AKADEMIA GÓRNICZO–HUTNICZA
IM. STANISŁAWA STASZICA W KRAKOWIE

Faculty of Computer Science, Electronics and Telecommunications

Towards Mobile Security

Voice based authentication protocol

to biometrically harden

secure encryption and

data communication schemes

Autoreferat

In the field of Computer Science
IT Security - Cyber Defense

submitted by

Sebastian Piotr Szlósarczyk

Kraków, 2017

Supervisor: Prof. dr hab. inż. Krzysztof Zieliński

Abstract

The dissertation thesis with the title Towards mobile security - Voice based authentication protocol to biometrically harden secure encryption and data communication schemes written by Sebastian Piotr Szlósarczyk focuses on the realisation of the improvements in the field IT security. IT security is mainly countering any kind of threats all users face in different environments of information technology and their (network) architecture. The contribution tackles biometric doubts and proposes a new cryptographic protocol which counters password protocol weaknesses. The innovation is a voice based authentication protocol which is able to harden any type of secure encryption and data communication schemes biometrically in order to overcome security threats. The complexity of the presented protocol is outlined in contrast to current schemes and the importance of the developed mathematical structure is presented. Further the research result concludes that the development improves security awareness as psychological fact with the voice's biometric fingerprints as well as it opens future research possibilities of stating security levels by examining audio fingerprints more thoroughfully.

Thesis Outline

The scope of this thesis was to show, how it is possible to limit human failure - especially in the area of IT: The keynote of the presented solution is a password authentication scheme where the mutual agreed keyed secret of the protocol is personalised to one user by the help of acoustic finger-prints.
This dissertation unifies encryption and authentication resulting in the development of a cryptographic protocol. It tackles known exploits and security concerns which are enumerated throughout related work and own research.
The proposition in this thesis is a cryptographic authentication protocol, where sensitive data (especially on mobile phones) can be secured or whereby services can be locked - all by the user's voice. The usage can be extended and is left open for future work and discussion.

The scientific contributions of the research in this thesis were subdivided into:

· Critical analysis of the current state in the area of password authenticated protocols, including capabilities and limitations of existing solutions which comprise

o known protocols which use passwords that correlate with the protocol presented in this dissertation,

o (authenticated) key agreement schemes which gave the step-in idea to design the protocol in this thesis,

o critical examination of voice authentication including research to improve security flaws of biometry.

· Specification of the methodology for realising the voice based authentication protocol:

o as innovative development,

o as applicable and working innovation.

· Whereas the specification of the protocol included:

o methodical definition of all environment parameters,

o utilisation of all parameters in protocol computations,

o declaration of challenge response mechanism.

o influence of voice into the protocol,

o categorising password authentication,

o configuration.

· Pointing out the strength of the cryptographic protocol:

o in comparison to other known protocols and related work,

o why it does improve security architecture,

o why it does offer an important scientific contribution.

· Covering and improving human failure:

o show people's awareness on base of an own survey and a public one,

o point out the reason why humans do interact in these manners,

o explain why the authentication protocol is able to leverage awareness failure.

· Proposal:

o in comparison to other known protocols and related work,

o why it does improve security architecture.

· The prototype implementation of the authentication protocol enfolded:

o implementation of proposed cryptographic means for the protocol in the Java Cryptographic Architecture (JCA),

o extension of Android architecture with use of the authentication protocol in cryptographic suite (JCA),

o implementation of lockscreen and data encryption with use of the authentication protocol,

o PoC for encryption by the use of a financial banking application.

· The practical evaluation of the proposed conception comprises:

o evaluation of prototype implementation of cryptographic Library,

o setting up the environment of the password based protocol presented,

o protocol verification whether the cryptographic primitives do work,

o entropy measurements achieved by the seed of the voice including ran-dom number generation,

o abnormal circumstances to compute acoustic fingerprints,

o ergonomics of protocol usability.

Approach

The roadmap for realizing the purposes in the dissertation was:
First covering security awareness as initial starting point where the philosophical and practical views introduce the reasoning for security in IT.
Further cryptographic basics which comprise number theoretic elements, entropy metrics and protocol algorithm structure in order to showcase the mathematical architecture of the password authentication protocol.
After the introductory themes, the focus relies on the description of the concept for the pass-word authentication protocol: The definition of the structure of the cryptographic algorithm in the presented protocol and its protocol structure is covered, as well as the description for the prototype implementation of the password authentication protocol realized in Android operating system.
The implementation includes the proof of concept (PoC) realization of the conceptual part of the authentication protocol.
The evaluation involves a set of 7 different experiments (P1 up to P6 included the entropy computations), which covers both the theoretical and practical dimensions of the password authentication protocol prototype.

Outcome - Practical and theoretical meaning of dissertation

The result is the voice based authentication protocol:

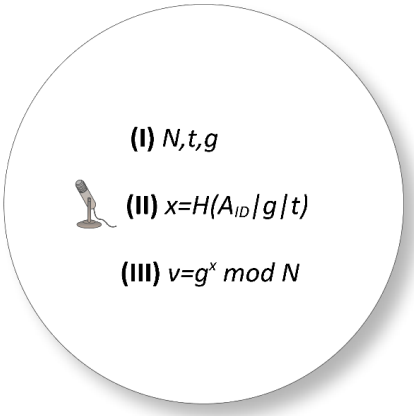
Two parties are defined to take part in the protocol who are inter-acting, where one party wants to authenticate and the other one wants to prove and verify it

In the protocol there are 3 steps defined

(1) the setup phase where
a. the voice is recorded

b. its acoustic fingerprint is computed and

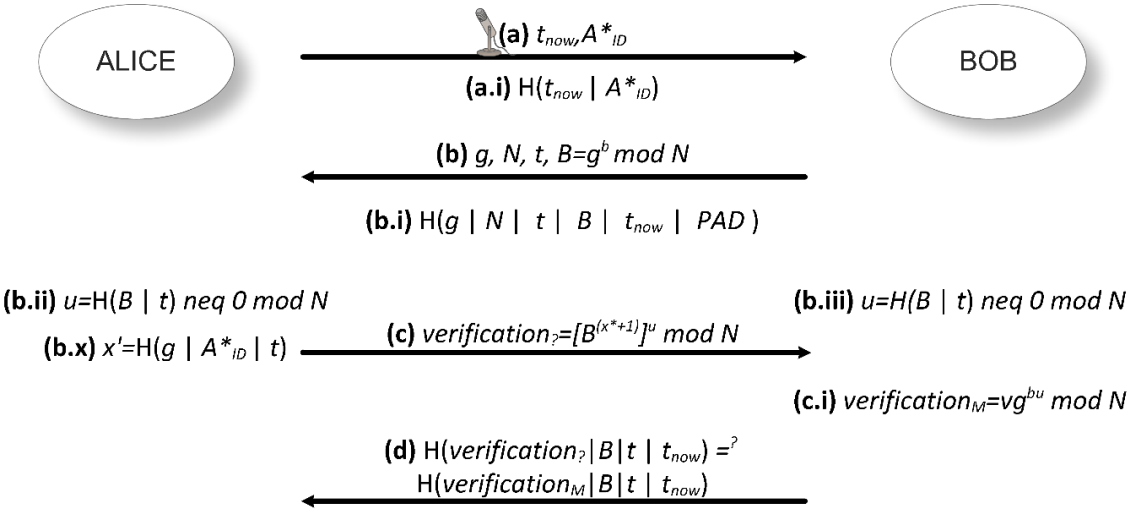
c. securely stored for further authentication



(2) authentication phase where
a. the proven voice is computed

b. validation is checked and

c. the authentication in form of a equality match is verified



The third step of the protocol is the practical meaning of computing the shared secret key for any further purpose which is shown in (d).
Protocol verification
The protocol works because:

$$B^{(x'+1)u} =$$

$$B^{x'u+u} = (g^b)^{x'u+u} = g^{bx'u+bu}$$

$$= g^{bx'u}\, g^{bu} = (g^{x'})^{bu}\, g^{bu} = v^{bu}\, g^{bu}$$

if x' = x, then: **the acoustic fingerprint *x'* to be verified**

is identic with the one of the setup x

$$= (vg)^{bu}$$

Concerning the number theoretical requirements, the protocol satisfies:
· *representation is easy and compact,*
· *fast arithmetic,*
· *DLP is computationally hard,*
· *group order can be computed efficiently.*

Summary of functional results of dissertation

· limitting human failure by the Improvement of awareness with the influence of the voice into the protocol algorithm,

· leveraging attacks on base of its cryptographic complexity structure,

· hardening the security kernel on account of the increased entropy of the voice,

· ability of authenticating users themselves to second party, e.g. a server,

· personal identification by the biometric charateristics,

· improving shelter from unauthorized access,

· contribution of a cryptographic secure protocol especially by the help of the discrete logarithm problem and challenge-response structure,

· compromission of the ephemeral keys does not lead to a compromission of the whole protocol,

· resistance to dictionary attacks,

· opportunity of execution of protocol in a non-exploitable environment, i.e. in the TEE,

· securing of password-equivalent data by the help of the discrete logarithm,

· computation of a shared secret for any further encryption leading into properties of diffusion and confusion,

· base for a logical system offering the property of soundness.

Practical propositions of prototype implementation:

· protocol messages,

· protocol setup,

· protocol verification,

· random number generation,

· prime number generation,

· password choice by the help of a chosen library for computing the acoustic fingerprint of the biometric voice influence.

· the password x consists as hash value of the computed acoustic fingerprint AID, generator g and timestamp t,

· a shared key is computed whenever the verification algorithm succeeds,

· the discrete logarithm problem (DLP) is used,

· the communication messages can be secured (e.g. via encryption),

· voice biometrics is used,

· entropy seeds are used in the setup of the protocol,

· high security level,

· an attacker, especially an eavesdropper cannot obtain enough information to be able to guess a password by the brute force method without further interactions with the parties for each guess,

· useable password-equivalent data are never stored. This means that an attacker who steals data (such as the parameter v) cannot masquerade as the authenti-cating person unless he first performs a brute force search for the password,

· the protocol aims to be resistant to dictionary attacks mounted by an eavesdrop-per as records of the voice do not success in impersonating (see evaluation)

· even if one or two of the cryptographic primitives it uses are attacked, it is still secure.

Further one can conclude the following particular explorations in contrast to present protocols:

· as all protocols the one presented in this dissertation can have a password consisting of a charset counting to text dependent voice recognition systems,

· security is set to a higher level by the use of the DLP,

· the protocol presented in this thesis is the only one were voice is used and it is the only one to specify how computed bytes of the recorded voice can be used,

· mutual authentication is offered as well.

The complexity for breaking the password and its needed ephemeral key of the presented authentication protocol can be counted as twice for all the algorithms presented in Table 1. Both, the password protection v = gx and the ephemeral key b rely on the discrete logarithm problem and makes the whole password authentication protocol thus cryptographically secure. In the latter table attacks against the contributed password authentication protocol in big O notation are summed up.

Algorithm	Complexity
Baby-step Giant step	O(2$\sqrt{N}$)
Pohlig Helman	O(2$\sqrt{N}$)
Shor	O(4(log N)2(log log N)(log log log N))
Index Calculus	O(2(N3+N2+uu))

If a new password is passed to the system in unencrypted form, security can be lost before the new password can even be installed in the password database. Of course either, if the new password is given to a compromised employee, so that a new text or a new spoken segment must lead to a new password key. The salts (padding PAD transferred in (b.i) and the request time tnow computed and transferred in (a)) prevent attackers from easily building a list of hash values for common passwords and prevents password crack-ing efforts from scaling across all users.

Evaluation

The factors that were evaluated are:

Nr.	Description
P1	Time, how long a computation of the acoustic signature takes.
P2	Time, how long a computation of all the environment parameters takes.
P3	False negatives of protocol execution between same individuals and different people under normal circumstances, i.e. without any influence of additional frequency.
P4	False positives of protocol execution between same individuals and different people under normal circumstances, i.e. without any influence of additional frequency.
P5	False positives of protocol execution between same individuals and different people under abnormal circumstances, i.e. having a cold, noisy influence and recorded voice.
P6	False negatives of protocol execution between same individuals and different people under abnormal circumstances, i.e. having a cold, noisy influence and recorded voice.

Future work

Protocol extensions

Each enlisted extension aspect of the possible future improvements is focused on the presented protocol structure itself.

Multi-parties
Not only two, but three or more (n) parties can engage the protocol. One party (the user) approves his authenticity towards the other ones. This scheme can be also pass-word related, where the password is a processing of the user's voice.
There are two options to be considered:
I. n:1 communication,

II. n:n communication.

From scratch, the scheme must be extended in this way for supporting these kind of communications, so that each party who wants to get involved in the verification process, needs to compute its own ephemeral key A = ga, C = gc etc., which needs to get influenced into the protocol.

Anonymous credentials
Anonymous credentials give the opportunity to authenticate anonymously on base of mathematic structures which are presented in [180, 184]. This technology can be considered to get involved in the presented password authentication protocol. The most profitable benefit that comes around is the anonymity of the voice sample.

Commercial prospects
Especially banks try to improve the security of their applications for the purposes of authentication and verification of their customers or workers. Further any e-commerce systems do try to increase the distinguishability of humans using biometric characteris-tics, as well as e-election systems aim in developing an easy but reasoned secure scope for election via the internet or mobile devices.

References

The significant references used can be classified into a category of their application field:

· current threats
· current user statistics
· psychological influence into IT
· worldwide IT security standards
· Advances in biometric schemes
· Cryptography
· Biometric advances

The most relevant references for the research are:

Nr.	Title
[9]	International Journal of Security and Its Applications: Cryptanalysis of a Biometric-based Multi-Server Authentication Scheme. TaoWan, Nan Jiang, Jianfeng Ma. February 2016.
[10]	Passwords and the Evolution of Imperfect Authentication. By Joseph Bonneau, Cor-mac Herley, Paul C. van Oorschot, Frank Stajano. Communications of the ACM, Vol. 58 No. 7, Pages 78-87, July 2015
[21]	Chenguang Yang: Security in Voice Authentication, A Dissertation, March 2014
[40]	Proceedings of IEEE 2014: Shawn Eastwood, Svetlana Yanushkevich: Modeling Risks in Biometric-Based Authentication Control Systems, September 2014.
[52]	BM Security, David Kaplan, Sagi Kedmi, Roee Hay, Avi Dayan: ATTACKING THE LINUX PRNG ON ANDROID, WEAKNESSES IN SEEDING OF ENTROPIC POOLS AND LOW BOOT-TIME ENTROPY, 2014.
[77]	Schneier, B Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. New York: Wiley, 1996.
[79]	On the generalization of Shannon entropy for speech recognition. Nicolas Obin; Marco Liuni. Spoken Language Technology Workshop (SLT), 2012 IEEE
[88]	The science of guessing: analyzing an anonymized corpus of 70 million passwords. Joseph Bonneau. IEEE Security & Privacy (Oakland) 2012. San Francisco, CA, USA.
[94]	The Design and Implementation of a Pseudo Random Number Generation Algo-rithm, Zuohu Liu; Minghe Huang; Shaojun Zhu, Computational Intelligence and Natural Computing. CINC '09. International Conference, 2009

Nr.	Title
[99]	Security in Voice Authentication by Chenguang Yang, A Dissertation, March 2014
[111]	J. Bonneau, S. Preibusch, and R. Anderson: Birthday Present Every Eleven Wallets? The Security of Customer-chosen Banking PINs. In Financial Cryptography and Data Se-curity (FC), 2012
[112]	J. Bonneau.Guessing Human-chosen Secrets. PhD Thesis, University of Cambridge, May 2012
[124]	Implementing Rainbow Tables in High-End FPGAs for Super-Fast Password Crack-ing. Kostas Theocharoulis; Ioannis Papaefstathiou; Charalampos Manifavas. Interna-tional Conference on Field Programmable Logic and Applications, 2010
[131]	Voice Encrypted Recognition Authentication – VERA. Sebastian Szlósarczyk; An-drea Schulte. Next Generation Mobile Applications, Services and Technologies, 9th In-ternational Conference, 2015
[139]	T. Wu, "The Secure Remote Password Protocol", In Proceedings of the 1998 Inter-net Society Symposium on Network and Distributed Systems Security, San Diego, CA, pp. 97-111.
[140]	The Stanford SRP Homepage – Documentation, Demonstration and References: http://srp.stanford.edu/doc.html
[144]	E.Battle P.Cano,T.Kalker,and J.Haitsma, A review of algorithms for fingerprinting. Multimedia Signal Processing,IEEE Workshop on,pp. 169ñ167,December 2002.
[167]	Trusted Computing Group: White Paper Trusted Platform Module (TPM) Sum-mary, 2010.
[180]	Foteini Baldimtsi, Anna Lysyanskaya: Anonymous credentials, 2011.
[184]	Sebastian Szlósarczyk: Master thesis, Anonymous pseudonyms, 2012

where the number in brackets [xx] denotes the number reference in the thesis.