Network and Information Security Management – Units 1 - 3

This 12-week module introduces the various core elements of the MSc. Cybersecurity programme at the University of Essex Online. It intends to ensure a basic understanding of the primary skills covered in complete detail during all relevant modules. It also provides insight and understanding of how the different practices and occupational roles combine to offer a robust body of knowledge and skillset required to succeed in the field. Furthermore, it is beneficial to all who would master this critical field to gain a fuller understanding of the contribution and importance of all elements. As the units tend to build one upon another and contain summary review and reflection every few units, these note entries will follow a similar track and cover three units in each.

This unit summary covers units between 1 - 3, including the following outcomes:

- Explain the basic principles of Information Security Management.
- Describe the 4 tenets/ principles of Information Security Management.
- Describe what constitutes a threat and vulnerability.
- List several common roles within the Information Security profession.
- Describe a number of typical vulnerabilities of modern electronic devices.
- Explain how common vulnerabilities can be exploited using software toolkits.
- Use industry standard toolkits to classify and evaluate threats and vulnerabilities.
- Describe the fundamental concepts of networks.
- Evaluate a number of widely available tools to use for basic network troubleshooting.
- Explain the differences between the IPv4 and IPv6 standards.

Progressive Learning Experience

As predicted, the module study is well-known to me. Describing fundamental concepts and definitions such as Networks, Information Security Management Systems (ISMS), or relation between threats and vulnerabilities were effortless to understand. Yet, it was particularly interesting using standard toolkits to classify and evaluate potential threats and vulnerabilities. In addition to that, the diversity of viewpoints and experiences of other students provided the opportunity for growth. Collaborative learning discussions were a noticeable focus area of the first three units. These discussions were more challenging than traditional courses that rely on exams and promote critical thinking simultaneously. However, these interactions of collaborative learning discussions were an exciting exchange and provided invaluable insight and expanded methods of critical examination.

Personal Take-Away for Units 1 - 3

Collaborative learning discussions, seminars and lecture casts were constructive, especially in further developing threat modelling and risk scoring techniques such as STRIDE and DREAD. Furthermore, working on real-world issues and potential implications of cybersecurity threats and vulnerabilities concerning medical devices and the healthcare industry significantly contributed to a better understanding of different viewpoints. Additionally, these unit discussions were particularly focused on healthcare IT systems’ threats and vulnerabilities, including potential mitigation techniques. And I tried to summarise my study in the following summary post:

'Security and Privacy of Healthcare IoT Devices'
In the initial post, we analysed potential vulnerabilities and threats mentioned in the "Compromising a Medical Mannequin" (Glisson et al., 2015) paper. Then, the researchers used various techniques to break the medical mannequin under a controlled environment, and I listed the following potential mitigations or countermeasures to overcome these threats:

There could be alternative ways of executing brute force attacks, such as in rapid coordinated (distributed brute-force attacks) or slow-paced manner. In order to counter these attacks, a wide variety of countermeasures, such as employing solid passwords, avoiding the use of default usernames or changing them something different, disabling SSH-based logins for administrative IDs (e.g., root account, or encouraging sudo), or running SSH on a non-standard port and the use of TCP wrappers to block IP addresses that used for repeated login attempts could be utilised. In addition, honeypots, IDSs (Intrusion Detection System) and NACs (Network Access Control) would be considered as other countermeasures, especially for DoS attacks and malicious intents such as eavesdropping of the internal network. For example, IDS could support avoiding taxation of hardware resources and help in mitigating brute force attacks too.

In summary, we observed that there are many ways to exploit or compromise M-IoT assets, including medical mannequins. However, there are also proven and effective countermeasures as mentioned above to mitigate these potential threats.

References:
Owens, J. and Matthews, J., 2008, March. A study of passwords and methods used in brute-force SSH attacks. In USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)
Raikar, M.M. and Meena, S.M., 2021, May. SSH brute force attack mitigation in Internet of Things (IoT) network: An edge device security measure. In 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC) (pp. 72-77). IEEE.
Anirudh, M., Thileeban, S.A. and Nallathambi, D.J., 2017, January. Use of honeypots for mitigating DoS attacks targeted on IoT networks. In 2017 International conference on computer, communication and signal processing (ICCCSP) (pp. 1-4). IEEE.

Required Reading
The following reading assignments were available during these units:

- Campbell, T. (2016) *Practical Information Security Management*. 1st ed. APRESS.
    - Chapters 1-3.
- Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015) Compromising a Medical Mannequin. Sighealth.
    - Case study
- Meier, J., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R. & Murukan, A. (2003) *Threat Modelling.*
    - STRIDE & DREAD description
- Smith, C. & Brooks, D. (2013) Security Science. 1st ed. Amsterdam: Elsevier, BH.

    - Chapter 1
- Parziale, L., Britt, D., Davis, C., Forrester, J., Lui, W., Matthews, C. & Rosselot, N. (2006) *TCP/IP Tutorial And Technical Overview.* 8th ed. New York: IBM.
    - Chapters 1-5. Especially Chapter 5 for routing protocols.

Additional Reading

The following reading assignments were available during these units:

- Smith, C. and Brooks, D. (2013) Security Science. 1st ed. Amsterdam: Elsevier, BH.
    - Chapter 1
- Blakley, B., McDermott, E. & Geer, D.(2001) Information Security is Information Risk Management. Proceedings of the 2001 workshop on New security paradigms. 1(1): 97-104.
- Humphreys, E. (2008) Information Security Management Standards: Compliance, Governance and Risk Management. *Information Security Technical Report* 13(4): 247-255.
- Connolly, D. (2000) A Little History Of The World Wide Web.
- The Risks Digest (1995) Forum on Risks to the Public in Computers and Related Systems. ACM Committee on Computers and Public Policy. 17(10).
- Bijalwan, A., Solanki, V. & Pilli, E. (2018) Botnet Forensic: Issues, Challenges and Good Practices. *Network Protocols and Algorithms* 10(2): 28 - 51.
- Moore, A. & Householder, A. (2019) Multi-Method Modelling and Analysis of the Cybersecurity Vulnerability Management Ecosystem. Proceedings of The International Conference of the System Dynamics Society 37(1):106-133.
- Schneier, B. (2004) *Secrets and Lies : Digital Security in a Networked World.* Indianapolis: Wiley.
    - Chapters 8 and 12
- Sinha, A. (2017) Beginning ethical hacking with Python. West Bengal: Apress
    - Chapters 4 and 5
- Tang, A. (2014) A guide to penetration testing. *Network Security* 2014(8): 8-11.
- McNab, C. (2004) *Network Security Assessment: Know Your Network.* Sebastopol, CA: O’Reilly Media.
    - Helps with the Scanning Exercise: Chapters 1-4