Thesis Project Portfolio

Hydrologic Modeling and System Optimization for IoT Flood Management

(Technical Report)

Privacy and Security Risks from Cybersecurity Attacks on Third-Party APIs in Flood Monitoring

(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Nicolas Khattar

Spring, 2023

Department of Information and Systems Engineering

Table of Contents

Sociotechnical Synthesis

Floods are a growing concern in Charlottesville, Virginia, as the area is prone to heavy rainfall and flash flooding. In August 2021, Charlottesville experienced severe flash flooding that damaged homes, businesses, and roads. Several steps are being taken to address the issue. However, the risk of flooding remains a significant concern for Charlottesville residents and businesses. One of the solutions is the Internet of Things (IoT) sensors. They provide real-time data on water levels, precipitation, and weather conditions. Our team deployed two sensors in the Dell pond, a flood-prone area in Charlotteville, and created a hydrologic model of the watershed and battery life prediction models. The LoRaWAN communication protocol is used to connect the sensors to the network server. A third-party Application Programming Interface (API) like "Grafana" is used to display the information for the managers to take decisions. Third-party APIs are created by people, and therefore they are imperfect and prone to insecurities. The most important risk is from cybersecurity attacks. This is a fairly new technology and is prone to cyberattacks that can affect people's privacy and security without them noticing and cause devastating damage. Actor-Network Theory (ANT) is the theoretical framework I applied to the study of this complex socio-technical system. ANT helps us understand the different actors and their relationships that can contribute to cybersecurity attacks. It is a useful framework for analyzing the flood alerting network and for identifying the factors that shape their impact on privacy and security.

In my research, I interviewed Angela Orebaugh, a professor at the University of Virginia who specializes in cybersecurity and privacy. I also read news articles, reports, and studies from 2018 until 2023 to register all the different events capturing third-party API cyberattacks, especially the ones connected to IoT devices affecting the privacy and security of the company, employees, and society. The sources are from major pioneers in cybersecurity like Gartner, Trustwave, and OWASP. At the end of my research, I found several drawbacks associated with using third-party APIs in flooding. Firstly, unencrypted sensitive data such as the location of flood-prone areas or personal employee information can be transmitted through them. Secondly, due to weak security protocols, hackers may gain unauthorized access to the APIs, leading to potential data loss or manipulation. Lastly, the flood monitoring system may be disrupted by malware infiltrated by hackers, resulting in false emergency alerts. Overall, this research will help water managers and their IT teams create preventive ways to reduce the risks and the privacy and security effects of cyberattacks on third-party APIs. The deployment of the sensors and the hydrological-battery models will serve as prototypes to help grow the IoT community.