Review of 3-D Secure Protocol

Shweta Rathour

Abstract*: Banks worldwide are starting to authenticate online card transactions using the `3-D Secure' protocol, which is branded as Verified by Visa and MasterCard Secure Code. This has been partly driven by the sharp increase in online fraud that followed the deployment of EMV smart cards (EMV comes from the initial letters of Euro-pay, MasterCard, VISA) for cardholder-present payments. 3-D Secure has so far escaped academic scrutiny; yet it might be a textbook example of how not to design an authentication protocol. It ignores good design principles and has significant vulnerabilities, some of which are already being exploited. Also, it provides a fascinating lesson in security economics. While other single sign-on schemes such as OpenID, InfoCard and Liberty came up with decent technology they got the economics wrong, and their schemes have not been adopted. 3-D Secure has lousy technology, but got the economics right (at least for banks and merchants); it now boasts hundreds of millions of accounts.

The 3-Domain Secure protocol specification defines an architecture and protocol for verifying cardholder account ownership during a purchase transaction in the remote environment. After initiating the final purchase action, the cardholder is placed into a dialog with his issuing financial institution. The Issuer authenticates the cardholder and sends a confirmation of identity back to the merchant; the merchant completes the transaction.

Index Terms*: Access Control Server (ACS), Address Verification Service (AVS), Payment Cards Industry Data Security Standard (PCIDSS), SSL/TLS Secure Socket Layer/Transport Layer Security, Secure Electronic Transaction (SET)

I. INTRODUCTION

The core 3-D secure protocol was designed for the support of "Internet shopping", where the cardholder is shopping using an Internet-enabled device, and the authentication takes place over the Internet. With the publication of the mobile Internet extension, the protocol was expanded to support shopping using Internet-capable mobile Internet devices. In particular WAP phones. However, both shopping and authentication can be performed using mobile phones with more limited capabilities, using either:

- Two-way messaging (SMS or USSD), which is becoming increasingly popular in both Asia and Europe, or
- The voice channel, particular using an Interactive Voice Response (IVR) system.

``While the vast majority of Internet transactions still take place via PCs, it is essential that a secure standard be in place for transactions that originate from mobile phones or other mobile devices," said Philip Yen, executive vice president, e-Visa International. ``Consumers need to feel the same sense of security when they shop online using a mobile phone as when they shop in the physical world."

Manuscript received on July, 2013.

Shweta Rathour, Asstt Professor, Computer Science and Engineering Department, I.T.S Engineering Collages, Greater Noida, India.

The Mobile 3-D secure specification supports global interoperability, enabling consumers to have a consistent and seamless experience regardless of the method or device being used to access the Internet. It minimizes the impact on merchants and requires no changes to backend payment systems [3].

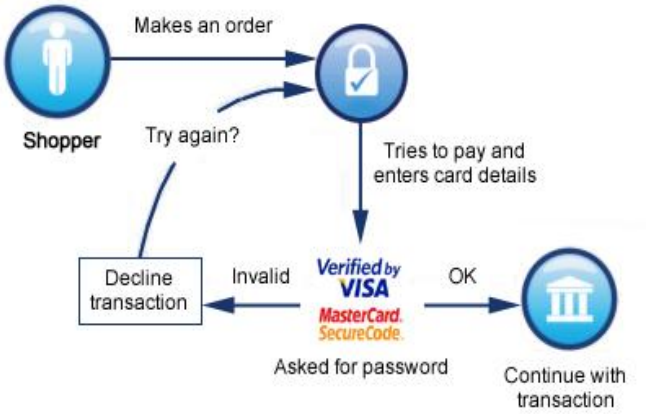

Figure 1 General flow chart for 3-D secure protocol

The growth in mobile phone usage shows a clear trend toward wireless Internet devices. According to Nokia, during 2002, more people will be accessing the Internet with handheld, wireless devices than via landlines. Analyst and consulting company Ovum Limited suggests that, globally, 373 million wireless subscribers will be buying on-line in 2004[1].

Security is a major concern for all involved in E-Commerce and particularly in the case of online transactions using debit / credit card. Following the failure of Secure Electronic Transaction (SET), 3-D Secure is an emerging industry standard for online transaction security[7]. Although 3-D Secure is a well designed protocol, it is still prone to some security problems and excessive numbers of messages which could reduce the speed of transaction. This paper uses a new cryptographic technique based on password only authentication and key exchange to present a new vision for 3-D secure. The new vision covers the security problems and reduces the number of messages for 3-D Secure. Moreover, the new vision has the development ability to simulate SSL/TLS in its simplicity and at the same time abolishes SSL/TLS security glitches. This simplicity and security are the necessary factors for online transaction protocol to be the future standard.

II. PURPOSE OF 3-D SECURE PROTOCOL

Security is a very important area that must be considered when choosing an online payments platform. The first step is to be sure that you are dealing with a reputable company who are PCI compliant. Payment Cards Industry Data Security Standard (PCI DSS) Performing a 3-D secure payment is split up into two

distinct processes. Firstly the customer submits their card details for verification of enrolment in the 3-D Secure scheme. This is achieved by processing a Card Query request.

A Card Query request submits information to a directory server hosted by a card issuer (e.g. Visa). If a card is in the 3-D Secure scheme the Card Query response will contain html that must be relayed to the customer. This html redirects the customer to a log-in screen enabling them to validate their identity through an Access Control Server (ACS) hosted by a card issuer. In addition to customer card details a Card Query request will contain a redirect URL (Term Url) enabling the customer to be redirected from the ACS back to the merchants site to finalise the authentication and perform the actual authorisation.

The second part of the process involves the merchant submitting an authorisation request with payment and additional 3-D secure validation information. The additional information required is obtained from the data that the ACS redirects to the merchant, details of which are highlighted in this document.

Benefits of the 3-D secure process include the enhanced security available when performing a 3-D secure transaction and the shift of liability in the event of fraudulent transactions. If a 3-D secure transaction is completed and has been determined to be fraudulent then the credit liability is usually shifted from the merchant and onto the card issuer. In most 3-D Secure cases the merchant will not receive any notification of a chargeback if the transaction is disputed by the cardholder. This is a major benefit in reducing lost revenue due to fraudulent transactions. Please note however, that 3-D Secure is not a 100% guarantee that no chargeback's will be incurred. There are some restrictions for each scheme although these cases should not occur very often.

A. ACS Providers.

In 3-D Secure protocol, ACS (Access Control Server) is on the issuer side (banks). Currently, most banks outsource ACS to a third party. This means the buyer's web browser shows unfamiliar domain names instead of the banks' domain names. RJ

B. MPI providers

As Each 3-D secure transaction involves two simple internet request/response pairs : VEReq / VERes and PAReq/ PARes. Visa and MasterCard don't license merchants for sending requests to their servers. They isolate their servers by licensing software providers which are called MPI (merchant plug-in) providers.

3-D Secure is a specification developed by Visa to improve transaction performance online and to accelerate the growth of electronic commerce. Verified by Visa (VbV) and MasterCard Secure Code (MSC) are authentication programs based on the 3-d secure Specification

The current protocol version is 1.0.2.

3-D Secure is a simple, password-protected system that tells on-line retailers and banks that cardholders are genuine. The increased benefits to retailers are:

- Reduces repudiated transactions
- Reduces fraud losses
- Reduces administration of disputes
- Lowers screen errors
- Increases your reputation
- Increases your sales
- Increases your transaction values

The 3-D secure protocol is a technical platform that includes technical specifications and requirements for Issuers, Acquirers, and Merchants. In addition to utilizing the widely supported Internet technology Secure Sockets Layer (SSL) encryption to protect payment card information during transmission over the Internet, 3-D Secure uses cardholder authentication to verify the parties involved in the transaction.

III. SECURITY AND FRAUD PREVENTION

Use Security is a very important area that must be considered when choosing an online payments platform. The first step is to be sure that you are dealing with a reputable company who are PCI compliant. Payment Cards Industry Data Security Standard (PCI DSS) is a worldwide security standard that applies to organizations that transmit process or store cardholder data. The next area to consider is the fraud prevention services offered by the PSP or payments bureau. Here is a list of the common services that you should expect to be offered:

A. Address Verification Service (AVS)

AVS is a service that allows the billing address provided by the customer to be verified with the issuing bank at the time of authorization. It is an extra security measure that can help to reduce the number of fraudulent transactions.

B. Card Verification Code (CVC).

The CVC is an extra security measure introduced to give increased protection against credit card fraud. A 3 or 4 digit security code is usually printed on the back of the card. The customer will be required to enter this along with the credit card number and expiry date. It will be verified along with this information by the credit card issuer. CVC is also known as Card Security Code (CSC) and Card Verification Value (CVV). The naming and the location of the number on the card may differ but the concept is the same.

C. 3D-Secure

3D-Secure is the payment's industries Internet authentication standard. It can be thought of as the online version of chip and pin. The Visa implementation of the standard is known as Verified By Visa and the MasterCard implementation is known as MasterCard Secure code. Cardholders who are registered for 3D-Secure will have a personal password that is

associated with their account. When they want to make a purchase online they can use their password to verify their identity. They can only do this if the website that they are making their purchase on supports 3D-Secure. There are advantages to both the Merchant and the customer for 3D-Secure. For the merchant it can help to reduce chargeback's and in the case where a chargeback occur's the liability can be shifted to the cardholders issuing bank if the authorization was verified by 3D-Secure. For the customer it will give them increased confidence when making a purchase as they can see that you care

about security [2].

D. Custom Fraud Checking

Some service providers will offer their own custom fraud checking routines or fraud scoring systems. Their fraud checks will highlight transactions that they suspect maybe fraudulent. Examples of such checks might be to look for transactions where the card is issued in a country with a high level of fraud, to highlight transactions where the delivery address differs from the billing address. Fraud checking is good as it can help reduce the number of fraudulent transactions and reduce the amount of chargeback's. The security of your own website is something that should also be considered. Depending on your method of integration to the Payment Gateway you may need to be PCI DSS compliant.

IV. CONCLUSION

After studying the various components of 3-D secure protocol We conclude that it will provide better security and remove the risk over the internet in online payment system. Thus, making the customer comfortable with the concept of online payment, and increase its usage and making things more comfortable for the customer and the merchants.

ACKNOWLEDGMENT

I want to thank my lovely husband Rohit Rajput for his love and support and my father S. C.Rathore and Mother Kumud for making me who I am and my brother Vishu for being there as a pillar of strength.

REFERENCES

1. APACS 2008 fraud _gures announced by APACS, March 2009. http://www.ukpayments.org.uk/media_centre/press_releases/-/page/685
2. 3-DSecure system overview. retrieve_ document.do?document RetrievalId=119.
3. Gartner, Inc., 2001. The Evolution of e-Business Security Requirements, a white paper prepared for Verisign. Inc, 2001.
4. http://www.cellular.co.za/technologies/mobile-3d/visa_mobile_ 3d.htm
5. http://www.springerlink.com/content/9363732532476t76/
6. http://www.webpayments.ie/web-payments/how-do-i-setup-online-payments/online-payment-security-and-fraud-prevention#3dsecure
7. Internet Retailer. Veri_ed by Visa security program used as bait in phishingscams,6January2005. http://www.internetretailer.com/dailyNews.asp?id=13764.
8.]J onVarco. Varied by Visa update.
9. http://www.barclaycardbusiness.co.uk/ information zone/customer forum/pdf/1315_jon_varco_visa.pdf.
10. Mohammed Assora and Ayoub Shirvani "Enhancing the Security and Efficiency of DSecure" Information Security Lecture Notes in Computer Science, 2006, Volume 4176/2006, 489-501, DOI: 10.1007/11836810_35
11. Nicholas Bohm, Ian Brown, and Brian Gladman. Electronic commerce: Who carries the risk of fraud? The Journal of Information, Law and Technology,(3),Oct2000.Cronto.http://www.cronto.com/download/Cronto_Products_Datasheet.pdf.
12. RBS Secure Terms of Use, December 2009. https://www.rbssecure.co.uk/rbs/ tdsecure/terms_of_use.jsp.
13. Saar Dimmer, Steven J. Murdoch, and Ross Anderson. Optimized to fail: Card readers for sonline banking. In Financial Cryptography, LNCS 5628. Springer, 2009. EMVCo, LLC. EMV 4.1, June 2004. http://www.emvco.com/.

AUTHOR PROFILE

Shweta Rathour, has done her Bachelor of Technology from G.I.E.T, Dehradun in 2009. She completed her M.Tech from D.I.T, Dehradun in 2011.Presently she is working in I.T.S. Engineering College, Greate Noida as an Asst. Professor in Computer Science and Engineering Department.