International Journal of Science and Advanced Innovative Research
ISSN: 2536-7315 (Print) 2536-7323 (Online)
Volume 5, Number 2, June 2020
http://www.casirmediapublishing.com

ACHIEVING EXPERT SYSTEM USER SECURITY IN COMPUTER SYSTEMS THAT EXHIBIT ARTIFICIAL INTELLIGENCE

Obioha Iwuoha, Oparah Camillus C. & Oyedepo Victoria
Department of Computer Science
Federal Polytechnic Nekede, Owerri
Email: ohaobi@yahoo.com

ABSTRACT
There is need for user security protocol in the developmental phases of expert systems so as to prevent intruder-programmers from maliciously exploiting the expert system to the detriment of the computer users who try to benefit from the services of the software. A malicious programmer could use an expert system to get sensitive user data in the guise of artificial intelligence provision. The aim of this paper is to proffer ways by which expert system user security could be achieved on artificial intelligence computer systems. The research methodology used is structured systems analysis and design methodology using the logical data modeling technique which involves identifying and documenting data requirements needed for the creation of a new system. The result of this research work is a precise account of ways to achieve expert system user security in artificial intelligent computer systems. The body of information communication technology can use this paper to ensure expert system user security in computer systems that exhibit artificial intelligence.

INTRODUCTION
In artificial intelligence, an expert system is a computer system that emulates the decision-making ability of a human expert. Expert systems are designed to solve complex problems by reasoning through bodies of knowledge, represented mainly as if–then rules rather than through conventional procedural code (Butterfield & Ngondi, 2016). An expert system is a computer program that uses artificial intelligence (AI) technologies to simulate the judgment and behavior of a human or an organization that has expert knowledge and experience in a particular field. Typically, an expert system incorporates a knowledge base containing accumulated experience and an inference or rules engine – a set of rules for applying the knowledge base to each particular situation that is described to the program. The system's capabilities can be enhanced with additions to the knowledge base or to the set of rules. Current systems may include machine learning capabilities that allow them to improve their performance based on experience, just as humans do (Cowley, 2017). The concept of expert systems was first developed in the 1970s by Edward Feigenbaum, professor and founder of the Knowledge Systems Laboratory at Stanford University. Feigenbaum explained that the world was moving from data processing to "knowledge processing," a transition which was being enabled by new processor technology and computer architectures. Expert systems have played a large role in many industries including in financial services, telecommunications, healthcare, customer service, transportation, video games, manufacturing, aviation and written communication. Two early expert systems broke ground in the healthcare space for medical

diagnoses: Dendral, which helped chemists identify organic molecules, and MYCIN, which helped to identify bacteria such as bacteremia and meningitis, and to recommend antibiotics and dosages. A more recently developed expert system, ROSS, is an artificially-intelligent attorney based on IBM's Watson cognitive computing system. ROSS relies on self-learning systems that use data mining, pattern recognition, deep learning and natural language processing to mimic the way the human brain works. Expert systems were among the first truly successful forms of artificial intelligence (AI) software. An expert system is divided into two subsystems: the inference engine and the knowledge base. The knowledge base represents facts and rules (Jim, 2014). The inference engine applies the rules to the known facts to deduce new facts. Inference engines can also include explanation and debugging abilities. Expert systems and AI systems have evolved so far that they have spurred debate about the fate of humanity in the face of such intelligence.

An expert system is application software that requires logical input from computer users to draw up inferences and produce results for the computer user as an expert professional would in a specified context. Once the expert system achieves this feat, it has displayed artificial intelligence, which is man-made intelligence that tries to imitate the natural human intelligence (Stevens, 2018). Questions requiring logical answers could be used to draw the computer user down a predefined path in order to obtain sensitive information from the user.

THEORETICAL FRAMEWORK

The theoretical framework for this paper is as follows;

ARTIFICIAL INTELLIGENCE COMPUTER SYSTEMS

Artificial intelligence can also be called man-made intelligence. This is intelligence built by man with the intention to imitate a human professional of any discipline. For artificial intelligence to be achieved an avenue must be used to achieve it. This avenue can be an electronic tool, for an electronic hardware to be intelligent; there must be a software present to control the activities of the electronic hardware (Lin, 2016). The marriage of the software and hardware gives birth to the computer system. The computer system is the ideal system for showcasing artificial intelligence. In order to achieve artificial intelligence in computer systems, a special type of software which belongs to the category of application software must be installed. This type of application software is called expert system. An expert system is an application software which poses questions to a computer user and insists only on logical answers from the computer user. Logical answers are the form of yes or no, true or false, on or off. Based on the input of logical answers from the computer user, an inference is deduced and a corresponding response made by the expert

International Journal of Science and Advanced Innovative Research
ISSN: 2536-7315 (Print) 2536-7323 (Online)
Volume 5, Number 2, June 2020
http://www.casirmediapublishing.com

system. An expert system is usually designed to behave and reason like a specified human professional of a particular discipline (Lin, 2017). These disciplines include and are not limited to computer science, history, medicine, law, engineering and psychology. In summary, a computer system will display or exhibit artificial intelligence with the aid of an expert system software installed in it. Examples of computer systems include laptops running windows 10, android phones and ATM – automated teller machine portals running defined operating systems. Examples of expert system software include interactive malaria specialist software, automated Nigerian judge and online relationship match-maker.

COMPUTER SECURITY

Computer security which is also known as cyber security or IT security is the protection of computer systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide. It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection, and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures (Marcel etal, 2014). Computer Security is concerned with four main areas, they include;

1. Confidentiality: - Only authorized users can access the data resources and information.
2. Integrity: - Only authorized users should be able to modify the data when needed.
3. Availability: - Data should be available to users when needed.
4. Authentication: - are you really communicating with whom you think you are communicating with?

Computer security is important for the following reasons;

1. It helps to prevent theft of sensitive data like bank account numbers, credit card information, passwords, work related documents and essential sheets.

2. It ensures that data present in a computer is not misused by unauthorized intrusions. An intruder can modify and change the program source codes and can also use your pictures or email accounts to create derogatory content such as pornographic images, fake misleading and offensive social accounts.

3. It prevents intruders from using an unsuspecting user's computer to attack other computers or websites or networks thereby creating havoc. Vengeful hackers might crash someone's computer system to create data loss. Attacks can also be made to prevent access to websites by crashing the server.

Some software tools used to ensure computer security include firewall and antivirus. A firewall is a security-conscious piece of software that sits between the Internet and a user's network with a single-

minded task of preventing online cyber-attacks from getting to the user's network. The firewall acts as a security guard between the Internet and a user's local area network (LAN). All network traffic into and out of the LAN must pass through the firewall, which prevents unauthorized access to the network (Melvin, 2014). An antivirus is a software which will find programs that might compromise a user's computer. It detects these kinds of harmful programs that are already installed on your computer or about to be installed. It can perform various protective measures like quarantine, permanent removal or fix.

EXPERT SYSTEM SECURITY

For instance, an expert system that detects malaria on patient users may demand payment for its service as a shareware in real-time. It could then start asking the user sensitive questions that require the user to give a logical answer. For example, is your bank first bank? Are you operating a savings account? Is your account number 8888333? If No, then state the correct account number. Is your BVN 234343434? If no, then state the correct BVN. Is your PIN all numbers? Is it 4545? If no, state the correct PIN. My service to you costs N500, type "Y" to pay. Thank you for your patronage. Let's now proceed to check you... Are you feeling dizzy? From the above context the user's confidential bank details have been obtained, thereby compromising the user's financial security.

Expert system user security involves a situation where the expert system user is protected from abusive, malicious imposters-programmers who would use a seemingly good AI software to dupe the software user (Millman, 2017). Steps taken to ensure expert system user security include the use of cheat-features identification and digital signature verification from ethical teams of certified developers.

Ways to Achieve Expert System User Security in Computer Systems that Exhibit Artificial Intelligence

Expert system user security could be achieved using the following means;

1. User enlightenment on relevant red flags that indicate a malicious expert system software: The expert system user must be made aware of some common factors that a malicious expert system software display, so that he/she may avoid the software (Reimers & Anderson, 2017). They include;

a. Asking the user for sensitive bank details like ATM pin, BVN and bank verification pins.
b. Asking for access to the user's device camera, system files and secured folders.
c. Asking for the user's computer login details.
d. Asking to gain access to the user's social media account and emails.
e. A software that has no uninstall feature.
f. Asking the user to allow it send diagnostic statistics via the user's network to its producers.

2. Using operating systems that ensure digital signature identification and verification before installing any expert system software: a digital signature is a signature of a software producer which he/she effects on any software he/she produces. The software producer called the signer then registers this signature with an ethical body or renowned operating systems, who before accepting the signers registration confirms that his/her software abides by stipulated rules and regulations governing the ethical body or operating system in which one of the rules include ensuring user security (Schatz, etal, 2017). Anytime a software is to be installed, a good operating system identifies and verifies the producer digital signature accompanying the software. If the software producer's digital signature is not registered on its database, the software will not be installed, hence protecting the user from the malicious software.

3. Reading user reviews on their experiences with existing expert system software in order to identify and avoid notorious malicious ones: It is always safe to learn from other people's experiences (Schlienger & Teufel, 2003). When the user reads user reviews on existing expert system software before installing and using the software, he/she becomes fully aware of the consequences of using such a software. If previous users all say the software is bad, the user avoids it completely else if previous users say the software is good and safe, the user can use the software with confidence.

FACTORS TO CONSIDER WHILE ENSURING EXPERT SYSTEM USER SECURITY

Here are some factors that can make an expert system user vulnerable to malicious expert system software. They include;

1. User's need: If a user stumbles on a rare software that could some an immediate problem, he/she tends to ignore all the red flags indicating that the software is intruding and malicious.
2. Cost of software: If the software is free and requires no additional charges before use.
3. Size of software: If the software does not consume hard drive space and could easily be downloaded or copied.
4. Software ease of use: If the software is efficient and very user friendly.
5. Doctored user reviews: If the malicious software producer flood the user review portal with lies and fake reviews that the software is so good.

CONCLUSION

It is worthy to note that a user whose security has been compromised is subject to heart attack or even depression. In order to ensure that an expert system user always has rest of mind, he/she must abide by the laid down ways of ensuring expert system user security for computer systems that exhibit artificial intelligence.

RECOMMENDATION

The following policies should be put in place by software regulatory bodies and software producers in order to ensure continued expert system user security in computer systems that exhibit artificial intelligence;

1. All Expert systems must carry the security caution message and allow it as splash screen for at least 1 minute for showing their main menu.
2. A button to check and verify software producer's digital signature be kept on the home screen of every expert system. Most operating systems like windows and android ensure strict digital signature verification before software installation.
3. Online search engines should display user reviews alongside any sort-for software.
4. Computer users should never compromise their security in the name of free software, small sized or easy to use software. Be very cautious no matter how nice the software is.

REFERENCES

Butterfield, A. & Ngondi, G. (2016). Spoofing. Oxford University Press, Oxford, UK.

Cowley, S. (2017). 2.5 Million More People Potentially Exposed in Equifax Breach. The New York Times Press, New York, USA.

Jim, F. (2014). Hacker to show passenger jets at risk of cyber-attack. Reuters printing press, London, UK.

Lin, T. (2016). "Financial Weapons of War". Minnesota Law Journal. SSRN 2765010.

Lin, T. (2017). "The New Market Manipulation". Emory Law Journal. 66: 1253. SSRN 2996896.

Marcel, S.; Nixon, M; Li, S. (2014). Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks. Springer books press, London, GB.

Melvin, B. (2014). Home Depot: 56 million cards exposed in breach. CNNMoney Press, New York, USA.

Millman, R. (2017). New polymorphic malware evades three quarters of AV scanners. SC Magazine UK.

Reimers, K. & Anderson, D. (2017). Post-secondary education network security:
the end user challenge and evolving threats. Kingston Publishers, Texas, USA.

Schatz, D.; Bashroush, R.; Wall, J. (2017). Towards a More Representative Definition of Cyber Security. Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215.

Schlienger, T. & Teufel, S. (2003). "Information security culture-from analysis to change". South African Computer Journal. 31: 46–52.

Stevens, T. (2018). Global Cyber security: New Directions in Theory and Methods. Journal on Politics and Governance. 6 (2): 1–4. doi:10.17645/pag.v6i2.1569.