Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 114 (2017) 93–99

Procedia Computer Science

www.elsevier.com/locate/procedia

Complex Adaptive Systems Conference with Theme: Engineering Cyber Physical Systems, CAS October 30 – November 1, 2017, Chicago, Illinois, USA

Secure Online Transaction Algorithm: Securing Online Transaction Using Two-Factor Authentication

Joseph Gualdoni, Andrew Kurtz, Ilva Myzyri, Megan Wheeler, and Syed Rizvi*

Department of Information Sciences and Technology, Penn State University, Altoona PA, 16601, USA

Abstract

Identity theft is a very scary and real threat to everyone. In an attempt to give people peace of mind a new algorithm of mitigating risk is presented, the Secure Online Transaction Algorithm (SOTA). The proposed SOTA seeks to use two-factor authentication with the random codes. This form of user authentication has become widely accepted and many companies have started to implement this security feature. This can be utilized to identify users and establish secure way of purchasing items online. The proposed SOTA uses mobile devices to log into card accounts via an application to view the randomly generated code. This is then inputted on an online retailer's website when prompted in order to authenticate the individual making the purchase. This minimizes the possibility that an illegitimate user can use someone else's information to make fraudulent purchases. Without a valid code, identity thieves cannot use the stolen card information to make purchases. This in turns protects both the consumer and the credit card companies, which could be harmed financially. In order to better understand how our model could protect someone from having a stolen credit card used, we provide one case study to showcase the security.

Peer-review under responsibility of the scientific committee of the Complex Adaptive Systems Conference with Theme: Engineering Cyber Physical Systems.

Keywords: Two-Factor Authentication; Secure Online Transaction Algorithm (SOTA); AES Encrpytion; SHA–256

1. Introduction

Credit cards are a common method for payment both purchases in retailer stores and online purchases. However, while using credit cards for an online purchase there is more security in place to secure an e-mail account than a credit card. With the growing popularity of two-factor authentication many services have adopted it as the new security standard.

* Syed Rizvi. Tel.: +1-814-949-5292
E-mail address: srizvi@psu.edu

1877-0509
Peer-review under responsibility of the scientific committee of the Complex Adaptive Systems Conference with Theme: Engineering Cyber Physical Systems.
10.1016/j.procs.2017.09.016

Two-factor authentication if implemented for online purchases that utilize a credit card could help reduce if not almost eliminate fraudulent purchases made with credit cards. Users of credit cards are the most susceptible to identity theft due to the complacency users have along with the lack of security already in use. Around 18 million adults in the United States, in 2014, were victims of Identity theft [2]. Of the total amount, 86% of identity theft victims were also victims of credit card and account theft [2]. It only makes sense to use the same if not more security to secure your assets as it is to secure your e-mail.

There are many different types of threats to credit card holders. Credit cards have a majority of the information needed to make a purchase found directly on the card such as card number, security code, and expiration date. This information can be viewed and even copied by someone who you give the physical card and allow them to walk out of your sight with the card, such as a waiter or waitress [3]. Another security threat could simply be the lack of knowledge of scams to gain access to the information or being too trusting of individuals that pretend to be in a position of authority that they are not. For instance, phone call scams asking for money to provide a service that needs immediate attention. College students are at greater risk to these attacks because they are too gullible [6]. Many times, employees will be to blame for misusing or handling personal identifiable information. In turn credit card information, can then exploited by attackers [5]. Attacks on businesses databases can also be used to gain a vast amount of individual's personal identifiable information. These attacks if successful could result in leaving those that are unknowingly victims of the attack vulnerable to future attacks with their stolen information.

Social engineering is a very dangerous scam that can be used by anyone to gain information. Social engineering is manipulating an individual(s) to perform a task or provide sensitive information. This type of scam can be used to gain credit card information from one individual or even used on an individual at a company to gain access to their databases [7]. A professional penetration tester named Mati Aharoni was tasked to attempt to break into a company that had little to no presence online. He found a high ranking company official that used his corporate e-mail on a forum about collecting stamps and was interested in stamps from the 1950's. Mati registered for a URL that was about a stamp collecting site and used Google to find images of old stamps from the 1950s. He then crafted an e-mail to the high ranking company official that said that he was selling stamps and provided a link to the website. He also left a message for the official saying that he recently took possession of some 1950's and 1960's stamps. However, Mati had embedded a malicious frame on the website link that he provided to the official. The official clicked the link and compromised the system [7]. This could have easily been a real attack that would have consequences for the company.

An identity thief could easily gather the information needed to use a stolen credit card and make fraudulent purchases online. In order to counter credit card fraud, redundancies are set. Two-factor authentication (TFA) is now a widely-accepted way to confirm user identity [1]. Random pin generators can be used in along with two-factor authentication. This code would be received by the individual that holds the account the credit card is registered to via a mobile application linked to the account. By using a random pin generator while attempting to use a credit card to purchase online goods, the identity of the individual using the credit card can be verified. A purchase could be attempted by an individual who has obtained stolen information, but without the randomly generated code, the purchase would not be approved. This provides yet another safeguard from possible credit card theft. Using two-factor authentication along with a random code generator could create a safe system that is also user friendly.

The Secure Online Transaction Algorithm (SOTA) is the only type of credit card security that offers both unique authentication, and multi-layered security for the consumer. The SOTA provides security that would be able to stop a fraudulent transaction if it is attempted. The model utilizes an application provided by the credit card company. This application would be able to provide the random code for every credit card transaction. The combination of a code and registered application provides the perfect vetting of a consumer and their credit card account.

2. Related Work

Everyone's personal identifiable information is always in danger. As long as the information exists, it is susceptible to being stolen. As an example, an attack took place via Facebook in 2011 in which an individual who was a "friend" sent