PROTECTION OF CYBER PHYSICAL SYSTEMS WITH BIOMETRICS

BY

ADENIYI AKANNI (Ph. D.)

ANCHOR UNIVERSITY LAGOS, NIGERIA

Abstract

The world wherein we live has witnessed diverse improvement brought about by the technological advancement. Several more will yet be born in the next few years going by the spate of development in Information Technology. Cyber physical systems (CPSs) have made these quite attainable. However, controlling access has been a major drawback to embracing this technology swing. This paper offers an enhanced access control in CPS with biometrics.

Keywords: cyber physical system, authentication, biometrics, bimodal and identity management.

1. Introduction

CPS has made life a lot easier. While concentrating on other things, CPS is capable of handling some activities that will eventually cut down unnecessary overhead and also reduce human stress. For instance, CPS such as an autonomous car will help to see this more closely. An autonomous vehicle can actually be sent on an errand when the owner is attending to some core and time-bound activities in the office. As beautiful as this technology may seem, controlling access remains a major challenge such that the authorized users can be distinguished from an impostor knowing that CPSs only grant access as configured – not minding whether or not there was an identity theft in whatever form. Recent privacy issues in Facebook affecting millions of users made many to be wary of CPS and its usefulness (Wagner, 2018; Zuckerberg, 2019). Effectively managed access control will then be necessary to safeguard this asset. This work designed fingerprint biometrics to control access to CPS.

2. MAJOR CONCEPTS

Major concepts used in the paper are discussed below:

a. Cyber Physical System

NIST (2019) explains CPS as a way of integrating network connections and physical systems that have computing capabilities. They have processors and sensors with which they can interact

with real world. These include autonomous vehicles, robots, energy farms and smart cities among others.

b. Access Control

Access to a resource describes the permission granted to make use of such a resource. Access control is the restriction of access to a place, facility or resource. Gaining access may therefore be by permission or authorization. Access control mechanism is a component that serves to receive the access request from the subject to decide and to enforce the access decision (Hu, et al, 2014). Access control can be physical or logical. Physical control can be in form of deadman door, security manning or door with a padlock. Logical access control involves usage of one or combination of user id, token, password, PIN and biometrics. According to Huth et al (2012), passwords are very important means of accessing information. They should be well and adequately protected so that wrongdoers do not capitalize on the weakness to steal users' identities.

c. Identity Management (IDM)

Identity management (IDM) is a way of identifying individuals in a system such as a country, a network or an organisation and controlling the access to the resources in that system by placing restrictions on the established identities (Gunjan et al, 2011). Identity theft is a fast growing crime whereby dishonest individuals illegally gain access to an unsuspecting person's account as if the rightful owner did (USA Social Security Administration). Access to the storage should be on need-to-have or need-to-know bases. Both users and services accessing cloud information should always be reviewed and amended accordingly when the need arises to be secured (Gopalakrishna 2009; Thornton, 2012). There are risks associated with mobile IDM similarly to those of the mobile devices. These include: identity theft, eavesdropping, spyware, phishing and lack of user awareness (Papadopouli, 2009). Gunjan, et al, (2012) defined identity management (IDM) as a way of identifying individuals in a system such as a country, a network or an organisation and controlling the access to the resources in that system by placing restrictions on the established identities. Akram and Hoffmann (2008) identified minimal disclosure of information for a constrained use as one of the ways of securing identity. This is to say that personal information should be kept by cyber physical users

d. Authentication

Authentication is a process of ascertaining that the identified person is the actual person he claimed to be. Prior to authentication, a resource user must have been recognized through the identification process. It can be in terms of user id. Authentication thus, can be through "something you know" like a password, "something you have" like a token (soft or hard) and "something you are" like biometrics. Using only one of "something you know", "something you have" and "something you are" is term as a single factor authentication. Where it uses two of these is called two-factor. If more than two, it is known as a multi-factor. Symantec 2011, opined that two factor authentication is embraced by corporate bodies due to its relative ease of use. Various two factor authentication method have been used by different banks (Northcutt, 2014). Some of these include online keyboard, complex ID's and passwords, software tokens that are generated and sent to mobile phones. However, the problem observed is that they are prone to shoulder surfing when the owner is keying in the details.

Aloul, et al (2009) researched into using multifactor authentication to secure online banking as well as ATM terminals for secure transactions. They used software token. A set of numbers would be generated and sent via short message services (sms) to a mobile phone. These numbers are copied out within a time space and used for authenticating transactions. This approach is secured as long as the phone is with the account owner. The problem here is that transactions cannot be consummated in the event that the phone is lost. More so, theft of the mobile phone can lead to fraud because it makes the fraudster the direct recipient of the token.

e. Biometrics

Biometrics is the measurement and analysis of unique physical or behavioural characteristics. It is usually for the verifying identity whether in form of genetical dispute resolution or access control. The latter is employed in this research as a form of second level authentication. It has some key benefits that made it readily useful in today's technology as an access control mechanism. Jacobs and Poll (2010) explained biometrics as the use of physical characteristics, behaviour or skills to identify a person. These include palm, finger, iris, voice, DeoxyriboNucleic Acid (DNA), face and a host of others. The basic idea about biometrics is that its features such as palm, iris and face become permanent shortly after birth and cannot be shared like password. For

convenience and security reasons, accesses are preferably controlled by biometrics (Nandakumar et al 2009). A comparative study carried out on biometric features places high reliability on finger print as shown in table 1. There are various biometrics that have been previously tested with some degree of reliability. There are cases where two or more biometric features are considered in order to increase the degree or level of reliability of an authenticating system. When two biometric features are combined to form an access control, it is known as bimodal biometric feature. When the combined features are more than two, it is regarded as a case of multimodal biometric features for access control. However, this study adopted fingerprint biometrics in order to increase the security level of authentication.

3. Pitfalls to Avoid in Controlling Cyber Physical Systems

a. Complex Design. Control for CPS should be designed not in such a way that it looks so difficult to understand.
b. Simple Design. While simple design is desirable in controlling CPS, an extremely simple design should be avoided.
c. Resources – not considering human life, key-man risk, making over provision or under provision of human and material resources. The most important asset in an environment or company is human being. Every construction, design or control must have adequately taken care of human.
d. Contingency Approach. When there is an incidence, chances are that other companies in the know may want to quickly put some controls hurriedly up. It is a necessity, yet this may never give the best available control option available.
e. False believe of a single control. In-depth control is inevitable. Using very strong authentications like biometrics may be good but encryption of data generation is very essential.

4. Protecting Cyber Physical Systems with Biometrics

Safeguarding CPSs is very important otherwise, great havoc can be caused by an impostor who tend to divert CPS to their own advantage. As the old saying goes, “the horse knows its owner”, identity theft can make CPS function as if the authentic user is the one making use of his system. Password protection is useful but cannot easily be compromised. Biometric features have proven

largely effective because no two individuals have the same biometrics. DeoxyriboNucleic Acid (DNA) ranks highest among other biometrics but it is still much expensive to implement. As technology improves, that barrier will soon be broken in a future time. For now, fingerprint may be a better alternative for the following reasons:

a. Back-up exists in other fingers where a finger is damaged.
b. It is relatively cheap to implement
c. It reduces administrative overhead occasioned by calling Administrator for password reset.
d. Fool proof against anti-skimming, shoulder surfing or social engineering that tend to bypass authentic user.

Conclusion

The world is preparing for an upsurge in CPS in the next few years to come but privacy issue will be a major challenge should adequate measure not be made. This paper thus, proposed fingerprint biometric as a means of authentication to ensure safety on CPS.

References

Akram, H. and Hoffmann, M. (2008). Laws of Identity in Ambient Environments: The HYDRA Approach. IEEE Computer Society, 978-0-7695-3367-4/08

Aloul, F., Zahidi, S. and El-Hajj, W. (2009). Multifactor authentication using mobile phone. International Journal of Mathematics and Computer Science 4(2009), no 2, 65-80.

Gopalakrishna, A. (2009). Cloud computing identity management. SETLabs Briefings Vol. 7 No 7, 2009

Gunjan, K., Sahoo, G. and Tiwari, R. (2012). Identity management in cloud computing –A Review. International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 4, June – 2012.

Hu, V., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R. and Scarfone, K. (2014). Guide to Attribute Based Access Control (ABAC) definition and considerations. National Institute of Standards and Technology. www.nvipubs.nist.gov

Huth, A., Orlando, M. and Pesante, L. (2012). Password security, protection and management. www.us-cert.gov.

Jacobs, B. and Poll, E. (2010). Biometrics and Smart Cards in Identity Management. www.cs.ru.nl.

Nandakumar, K., Ross, A. and Jain, A. (2009). Biometric fusion: does modeling correlation really matter? IEEE 3rd Intl. Conf. on Biometrics: Theory, Applications and Systems (BTAS 09), Washington DC

National Institute of Standards and Technology (NIST), 2019. Cyber-physical systems and internet of things.Publ. 1900-202

Northcutt, S. (2014. Two factor authentication for online banking. www.sans.edu

Papadopouli, M. (2009). Mobile identity management. www.eniza.europa.eu.

Symantec (2011). Two-factor authentication: a TCO viewpoint. www.symantec.com

Thornton, G. (2012). Global projects in identity management and infrastructure security. www.isaca.org.

USA Social Security Administration. Social Security.Identity theft and your social security number. www.socialsecurity.gov.

Wagner, K. 2018. Another facebook bug may have exposed millions of users' private photos to app developers. www.vox.com

Zuckerberg, M. (2019). Mark Zuckerberg joins Tim Cook in calling for GDPR-like privacy regulation in the US. **www.9to5mac.com**