Prospectus

Staunton Makerspace Communication Management System
(Technical Topic)

The United States Government's Role in Shaping the Field of Cybersecurity and its Related Technologies
(STS Topic)

By

Michael Wood

10/30/2019

Technical Project Team Members: Evan Typanski, Michael Laterza, Samuel Ting

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.

Signed: _____

Approved: _____ Date _____
Rider Foley, Department of Engineering and Society

Approved: _____ Date _____
Ahmed Ibrahim, Department of Computer Science

Introduction

In any community where there is a management structure, as well as a hierarchy of membership, one of the most important things that must be present is good, thorough communication. That is to say, the information that is disseminated to the full membership (and smaller subsets thereof) should be delivered to exactly its intended recipients, in its intended form, in a timely manner to allow for response. Mathieu and Woodard outline these concepts under the umbrella term data quality, saying that data quality can be measured using the metrics of "accuracy, timeliness, and consistency," and that these characteristics are necessary to ensure "good decision-making" (1996, p. 93). The Staunton Makerspace, located in the West End of Staunton, VA, is an example of one such community. The Makerspace occupies a building which houses a multitude of creative equipment, such as laser cutters, 3-D printers, and bandsaws. The Makerspace is made up of members, or people who pay dues and regularly make use of the provided equipment. Members can also be part of "Guilds," or sub-groups of members with a focus on one specific Makerspace offering, e.g. the 3-D Printing Guild. Under this organizational framework, Makerspace members can achieve maximum communication efficiency if they are able to message whomever they want and have the message seen by the intended recipient (or recipients) as soon as possible within specific guilds.

Herein lies the problem the Makerspace is currently facing. The Makerspace's current work practice with respect to intra-membership communication is to use Slack, which is an instant messaging application. According to a customer representative at the Makerspace, many members find Slack to be confusing, inaccessible, and/or overwhelming. Harrison et al (2008) writes that the main charge of a computer system is to enable and enhance communication between the machine and person. Our team's customer at the Makerspace views the current work

practice, Slack, as not serving the goal of good communication in an effective way. Because of these issues, our team will develop a user-facing communication management system that brings the notifications to the users and reduces overall member effort to stay informed so that the Makerspace can run as effectively as possible.

Technical Topic

The Staunton Makerspace has a technologically diverse community of members. They have technologies including 3-D printers, woodworking tools, and electronics stations. This means enthusiasts and professionals with different skill sets are drawn to the Makerspace. As mentioned above, the current mode of communication used by members is Slack, and it is used alongside email. This is a fairly slow operation for them, as they must log into many different accounts. After logging in and sending a message, there is no guarantee that the other members will actually view their messages. Many members do not check Slack or their email, and the leadership wishes to create a better system to effectively communicate with all members of the Makerspace. This communication barrier decreases participation in the Makerspace and leaves many members uninformed, and our team has been tasked with lowering this barrier by creating a uniform communication system for the Staunton Makerspace.

Since the Makerspace provides a physical location that members go to, we are developing a “smart bulletin board” that will automatically show members both general and user-specific information once they scan their RFID (Radio Frequency Identification) chips to enter into the facility. This solution will provide all members with a centralized location to view any messages they may have from leadership or other members. With the added benefit of having a physical location that all members use, all members of varying technical abilities and strengths will be

able to promptly view any and all messages sent to them. This will help leadership and general members better share correspondence within the Makerspace community.

Our goals for this project are to develop a cloud-hosted web application for the Staunton Makerspace to enhance communication. In essence, our team desires to bring the notifications that need to be seen by each user directly to them, thereby reducing the amount of effort required to stay informed.

In order to ensure that our product meets our clients' expectations, we worked directly with them to develop a list of important system requirements that our team will continue to work on. Our team has been given several minimum requirements which must be met by the end of this semester. These include allowing users to use our system to send messages to other individuals, the entire membership of the Makerspace, or members of specific guilds. We must also make a display mode that the Makerspace can use to show notifications to members as they enter the building via a key fob. This display mode will be used in a kiosk near the entrance, so notifications must be clearly visible and kept relatively short. Our team also has desired requirements, which must be met by the end of next semester. The most significant of these is the task of displaying messages from all of the Makerspace's preexisting forms of communication, such as Slack and email, as additional notifications. Our system must also allow for users to create accounts and then subsequently log in to view personal messages without having to look at the kiosk display.

In addition, we have a set of optional requirements, and these requirements do not all have to be met by the end of the project. These include the ability for users to view information about their status in various guilds and current machine certifications, as well as giving users the ability to edit their guild membership. Another optional requirement is to be able to let users set

notification preferences for the display mode, and we also plan on showing various general notifications (and potentially a ticker for praising members) on the display when someone isn't entering the building. The minimum requirements, such as direct and general message sending capabilities, will be completed at the end of the Fall 2019 Semester. The optional requirements, such as styling with CSS and user notification preferences, will be completed prior to the end of the Spring 2020 semester.

Government's Role in Cyberspace

Paramount in the development of any system that relays information, especially sensitive or proprietary information, is security. The information that is going from place to place should not be able to be changed, nor should it be viewed by anyone other than its intended recipient, and the system itself should be robust against attacks from external actors. Briscoe (2000) states that to accomplish this, most systems today employ some sort of security on each layer of the OSI 7-layer Model, which is used to describe how applications interact through networks. The OSI 7-layer Model includes, from closest to user interaction to furthest away, the application, presentation, session, transport, network, data link, and physical layers. Such security measures, however, were not always in place. One group of entities with significant effect on the development of cybersecurity technologies is the United States Government, and more specifically agencies within the Executive Branch and the Department of Defense.

Explaining the relationship between the field of cybersecurity and the US Government is best done using the framework of Actor-Network Theory. One of the foremost research papers written on the subject of Actor-Network Theory (hereafter referred to as ANT) is Bruno Latour's "Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts." Latour's thesis is

that technologies in themselves are not passive objects, subject only to human agents. By their nature and design, they discriminate, and actually take on some agency and shape the human agents' interactions with them. Latour backs up his argument by making use of several case studies, the first of which is the door. Using ANT as a guide, analysis of the interactions between the door and humans becomes much more interesting. Doors are designed to allow humans to pass through an otherwise impenetrable wall or surface. This door serves as a substitute for having to do the work of getting through the wall by other means. The door has been delegated work or effort by the human "actor" in this case. It shapes the interactions that humans have with it based on its design.

Similar points can be applied to the field of cybersecurity, as well as the malware and networked systems that comprise it. Balzacq & Cavelty (2016) argue that the ANT framework can be used to understand the field of cybersecurity more completely. It treats cybersecurity as "both a process and an outcome" (p.176). This statement is best understood as an example timeline. First, a virus, or set of malware, is developed. The virus attacks a networked system and releases its payload. Affected by the malware, the network system must either improve its cybersecurity standard or face future attacks. The creators of the virus, in turn, must improve its their strategy and attack vector so that it is able to be effective in the future. In this way, the outcomes of cyber events have effects on both the human and non-human actors in the Actor-Network. Balzacq et al. map the characteristics of an Actor-Network, such as actors (both human and nonhuman), punctualization/depunctualization (the makeup/"breaking down" of different parts of the network), and spatial performance (entities/actants and their relations make up spaces) to aspects of cybersecurity.

One case that I will dive into is the Stuxnet Virus. Stuxnet was an aggressive worm, meaning cyber-attack that took aim at the SCADA (Supervisory Control and Data Acquisition) computing technology supporting Iran's nuclear program (Kenney 2015, p. 124). Although no entity has officially stepped forward to take credit for it, the worm was a result of a joint Israeli-United States effort, as reported in the New York Times by Broad, Markoff & Sanger (2011). Ultimately, the worm was able to incapacitate a significant portion of Iran's nuclear facilities. Stuxnet, as well as its developers and the researchers who studied its effects following its impact, become actors within the network which also includes the physical space of the Iranian nuclear program computers.

Another case that I will analyze is the Distributed Denial of Service (DDoS) attack that was levied against that country of Georgia in 2008. Korns and Kastenberg (2009) write that as a result of this attack, Georgian governmental websites were rendered largely unusable. Following this, the government of Georgia transferred much of its critical information to servers located in the United States. For example, "Ministry of Foreign Affairs media releases and government news sites [were transferred to] Google's Blogspot" (Korns et al. 2009, p. 67). The US did not take much action, and these servers were later attacked by some of the same DDoS attacks. The article asks the question: "can the United States remain neutral (or cyber neutral) during a cyber conflict?" (Korns et al. 2009 p. 61). Again, I will analyze this case and this unique question in terms of the ANT framework.

Research Question and Methods

How has the United States Government shaped the field of cybersecurity and its technologies in the last quarter century, and how might this inform future actions and outcomes?

Such a topic is important to analyze because the United States Government is a heterogenous actor that has a great degree of influence at a global scale. Analyzing the cybersecurity events in the past quarter century, the government's role in those events, and the way that the technology was shaped will be useful for informing future action. I will be analyzing the topic using historical case studies. I plan on identifying major cybersecurity events in the recent past, discerning the US Government's role, and then applying Actor-Network Theory in order to more deeply understand the situations. One such cybersecurity-related governmental action that I plan on analyzing is the Office of Budget & Management's "Policy to Require Secure Connections across Federal Websites and Web Services" (Scott 2015). The policy affects the technology that the Federal Government is able to use with regard to website services. Such a policy can be interpreted as a constraint, but in reality, as technology develops it will serve to modify the relationships between actors (human and nonhuman) in the Government space. I will also analyze Landwehr's personal perspective on the history of cybersecurity as an in-depth case study. Landwehr (2010) conducts an inquiry into how government funding has been allocated to cybersecurity research, and how such allocation has affected the growth of cybersecurity as a field.

In terms of methods, I will interview professors from the Computer Science Department at the University of Virginia. Specifically, I will interview Professors Aaron Bloomfield and Ahmed Ibrahim. In the Fall Semester of 2019, Professor Bloomfield is teaching CS 3710: Introduction to Cybersecurity. He also has cybersecurity listed under "Research Interests" on his department profile page. Professor Ibrahim is teaching CS 4760: Network Security and also lists cybersecurity as a research interest. Additionally, I will interview Professor Brad Carson of the Frank Batten School of Leadership and Public Policy at U.Va. Professor Carson teaches a course

called “Hacking for Defense,” and served as Under Secretary of Defense for Personnel & Readiness at the Department of Defense during the Obama administration. I believe Professor Carson will be able to offer a perspective that will enhance the accuracy of my Department of Defense knowledge, as his experience within it is extensive. Interviewing professors will lend a degree of expertise to my research, and because all are professors here at U.Va., it will be convenient for all parties involved. I will also contact Ellen M. Lord, Under Secretary of Defense for Acquisition, Technology, and Logistics, and inquire about in interview to gain an up-to-date view into the Department of Defense’s technology use. I will gain useful data originating from experts within the fields of cybersecurity and government in order to clarify my main points. I also hope to utilize these interviews to inquire about additional relevant resources (both social and technical) that I might not previously have been aware of for use in my Thesis. Following these interviews, I will use the claims and evidence provided to me in order to analyze and contextualize, using the STS framework identified above, the case studies that will make up a significant part of my Thesis.

Conclusion

The technical capstone project will be completed over the course of the 2019-2020 academic year. At a high level, the first semester of the year will be devoted to developing a minimally shippable product, meaning a system that includes all of the minimum requirements but has not been refined or tested to a great extent. The second semester’s work will be focused on that refinement element and making quite sure that the system we are developing is solving the problem identified in the best way possible. Work throughout the year will be done within an Agile Scrum methodology, with 2-week “sprints” during which specific small-scale aspects of

the system will be completed. In terms of the STS research paper, I expect to land upon an informed estimation about how the interactions between government and the field of cybersecurity will look in the future, as cyber threats become more complex and aggressive. In the first week of the Spring 2020 semester, I will begin contacting the people I have identified as interviewees. During this time, I will contextualize the information gained from interviews with my findings from the historical case study analysis in order to find common themes and answer the question identified above. I estimate that research and writing will take approximately a month and a half each, so I plan on completing my Thesis towards the end of March 2020.

To reiterate from the technical topic section, this solution will bring all relevant notifications to the direct attention of the user that they are intended for. To put it in Latour's ANT terms, our team's system will enforce the program of action (sociological requirement based on the design of a system) that if a member has swiped into the Makerspace, he/she has seen and processed all relevant notifications.

References

Balzacq, T., & Cavelty, M. D. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, 1(2), pp. 176–198. doi: 10.1017/eis.2016.8

Briscoe, N. (2000). Understanding the OSI 7-layer model. PC Network Advisor, 120(2).

Broad, W. J., Markoff, J., & Sanger, D. E. (2011, January 15). Israeli test on worm called crucial in Iran nuclear delay. *New York Times*, 15, 2011.

Harrison, S., Tatar, D., & Sengers, P. (2007). The three paradigms of HCI. alt. In *CHI'07*.

Kenney, Michael. (2015). Cyber-Terrorism in a Post-Stuxnet World. *Orbis*. 59. 10.1016/j.orbis.2014.11.009.

Kerr, P. K., Rollins, J., & Theohary, C. A. (2010). The stuxnet computer worm: Harbinger of an emerging warfare capability. Congressional Research Service: Washington DC.

Korns, S. W., & Kastenberg, J. E. (2009). Georgia's cyber left hook. Army War College Carlisle Barracks PA Strategic Studies Institute. pp. 60-76

Landwehr, C. E. (2010). History of US Government Investments in Cybersecurity Research: A Personal Perspective. 2010 IEEE Symposium on Security and Privacy. doi: 10.1109/sp.2010.41

Latour, B. (1992) 'Where are the missing masses? The sociology of a few mundane artifacts', in Bijker, W. E. and Law, J. (eds) *Shaping Technology/Building Society: Studies in Sociotechnical Change*, Cambridge, MA, MIT Press, pp. 225-58.

Mathieu, R. and Woodard, R. (1996), "Data integrity and the Internet: implications for management", *Internet Research*, Vol. 6 No. 1, pp. 92-96.

Scott, T. (2015) *Policy to Require Secure Connections across Federal Websites and Web Services.* Office of Management and Budget, Washington DC.