Abstract reading

A broad review on non-intrusive active user authentication in biometrics

Authentication is the process of keeping the user's personal information as confidential in digital applications. Moreover, the user authentication process in the digital platform is employed to verify the own users by some authentication methods like biometrics, voice recognition, and so on. Traditionally, a one-time login based credential verification method was utilized for user authentication. Recently, several new approaches were proposed to enhance the user authentication framework but those approaches have been found inconsistent during the authentication execution process. Hence, the main motive of this review article is to analyze the advantage and disadvantages of authentication systems such as voice recognition, keystroke, and mouse dynamics. These authentication models are evaluated in a continuous non-user authentication environment and their results have been presented in way of tabular and graphical representation. Also, the common merits and demerits of the discussed authentication systems are broadly explained discussion section. Henceforth, this study will help the researchers to adopt the best suitable method at each stage to build an authentication framework for non-intrusive active authentication.

A hybrid scheme for an interoperable identity federation system based on attribute aggregation method

Several countries have invested in building their identity management systems to equip citizens with infrastructures and tools to benefit from e-services. However, current systems still lack the interoperability requirement, which is the core issue that could lower the wide benefits of having an identity management system. In fact, in the existing systems, the user is allowed to choose only one partial identity from an identity provider (IdP) during a single session with a service provider (SP). However, in some scenarios, an SP needs to retrieve information about user's identities managed by multiple IdPs. The potential method to tackle these shortcomings is attribute aggregation from multiple identity providers. A number of initiatives and projects on attribute aggregation have been explored. Nevertheless, these constructions do not fulfill some identity management requirements. This paper describes a new flexible model that aims to provide the necessary mechanisms to ensure attribute aggregation in order to meet the interoperability challenges of current identity management systems. The proposed scheme is a scalable solution, based on identity federation technologies, that introduces a new IdP called an account linking provider (ALP). The purpose of this ALP is to link together different accounts, holding end users' attributes, whenever more than one source of data is needed to grant access to the requested web resource in a single session. Furthermore, the proposed identity federation system is based on a streamlined, cost-effective, and interoperable architecture, which makes this model suitable for large-scale identity federation environments.

A review on electronic payments security

Modern technology is turning into an essential element in the financial trade. We focus the emphasis of this review on the research on the E-wallet and online payment, which is an element of an electric payment system, to get the pattern of using this service. This research presents a review of 131 research articles published on electronic payment between 2010 and 2020 that uses a qualitative method of answering the research questions (RQ): RQ1: “What are the major security issues regarding using electronic payments”? and RQ2: “What security properties need to comply for secure electronic payments?” With the systematic literature review approach, the results show that interest in E-wallet and online payment has grown significantly during this period, and it was found that for the increasing uses of electronic payments, researchers are more focused on security issues. The results show that, to conquer the key gaps, electronic payment must have some protection properties, namely, availability, authorization, integrity, non-repudiation, authentication, and confidentiality. Nowadays, security problems in electronic payment are usually more demanding than the present security problems on the web. These findings can enable electric transaction providers to strengthen their security methods by boosting their security gaps, as required for relevant services.

A survey on multi-factor authentication for online banking in the wild

In recent years, the usage of online banking services has considerably increased. To protect the sensitive resources managed by these services against attackers, banks have started adopting Multi-Factor Authentication (MFA). To date, a variety of MFA solutions have been implemented by banks, leveraging different designs and features and providing a non-homogeneous level of security and user experience. Public and private authorities have defined laws and guidelines to guide the design of more secure and usable MFA solutions, but their influence on existing MFA implementations remains unclear. In this work, we present a latitudinal study on the adoption of MFA and the design choices made by banks operating in different countries. In particular, we evaluate the MFA solutions currently adopted in the banking sector in terms of (i) compliance with laws and best practices, (ii) robustness against attacks and (iii) complexity. We also investigate possible correlations between these criteria. Based on this study, we identify a number of lessons learned and open challenges.

An extensive formal analysis of multi-factor authentication protocols

Passwords are still the most widespread means for authenticating users, even though they have been shown to create huge security problems. This motivated the use of additional authentication mechanisms used in so-called multi-factor authentication protocols. In this paper we define a detailed threat model for this kind of protocols: while in classical protocol analysis attackers control the communication network, we take into account that many communications are performed over TLS channels, that computers may be infected by different kinds of malwares, that attackers could perform phishing, and that humans may omit some actions. We formalize this model in the applied pi calculus and perform an extensive analysis and comparison of several widely used protocols - variants of Google 2-step and FIDO's U2F. The analysis is completely automated, generating systematically all combinations of threat scenarios for each of the protocols and using the PROVERIF tool for automated protocol analysis. Our analysis highlights weaknesses and strengths

of the different protocols, and allows us to suggest several small modifications of the existing protocols which are easy to implement, yet improve their security in several threat scenarios. © 2018 IEEE.

Authentication and Authorization for Mobile IoT Devices Using Biofeatures: Recent Advances and Future Trends

Biofeatures are fast becoming a key tool to authenticate the IoT devices; in this sense, the purpose of this investigation is to summarise the factors that hinder biometrics models' development and deployment on a large scale, including human physiological (e.g., face, eyes, fingerprints-palm, or electrocardiogram) and **behavioral features (e.g., signature, voice, gait, or keystroke)**. The different machine learning and data mining methods used by authentication and authorization schemes for mobile IoT devices are provided. Threat models and countermeasures used by biometrics-based authentication schemes for mobile IoT devices are also presented. More specifically, we analyze the state of the art of the existing biometric-based authentication schemes for IoT devices. Based on the current taxonomy, we conclude our paper with different types of challenges for future research efforts in biometrics-based authentication schemes for IoT devices. © 2019 Mohamed Amine Ferrag et al.

Explainable Security

In 2017, the Defense Advanced Research Projects Agency (DARPA) launched the Explainable Artificial Intelligence (XAI) program that aims to create a suite of new AI techniques that enable end users to understand, appropriately trust, and effectively manage the emerging generation of AI systems. In this paper, inspired by DARPA's XAI program, we propose a new paradigm in security research: Explainable Security (XSec). We discuss the "Six Ws"of XSec (Who? What? Where? When? Why? and How?) and argue that XSec has unique and complex characteristics: XSec involves several different stakeholders (i.e., the system's developers, analysts, users and attackers) and is multi-faceted by nature (as it requires reasoning about system model, threat model and properties of security, privacy and trust as well as concrete attacks, vulnerabilities and countermeasures). We define a roadmap for XSec that identifies several possible research directions. © 2020 IEEE.

Formal Analysis of Mobile Multi-Factor Authentication with Single Sign-On Login

Over the last few years, there has been an almost exponential increase in the number of mobile applications that deal with sensitive data, such as applications for e-commerce or health. When dealing with sensitive data, classical authentication solutions based on username-password pairs are not enough, and multi-factor authentication solutions that combine two or more authentication factors of different categories are required instead. Even if several solutions are currently used, their security analyses have been performed informally or semiformally at best, and without a reference model and a precise definition of the multi-factor authentication property. This makes a comparison among the different solutions both complex and potentially misleading. In this article, we first present the design of two reference models for native applications based on the requirements of two

real-world use-case scenarios. Common features between them are the use of one-time password approaches and the support of a single sign-on experience. Then, we provide a formal specification of our **threat model** and the security goals, and discuss the automated security analysis that we performed. Our formal analysis validates the security goals of the two reference models we propose and provides an important building block for the formal analysis of different multi-factor authentication solutions. © 2020 ACM.

Mobile device integration of a fingerprint biometric remote authentication scheme

Various user authentication schemes with smart cards have been proposed. Generally, researchers implicitly assume that the contents of a smart card cannot be revealed. However, this is not true. An attacker can analyze the leaked information and obtain the secret values in a smart card. To improve on this drawback, we involve a fingerprint biometric and password to enhance the security level of the remote authentication scheme Our scheme uses only hashing functions to implement a robust authentication with a **low computation** property. Copyright © 2011 John Wiley & Sons, Ltd.

MoLaBSS: Server-specific add-on biometric security layer model to enhance the usage of biometrics

With high-paced growth in biometrics, and its easy availability to capture various biometric features, it is emerging as one of the most valuable technologies for multifactor authentication to verify a user's identity, for data security. Organizations encourage their members to use biometrics, but they are hesitant to use them due to perceived security risks. Because of its low usage rate, many medium and small segment organizations find it unfeasible to deploy robust biometric systems. We propose a server-specific add-on biometric security layer model (MoLaBSS) to enhance confidence in the usage of biometrics. We tested this model via a biometric mobile app, and the survey showed a favorable response of 80%. The innovative mobile app was tested for its usability and got a score of more than 71%. For test tool reliability, we examined the equal error rate (EER) of the app and got a reasonably low score of 6%. The results show good potential of this framework to enhance users' confidence level in the usage of biometrics. Higher usage rates may make deployment of biometrics more cost-eective for many organizations to decrease their information security risk. © 2020 by the authors.

MuFASA: A Tool for High-level Specification and Analysis of Multi-factor Authentication Protocols

In recent years, the usage of online services (e.g., banking) has considerably increased. To protect the sensitive resources managed by these services against attackers, Multi-Factor Authentication (MFA) has been widely adopted. To date, a variety of MFA protocols have been implemented, leveraging different designs and features and providing a non-homogeneous level of security and user experience. Public and private authorities have defined laws and guidelines to guide the design of more secure and usable MFA protocols, but their influence on existing MFA implementations remains unclear. We present MuFASA, a tool for high-level specification and analysis of MFA protocols, which aims at supporting normal users and security experts (in the design phase of an

MFA protocol), providing a high level report regarding possible risks associated to the specified MFA protocol, its resistance to a set of attacker models (defined by NIST), its ease-of-use and its compliance with a set of security requirements derived from European laws. © 2020, Springer Nature Switzerland AG.

Multi-factor authentication model based on multipurpose speech watermarking and online speaker recognition

In this paper, a Multi-Factor Authentication (MFA) method is developed by a combination of Personal Identification Number (PIN), One Time Password (OTP), and speaker biometric through the speech watermarks. For this reason, a multipurpose digital speech watermarking applied to embed semi-fragile and robust watermarks simultaneously in the speech signal, respectively to provide tamper detection and proof of ownership. Similarly, the blind semi-fragile speech watermarking technique, Discrete Wavelet Packet Transform (DWPT) and Quantization Index Modulation (QIM) are used to embed the watermark in an angle of the wavelet's sub-bands where more speaker specific information is available. For copyright protection of the speech, a blind and robust speech watermarking are used by applying DWPT and multiplication. Where less speaker specific information is available the robust watermark is embedded through manipulating the amplitude of the wavelet's sub-bands. Experimental results on TIMIT, MIT, and MOBIO demonstrate that there is a trade-off among recognition performance of speaker recognition systems, robustness, and capacity which are presented by various triangles. Furthermore, threat model and attack analysis are used to evaluate the feasibility of the developed MFA model. Accordingly, the developed MFA model is able to enhance the security of the systems against spoofing and communication attacks while improving the recognition performance via solving problems and overcoming limitations. © 2016, Springer Science+Business Media New York.

Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics

The IoT is the upcoming one of the major networking technologies. Using the IoT, different items or devices can be allowed to continuously generate, obtain, and exchange information. Different IoT applications nowadays are centered on computerizing various errands and are attempting to engage the inanimate physical items to act without direct supervision of a human. The current and forthcoming IoT services are exceptionally encouraging to build the degree of solace, proficiency, and automation for the clients. To obtain the option to actualize such a world in a continuously developing manner requires high security, protection, verification, and recuperation from assaults. Right now, incorporating the requisite changes in IoT systems engineering to achieve end-to-end, stable IoT infrastructure is paramount. In this research, a comprehensive analysis is incorporated into the security-relevant problems and **threat wellsprings** in IoT resources or applications. Specific that and current advancements based on maintaining a high degree of confidence in IoT apps are addressed while looking at the security issues. Four distinct developments are investigated, including cryptography, fog computing, edge computing, and ML (Machine Learning), to extend the degree of IoT security. © 2020 Elsevier Ltd

Secure multi-factor remote user authentication scheme for Internet of Things environments

Because of the exponential growth of Internet of Things (IoT), several services are being developed. These services can be accessed through smart gadgets by the user at any place, every time and anywhere. This makes security and privacy central to IoT environments. In this paper, we propose a lightweight, robust, and multi-factor remote user authentication and key agreement scheme for IoT environments. Using this protocol, any authorized user can access and gather real-time sensor data from the IoT nodes. Before gaining access to any IoT node, the user must first get authenticated by the gateway node as well as the IoT node. The proposed protocol is based on XOR and hash operations, and includes: (i) a 3-factor authentication (ie, password, biometrics, and smart device); (ii) mutual authentication; (iii) shared session key; and (iv) key freshness. It satisfies desirable security attributes and maintains acceptable efficiency in terms of the computational overheads for resource constrained IoT environment. Further, the informal and formal security analysis using **AVISPA** proves security strength of the protocol and its robustness against all possible security threats. Simulation results also prove that the scheme is secure against attacks.

Security analysis of unified payments interface and payment apps in India

Since 2016, with a strong push from the Government of India, smartphone-based payment apps have become mainstream, with over $50 billion transacted through these apps in 2018. Many of these apps use a common infrastructure introduced by the Indian government, called the Unified Payments Interface (UPI), but there has been no security analysis of this critical piece of infrastructure that supports money transfers. This paper uses a principled methodology to do a detailed security analysis of the UPI protocol by reverse-engineering the design of this protocol through seven popular UPI apps. We discover previously-unreported multi-factor authentication design-level flaws in the UPI 1.0 specification that can lead to significant attacks when combined with an installed attacker-controlled application. In an extreme version of the attack, the flaws could allow a victim's bank account to be linked and emptied, even if a victim had never used a UPI app. The potential attacks were scalable and could be done remotely. We discuss our methodology and detail how we overcame challenges in reverse-engineering this unpublished application layer protocol, including that all UPI apps undergo a rigorous security review in India and are designed to resist analysis. The work resulted in several CVEs, and a key attack vector that we reported was later addressed in UPI 2.0.

Systematic survey of mobile payments, protocols, and security infrastructure

Mobile payments makeup one of the fastest-growing mobile services available today and are widely used by smartphones for utility payments, bill payments, and online shopping, among other applications. Mobile payments are playing a vital role in the fast growth of online markets and are revolutionizing the supply chain of businesses and industries. Mobile payments are becoming dominant compared to conventional off-line mode payment channels and online e-channels such as ATM, e-cheque, and e-card payments. The success of e-business depends on several factors,

including the type of mobile payment channel used, the associated security infrastructure, the stakeholders involved, and the m-business models adopted. In this paper, we present a systematic literature review (SLR) of mobile payments and characterize the state-of-the-art research conducted in this area, covering articles published during the past two decades, from 2000 to 2020. Following the SLR process, we examined over 350 research papers with a comprehensive and detailed inspection of the mobile payment domain's literature. Based on the analysis, we present the trends, patterns, new technologies, innovations, gaps in the existing literature, and critical challenges. The recommendations given will help identify the primary areas requiring advancement in future research on mobile payment systems.

Two-factor authentication scheme for mobile money: A review of threat models and countermeasures

The proliferation of digital financial innovations like mobile money has led to the rise in mobile subscriptions and transactions. It has also increased the security challenges associated with the current two-factor authentication (2FA) scheme for mobile money due to the high demand. This review paper aims to determine the threat models in the 2FA scheme for mobile money. It also intends to identify the countermeasures to overcome the threat models. A comprehensive literature search was conducted from the Google Scholar and other leading scientific databases such as IEEE Xplore, MDPI, Emerald Insight, Hindawi, ACM, Elsevier, Springer, and Specific and International Journals, where 97 papers were reviewed that focused on the topic. Descriptive research papers and studies related to the theme were selected. Three reviewers extracted information independently on authentication, mobile money system architecture, mobile money access, the authentication scheme for mobile money, various attacks on the mobile money system (MMS), threat models in the 2FA scheme for mobile money, and countermeasures. Through literature analysis, it was found that the **threat models in the 2FA scheme for mobile money** were categorised into five, namely, attacks against privacy, attacks against authentication, attacks against confidentiality, attacks against integrity, and attacks against availability. The countermeasures include use of cryptographic functions (e.g., asymmetric encryption function, symmetric encryption function, and hash function) and personal identification (e.g., number-based and biometric-based countermeasures). This review study reveals that the current 2FA scheme for mobile money has security gaps that need to be addressed since it only uses a personal identification number (PIN) and a subscriber identity module (SIM) to authenticate users, which are susceptible to attacks. This work, therefore, will help mobile money service providers (MMSPs), decision-makers, and governments that wish to improve their current 2FA scheme for mobile money.

Unified threat model for analyzing and evaluating software threats

Design-level vulnerabilities are a major source of security problems in software programs. For the purpose of improving the trustworthiness of software designs, this paper presents a unified threat model for representing, analyzing, and evaluating software threats at various design stages. Unified threat models represent software threats via tree structures with AND/OR logical relationships and evaluates software threats in a cost-effective way based on attack paths. Mitigation measures for

software threats are designed and prioritized based on the evaluation results, which make it possible to design high-quality software security programs that resist identified software threats. A case study for an online banking system is given to systematically demonstrate the application of unified threat models in software threat analysis and evaluation. The results from the case study demonstrate that the unified threat model is superior to traditional threat trees in accurately evaluating results, designing mitigation measures, and guiding software security testing.

Verification of pattern unlock and gait behavioural authentication through a machine learning approach

Purpose: The existing authentication procedures (pin, pattern, password) are not very secure. Therefore, the Gait pattern authentication scheme is introduced to verify the own user. The current research proposes a running Gaussian grey wolf boosting (RGGWB) model to recognize the owner. Design/methodology/approach: The biometrics system plays an important role in smartphones in securing confidential data stored in them. Moreover, the authentication schemes such as passwords and patterns are widely used in smartphones. Findings: To validate this research model, the unauthenticated user's Gait was trained and tested simultaneously with owner gaits. Furthermore, if the gait matches, the smartphone unlocks automatically; otherwise, it rejects it. Originality/value: Finally, the effectiveness of the proposed model is proved by attaining better accuracy and less error rate.