SECURITY ASSURANCE OF WEB APPLICATION

ABSTRACT

of the Ph.D. Thesis

Submitted to

Jamia Millia Islamia

for the award of the Degree of Doctor of Philosophy

Submitted by

HABIB UR REHMAN

Dr. Mohammad Nazir
Supervisor
Associate Professor
Department of Computer Science
Faculty of Natural Sciences
Jamia Millia Islamia
NEW DELHI

Dr. Khurram Mustafa
Co-Supervisor
Professor
Department of Computer Science
Faculty of Natural Sciences
Jamia Millia Islamia
NEW DELHI

Department of Computer Science
Faculty of Natural Sciences
Jamia Millia Islamia
NEW DELHI

September 2018

ABSTRACT

Keywords: Security Assurance, Credential Safety, Application Security, Human Cognition, Cognitive Privilege, Comfort Level Security, Authentication, Authorization.

System security is largely incomplete without credential safety. These are two faces of same coin, but rarely touch together while addressing the concern of unauthorized access attack from a compromised system. If credentials are expressed over a compromised system, there is a high possibility of man in the middle attack. User express the credentials as an evidence to show the authenticity as benign user of the application. Security assurance provides confidence in the security-related properties and functionalities.

Traditional security assurance methods do not consider human intent (human cognition in general) while building security critical applications. Internet has evolved to a stage of maturity and different people have different level of comfort while accessing web applications. Users are also concerned about the security (same as the service providers) and hesitate to avail the online services due to the involved risks and attack incidences but the traditional access methods neither entertain end-user intent to login the application nor consider privilege disintegration. We believe that internet users are now quite familiar and comfortable in accessing web application.

We have leveraged this fact (users maturity to use internet) and proposed 'Comfort Level Security Assurance (CLSA)' framework that incorporates user intent (human

cognition) to strengthen security of web application and this also empowers users to define and choose different credentials for different functionalities (varying criticality). The proposed CLSA framework is an advanced authentication mechanism that incorporates human cognition in general and user intent in particular.

Utilizing human cognition, the proposed PvC Modelling is built upon multi-layer trust that may provide fine-grained access control which would not be possible under monolithic binary model. We apply functionality separation approach for application security and balance it with credential safety measure driven by user cognition. It provides expanded concept of perimeters to include both user identity and intent. Access to the resources is provided based on multi-layer trust instead of solely user's identity (credentials), although user cognition should be an exemplary constituent of the overall judgment.

Proposed work alleviates following limitations of current security assurance methods.

- Multiple level of credentials depending upon different levels of criticality.
- This will ensure that only a portion of web application functionality will be compromised in case of credential theft. Hence reduces the attack surface.
- In order to get the complete access of web application attacker need to hijack highest level of credential expression.
- It has been observed that the most critical functionality is less frequently used than more frequently used less critical functionality. Hence, significant reduction to credential theft.

- It safeguards the credentials, which are never expressed over a compromised system.

CLSA framework is the true representation of defence-in-depth strategy and PvC modelling explains how human, technological, and operational capabilities are comprised and integrated to establish variable protective barriers across multiple layers and dimensions against unauthorized access of the system. The prototype is an implementation of the proof of concept. The framework and PvC (Privileged vs Credential modelling) has been proved in three ways:

1. Proof of Concept (PoC) of the framework.

2. Demonstration of the proposed approach using PvC model.

3. Mathematical validation of the framework.

Mathematic has long been an ideal tool for modelling as it provides high level of validation. Our study is crucial for business-critical applications, where exploits can have severe economic consequences. We performed the validation of our study through formal method that reduces possibility of error and eliminates ambiguity.

HABIB UR REHMAN
E-mail: **way2habibmca@gmail.com**
Cell: +919811310263

Academic Profile:

- MCA in "Computer Application" from Jamia Hamdard, Department of Computer Science, New Delhi.

- B.Sc.(Hons) in "Electronic Science" from Delhi University, Zakir Husain College, New Delhi.

Personal Details:

- Nationality : Indian
- Father's Name : Late Mr. Mukhtar Uz Zaman
- Date of Birth : 27/07/1978
- Place of Birth : Delhi
- Gender : Male
- Marital Status : Married
- Phone : +919811310263