JISSec
Journal of Information System Security

Journal of Information System Security is a publication of the Information Institute. The JISSec mission is to significantly expand the domain of information system security research to a wide and eclectic audience of academics, consultants and executives who are involved in the management of security and generally maintaining the integrity of the business operations.

ISSN: 1551-0123
Volume 17, Issue 3

www.jissec.org

EDITORIAL

These three papers examine three distinct conduits where weak cyber-security has led to rampant cyber-crime, namely: online platforms, web browsers, and video conferencing. The respective authors, who are from three different countries, analyze these phenomena in depth and then go on to either propose solutions, or describe how effective solutions were rapidly implemented by government authorities and service providers alike in an attempt to guarantee more secure internet practices.

The first paper, entitled "Cyber Security and Its Reality in Bangladesh: An Analysis of Existing Legal Frameworks", is by Kudrat-E-Khuda Babu from Bangladesh. It explores how more and more national and multinational companies are offering online services for their services in Bangladesh via the Internet, as they follow the government's 'Digital Bangladesh' agenda. However, criminals are also using the same online platform to commit various sorts of cyber-crime. The author highlights the gravity of the threat posed by cyber-crime in Bangladesh, where 90% of software is unlicensed.

In the second paper, "A Framework for Secure Web Browsing, using Trusted Platform Module (TPM)", the authors Harshad S. Wadkar and Arun Mishra, from India, address the danger of browser-based attacks caused by the security misconfiguration of browsers, which can lead to information leakage, sharing of data with a third party, and insecure data transfer. The paper proposes a novel approach for configuring browsers in an attempt to ensure secure browsing and maintain the environment in a secure state. A control mechanism is also proposed in the form of a finite state machine model for assessing the operating system configuration of browsers.

The third paper is entitled "*Zoombombing*: Hype and Reality", and is by Simran Dhillon, from the USA. It explores the plethora of security issues associated with Zoom's video conferencing platform. For while video conferencing has been around for a while, few providers took precautions to consider the associated risks until the advent of *Zoombombing* attacks in 2020. This paper adopts a theoretical perspective to evaluate the security challenges in Zoom and provides principles that scholars and practitioners should adopt in evaluating security breaches.

I am sure that you will find this Issue to be informative reading.

Gurpreet Dhillon, Editor-in-Chief