CSC 466 project proposal
An analysis of Secure Authentication based online payment protocol

Group members: Xinran Wang, Kaiheng Zhang, Xiling Zhang

What's the problem? Why is it important?

Nowadays, technology is closely related to our life, and online payment has become an indispensable thing. There are many ways to pay online, such as debit cards, credit cards, and PayPal; nevertheless, not every payment method is reliable. We also can assume none of them is one hundred percent safe. For example, the most popular method of payment in China is scanning QR codes. More and more people do not use cash anymore. However, when people scan QR codes, they have no idea what are those codes. Those codes may steal personal information on the devices, or they may charge more money when people scan the codes. For instance, when people want to pay through QR codes, they need to scan them first then set the amount that they want to pay by themselves. This is a single consumption by default, but that QR code may have tampered. It can charge people more than once. QR code is just one method of payments, we believe there must be some problems for other methods. That is why we want to figure out how to make online payment more reliable and discuss the problems that exist.

What has been done? Why are they not sufficient? Including any of your previous, other and ongoing projects too

In order to protect the security of online payment, there have been four common models of bank card-based payment. I will explain to them and analyze their advantages and disadvantages:

1. The model with no security measures in the payment system. The merchants have full information about the user's bank card and the transmission of bank card information without security guarantees. This model requests the good integrity of the merchants.
2. The model of payment through a third-party broker. Its characteristic is that the bank card information is not transmitted in an open network, and the payment is done through a third party (broker) that both the user and the merchant trust. The disadvantage is that
3. The simple encrypted payment system model. It uses encryption technology for key information such as bank card encryption, confirming the authenticity of information with a digital signature, which requires the support of business servers and service software.
4. The "Security Electronic Transaction" model, referred to as SET, is an international implementation of secure electronic transactions. Its characteristics are that SET provides authentication for transaction participants, ensuring the security, integrity and non-repudiation of transaction data, especially ensuring that cardholder account information is not leaked to merchants. It uses registered names The way of consumption, while strengthening the security of the system, has lost the characteristics of anonymity, and cannot protect the privacy of consumers well.

What's your approach? Why can it do better or differently?

There are many methods to pay online. For this project, we will try to find the most secure method or find a new way to pay and discuss the differences between different protocols. We may also try to combine those methods as a new one to reduce the possibility of problems caused by online payment. If we can do that, online payment will be more secure than now.

Expected deliverables and a rough biweekly time schedule

February 18th: Find the payment methods that we want to discuss and do some research about it. List all the problems that we think there are about those methods
March 4th: Do some research about online payment protocols. Find out some common protocols.
March 18th: Figure out ways to solve those problems or some ideas to improve them
March 31st: Finish the report

website url：https://csc466teamproject.wixsite.com/mysite

References

Fisher, Michelle. "Conducting an online payment transaction using an NFC enabled mobile communication device." U.S. Patent No. 8,352,323. 8 Jan. 2013.

Kadhiwal, Saleem, and Anwar Usman Shaheed Zulfiquar. "Analysis of mobile payment security measures and different standards." *Computer Fraud & Security* 2007.6 (2007): 12-16.

Kieseberg, Peter, et al. "QR code security." *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia*. 2010.

Lu, Shiyong, and Scott A. Smolka. "Model checking the secure electronic transaction (SET) protocol." *MASCOTS'99. Proceedings of the Seventh International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems*. IEEE, 1999.

Montague, David A. *Essentials of online payment security and fraud prevention*. Vol. 54. John Wiley & Sons, 2010.

Wang, Yong, Christen Hahn, and Kruttika Sutrave. "Mobile payment security, threats, and challenges." *2016 second international conference on mobile and secure services (MobiSecServ)*. IEEE, 2016.

Zhang, Yifei. "Research on online payment pattern and security strategy of e-commerce." *2010 International Conference on Internet Technology and Applications*. IEEE, 2010.