46, DIMACS Center, Rutgers University, 2002. URL <http://dimacs.rutgers.edu/TechnicalReports/abstracts/2002/2002-46.html>.
- [20] Michel Abdalla, Olivier Chevassut, and David Pointcheval. One-time verifier-based encrypted key exchange, 2005. URL <http://www.di.ens.fr/~mabdalla/papers/ACP05-letter.pdf>. Extended abstract published as [ACP05a].
- [21] Liang Fang, Samuel Meder, Olivier Chevassut, and Frank Siebenlist. Secure password-based authenticated key exchange for web services. In Proc. 2004 Workshop on Secure Web Service (SWS), pp. 9–15. ACM, 2004. DOI:10.1145/1111348.1111350.
- [22] Douglas Stebila. Classical Authenticated Key Exchange and Quantum Cryptography. PhD thesis, University of Waterloo, 2009. EPRINT <http://hdl.handle.net/10012/4295>, URL <http://www.douglas.stebila.ca/research/papers/ste09/>.
- [23] Michel Abdalla, Olivier Chevassut, and David Pointcheval. One-time verifier-based encrypted key exchange. In Serge Vaudenay, editor, Public Key Cryptography (PKC) 2005, LNCS, volume 3386, pp. 47–64. Springer, 2005. DOI:10.1007/b105124. Full version available as [ACP05b].
- [24] Olivier Chevassut, Frank Siebenlist, and Mike Helm. Secure (one-time-) password authentication for the Globus toolkit. In GlobusWorld Conference, February 2005. URL <http://acs.lbl.gov/Projects/OPKeyX/Talks/GlobusWorld05/GlobusWorld05.html>.