Network Architecture

Morgan Villano

CYB 605 – Principles of Cybersecurity

Utica College

Abstract

Begin typing your abstract paragraph here. The abstract is a brief summation of your paper. **Lab Reports do not require an abstract.** The abstract allows readers review the key points and purpose of the paper. **The abstract should not be indented, and should be between 150 and 250 words.** After the abstract, there is a page break. The body of the paper will start on the next page. This should be accurate, well written, and concise. This is the most important single paragraph in this paper.

*Keywords:* Enter any key words used to research the subject

Network Architecture

**Results and Analysis**

**Application Vulnerabilities**

The Green Button is an industry-led effort that responds to a white house call-to-action to provide utility customers with easy and secure access to their energy usage information in a consumer-friendly and computer-friendly format (“Green Button | Department of Energy”, n.d.). The Green Button Connects the customer’s data. This allows utility customers to make an automated secure transfer of their energy usage data to third parties. This is based on affirmative (opt-in) customer consent and control (“Green Button | Department of Energy”, n.d.)  
 On the electric utility websites, customers can securely download their detailed energy usage with a simple click of a literal “green button”.

Many utilities have been committed to the Green Button and implementing it such as; Ameren Illinois, American Electric Power, Austin Energy, Baltimore Gas & Electric, Bangor Hydro Electric Company, CenterPoint Energy, Central Maine Power, Chattanooga EPB, Commonwealth Edison, Connecticut Light and Power, Consolidated Edison, Efficiency Vermont, Glendale Water, and Power, JEA, Kootenai Electric Cooperative, Inc., National Grid, NSTAR, Oncor, Pacific Power, PacifiCorp, PECO, Pepco Holdings Inc., PG&E, PPL Electric Utilities, Public Service Company of New Hampshire, Reliant, Rocky Mountain Power, Sawnee Electric Membership Corporation, SDG&E, Southern California Edison, The United Illuminating Company, TNMP, TXU Energy, Virginia Dominion Power, Western Massachusetts Electric Company and finally Yankee Gas ((“Green Button | Department of Energy”, n.d.).

As much as the customers want to believe that these web applications are securing their sensitive and private information 100%, there is always a way to breach any system or web application. The existence of vulnerable applications and outdated versions can cause website application vulnerabilities (“SecurityScorecard Cyber Risk Factors Explained ..”, 2020). The energy utilities are installing hundreds of “smart meters”. The off switch creates security vulnerabilities for the companies that use the green button. These automated secure transfers can cause the ideal attack on a target country which can interrupt the electricity supply. A utility attack can be a “cyber equivalent of a nuclear strike” (Anderson & Fuloria, 2010). Attacks on the transmission and distribution assets can cause a “Cyber equivalent of a nuclear strike”. To interrupt the supply, and software upgrades, the combination of commands will cause it to interrupt. The cryptographic keys are used to authenticate the commands and software changes. This can create a vulnerability (Anderson & Fuloria, 2010). A Social engineering attack can occur on customers that are a part of “Green Button”. The customer might get a vishing attack or even a spear-phishing attack that can occur by impersonating someone specifically from the green button or the utility company to gain sensitive information about the customer. A vishing attack is when the “Visher might first send a text message to potential victims in high volumes from a long list of phone numbers. The message might ask users to make a phone call to the attacker’s number” (“What Is Phishing? - Definition, Types of Attacks & More | Proofpoint US”, 2021). The attacker can obtain credentials to access their account where they can find the customer’s financial information (knowbe4, 2022).

The Green Button is also an app that consumers can download on their phones to track the usage of energy and electricity not just tracking it through an online website. A mobile application can cause many security vulnerabilities. If the mobile applications are developed poorly, it can cause data to be exchanged between the client and server-side. The attackers can then be able to view sensitive data in transit (Data Defense, 2020).

In the 21st century, there is a demand for cleaner more efficient energy. As much as going digital can help with environmental purposes, it can cause a big weakness within the utility sector. “Going digital can expand the attack area to not just nation-state actors but also cybercriminals overall” (Layton, 2022). For example, “The pipeline distribution management, solar of wind generation and bulky electricity systems and increase internet-enabled, introducing greater cybersecurity risks” (Layton, 2022). Back in 2021, malicious actors from China and Russia caused disruption to the Colonial Pipeline Systems that originated in Houston Texas by implementing a ransomware attack on the pipeline. This caused a shortage of fuel and jet fuel across 17 states.

Many countries and companies throughout the world, not just the United States do not know the importance of assessing and determining the vulnerabilities within their critical infrastructure (Layton, 2022).

# Conclusion

The conclusion is a synthesis of key points of the report. For most reports in this class, one well-written paragraph is sufficient, in some cases; a two or three paragraph conclusion may be required (University of Southern California, 2016). There are some general rules for writing a conclusion, which include: State your conclusions in clear, simple language; do not reiterate your results or the discussion, provide an analysis of the information presented in the paper, and do not introduce any new information (University of Southern California, 2016).

**From the rubric**: Be sure to go back and reread your introduction and objective before writing your conclusion. Examine the results that you obtained. This section should be short, concise and to the point. Your conclusion should be tied to the objective of the lab. Was the objective for the experiment met? State whether or not you achieved your objective. What are your opinions of the software that you used? Relate your opinion to what you do at your job or where you think tools like this could be useful. Essentially, what did you learn from working on the lab? A strong paragraph should be enough.

**References:**

Anderson, R., & Fuloria, S. (2010, July 29). *Security Vulnerabilities of Smart Electricity Meters. Retrieved May 21, 2022, from* [*https://www.schneier.com/blog/archives/2010/07/security\_vulner.html*](https://www.schneier.com/blog/archives/2010/07/security_vulner.html)

Data Defense, C. (2020, June 29). *OWASP Top 10 Mobile Vulnerabilities Developers Need to understand. Retrieved May 21, 2022, from* [*https://www.cypressdatadefense.com/blog/owasp-mobile-top-10-vulnerabilities/*](https://www.cypressdatadefense.com/blog/owasp-mobile-top-10-vulnerabilities/)

Green Button | Department of Energy*. Retrieved May 21, 2022, from* [*https://www.energy.gov/data/green-button*](https://www.energy.gov/data/green-button)

Knowbe4. (2022). *What is Social Engineering? from* [*https://www.knowbe4.com/what-is-socialengineering/#:~:text=Social%20engineering%20is%20the%20art,CEO%20Fraud%20are%20all%20examples*](https://www.knowbe4.com/what-is-socialengineering/#:~:text=Social%20engineering%20is%20the%20art,CEO%20Fraud%20are%20all%20examples)

Layton, R. (2022, May 12). *The Tech To Make Green Energy More Efficient Also Increases . Retrieved May 21, 2022, from https://www.forbes.com/sites/roslynlayton/2022/05/12/the-tech-to-make-green-energy-more-efficient-also-increases-cyber-risk/*

What Is Phishing? - Definition, Types of Attacks & More | Proofpoint US. (2021*). Retrieved May 21, 2022, from https://www.proofpoint.com/us/threat-reference/phishing*

SecurityScorecard Cyber Risk Factors Explained . (2020, November 2)*. Retrieved May 21, 2022, from* [*https://securityscorecard.com/blog/securityscorecard-10-risk-factors-explained*](https://securityscorecard.com/blog/securityscorecard-10-risk-factors-explained)