DYNAMIC NETWORK SIMULATION METHODOLOGY

THE EFFECT OF ADAPTIVE MOVING TARGET DEFENSE ON SOCIAL TRUST

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Daniel Lower-Basch

October 27, 2022

Technical Team Members:
Daniel Lower-Basch

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.

ADVISORS

Rider Foley, Department of Engineering and Society

Briana Morrison, Department of Computer Science

Background

Essential services are becoming more intertwined with network technology as time passes. Banking, voter registration, and health information are all now available online. This trend will only continue, greatly increasing the importance of effective network security. Network security is 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.

This summer I participated in a research internship with Noblis on determining the amount of time, money, and researchers needed to develop adaptive moving target defense (MTD) into an effective network security mechanism. Noblis is a non-profit government contractor based in Virginia that does technical research in several different areas, including computer vision, system simulation, forensic investigation, and many more (Noblis, 2016). They also do independent research projects, my internship among them. As a government contractor, Noblis has potentially sensitive data on their networks, making security a particular focus. As a potential area of research, adaptive MTD caught their interest. With prior examples of MTD research, adaptive MTD seemed like a path Noblis could go down without much effort. But should they?

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. Although adaptive MTD has the potential for great good if used properly, it also has the potential for great evil if it is not. As such, I want to research the effect of the development of adaptive MTD 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). We have the capability to develop Adaptive MTD, but would it be more helpful or harmful overall?

Adaptive Moving Target Defense

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 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). As such my research internship was created to determine how difficult it would be to implement adaptive MTD.

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.

Network Security in Society

Network security is an important field that shifts constantly, especially now as technology is integrated into more of our lives. Jain and Shirvastava (2014) wrote about the different types of cybercrime, including malicious code, denial of service, cyberstalking, financial crimes, and more (Jain and Shirvastava, 2014). In 2022, when autonomous vehicles are transitioning from science fiction to reality, the damage that hackers can do has only gotten greater. Infrastructure that includes the metro, traffic systems, and airports are controlled via networks. Hospitals rely on networks to receive and transmit signals to and from medical equipment, as well as for storing and transferring medical data. The stock market does not rely on a network, it is a network in and of itself, and is inherently vulnerable. Manufacturing can be greatly impacted by cyber-attacks (Giehl et. al., 2019). Email, social media, and news sites are all based on the internet. Productivity, the economy, personal data, and even lives are all potentially under threat if network security is not upheld. According to Yuchong Li and Qinghui Liu (2021) cyber warfare can include government systems being overthrown and the initiation of physical warfare (Yuchong and Qinghui, 2021). Additionally, cyber-attacks are increasing over time, making network security a greater priority (Werner et. al., 2017). I cannot stress the importance of effective network security enough. However, there are always tradeoffs between defense and ease of use.

There are methods for evaluating the results of MTD's, but not for how to evaluate their knock-on effects (Xu et. al. 2014). I intend to use the actor-network theory to evaluate these effects. Actor-network theory 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). Actor-network theory 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.

Research Question

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 intend to use a combination of surveys and articles as my research sources (Ponto, 2015). The surveys will include the questions of how safe college students think online banking,

online voter registration, and online health records are on a scale from 1 to 5 as well as whether new network defense methods make them feel better or worse about their previous answers on safety. I will investigate research articles on social trust and network defense to see the correlation between the two, such as Baki, et. al.'s work (Baki et. al., 2020), and how social trust can be measured to gather data on social trust from my surveys. This will let me gather data on trust in online services, trust in new defense methods, and measures of social trust. By creating a scatter plot of the combined trust in network defense methods and the combined social trust scores, I can measure the trend to find out whether there is a positive or negative correlation between the two overall categories (Interpreting Scatterplots, 2022). Further research would be required to determine which is the cause and which is the effect (Statistics, 2022), or what other factors need to be considered, but it should give a general basis for whether adaptive MTD would have a positive or negative impact on social trust.

Conclusion

In conclusion, we do not currently know the effect that the development of adaptive MTD will have on social trust. As the possibility exists, it is important to put research into the matter to limit the effect of unintended consequences. If the results of the research are that adaptive MTD will have a positive effect on social trust, it increases the reasons to develop it, whereas if it is negative effort should be put into researching why this is the case, and how to prevent or work around the issue. If it is a neutral effect, then there will not be an increase in reasons to develop adaptive MTD, but neither will there be a decrease. The expected results of this research are a positive or neutral correlation between the development of adaptive MTD and social trust.

References

About Us. (n.d.). Noblis. Retrieved October 25, 2022, from https://noblis.org/about-us/

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

Atighetchi, M., Pal, P., Webber, F., & Jones, C. (2003). Adaptive use of network-centric mechanisms in cyber-defense. *Second IEEE International Symposium on Network Computing and Applications, 2003. NCA 2003.*, 179–188. https://doi.org/10.1109/NCA.2003.1201154

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

Giehl, A., Wiedermann, N., & Plaga, S. (2019). A framework to assess impacts of cyber attacks in manufacturing. *Proceedings of the 2019 11th International Conference on Computer and Automation Engineering*, 127–132. https://doi.org/10.1145/3313991.3314003

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

Werner, G., Yang, S., & McConky, K. (2017). Time series forecasting of cyber attack intensity. *Proceedings of the 12th Annual Conference on Cyber and Information Security Research*, 1–3. https://doi.org/10.1145/3064814.3064831

Xu, J., Guo, P., Zhao, M., Erbacher, R. F., Zhu, M., & Liu, P. (2014). Comparing Different Moving Target Defense Techniques. *Proceedings of the First ACM Workshop on Moving Target Defense*, 97–107. https://doi.org/10.1145/2663474.2663486

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.