COMP260-Research Journal

Network Security

1506530

March 31, 2017

1 Journal

Internet security is a hot topic in todays technical society, and many researchers are always looking into new ways to break and make this security. Over this journal I looked into varying methods of breaking past the security methods adopted by TCP connections as well as the ethical nature of these papers. As releasing methods for hacking into devices using TCP could be abused by the more negative acting public that have access to this information, though this information could also be used to prevent these attacks.

Title: Collaborative TCP Sequence Number Inference Attack: How to Crack Sequence Number Under a Second [1]
This paper summarize multiple methods for hijacking a TCP client session in seconds, using side channels that are "sequence number dependent. This method does require an on device malware to be present on the targeted device. This malware then communicates with an off-path attacker to inject a javascript into a live facebook session, and allow the attacker to perform unrestricted access to their accounts. The paper then continues on to take the reader through various steps required for these actions, from the requirements for the execution and for varying Operating systems, including Mac OS, Windows and Linux. Though they do not provide cod samples for the required malware this paper could still be ethically questionable, internet security is a risk for everyone and handing the methods and sugestions on how to do it may not be the wisest method of preventing it. Though looking on the other side of the argument providing this information could help people understand how these attacks are done and help the victims prevent them from happening. On that note though the majority of internet users would not have the required knowledge or skill to understand and prevent attacks. Ethically this paper is still in the gray area, but none the less provides useful information to people on the gaps in network security.

Title: Network security via reverse engineering of TCP code: vulnerability analysis and proposed solutions [2]
In this paper the authors went quite the opposite direction to the "Inference Attack"[1], where they reverse engineered a TCP protocol to find its weaknesses and moved forward to suggest fixes for those weaknesses. This was done using a technique called "program slicing". As stated in the paper, "program slicing is an abstraction mechanism in which code that might influence the value of a given variable or a set of variables at a location is extracted from the full source code of the program". This part of the paper was difficult to understand but the aim of the paper was clear, they wanted to use this slicing technique on many commercial TCP servers to allow the owners of those servers release patches to cover the gaps in heir security. Providing a method to find and fix these security issues place these authors in an ethically different light to the previous paper.

Title: Cross-path Inference Attacks on Multipath TCP [3]
MPTCP or "MultiPath TCP" allows the concurrent use of multiple paths between two end points, which has potential to provide greater performance for application connections. This paper explains the usefulness of MPTCP over standard TCP but also delves into the security risk of having multiple connections. Due to the deliberate design of MPTCP, its subflows are inherently coupled with each other, resulting in potential side-channels that can be exploited to infer cross-path properties. This paper does not address the issue directly to solve it but rather provide a base line for further research into this new security risk so the issues can be addressed before MPTCP gets widely adopted by ISP's. At the end of this paper the authors urge the community to look into this further. the research community has an ethical responsibility to look into this. It seems that as this issue has been designed into the MPTCP, it should fall to the designers of this method to help address it.

Title:Ancillary Impacts of Multipath TCP on Current and Future Network Security [4]
Here is an example of research into MPTCP's current and future security, the authors look into the basics of MPTCP, its applications and security, comparing it to traditional TCP for their differences in security. Mainly concentrating on network monitoring this paper provides more of an understanding behind the risks of MPTCP rather than how to solve them, this reinforces the current worry that MPTCP needs to be looked into more before it can be widely distributed. Though they paper does state the need for an updates TCP as the current speeds of networking are beginning to out pace TCP.

As there are other methods for networking it may be wise to research these other methods as well. Also looking from an ethical point of view at this time it would be a bad idea to release MPTCP until many of these security issues are resolved.

Title:An Empirical Study of TCP Vulnerabilities in Critical Power System Devices [5]
As apposed to the other papers the authors of this paper began working with vendors to solve the issues presented. The issues presented are that most power systems work with an outdated TCP network that uses predictable sequence numbers in their initial sequence numbers. This can allow a hacker to gain access into the power grid and case physical harm to several public sector services, for example a hospital. This is an alarming threat that has been addressed by this paper and is hopefully now secure, which according to the authors is about time, as this issue has been present for around thirty years, and is only now being addressed sue to the higher activity over the internet. This paper provides good news for the security of TCP networks and the authors, now working with the vendors using the TCP's can further develop the network to ensure it stays safe.

Title:A Survey on Future Internet Security Architectures [6]
Moving on from that this paper looks at the different architectures for internet security in their survey for the future. The authors took a heuristic approach to this survey, by deciding several criteria to compare the architectures to. The paper does suggest that when designing the architecture for networking the designers must use a clean slate for the design and not rely on preexisting architectures as well as keeping security in mind as their prime goal. Going forwards it seems that the current architecture that we use which is some 40 years old, must be replaced with a band new method that is build for both security and for a wide distribution. Its clear that much research has gone into these security issues, but the question is that has come from reading this is that do we continue with the current methods and try to improve them, or look into a completely new method that has not been tried yet.

References

[1] Z. Qian, Z. M. Mao, and Y. Xie, "Collaborative tcp sequence number inference attack: How to crack sequence number under a second," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, (New York, NY, USA), pp. 593–604, ACM, 2012.

[2] B. Guha and B. Mukherjee, "Network security via reverse engineering of tcp code: vulnerability analysis and proposed solutions," in *INFOCOM '96. Fifteenth Annual Joint Conference of the IEEE Computer Societies. Networking the Next Generation. Proceedings IEEE*, vol. 2, pp. 603–610 vol.2, Mar 1996.

[3] M. Z. Shafiq, F. Le, M. Srivatsa, and A. X. Liu, "Cross-path inference attacks on multipath tcp," in *Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks*, HotNets-XII, (New York, NY, USA), pp. 15:1–15:7, ACM, 2013.

[4] C. Pearce and S. Zeadally, "Ancillary impacts of multipath tcp on current and future network security," *IEEE Internet Computing*, vol. 19, pp. 58–65, Sept 2015.

[5] D. Formby, S. S. Jung, J. Copeland, and R. Beyah, "An empirical study of tcp vulnerabilities in critical power system devices," in *Proceedings of the 2Nd Workshop on Smart Energy Grid Security*, SEGS '14, (New York, NY, USA), pp. 39–44, ACM, 2014.

[6] W. Ding, Z. Yan, and R. H. Deng, "A survey on future internet security architectures," *IEEE Access*, vol. 4, pp. 4374–4393, 2016.