

User's Verification to Prevent Malicious Access in Web-based Forums

Mahdi Taheri Tabar

Faculty of Computing

Universiti Teknologi Malaysia,
81310, Johor, Malaysia

Imran Ghani

Faculty of Computing

Universiti Teknologi Malaysia,
81310, Johor, Malaysia

Mohd Shafie Abd Latiff

Faculty of Computing

Universiti Teknologi Malaysia,
81310, Johor, Malaysia

ABSTRACT

This paper aims to address the issue of malicious accounts that are created and used to imitate real users in web-based forums. In fact, form bots are used to create fake users on forums for several purposes. As a result hundreds of fake users start appearing in the forums and normally placing spam URLs. For forum administrators/managers/moderators, it is a frustrating job to keep members' list clean. In order to overcome this issue, a novel approach is proposed that would be useful in order to prevent malicious users' access and decrease rate of deception in web-based forums. We present a comparison between the proposed approach and IDology approach. The results illustrate that our proposed approach addresses the issue more efficiently as compared with IDology approach.

Keywords

Identity theft, verification service, identity management, malicious users, forums.

1. INTRODUCTION

Forums on the internet are popular and free knowledge sharing platforms to express and share ideas and find answers to questions among millions of users. However, it has been noticed that the users of forum are not always the real people [14]. An apparent real user could be malicious user or a robot whose purpose is to steal information, fraud, share wrong information or even sabotage the system [15]. In this new situation, user's verification has become a vital problem specially after increasing the number of forums on the internet. Thus, there is a need for a mechanism which could help ensure that the users are real people who they claim [7][8].

2. PROBLEM BACKGROUND

Since the advent of web-based forums in 1994, the number of forum users has been continuously increasing. These users, nowadays, report facing problems such as fraud, imitating celebrity people, threatening from people, defamation, posting fake posts and spam URLs (redirecting users to unknown websites) [17]. So the web-based forums have become the easy platforms for attacker to operate their misuse plans. On the other hand forum administrators are not able to track malicious users' accounts. They need to monitor the activities of each user and identify the malicious users and block them, which itself is a time consuming and frustrating job.

Though the forum's developers have taken initiative and trying to block them by using technology like CAPCHA or random questions, however, sometimes this is not considered user-friendly and frustrates the real users in order to create

new profile and benefit from that forum (Rabkin, 2008). In order to address the highlighted issues, this paper presents a 3rd party user's verification service approach.

3. RELATED WORK

A number of Identity management system (IMS) approaches, services and systems have been introduced to over the issue of malicious user's detection and prevention. In the following sub-sections we briefly describe the IMS and services.

3.1 Identity Management System (IMS)

Identity management system (IMS) refers to the administration mechanism to keep the users identity within the organization, a network and even country or maybe the world. It is about managing the roles and privilege of the users. The core objective of IMS is "one identity per individual" [12].

3.2 Identity Verification Services

The online service is used to connect a person's online identity to their real life identity. These services are utilize by some social networking sites, Internet forums, dating sites and wikis to stop sock puppetry, underage sign-ups, spamming and illegal activities like harassment and scams. The identity confirmation process requires the individual whose identity is to be confirmed to provide personal data online, to the identity verification firm. The firm then checks public and private databases for a match and prompts the user to answer questions based on the records. An identity "score" is calculated, and the identity of the online user is either given the "verified" status, or not, based on the score [10][11].

We discuss two of the famous identity verification providers.

3.3 IDology

IDology [16] is an identity and age verification provider founded in 2003. It provides various services to prevent fraud and phishing. Apart from IT related verifications, it also offers other social verifications such as validating age for alcohol and tobacco sales, gaming, rated entertainment, wireless mobile content, subscription based services, online dating, restricted access websites and so on. However this service verifies the users but users must be paid for verification. More over users could not use their verified account in order to login to the other web sites.it must be considered that verification process through this service takes at least one day.

3.4 Trufina

Trufina provides online identity verification and management service. This service enables the individuals to verify their identity and share their verified identity to other internet websites and services. Trufina issues identity cards to its

members called online driver's licenses. With this card, users can create and use different credential in different situations such as online dating, reputation management, and selling or buying goods in online auctions. Trufina permits its members to control which information to be shared with which particular website. In addition, the specific companies that want to check Trufina members verified card should have issued Trufina cards and have a membership account in Trufina service. Then company can ask Trufina member to give them access code in order to have permission to view the member Trufina verified card. The important thing about Trufina is that in order to verify their members they collect

information about members from searching the sources such as county records, state repositories, state departments of corrections, sex offender registries, OFAC terrorism watch list, denied persons list Interpol most wanted [2].

4. PROPOSED APPROACH

This paper presents an external authentication mechanism to authenticate users of forums [5]. The Fig 1 illustrates the identity consumption process.

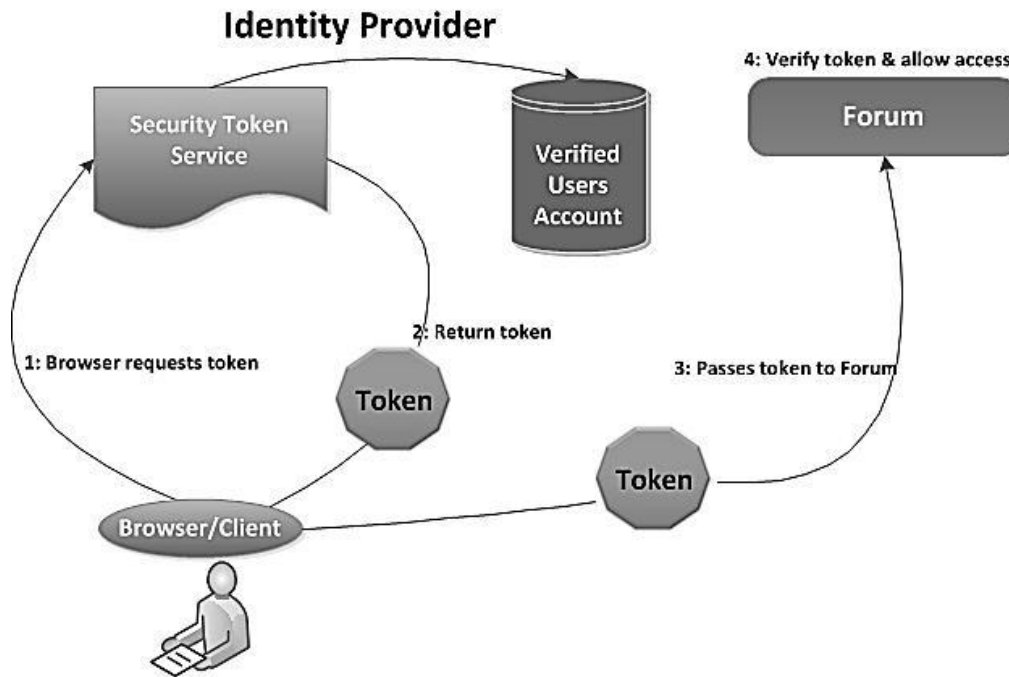


Fig 1 Identity consumption process

The idea is to externalize authentication process beyond the forums and add verification mechanism to authentication process [4][6][9]. The scenario is that, if users need to use forum and forum have partnership agreement with verification service then forum ask user to create verified account in verification service partner. Then after user verifies its information in that service then can use provided information in verification service in order to login to that forum and other partners of verification service.

4.1 How Does Verification Process Works

The sequence diagram (Fig 2) illustrates show the flow of verification process. In Fig 2 there are three main processes as described below.

I. User registration process in verification system:

1. Firstly user registers in the verification system and fill up the registration form. There is one mandatory information about the partner that user needs to provide. The partner that user must select it from provided list of partners from verification system are organizations that could be governmental, private companies, public banks and universities that have partnership agreement with verification system. So those partners provide verified users records to the verification system and verification system use those records to verify users information. it is mandatory for user to choose partner that is able to

provide user records to the verification system. After registration, "successful registration" message is shown to the user.

II. User verification process through verifier partner:

1. In this step user needs to login to the system by using credentials provided in registration process. Then the user sends request for account verification to verification system.
2. Verification system sends user identifier to the partner system. This is the same partner that user selected in registration process.
3. Partner system checks the identifier and if the record is found then it returns the email address of the person being verified.
4. Verification system sends an account verification link to the email address that was retrieved from the partner.
5. Real user receives verification link in his inbox. In order to do verification user needs to click on verification link, so verification request will be forwarded to the verification system.
6. Again verification system asks from partner for user information.

7. Partner sends user information to the verification system.
8. Verification system checks the received user information with information that user provided in registration process hence the user verification is completed.

III. User Login into The Third Party System (Forum) Through Verification System:

1. User visits third party website, but third party website ask the user to login in order to access its contents.
2. As third party uses verification system for login process through the web API. Then user is able to login by

providing the credentials that were used to register the account in verification system.

3. User fills the login form in third party web site and third party sends request to the verification system in order to verify him.

5. Verification system checks if provided credential is valid then it sends true flag to the third party otherwise a false flag is sent.

6. Finally if third party receives true response from verification system then it redirects user to welcome page otherwise access is denied.

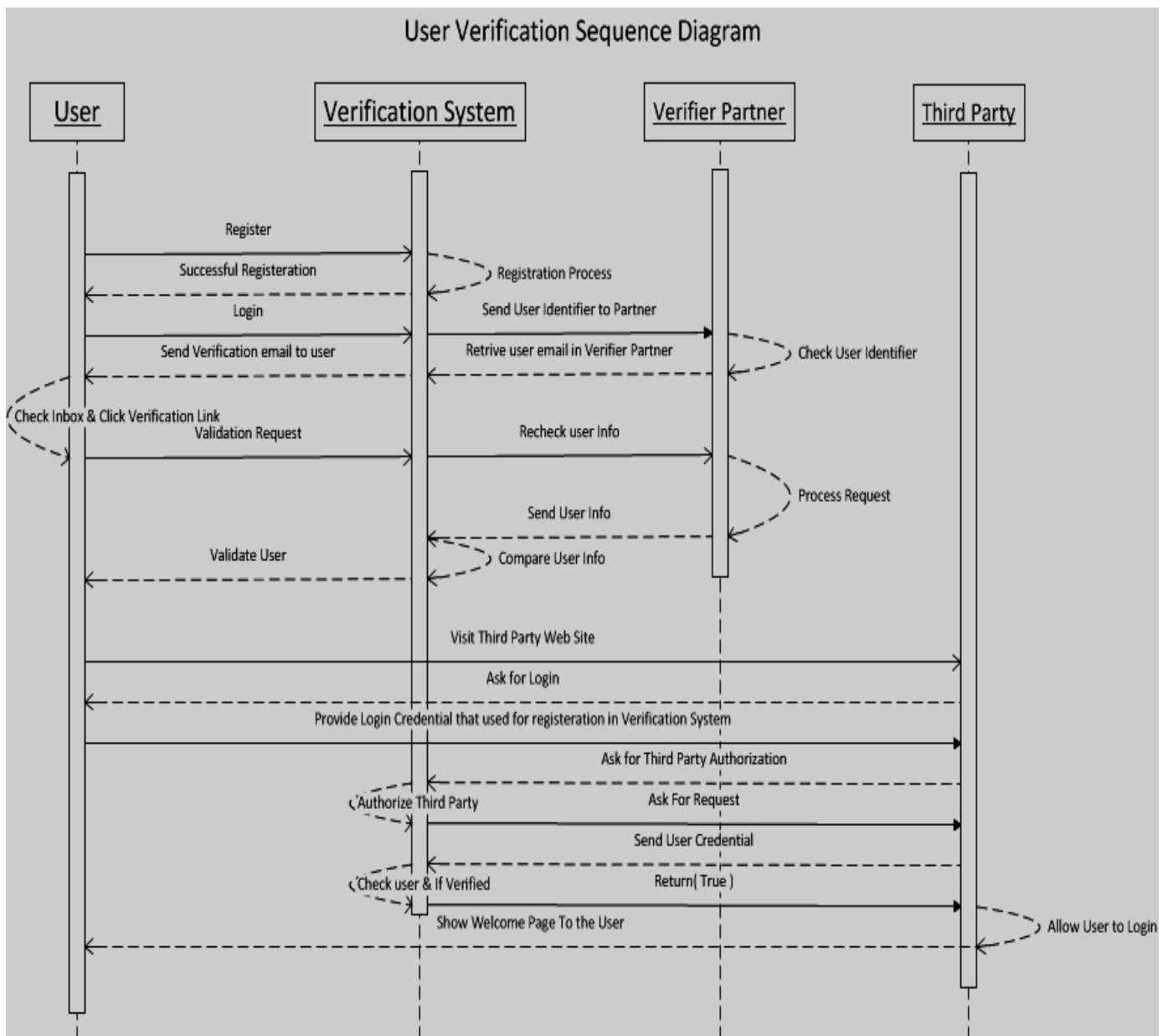


Fig 2: Sequence Diagram

5. EVALUATION OF THE PROTOTYPE

In the following Table 1, technical characterization of proposed verification approach and IDology verification system is presented. The main difference between the

proposed approach and IDology is about verification method. IDology uses phone but the proposed performs verification through 3rd party partner which is faster and free of charge for users.

Table 1. Technical Characteristics of Proposed Approach and IDology

Features	Verification System	IDology
User Self Enrolment	Yes	Yes
Third Party Service Consumption	Yes, Web API	None
Safe connection	SSL , Https	None , Http
Claim your Identity	Any Time Any Where	Must Be Integrated
Cost	Free	Cost
Verification Method	Third Party Partner	Phone
Verification Speed	Less Than 5 Minute	A day
Multi Language	Yes	No
Overall Security	Secure	Secure
Open Source	No	No
OS	Windows,Linux,Mac	Windows,Linux,Mac
Framework	.Net	PHP
Gadget function	Mobile , Tablet	Mobile , Tablet

In table 2 differences between proposed approach and IDology is shown. Another major difference is about consumption of service which in proposed approach the third party can authenticate module easily through Web API (using

SSL) which is part of proposed approach. In IDology, however, third party is only able to claim the user identity and not able to integrate to the authentication and authorization process.

Table 2. Comparison of Proposed Approach and IDology

Features	Verification System	IDology
Third Party Service Consumption	Yes, Web API	None
Safe connection	SSL , Https	None , Http
Claim your Identity	Any Time Any Where	Must Be Integrated
Cost	Free	Cost
Verification Method	Third Party Partner	Phone
Verification Speed	Less Than 5 Minute	A day
Multi Language	Yes	No
Framework	.Net	PHP

The verified user in proposed approach is able to claim its identity to any one in any time. It means you will be able to show that your identity is verified to any people or organizations only by provide your requested identity code to others. Another feature is about that this service is designed for variety of languages and in the prototype support English and Persian. Also it tried to provide free verification service for the users to encourage people that verify their identity.

The comparative analysis between proposed approach and IDology has been performed using Acunetix software [13]. Acunetix software is automatically checks web applications for SQL Injections, cross site scripting and other vulnerability. It also includes a number of advanced penetration testing tools to ease manual security audit processes, and has the ability to create professional security audit and regulatory compliance reports. The comparative analysis is illustrated in Fig 3.

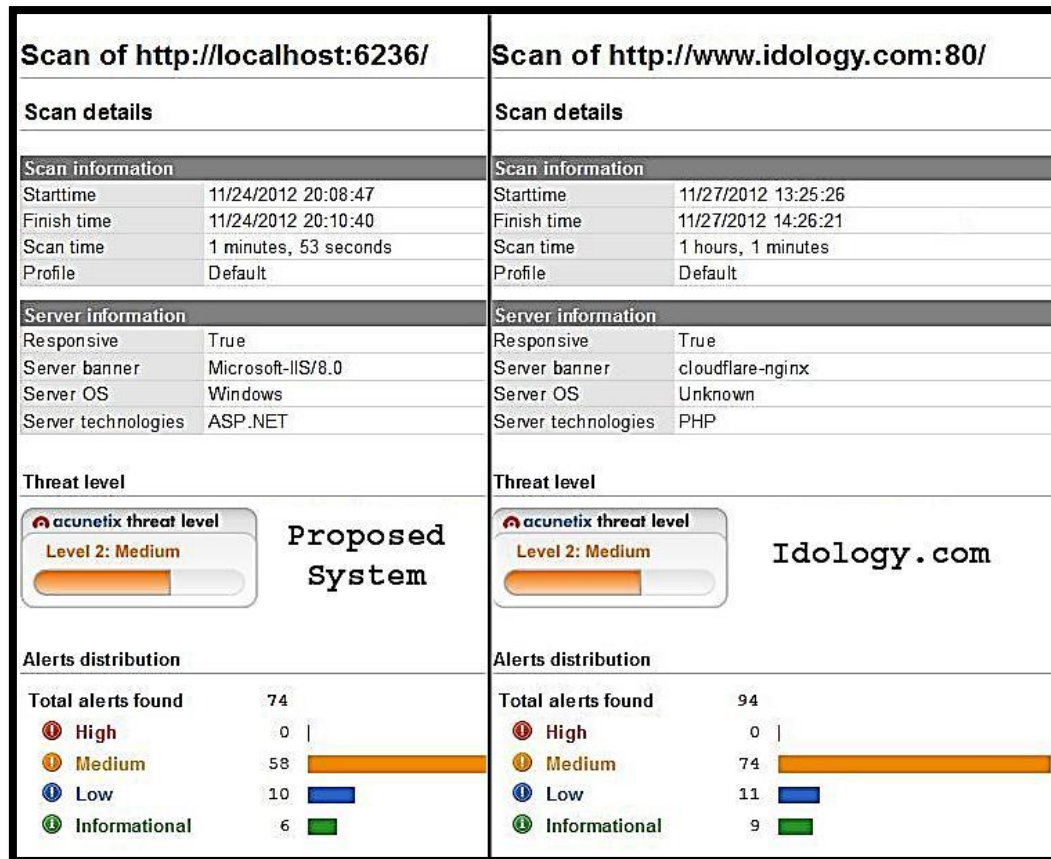


Fig 3 Comparison of Vulnerability Test Report

The report in Fig 3 shows that both systems do not suffer from high level and important vulnerability. Moreover it is obvious that proposed verification approach (left side) has less detected vulnerability in comparison by IDology system (right side). Acunetix software alerts are categorized according to 4 severity levels and show all vulnerabilities found on the target website:

High: Vulnerabilities categorized as the most dangerous, which put a site at maximum risk for hacking and data theft.

Medium: Vulnerabilities caused by server misconfiguration and site-coding flaws, which facilitate server disruption and intrusion.

Low: Vulnerabilities derived from lack of encryption of data traffic, or directory path disclosures.

Informational: Sites which are susceptible to revealing information through Google hacking search strings, or email address disclosure.

6. ACHIEVEMENTS

The main contributions of this paper cover two main aspects. First, we proposed a novel verification approach that can verify the user information faster and free of charge than existing popular system. Second aspect is that we implemented the prototype of the proposed framework that can be used practically in web based forum. Users do not need to create new account in the forum and they just need to provide their credential generated by verification system in order to login to the 3rd party forum then they would be authenticated easily and securely. In addition, following benefits are the by-product of proposed approach.

- Accountability: Each user will be accountable for his online activity because his identity is verified in verification system.
- Avoid bogus accounts: Account registration process eliminated from forums, instead each user could create one verified account in verification system.
- Less effort for design: Reduce the effort of designing authentication module by forum developers.

Other than the above listed features, the verification system could be used for other purposes that are listed:

- Prove you are who you claim: across social networks, dating, online markets and organizations.
- When you share your personal information with someone online, they only see the information you have decided to disclose. Crucially, this will never include enough information to recreate or steal your identity. For example, you may choose to display your age but never your actual date of birth.
- Benefit from this system in online business deals as you can be a verified seller or buyer.

7. FUTURE WORK

Based on the analysis and conclusions derived from this work, there are many related improvement that need further investigation such as use of facial/voice recognition in verification systems in order to improve security of accounts to be hacked by hackers [1][3].

8. CONCLUSION

Account verification is becoming progressively more important these days and it is one of the top priority challenges of cyber space such as forums and social networks. This is because with the digital revolution online activities are increasing rapidly. Thus, this is prime time for malicious users, online hackers and identity thieves to make their move and do some misuse activity through other users' identities. In this research we proposed an approach to verify users online, fast and secure also allowing the third party consumer to benefit from verified accounts in a prototyped verification system. So they could use this system to verify users' accounts instead of registering new users in their system. If this system is widely used by third parties at least users do not need to register new account on many different sites. The proposed verification approach would help to prevent malicious users to access web based forums.

Acknowledgement

This research work has been supported under the grant allocated by Ministry of Science, Technology and Innovation (MOSTI), Malaysia. The grant Vot No. is 4S028.

9. REFERENCES

- [1] Wang, Y., Tan, T., & K. Jain, A. (2003). Combining Face and Iris Biometrics for Identity Verification. Combining Face and Iris Biometrics for Identity Verification. to appear on Proc.AVBPA 2003.
- [2] Trufina. (2011). Retrieved from [www.trufina.com: http://www.trufina.com/new/background_verification.php](http://www.trufina.com/new/background_verification.php)
- [3] Sanderson, C., & K. Paliwal, K. (2001). Robust Face Based Identity Verification. MICROELECTRONIC ENGINEERING RESEARCH CONFERENCE.
- [4] Privaris. (2007). Achieving Universal Secure Identity Verification with. Virginia: Privaris.
- [5] Schejbal, J. (2010). Building an authentication system under strict real-world constraints.
- [6] Netidme. (n.d.). Age and Identity Verification Services. East Kilbride, United Kingdom: Netidme.
- [7] Mercuri, M. (2007). Beginning Information Cards and CardSpace: From Novice to Professional. Apress.
- [8] Kimsal, M. (2007). Intro to OpenID. TriPUG.
- [9] IOCS.Ltd. (2011). Electronic Identity Verification for E-Approval. London: IOCS.Ltd
- [10] Gupta, J. (2007, January 29). Retrieved from [www.readwriteweb.com: http://www.readwriteweb.com/archives/nobody_knows_youre_a_dog.php](http://www.readwriteweb.com/archives/nobody_knows_youre_a_dog.php)
- [11] Weiss, T. R. (2002, December 10). Retrieved from [http://www.computerworld.com: http://www.computerworld.com/article/76558/VeriSign_unveils_new_online_identity_verification_services](http://www.computerworld.com/article/76558/VeriSign_unveils_new_online_identity_verification_services)
- [12] Waters, J. K. (2012). Retrieved from [csoonline: http://www.csoonline.com/article/205053/the-abcs-of-identity-management](http://www.csoonline.com/article/205053/the-abcs-of-identity-management)
- [13] Acunetix Corporation. (2012, December 1). *Home page*. Retrieved December 1, 2012, from Acunetix Corporation Web site: <http://www.acunetix.com/>
- [14] BBC NEWS. (2011, November 24). *Technology*. Retrieved December 2, 2012, from BBC NEWS: <http://www.bbc.co.uk/news/technology-15869683>
- [15] Hindocha, N., & Chien, E. (2003). *Malicious Threats and Vulnerabilities*. Cupertino: Symantec.
- [16] IDology. (2009, July 21). *Press-Release*. Retrieved November 5, 2012, from IDology Corporation Web site: <http://www.idology.com/press-release/idology-approved-as-identity-and-age-verification-provider-for-state-of-kansas>.
- [17] Moore, T., & Anderson, R. (2011). *Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research*. Massachusetts: Harvard University.
- [18] Rabkin, A. (2008). *Personal knowledge questions for fallback authentication: Security questions in the era of Facebook*. Pittsburgh: Symposium on Usable Privacy and Security.