# SSD Individual and Group Activities

## Collaborative Discussion One

Broken Access Control

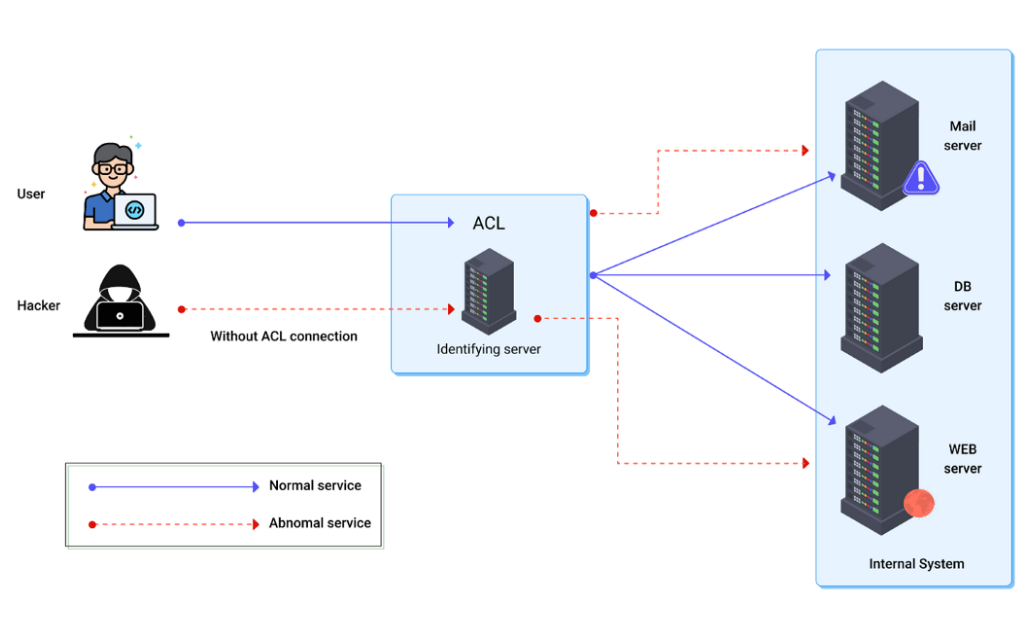


Figure 1- Medium. (2021). A Closer Look at OWASP Top 10 Security Risks & Vulnerabilities.

Access control is a a way to determine the right of access to data and functions, as well as identifying whether or not an authenticated individual has access to the specified data. It defines an authenticated person's access rights to data. When an unauthorised user gets access to unauthorised data or functions in malicious ways then it is referred as Broken Access Control as illustrated in the diagram above.

**Reference**

Medium. (2021). *A Closer Look at OWASP Top 10 Security Risks & Vulnerabilities*. [online] Available at: <https://medium.com/purplebox/owasp-top10-e9d1dd17c804> [Accessed 16 September 2021].

## Unit 2 Seminar Activity

Five terms: Access Control, Attack, Authentication, Confidentiality, Governing body

Access control is essential as a security method because it can be utilised to manage who can view or utilise a particular resource. In the context of an organisation this would mean who has access to and can edit a certain file, or who has access to specific devices. Sandhu,

The end purpose of access control is to offer a degree of security that reduces risk to a business or organisation by assisting in the protection of facilities, data, and people.   Without effective access management, employee within organisations can be the culprit of the risks such as data loss, theft, or a violation of privacy and data protection laws. (Kalam et al, 2003)

Some examples of Access control used in organisations are Pin/Passcodes on devices, the usage of VPN, Files which are secured by passwords, Firewalls, Encryption, biometric systems etc. (Getkisi.com, 2021)

Confidentiality is key in organisations especially the ones which handle sensitive data.  By securing the client's data, it is not only demonstrating common decency, but it is also meeting the legal obligation to prevent sensitive information from being disclosed. (Kalam et al, 2003)

Such breaches of confidence may have disastrous implications for organisations, for example the Yahoo breach caused more than a billion user accounts data to be disclosed. (Ncsc.gov.uk, 2021)

It was only a mistake of the internal person which clicked on an unknown link,

therefore it is critical that there is an understanding within the workplace of how to adhere to this ethical and legal duty. An example of how this could have been avoided would be to provide sufficient training to the people of the organisation (McBride et al, 2012)

Another way to manage the security of the organisation is by having a security governor. (Ncsc.gov.uk, 2021) Security governance is the process of controlling and directing an organisations approach to security. This would be helpful as they would ensure all security requirements are being met at the organisation and there aren’t any security risks caused by any of the people in the organisation. (Ncsc.gov.uk, 2021)

**Reference**

Getkisi.com. (2021). *Access Control Planning Examples | Kisi*. [online] Available at: <https://www.getkisi.com/guides/access-control-planning-examples> [Accessed 8 September 2021].

Kalam, A.A.E., Baida, R.E., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miege, A., Saurel, C. and Trouessin, G., (2003), June. Organization based access control. In *Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks* (pp. 120-131). IEEE.

McBride, M., Carter, L. and Warkentin, M., (2012). Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. *RTI International-Institute for Homeland Security Solutions*, *5*(1), p.1.

Ncsc.gov.uk. (2021). *Introduction to security governance*. [online] Available at: <https://www.ncsc.gov.uk/collection/risk-management-collection/governance-cyber-risk/security-governance-introduction> [Accessed 8 September 2021].

Ncsc.gov.uk. (2021). *Yahoo data breach: NCSC response*. [online] Available at: <https://www.ncsc.gov.uk/news/yahoo-data-breach-ncsc-response> [Accessed 8 September 2021].

## Unit 3 Team Activity

1. What factors determine whether a programming language is secure or not?

* Confidentiality
* Integrity
* Availability
* Authentication
* Authorisation
* Non-reputability

1. Could Python be classed as a secure language? Justify your answer.

Some could say that Python is not a secure language because of the security loop holes hackers can exploit such as through the reading output, overflow errors evaluating arbitrary input. However there are work-arounds for this to prevent hackers exploitation it is possible to avoid using certain coding such as by when reading the console input it is a better strategy to use raw input rather than input. For expressions it is better not to use eval apart from situations where you have control and trust the input sources and return values from functions. So Python is a secure language but only if you understand properly how you can make your coding secure by using certain strategies and avoiding others.

1. Python would be a better language to create operating systems than C. Discuss.

Python is considered a very high level programming language so it is not so suitable to create a operating system with it. C is more commonly used to create operating system

## Unit 5 Formative Activity

Artificial Intelligence would present the next phase of evolution history. AI started in 1956 when it was formally founded, before this philosophers strived to give AI a name, they continually described it as a human thinking integrated into a symbolic system. (livescience.com, 2004).

Researchers claim that AI, in todays world, are gradually nearing human capabilities while doing "basic" activities like comprehending spontaneously spoken language or assessing unfamiliar, novel circumstances. For example Google Assistant. AI, despite several improvements, still lack the ability to process profound emotional intelligence. (Beck and Libert, 2017)

However, organisations are adopting cognitive technologies into their business practises in the form of virtual assistents/agents which handle customer enquiries, these robots can develop responses based on the customers questions or discussions through inovative detection technology. This means AI can form engaging relationships with humans which as a result forms three core paradigms for the future of AI technology, 1) Conversational AI, 2) Mass Individualization 3) AI enabled Convergance. (Medium, 2017)

References

Beck, M. and Libert, B., (2017). The rise of AI makes emotional intelligence more important. *Harvard Business Review*, *15*.

livescience.com. (2004). *A Brief History of Artificial Intelligence*. [online] Available at: <https://www.livescience.com/49007-history-of-artificial-intelligence.html> [Accessed 13 September 2021].

Medium. (2017). *The Rise of AI in the Modern World*. [online] Available at: <https://medium.com/cityai/thinking-with-technology-the-rise-of-ai-in-the-modern-world-a7566740581f> [Accessed 13 September 2021].