**David: System Security**

* <https://ucelinks.cdlib.org/sfx_local?genre=article&atitle=ISO%2027001%20--%20INFORMATION%20SYSTEMS%20SECURITY%2C%20DEVELOPMENT%2C%20TRENDS%2C%20TECHNICAL%20AND%20ECONOMIC%20CHALLENGES.&title=Annals%20of%20the%20Faculty%20of%20Engineering%20Hunedoara%20-%20International%20Journal%20of%20Engineering&issn=15842665&isbn=&volume=17&issue=4&date=20191101&aulast=%c5%a0IKMAN,%20Lilja&spage=45&pages=45-48&sid=EBSCO:Academic%20Search%20Complete:141517181> - *Information Systems Security, Development, Trends, Technical and Economic Challenges*
* <https://www.sciencedirect.com/science/article/pii/S0167404813000801> - *From Information Security to Cyber Security*
* <https://academic.oup.com/cybersecurity/article/6/1/tyaa003/5766337?searchresult=1> - *SMART: security model adversarial risk-based tool for systems security design evaluation*
* <https://study.com/academy/lesson/systems-security-firewalls-encryption-passwords-biometrics.html> - *Study.com, Lesson on Systems Security*

**Summary**:

The lesson from study.com provided a good overview of what system security is, and also what forms of system security are prevalent today. System security refers to the protection of information and property from corruption, theft, and other types of damage. The use of firewalls, data encryption, passwords, and other security countermeasures falls under the category of system security. According to the article from study.com, “Encryption is the process of encoding messages so that it can only be viewed by authorized individuals”. (Study.com, Systems Security: Firewalls, Encryption, Passwords & Biometrics”. Ecommerce and internet banking systems use encryption to protect sensitive information such as passwords and credit card information for users. Firewalls use a combination of software and hardware measures to filter files and unauthorized access from the Internet. This can protect systems from unauthorized network users or malicious viruses from the Internet. Study.com’s site also offered information on strong passwords, data encryption, and other helpful information on system security.

The article, ISO 27001 -- *Information Systems Security, Development, Trends, Technical and Economic Challenges* focused on the introduction and integration of system security methods to protect businesses, government, and other institutions from attacks and security threats. With the rise of information technology usage in companies and organizations, the need for system security has risen as well. The article details the cost analysis and implementation challenges of introducing security measures to systems. The article is peer-reviewed, and provides valuable diagrams and analyses on cost versus benefits for organizations adopting system security.

The article *From information security to cyber security*, taken from ScienceDirect’s database of scientific and medical research, focuses on the differences between types of security. The focus is mainly on differences between cyber security and information security. Most people use the two terms interchangeably, and the article highlights the importance of differentiating between the two terms.  The article lists examples of security risks and scenarios that help to separate cyber and information security. To summarize the article’s findings, the conclusion stated,

“Information security is the protection of information, which is an asset, from possible harm resulting from various threats and vulnerabilities. Cyber security, on the other hand, is not necessarily only the production of cyberspace itself, but also the protection of those that function in cyberspace and any of their assets that can be reached via cyberspace”.  (*From Information security to Cyber security*, Rossouw von Solms, Computers & Security vol. 38 pgs 97-102)

I think that articles like this one are especially useful for understanding systems security. While looking for articles on the topic it was very easy to come across results dealing with many different types of system security topics and I could see how the topic would be very confusing to nonprofessionals. It is for that reason that I chose mostly introductory and explanatory articles as my sources of research for Systems Security.

The final article is on SMART, an attack graph security risk tool. The tool is designed primarily to evaluate systems for vulnerabilities and other problems. SMART uses an attack graph to collect information and determine which security solution would be best for scenarios based on costs and monetary value. The tool is valuable because of its ability to efficiently and automatically provide useful information that professionals can look at to help them determine which security solutions are more efficient in terms of cost and also implementation difficulty. I chose this article because it was a direct example of a system security tool designed by professionals for cybersecurity evaluations.