2017

Big Data and the Perceived Expectations Gap in Digital Authentication Processes

Thomas G. Calderon, *The University of Akron*
Colin G. Onita, *University of Akron*

Big Data and the Perceived Expectations Gap in Digital Authentication Processes

Thomas G. Calderon
*Colin G. Onita**

Introduction

Cybercrime has increased almost exponentially since 2000. The most recently published FBI reports show an increase from 262,813 incidents ($781 million loss) in 2013 to 269,422 incidents ($800 million loss) in 2014 (FBI 2013, 2014). According to the Ponemon Institute (2015), cybercrimes cost U.S. companies an annualized average of $15.4 million in 2015, which represented a 21.5% increase compared with 2014. Several recent incidents covered by the financial press highlight the prevalence and costs of cybercrime, including the theft of eighty-one million dollars from a consortium of global financial institutions via the SWIFT system (Corkery 2016; Finkle and Miglani 2016), the hacking of IRS files (Chew 2016), the data breach at the Office of Personnel Management of the U.S. Government (Gillum 2015), the penetration of Sony Pictures networks (Peterson 2014), and theft of personal information of over 100 million customers at JP Morgan Chase (Hurtado and Farell 2015). Many of the reported fraudulent incidents were a result of failures in properly identifying and authenticating entities that initiated financial transactions or accessed financial data (FBI 2013; FBI 2014; FFIEC 2014). Accordingly, a key consideration in fraud risk management is effective authentication and authorization of information systems users.

Users of information technology expect their systems to be secure, reliable, and not vulnerable to fraud. However, recent trends suggest at least a perceived gap between user expectations and the actual state of the security of information systems. Thus, there is a need to understand the public's perceptions of strengths and weaknesses of current and emerging identification and authentication methods. Perceptions of the security and efficacy of technological innovations significantly affect behavioral intentions and the eventual diffusion of such innovations in organizations and the broader society (Yi et al., 2006; Pons and Polak 2008; Ngugi and Kamis 2013; Piccolotto and Maller 2014).

This article uses Twitter as a data source to investigate the public's perceptions of current authentication methods in financial institutions. This data source has not been used previously in the literature to examine perceptions of authentication methods. Yet it offers significant potential as a rich and authentic source of both perceptions and attitudes toward authentication methods that the public actually uses. We focus on the financial sector because of its high vulnerability, the extensive use of information technology in both products and value chain (i.e., its high business information intensity), and the widespread use of online financial services by all entity types (e.g., business, non-profit organizations, governments, and individuals) across geographical and political boundaries. While cybercrime affects all industries, the global financial services industry is hit the hardest with an average annual cost per company of $13.5 million in 2015, compared with an average of about $7.7 million for all industries (Ponemon Institute 2015).

The remainder of the paper presents background information about authentication, including a discussion of the more prevalent approaches to verifying the identity of users of financial systems. Next is an analysis of perceptions about authentication in the financial sector. We close the paper with a discussion of the implications, conclusions, and opportunities for further research.

Background

Most current digital methods for authentication of individuals rely on three main pillars—something that you know, something that you possess and something that you are. The first pillar (something that you know) includes items like passwords, personal identification numbers, paraphrases, codes, secret question and answer combinations, and anything else that an individual knows and can verify the unique identity of the individual. This type of authentication is usually

*The authors are, respectively, Professor of Accounting at the University of Akron, and Assistant Professor of Accounting Information Systems at the University of Akron.

used in conjunction with a user name/number or other type of identification assigned specifically to the individual. The second pillar (something you possess) includes such devices as magnetic and smart cards, physical or digital keys, electronic tokens, one time passwords (OTP) delivered via short message services (SMS) on mobile devices, near field communication (NFC) devices and other devices that when possessed can be used to authenticate the identity of an individual. The last pillar (something you are) is often a unique biometric identifier such as fingerprints, retina scans, facial and voice recognition, palm prints, or infrared body signatures, DNA tests and other methods that can unambiguously detect an individual simply by the person's physical or physiological characteristics. In recent years, another pillar has been added which looks at something you do. This pillar, which is sometimes grouped with biometrics, includes keystroke identification, behavioral identification, and other types of social patterns that are unique to a specific individual.

Something You Know

Authentication based on something you know relies on credentials that include the unique knowledge of an individual that enables them to access computer based information and transaction systems (Chandra and Calderon 2003). In most cases, a system first identifies a user through a unique user name and then uses only one factor (such as a password) to authenticate the user's identity (AlFayyadh et al., 2012).

A user name and password combination is a somewhat vulnerable method of authentication and has many drawbacks. These drawbacks can include poor choice of passwords by users, the inability of individuals to remember long and complex passwords, the reuse of passwords and use of passwords for multiple sites, susceptibility to social engineering and dumpster diving attacks, etc. (Almazyad and Ahmad 2009; Brainard et al., 2006; Karthiga and Aravindhan 2012; Sobotka and Dolezel 2010). User name and password combinations also are vulnerable to phishing attacks, man-in-the-middle attacks, and fake web page schemes (Huang et al., 2011; Yue and Wang 2010).

Given the inherent drawbacks of passwords as a method of authentication, and given the ubiquity of their usage, especially for banking and financial applications, it becomes paramount to find ways of protecting users against credential theft (Garris et al., 2008; Yue and Wang 2010; Yin et al., 2007). One way of ensuring a more secure level of authentication is to use more than one factor in the authentication of users—multi-factor authentication (MFA) (Kim and Hong 2011). The simplest type of MFA is the two-factor authentication, which is usually a combination of something you know and something you have (Liou and Bhashyam 2010). [see Figure I, pg 743]

Something You Have

Two-factor authentication often relies on the individual possessing an item such as a smart card, personal mobile device, or a hand-held token (Liou and Bhashyam 2010; van Thanh et al., 2009). Smart cards have embedded electronic certificates that are used to identify the holder. They are typically used in conjunction with a secret personal identification number (PIN) known only to the user. The combination of the PIN and the smart card is a commonly used MFA.

A frequently used token application contains a number generator that employs an algorithm that is synchronized with an authentication server (van Thanh et al., 2009). This number changes at regular intervals and the user is required to enter the correct number within the interval of time provided along with their user name and password. Authentication hinges on possession of the precise token and an accurate number displayed on the token.

Recent developments in mobile communication technology have seen an increase in the use of mobile phone based OTP methods for authenticating users, especially for authentication in banking and financial institution applications (Gurav and Dhage 2012; Me et al., 2006; Raddum et al., 2010). OTPs are valid for one connection session at a time and are communicated to the user usually via voice or SMS (Aravindhan and Karthiga 2012; Fang and Zhan 2010; Lisoněk and Drahanský 2008; Parameswari and Jose 2011). These types of mobile OTPs are typically used in conjunction with a user name and password. Banks and financial institutions use OTPs sent to a mobile device as a method to conveniently authenticate a user that is engaged in an unusual transaction or accessing a system from an unknown or new computer (Aloul et al., 2009; Almazyad and Ahmad 2009; Singhal and Tapaswi 2012; Sun et al., 2012).

The major drawback associated with the possession-based (something you have) authentication is that users' credentials may be compromised and possibly abused if they lose their tokens or have their authenticating device stolen (Bora and Singh 2013). A further drawback is the potential for the system to be unavailable to a valid user in situations where the token is lost or malfunctions.

Both the single factor and two-factor methods of authentication, based on knowledge or possession, suffer from the drawback of not really ensuring that the person requesting authentication is indeed the legitimate person who should be authorized. These methods only ensure that an entity knows or possess the correct credential. No assurance is offered as to the real identity of the user. Thus, one and two-factor electronic authentication methods that are based on knowledge and possession will not guarantee certification of the identity of the individual requesting authentication nor can they ensure the non-repudiation of the transactions conducted by the true owner of the credential (Kim et al., 2009; Milanovic et al., 2010; Tsai 2002).

These drawbacks can, in part, be mitigated by using an authentication method that is geared toward assuring that a user who presents a credential is indeed the person who owns it. This verification is the premise behind authentication approaches that rely on the physical characteristics or biometrics, of the person requesting authentication.

Something You Are

Authentication based on a user's unique physical or behavioral characteristics (referred to as biometrics) can include fingerprints, voiceprints, hand geometry, retinal or iris scans, handwriting, or keystroke analysis (Bridgwater 2016; Chandra and Calderon 2003). Biometrics can provide strong authentication, but they are susceptible to errors that may not be tolerable in certain applications. Type 1 errors (or false rejections) occur when the system falsely rejects a legitimate user. Type 2 errors (or false acceptance errors) occurs when the system falsely identifies a user who is not authorized as a legitimate user. Furthermore, certain applications of biometrics are vulnerable to spoofing through physical surveillance methods such as voice recordings, fingerprint scanning, or illicit photographing of facial features (Bridgwater 2016).

Risk-Based or Adaptive Authentication Methods

In an effort to mitigate the weaknesses of one, two, or three factor authentications, many practitioners and academicians propose a risk based approach to authentication (Bridgwater 2016; Kim and Hong 2011; Calderon et al., 2006). This approach to authentication seeks to apply stronger authentication requirements to high exposure activities and transactions that are vulnerable to fraud. One approach to risk based authentication is to initially require a one or two-factor authentication, and then incrementally harden the authentication process by posing challenge questions as the user seeks to initiate transactions that increases exposure, vulnerability, and the likelihood of loss. As an entity tries to engage in riskier transactions, this approach blocks access unless the entity answers one or more challenge questions correctly.

Some of the more commonly used methods for risk-based authentication applications rely on a user's device, location, role, activity, and transaction patterns. Device based authentication verifies if the device used to access a financial system is authorized and registered to the user attempting access. This type of risk monitoring relies on IP or MAC addresses of the system and on cookies downloaded on the device for authentication. For location based authentication, the system may allow access to only users who log in from a specific country or geographic location or zip code. The system also may check for uncommon variations in geographic location and blocks access if a variation seems unusual. For example, if a user logs in from San Francisco, and, within a few minutes, logs in again from New York City, the system may tag this situation as unusual and block the user until he/she responds correctly to a challenge question.

Role-based authentication schemes rely on the membership of the user to various classes or categories of users. Often vulnerability, potential for harm, and exposure differ across roles. For example, authorization to add an employee to a group with mortgage approval privileges is inherently riskier than permission to grant read only access to the human resources policies of a bank. Thus, different classes or categories of users may have different levels of access and may require more stringent authentication to be granted access.

Activity based risk estimations take into consideration what the user is likely to do after accessing the system. For example, when a user seeks access to a system that grants permission to perform a large value transaction such as a multi-million-dollar wire transfer, additional authentication steps may be required. Exposure (millions of dollars) and potential for immediate harm (transfer to an imposter) would be significant in such situations. Therefore, it would be necessary to apply stronger authentication measures on users who engage in such transactions.

Finally, transaction pattern or behavioral risk analysis compares current transactions patterns or behaviors with a historical pattern of transactions or behaviors that have been created for the user. If the current transaction patterns differ significantly from the recorded historical transaction patterns, then that may be indication of possible fraud; the system then executes additional authentication steps to ensure that the person engaging in the transactions is authorized to do so. This type of risk based monitoring and authentication scheme is frequently used for credit card transactions.

In a typical financial transaction cycle, users gain access to an enterprise system through a simple one or two-factor authentication method. However, risk-based systems use adaptive algorithms to assess the likely harm and exposure associated with potential transactions and then determine the required hardness of the authentication process. For example, if the assessed level of risk associated with potential user activity is elevated, the system may initiate a challenge process to ensure that the user is properly authenticated and authorized to engage in the activity. [see Figure II, pg 744]

In certain environments, risk and exposure may be extremely high and more innovative methods may be needed to protect financial transactions and business data. Calderon et al., (2006) proposed a continuous authentication (CA) system for globally distributed networks where user profiles are constantly changing. The authors posit that static authentication systems, even if initially secure, authenticate a user only at the start of a session and presume that the user's identity remains the same for the duration of a session. However, some high-risk systems need to verify the identity of a user throughout a session and not just at the start. Calderon et al., (2006, 91) offer "swarm intelligence, which has the capacity to handle complex profile changes, as a technology for implementing CA in a dynamic, distributed network environment where user profiles are constantly changing."

Prior Studies on Perceptions of Security

Prior studies have investigated perceptions of security in several areas, including adoption of biometrics (Pons and Polak 2008; Ngugi and Kamis 2013; Piccolotto and Maller 2014), use of biometrics for ATMs (Byun and Byun 2013), and for physical access in the Hospitality industry (Kim et al., 2008; Morosan 2011; Ko and Yu 2015), comparisons of perceptions of one versus two-factor authentication in banking (Gunson et al., 2011) and perceptions of security tokens for authentication (Weir et al., 2009).

Most studies used surveys, except for Gunson et al., (2011), which used an experiment to compare the use of one factor authentication (password) versus two-factor authentication (token and password) in the banking industry. They report that two-factor authentication was perceived to be more secure than one factor authentication, but also was perceived to be less easy to use and less convenient. Similarly, the perceptions of biometric security were in line with expectations—biometrics were considered more secure than traditional authentication systems, but also less easy to use and less convenient (Kim et al., 2008; Pons and Polak 2008; Morosan 2011; Byun and Byun 2013; Ngugi and Kamis 2013; Piccolotto and Maller 2014; Ko and Yu 2015). Finally, Weir et al., (2009) compared different two-factor authentication methods used in banking and interestingly found that users choose to sacrifice some security to gain usability and convenience.

Prior research uses surveys or experiments to gage the perceptions of individuals regarding authentication methods. No prior study employs large, unstructured data (e.g., Twitter feeds) to gage the perceptions of a larger audience regarding authentication methods.

Research Question and Method

Our primary research objective is to investigate how the public perceives authentication measures employed in the financial sector to minimize the risk of identity theft and reduce fraud. Rather than utilizing a survey or experiment, we used an unstructured "big data" sample that contains perceptions about authentication of a wide, cross section of individuals who are likely to use online banking.

To ascertain authentication methods used in the financial sector, we reviewed the customer authentication processes of a small sample of financial institutions, including the major money center banks, five regional banks, five brokerage services, four insurance companies, and four companies that offer pension and wealth management services. One hundred percent of the investigated sample use an ID/password combination to authenticate users. Most of the organizations permit three tries to enter the correct password and then block the user's access until they successfully respond to a challenge process. The challenge process requires the user to initiate a new session and authenticate through an alternative process such as OTP sent to a mobile device registered to the true owner of the account, an email address, or a landline. Additionally, it is now ubiquitous to employ a challenge question to verify users' identity when they use a computer for the first time or when they seek to undertake a new transaction. Biometrics are used, but mainly to access their mobile devices and ultimately their bank accounts. Thus, financial institutions use all three pillars of authentication described in this paper.

To investigate the perceptions of the public regarding the authentication of individual users of online banking services, we collected social network data from a social network service—Twitter—for the period March 1, 2015 to April 1, 2016. We had access to a random sample of ten percent of the Twitter content for the above period and collected a total of 15,463 tweets in English related to banking authentication, banking identity theft/fraud, authentication fraud, and related key words. Table I shows the specific list of hash tags used for data collection. Furthermore, to ensure that the collected tweets were not biased by comments from specific authentication tools vendors or promoters, we collected data on specific authentication tools and ascertained that it would not pose a statistically significant difference to our results. [see Table I, pg 743]

We used an artificial intelligence system—IBM Watson Analytics (Moreno and Redondo 2016)—that crawled through the unstructured data set and categorized each tweet as exhibiting positive, negative, neutral, or ambivalent sentiment based on a content analysis of the words used by the authors. A small number of tweets were unclassifiable. The system classifies tweets as positive or negative based on the sentiment conveyed in the words used by the author.

Results

Our sample of 15,463 tweets contained 4,236 authors who were male, 1,812 who were female, while the rest had no gender information disclosed. Thirty-nine percent of the authors were based in the United States (6,164), eight percent were from the United Kingdom, and 5.6% were from Canada. Other countries were also represented, albeit in small numbers and many authors chose not to disclose their country of origin (thirty-three percent). The number of tweets was distributed evenly throughout the year with an average of 1187 tweets related to the above topics per month for thirteen months from March 1, 2015 to April 1, 2016. Furthermore, we collected Twitter data on hashtags containing the names and products of the largest four providers of authentication software (Storm 2014). The search resulted in only eighty vendor specific tweets (0.005% of the total number of tweets collected). These vendor specific tweets do not have a statistically significant impact on the results of our analysis.

Of the 15,463 tweets we examined, the system classified 10,588 as neutral, 2763 as positive, 1300 as negative, 573 as undetermined, and 239 as ambivalent (Figure III). Interestingly, only eighteen percent of tweeters have a positive perception of current authentication practices. The clear majority (seventy-eight percent) are ambivalent, negative, or neutral. This result suggests a vast gap between the expectations of tweeters and their actual experiences with digital authentication. The data, however, suggests significant opportunities for business and financial institutions to close the expectations gap since as many as sixty-eight percent of tweeters have a neutral disposition toward the current approaches to authenticating digital identities. [see Figure III, pg 744]

To further understand the sentiments expressed by tweet authors, we examined the specific words used to express positive and negative sentiments associated with the pool of hash tags selected for study (Table I). The results, in the form of word maps, are depicted in Figures IV and V. Word maps show the frequency of words used in tweets by assigning the largest fonts to the most commonly used words. [see Figures IV and V, pg 745]

As seen in Figure IV, the positive sentiment signals relate most probably to specific desirable characteristics of or expectations for effective authentication systems. Words like best, available, and seamless are the most often used in tweets that express positive sentiments. These are followed by such words as tops, stronger, improve, equal, easy, and good. These words also may reflect ways of preventing or recovering from identity incidents. By contrast, the negative sentiment signals (Figure V) are related to the actual breach incident, stolen identities, criminals, scams, and complaints related to incidents.

Perceptions of the Three Pillars

We examined perceptions regarding each of the three pillars of authentication—something you know (#passwords, #paraphrase, etc.), something you possess (#tokens, #smartcards, etc.), and something you are (#biometrics). The results are shown in Figures VI and VII for knowledge, Figures VIII and IX for possessions, and Figures X and XI for biometrics. The results show that in our sample, of the tweets that contained references to knowledge-based authentication (passwords), 4,195 (forty-one percent) tweets contained positive sentiments regarding knowledge, while 997 (ten percent) were negative and 4,923 (forty-eight percent) were neutral. For tweets containing results for authentication based on something one possesses (tokens), 552 (thirty percent) tweets in our sample were positive, eighty-six (five percent) negative and 1,152 (sixty-four percent) neutral. Finally, for biometrics, the sample contained 1,326 (twenty-one percent) positive tweets, 348 (5.5%) negative tweets and 4,614 (seventy-four percent) neutral tweets. [see Figures VI–XI, pg 745]

Biometrics has the widest expectations gap (seventy-nine percent either negative or neutral), followed by tokens (seventy percent either negative or neutral), and then knowledge (fifty-nine percent either negative or neutral). This data suggests that the public perceives authentication based on tokens and other possessions more positively than either passwords or biometrics with tokens having the lowest negative perceptions at five percent of the three authentication pillars. A possible implication is that designers of security might seek to leverage the potential to link the presence of a physical token to a specific individual. Such a link could be readily established by using smart phones and other smart devices to test physical presence of a user as part of the digital authentication process. The data further indicates that more recent authentication methods such as possessions or biometrics are viewed with somewhat more uncertainty than more established methods such as passwords or personal identification numbers (forty-eight percent neutral perceptions for knowledge-based authentication vs. sixty-four percent for possession based and seventy-four percent for biometric based authentication).

Linking the Three Pillars to Identity Theft

We examined the data further to assess the relationship between sentiments about the three pillars of authentication (passwords, tokens, and biometrics) and sentiments about identity theft. If the hashtag #identitytheft was present in a tweet, the #identitytheft variable would be coded as a one; otherwise, it was coded as a zero. This categorical analysis allowed us to identify the relationships between perceptions of biometrics (#biometrics), tokens (#tokens) and passwords (#passwords) and identity theft (#identitytheft).

The data indicated that tweets containing references to biometrics were significantly likely not to contain references to identity theft (p-value <0.001). The results show that of the 15,463 tweets, 7361 contained the hashtag biometrics (forty-eight percent), 6,781 contained identity theft (forty-three percent) and 1,316 (nine percent) continued neither, while only five (<one percent) tweets mentioned both (see Figure XII). In other words, identity theft is almost absent in tweets when the conversation is biometrics. In contrast, about 17.5% of the tweets contain references to identity theft when biometrics are not included in the topic.

Similarly, for the token and identity theft pair, tweets containing the hash-tag “token” were significantly less likely to contain references to identity theft (p-value<.001). A total of 1,751 tweets contained #token, 6,781 tweets contained #identitytheft and 6,841 contained neither (see Figure XIII). Thus, when tokens are present in a tweet, it is unlikely that any of them will contain references to identity theft. Identity theft is mentioned approximately fifty percent of the times when tokens are absent in a tweet. The same was true of the “identity theft” and “password” pair, with tweets containing the hash-tag “password” being significantly less likely to contain references to identity theft (p-value<.001). A total of 7,568 tweets contained the hashtag password, 6,781 tweets contained the hashtag identity theft, and 1,092 contained neither. Only twenty-two tweets contained both the hashtag “identity theft” and the hashtag “password”. [see Figures XII–XIV, pg 746–747]

Conclusions and Suggestions

A key consideration in effective fraud risk management activities must be the authentication and authorization of end users especially since many incidents of fraud can be traced back to improper and ineffective authentication and authorization practices (FBI 2013, FBI 2014, FFIEC 2014). This research investigates the public’s perceptions of various authentication methods used by the financial sector. To achieve this goal, the article employs a new data source (Twitter data), which has not been used before to look at the above topic. Tweets provide insight into what the public thinks about specific topics. Our investigation uncovered an expectation gap in the perception of the efficiency and effectiveness of different authentication methods. Further, our correlation analysis showed that the public does not appear to link identity theft to their choice of authentication method (password-based, token-based, or biometrics-based). This lack of a link can be interpreted as the public being less likely to associate identity theft with any authentication method. Perhaps they associate other factors with identity theft. However, authentication method is not among the factors they appear to consider. Thus, the public seems to expect that even the most basic authentication method will protect them from identity theft and by extension digital fraud.

This expectation gap is something that organizations can reduce by providing stakeholders and the public with a better understanding of the available authentication methods along with the associated benefits and drawbacks. This education is especially important given the broad need for better privacy and security, the cost to remediate digital fraud incidents, and, in general, the need to provide clients with more secure processes for accessing financial services.

Implications for Research

Literature on the effectiveness and efficiency of authentication methods usually employ technical methodologies (e.g., Gurav and Dhage 2012; Liou and Bhashyam 2010; Me et al., 2006; Raddum et al., 2010; van Thanh et al., 2009), small scale perception surveys (e.g., Kim et al., 2008; Pons and Polak 2008; Morosan 2011; Byun and Byun 2013; Ngugi and Kamis 2013; Piccolotto and Maller 2014; Ko and Yu 2015), or experiments (Gunson et al., 2011). This study adds to the current literature by employing a large public dataset (Twitter) to assess the perceptions of individuals regarding specific authentication schemas. We focus specifically on the expectation gap present in public perceptions regarding authentication methods. The public seems to view even simple authentication methods (e.g., passwords, password, and challenge/response) as providing high security and convenience. This type of commonly used authentication has been shown to be somewhat less secure than authentication based on biometrics or tokens. Furthermore, our data shows that the public views biometrics and token-based authentication with greater uncertainty than password-based authentication, which may lead some individuals to forego the use of more secure authentication methods.

The gap between the perceptions of security of the public and actual efficacy can provide a ripe avenue for understanding fraud risk and managing fraud incidents. Future research can explore this gap to better understand the implications for effective security practices at the end-user level and the potential cascading effects across networks. Understanding the association between the extent of the authentication perception gap and specific incidents of digital fraud is a fertile research area. Such research might explore, for example, whether end-users and decision-makers in corporations with wider perception gaps are at higher risk of digital fraud than others who have a narrower authentication perception gap. Similarly, researchers might explore the association between effective response to cyber fraud incidents and the authentication perception gap.

Implication for Practice

Biometrics, tokens, and other advanced authentication solutions have become easier to use and implement. Even so, the public does not seem to view these types of authentication methods as particularly convenient or even secure. Practitioners would be well served in finding ways to better educate the public in the use, efficacy and effectiveness of newer authentication methods, especially in the light of recent cyber security fraud and failure incidents (e.g., Chew 2016; Corkery 2016; Finkle and Miglani 2016; Gillum 2015; Hurtado and Farell 2015; Peterson 2014). Furthermore, since end users perceive multi-factor authentication as providing stronger security than traditional access control methods, application developers might consider deploying more adaptive risk-based controls that leverage multi-factor authentication methods as a preventive strategy to minimize digital fraud, particularly in the financial sector.

Figures and Tables

Table I: Hash Tags Used for Searches

Twitter Hashtags used	#identitytheft #bankingauthentication #authentication #riskbasedauthentication #onlineauthentication #identityfraud #multifactorauthentication #biometrics #authenticatoinfraud #password #token #keycard #smartcard #personalidentificationnumber #pin

Figure I: Traditional Authentication Methods

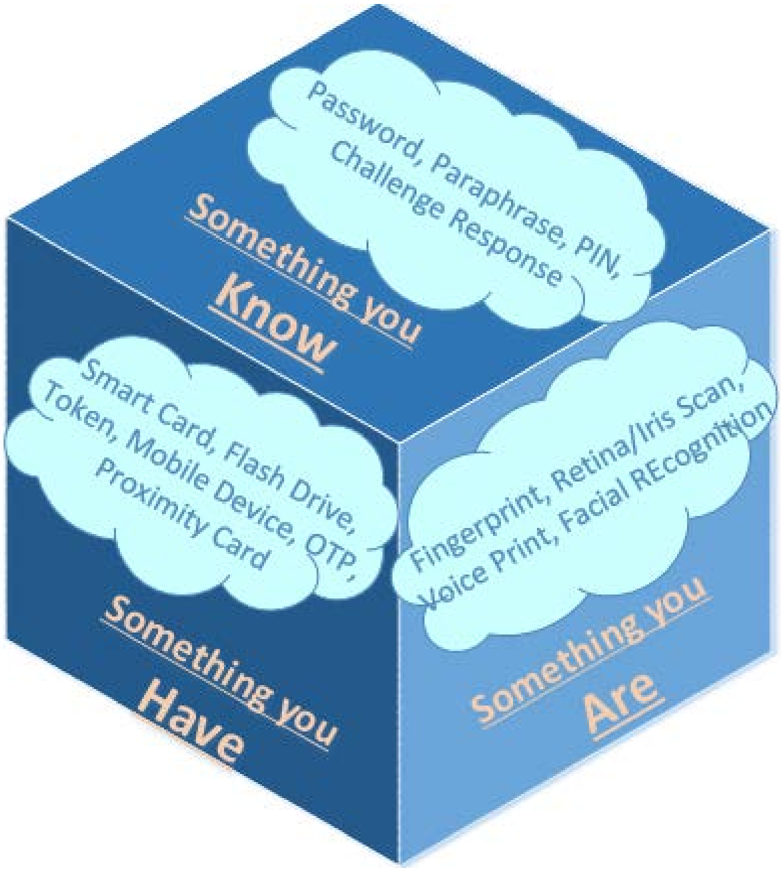
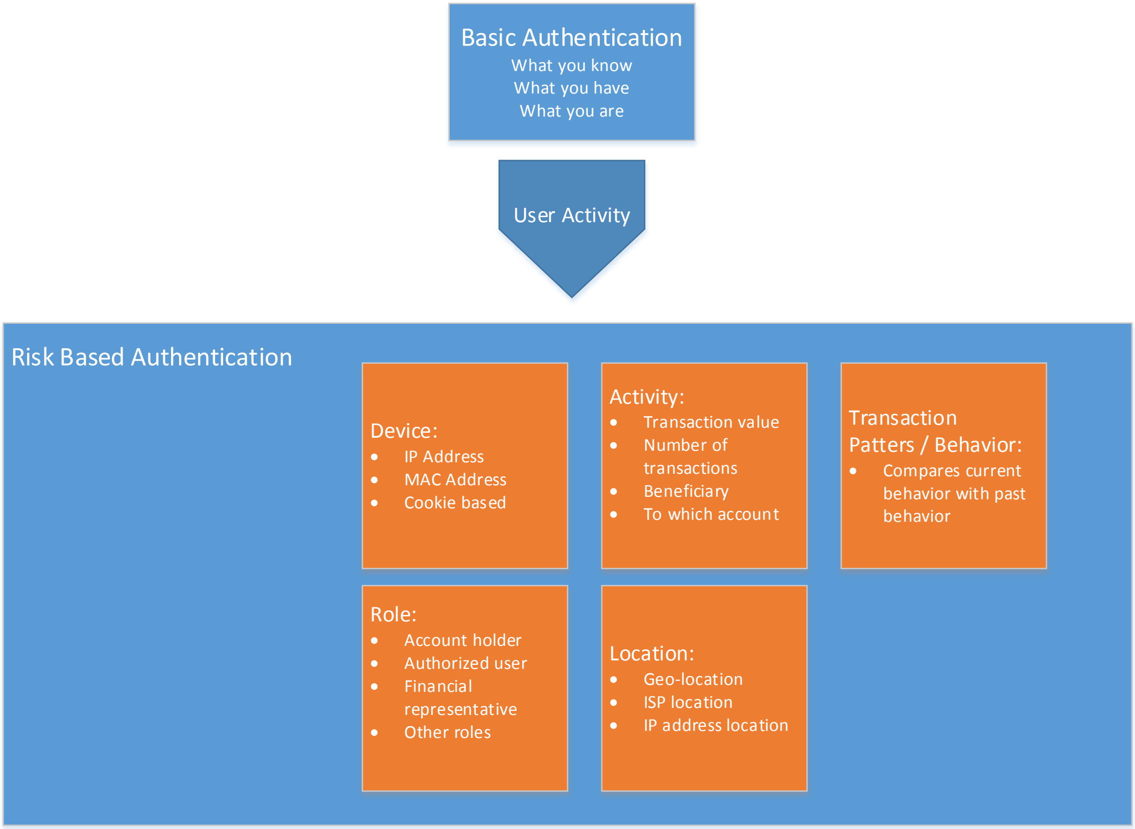

Password, Paraphrase, PIN, Challenge Response
Something you Know
Smart Card, Flash Drive, Token, Mobile Device, OTP, Proximity Card
Something you Have
Fingerprint, Retina/Iris Scan, Voice Print, Facial REcognition
Something you Are

Figure II: Risk Based Authentication



Basic Authentication
What you know
What you have
What you are

User Activity

Risk Based Authentication

Device:
- IP Address
- MAC Address
- Cookie based

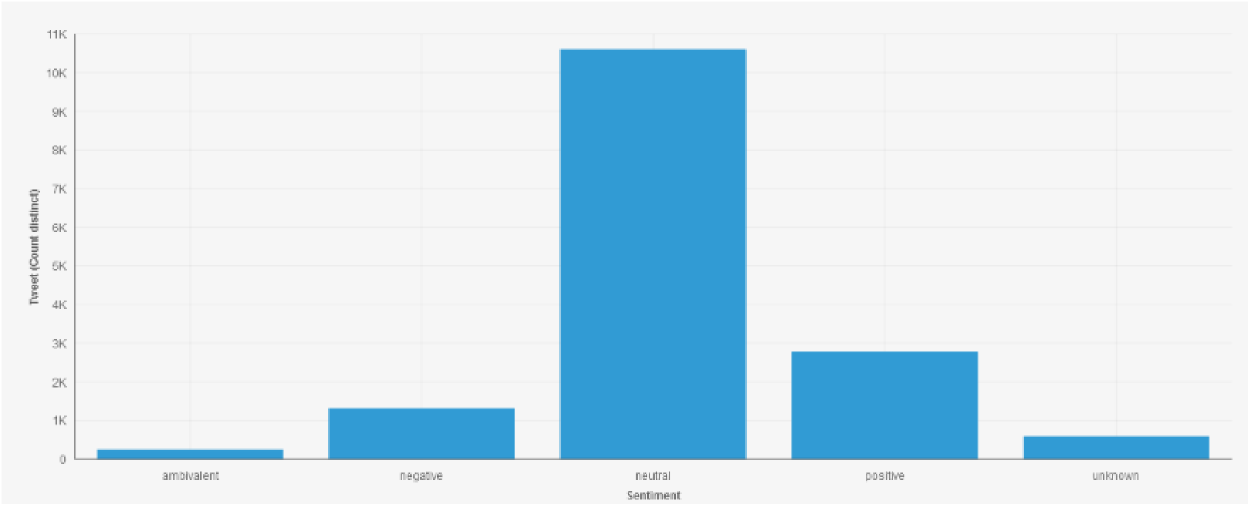
Activity:
- Transaction value
- Number of transactions
- Beneficiary
- To which account

Transaction Patters / Behavior:
- Compares current behavior with past behavior

Role:
- Account holder
- Authorized user
- Financial representative
- Other roles

Location:
- Geo-location
- ISP location
- IP address location

Figure III: Tweets Categorized by Sentiment



Sentiment	Ambivalent	Negative	Neutral	Positive	Unknown	Total
Tweets	239	1,300	10,588	2,763	573	15,463
Percent	2%	8%	68%	18%	4%	100%
Cumulative Percent	2%	10%	78%	96%	100%	

Figure IV: Positive Sentiment Signals for Authentication

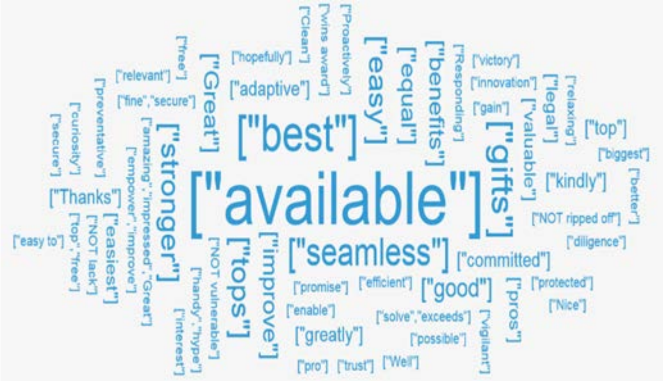


Figure V: Negative Sentiment Signals for Authentication

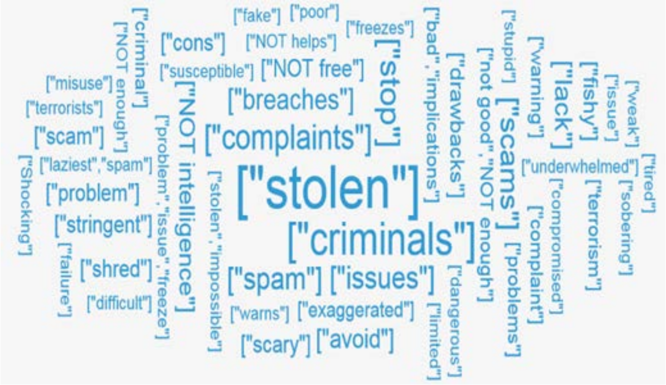


Figure VI: Figure VI: Positive Sentiment Signals for #Passwords

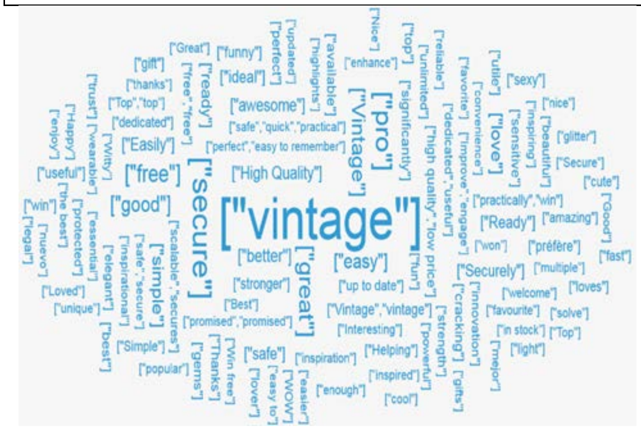


Figure VII: Negative Sentiment Signals for #Passwords

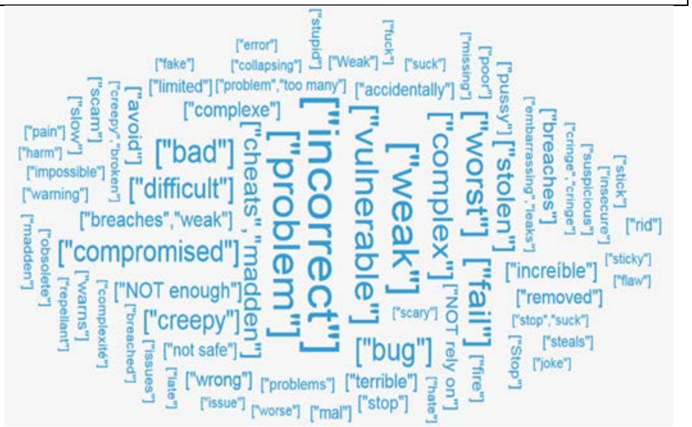


Figure VIII: Positive Sentiment Signals for #Tokens

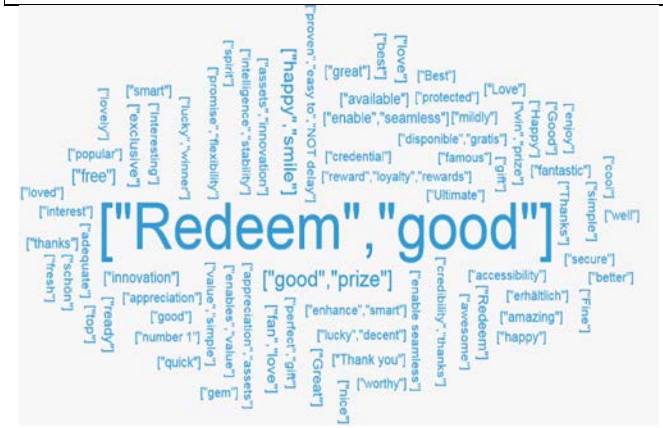


Figure IX: Negative Sentiment Signals for #Tokens

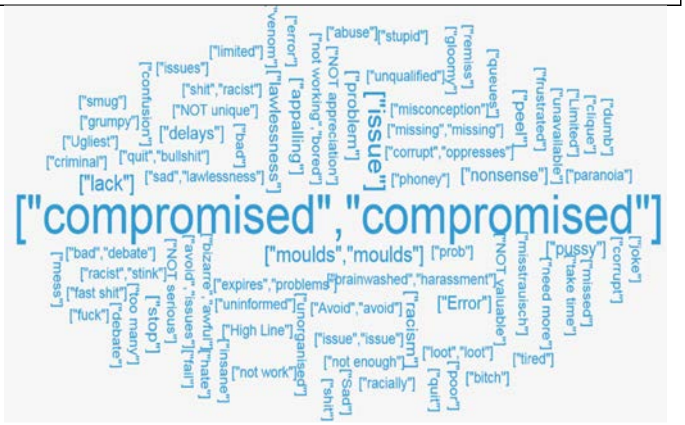


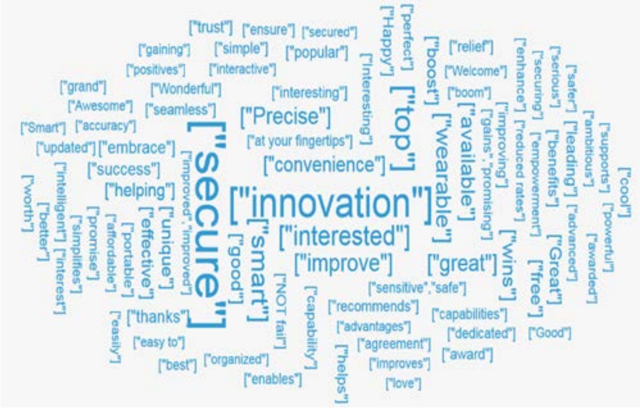
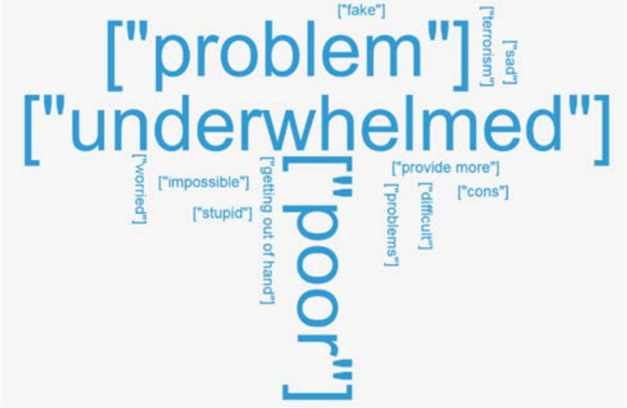
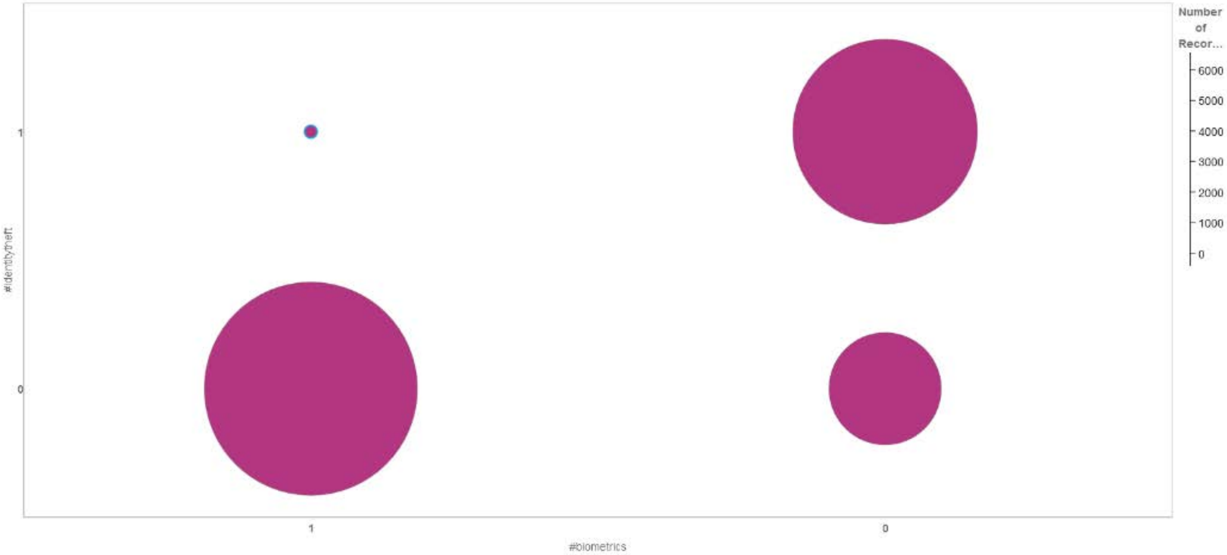
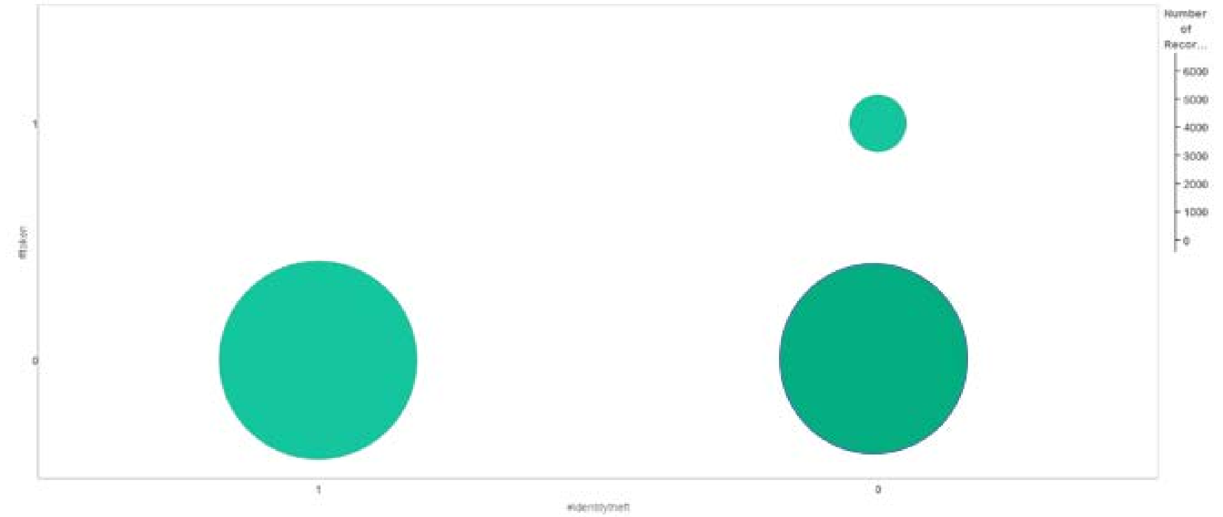
Figure X: Positive Sentiment Signals for #Biometrics	**Figure XI: Negative Sentiment Signals for #Biometrics**
	

Figure XII: Correlation Between Tweets That Contain #Biometrics and Tweets That Contain #Identitytheft



Number of tweets with references to biometrics (1) and identity theft (1); p-value < .001, Chi-Square test of homogeneity.

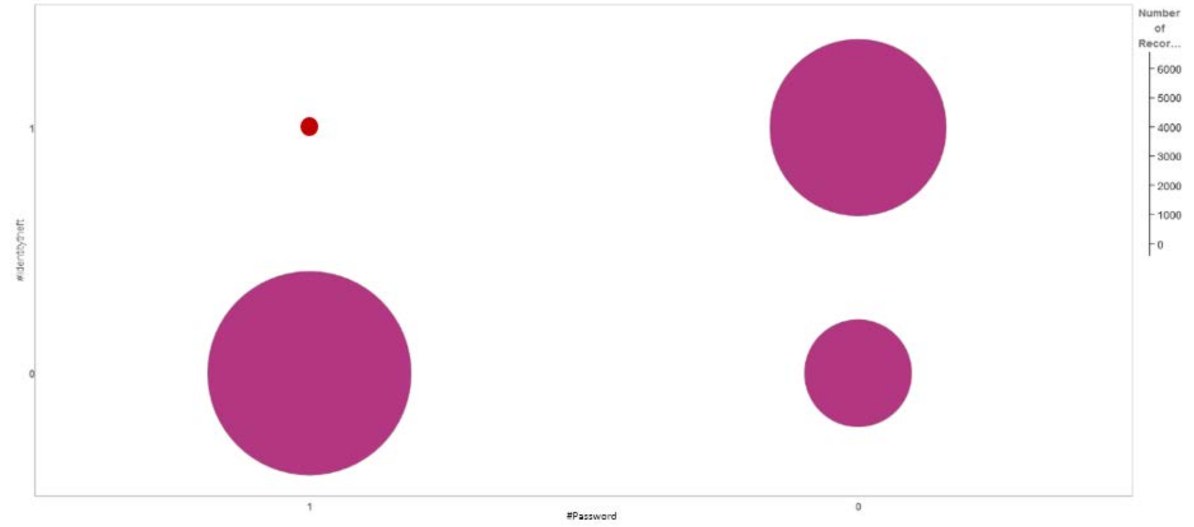
Figure XIII: Correlation Between Tweets That Contain #Token and Tweets That Contain #Identitytheft



Hashtag		Identity theft	
		0	1
Tokens	0	6,841 (44%)	6,781 (44%)
	1	1,751 (12%)	0 (0%)

Number of tweets with references to tokens (1) and identity theft (1); p-value < .001, Chi-Square test of homogeneity.

Figure XIV: Correlation Between Tweets That Contain #Password and Tweets That Contain #Identitytheft



Hashtag		Identity theft	
		0	1
Password	0	1,092 (7%)	6,781 (44%)
	1	7,568 (49%)	22 (<0.1%)

References

AlFayyadh, B., Thorshein, P., Josang, A., and Klevjer, H. (2012). Improving Usability of Password Management with Standardized Password Policies, *Proceedings of the 7th Conference on Network and Information Systems Security* (SAR-SSI), Available at http://folk.uio.no/josang/papers/ATJK2012-SARSSI.pdf, Last accessed 2016.07.07.

Almazyad, A. S. and Ahmad, Y. (2009). A New Approach in T-FA Authentication with OTP Using Mobile Phone. Volume 58, *Communications in Computer and Information Science*. 9–17.

Aloul, F., Zahidi, S. and El-Hajj, W. (2009). Two Factor Authentication Using Mobile Phones. I*EEEXplore*, 641–644.

Aravindhan, K. and Karthiga, R. R. (2013). One Time Password: A Survey. *International Journal of Emerging Trends in Engineering and Development*. 1(3), 613–623.

Bora, M. S. and Singh, A., 2013. Cyber Threats and Security for Wireless Devices. *Journal of Environmental Science, Computer Science and Engineering and Technology* (JECET), 2, 277–284.

Brainard, J., Juels, A., Rivest, R. L., Szydlo, M., and Yung, M. (2006). Fourth-factor authentication: somebody you know. *ACM CCS*, 168–178.

Bridgwater, A. (2016). Biometrically challenged: three-factor authentication systems too weak for web banking. *SC Magazine*. Available at: http://www.scmagazine.com/biometrically-challenged-three-factor-authentication-systems-too-weak-for-web-banking/article/484580/. Last accessed 2016.07.07.

Byun, S., & Byun, S. (2013). Exploring perceptions toward biometric technology in service encounters: A comparison of current users and potential adopters. *Behavior and Information Technology*, 32(3), 217–230.

Calderon, T. G., Chandra, A., and Cheh, J. J. (2006). Modeling an intelligent continuous authentication system to protect financial information resources. *International Journal of Accounting Information Systems*, 7(2), 91–109.

Chandra, A., and Calderon, T. G. (2003). Toward a Biometric Security Layer in Accounting Systems. *Journal of Information Systems*, 17(2), 51–70.

Chew, J. (2016). The IRS Says Identity Thieves Hacked Its Systems Again. *Fortune Magazine*. Available at: http://fortune.com/2016/02/10/irs-hack-refunds/. Last accessed 2016.07.07.

Corkery, M. (2016). Hackers' $81 Million Sneak Attack on World Banking, *NY Times*. http://www.nytimes.com/2016/05/01/business/dealbook/hackers-81-million-sneak-attack-on-world-banking.html?_r=1. Last accessed 2016.07.07.

Fang, X. and Zhan, J. (2010). Online Banking Authentication Using Mobile Phones, in 5th *International Conference on Future Information Technology* (FutureTech), IEEEXplore: Busan. 1–5.

Federal Bureau of Investigation (2013). *Report on Cyber Crime*—FBI, Available at: https://www.fbi.gov/about-us/investigate/cyber. Last accessed 2016.07.07.

Federal Bureau of Investigation (2014). *Report on Cyber Crime*—FBI, Available at: https://www.fbi.gov/about-us/investigate/cyber. Last accessed 2016.07.07.

Federal Financial Institution Examination Council (FFIEC) (2014). *Cybersecurity Assessment General Observations*, Available at: https://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Assessment_Observations.pdf. Last accessed 2016.07.07.

Finkle J., and Miglani S. (2016). Bangladesh Bank heist similar to Sony hack; second bank hit by malware, *Reuters*. Available at: http://www.reuters.com/article/us-usa-fed-bangladesh-idUSKCN0Y40Z1. Last accessed 2016.07.07.

Garriss, S., Caceres, R., Berger, S., Sailer, R., L. van Doorn, and Zhang, X. (2008). Trustworthy and Personalized Computing on Public Kiosks, *6th International Conference on Mobile Systems, Applications, and Services*, 2008, ACgM: USA. 199–210.

Gillum, J. (2015). 21 Million Social Security Numbers Stolen, Feds Say, *US News*. Available at: http://www.usnews.com/news/articles/2015/07/09/more-than-21-million-affected-by-government-hacking. Last accessed 2016.07.07.

Gunson, N., Marshall, D., Morton, H., and Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers and Security*, 30(4), 208–220.

Gurav, T.H., and Dhage, M. (2012). Remote Client Authentication using Mobile phone generated OTP. *International Journal of Scientific and Research Publications*, 2(5), 4.

Huang, C. Y., Ma, S and Chen, K. (2011) Using one-time passwords to prevent password phishing attacks. *Journal of Network and Computer Applications*, 34(4), 1292–1301.

Hurtado, P. and Farell, G. (2015). JPMorgan's 2014 Hack Tied to Largest Cyber Breach Ever, *Bloomberg*. Available at: http://www.bloomberg.com/news/articles/2015-11-10/hackers-accused-by-u-s-of-targeting-top-banks-mutual-funds. Last accessed 2016.07.07.

Karthiga R. R. and Aravindhan K. (2012). Enhancing Performance of User Authentication Protocol with Resist to Password Reuse Attacks. *International Journal of Computational Engineering Research (IJCER)*, 2(8), 106–115.

Kim, H. C., Lee, Y. G., Lee, K. S. and Jun, M. S. (2009). Design and Implementation of Multi Authentication Mechanism for Secure Electronic Commerce, *The 10th ACIS International Conference on Software Engineering, Artificial Intelligences, Networking and Parallel/ Distributed Computing*, 215–219.

Kim, J., Brewer, P., and Bernhard, B. (2008). Hotel customer perceptions of biometric door locks: Convenience and security factors. *Journal of Hospitality and Leisure Marketing*, 17(1), 162–183.

Kim, J. J, and Hong, S. P. (2011). A Method of Risk Assessment for Multi-Factor Authentication. *Journal of Information Processing Systems*, 7, 187–198.

Ko, C. H., and Yu, C. C. (2015). Exploring employees' perception of biometric technology adoption in hotels. *International Journal of Organizational Innovation*, 8(2), 187–199.

Liou, J. C. and Bhashyam, S. (2010). On Improving Feasibility and Security Measures of Online Authentication. *International Journal of Advancements in Computing Technology*. 2(4.1), 11.

Liou, J. C. and Bhashyam, S. (2010). A feasible and cost effective two-factor authentication for online transactions. *2nd International Conference of Software Engineering and Data Mining (SEDM)*, IEEEXplore: Chengdu, China, 47–51.

Lisoněk, D. and Drahanský, M. (2008). SMS Encryption for Mobile Communication. *IEEEXplore*, 198–201.

Me, G., Pirro, D. and Sarrecchia, R. (2006). A mobile based approach to strong authentication on Web, *International Multi-Conference on Computing in the Global Information Technology*, IEEE Xplore, 67.

Milovanovic, M., Bogiüeviü, M., Lazoviü, M., Simiü, D., and Starþeviü, D. (2010). Choosing Authentication Techniques in e-Procurement System in Serbia. *International Conference on Availability, Reliability and Security*, IEEE Xplore, 374–379.

Moreno, A., and Redondo, T. (2016). Text Analytics: the convergence of Big Data and Artificial Intelligence. *International Journal of Interactive Multimedia and Artificial Intelligence*, 3(6).

Morosan, C. (2011). Customers' adoption of biometric systems in restaurants: An extension of the technology acceptance model. *Journal of Hospitality Marketing and Management*, 20(6), 661–690.

Ngugi, B., and Kamis, A. (2013). Modeling the impact of biometric security on millennials' protection motivation. *Journal of Organizational and End User Computing*, 25(4), 27–49.

Parameswari, D. and Jose, L. (2011). SET with SMS OTP using Two Factor Authentication. *Journal of Computer Applications (JCA)*. 4(4), 4.

Peterson, A. (2014). The Sony Pictures hack, explained. *The Washington Post*. Available at: https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/. Last accessed 2016.07.06.

Piccolotto, P., and Maller, P. (2014). Biometrics from the user point of view: Deriving design principles from user perceptions and concerns about biometric systems. *Intel Technology Journal*, 18(4), 30–44.

Ponemon Institute (2015). *Cost of Cyber Crime Study: Global Ponemon Institute Research Report Sponsored by Hewlett Packard Enterprise Independently conducted by Ponemon Institute LLC*. Available at: https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf). Last accessed 2016.07.07

Pons, A. P., and Polak, P. (2008). Understanding user perspectives on biometric technology. *Communications of the ACM*, 51(9), 115–118.

Raddum, H., Nestas, L. H. and Hole, K. J. (2010). Security Analysis of Mobile Phones Used as OTP Generators. *International conference on Information Security and Privacy of Pervasive Systems and Smart Devices*, International Federation for Information Processing (IFIP), ACM: Berlin. 324–331.

Singhal, M. and Tapaswi, S. (2012). Software Tokens Based Two Factor Authentication Scheme. *International Journal of Information and Electronics Engineering*, 2, 383–386.

Sobotka, J. and Doležel, R. (2010). Multifactor authentication systems. *Elektro revue*. 1(1213-1539), 1–7.

Storm. D. (2014). Comparing the top multifactor authentication vendors. *TechTarget.* Available at: http://searchsecurity.techtarget.com/feature/The-fundamentals-of-MFA-Comparing-the-top-multifactor-authentication-products. Last accessed 2016.09.02.

Sun, H. M., Chen, Y. H. and Lin, Y. H. (2012). O-Pass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks. *IEEEXplore*, **7**(2), 651–663.

Tsai, C. H. (2002, Oct. 30-Nov. 1). Non-repudiation in practice. *The Second International Workshop for Asian Public Key Infrastructures*. Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan.

van Thanh, D., Jorstad, I., Jonvik, T., and van Thuan, D. (2009). Strong authentication with mobile phone as security token. *IEEEXplore*, 777–782.

Yin, H. Song, D., Egele, M., Krugel, C., and Kirda, E. (2007). Panorama: capturing system-wide information flow for malware detection and analysis. *ACM conference on Computer and Communications Security*, ACM: USA. 116–127.

Yue C. and Wang Y. (2010). BogusBiter: A Transparent Protection against Phishing Attacks. *ACM*, 10(2), 31.

Weir, C. S., Douglas, G., Carruthers, M., and Jack, M. (2009). User perceptions of security, convenience, and usability for e-banking authentication tokens. *Computers and Security*, 28(1), 47–62.

Yi, M. Y., Jackson, J. D., Park, J. S., Probst, J. C. (2006). Understanding information technology acceptance by individual professionals: Toward an integrative view. *Information and Management*, 43(3), 350–363.