Levi George

10/12/2020

CS 30600: Computers in Society

Professor Chansavang

Cybersecurity in Medicine

Computer Security is a vital thing in most industries. Without it, sensitive data can be breached by hackers or through corporate espionage. Worst yet, people can have savings stolen from them, millions of dollars can be stolen from banks and other companies, which in turn can harm the economy. However, it doesn’t stop at finance and banking industries, if computers are not secure in the field of medicine people can die. If someone gets the wrong amount of medicine during some treatment they can go into a coma or become irradiated during chemo.

It is important to improve security in hospitals and the software and hardware that are utilized in their systems. Common types of vulnerabilities can range from reverse engineering to software vulnerabilities and even physical attacks. A lot of companies will utilize reverse engineering, often because it is less expensive than Research and Development for new algorithms or software. Vulnerabilities can arise from unsecure firmware updates and overlooking physical attacks on a system. However, it is possible to reduce these vulnerabilities by tracking devices, knowing where vulnerabilities occur in the Software development life cycle and avoiding assumptions of safety.

Knowing these things is important in any computer field. Securing your software protects your users. Cleansing your database inputs protects your company and the user information. Networking securely can protect you and others from computer viruses. It is an essential part of any degree to program and learn security. Otherwise you sacrifice the privacy and security of others.

Works Cited

Zorz, Zeljka. “How to build up cybersecurity for medical devices.” *HelpNetSecurity*. October 12, 2020. <https://www.helpnetsecurity.com/2020/10/12/how-to-build-up-cybersecurity-for-medical-devices/>. Accessed Oct. 12 2020.