High Resolution Satellite Imaging of Nitrogen Dioxide from Low Earth Orbit

(Technical Paper)

Smart Cities: An Inspection of Cybersecurity Vulnerabilities and Prevention

(STS Paper)

A Thesis Prospectus Submitted to the

Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree

Bachelor of Science, School of Engineering

Matthew Moore

Fall, 2019

Technical Project Team Members

Isabel Araujo, Genesis Brockett, Alex Brookes, Noah DeMatteo, Max Diamond, Sami Khatouri, William McNicholas, Matt Moore, Adelaide Pollard, William Schaefermeier, Huy Tran, Hannah Umansky

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature ____ Date __________

Matthew Moore

Approved ____ Date __________

Chris Goyne, Department of Mechanical and Aerospace Engineering

Approved ____ Date __________

Sean Ferguson, Department of Engineering and Society

Technical Report

The primary objective of this project is to develop a spectrograph suited to the constraints of a 3U CubeSat bus capable of measuring nitrogen dioxide (NO_2) columns at a spatial resolution better than 1 km^2 with a secondary objective of forming a basis for a new educational program that connects space sciences, engineering, remote sensing, and environmental science here at UVA. The data that is collected will be used for improving the understanding of NO_2 emissions and concentrations on urban landscapes. This is a continuation of the same 3U cubesat project that recent 2019 graduates were working on and will extend upon the time of this teams graduation in 2020.

The whole 3U team is composed of multiple subsystem groups with a couple of students in each group as well as working in collaboration with the Department of Astronomy and Environmental Science here at UVA. The five subsystem groups are attitude determination/control, communications, power/thermal/environmental (PTE), structures/integration, and software/avionics. As part of the power, thermal, and environmental team we are in charge of things such as thermal expansion or contraction of materials, radiation in low earth orbit, providing power to the satellite, and charge to the battery through solar panels. So far the 3U team has worked together to produce two presentations on the project with a third coming up on November 11th 2019. The first being the *Objectives and Constraints* in which the objectives, requirements, and constraints of the overall mission were defined, the primary players were identified, a rough timeline was established which can be seen in the Appendix as Table 1, and each subsystem team defined their individual objectives and constraints.

The second presentation was the *Definition of Mission Concepts and Design.* In this presentation we worked together to come up with alternative mission architectures, alternative mission concepts, and define the system drivers. The alternative mission architectures looked at alternative options for things like payload, the ground segment, orbit, and mission operations while alternative mission concepts looked at alternatives to things like the data delivery process, tasking/scheduling/control, and communications. At the end we had three alternative mission architectures and concepts to consider. While the structure of the mission was mostly already decided by last years class, this presentation made us look at what the team did last year and consider any changes we might make to the mission architecture and concepts. System drivers are principal mission parameters that can be controlled which influence cost, risk, performance, or schedule. In the end we decided on four main system drivers for our mission which are size/weight, communication/data transfer, coverage (orbit, controls), and power. A more detailed look at the system drivers can be seen in the Appendix as Table 2.

Our next presentation is the *Evaluation of Alternative Architectures* in which we look more in depth at the three architectures and concepts. This includes looking at important tradeoffs that come with each of the alternative mission architectures and concepts, the measures of effectiveness (MoEs), and deciding on a final mission architecture. The next steps we have for this mission are after the *Evaluation of Alternative Architectures* we have a technical report or preliminary design review at the end of this semester in December. Moving into next semester we are looking to secure funding in the spring to purchase some of the equipment that is needed for this mission as well as work on the critical design review throughout the semester so that the build phase may start in the summer of 2020 and hopefully launch sometime in 2021.

STS Research Paper

Introduction

A 2016 survey of chief information officers of cities and counties reported around 25% of local US governments were facing attempted cyber attacks every hour (Pandey, Golden, Peasley, & Kelkar, 2019). These types of attacks are on the rise as cities become more connected with an increase of 38% of global security incidents between 2014 and 2015 (Norwich University, 2016). Smart cities are a great example of how the implementation of modern technology into services such as transportation or public security can increase efficiency, safety, and well-being of the city and its citizens. The integration of IoT devices, such as sensors and cameras, into cities and homes are just one of the advancements that helps develop these cities. With the blending of technology and infrastructure, there is an abundance of user data that is now collected and stored by companies and governments. As these cities grow "smarter," the amount of data collected and the danger of cyber attacks rise. Through the technology transfer framework, this research will explore the vulnerability of smart cities to cyber attacks, as well as how organizations and cities are working together to combat the issue with the rapid rise in IoT devices and automated services.

Vulnerabilities in Smart Cities

Infrastructure in these smart cities is changing with the integration of systems for monitoring and automation of services. The number of IoT devices is expected to increase from 8.4 billion this year to almost 20 billion by 2020. (Pandey, Golden, Peasley, & Kelkar, 2019) This will enhance interconnectivity and efficiency of services, however, the risk of cyber attacks will rise. These types of attacks have momentous impacts on data or financial loss and even city infrastructure and services such as power and utility, transportation, or health care. In March of 2018, the city of Atlanta was targeted with ransomware on their city's connected systems. Ransomware is a type of malicious software that blocks access to a computer system until a ransom is paid, in this case the attackers requested a $50,000 payment in bitcoin. The malware disrupted programs dealing with law enforcement and court systems and citizens found themselves unable to do basic city-based tasks like paying parking tickets or utility bills. In June 2018, more than a third of the 424 software programs used by the city were still offline or partially disabled. This attack cost the city $2 million in emergency procurement, as well as an additional $9.5 million added to the original $35 million budget allocated for the Atlanta Information Management. This is just one example from the past year of the damage these cyber attacks can really have on a city. These types of attacks are not domestic, but happen everyday all around the world, targeting large corporations, government entities, and your everyday citizen.

Despite these dangers, the research into the vulnerabilities of smart cities is relatively new. There are many weaknesses but for the purpose of this research they can be broken into two critical sections for smart cities worldwide. The first being how a city's infrastructure can be compromised through its computer control systems like in the attack in Atlanta. The implementation of industrial control systems (ICS) into modern city infrastructure has allowed the control of these systems to be done remotely through the internet. Recently there has been a push towards open standards for ICS devices instead of proprietary. As a result, hackers will be able to find a large amount of detailed knowledge on how these devices work and find vulnerabilities in them from the public domain (Joo & Tan, 2018). If these ICS devices become overtaken by hackers, they can control the entire infrastructure. For example, in 2015 Russian hackers took down Ukraine's power grid by subverting the ICS that controlled the power grid leaving 230,000 without power for hours. Ukrainian officials were luckily able to limit the severity of the attack by switching back to manual control (Joo & Tan, 2018). The outcome of such an attack would likely be much worse in a smart city due to the interconnectivity of these infrastructures. A collapse of one system has the potential to result in a domino effect shutting down multiple systems and services.

The second crucial vulnerability stems from the smart cities being susceptible to attacks through poorly protected edge devices with limited computing power, firewall protection, or anti-virus protection. Research shows that many IoT devices such as sensors, cameras, or smart-meters in these smart cities are both digitally and physically vulnerable. Digitally, in the sense that the devices lack security measures such as anti-virus protection or firewalls. This leaves them vulnerable to cyber attacks. Physical vulnerability refers to the possibility of tampering or the installation of modifications. The root of this vulnerability is the necessitation for these devices to be left in the wide open (Joo & Tan, 2018). Things like smart gas or electricity meters, surveillance cameras, and smart traffic lights are examples of such devices. These risks are compounded by the fact that many of these devices are mass produced. Once a successful cyber attack is engaged on one of these devices, it can be replicated on the entire product line. Each device is produced in a large homogeneous batch.

Steps Towards Greater Security

To combat the first issue of the vulnerability of ICS devices, organizations are working together with network providers, government agencies, and industrial associates to provide response to computer security incidents, research and analysis of such incidents. Ultimately these efforts will help disseminate this information to better inform the public. One such organization is the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) who is working on proactive security measures in Japan. These measures include providing guidelines and best practices for ICS security, security assessments of important Windows systems, and security assessments of ICS personnel (Abe, Fujimoto, Horata, Uchida, & Mitsunaga, 2016) . JPCERT/CC also provides a middle-man connecting these entities that use the ICS devices to the cyber security industry to improve security measures and promote proactive approaches. These efforts are determined to prevent attacks from happening.

Addressing the second critical issue of IoT devices, many countries are seeing legislation introduced to have these devices meet certain security requirements and regulations, but the legislation is often not realized. There are concerns that restrictions may hinder IoT innovation and development. While many formal policies have not passed through US Congress on IoT security, the US federal agencies are still very much involved in support of the IoT by providing direction on standards of development and interoperability. The FTC published guidance on how to build security into IoT devices for businesses and the Department of Defense published *"Strategic Principles for Securing the Internet of Things,"* which discussed security issues of IoT devices as well as provided principles for responsible cybersecurity practices (Chatfield & Reddick, 2019). This sort of minimalist approach to IoT policy making was seen in the UK as well, but as of late there has been a push towards real government regulations of IoT devices. While no official policy has been passed on IoT devices directly, they fall under the scope of other laws that are being changed or updated. For example, in 2016 the EU passed the General Data Protection Regulation (GDPR) which went into effect in the UK in May of 2018, unaffected by their decision to leave the EU. The GDPR introduced the two principles of "data protection by design" and "data protection by default" meaning that products must have data integrity defenses built in from the earliest stages of development (Tanczer, Brass, Elsden, Carr, & Blackstock 2019). This will have a massive impact on how IoT providers develop their products as well as how they collect and store data as they are pushed into making more secure devices.

Conclusion

It is clear that cyber attacks can affect enormous amounts of people, cause extensive damages, cost millions of dollars, and can happen at home or abroad. As we progress towards smarter technology and tighter regulations on the development of this technology, these attacks will become more sophisticated to defeat security measures. There is no clear solution to this problem, as it is a dynamic landscape that evolves constantly. The implementation of more secure systems into smart city infrastructure as well as smart governing policies or principles on the development of IoT devices and data protection are steps in the right direction. Communication between industries in which these cyber attacks are prevalent and the cyber security industry is key to future prevention of these constantly changing security threats. This sharing of knowledge will promote smarter cybersecurity practices in the future as well as introduce a symbiotic relationship between the two industries. As these attacks become smarter it will be crucial for governing agencies to adapt and react to the rapidly changing world of cyber security.

Bibliography

Abe, S., Fujimoto, M., Horata, S., Uchida, Y., & Mitsunaga, T. (2016). Security threats of Internet-reachable ICS. *2016 55th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE).* doi: 10.1109/sice.2016.7749239

Chatfield, A. T., & Reddick, C. G. (2019). A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government. *Government Information Quarterly*, *36*(2), 346–357. doi: 10.1016/j.giq.2018.09.007

Joo, Y.-M., & Tan, T.-B. (2018). Smart Cities: A New Age of Digital Insecurity. *Survival*, *60*(2), 91–106. doi: 10.1080/00396338.2018.1448577

Tanczer, L. M., Brass, I., Elsden, M., Carr, M., & Blackstock, J. (2019). The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. In R. Ellis & V. Mohan (Eds.), Rewired: Cybersecurity Governance (pp. 37–56). Hoboken, New Jersey: Wiley

The Rise of Cyber Threats. (2016). Retrieved November 7, 2019, from https://online.norwich.edu/academic-programs/masters/diplomacy/resources/infographics/the-rise-of-cyber-threats.

Pandey, P., Golden, D., Peasley, S., & Kelkar, M. (2019, April 11). Making smart cities cybersecure. Retrieved November 6, 2019, from https://www2.deloitte.com/us/en/insights/focus/smart-city/making-smart-cities-cyber-secure.html#endnote-sup-3.

Hatmaker, T. (2018, June 7). The damage from Atlanta's huge cyberattack is even worse than the city first thought. Retrieved November 6, 2019, from https://techcrunch.com/2018/06/06/atlanta-cyberattack-atlanta-information-management/.

Appendix

Task	Date
Conceptual Design Review	May 2019
Benchtop Spectrograph Testing	Summer 2019
Spectrograph Proof of Concept	December 2019
Preliminary Design Review	December 2019
Additional Funding Obtained	Spring 2020
Critical Design Review	May 2020
Build Phase	May 2020 - May 2021
Integration/Launch	Summer/Fall 2021

Table 1: Estimated Timeline of Mission created by 3U team

Driver	**What Driver Limits**	**What Limits Driver**
Size & Weight	Available payload specifications, ADACS, externally mounted components	3U dimensions (CubeSat form factor), dispenser system, LV available space, critical hardware, scientific instruments
Communication & Data Transfer	Data transmission rate, responsiveness to commands, data transfer (volume) per cycle	Ground station capability & reliability, orbit path, onboard data storage, antenna types, carrier frequency
Coverage (Orbit, Controls)	Spatial resolution, temporal resolution, geolocation, accuracy, data collection, precision, mission lifespan	Cost, weight, available volume for ADACS, orbit, orientation of instrument, deployment method
Power	Operational time, data transfer, heating/cooling abilities, data collection time	Battery size, time in Sun/eclipse, solar panel efficiency, solar panel configuration

Table 2: System Drivers defined by 3U team