Security is the Weakest Link: Prevalent Culture of Victim Blaming in Cyberattacks

Surya Nepal
CSIRO Data61
Sydney, Australia
surya.nepal@data61.csiro.au

ABSTRACT

We have witnessed a large number of cyber incidents in recent times. Despite a lot of efforts in cybersecurity awareness program and technological advancements, cyber incidents are on the rise every year. The effectiveness of cybersecurity measures is often questioned in the wake of recent hard-hitting security incidents. The post-incident analysis usually concludes that users are the weakest link in the information security chain, and blamed on their awareness of security and safe use of the cyber systems. The attribution of blame is unfairly put on the end users. The judgment of causality, responsibility, and culpability in cyber incidents are affected by more widely held cultural views. The true cause of the problem is usually inherent in the structure of society. Blame is often placed on a victim. Instead of usability, the attribution is given to users.

We often forget that underlying security systems should also bear some responsibilities for introducing bugs and vulnerabilities due to the poor practice of designing and building secure systems [1]. Furthermore, usability is not given due consideration while implementing security solutions. For example, security practices such as passwords rely on western cultural knowledge [2]. Security solution designers and developers need to learn and adopt more scientific methodologies. They also need specific guidance and training to make security solutions more human-centric, and less vulnerable [3]. This talk aims to highlight the current culture of blaming the victims prevalent in the cybersecurity research community, present the current research initiatives in human-centric cybersecurity, and outline the potential future research areas.

CCS Concepts/ACM Classifiers

Human and societal aspects of security and privacy.

Author Keywords

Human-Centric Security, Usable Security, and Privacy, Cybersecurity

BIOGRAPHY

Dr. Surya Nepal is a Senior Principal Research Scientist at CSIRO Data61. He currently leads the distributed systems security group consisting of 15 staff and 57 Ph.D. students. His main research focus is in the development and implementation of technologies in the area of distributed systems (including cloud, IoT and edge computing) and social networks, with a specific focus on security, privacy, and trust. He has more than 200 peer-reviewed publications to his credit. He has co-edited three books including security, privacy, and trust in cloud systems by Springer, and co-invented three patents. He has successfully supervised several Ph.D. students. He is a member of the editorial boards of IEEE Transactions on Service Computing, ACM Transactions on Internet Technology and Frontiers of Big Data- Security Privacy, and Trust. He is currently a theme leader of Cybersecurity Cooperative Research Centre (CRC), a national initiative in Australia. He holds a conjoint faculty position at UNSW and an honorary professor position at Macquarie University.

REFERENCES

[1] D. Votipka, R. Stevens, E. Redmiles, J. Hu and M. Mazurek, "Hackers vs. Testers: A Comparison of Software Vulnerability Discovery Processes," 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, 2018, pp. 374-391.

[2] L. Simko, A. Lerner, S. Ibtasam, F. Roesner and T. Kohno, "Computer Security and Privacy for Refugees in the United States," 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, 2018, pp. 409-423.

[3] C. Herley and P. C. v. Oorschot, "SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit," 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2017, pp. 99-120.

AsiaCCS '19, July 9–12, 2019, Auckland, New Zealand.

ACM ISBN 978-1-4503-6752-3/19/07.
DOI: https://doi.org/10.1145/3321705.3329914