***Nguyen Thai Son – Group: 931924 – TSU***

Since networking and remote connections started to evolve until now, user authentication has always been a very important issue. As can be seen, passwords are in most cases the most reliable and almost unique method to authenticate users. There is a research article on Password Authentication, and I will do a short summary about it.

So that research is: **Securing Password Authentication for Web-based Applications,** by **Teik Guan Tan**, **Pawel Szalachowski**, and **Jianying Zhou** from **Singapore University of Technology and Design.** As its name, this reseach is about:

-Threat modeling and analysis of web password login process which uncovered the design vulnerability of the input password field.

-Identification of four protocol properties that encapsulate the requirements to stop password phishing for any web login system.

-Design and validation of a proposed security protocol that complies with the four identified properties.

Researcher said that, there are many victims of web-based password phishing. The adversary which they were dealing with is a phishing attacker with the goal to  
authenticate successfully to an honest Web Server on behalf of a user. To reduce the threats, the authors require 4 properties: *Credential Derive one-way function, Credential Specific one-time use,**Credential Store one-way function, Non-interactive input credential field.* To meet all 4 properties, the authors have proposed a new password login protocol, which they have focused on increasing password entropy, device verification, and asymmetric key authentication to provide a suitable construction.

This new protocol seems really efficient and powerful, as it satisfies the 4 required properties and is very resistant to abuse cases. This protocol outperforms the protocol created in the past, where the old protocols cannot satisfy all four properties at the same time, and there are vulnerabilities that can lead to serious consequences. The new protocol can prevent common attacks, such as spoofed URL, password sniffed, multiple credentials harvested, an so on. Also, about the User experiment is good, user privacy can be improved by using a separate salt for each user when stored on the database (the Store () function), however that will slow down the blacklist browsing. significantly. Furthermore, the implementation of this new protocol is quite feasible and the performance is acceptable (the password information has been hashed with SHA-512 1000 iterations before archiving, only takes 33 milliseconds) and possibly many more optimal way.

In the conclusion, the authors claim that the potential benefits in stopping phishing outweigh the costs. But there are still many way to steal password(Social engineering, poor password hygiene,...) and in the future there will be more and more new attack techniques. The authors is also said that this proposed solution must still be complemented with existing efforts of detection and takedown, plus continued user awareness and training, in order to be effective in removing instances of successful password compromises.