HANDHELD HYBRID OFFLINE OTP AUTHENTICATION FRAMEWORK

BY

BURHAN UL ISLAM KHAN

A thesis submitted in fulfilment of the requirement for the degree of Doctor of Philosophy (Engineering)

Kulliyyah of Engineering
International Islamic University Malaysia

AUGUST 2021

ABSTRACT

Numerous applications are widespread on Internet and mobile communications that transfer personal information and money. Foolproof user authentication becomes imperative in such applications for confirming customer legitimacy. One pragmatic solution for user authentication is that of employing One Time Password (OTP) with validity for a single transaction or session. Two contextually active user authentication models for internet banking in Malaysia include i.) Receiving OTP over the phone via an SMS, ii.) Generating the OTP over a dedicated hardware token provided by the Bank. SMS OTPs are the most common means used for access control over different online applications, especially Internet banking. However, with this setup, the password generated remains afloat in an unsecured cellular network, thereby increasing the probability of security breaches. Additionally, users need to maintain two active communication channels (Cellular & Internet) with the Authentication Server for proving legitimacy. Other inherent problems include delay-in-delivery, coverage areas/unavailability of service, roaming restrictions, dependency on government regulations, etc. Usage of dedicated hardware for OTP generation is also quite popular. Some of these tokens can even generate OTPs asynchronously. However, this setup brings forth additional logistical and administrative burdens for the customers. Besides, users availing multiple service providers need to maintain distinct tokens for each service. The research focussed on developing a standalone authentication framework for generating unique OTPs from trusted handheld devices using a hybrid approach (based on time as well as challenge response strategy), complying with the degree of authentication assertion essential for Internet-banking applications. The prime intent is to eradicate dependence over additional cellular communication channels and eliminate the use of extra hardware tokens for generating/receiving OTPs by Internet banking clients without compromising the security traits of the system. The proposed authentication framework generates time-based dynamic authentication components (OTPs) in an offline manner (without requiring any cellular or internet connectivity) on user's smartphones by invoking possession, knowledge, and inherence factors of legitimate users. This is achieved by asynchronously operating secure random challenge formations as hash counters upon dynamic seeds, comprising of varying current timestamps, distinct device and identity profiles. It drastically reduces the operational costs, improves upon security, scalability, and convenience factors. Additionally, the system has been equipped to generate OTPs as three Bahasa Malaysia dictionary words as the usage of native language words during verification could help clients to feel more confident and secure compared to making foreign-language entries. The system has been implemented and examined for leading mobile/desktop platforms to ascertain its technical adoptability. The results of performance metrics obtained employing the confusion matrix with Accuracy = 98.55%, Error rate = 1.45%, Specificity = 100%, Alarm rate = 0%, Recall = 98.40% and Precision = 100% validate the authentication robustness. The generation and extraction aspects of the hybrid OTP design are comparatively analysed against prior asynchronous/synchronous OTP generation schemes. Furthermore, the authentication framework is comparatively comprehensively parsed for its ability to thwart common authentication attacks over the Internet.

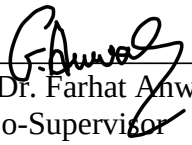
خلاصة البحث

تنتشر العديد من التطبيقات على الإنترنت والاتصالات المتنقلة التي تنقل المعلومات الشخصية والمال. وأصبحت مصادقة المستخدم المضمونة ضرورية في مثل هذه التطبيقات لتأكيد شرعية العملاء. ويوجد حل عملي واحد لمصادقة المستخدم وهو استخدام كلمة مرور لمرة واحدة (OTP) مع صلاحية معاملة أو جلسة واحدة. ويتضمن نموذجان مصادقة مستخدمين نشطين في السياق للخدمات المصرفية عبر الإنترنت في ماليزيا وهما i.) تلقي OTP عبر الهاتف عبر رسالة نصية قصيرة ، ii.) إنشاء OTP على جهاز مخصص للرمز المميز من قبل البنك. OTPs SMS هي أكثر الوسائل شيوعًا المستخدمة للتحكم في الوصول عبر التطبيقات المختلفة عبر الإنترنت ، وخاصة الخدمات المصرفية عبر الإنترنت. ومع ذلك ، مع هذا الإعداد ، فتظل كلمة المرور التي تم إنشاؤها طافية في شبكة خلوية غير آمنة ، وبالتالي زيادة احتمال حدوث خروقات أمنية. بالإضافة إلى ذلك ، يحتاج المستخدمون إلى الحفاظ على اتصالين نشطين في القنوات (الخلوية والإنترنت) مع خادم المصادقة لإثبات الشرعية. وبذلك تشمل المشاكل المتأصلة التأخير في التسليم ، ومناطق التغطية / عدم توفر الخدمة ، وقيودالتجوال ، والاعتماد على اللوائح الحكومية ، إلخ. ويمكن استخدام الأجهزة المخصصة لـ OTPالجيل شائع أيضًا. كذلك يمكن لبعض هذه الرموز المميزة إنشاء برامج تشغيل عبر الإنترنت بشكل غير متزامن. ومع ذلك ، فإن هذا الإعداد يجلب أعباء لوجستية وإدارية إضافية للزبائن. إلى جانب ذلك ، يحتاج المستخدمون الذين يستفيدون من العديد من مزودي الخدمة إلى الحفاظ على رموز مميزة لكل خدمة. ركز البحث على تطوير إطار توثيق مستقل لأنشاء برامج تشغيل OTP فريدة من الأجهزة المحمولة الموثوقة باستخدام نهج هجين (بناءً على الوقت بالإضافة إلى استراتيجية الاستجابة للتحدي) ، الامتثال لدرجة تأكيد المصادقة ضروري لتطبيقات الخدمات المصرفية عبر الإنترنت. القصد الرئيسي هو القضاء على الاعتمادعلي قنوات اتصال خلوية إضافية والقضاء على استخدام رموز إضافية للأجهزة لتوليد / استقبال OTPs من قبل عملاء الخدمات المصرفية عبر الإنترنت دون المساومة على سمات أمن النظام. يولد إطار المصادقة المقترح ديناميكية قائمة على الوقت مكونات المصادقة (OTPs) بطريقة غير متصلة بالإنترنت (دون الحاجة إلى أي خلوي أو اتصال الإنترنت) على الهواتف الذكية للمستخدم من خلال الاحتجاج بالامتلاك والمعرفة وعوامل المستخدمين الشرعيين. يتم تحقيق ذلك عن طريق التشغيل العشوائي الآمن بشكل غير متزامن تشكيلات التحدي حيث يقاوم التجزئة على البذور الديناميكية ، التي تتكون من تيار متفاوت الطوابع الزمنية والجهاز المتميز وملفات تعريف الهوية. إنه يقلل بشكل كبير من تكاليف التشغيل ويحسن عوامل الأمان وقابلية التوسع والراحة. بالإضافة إلى ذلك ، كان النظام مجهزة لإنشاء OTPs على أنها ثلاث كلمات قاموس Bahasa Malaysia مثل استخدام اللغة الأصلية يمكن أن تساعد الكلمات اللغوية أثناء التحقق العملاء على الشعور بمزيد من الثقة والأمان مقارنة بإجراء إدخالات بلغة أجنبية. تم تنفيذ النظام وفحصه لمنصات الهاتف المحمول / سطح المكتب الرائدة للتأكد من قابليتها للتبني الفني. نتائج مقاييس الأداء التي تم الحصول عليها باستخدام مصفوفة الارتباك مع الدقة = 98.55٪ ، خطأ المعدل = 1.45٪ ، النوعية = 100٪ ، معدل التنبيه = 0٪ ، الاستدعاء = 98.40٪ والدقة = 100٪ التحقق من قوة المصادقة. جوانب توليد واستخراج OTP الهجين يتم تحليل التصميم نسبيًا مقابل توليد OTP غير المتزامن / المتزامن السابق المخططات. علاوة على ذلك ، يتم تحليل إطار المصادقة بشكل شامل نسبيًا لقدرتها على إحباط هجمات المصادقة المشتركة عبر الإنترنت.

APPROVAL PAGE

The thesis of Burhan Ul Islam Khan has been approved by the following:

Assoc. Prof. Dr. Rashidah Funke Olanrewaju
Supervisor



Prof. Dr. Farhat Anwar
Co-Supervisor

Prof. Dr. Aisha Hassan Abdalla Hashim
Internal Examiner

Prof. Ts. Dr. Salwani Mohd Daud
External Examiner

Prof. Ts. Dr. Rabiah Ahmad
External Examiner

Assoc. Prof. Dr. Noor Mohammad Osmani
Chairman

DECLARATION

I hereby declare that this thesis is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Burhan Ul Islam Khan

Signature ..... Date .....

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

HANDHELD HYBRID OFFLINE OTP AUTHENTICATION FRAMEWORK

I declare that the copyright holders of this thesis are jointly owned by the student and IIUM.

No part of this unpublished research may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without prior written permission of the copyright holder except as provided below

1. Any material contained in or derived from this unpublished research may be used by others in their writing with due acknowledgement.

2. IIUM or its library will have the right to make and transmit copies (print or electronic) for institutional and academic purposes.

3. The IIUM library will have the right to make, store in a retrieved system and supply copies of this unpublished research if requested by other universities and research libraries.

By signing this form, I acknowledged that I have read and understand the IIUM Intellectual Property Right and Commercialization policy.

Affirmed by Burhan Ul Islam Khan

……..…….. ……..
Signature Date

ACKNOWLEDGEMENTS

All praise and gratitude to Almighty Allah for His countless mercy, sustenance in my life and allowing me to complete this dissertation successfully. It's my privilege to express my heartiest gratitude to my honorable parents and younger brother for their love, sacrifice, endurance and patience.

Secondly, I have to thank my research supervisors: Assoc Prof Dr Rashidah F. Olanrewaju and Prof Dr Farhat Anwar. Without their assistance and dedicated involvement in every step throughout the process, this thesis would never be accomplished. I want to thank you very much for your support and understanding over these past three and a half years. It would be unfair, if not to mention the fact that their contribution to this research is more than this beneficiary.

Getting through my dissertation required more than academic support, and I have many, many people to thank for listening to and, at times, having to tolerate me over the past three years. I cannot begin to express my gratitude and appreciation for their friendship. M. Mueen Ul Islam and Afsah Sharmin, have been unwavering in their personal and professional support during the time I spent at the University. For many memorable evenings out and in, I must thank everyone above as well as Awan Abass, Mohsin Shah, Ahmad Raza, Mohammad Shahdad, Mohammad Aabis, Suhail Aalam and Zaid Shah.

Finally, I must express my very profound gratitude towards Bisma Rasool for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without you. Thank you.

Although not much in worth, still whatever it is, I would like to dedicate the same in whole to the people of Kashmir, who continue to fight the tyranny with whatever means they have, for last seven decades now.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

2FA	Two Factor Authentication
ADC	Alternative Delivery Channel
ADTCXO	Analog Digital TCXO
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AKE	Authenticated Key Exchange
AMD	Advanced Micro Devices
API	Application Programming Interface
ARM	Advanced RISC Machine
ATM	Automated Teller Machine
B2B	Business-to-business
BAN	Body Area Network
BNM	Bank Negara Malaysia
BSD	Berkeley Software Distribution
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CBAC	Context-Based Access Control
CNII	Critical National Information Infrastructure
CPU	Central Processing Unit
CSF	Critical Success Factor
CSS	Cascading Style Sheets
DBMS	Database Management System
DDoS	Distributed Denial of Service

DFD	Data Flow Diagram
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EE	Enterprise Edition
ERR	Equal Error Rate
ESR	Extended Support Release
FAR	False Acceptance Rate
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
FPR	Fast Polynomial Reconstruction
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
GPS	Global Positioning System
GSM	Global System for Mobile communication
GSMA	GSM Association
GUID	Globally Unique Identifier
HMAC	Hash Message Authentication Code
HNWI	High Net Worth Individuals
HOTP	HMAC based OTP
HTML	HyperText Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
I/O	Input/Output
IC	Identification Code
ID	Identification

IDE	Integrated Development Environment
ILHC	Infinite Length Hash Chains
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
iOS	iPhone Operating System
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
ITS	Internet Time Service
IVR	Interactive Voice Response
JCE	Java Cryptography Extension
JCP	Java Community Process
JDBC	Java Database Connectivity
JDK	Java Development Kit
JRE	Java Runtime Environment
JSP	Java Server Pages
JUG	Java User Groups
JVM	Java Virtual Machine
LAMP	Linux, Apache, MySQL, and PHP
LCG	Linear Congruential Generator
LFSR	Linear-Feedback Shift Register
LPCA	Linear Partition Combination Algorithm
MAC	Message Authentication Code
MCC	Mobile Country Code
MD5	Message-Digest algorithm 5

MIPS	Microprocessor without Interlocked Pipeline Stages
MITM	Man-In-the-Middle Attack
MITPhone	Man In The Phone
MMS	Multimedia Messaging Service
MNC	Mobile Network Code
M-OTP	Manageable One Time Password
MSIN	Mobile Subscriber Identification Number
MSISDN	Mobile Subscriber Integrated Services Digital Network Number
mTAN	Mobile Transaction Authentication Number
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
ODBC	Open Database Connectivity
OOP	Object-Oriented Programming
OS	Operating System
OTA	Over The Air
OTN	Oracle Technology Network
OTP	One Time Password
PC	Personal Computer
PGP	Pretty Good Privacy
PIN	Personal Identification Number
POS	Point Of Sale
PSD2	Second Payment Services Directive
RAM	Random Access Memory
RFC	Request for Comments

RGM	Rapid Growth Markets
RIM	Research in Motion
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
RTC	Real-Time Clock
RTS	Regulatory Technical Standards
S/MIME	Secure/Multipurpose Internet Mail Extension
SDK	Software Development Kit
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SPOF	Single Point of Failure
SQL	Structured Query Language
SS7	Signaling System 7
SSH	Secure Shell
SSL	Secure Sockets Layer
TAC	Transaction Authorization Code
TCXO	Temperature-Compensated Crystal Oscillator
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TOTP	Time-based OTP
UI	User Interface
UK	United Kingdom
URL	Uniform Resource Locator
USB	Universal Serial Bus

UTC	Coordinated Universal Time
UX	User Experience
WiFi	Wireless Fidelity
WWW	World Wide Web
XD	Execute Disable
XML	eXtensible Markup Language
ZEBRA	Zero-Effort Bilateral Recurring Authentication
ZITMO	ZeuS in the Mobile

LIST OF SYMBOLS

Ad	Adversary/Attacker on the authentication set-up
Ap_Id	Application Identifier
As	Authentication Server employed by Bank/Service Provider
Bio_Pk	Biometric Passkey
C_Ts	Current Timestamp
C_i	Identity of a valid Internet Banking Customer/User, registered in the service pool of size n
$H^N(x)$	Cryptographic hash chaining with N iterations
IMEI	IMEI Number
IMSI	IMSI Number
K_{seed}	Shared secret seed information
OS_Id	OS Identifier
Qc	4-digit (Q1 Q2 Q3 Q4) challenge sequence from the Authentication Server. Each digit ϵ [1, 9]
S_Id	Service ID
S_i	Registered handheld device of the Customer/User in the service pool of size n
Us_Pp	User Passphrase
δT	Valid time interval for the generated session OTP
$\leftarrow$	Assignment Operator
$\|\|$	Concatenation Operator
$\oplus$	Bitwise XOR Operator

+=	Addition Assignment Operator
~	Weak Approximation
∀	Universal Quantifier
∈	Set Membership
{ }	A collection of elements
^	Exponentiation Operator
[ ]	Closed Interval Notation
≈	Approximation
≤	Inequality symbol denoting 'less than or equal to'