ABSTRACT

With the developments in the Information Technology and improvements in the communication channels, fraud is spreading all over the world, resulting in huge financial losses. Online payment is apparently the key for the online transactions, so its security issue becomes the center of focus in the e-commerce development. We investigated the top-400 online merchants’ payment sites, and realized that the current landscape facilitates a distributed guessing attack. This attack subverts the payment functionality from its intended purpose of validating card details, into helping the attackers to generate all security data required to make online transactions. We will show that this attack would not be practical if all payment sites perform the same security checks. We will discuss potential solutions to the problem and the practical difficulty to implement these, given the varying technical and business concerns of the involved parties.

Keywords—security; online payment; distributed attack; fraudulent transactions; survey; ethical disclosure

1. Introduction

Fraud can be defined as wrongful or criminal deception intended to result in financial or personal gain [1], or to damage another individual without necessarily leading to direct legal consequences. As the value of online sales has increased, so cards are the de facto means of paying for online purchases the amount of online fraud. As an example, UK online sales in 2014 was worth £45 billion, which represents a 16% growth between 2013 and 2014 [2]. In the same time period, the value of online fraud in the UK has increased by 33% to £217 million [3].

In this survey, we show the online card payment security in brief. Here we highlighted, different patterns of online payment performed, and various security measures put by online merchants as from checking card numbers, expiry date, cvv to many security questions. [4] But does the difference cause a security problem? If yes how common is the problem and can it be exploited? How much damage can be done? How could it be resolved in the future? To determine this problem, we survey ‘Online Payment Card System Security’.

We demonstrate the practicability of exploiting the vulnerabilities with software that implements the distributed guessing attack. We will show that the potential impact of these vulnerabilities is substantial because the card details generated by this distributed attack can be used to transfer money from a victim’s bank account to an anonymous recipient overseas using a financial services company such as the Western Union as a conduit.

The vulnerabilities described in this article apply to cards that do not enforce centralized checks across transactions from different sites. Our experiments were conducted using Visa and MasterCard only. Whereas MasterCard’s centralized network detects the guessing attack after fewer than 10 attempts (even when those attempts were distributed across multiple websites),[5] Visa’s payment ecosystem does not prevent the attack (see Section VI.D). Because Visa is the most popular payment network in the world, the discovered vulnerabilities greatly affect the entire global online payments system.

2. Overview of the Online Payment System

An e-commerce payment system facilitates the acceptance of electronic payment for online transactions. Also known as a sample of Electronic Data Interchange (EDI), e-commerce payment systems have become increasingly popular due to the widespread use of the internet-based shopping and banking.

An online payment site uses a customer’s existing credit or debit card to transfer funds from the customer’s bank account into the merchant’s bank account. For this to happen, the customer needs to provide their card information during checkout. These pieces of information are then passed to the card issuing bank, who will process the
information further before authorizing or rejecting the payment request. This process involves a number of parties, each with different responsibilities.

Figure 2.1. Actions and parties in online payment.

A. Online Payment Process and Parties Involved

Figure 2.1 illustrates the actions and parties involved in processing online payments. The process involves the customer/cardholder entering their payment card details on the payment page of the online merchant’s website. The merchant controls which data fields are used to authorize the payment.

The merchant then passes the card details to their chosen payment gateway, which provides a service of authorizing and processing the merchant’s payment request. The payment gateway then connects the merchant to the card payment network to request payment from the customer’s bank account held at the card issuing bank. The payment networks (such as Visa and MasterCard) provide the link between payment gateways and the thousands of card issuing banks.

The card-issuer holds the customer’s bank account and makes the approval of the payment. The issuer maintains the customer’s card record file, which contains information such as account balance, customer name, full address, and other card details not visible to the rest of the payment network. In the final step, called a settlement, the card issuing bank subsequently deposits the customer’s money to the merchant’s bank account.

B. Payment Card Data Fields

An online payment is a “card-not-present” credit or debit card transaction [6]. This implies the merchant cannot physically verify that the customer actually has the card. The security of online payment is therefore dependent upon the customer providing data that only the owner of the card could know.

However, there is no requirement for the merchant to request all of the data fields during an online payment authorization, nor is there a mandatory requirement for the merchant to implement any of the optional security filters. Five pieces of information are typically used when making an online payment:

- **Cardholder Name**: the account holder’s name as printed on the card. We found that no website checks that a name entered is correct.

- **16-digit Card Number**: a unique identifier printed on the front of the card by the issuing bank. Referred to as the **Primary Account Number (PAN)**, it links the card to the customer’s bank account.

- **Card Expiry Date**: printed or embossed on the front of the card. The expiry date and the PAN constitute the minimum set of card authentication data.

- **Card Verification Value (CVV2)**: a 3-digit number printed on the reverse side of the card. It is meant to be known only to the person possessing the card. It should not be stored electronically anywhere in the payment ecosystem [7].
3. Distributed Guessing Attack

Card fraud begins either with the theft of the physical card or with the compromise of data associated with the account, including the card account number or other information that would routinely and necessarily be available to a merchant during a legitimate transaction. The reason this attack works in practice is due to two weaknesses, each not too severe on its own, but when used together present a serious risk to the global payment system.

The first weakness is that in many settings, the current online payment system does not detect multiple invalid payment requests on the same card from different websites. Effectively, this implies that practically unlimited guesses can be made by distributing the guesses over many websites, even if individual websites limit the number of attempts.

Secondly, the attack scales well because different web merchants provide different fields, and therefore allow the guessing attack to obtain the desired card information one field at a time. To understand how essential the scaling issue is, we look at the differences in websites in some more detail. The data fields that web merchants use can be divided into three categories:

- 2 fields: PAN + Expiry date (the absolute minimum)
- 3 fields: PAN + Expiry date + CVV2
- 4 fields: PAN + Expiry date + CVV2 + Address

Starting with a valid card number (PAN), to guess the expiry date an attacker can utilize several merchants’ websites that check only two fields: the card number and the expiry date. Once the expiry date is known, the attacker can use it along with the card number to guess the CVV2 information using another set of websites that check 3 fields (the card number, the expiry date, and the CVV2).

Guessing an expiry date takes at most 60 attempts (banks typically issue cards that are valid for up to 60 months), and subsequently, guessing the 3-digit CVV2 takes fewer than 1,000 attempts. Hence, expiry date and CVV2 are guaranteed to be obtained within $60 + 1,000 = 1,060$ guesses.

For many purposes, knowing the PAN, expiry date and CVV2 is sufficient to use a card online, but for some purchases, an attacker would also need to obtain address information. To guess address information, the attacker needs to use websites that ask for 4 fields. The address field is used in a variety of manners, based on the Address Verification System (AVS), which validates the billing address provided by the customer against the address information stored by the card-issuing bank [6][8][9].

4. Experiments

We implemented a set of software tools to carry out the distributed guessing attack, using the research team’s own cards to verify that it is indeed possible and practical to obtain all the information of the card. Included are seven Visa cards with a spread of PAN, expiry date, and CVV2 values. We selected 400 Alexa [12] top rated commercial websites for our investigation. These include many global websites such as iTunes, Google, PayPal, and Amazon.

A. Software Tools

The software tools implemented for the experiments consist of a website bot and automated scripts written in Java Selenium browser automation framework [13]. All the experiments were run on Mozilla Firefox web browser. Fig. 2 shows a screenshot of the website bot, which was used to automate the process of guessing relevant card information. The bot cycles through the possible values for each field to find the correct information.
A. Obtaining Card Data

The PAN is the starting point for the generation of all of the other card data fields. There are at least two known methods of obtaining valid PANs. Criminals sell bulk lists of card details online. These lists are considered less valuable when they do not contain the CVV2; nevertheless, such a list could be used as a source of PANs from which the expiry date, CVV2 and address information can be generated.[13]

The next step in card data generation involves getting the card’s CVV2. To find the correct CVV2, the bot will simply need to cycle through the possible values starting from 001 until the payment website blocks further attempts. A handful of payment sites allowed unlimited attempts while most of the other payment sites allowed 5, 10 or even 50 attempts to enter a correct CVV2. In our scenario, we “farm out” the brute force guessing attack to tens or even hundreds of payment systems, which practically means we can carry out unlimited guesses. The final step generates the cardholder’s address. An attacker can exploit the different variants of address verification system (discussed in Section III) to find the full address of the cardholder.[11]

B. Transferring the Money

Once either two, three, or four fields of the card data have been obtained, the attacker can use them to purchase goods on a website. Rather than buying online goods from an e-commerce website, we created an attack scenario that uses the card details to open a money transfer account, sends the money to an anonymous recipient abroad, where the money is picked up within minutes of issuing the transfer.[12] The attacker needs to be able to clear the funds before the issuing bank reverses the payment and thwarts the attack. It is therefore desirable from the attacker’s point of view that the funds are transferred to an account outside the country (because it is more time consuming and costly to reverse payment across countries) or be conducted through a wire transfer to an anonymous cash recipient by using services such as the Western Union.[13]

5. Diffie Hellman Algorithm

![Diffie-Hellman Key Exchange Diagram]

**Diagram:**

- **Step 1:** Alice chooses a private key and calculates the corresponding public key.
- **Step 2:** Bob chooses a private key and calculates the corresponding public key.
- **Step 3:** Alice and Bob exchange their public keys.
- **Step 4:** Alice and Bob calculate shared secret keys using their own private keys and the public key they have received.

---

**Fig.ure4.1:** Screenshot of the website bot, farming CVV2 from multiple sites.
- P and G are both publicly available numbers. P is at least 512 bits.
- Users pick private values a and b.
- Compute public values
  - $x = g^a \mod p$
  - $y = g^b \mod p$
- Public values x and y are exchanged

- Compute shared, private key
  - $k_a = y^a \mod p$
  - $k_b = x^b \mod p$
- Algebraically it can be shown that $k_a = k_b$
  - Users now have a symmetric secret key to encrypt.

A. Case study
- Alice and Bob get public numbers
  - $P = 23$, $G = 9$
- Alice and Bob compute public values
  - $X = 9^4 \mod 23 = 6561 \mod 23 = 6$
  - $Y = 9^3 \mod 23 = 729 \mod 23 = 16$
- Alice and Bob exchange public numbers
- Alice and Bob compute symmetric keys
  - $k_a = y^a \mod p = 16^4 \mod 23 = 9$
  - $k_b = x^b \mod p = 6^b \mod 23 = 9$

6. Conclusion
We showed that the attack works if the card payment network is not able to relate card activities from different websites. Fundamentally, much of the problem with card payment stems from the fact that the identity of the payer needs to be established in the ‘card-not-present’ mode. To prevent the attack, either standardization or centralization can be pursued (some card payment networks already provide this). Standardization would imply that all merchants need to offer the same payment interface, that is, the same number of fields. Then the attack does not scale anymore. Centralization can be achieved by payment gateways or card payment networks possessing a full view over all payment attempts associated with its network. Neither standardization nor centralization naturally fit the flexibility and freedom of choice one associates with the Internet or successful commercial activity, but they will provide the required protection. It is up to the various stakeholders to determine the case for and timing of such solutions.

REFERENCES
London:UK Cards Association, 2015,


