Article Analysis

Dylan McCann

7/21/2024

This article goes over the risks of the rapid expansion of IoT devices and how their poor regulation and quality can put people at risk. They conduct a systematic mapping review of relevant literature to better understand the current problems with IoT devices and how they relate to cyber incidents and look to provide a road map for future work and possible solutions.

To better understand this article and how it relates to cybersecurity and its impact socially, we will be looking at three ways this article uses principles of social science. The principle the article showcases is objectivity. Within the article it is discussed that this is an overview of the current literature, and they are seeking to only find current trends and offer possible explanations and examples of how some seem to be mitigating disadvantages. The second principle showcased is determinism, determinism is showing that behavior is caused, this is discussed in the article when talking about how the collection of personal data has been profitable since before widespread IoT devices, so it also affects emerging IoT fields such as smart devices and wearable that have even more access to personal identifiers, allowing for better tracking. The last principle I will discuss is parsimony which looks to explain things as simply as possible, the article achieves this by condensing down a large pool of literature from different industries to showcase trends in different security concerns in a more digestible format, using tables, graphs, and explanations of overall findings.

There is not an actual hypothesis to this article as it is an overview of findings from a collection of studies, but the main research question is what the current state of privacy issues in the context of IoT is, with specific emphasis on how personal data storage policy could help mitigate such challenges. The three main questions presented within the mapping for this study are 1. What are the main foci of the published studies regarding privacy within the IoT domain? 2. What issues are addressed by Personal Data Stores in the IoT context? 3. How have Personal Data Stores been used to address privacy issues in a general context?

The main research method conducted by the article is overall literature review and systematic mapping of different studies, compiling relevant information that can be compared across different sectors to gain a clearer picture of the problems facing IoT privacy within the technological space. It examines areas such as smart devices in private and public sectors, current attack strategies, challenges of security programs, data storage and farming, and technologies within industrial, commercial, and public sectors. They used five different databases with totals of over one hundred relevant studies for different contexts and questions. They also took effort to remove any studies that were duplicates and required studies to be academically relevant such as academic journal articles, book chapters, or conference papers with the majority of relevant studies having been published within the past 5 years.

The article relates to concepts in class in multiple ways. The first way is through social engineering, the discussed topics on IoT vulnerabilities and the information that it has access to, and how these attacks are conducted all relate to social engineering as many of these attacks where committed through phishing schemes, and many of these attacks looked to steal personally identifiable information that could be used to tailor possible attacks to victims in a manor more relevant to them. The article also relates to the idea of cyber victimization, specifically hyperbolic bias, this study highlights the ever-growing concern with security vulnerabilities pertaining to personal identifiers and how companies that farm large amounts of data need to be vigilant and act preemptively as when security breaches happen it can be catastrophic for individuals who use these networks. Another relation is the social paradigm of conflict theory where those in power can create inequality through the use of that power, this is shown in the article through the idea presented in the article of profiling, where companies use data gathered and analyzed about individuals to categorize them based on characteristics, profiling can be a problem if not properly accounting for outside factors such as race or socio economic background so those that are creating profiling algorithms must act carefully to not put any extra risk on those that may be negatively affected. Lastly, a topic in class that relates to the article is psychological awareness about cybersecurity where people need to be trained to and updated about cybersecurity practices to stay safe if the system will not do it for them, one thing brought up is information leakage, when breaches do occur, consumers should be made aware as it would be difficult for any person to keep track of all possible data leakages related to their data.

The idea of IoT vulnerabilities relates greatly to minorities as leakages of data can be much more costly to those that are handicapped or of a protected groups as it may be more difficult for them to have the resources required to adequately track accounts for possible identity theft. The other idea of profiling due to data farming also relates greatly as these companies develop algorithms based on those data sets it could cause discrimination if not properly accounted for.

Possible contributions of this work could end up being roadmaps for better security in IoT devices as it has stated the data collected on the effectiveness of already implemented strategies, and it could lead to a legislation roadmap for policy makers that would allow them to implement laws that would help ensure companies are taking best care and implementing safe practices to protect the consumers.

**Article Reviewed**

Pinto, G. P., Donta, P. K., Dustdar, S., & Prazeres, C. (2024). A Systematic Review on Privacy- Aware IoT Personal Data Stores. *Sensors (14248220)*, *24*(7), 2197. https://doi- org.proxy.lib.odu.edu/10.3390/s24072197