Online Business Security: SSL, TLS, SET and 3D-Secure

Anupama Chowdhary
Principal, Keen College,Bikaner (Rajasthan),India

Abstract – In online business shoppers must feel completely assured that their credit card and banking details are secure and cannot be accessed by hackers. SET (Secure Electronic Transaction) was developed to fill this need and to basically guarantee payment transactions, from the shopper's desktop to the merchant's website and on to the banking gateway. 3D-Secure protocol was designed to be an additional security layer for online credit and debit card transactions; it is an XML-based protocol. SSL (Secure Socket Layer) and TLS (Transport Layer Security) on the other hand, was designed to provide secure communications over the internet, not secure financial transactions. The 3D-Secure protocol uses XML messages sent over SSL/TLS connections with client authentication.

Index terms – SET (Secure Socket Layer), XML (Extensible Markup Language), TLS (Transport Layer Security), S-HTTP (Secure Hypertext Transfer Protocol), PKI (Public Key Infrastructure), POODLE.

I. INTRODUCTION

For the safe electronic transactions on the internet a universally accepted protocol was required by consumers, vendors and even banking institutions. These safety measures also had to work across different applications and platforms, such as HTTP, Telnet and FTP for instance. In 1994, Netscape came with SSL to secure transactions on insecure network. Within a year this became the most widely accepted way to encrypt data, provide client and vendor authentications and secure the integrity of data transmitted over insecure networks. SSL is used to secure data in emails, web browsers, internet faxing, instant messaging and VoIP.

Thai Duong and Krzysztof Kotowicz from the Google security team discovered the POODLE attack on SSL 3.0 and they disclosed the vulnerability publicly on October 14, 2014 [1]. The POODLE stands for "Padding Oracle On Downgraded Legacy Encryption". It is a man-in-the-middle attack which takes advantage of Internet and security software clients' fall back to SSL 3.0.[1][2][3]. If attackers successfully exploit this vulnerability, on average, they only need to make 256 SSL 3.0 requests to reveal one byte of encrypted messages. This attack allows hackers to access passwords and reveal users' account information on websites.

TLS was designed in January 1999 as the upgraded version of SSL. Many websites and servers supporting both SSL and TLS is that hackers can still gain access to private information by backtracking from TLS to SSL. The solution to this problem is to ensure that your website, and the server it's hosted on, only supports TLS 1.2 and that SSL support has been disabled.

SET was developed by the SET Consortium, in 1996. It is backed by financial institutions, MasterCard and Visa. It provides a secure payment gateway for consumers, vendors and financial institutions. SET was not itself a payment system, but rather a set of security protocols and formats that enabled users to employ the existing credit card payment infrastructure on an open network in a secure fashion. SET makes use of Netscape's Secure Sockets Layer (SSL), Microsoft's Secure Transaction Technology (STT), Terisa System's Secure Hypertext Transfer Protocol (S-HTTP) and some aspects of a public key infrastructure (PKI). But, it failed to gain attraction in the market. VISA now promotes the 3D-Secure scheme.

3D-Secure protocol was designed to be an additional security layer for online credit and debit card transactions; it is an XML-based protocol. It was first deployed by Visa with the intention of improving the security of Internet payments [4]. MasterCard, JCB International and American Express also adopted services based on this protocol. Analysis of the protocol by academic world has revealed that it have many security issues that affect the consumer, majorly phishing and a shift of liability in the case of fraudulent payments [5].

II. SSL (SECURE SOCKET LAYER)

For establishing an encrypted and secure link between a web server and a browser the standard security technology SSL is used. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers. There are three versions of SSL protocol; SSL 1.0, 2.0 and 3.0. SSL Protocol has three sub-protocols namely: handshake, record and alert protocols. Communication using SSL begins with an exchange of information between the client and the server known as the SSL handshake. The main resolutions of the SSL handshake are:

- Negotiate the cipher suite: The cipher suite includes information about the public key exchange algorithms, secret key encryption algorithms, and cryptographic hash functions. The client tells the server which cipher suites it has available, and the server chooses the best mutually acceptable cipher suite.
- Authenticate identity (optional): To prove that a server belongs to the organization that it claims to represent, the server presents its public key certificate to the client. If this certificate is valid, the client can be sure of the identity of the server. In an e-commerce transaction over the Web, the client will generally want to authenticate the server. The client and server exchange information that allows them to agree on the same secret key (symmetric key).
- Establish information security by agreeing on encryption mechanisms: With each message, they use the cryptographic hash function, chosen in the first step of this process, and shared secret information, to compute an HMAC that they append to the message. They then use the secret key (symmetric) and the secret key algorithm negotiated in the first step of this process to encrypt the secure data and the HMAC. The client and server can now communicate securely using their encrypted and hashed data.

After a successful handshake record protocol provides mainly two services:

- Confidentiality: It is achieved via shared secret key.
- Integrity: It is achieved via MAC (Message Authentication Code)

Alert protocol is activated whenever error is detected by either client or server. Detecting party sends alert message to the other party. There are two types of errors:
Fatal errors: the connection is terminated on detection of error.
Normal errors: the error is handled and connection is not terminated.
The overall scenario is given in figure 1.

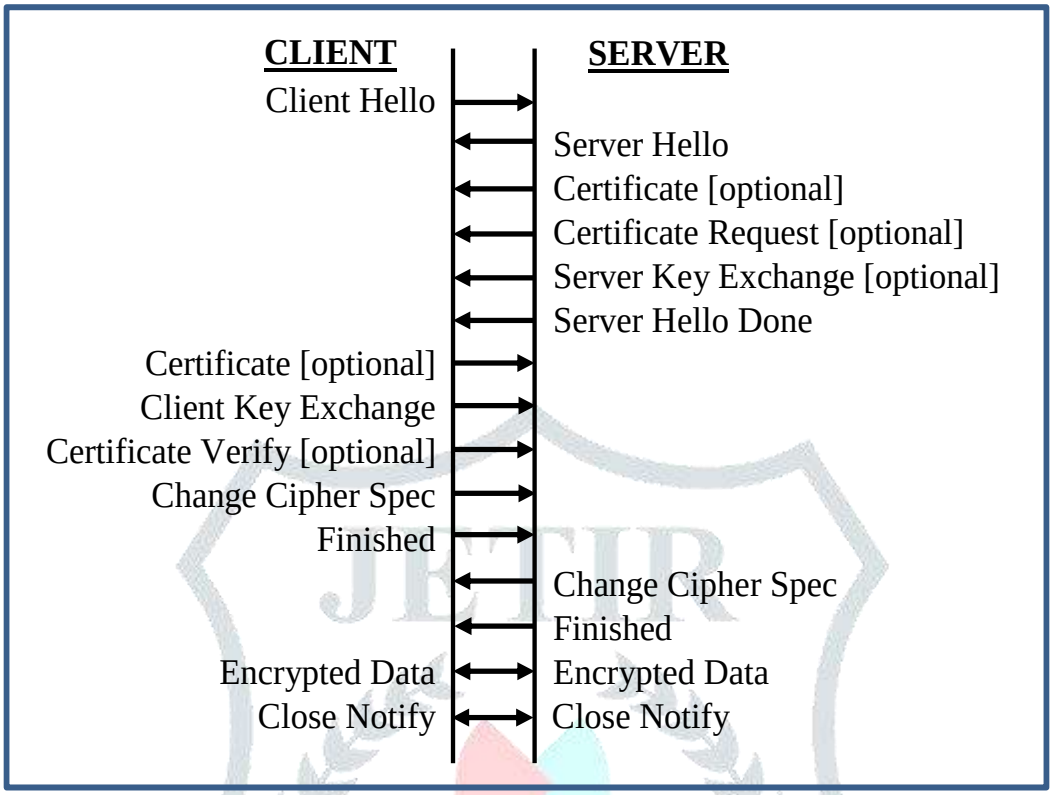

Figure 1 Working of SSL Protocol

III. TLS (TRANSPORT LAYER SECURITY)

To prevent eavesdropping and tampering in client-server applications the TLS protocol is used to communicate across a network. TLS protocol is currently having three versions 1.0, 1.1 and 1.2. TLS protocol also has three sub-protocols namely: handshake, record and alert protocols same as in SSL and the working procedure is approximately similar. The major differences between SSL and TLS protocols are:

- TLS has more alerts.
- TLS requires DSS/DH support.
- Key derivation functions are different.
- MACs are different – SSL uses a modification of an early HMAC while TLS uses HMAC.
- The Finished messages are different.
- To protect against Cipher block chaining (CBC) attacks:
  - Handling of padded errors is changed to use the bad_record_mac alert rather than the decryption_failed alert.
  - The Implicit Initialization Vector (IV) is replaced with an explicit IV
- IANA registries are defined for protocol parameters.
- Premature closes no longer cause a session to be non-resumable.
- The MD5/SHA-1 combination in the
  - Pseudorandom function (PRF) was replaced with cipher-suite-specified PRFs.
  - Digitally-signed element was replaced with a single hash.
- Additional data modes were provided for addition of support for authenticated encryption.
- TLS Extensions definition and AES Cipher Suites were merged in.
- Tighter checking of Encrypted PreMasterSecret version numbers.
- Verify_data length depends on the cipher suite
- How to defence Bleichenbacher/Dlima attack is detailed.

Sheffer, et al. [6] summarise the various known attacks against TLS. The major attacks are:

- Renegotiation attack: An attacker who can hijack an https connection could merge their own requests into the beginning of the conversation the client has with the web server. To fix the vulnerability, a renegotiation indication extension was proposed for TLS.
- Attacks due to implementation errors: Heartbleed bug – It allows attackers to steal private keys from servers. It is caused by a buffer over-read bug in the OpenSSL software. Cloudbleed – allowed unauthorized third parties to read data in the memory of programs running on the servers. It is caused by a single mistyped character in code used to parse HTML created a buffer overflow error on Cloudflare servers.Downgrade attack: It tricks a web server into negotiating connections with previous versions of TLS.
- POODLE attack: It could be avoided by disabling SSL 3.0. However, a variant of POODLE impacts TLS implementations that do not properly enforce padding byte requirements [7].
- Timing attacks on padding: A fix was released as the Encrypt-then-MAC extension to the TLS specification, released as RFC 7366 [8].
- RC4 attacks: Microsoft, Google and Mozilla disabled RC4 cipher suites as default in their browsers [9][10].

- Cross-protocol attacks: It attacks servers supporting contemporary SSL/TLS protocol suites by exploiting their support for the obsolete, insecure, SSLv2 protocol.
- BEAST (Browser Exploit Against SSL/TLS) attack: Microsoft [11] check this attack by restricting the use of TLS to 1.1 or higher version and NSS (Network Security Services) is used by Mozilla Firefox and Google Chrome to implement SSL.
- CRIME and BREACH attacks: It allows an attacker to recover the content of web cookies when data compression is used with TLS and thus hijack the session. CRIME can be defeated by preventing the use of compression and BREACH could be defeated by disabling HTTP compression whenever the referrer header indicates a cross-site request, or when the header is not present [12].
- Truncation attack: It blocks a victim's account logout requests so that the user unknowingly remains logged into a web service.
- Sweet32 attack: It breaks all 64-bit block ciphers used in CBC mode as used in TLS to capture enough traffic to mount a birthday attack [13].
- PAC attack: It exploits weaknesses in the Web Proxy Autodiscovery Protocol (WPAD) to expose the URL that a web user is attempting to reach via a TLS-enabled web link. Disclosure of a URL can violate a user's privacy [14].

However, TLS 1.3 will be available for public in March/April 2018 [15][16][17] patching most of the attacks. The major differences from the earlier versions will be:

- Digital signatures are required even when a previous configuration is used.
- Integrating HKDF and the semi-ephemeral DH proposal.
- Resumption will be replaced with PSK and tickets.
- Support for weak and lesser-used named elliptic curves will be removed.
- Support for MD5 and SHA-224 cryptographic hash functions will be removed.
- Supporting 1-RTT handshakes and initial support for 0-RTT
- The Ed25519 and Ed448 digital signature algorithms are added.
- For many insecure or obsolete features the support will be dropped including Hello message UNIX time, compression, renegotiation, non-AEAD ciphers, custom DHE groups, static RSA and static DH key exchange, point format negotiation, Change Cipher Spec protocol and the length field AD input to AEAD ciphers.
- The x25519 and x448 key exchange protocols are added.
- SSL or RC4 negotiation for backwards compatibility will be prohibited.
- Use of session hash will be integrated.
- The use of record layer version number is deprecated and the number is freeze for improved backwards compatibility.
- The ChaCha20 stream cipher id added with the Poly1305 message authentication code.
- Some security-related algorithm details are moved from an appendix to the specification and transferring Client-Key-Share to an appendix.

IV. SET (SECURE SOCKET LAYER)

The major tasks of SET protocol are to ensure confidentiality of information, integrity of data, authentication of cardholder account and authentication of merchant. There are six participants in the SET system namely; cardholder, merchant, issuer, acquirer, payment gateway and certification authority. Cardholders and merchants both must be registered with CA (certificate authority), before buying or selling on the Internet. Once registration is done, cardholder and merchant can perform transactions. Majorly SET supports following transactions:

1. Purchase request
2. Payment Authorization
3. Payment Capture

Purchase request has four messages: initiate request, initiate response, purchase request and purchase response. Payment authorization transaction has two messages: authorization request and authorization response. Payment capture has two messages: capture request and capture response. The SET system has a nine step process that is illustrated in figure 2.

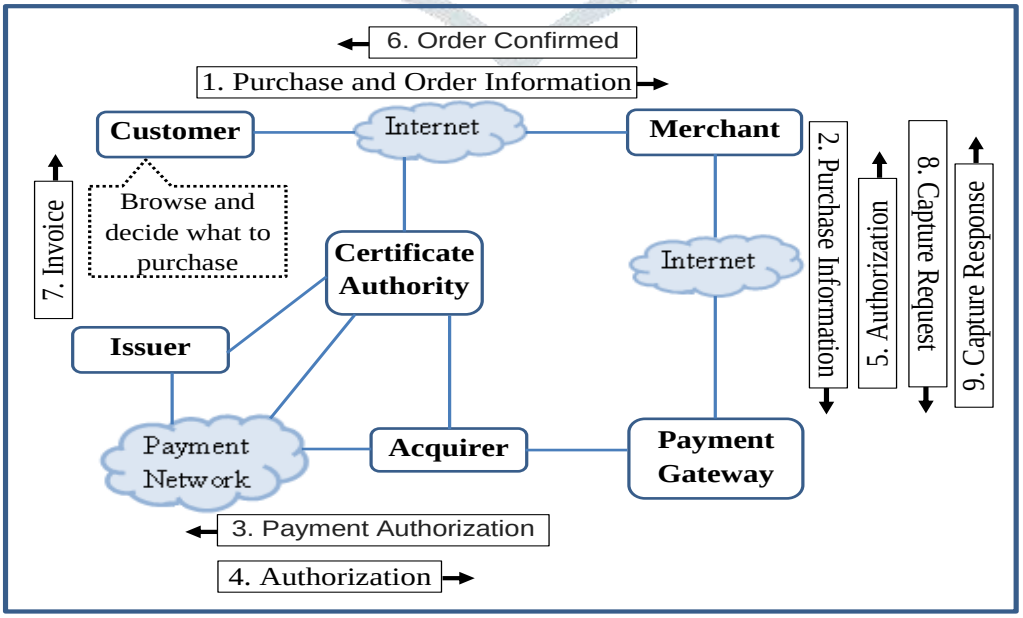

Figure 2 Working of SET Protocol

Purchase and order information have two packets; one for order information for the merchant and the other one is purchase information for the payment gateway. Both the packets contain dual signature. The procedure for calculating dual signature is illustrated in figure 3.

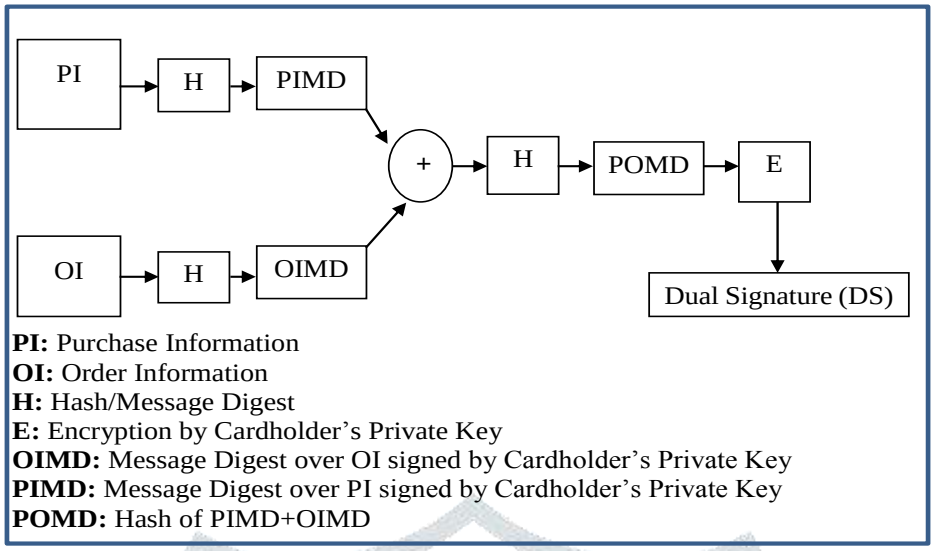

Figure 3 Dual signature

V. 3D-SECURE

3D-Secure protocol ties the financial authorization process with an online authentication i.e. it adds an authentication step for online payments. 3D refers to a three-domain model:

- Acquirer Domain: This domain includes the bank and the merchant to which the money is being paid. It has systems and functions of the acquirer and its customers: merchant plug-in and signature validation server. The Acquirer is responsible for [18]:
  - Defining the procedures to ensure that merchants participating in Internet transactions are operating under a merchant agreement with the Acquirer, and
  - Providing the transaction processing for authenticated transactions.
- Issuer Domain: It includes the bank which issued the card being used and the card holder. It has systems and functions of the card issuing financial institutions and its customers: card holder browser, related card holder software, enrolment server, access control server, and universal cardholder authentication field generation process. The Issuer is responsible for [18]:
  - Managing the enrolment of their cardholders and authenticating cardholders during online purchases.
- Interoperability Domain: It has Systems, functions, and messages that allow the Issuer Domain and Acquirer Domain to interoperate. These components will be globally operated and managed by finance card issuer such as Visa, MasterCard etc. It includes: directory server, certificate authority, authentication history server and attempts processing server.

The protocol uses XML messages sent over SSL/TLS connections with client authentication. EMVCo, a company jointly owned by Visa, MasterCard, American Express, JBC, UnionPay, and Discover, upgraded 3D-Secure. The improved version has features such as [19]:

- Datasets were improved for risk-based authentication.
- Messaging is improved with supplementary information for better decisions on authentication.
- Non-payment user authentication.
- To meet specific regulations and requirements non-standard extensions are provided, including proprietary out-of-band authentication solutions, used by card issuers.
- The performance of end-to-end message processing is improved.
- Unauthenticated payment is prevented, even if a cardholder's card number is stolen or cloned.

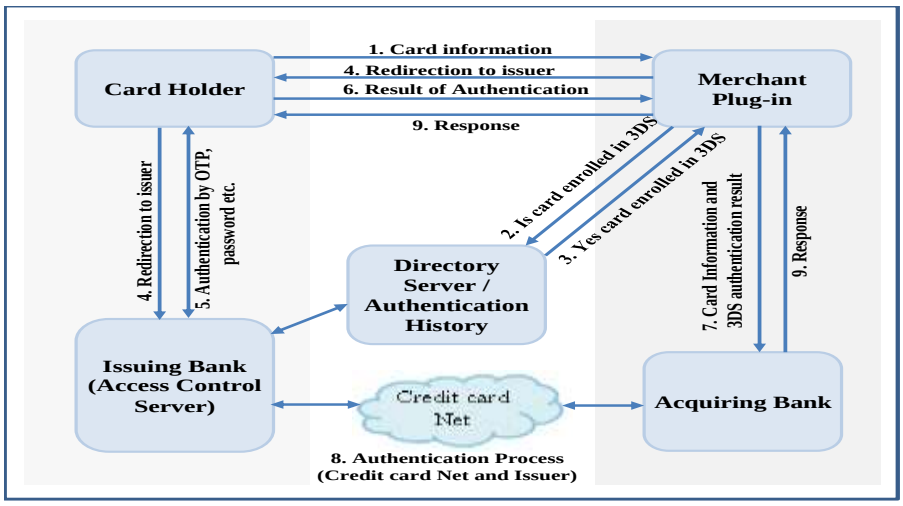

Figure 4 Working of 3D-Secure Protocol

VI. CONCLUSION

Any transaction that takes place over the internet should be secure. Customers will lose faith in e-business if its security is compromised. For the purpose network security protocols were developed for securing private data or financial transactions over the internet. Any website that accepts any type of private information, such as customers' details, then your browser should support TLS. In TLS 1.3 many improvements are made to make it stronger. Any Merchant that accepts online payments, then SET or 3D-Secure is required. Major Credit card issuers support 3D-Secure for online payments and efforts are made to improve these protocols. There are numerous security loopholes which point towards including the end-user within the scope and a need to have uniform standards across banks worldwide for end-user verification/authentication. Strong recommendation is there to make compulsory use of One Time Pad (OTP) tokens. The OTP token would restrict the damage in case of a phishing or key logging attack to that particular transaction. Without these security protocols, you may lose customers and leave money on the table.

REFERENCES

[1] Möller, Bodo; Duong, Thai; Kotowicz, Krzysztof (September 2014). "This POODLE Bites: Exploiting The SSL 3.0 Fallback".

[2] Bright, Peter (October 15, 2014). "SSL broken, again in POODLE attack". Ars Technica.

[3] Brandom, Russell (October 14, 2014). "Google researchers reveal new Poodle bug, putting the web on alert".

[4] "Visa USA tightens security with Arcot". ZDnet.

[5] Murdoch, Steven J., and Ross Anderson. "Verified by Visa and MasterCard securecode: or, how not to design authentication." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2010.

[6] Y. Sheffer, Porticor, R. Holz, "RFC 7457: Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS)". Internet Engineering Task Force (IETF), ISSN: 2070-1721, February 2015. https://www.rfc-editor.org/rfc/pdfrfc/rfc7457.txt.pdf

[7] Langley, Adam (December 8, 2014). "The POODLE bites again". December 8, 2014. https://www.imperialviolet.org/2014/12/08/poodleagain.html

[8] P. Gutmann (September 2014). "Encrypt-then-MAC for Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)". https://tools.ietf.org/html/rfc7366

[9] "Ending support for the RC4 cipher in Microsoft Edge and Internet Explorer 11". Microsoft Edge Team. September 1, 2015.https://blogs.windows.com/msedgedev/2015/09/01/ending-support-for-the-rc4-cipher-in-microsoft-edge-and-internet-explorer-11/

[10] Barnes, Richard (Sep 1, 2015). "Intent to ship: RC4 disabled by default in Firefox 44". https://lists.mozilla.org/pipermail/dev-platform/2015-September/011541.html

[11] "Vulnerability in SSL/TLS Could Allow Information Disclosure (2643584)". Published: January 10, 2012 | Updated: July 17, 2013.https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2012/ms12-006

[12] Ivan Ristic (October 14, 2013). "Defending against the BREACH Attack". Qualys.com. https://blog.qualys.com/ssllabs/2013/08/07/defending-against-the-breach-attack

[13] [Goodin, Dan (August 24, 2016). "HTTPS and OpenVPN face new attack that can decrypt secret cookies".https://web.archive.org/web/20160824181630/http://arstechnica.com/security/2016/08/new-attack-can-pluck-secrets-from-1-of-https-traffic-affects-top-sites/

[14] Goodin, Dan. "New attack bypasses HTTPS protection on Macs, Windows, and Linux".https://web.archive.org/web/20160727160434/http://arstechnica.com/security/2016/07/new-attack-that-cripples-https-crypto-works-on-macs-windows-and-linux/

[15] draft-ietf-tls-tls13-28 – The Transport Layer Security (TLS) Protocol Version 1.3

[16] draft-ietf-tls-tls13-latest Archived 2016-01-04 at the Wayback Machine.

[17] Protocol Action: 'The Transport Layer Security (TLS) Protocol Version 1.3' to Proposed Standard (draft-ietf-tls-tls13-28.txt)

[18] "3-D Secure Introduction" September 26, 2002 http://us.sterlingcardps.com/uploads/userfiles/trk_3dsec_intro_v102(1).pdf?phpMyAdmin=933c4a5b49fat52366f8a

[19] "3D Secure 2.0 Specification by EMVCo". EMVCo. https://www.emvco.com/emv-technologies/3d-secure/