Unit 1 Reflection

Thoughts on Learning

This unit introduced students to information security management (ISM) which encompasses people, processes, information, and information technology. I consider that no information system exists in isolation but has actors that act upon it and things upon which it acts. Therefore, information security management must encompass all these parts. I learned that the foundation of ISM is a triad of information security management known as Confidentiality, Integrity and Availability (CIA). Confidentiality deals with unauthorized persons' ability to read and take advantage of information stored in the computer; Integrity deals with unauthorized persons' ability to make changes to stored information; Availability deals with preventing authorized users from referring to or modifying information. Research referred to Non-Repudiation in addition to CIA, which I found interesting because non-repudiation deals with a system's ability to prove who/what performed actions within the system—frequently monitoring application log files helps here.

I enjoyed delving into the concepts of a threat which is an unexpected security breach and a vulnerability which is an attack against an asset that is not secured correctly. The two definitions cleanly separate between different aspects of cybersecurity attacks. Since vulnerabilities are at the heart of information security, they can be found in areas such as weak passwords, privilege escalations, infrastructure (e.g., hypervisors, software switches, storage nodes, and load balancers), software flaws such as the OpenSSL TLS heartbeat extension information leak, web application flaws such as session management, HTTPS or SSH sessions, input validation failures, insecure temporary files, poor code quality and even insecure memory access.

I came across various public websites that disclose vulnerabilities, such as

- National Vulnerability Databases (https://nvd.nist.gov/)
- Offensive-Security Exploit Database (http://www.exploit-db.com/)
- HackerOne Internet Bug Bounty (https://hackerone.com/internet)
- CERT Vulnerability Notes (http://www.kb.cert.org/vuls)
- Vulnerability Databases (https://vuldb.com/?)
- Common Vulnerability and Exploits (https://cve.mitre.org/cve/).

To categorise and assess threats, I looked at Microsoft's STRIDE[1] threat classification and DREAD[2] risk rating models. Hussain et al. (2014) consider STRIDE as the most widely used threat model, which applies DREAD ratings to each security risk. They also list other models such as STRIDE Average Model, Attack Trees, Fuzzy Logic, SDL Threat Modelling, T-MAP (used for Commercial Off The Shelf software) and CORAS (a UML graphical threat modelling tool). I found these models very enlightening, as they each provide a foundation to assess information system threats. Further, I investigated the Skills Framework for the Information Age (SFIA, https://sfia-online.org/en) to consider skills related to information security and identified several roles applicable to ISM, such as Information Security Technician, Infrastructure Specialist or Operations Support analyst.

Collaborative Discussion

The collaborative discussion, initiated in this unit, helped me consider threat prevention that takes multiple forms and must involve infrastructure managed by organisations or cloud providers. For example, firewalls, two-factor authentication, intrusion detection systems, password policies, and data encryption. To me, assigning the least privilege to user accounts is the quickest and simplest means to reducing potential threats. Important too is *enabling* customers to easily report new threats and to consider not just software aspects of information systems, but also mundane items such as the buildings, a business's processes and the people that interact.

Team Allocation

This week I was assigned to Group 3 and was tremendously thrilled to be working with fellow students I worked with previously. Working with fellow students who are engaged with the content and with whom one can freely engage with conversations concerning the module content is, to me, tremendously valuable and facilitates an enjoyable learning experience. My allocation into a team was a little slow in the first few days due, however, the university's support team were tremendously helpful with facilitating quick signup and enrolment.

References

[1] Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of Privilege.
[2] Damage potential, Reproducibility, Exploitability, Affected Users, Discoverability.

Hussain, S., Kamal, A., Ahmad, S., Rasool, G. & Iqbal, S. (2014). Threat modelling methodologies: a survey. *Science International,* 26(4):1607-1609.