International Journal of Security and Its Applications
Vol.7, No.6 (2013), pp.249-258
http://dx.doi.org/10.14257/ijsia.2013.7.6.25

Analysis on the Attribute Binding based Enhanced User Authentication

Tae Kyung Kim[1] and Jae Hoon Nah[2]
[1]*Dept. Liberal Art, Seoul Theological Univ.*
101 Sosabon2-dong, Sosa-gu, Bucheon-City, Kyonggi, Korea
[2]*Electronics and Telecommunications Research Institute*
Gajeong-ro, Yuseong-gu, Daejeon, Korea
[1]*tkkim@stu.ac.kr*, [2]*jhnah@etri.re.kr*

Abstract

In this paper, we proposed the attribute binding based enhanced user authentication. User authentication is a simple process that is used to determine if an identity is real. Age restricted commerce such as lottery, online gaming, wine & spirits, tobacco, social networking, wireless and others are not invulnerable to the risks associated with identity theft and fraud. And, as this dynamic industry continues to grow, only assessing if a customer is of age will no longer be sufficient. Determining a minimum age needs to be combined with gaining a deeper insight into the validity of an identity along with fraud patters to help protect customer privacy, meet compliance and prevent fraud. The suggested model in this paper can be used to protect the child effectively in the internet environments.

Keywords: *Child Online Protection, Age Verification, Authentication*

1. Introduction

As the number of users using the Internet increases, technical measures are an important element in authentication methods. Technologies can be used to keep certain risks away from users, reversely admit only certain users to specific websites and create safe zones on the Internet.

There are a little problems in the Internet services, such as white washing, ID fraud/spoofing, access to inappropriate contents through Web hard, P2P(peer-to-peer) and so on with regard to user authentication. Methods currently used to authenticate the user identification are various, which can involve credit cards, national ID cards and even face-to-face verification. Reliance on credit cards to establish minimum age is the most widely deployed framework and has been criticized for its many circumvention possibilities such as using parent's credit cards or new forms of pre-paid credit cards [1].

Therefore verification framework is required to verify the user's identification correctly. Technical works already underway related to user authentication are like these: World Wide Web Consortium (W3C) developed POWDER. The POWDER standard is used worldwide as the principal technical platform for dealing with user authentication related content; Internet Watch Foundation (IWF) Board agreed to develop standards and procedures under which a child sexual abuse content URL list would be implemented. Since 2004 many companies worldwide have chosen to make use of this list to protect their customers [2, 3].

ISSN: 1738-9976 IJSIA

2. Related Works

Verifying identities is critical when it comes to stopping fraud against an enterprise. Identity proofing is used to verify identities applying for new accounts or requesting the execution of a high-risk transaction. Many companies supported the identity-proofing services like these [4]:

Verid provides online knowledge-based identity-proofing services, which it calls "knowledge-based authentication" (KBA), using an application service provider model. Verid's value proposition is its usage of multiple public records sources rather than credit data for KBA. The theory behind this was that credit bureau data was increasingly falling into criminal hands, but it would be much more difficult for criminals to gather data on an individual across diverse data sources. Verid dynamically adjusts the questions it asks based on the assessed risk of an online identity. For example, if a new account application is logging in from Iraq but is using a U.S. residential address, the Verid service will ratchet up the difficulty of the questions it asks the applicant to verify their identity.

Aristotle's Integrity service verifies identity and age. It relies completely on public data sources —notably government- issued ID data sources in multiple countries. The service has real-time links to some state motor vehicle databases. Aristotle assures customers against incorrect identity proofing in sales with the potential for underage purchases.

IDology offers three services that verify identity, age or phone number. Its data sources include credit headers, real estate, property and employment records, and numerous other government sources. In addition to performing matches of consumer-provided data against these data sources, IDology offers a service that augments the standard matching with customized challenge questions to the consumer, and the answers can be verified against the data sources. Results can be returned in the form of a pass/fail, a grade, or text message formats that describe a particular condition encountered by the matching algorithms.

Verifying identities of customers, prospects, claimants or other types of users is challenging, and more than 65% of Gartner financial services enterprise clients in the U.S. rely on aggregated public data [4] (when available) to corroborate the authenticity of an individual's claimed identity. This corroboration typically involves asking users questions that only they should know the answers to, such as where they lived or what type of car they drove in the past. The questions and choice of answers (including the correct choice) are served up by public data aggregators, including credit bureaus or other specialty firms.

This identity corroboration process, also known as "out of wallet" knowledge-based authentication, is generally invoked when external users are requesting a high-risk transaction - for example, opening a new account; applying for financing; asking a call center representative sensitive, account-related questions; or requesting a high-value money transfer.

KBA is convenient for enterprises. It does not require special hardware or application programming. It only involves sending key user data (such as name and address) to the KBA service, which then returns a list of stored questions for that user and their choice of answers, including the correct response, which the user must provide to verify his or her identity. This process is commonly used in high-risk interactions with users over the phone, online or in person.

In the past 12 months, however, every client Gartner has spoken to about public-data KBA has complained about high failure rates of at least 10% to 15% with KBA identity verification [5]. Most failures are experienced by legitimate users who cannot answer the questions properly, either because they cannot remember the answers, or because the questions are based on incomplete or incorrect information. This drives up enterprise service costs and user dissatisfaction.

Further, and perhaps more ominously, criminals are sometimes able to answer the KBA questions successfully while impersonating a legitimate user, because they stole the KBA information directly from someone who had access to it, or they were able to cull enough data from Web-based social networks to piece together the answers to the questions themselves.

Therefore to compensate for failures of conventional authentication, adopting an attribute binding approach is needed for an identity proofing that combines several identity attribute. In Chapter 3, we described the architecture of attribute binding based enhanced user authentication model.

3. Attribute Binding based Enhanced user Authentication Model

Identity theft remains one of the more prevalent issues on the Internet today. Electronic authentication guideline [6] defines four levels of assurance, Levels 1 to 4, in terms of the consequences of authentication errors and misuse of credentials. Level 1 is the lowest assurance level, and Level 4 is the highest.

Table 1. Assurance Levels for Multi Token E-Authentication Schemes

	Memorized Secret Token	Pre-registered Knowledge Token	Look-up Secret Token	Out of Band Token	SF OTP Device	SF Cryptographic Device	MF Software Cryptographic Token	MF OTP Device	MF Cryptographic Device
Memorized Secret Token	Level 2	Level 2	Level 3	Level 3	Level 3	Level 3	Level 3	Level 4	Level 4
Pre-registered Knowledge Token	X	Level 2	Level 3	Level 3	Level 3	Level 3	Level 3	Level 4	Level 4
Look-up Secret Token	X	X	Level 2	Level 2	Level 2	Level 2	Level 3	Level 4	Level 4
Out of Band Token	X	X	X	Level 2	Level 2	Level 2	Level 3	Level 4	Level 4
SF OTP Device	X	X	X	X	Level 2	Level 2	Level 3	Level 4	Level 4
SF Cryptographic Device	X	X	X	X	X	Level 2	Level 3	Level 4	Level 4
MF Software Cryptographic Token	X	X	X	X	X	X	Level 3	Level 4	Level 4
MF OTP Device	X	X	X	X	X	X	X	Level 4	Level 4
MF Cryptographic Device	X	X	X	X	X	X	X	X	Level 4

A summary of the technical requirements of the four levels as follows:

1. Level 1 - there is no identity proofing requirement at this level.

2. Level 2 – This level provides single factor remote network authentication.

3. Level 3 – This level provides multi-factor remote network authentication.

4. Level 4 – This level is intended to provide the highest practical remote network authentication assurance.

If we use knowledge based authentication, the attacker might guess a password or Personal Identification Number. Where the token is a shared secret, the Attacker could gain access to the Credential Service Provider or Verifier and obtain the secret value. An Attacker may install malicious software (*e.g.*, a keyboard logger) to capture the secret. Additionally, an Attacker may determine the secret through offline attacks on network traffic from an authentication attempt.

To compensate for failures of knowledge based authentication, adopting an attribute binding approach is needed for an identity proofing that combines several identity attribute

information. By employing a combination of various attributes (system level, application level, service level) concerning a user, the higher levels of assurance can be achieved so that the person being authenticated is truly who they claim to be. It also decreases the likelihood that an attacker successfully impersonates a legitimate user.

In the field of identity proofing, knowledge based authentication has a level 2 assurance. But by using the attribute binding methods with the knowledge authentication, the identity proofing can be a level 3 assurance.

3.1. Enhanced user Authentication by Attributes Binding

In this section, we explained the attribute binding architecture. Combining two or more of factors provides higher levels of assurance that the person being authenticated truly is who they claim to be. It also decreases the likelihood that it is an attacker posing as a legitimate user. And user identification is supposed to periodically check the reliability of user information.

We don't consider biometric authentication in this paper. Biometric authentication by itself can provide mid-level to high-level assurance. However, established, non-biometric alternatives can cost less. Furthermore, the levels of assurance provided by biometric authentication are less concrete. Electronic Authentication Guideline [6] notably omits biometric authentication from its assessment because biometric traits are difficult to copy or share between service providers.

Behavioral analytics is required to enhance the user authentication. This means that the practice of applying analytic techniques such as fusion (using inner joins to combine records from different databases based on common fields) and segmentation (identifying combinations of elements that represent significant groupings of records), to extract actionable intelligence and increase the utility of behavior data. Behavior tracking is the practice of capturing and retaining data about individuals' actions that are considered relevant to an organization. Such data is predominantly, but not exclusively, derived from online (including mobile) activities. It's essentially multichannel in nature, aggregated from a wide variety of sources.

3.2. Attribute Information for Enhanced Authentication

Generally data used in the verification process may come from government agencies or private sources [4]. The three U.S. credit bureaus - Experian, TransUnion and Equifax - have a long history of collecting credit application and transaction data and can draw from those sources. In turn, they also sell credit header information to other IdPSs to be used as a source of data for their services. There are many publicly available data sources that can be used by IdPSs: Social insurance agencies, motor vehicle agencies, property offices, phone databases, bankruptcy courts, criminal justice agencies, business listings, consumer address databases, electoral registers, passport offices, hunting and fishing license agencies, weapons and explosives permit agencies.

But these kinds of data have some privacy issues. When it comes to privacy principles, organizations will need to strike an internal balance based on a careful consideration of the trade-offs involved in certain activities. In this paper, we only consider the technique related information as shown in below Table 2- Table 5.

Attribute information can be the data supplied from all of the components for analyzing a user's authenticity. Generally, information source can be separated into people, application service, technology and environment. In order to monitor the user authentication, all kinds of information is collected and analyzed in each parts. To enable more accurate assessments of

whether a given user should be allowed or denied, all concerned information is incorporated at the time a security decision is made.

The information associated with people can be classified as follows.

Table 2. People Concerning Information

Layer	Example Categories	Example Information
Community	Friends Family Social networks	Relationships Patterns of uptake Presence Links Tagging
Identity	Organization User Group	Reputation of the user Strength of authentication Current role Team membership Transaction amount limit Credit rating

The information associated with application service can be classified as follows.

Table 3. Application Service Concerning Information

Layer	Example Categories	Example Information
Contents	Files Databases Executable content E-mail Input	Sensitivity of content Trust of the content Reputation of executable code Reputation of the e-mail Known vulnerabilities Input from the collective
Application	Application Service Transaction APIs Uniform resource identifier	Reputation of the application Reputation of the URL Sensitivity of the transaction Amount of the transaction Historical patterns of behavior Patch level Known vulnerabilities SLA requirements
Process	Customer facing Revenue producing	Importance of the process Impact on revenue if down SLA requirements Current users of the process

The information associated with technology can be classified as follows.

Table 4. Technology Concerning Information

Layer	Example Categories	Example Information
Operating System	Processes Threads System calls Device drivers Virtualization platform	Historical patterns of behavior State of the OS Patch level Known vulnerabilities Root of trust measurements
Device	Device type Virtual or physical machine IP Address	Reputation of the IP address Device reputation State of the device Storage encryption Strength of encryption
Network	Packets Connection types Port/protocol	Traffic encryption Strength of encryption Historical patterns of behavior Known vulnerabilities

For example, a criminal applying for new accounts in a financial institution will typically use the same one device when applying for multiple accounts. In other cases, the device can be thousands of miles away from a new account applicant's residential address, indicating a potentially suspect applicant. Also, if the user's true IP address indicates that user is sitting behind a known criminal proxy server, the enterprise should flag the access as suspicious.

The information associated with environment can be classified as follows.

Table 5. Environment Concerning Information

Layer	Example Categories	Example Information
Environment	Local environment	Location Prior location Time of the day, month, year Time elapsed since last action

For example, if the user is applying for a new account from a PC located in South Africa, but the user's mobile phone (as listed in the account application) is located in Singapore, the account applicant can be flagged as suspect.

3.3. Attribute Information Sharing Model

There are three standards with considerable momentum in the standards development bodies, but each has different backers and maturity levels. OpenID Connect is primarily for federated authentication and will be an alternative to SAML. OAuth is primarily geared toward authorization but includes authentication elements, and UMA is an administrative specification to allow users to manage access to their resources by others [7].

This paper suggested a model which can share the attribute information between ISPs and third-party vendors. Also, attribute information sharing model must be balanced against concerns for the privacy and security of user information.

As shown in Figure 1, age verification steps are like these:

1. Capture basic customer information such as name and address. Also maintain the ability to collect date of birth or social security information as well.

2. Utilize an age verification platform that is combined with a robust identity solution to conduct an analytical search on billions of trusted data sources and return a result, including any identity discrepancies it finds.

3. Check that returned identity for minimum age requirements and potential fraudulent activity, applying a deep set of fraud detection analytics to help minimize risk and loss.

4. Depending on the results, approve or fail the transaction.

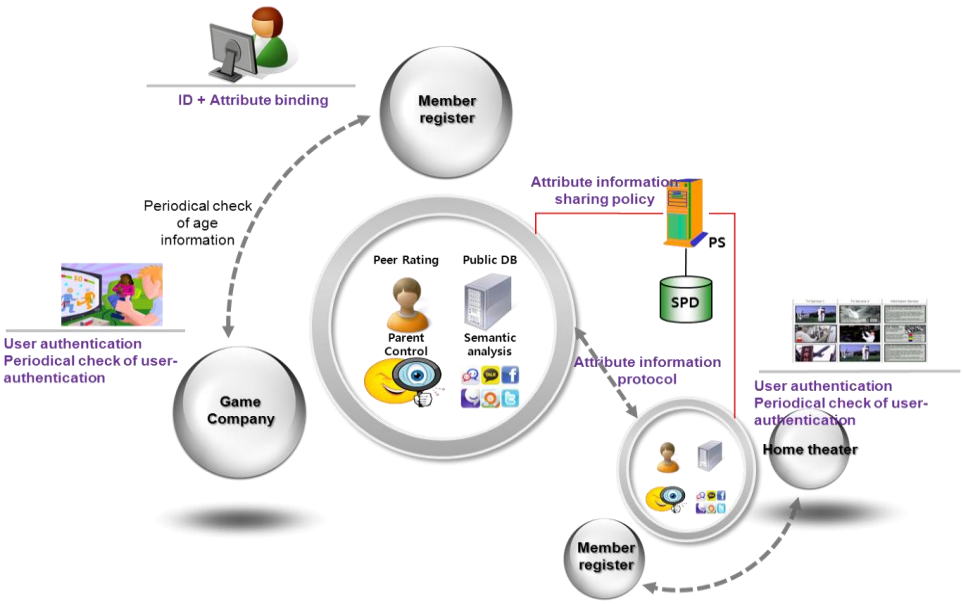

Figure 1. Attribute Information Sharing Model

Enhanced authentication model is shown in Figure 2.

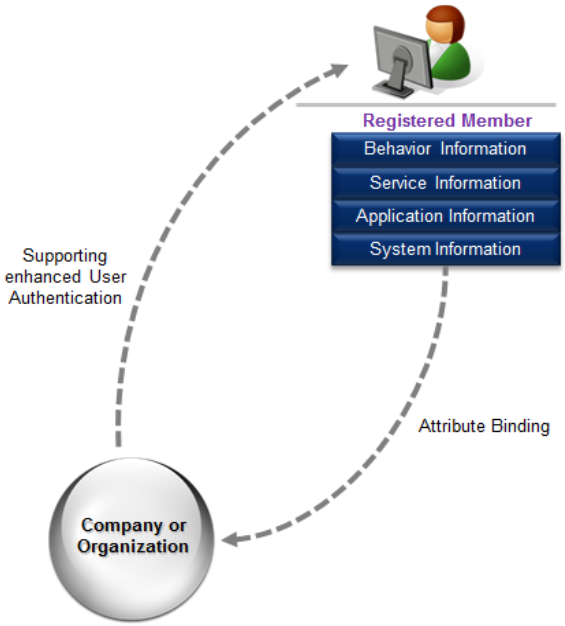

Figure 2. Attribute Binding Model

Attribute binding sources can be system, application, service and behavior information. Each information of user attribute showed in Table 2 - Table 5. Attribute binding procedures are like these:

1. Endpoint analysis: These processes provide the first layer of defense and can detect if the transaction is originating from a suspect location or device. For example device fingerprinting and geolocation analysis service can be done.

Device fingerprinting gathers as much information as possible from the endpoint (e.g., PC or mobile browser characteristics, true IP location, hardware device ID) so that the endpoint can be fingerprinted and correlated with other information that indicates unauthorized or fraudulent access. And geolocation analysis is often a subset of endpoint fingerprinting, but is sometimes used as a stand-alone application. Geolocation analysis seeks to identify the true virtual location of an online user (*e.g.*, by piercing through proxy servers or other anonymizers if necessary) so as to compare that location with what is expected.

2. Navigation analysis: This step analyzes the navigation of a user session to determine if the access appears legitimate or otherwise. The optimal navigation-centric solution will automatically profile and model the behavior of a website's activity so that abnormal sessions stand out as outliers or potential fraud.

3. System analysis: This step analyzes the conditions of user device such as state of the OS, patch level, state of the device, storage encryption etc. Periodically check the user's device conditions to identify the true user device so as to compare that device with what is expected.

4. Pattern analysis: This step analyzes the behavior pattern of user activity using the information such as login time, use time, historical patterns of behavior etc. If unexpected service usage patterns are founded, enhanced authentication methods are performed to confirm a user authenticity.

4. Conclusions

Identity theft remains one of the more prevalent issues on the Internet today. Studies indicate that digital identity fraud is still on the rise, with an increase in sophistication (e.g., phishing, man-in-the-middle, DNS (Domain Name Server) poisoning, malware, social engineering, *etc.*). Authentication methods embrace many different kinds of credentials and mechanisms, often in combination with various form factors.

Multifactor authentication refers to a compound implementation of two or more classes of human-authentication factors: something known to only the user—knowledge-based, something held by only the user—possession-based, and something inherent to only the user—biological or behavior biometric traits. For example, many enterprise extranet/VPN (Virtual Private Network) solutions today require both simple credentials (something known, such as ID (IDentifier) and password) and hardware tokens (something held, such as secure ID with time-based one-time password generators, smart cards that use embedded PKI (Public Key Infrastructure) solutions, and so on) in order to gain access. The combination of the two "known" and "held" factors makes up the multifactor authentication method, and significantly improves the authentication strength, as it curtails the threat of stolen digital identities.

But new attack methods are discovered such as Man-in-the-PC and Man-in-the-Brower attacks. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances.

To compensate for failures of conventional authentication, adopting an attribute binding approach is needed for an identity proofing that combines several identity attribute. By employing a combination of various attributes (system level, application level, service level) concerning a user, the higher levels of assurance can be achieved so that the person being authenticated is truly who they claim to be. It also decreases the likelihood that an attacker successfully impersonates a legitimate user.

Also it can make the user profile by using the attribute binding. The profile can be used to detect the abnormal activity of user. With the conventional authentication methods, this suggested architecture can provide the reinforcement identity assurance by supporting the control of unauthorized access in the back-end.

Acknowledgements

This research was supported by the ICT Standardization program of MISP(The Ministry of Science, ICT & Future Planning).

References

[1] T. K. KIM, "Trends for COP Security Technology", Journal of Information Security", vol. 22, no. 3, pp. 13-18, **(2012)** May.
[2] ITU-T SG17 TD 2506 Rev.2, "Report of the Correspondence Group on COP17 (Child Online Protection/ITU-T)", September 2011-February 2012.
[3] ITU Global Cybersecurity Agenda on Child Online Protection: http://www.itu.int/osg/csd/cybersecurity/gca/cop/index.html.
[4] G. Kreizman and A. Litan, "Identity-Proofing Vendors Differentiate on Techniques and Pedigree", Gartner research, **(2007)** March.
[5] A. Litan, "When Knowledge-Based Authentication Fails, and What You Can Do About It", Gartner research, **(2012)** September.
[6] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-1 "Electronic Authentication Guideline", **(2011)** December.
[7] G. Kreizman, "Evolution of Identity in the Cloud: Take-Aways From the Cloud Identity Summit", Gartner research, **(2011)** August.

Authors

Tae Kyung Kim
1997 : Dankook University, Korea (BS in mathematics education)
2001 : Sungkyunkwan University, Korea (MS in Computer Science)
2005 : Sungkyunkwan University, Korea (PhD in Computer Science)
2008 - Present : Seoul Theological University, Korea (Professor)
Research interests: Network Security, Network QoS, Cloud Computing, and COP

Jae Hoon Nah
985 : Chung-Ang University, Korea (BS in Computer Science)
1987 : Chung-Ang University, Korea (MS in Computer Science)
2005 : HANKUK University of Foreign Studies, Korea (PhD in Computer Science)
1987 - Present : Electronics and Telecommunications Research Institute, Korea (Senior Researcher)
Research interests: IPv6/MIPv6, P2P, IPTV, and Mashup Web Security