Human Factors in Cybersecurity, Vol. 127, 2024, 30–40
https://doi.org/10.54941/ahfe1004763

Biometric Authentication for the Mitigation of Human Risk on a Social Network

Aldrewvonte Jackson[1], Kofi Kyei[2], Yasmin Eady[2], Brian Dowtin[2], Bernard Aldrich[2], Albert Esterline[2], and Joseph Shelton[1]

[1]Computer Science Dept., Virginia State University, St. Petersburg, VA 23806, USA
[2]Computer Science Dept., North Carolina A&T State University, Greensboro, NC 27411, USA

ABSTRACT

The increasing reliance on digital systems in today's interconnected world has brought about a corresponding surge in cyber threats, making cybersecurity a critical concern. While technological advancements have bolstered the defence mechanisms, human factors remain a significant vulnerability. This paper explores the intersection of human factors and cybersecurity, focusing on how biometric authentication can serve as a potent mitigating strategy. The human element in cybersecurity encompasses a range of factors, including user behaviour, cognitive biases, and susceptibility to social engineering attacks. This paper proposes a one-time facial recognition system in conjunction with an online social network, where individuals belonging to the network have their own server participating in the WebID protocol. The WebID protocol enables control of individual identity and representing a network of individuals in a decentralized web of trust. A social network with the WebID protocol consists of trusted individuals, and acceptance can be done through a voting scheme where individuals must be able to vouch for a new member. Controlling the member population of a network can help to prevent against phishing attacks, by restricting communications to only members of the social network. In essence, everyone knows who every other member of the network is or can be reasonably assured that other members can be trusted. However, this is not a perfect system, and biometrics can be used as an added layer of security to prevent successful attacks spurred on by human factors. Additionally, while biometrics-based authentication systems have added security, privacy can be compromised if the network traffic is not properly protected. We will discuss techniques to preserve privacy by representing biometric information in a one-time fashion.

Keywords: Biometrics, Human factors, Cyber security, Semantic web, Convenience technology, Trust

INTRODUCTION

In this digital age, where the majority of people use electronic devices for personal and professional use, where people are networked in some capacity, and where government and corporate institutions are supported by massive infrastructure of devices, cybersecurity is important to prevent people from suffering harm or losses. Cybersecurity solutions are constantly evolving to meet the cyber-attacks that are growing more refined with time. While modern cybersecurity solutions are fairly robust against most attacks (consider trying to solve an encryption algorithm without having the decryption key or attempting to bypass a firewall), the single weak spot of these solutions are the human. Humans may not be properly educated in technical matters and are thus susceptible to social engineering attacks, where their lack of knowledge can be used against them.

With regards to authentication systems, traditional methods such as passwords and PINs, which heavily rely on user memory, are inherently vulnerable to human error, leading to weak access controls and unauthorized access. One key advantage of biometrics is the inherent difficulty in replicating or forging an individual's unique characteristics. Unlike passwords that can be forgotten, shared, or stolen, biometric traits are inherently tied to an individual, providing a more reliable means of authentication. Moreover, the seamless integration of biometrics into daily activities reduces the cognitive burden on users, potentially leading to increased compliance with security protocols. Biometric authentication presents a promising avenue for overcoming the limitations associated with traditional methods. By leveraging unique physiological characteristics, biometrics offer a more secure and user-friendly approach to identity verification.

While biometrics are useful for many networked enterprises, the focus of this paper will be on the semantic web. Semantic Web uses semantic information to show how social networks are connected (Zhou, 2011). A unique character string (URI) designates a logical or physical resource (Nick, 2017) and are used by the Semantic Web to refer to real objects, connections between people, classes, etc. Resources on the Web are described using the Resource Description Framework (RDF). Subject, predicate, and object are the three components that make up the structure of RDF data. The subject is the resource, the predicate is a representation of its attributes or relationships, and the object is a trait value or linked resource (Martin, 2019). Additional methods for organizing data in RDF include using the FOAF (Friend Of A Friend) ontology. Using the foaf:knows properties, some of the triples in the profile's FOAF graph connect the subject to their friends; other triples offer the subject's characteristics, such name. The user is positioned in a community of friends by this graph, helping with authentication (Eady, 2023).

Replacing traditional passwords with biometrics can help to mitigate social engineering attacks, though human privacy is still an important consideration for many individuals. Biometrics can compromise privacy, and we propose a scheme to represent biometrics in a one-time fashion that can still preserve a high recognition rate for accurate acceptance/rejection of individual verification. This is done using a combination of the Local Binary Patterns feature extraction technique (Ahonen, 2017) with evolutionary computation techniques to evolve unique feature extractors (to be used one-time) that also maintain accurate recognition rates. Prior results (Shelton, 2017) have shown this technique to be effective on preliminary datasets; the work shown in this paper will show the effectiveness of this technique in a social network combined with the WebID.

The remainder of this paper is as follows: The next section will discuss biometric recognition, from its introduction to society up until recent trends in biometrics, Following this, we will discuss human factors in cybersecurity, The fourth section will touch on how biometrics can be used as a cybersecurity solution to minimize the threat of human intervention, the fifth section will introduce the Semantic Web as well as integrating biometrics in this framework. It is in this section where we discuss the current state of implementing this framework utilizing the Semantic Web and biometrics. The final section shows the conclusion.

BIOMETRIC RECOGNITION

Biometrics, as a revolutionary aspect of identity verification, encompasses a diverse spectrum of characteristics and methodologies. Defined as the measurement and statistical analysis of unique physical and behavioural attributes, biometrics is primarily classified into two main types. Physiological biometrics relies on inherent, physical features of an individual, exemplified by fingerprints, the intricate contours of facial features, and the distinct patterns of iris recognition. On the other hand, behavioural biometrics delves into the distinctive behavioural patterns exhibited by individuals, ranging from keystroke dynamics, capturing nuances in typing styles, to voice recognition, which analyses vocal characteristics. The advantages of biometrics are evident in its ability to provide a highly secure and personalized means of identification, surpassing traditional methods like passwords. However, this innovation comes with its own set of limitations, such as potential vulnerabilities in the case of compromised biometric data and concerns about privacy. In the realm of cybersecurity, biometrics finds widespread applications. From securing physical access to buildings and devices to safeguarding digital spaces, biometric authentication is increasingly prevalent. Its integration into cybersecurity protocols enhances security measures, offering a more robust defence against unauthorized access and identity fraud. The multifaceted nature of biometrics, encompassing various modalities and applications, underscores its transformative potential in shaping the future of identity verification and cybersecurity.

Physiological Biometrics

Starting off on the physiological side there is facial recognition (Ammour, 2020). Facial recognition can be seen on both a government and personal level. For instance, on government level agencies may use facial recognition when labelling terrorists or criminals. On the personal side facial recognition can be used for logging into or locking devices. Despite the level facial recognition is used on, it is one of the most successful biometric applications. The process that occurs when using facial recognition is first face detection, then feature extraction and then face recognition.

Fingerprint recognition (Liu, 2020) is another physiological biometric that's been commonly used in the recent world of technology as well. Before

Apple started relying solely on facial recognition on their personal devices, they were known to use fingerprint recognition. Fingerprint recognition essentially scans the entire print of the finger and then uses partial fingerprint to save in the database to remember the authorized user. Fingerprint isn't just seen in personal use. Other examples include law enforcement, border control, and consumer biometrics (door access).

Fingerprint recognition is still widely used due to its uniqueness. No person has the same fingerprint as another, even in identical twin instances. Though this form of authentication is widely used it isn't perfect. Issues such as stolen image of a fingerprint, fingerprint extraction from surfaces as well as false fingerprints being made are all major concerns. This is huge because biometrics can't be revoked or reissued unless using the original authenticated feature.

Behavioural Biometrics

Behavioural biometrics (Alsaadi, 2021) can be seen when keystroke, signature, speech or gesture authentication is being used. Though these are still unique forms of biometrics they aren't as commonly used as other physiological types.

Keystroke authentication isn't the most popular use of biometrics but due to its low cost its gaining more usage (Raul, 2020). Along with its low cost it has user transparency, and its non-invasive. The reason behind keystroke not having a lot of usage in today's world is because of the low accuracy of the biometric.

Keystroke authentication works by measuring an individual's typing pattern. This type of biometric can be seen by a team working on a project and remotely logging in on a secured server. This method of made up of the following components. Data collection, feature extraction, feature classification/matching, decision making, retraining and evaluation. The most important component is the feature classification. This component is responsible for categorizing extracted features.

Mouse Dynamics is a behavioural biometrics technology used to validate a user's identity by analysing unique patterns—such as tiny hand motions—detected in the user's interaction with their mouse or pointer. Because it enables continuous authentication, mouse dynamics is a great fit for intrusion detection solutions. Shelton et al. (2013) proposed an authentication approach that attempted to distinguish users based on mouse movement.

HUMAN FACTORS IN CYBERSECURITY

Human factors, within the realm of cybersecurity, constitute the intricate interplay between human behaviour and the digital landscape, significantly shaping the efficacy of security measures. The definition and significance of human factors lie in the understanding that individuals play a pivotal role in the success or failure of cybersecurity protocols. Human factors encompass the cognitive, social, and psychological aspects that influence how individuals interact with technology, making it imperative to comprehend and address these elements to fortify digital defences effectively. However, these factors also introduce vulnerabilities that threat actors exploit. Common human vulnerabilities in cybersecurity include phishing attacks, where individuals may unwittingly divulge sensitive information in response to deceptive emails or messages. Social engineering leverages psychological manipulation to deceive individuals into divulging confidential information or performing actions that compromise security. Additionally, user errors, stemming from inadvertent actions, can lead to unintended security breaches. Human behaviour plays a central role in the success of cyber threats, emphasizing the need for comprehensive cybersecurity strategies that not only acknowledge but actively consider the human element in the defence against evolving cyber threats.

Social Engineering

There are a variety of social engineering attacks that leave individuals in vulnerable positions to give away confidential information. The process of social engineering involves the attacker attempting to tricking an individual through attacks such as phishing and malware. The motive behind the attacks seen in social engineering is for the attacker to obtain this information for reasons such as financial gain. These attacks don't stop there they've also expanded as technology has increased. Telephone calls and face-to-face interactions have displayed recent evolution within social engineering. Methods included within these attacks consist of impersonation, automated social engineering, and semantic attacks. Most social engineering attacks are successfully executed due to human interactions (factors). Cybercriminals specifically hone in on social media hotspots such as YouTube, Facebook and Twitter.

Social engineering can be seen in four different types. Physical, Social, Technical and Socio-Technical. The physical type focuses on attackers performing actions such as searching for personal data, memos, or dumpster diving for personal information. The social type is more commonly used over the other three types of social engineering. This type is mostly seen in relationship building, phishing, and baiting which are conducted via email, text, or phone call. Third, is the technical type. This type is used over the internet. Cybercriminals look over individuals' history and determine how can they put individuals in the most vulnerable position to be susceptible to a successful attack. The attackers also guess passwords to try to obtain the individuals information. Lastly, the most powerful of them all, the socio-technical type. Through combining both social and technical engineering, attackers target the victims' culture, environment, and behaviours to manipulate them. By combining both types the success rate is much greater.

Phishing

Phishing has become a common attack seen throughout the evolution of technology and the internet (Alkhalil, 2017). With technology rapidly evolving throughout the years, there hasn't been a singular or particular definition placed on phishing due to it also rapidly evolving. Though, there is no one particular definition, there is a process that describes phishing. This process is described as cyber criminals tricking recipients to leaking valuable information, being either personal or corporate. Some definitions of phishing that display the process above include replicas of other websites and fraudulent emails that both seek private credentials.

Phishers go about planning their attack by gathering the recipient's information and then choose which process of phishing they think would be most successful. Once the process is chosen, the phisher is tasked with the searching of vulnerabilities based upon the recipient. Next, the trap is set, and the phisher waits for the recipient to bite. After the recipient bites the vulnerable trap, the phishing process is completed and successful. The attacker has full access to the recipient's information.

As mentioned before phishing attacks are becoming more sophisticated as technology is evolving. Even individuals with a considerate amount of knowledge in technology have a hard time recognizing these attacks. Real world examples can be seen through college email systems. One may see an email displaying urgency or a need to fill a position that requires you to put in personal information in order to "obtain the role". Other real-life examples are seen during times of disaster such as Covid-19. Phishers used fraudulent attacks disguised as Covid-19 warning emails to get hospital workers as well as patients to become vulnerable.

Malware

In the same case as phishing, malware is another social engineering attack used by cyber criminals as technology has evolved throughout the years. That said, it is much different than the phishing process. Malware is considered to be malicious software that is implemented and has taken control over an individual's machine ranging from computers, phones and computer networks (Abraham, 2010). One may see malware in the form of virus, ransomware, and Trojan horse. Once these methods successfully attack the victim's system, it directly damages the system, allows remote code execution, or steals confidential data.

Just as phishing has evolved over the years so has malware. Malware used to be seen as "Traditional Malware". This was due to it being relatively simple to detect and defend against in its early stages of development. Currently, malware is harder to detect and defend against and is seen in "Kernel mode". This type of malware is most commonly known as "New generation malware". It is extremely more potent than the earlier stages of malware. It can bypass protection software such as firewalls and antivirus software. These software's are supposedly capable of detecting "Kernel mode" malware but "New generation malware" bypasses it without hesitation. The current generation of malware disguises itself so well by using different processes being new and old, then combines them into one.

Malware files today are created by the millions each day with mobile malware on the rise. Commonly seen malware attacks on mobile devices are seen as fraudulent applications and banking Trojans. As well as, social media, cloud computing, healthcare industry and cryptocurrency related malware attacks. To resolve these issues caused by this malware, new innovative software needs to be able to detect current or new generation malware.

INTEGRATION OF BIOMETRICS AND HUMAN FACTORS

The integration of biometrics and human factors represents a pivotal frontier in the quest for fortified cybersecurity. In the pursuit of strengthening authentication protocols, one transformative approach involves multi-modal biometrics. This entails the simultaneous utilization of multiple biometric identifiers, such as fingerprints, facial recognition, and voice patterns, to enhance the accuracy and reliability of identity verification. Additionally, continuous authentication emerges as a dynamic strategy that adapts to evolving scenarios. Unlike traditional authentication methods that grant access once, continuous authentication continuously verifies the user's identity throughout an interaction, thereby mitigating the risk of unauthorized access even after the initial login. This integration not only fortifies security but also addresses human vulnerabilities. By incorporating biometric solutions, organizations can counteract threats such as phishing attacks and social engineering, leveraging the uniqueness of physiological or behavioural traits for robust identification. However, this fusion of biometrics and human factors is not without challenges and ethical considerations. The inherent risks include potential breaches of privacy and concerns regarding the secure storage and handling of biometric data. Ethical considerations encompass issues such as consent, transparency, and the responsible use of biometric information. Striking a delicate balance between maximizing security and respecting individual privacy and ethical standards remains a critical aspect of navigating this intricate integration. In essence, the harmonious integration of biometrics and human factors holds immense potential for fortifying cybersecurity measures, but a thoughtful and ethical approach is paramount to ensure its effectiveness and societal acceptance.

BIOMETRICS AND THE SEMANTIC WEB

The semantic web is a proposed evolution of the existing web in which all data is machine readable. This allows for relationships between entities to be formally represented, which allows for analysis of the relationships. This is relevant when proposing social networks where trust can be determined between two entities (which can be devices, individuals, etc.), and then a degree of trust can be extended to connected entities, forming a graph of connected entities. The semantic web can be enabled to allow individuals to join if they are "trusted" enough, and certain actions can be allowed depending on the measure of trust. This semantic web can be implemented in an informal setting of colleagues who just want to socialize, or for a dedicated group who are collaborating on some open-source project, or even in a company setting working on company projects. This approach can be useful for preventing human error in cybersecurity as individuals must be able to prove some measure of trust, which can help to prevent phishing attempts from individuals not belonging to the network.

To establish identity, the concept of WebID must be introduced. WebIDs are a way to uniquely represent some entity (individual, company, organization) using a Uniform Resource Identifier (URI). The URI can take the form of a name, location, or some public key. A digital certificate can be used to enable authentication by linking a certificate to an individual's device and the private key information will be set inside of the certificate. If attempting to authenticate, the key information from the certificate must match the public key that is associated with the individual. Some works to note in this area are shown in Kyei 2023, where the authors proposed a strategy for allowing potential members into a network, and voting for each individual belonging to the network was weighted based on their established trustworthiness in the network. While this technology is promising, there is still the underlying concern that identity of some entity is predicated on credentials provided from the machine. Deceit is one of the major challenges of the semantic web as if an individual's machine is taken after trust has been established, the thief can execute some malicious actions. There are work arounds to this concern, and one of those is biometric-based authentication.

Nick et al. (Nick, 2017) proposed a biometric based authentication scheme in conjunction with a WebID based protocol for authentication. The proposed scheme begins authentication of an individual by establishing a TLS connection between the client attempting access and their profile server. In a traditional WebID system, the certificate would be check with the key information of the individual, and if there is a proper match, then authentication is confirmed. In the biometric scheme, an individual using the machine must provide their live biometric captured from the client device. The captured biometric information is sent to be compared with some biometric information of the individual that would have been previously enrolled.

Richardson et al. (2022) proposed an extension of the WebID + biometric authentication framework that utilized the disposable feature extraction technique (Shelton et al., 2017) to unique represent an individual's biometrics for each access attempt. The feature extractors were created using the BIPLab MICHE image database of iris images. The baseline LBP approach obtained a recognition accuracy of 96% on the dataset whereas the genetic-based feature extraction approach obtained an average 100% recognition accuracy on the test dataset. The intent of this is to prevent replay attacks, and prior results have shown this approach to be effective. See Figure 1 for a sequence diagram showing this protocol.

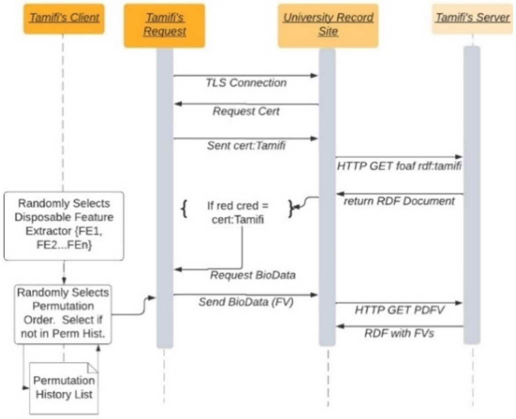

Figure 1: WebID + biometrics sequence diagram.

Technical Implementation

Previous research has been done to theorize the semantic web with the permitted disposable feature extractions approach for enhanced security. In this work, we have begun the implementation of this system. The main components required for the implementation of this prototype system are a client machine, multiple server machines, and a network connection with the capability for a TLS connection. One of the servers is representing an individual's unique and personal server. This server will store the RDF documentation, as well as the biometric data represented as a feature vector. On the client side, the webcam is enabled to capture an individual's biometric when they initially register into this system. The system has pre-programmed a number of disposable feature extractors represented in the format <L, Xi, Yi, W, H>, where L denotes the label of the disposable FE, Xi = {$x_{i,0}$, $x_{i,1}$,…, $x_{i,n-1}$} represents the x-coordinates of the centre pixel of the n possible regions and Yi = {$y_{i,0}$, $y_{i,1}$, …, $y_{i,n-1}$} represents the y-coordinates of the centre pixel of the *n* possible regions. The widths and heights of the n patches are represented by W and H respectively.

Feature extractors will be stored in a secure text file on the personal server. The other server is implemented to be representative of some online resource, such as a website that is seeking authentication. Connections will be implemented to have a TLS connection from the client to the resource server. Based off the client's certificate, the resource server will reach out to the client's personal server to request the RDF documentation. Web ID protocols will be incorporated to enable this connection. Upon authentication with the Web ID, the personal server will randomly select a unique feature extractor, and that future extractor will be sent to the client side. The client-side program will enable the webcam to gather an individual's facial image. A series of methods have been implemented to confirm that the facial image is in the correct position, and then the future extractor will be used to convert the facial image into a feature Vector. That feature Vector will then be sent to the resource server. The client's personal server will then select one of the enrolled feature vectors that were created with the same feature extractor by looking at the feature extractor labels. That feature Vector will be sent to the resource server, and a matching function will be used to compare the two feature vectors. If the similarities score falls below a specified threshold, then the user will be granted access. Otherwise, the connection will be terminated.

CONCLUSION

In conclusion, as technology continues to advance, cybersecurity remains as an essential role in the safety of individuals, organizations, and governments against malicious cyber attackers seeking to exploit vulnerabilities. The human factor element still remains a weak point even though current cybersecurity systems have significantly improved from previous years. This stems from social engineering tactics, such as phishing, malware, and weak password practices.

To address these vulnerabilities, emerging technologies like semantic web and biometrics offer promising solutions. Semantic web technology enhances data understanding, enabling more robust security measures and mitigating the risks associated with social engineering attacks. Through capitalizing on semantic web standards such as Resource Description Framework, Ontology, and Web Ontology Language, systems can improve data validation, access control, and contextual awareness, which enhances their ability to detect and prevent social engineering attacks.

Biometric authentication/recognition, which relies on unique behavioural and physiological traits, insures individuals with an additional layer of security by mitigating fraudulent activities and improving user safety. Physiological biometrics like iris recognition, fingerprint recognition and ear structure recognition, along with behavioural biometrics such as keystroke dynamics and voice recognition, offer diverse and reliable user authentication. Even though these biometric systems enhance security, proper administration and implementation are key to mitigate vulnerabilities and prevent administrative attacks.

While technological advancements offer powerful tools to bolster cybersecurity defences, comprehensive education and awareness programs are just as crucial to teach individuals the skills needed to recognize and prevent social engineering attacks. Through doing this and integrating technology and education individuals, companies and governments can collectively strengthen cybersecurity and mitigate threats posed by cybercriminals.

REFERENCES

Abraham, S. and Chengalur-Smith, I., 2010. An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, *32*(3), pp. 183–196.

Ahonen, T., Hadid, A. and Pietikainen, M., 2006. Face description with local binary patterns: Application to face recognition. *IEEE transactions on pattern analysis and machine intelligence*, *28*(12), pp. 2037–2041.

Alkhalil, Z. *et al.* (2021) *Phishing attacks: A recent comprehensive study and a new anatomy*, *Frontiers*. Available at: https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full (Accessed: 14 February 2024).

Alsaadi, I. (2021) *Study on most popular behavioral biometrics, advantages, disadvantages and recent applications: A Review*, *Academia.edu*. Available at: https://www.academia.edu/64167481/Study_On_Most_Popular_Behavioral_Biometrics_Advantages_Disadvantages_And_Recent_Applications_A_Review (Accessed: 14 February 2024).

Ammour, B., Boubchir, L., Bouden, T. and Ramdani, M., 2020. Face–iris multimodal biometric identification system. *Electronics*, *9*(1), p. 85.

Eady, Y., Kyei, K., Esterline, A., and Shelton, J. (2023) 'Measuring suitability of servers for jobs in a simulated distributed system', *Int. Conf. on Electrical, Computer, Communications and Mechatronics Engineering* (*ICECCME 2023*), Tenerife, Spain.

Kyei, K., Eady, Y., Esterline, A. and Shelton, J., 2023, April. Trust-based Enrollment in a Group in a Distributed Setting. In *Proceedings of the 2023 ACM Southeast Conference* (pp. 120–127).

Liu, F., Liu, G., Zhao, Q. and Shen, L., 2020. Robust and high-security fingerprint recognition system using optical coherence tomography. *Neurocomputing*, *402*, pp. 14–28.

Martin, T., Eady, Y., Zhang, T., Sacol, C., Esterline, A., and Mason, J., (2019) 'The WebID Protocol Enhanced with Biometrics and a Federated Enrollment Protocol' *2019 SoutheastCon*, Huntsville, AL, pp. 1–5.

Nick, W., Shelton, J., Sabol, C. and Esterline, A., 2017, July. Federated protocol for biometric authentication and access control. In *2017 Computing Conference* (pp. 854–862). IEEE.

Raul, N., Shankarmani, R. and Joshi, P., 2020. A comprehensive review of keystroke dynamics-based authentication mechanism. In *International Conference on Innovative Computing and Communications: Proceedings of ICICC 2019, Volume 2* (pp. 149–162). Springer Singapore.

Richardson, T., Shelton, J., Eady, Y., Kyei, K. and Esterline, A., 2022, April. WebID+ biometrics with permuted disposable features. In *Proceedings of the 2022 ACM Southeast Conference* (pp. 99–105).

Shelton, J., Jenkins, J. and Roy, K., 2017. Extending disposable feature templates for mitigating replay attacks. *International Journal of Information Privacy, Security and Integrity*, *3*(2), pp. 96–116.

Zhou, L., Ding, L., and Finin, T., (2011) 'How is the Semantic Web evolving? A dynamic social network perspective', *Computers in Human Behavior*, Vol. 27, Iss. 4, pp. 1294–1302.