Network Defense Methods Effect on Social Trust

A Research Paper submitted to the Department of Engineering and Society

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

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Daniel Lower-Basch

Spring 2023

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

Advisor

Rider W. Foley, Department of Engineering and Society

STS Research Paper

Essential services are becoming more intertwined with network technology. Banking, voter registration, and health information are all now available online, greatly increasing the importance of effective network security. Network security is defined as the combined techniques and technologies that are used to prevent malicious actors from accessing and/or modifying private data (Li and Liu, 2021). Viruses, worms, trojans, ransomware, and direct hacks are all examples of these malicious actors (Jain, 2014). Anyone using networked technology for important tasks is trusting in the defenses they have and that the service they are using will prevent hackers from affecting them negatively. As new defense methods develop, it is important to determine whether or not trust is positively or negatively impacted.

Society depends on trust (Lewis and Weigert, 1985). Currency, laws, and politics in the US cannot work without trust. Money holds no inherent value beyond the worth of its materials, yet we trust the government to uphold the stated value, which allows for the economy to exist beyond barter (Carruthers and Babb, 1996). Laws are not an intrinsic part of the world, and any weight they hold comes about because of trust that the stated consequences will be upheld. We trust our representatives to act in our best interests and vote for them in elections as a result. All these key parts of society are dependent on trust. Services that provide vital services through the internet are in many ways even more dependent on trust than similar services in reality. Online banking depends on trust in the provider and their defenses against attacks. If anyone could break through online banks defenses, then nobody would use them for fear of losing all their money (Twum and Ahenkora, 2012). As such, the effectiveness of network defenses and the peoples trust in these defenses has a major effect on social trust, especially as we integrate more vital services into the internet. As such, I wanted to research the effect of new network defense

methods on social trust in the US, social trust being defined as a belief in the reliability, honesty, and integrity of others (Taylor et. al., 2007). I will explore whether new network defense methods will have an overall positive or negative impact on society in this paper.

CASE CONTEXT

Depending on how a network is configured, there are different ways that hackers can attack. For example, a computer linked to the internet is more easily accessible by an attacker than one solely connected to an internal network. The attack surface of a network is defined as the system resources exposed to attackers, which includes communication ports, publicly sourced software, and component vulnerabilities (Zhuang et. al.). Networks can be configured in different ways with equal efficiency on the same devices. The idea behind Moving Target Defense (MTD) is that by generating new configurations that are equally efficient, attack surfaces can be regularly changed by cycling the network through these different setups (Zhuang et. al., 2014). Research has been done on the adaptive use of many network defense mechanics, but MTD was not included (Atigetchi et. al. 2003).

The benefit of MTD is that it reduces the inherent advantages attackers hold. Attackers will always have the ability to study networks they mean to attack and to choose the time of attack for their maximum benefit. MTD regularly changes the network, meaning that studying the network will only help until the next shift. This means that attacks take more time and are more likely to trigger defense mechanisms, which means that the overall attack is less likely to succeed. Additionally, MTD can be combined with other security methods for greater overall ability (Alavizadeh et. al., 2021). However, nonadaptive MTD has the disadvantage that it does not take the attacker into account when it shifts. Adaptive MTD seeks to overcome this weakness by including the feedback from other defense mechanisms into its inputs (Cho et. al. 2019). For

example, if a firewall goes off as a result of an attacker trying to infect a computer, the adaptive MTD will trigger a shift to a configuration in which the potentially infected computer is shifted away from the attack surface, preventing the attacker from continuing that avenue of attack. While this has the potential to greatly increase the security potential of MTD, we do not know the tradeoffs in terms of the ease of use of networks where adaptive MTD is implemented. Thus, my internship involved working on simulating the effects of adaptive MTD on a network in terms of security and ease of use.

If adaptive MTD can be broadly implemented, it could greatly increase the difficulty of network attacks. This in turn would increase the trust people have in network defense methods, increasing social trust. But this is only one potential outcome. Alternatively, adaptive MTD is implemented and no one beyond security enthusiasts even notices. Overall, a nonimpact on social trust in either direction, which would still be a positive outcome, but less of one than the first outcome. Finally, hackers could figure out the algorithms adaptive MTD uses and attack systems in such a way that the shifts in network help the attackers instead of hinder. This does not seem likely, but if it occurred it would be a massive hit to trust in network security, which could have massive negative effects.

THEORETICAL FRAMING

I used the actor-network theory (ANT) to evaluate the knock-on effects of network defense methods. ANT defines each actor impartially, whether they are human or non-human, and whether they act through social, natural or technological means (Lepa and Tatnall. 2016). ANT transitions through four main phases, starting with designing technology with certain values and goals in mind, not necessarily consciously. Then, humans delegate work to the technology. Next, the technology constrains human actions in accordance with its program of

action, enforcing its purpose. Finally, technology shapes society in how it affects the world, discriminating against those who cannot or will not work in line with its goals. In my actor network I have users and hackers as human participants, and services and security methods as nonhuman participants. We inscribe the goal of the transfer of information into services, and the authorization of allowed requests and denial of nonallowed requests to security methods. We delegate the transfer of information between people to services, instead of our previous methods of writing down information, mass producing said writing, and conveying the information to the larger populace through physical means. Security methods act to enforce the prescription that users and hackers will only access authorized information, and in doing so discriminate against hackers. I chose ANT because I could parallel the technical research done by simulating networks for adaptive MTD with the research done on the network made up of users and security devices.

RESEARCH QUESTION AND METHODS

My research question is what is the impact of adaptive MTD on social trust? This question is important to determine whether developing adaptive MTD will have positive or negative impacts on its users, especially as the trends of further integration of technology progress. I used a combination of surveys and articles as my research sources (Ponto, 2015). The surveys were made using Google Forms, and included the questions of how safe college students think online banking, online voter registration, and password managers are on a scale from 1 to 5 as well as whether new network defense methods make them more or less confident about their previous answers on safety (Appendix A).

I investigated research articles on social trust and network defense to see the correlation between the two, including Baki, et. al.'s (2020) work to understand how social trust can be

measured. This let me gather data on trust in online services, trust in new defense methods, and measures of social trust. I used the answers to my survey to create positive or negative scores for each question depending on how far from the center of the range of scores the answer was. I divided the questions by whether they conveyed knowledge of network defense methods or trust in network defense methods, then combined them. By creating a scatter plot of the combined knowledge of network defense methods and the combined social trust scores, I created a line of best fit to measure the trends of the two variables. This was done to find out whether there was a positive or negative correlation between the two overall categories (Interpreting Scatterplots, 2022).

RESULTS

The survey results suggests that there is no impact on social trust as a result of new defense methods. The connection between new methods of network defense and social trust is not statistically significant, with an R squared value of .04. The R squared value is the proportion of the variance in the response variable that can be explained by the predictor model in the model (Zach, 2022). With the given R squared value, only four percent of the trust values can be explained by their paired network defense method knowledge scores. As such according to the found data, there is no connection between knowledge of network defense methods and trust in these defense methods.

The collected data consists of 39 responses to the survey, with one being discounted for being turned in blank, leaving 38 usable data points. The survey consisted of eight questions, four for the knowledge and four for the trust. The questions were focused on three types of commonly used applications that rely on network defense methods, antivirus, online banking/voting registration, and password managers, with online banking and voter registration

put together based on their relative similarity in terms of usage and dependencies on network defense. The knowledge questions focused on how much they understood their antivirus, whether they would change their antivirus, and how new defense methods affected their confidence in the other two applications. The trust questions focused on how confident they felt in the three types of application, and whether they actually used a password manager. Each question could add or subtract a maximum of two points from the overall score, leaving the absolute range for both overall scores from negative eight to positive eight. Negative scores indicated minimal knowledge or trust while positive scores indicated maximum knowledge or trust. Each of the 38 data points had their two scores calculated, and then a scatter plot of the results was created, as shown below.

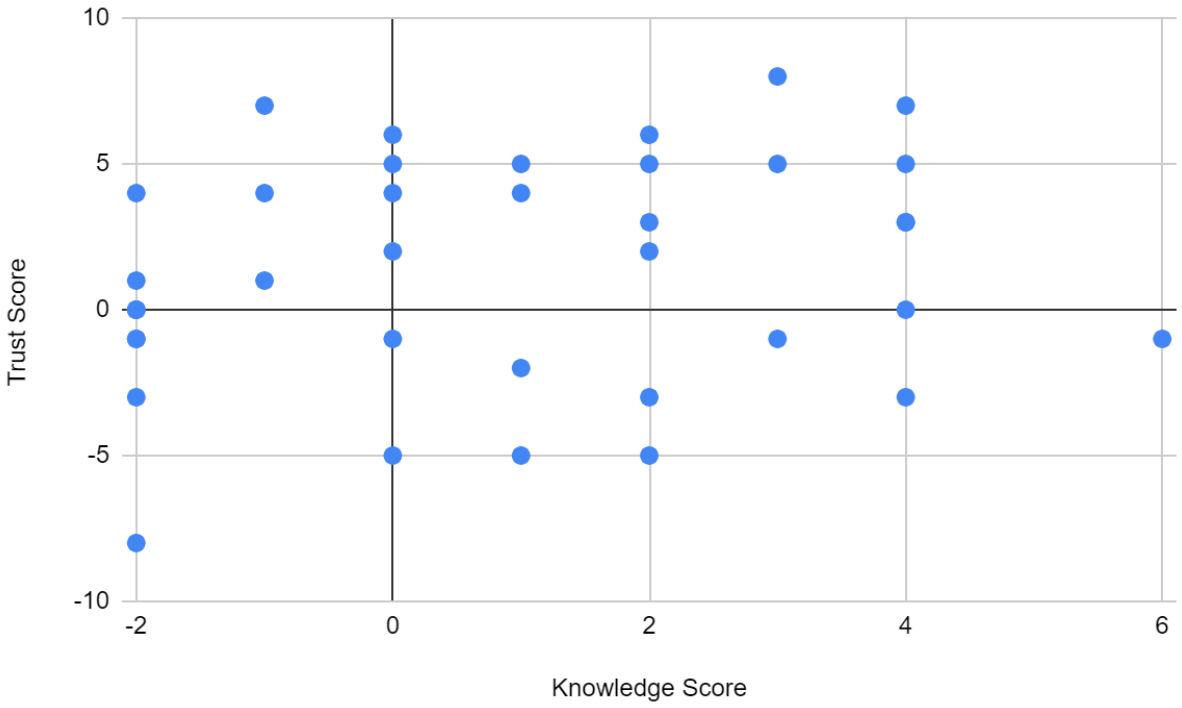

Figure 1. Scatter plot of survey results (Lower-Basch, 2023)

After the scatter plot was created, a line of best fit was created for the resulting graph, shown below.

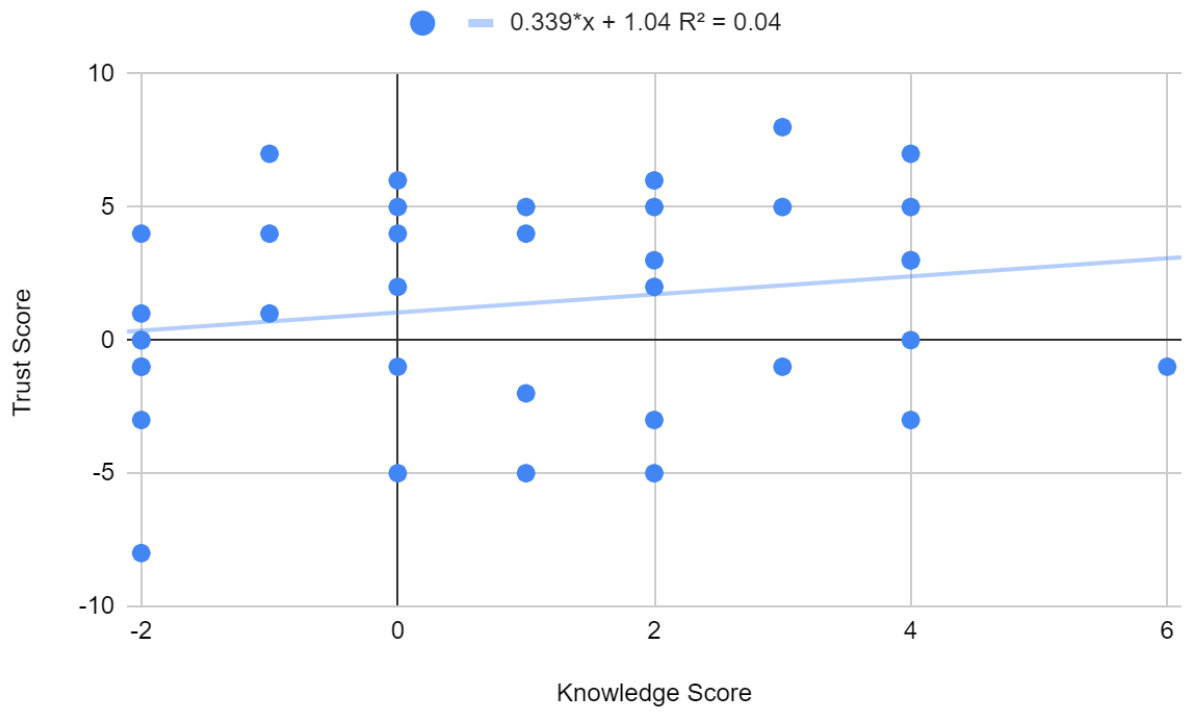

Figure 2. Scatter plot of survey results with line of best fit (Lower-Basch, 2023)

The resulting line of best fit has a positive slope, indicating a positive correlation between the knowledge scores and the trust scores. However, the R squared value is 0.04, which demonstrates that the line of best fit does not accurately model the provided data, which should be fairly clear just from looking at the graph. The data points are scattered enough that there is no definitive correlation between the two values, suggesting the aforementioned final result, that there is no impact on social trust as a result of new defense methods. This lack of connection can be explained by the fact that people in general do not need to understand a network defense to use it, only to develop it. People do not need to understand how airplanes work to use them to get from location to location. As such, due to the general populations ignorance as regards the

specifics of their network defense methods, their trust in these methods is based on their own values and assumptions instead of their knowledge, and these preconceptions remain even after learning the specifics of the defense methods. As a result, there is no connection between the knowledge of a network defense method and trust in it.

DISCUSSSION

Overall, it is taken as a given that improving network defense methods is a self-evident good. The existence of hackers demands a response, otherwise we surrender our capacity for secure online transactions. Computer Network Defense is defined as "Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks" (pg. 193, Andress, 2014). While there is a great deal of research on why network defense is required, there is much less research done on the side effects of network defense, especially when developing new methods of defense. My research was made to expand on this concerning lack by determining the effect of new network defense methods on social trust. Hopefully, this will encourage other defense developers to consider the greater effect their work has on the overall actor network that makes up our society.

My work is fundamentally limited on a number of levels. The sample size is low, less than 50, those who participated had selection bias due to being those who chose to take the survey, and the survey had a small number of questions that could be interpreted differently by different respondents. I had to balance between making the survey long enough to convey sufficient data to count as a data point, while making it short enough that it would not put people off from responding, thereby reducing the number of data points I was given. Questions in the same category could cancel each other out with opposing answers, so someone who strongly supported password managers while hating online voting would register similarly to someone

who was neutral for both, which for the purpose of the overall scores makes sense, but does remove some of the nuance of the answer. Additionally, all my respondents are from the University of Virginia, mostly if not all students there, further biasing the results from the overall population of the US.

Future research should determine the causative link between social trust and network defense knowledge (Statistics, 2022), or what other factors need to be considered, increase the range of my respondents beyond UVA, add more questions to the survey so as to hopefully better observe the trends, and incentivize people responding to the survey to increase the number of people responding. As an example, I could potentially add everyone who responded to a lottery with prizes, which would hopefully get me more responses. Beyond that, I would try to get a second opinion on the survey questions, and work to plan out how I linked the questions responses to my overall scoring more clearly in advance.

I plan to use this research to support the development of adaptive MTD. While this study is flawed in many ways, it does serve as a broad overview of the effect that new defense methods have on social trust. I would not say that this proves definitively there is no link between the two, but I would say that it does provide evidence to that effect. As such, given the other benefits adaptive MTD has in terms of network defense, these being increased security strength and responsiveness to attacks, I would support its development.

CONCLUSION

New defense methods as a whole does not seem to have a strong impact on social trust, either positively or negatively. For those taking this research further, I would suggest a broader base to gather data from, more specificity in terms of adaptive MTD as opposed to general

network defense methods, and potentially comparisons between applications with and without adaptive MTD. I would say that this study supports the overall development of adaptive MTD.

References

Alavizadeh, H., Aref, S., Kim, D. S., & Jang-Jaccard, J. (2021). *Evaluating the Security and Economic Effects of Moving Target Defense Techniques on the Cloud* (arXiv:2009.02030). arXiv. http://arxiv.org/abs/2009.02030

Andress, Jason, and Steve Winterfeld. 2014. "Chapter 11 - Computer Network Defense." Pp. 193–205 in *Cyber Warfare (Second Edition)*, edited by J. Andress and S. Winterfeld. Boston: Syngress.

Baki, S., Verma, R. M., Mukherjee, A., & Gnawali, O. (2020). *Less is More: Exploiting Social Trust to Increase the Effectiveness of a Deception Attack* (arXiv:2006.13499). arXiv. https://doi.org/10.48550/arXiv.2006.13499

Carruthers, B. G., & Babb, S. (1996). The Color of Money and the Nature of Value: Greenbacks and Gold in Postbellum America. *American Journal of Sociology*, *101*(6), 1556–1591.

Cho, J.-H., Sharma, D. P., Alavizadeh, H., Yoon, S., Ben-Asher, N., Moore, T. J., Kim, D. S., Lim, H., & Nelson, F. F. (2019). *Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense* (arXiv:1909.08092). arXiv. https://doi.org/10.48550/arXiv.1909.08092

Interpreting Scatterplots | Texas Gateway. (n.d.). Retrieved October 25, 2022, from https://www.texasgateway.org/resource/interpreting-scatterplots

Jain, N. (2014, March). *Cyber Crime Changing Everything – An Empirical Study*. https://www.researchgate.net/publication/275709598_CYBER_CRIME_CHANGING_EVERYTHING_-_AN_EMPIRICAL_STUDY

Lepa, J., & Tatnall, A. (2006). Using Actor-Network Theory to Understanding Virtual Community Networks of Older People Using the Internet. *Journal of Law and Governance*, *1*(4), Article 4. https://doi.org/10.15209/jbsge.v1i4.87

Lewis, J. D., & Weigert, A. (1985). Trust as a Social Reality. *Social Forces*, *63*(4), 967–985. https://doi.org/10.2307/2578601

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Ponto, J. (2015). Understanding and Evaluating Survey Research. *Journal of the Advanced Practitioner in Oncology*, *6*(2), 168.

Statistics, A. C. of A. ou=Australian B. of. (n.d.). *Statistical Language—Correlation and Causation*. c=AU; o=Commonwealth of Australia; ou=Australian Bureau of Statistics. Retrieved October 25, 2022, from https://www.abs.gov.au/websitedbs/D3310114.nsf/home/statistical+language+-+correlation+and+causation

Taylor, P., Funk, C., & Clark, A. (2007, February 22). Americans and Social Trust: Who, Where and Why. *Pew Research Center's Social & Demographic Trends Project*. https://www.pewresearch.org/social-trends/2007/02/22/americans-and-social-trust-who-where-and-why/

Twum, F., & Ahenkora, K. (2012). Internet Banking Security Strategy: Securing Customer Trust. *Journal of Management and Strategy*, *3*(4), Article 4. https://doi.org/10.5430/jms.v3n4p78

Zach. (2022, March 24). How to interpret adjusted R-squared (with examples). Retrieved February 19, 2023, from https://www.statology.org/adjusted-r-squared-interpretation/

Zhuang, R., DeLoach, S. A., & Ou, X. (2014). Towards a Theory of Moving Target Defense. *Proceedings of the First ACM Workshop on Moving Target Defense*, 31–40. https://doi.org/10.1145/2663474.2663479

Zhuang, R., Zhang, S., DeLoach, S. A., Ou, X., & Singhal, A. (n.d.). *Simulation-based Approaches to Studying Effectiveness of Moving-Target Network Defense*. 12.

Appendix A: Survey Questions

1. How much do you understand your antivirus?
2. How much do you trust your antivirus?
3. Would you switch your antivirus for a newer antivirus?
4. How confident do you feel in online banking/voter registration?
5. If your online banking/voter registration announced it was upgrading their security methods, how would that affect your confidence in it?
6. Do you use a password manager?
7. How much confidence do you place in password managers?
8. If a password manger announced it was upgrading their security methods, how would that affect your confidence in it?
9. Do you have any questions, comments, or suggestions?