Prospectus

The Economic and Technical Viability of Dedicated, Independent Web Hosting
(Technical Topic)

Cyber-Security in the Residence: An Application of Actor-Network Theory
(STS Topic)

By

Sean Benish

April 5, 2021

Technical Project Team Members: N/A

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: Sean Benish
Technical Advisor: _____
STS Advisor: _____

Introduction

The Internet facilitates interaction across vast physical distances. Social media then revolutionized how people interact (Jimenez & Morreale, 2015). Currently, concern grows among the people of the United States as major data breaches and misuse puts them in jeopardy (McCarthy, 2018) (Knutson, 2021). At this crossroad in time, new paradigms for social interaction online become considerable. Federated social media, for instance, can minimize the privacy threat by centralizing the user's data closer to the user. With a federated system, information spreads across the network, hosted by those who own it. In practice, this entails linking one's account to a node or creating a new node (Mastodon, 2017). Despite its significantly improved privacy protection, federated servers—especially one-user servers—become costly for long-term use (Carmichael et al., 2020). Yet, a gap exists for a general-purpose, low-cost device for hosting federated content. Therefore, the viability of such a device should be addressed.

As the Internet of Things in the home expands, cybersecurity at home must reinforce itself. If social media threats turn towards a home environment, a less secure space, then the privacy problem would only escalate. Institutional suggestions for securing home networks already exists (U.S. Cybersecurity and Infrastructure Security Agency, 2020) yet cybersecurity literacy lags (Furnell & Moore, 2014). Moreover, if federated networks increase in popularity, then the goldmine of user data also migrates to the home. Therefore, cybercrime may become more profitable, another inhibitor. Although businesses and organizations can rely on internal security teams and documentation to keep security up-to-date, home users do not have such luxuries. Some devices update themselves when needed, but keeping up-to-date becomes challenging for others, especially IoT devices (Lu & Xu, 2019). As a result, a detailed examination of cybersecurity in the home environment must come forth.

The Economic and Technical Viability of Dedicated, Independent Web Hosting

With all the personal information that social media stores, hackers target these centralized data stores. Despite the threats, social media still collects more information on its users (Leetaru, 2018). In addition, data breaches leak personal information and hijack other user accounts (Mitra, 2020). To enhance support of federated content, resolve privacy concerns, and reduce leaks of personal information, a stand-alone, dedicated machine for hosting a user's social media content should exist and be viable. It can enable an alternative social media experience to protect the public's data by spreading sensitive data out, data breaches becoming less lucrative. Furthermore, the standardized protocols for this content only recently formed (World Wide Web Consortium, 2018), so applications are few. The device should compete fiercely with alternative content-hosting options, and function in a wide variety of network capabilities. If successful, this research would provide justification and groundwork for engineers to create devices in this niche.

Under the assertion that the device needs to be as simple as possible, the field of embedded research gives a baseline with which the device can be built upon. Groba and

Clarke (2010) investigated using web-enabled technologies on small, embedded-level devices and demonstrated the overhead between different communication technologies. The quantitative data given from this study will be used to retroactively estimate hardware requirements based on networking capabilities. With the hardware sorted, Kyusakov et al. (2014) provide the Efficient XML Interchange (EXI) for fast, low-usage XML communication between web servers. Finally, the World Wide Web Consortium provides ActivityPub, a web protocol for managing user content and communicating between server, the core of the design and of the requirements.

The research begins with a literature review of economic data (rented server hosts, energy usage, etc.), social media server usage, embedded technologies for hosting web content, and residential networking capabilities. In addition to scholarly journals, libraries and open-source resources will be investigated. By the end of this phase, the researchers can justify estimates for bandwidth and storage requirements, infer which households can use them, and suggest libraries and frameworks useful for implementing ActivityPub on an embedded device. Afterwards, the researchers will begin the prototype stage. Based on the requirements estimated, storage devices and networking devices will be selected followed by the embedded controller acting as the web server. During this design stage, custom hardware for server processing can be considered and implemented if cost-efficient. Finally, the researchers will implement and benchmark both the web server and the ActivityPub protocol. Specifically, quantitative data on bandwidth, throughput, and latency associated with uploading, downloading, and communicating with the webserver will be needed. For the qualitative data, bottlenecks and design limitations must be known. To benchmark ActivityPub, utilizing the device for an existing protocol such as Nextcloud will give information of performance. Similar quantitative data can be collected for these tests.

Cyber-Security in the Residence: An Application of Actor-Network Theory

In 2016, Balzacq and Cavelty contextualized cybersecurity as the formation of a stabilized actor-network. In their paper, they describe how cyber threats target parts of this stable system and cause depunctualisation—the transition into an unstable network. With this framework, the researchers applied their model to understand the political implications of cyber incidents, such as cyber-attacks. In cybersecurity, a hole remains mostly empty—an understanding on how the average person approaches cybersecurity. Researchers have already examined outcomes of cybersecurity across age groups (Jiang et al., 2016) and provided tools for managing their cybersecurity (Alotaibi et al., 2020), but an in-depth, generalized model for understanding recognition, response, and resolution to cyber-incidents does not exist. Therefore, this research intends to bridge that gap by modeling cybersecurity in the home, where users lack knowledge and where security lacks (Furnell & Moore, 2014).

Using the actor-network model, this research can unveil both an individual's decision making, categorize behaviors, and suggest possible avenues to remedy the

problems. Moreover, this research examines attacks, vulnerabilities, and responses for the Internet of Things, as adoption of it continues to grow (Riggins et al., 2015).

The research begins and ends with the actor-network model. Therefore, a preliminary model for cybersecurity must be developed. Under the Buildings Cybersecurity Framework (Mylrea et al., 2017), cybersecurity involves five processes: identify, protect, detect, respond, and recover. As the typical user does not know their vulnerabilities, identifying them must be done by external organizations, home networking equipment manufacturers, and operating system developers (identifiers). Protecting these vulnerabilities revolves around the interaction between the end user and the identifiers. The identifiers can emplace protections in some cases, but the communication with the user is paramount to protect against constantly-evolving threats. Moreover, research into cybersecurity in the Internet of Things yields classifications (Anwar et al., 2017) and threats (Schiefer, 2015) (Bugeja et al., 2017) that can be organized under the identify and protect stages.

Detection of a cyber-incident relies on three agents: the end user, the device, and the application in use. Each threat places different strains on these agents and, due to their lack of knowledge, end users do not reliably detect threats. In other terms, the user interacts with the network in many predefined ways—accessing applications, configuring devices, etc.—but users may not utilize all interactions. If a cyber-incident causes the network to depuntualize but does not alter the interactions for the user, they will not detect the attack. Note that this behavior is true of all actors analyzing the cybersecurity network, but other agents analyze many of its interactions due to their security focus.

The greatest unknown, the user response, holds the most insightful information—how the user stabilizes the cybersecurity actor-network. Perhaps relatives and tech support (Jiang et al., 2016) lie, but the usage of these actors must be verified and the existence of other actors must be discovered. Similarly, the recover stage depends on what actor was attacked. It could be a device (a laptop or IoT sensor) an account, etc. As every target's individual actor-network differs, the response will be categorized into general terms, with general models in the attacks discussed.

Although the research will continue with a literature review to refine the model described, the evolution of the model must involve actual incidents. Therefore, a case study or experimental trials can be used to collect data on cybersecurity incidents in the home or a home-like environment. In the case study method, many individuals would be asked to relay information about cybersecurity incidents that they have experienced. Their stories would then be broken down and inserted into the model. In aggregate, many stories coalesce and may give insight into what assumptions in the model appear to hold, which assumptions fall short, and new agents not previously considered. Balzacq and Caveltry (2016) have already demonstrated the effectiveness of this method with their analysis of the Stuxnet worm.

However, the conclusions drawn from a case-study, especially a narrative one with little to no verification of the cases, may not be as reputable as desired. Therefore, an

experimental method can also drive the model's evolution. In an experimental setting, a select few attacks would be simulated in a home-like environment such that participants would react similarly to real attack. Furthermore, debriefing can include an interview to have participants relay their thought process, generating a first-hand account with more verification than a case study. Performing an experimental study, despite its usefulness, and—to some degree—the case study would consume too much time for a one-semester, undergraduate project. Therefore, this research will formulate the foundation of the experimental options and target a small sample of case studies. A more complex review of the model with the experimental methods described will have to come in future studies.

Conclusion

With social media's privacy concerns (McCarthy, 2018) and the general public's lack of cybersecurity knowledge (Furnell & Moore, 2014), our society does not appear ready to face the challenges of our digital realm responsibly. Through a technical solution, an individual's data can be centralized and self-controlled through a web server of their own. If a device can be made and fulfil many roles for different federated technologies, people may interact with social media differently. Ideally, this responsibility on the self could slowly increase digital literacy and inspire the new generation through interacting with their own web server. With an actor-network model of cybersecurity, cybersecurity policy makers gain insight into the behaviors of typical users during incidents and details describing responsibilities of other actors in the network. For instance, if close social relationships continue to play a large role (Jiang et al., 2016), cybersecurity and digital education may become a larger focus in schooling. Social media and cybersecurity will continue to evolve and change, so let us make sure we understand them a bit more before they race past.

References

Alotaibi, F. G., Clarke, N., & Furnell, S. M. (2020). A novel approach for improving information security management and awareness for home environments. *Information & Computer Security*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/ICS-05-2020-0073

Anwar, M. N., Nazir, M., & Mustafa, K. (2017). Security threats taxonomy: Smart-home perspective. *2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall)*, 1–4. https://doi.org/10.1109/ICACCAF.2017.8344666

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

Bugeja, J., Jacobsson, A., & Davidsson, P. (2017). An analysis of malicious threat agents for the smart connected home. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 557–562. https://doi.org/10.1109/PERCOMW.2017.7917623

Carmichael, C., Whitfield, H., & Willett, N. (2020, December 17). How Much Does It Cost to Host a Website? *WebsiteBuilderExpert*. https://www.websitebuilderexpert.com/web-hosting/cost-to-host-a-website/

Furnell, S., & Moore, L. (2014). Security literacy: The missing link in today's online society? *Computer Fraud & Security*, *2014*(5), 12–18. https://doi.org/10.1016/S1361-3723(14)70491-9

Groba, C., & Clarke, S. (2010). Web services on embedded systems—A performance study. *2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, 726–731. https://doi.org/10.1109/PERCOMW.2010.5470528

Jiang, M., Tsai, H. S., Cotten, S. R., Rifon, N. J., LaRose, R., & Alhabash, S. (2016). Generational differences in online safety perceptions, knowledge, and practices. *Educational Gerontology*, *42*(9), 621–634. https://doi.org/10.1080/03601277.2016.1205408

Jimenez, Y., & Morreale, P. (2015). Social Media Use and Impact on Interpersonal Communication. In C. Stephanidis (Ed.), *HCI International 2015—Posters' Extended Abstracts* (Vol. 529, pp. 91–96). Springer International Publishing. https://doi.org/10.1007/978-3-319-21383-5_15

Knutson, J. (2021, April 3). Personal data of 500 million users surfaces in leak that Facebook calls "old." *Axios*. https://www.axios.com/facebook-data-533-million-leak-bda53583-363a-4e4a-bc38-b147c3e12a8c.html

Kyusakov, R., Pereira, P. P., Eliasson, J., & Delsing, J. (2014). EXIP: A Framework for Embedded Web Development. *ACM Transactions on the Web*, *8*(4), 1–29. https://doi.org/10.1145/2665068

Leetaru, K. (2018, October 25). Social Media Companies Collect So Much Data Even They Can't Remember All The Ways They Surveil Us. *Forbes*. https://www.forbes.com/sites/kalevleetaru/2018/10/25/social-media-companies-collect-so-much-data-even-they-cant-remember-all-the-ways-they-surveil-us/?sh=5eecf1da7d0b

Lu, Y., & Xu, L. D. (2019). Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics. *IEEE Internet of Things Journal*, *6*(2), 2103–2115. https://doi.org/10.1109/JIOT.2018.2869847

Mastodon. (2017). *Mastodon User Guide*. WaybackMachine. https://web.archive.org/web/20170409030653/http://mastoguide.info/Pages/fedFAQ.html

McCarthy, J. (2018). *Worries About Personal Data Top Facebook Users' Concerns*. Gallup. https://news.gallup.com/poll/232343/worries-personal-data-top-facebook-users-concerns.aspx

Mitra, M. (2020, December 16). What Happens to My Personal Information After a Data Breach? *S*. https://www.msn.com/en-us/money/personalfinance/what-happens-to-my-personal-information-after-a-data-breach/ar-BB1bZ27g

Mylrea, M., Gourisetti, S. N. G., & Nicholls, A. (2017). An introduction to buildings cybersecurity framework. *2017 IEEE Symposium Series on Computational Intelligence (SSCI)*, 1–7. https://doi.org/10.1109/SSCI.2017.8285228

Riggins, F. J., & Wamba, S. F. (2015). Research Directions on the Adoption, Usage, and Impact of the Internet of Things through the Use of Big Data Analytics. *2015 48th Hawaii International Conference on System Sciences*, 1531–1540. https://doi.org/10.1109/HICSS.2015.186

Schiefer, M. (2015). Smart Home Definition and Security Threats. *2015 Ninth International Conference on IT Security Incident Management & IT Forensics*, 114–118. https://doi.org/10.1109/IMF.2015.17

U.S. Cybersecurity and Infrastructure Security Agency. (2020). *Home Network Security*. https://us-cert.cisa.gov/ncas/tips/ST15-002

World Wide Web Consortium. (2018). *ActivityPub*. https://www.w3.org/TR/2018/REC-activitypub-20180123/