3D Secure ™ Security Protocol

Presented by Emre Kaplan

Introduction

- Credit cards and online payment are now become a part of our daily life.
- Most of us use credit cards based on either Visa or Mastercard.
- These companies produces the credit cards and other payment solutions for the banks.
- As seen, Visa or Mastercard which we call "the type of the card" is actually the brand of the payment solution (brand of your credit card in case of cards).

Introduction -cont.

- These companies are responsible for maintaining the security of the whole solution (credit cards, the data communication, underlying protocols etc.)
- So What is 3D Secure???
- It is an XML-based protocol used as an layer of security for online credit or debit card transactions.
- It is developed by Visa.
  - Aim is to improve the security of Internet payments.
- Visa and Mastercard uses this technology nowadays and they provide this service under different names.
  - Visa calls it as *Verified by Visa.*
  - Mastercard calls it as *Mastercard SecureCode*
  - JCB International calls it as J/Secure.

Introduction –cont.

- 3D Secure is introduced as a means of shifting responsibility for fraud away from credit card companies.
- It introduces more secure transactions, where the party not implementing the technology is responsible for money lost due to fraud.
- Overall, 3D Secure is popular nowadays and used almost in all credit cards and internet payments.
- Goal is to provide securer protocol for this transactions and shifting fraud responsibility.

Basic Aspects of the Protocol

- Basic concept of the protocol is to tie the financial authorization process with an online authentication.
- authentication is based on a 3 domain model (that is the 3-D in the name).
- The three domains are:
  - Acquirer Domain (the commerce)
  - Issuer Domain (the bank issuer of the credit card)
  - Interoperability Domain (Worldwide credit card and support)
- The protocol uses XML messages sent over SSL connections with Client Authentication (this ensures the authenticity of both peers, the Server and the Client, using Digital Certificates).

Basic Aspects –cont.

- A transaction using Verified by Visa/SecureCode will initiate a redirect to the website of the card issuing bank to authorize the transaction.
- Each Issuer could use any kind of authentication method (the protocol does not cover this)
  - but typically, a password-based method is used, so to effectively buy on the Internet means using a secret password tied to the card.
- The Verified by Visa protocol recommends the bank's verification page to load in an inline frame session. In this way, the bank's systems can be held responsible for most security leaks.

Domains

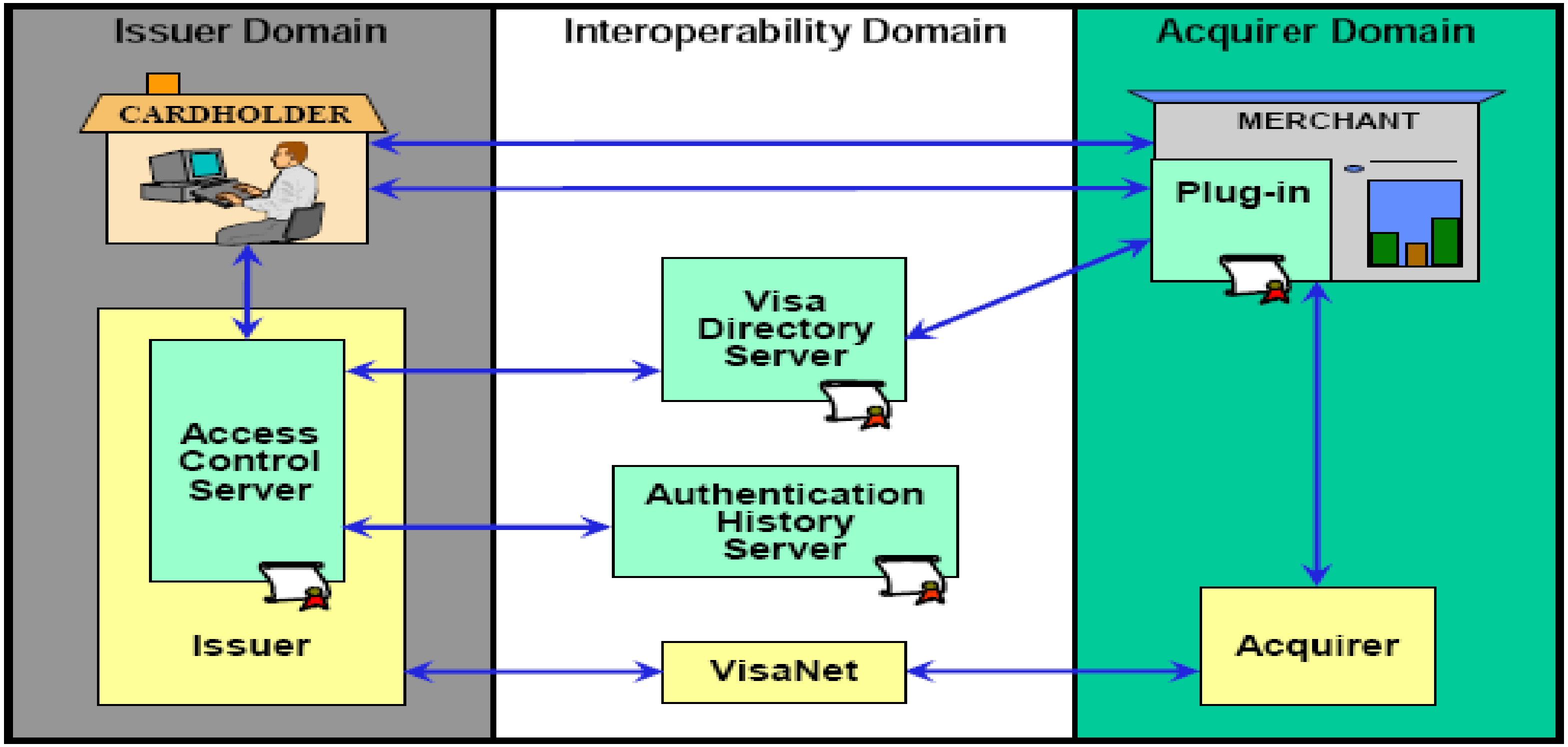
- **Issuer Domain ->** the Issuer is responsible for:
  - Managing the enrollment of their cardholders in the service (including verifying the identity of each cardholder who enrolls) and authenticating cardholders during online purchases.
- **Acquirer Domain->** the Acquirer is responsible for:
  - Defining the procedures to ensure that merchants participating in Internet transactions are operating under a merchant agreement with the Acquirer,
  - Providing the transaction processing for authenticated transactions.
- **Interoperability Domain**
  - This domain facilitates the transaction exchange between the other two domains with a common protocol and shared services.

Software Components

The 3-D Secure protocol divides the authentication process into three parts or "domains" according to the participants involved:

Issuer Domain	Issuers and Cardholders
Acquirer Domain	Acquirers and Merchants
Interoperability Domain	Visa-operated systems that connect the Issuer and Acquirer Domains

Figure 1 illustrates and the remainder of this section describes the key software components in each domain.



3-D Secure Protocol Features

- Provides global framework for the authentication of remote payments
- Reduces operational expense by minimizing chargeback for unauthorized use
- Can be implemented without requiring specialized cardholder software or hardware
- Can be enhanced by the issuer as needed to meet customer management and security requirements without impact on the acquirer or merchant

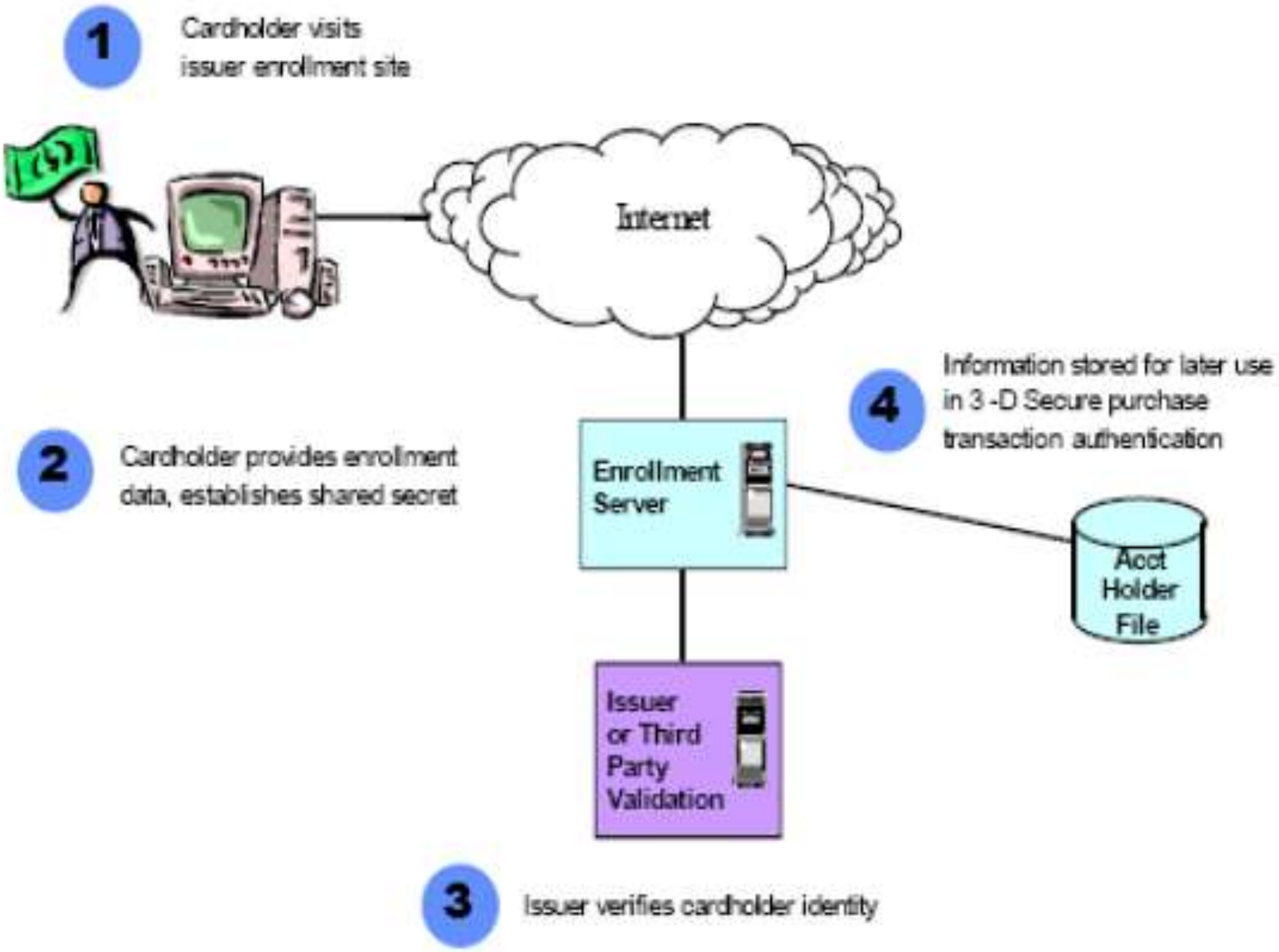
3-D Secure Protocol Features

- Is extensible into emerging channels such as mobile telephones, PDAs, and digital TV
- Is based on globally accepted technical standards provided by international standards bodies such as IETF
- Provides a centralized archive of payment authentications for use in dispute resolution

Overall, what does 3D Secure bring?

- 3-D Secure leverages Transport Layer Security (TLS) technology, which is incorporated in most browsers currently in use.
- Provides confidentiality of information, ensures payment integrity, and authenticates cardholders.
- Shifts the security responsibility from card company to bank or merchant.
- Enrollment and Purchase transaction processes are illustrated in the next slides.

Figure 3–4: Sample Cardholder Enrollment Process



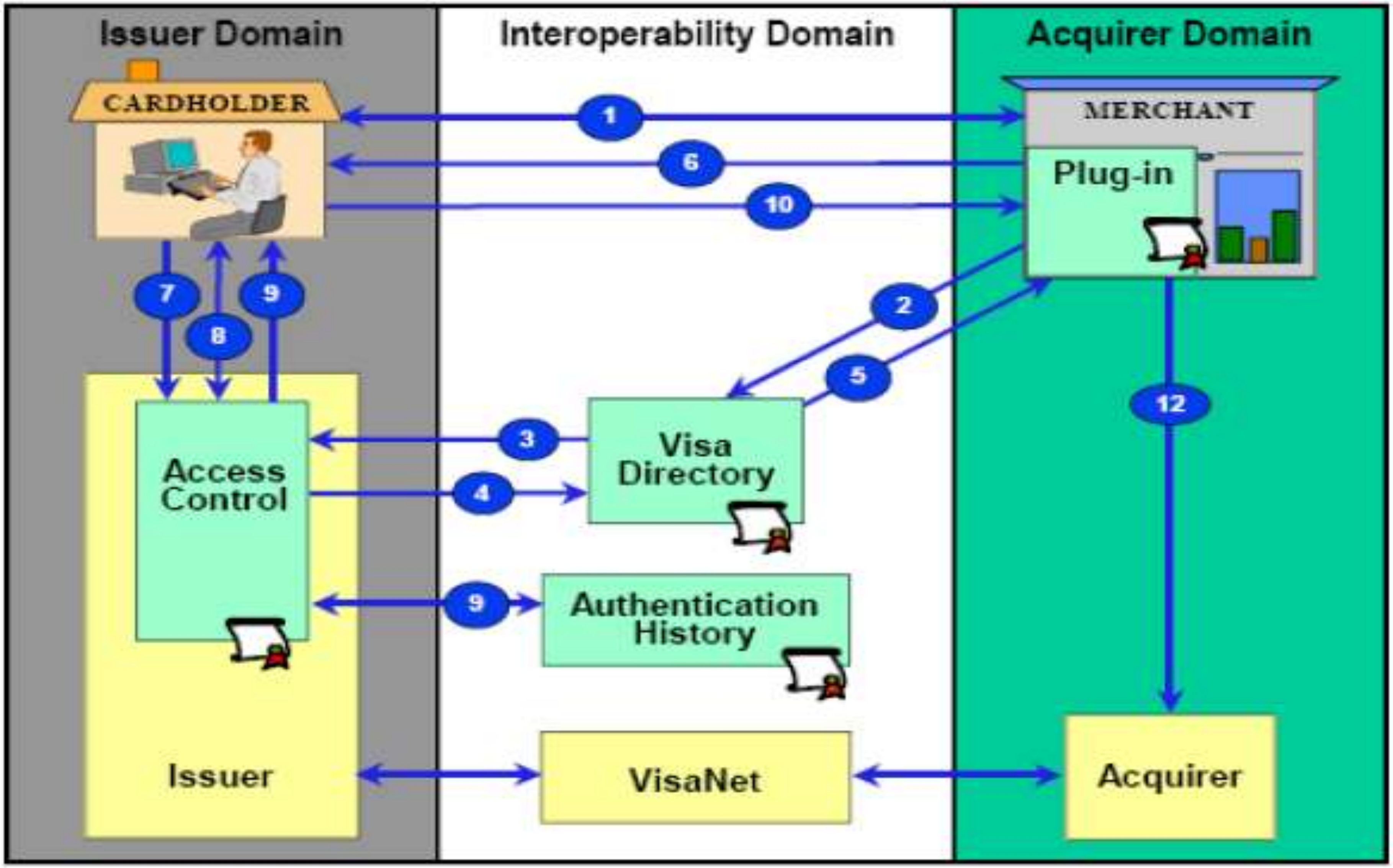
1 Cardholder visits issuer enrollment site

2 Cardholder provides enrollment data, establishes shared secret

3 Issuer verifies cardholder identity

4 Information stored for later use in 3 -D Secure purchase transaction authentication

Figure 3–3: Purchase Transaction Flow



Criticism and Drawbacks

- The "Verified by Visa" system has drawn some criticism, since it is hard for users to differentiate between the legitimate Verified by Visa pop-up window or inline frame, and a fraudulent phishing site.
- This is because the pop-up window is served from a domain which is:
  - Not the site where the user is shopping.
  - Not the card issuing bank.
  - Not visa.com.

Criticism –cont.

- Newer recommendation to use an inline frame (IFrame) instead of a popup window has reduced user confusion, but at the cost of making it is harder for the user to verify that the page is genuine in the first place.
  - As of 2008, most web browsers do not provide a simple way to check the security certificate for the contents of an iframe.
- Some card issuers also use Activation During Shopping (ADS), in which cardholders who are not registered with the scheme are offered the opportunity of signing during the purchase process. This will take them to a form in which they are expected to confirm their identity by answering security questions which should be known to their card issuer.
  - This will take users to registration form in an iframe which they can NOT easily verify the site.

Criticism –cont. Man in the Middle Attack

- Cardholders who are not willing to take the risk of registering their card during a purchase at commerce site can go to their bank's home page in a separate window and register from there.
- When they go back to the commerce site and start over they should see that their card is registered.
- The presence on the password page of the Personal Assurance Message (PAM) that they chose when registering is their confirmation that the page is coming from the bank.
- This still leaves some possibility of a man in the middle attack if the card holder cannot verify the SSL Server Certificate for the password page.

A possible solution for Man in the Middle Attack

- Some commerce sites will devote the full browser page rather than iframe.
  - In this case the lock icon in the browser should show the identity of either the bank or the operator of the verification site.
- The cardholder can confirm that this is in the same domain that they visited when registering their card, if it is not the domain of their bank.
- If it is neither bank nor the merchant then it is said to be fraud.

Criticism –cont. USA Case

- When signing up for "Verified by Visa" in the USA the user is required to enter last 4 digits of their social security number.
- If the digits are incorrect, the user gets to try a different combination and the number of attempts is unlimited.
- This makes it theoretically possible to "guess" someone's last 4 social security digits, simply by trying all numbers from 0001 to 9999.

Passwords

- Protocol allows up to 8 digit of password thus not allowing passwords of adequate length for proper security.
- 8 digit = 64 bit, so is it secure enough?
- It is *computationally secure* depends on the encryption methods used.
  - One may break up the system with enough computer power and enough patience ☺

Conclusion

- Many of the security requirements are handled by TLS/SSL, since 3D Secure is made top of TLS/SSL.
- It is securer than the prior protocol called SET.
- The fraud responsibility is no longer held by the card companies.
- It is an extensible global framework that provides confidentiality of information, ensures payment integrity, and authenticates cardholders.

References

- Wikipedia
  - http://en.wikipedia.org/wiki/3-D_Secure
- Verified by Visa Merchant Implementation Guide
- Verified by Visa Introduction
- Verified by Visa System Overview
  - www.visa.com