Vendor Verification: Boosting Consumer Confidence in E-Commerce

Thomas C. Stroud

East Carolina University

April 12th, 2015

Abstract

The purpose of this paper is to propose a new method for verifying the identities of vendors in electronic transaction processing as it relates to consumer confidence in e-commerce. Current problems plaguing consumers in the private sector will be discussed with particular attention given to ransomware and similar unwanted programs. This is followed by a discussion of the Secure Electronic Transaction protocol, which provides a framework for vendor verification, and offers one potential solution for verifying the identities of vendors on the internet. The paper wraps up with implications of vendor verification, including its pros and cons, and finally a summary of the information presented.

Consumers are bombarded daily with advertisements and solicitations providing a wide range of goods and services. This endless stream of commercials, billboards, radio advertisements, and other marketing media is almost inescapable. With the growth of e-commerce, and the constant growth in the availability of the internet, companies have the ability to promote their products in more ways and places than ever before. This has made it incredibly difficult for consumers to know which companies to trust, and which products to avoid. In the real world, companies are subject to laws and regulations that help to curb consumer fraud, and although these same laws apply to e-commerce, they are incredibly difficult to enforce.

In 2013, e-commerce accounted for $260.67 billion dollars in sales in the U.S. economy alone, and trends show that this number will continue to climb (Statista, 2015). This continued growth has created an ideal target for criminals hoping to steal a piece of the pie. With real-world commerce, consumers have the means to review the companies and products they intend to spend their money with, but this is not the case online. For nearly every negative review of an electronic product or service, a positive review can be found from an equally reputable source. Additionally, many cyber criminals have no problem impersonating well-known companies, making consumers even more likely to trust the information that they're presented with.

As a result, cyber criminals have developed a whole host of tools in an attempt to defraud unsuspecting consumers. A quick look at the FBI's Internet Crime Complaints website reveals a number of online fraud schemes, ranging from internet auction fraud and illegitimate debt elimination services to credit card fraud and letters from Nigerian princes (IC3, 2015). Many of these schemes are associated with real-world transactions involving wire-transfers and cashiers' checks, and the only defense that consumers have is awareness of these various schemes and how to avoid becoming a victim.

Other schemes are purely electronic, and require little more than an ability to trick the victim into giving up their credit card information and making a purchase. These schemes depend heavily on the average computer user's willingness to believe whatever they see on their computer screen. For the average user, any indication that their machine is misbehaving is cause for panic, and criminals have no problem using this to their advantage.

Consumer Vulnerabilities

Purely electronic fraud schemes present a unique challenge for wary consumers, and the criminals perpetrating these schemes are fully aware of these difficulties. These schemes can take many forms, but three of the most prominent are illegitimate and useless software, cyber extortion or ransomware, and fraudulent tech support scams. These types of scams present major problems to consumers because most consumers are ill-informed about their existence. To compound the problem, criminals can easily update and alter their chosen approach to account for increased consumer awareness and vigilance. This makes combating this kind of electronic fraud nearly impossible.

Useless Applications

One of the more prominent schemes related to electronic transactions deals with the promotion and dissemination of faulty and useless applications. Many of these applications are referred to as potentially unwanted programs, and a few have been classified as pure malware by many reputable antivirus software companies. These applications generally claim to solve a

variety of problems, to include keeping drivers up to date, removing viruses, applying system updates, and speeding up normal PC function. In each case, the application will either perform a needless operation (an operation effectively undertaken by the operating system), or the application will not perform any function at all.

One example is an application called Driver Support. This application claims to monitor the hardware on a system, manage the installed drivers, scan the web for updated driver versions, and install them easily with minimal user interaction. The application is available at a cost of $29.95 per year, as detailed on DriverSupport.com, and has a three and a half star rating on CNET.com. Driver Support is also mentioned as malware in several forums hosted at Malwarebytes.org, Kaspersky.com, and answers.Microsoft.com, to name a few. Another similar application is PC Optimizer Pro, which can be purchased for a one-time payment of $50. PC Optimizer Pro is recognized as malware and removed by most well-known antivirus applications.

Cyber Extortion

Cyber extortion is another common form of electronic fraud that occurs when a hacker or virus blocks access to an information asset until a payment is made. "In the digital age, data has incredible value," and because of this, "It draws the interest of cyber extortionists" (Kostadinov, 2014). In consumer computing, this sort of electronic fraud typically takes the form of ransomware.

One common form of ransomware is known as the FBI virus. This virus will typically seize control of the user's machine, display a warning that child pornography has been found on the machine, activate the built in or attached camera, and demand a ransom to sanitize the

machine and release control. For most casual users, a notice like this will induce panic and a scramble for the credit card, resulting in a charge ranging from $100 to $500. In the end, the user never regains control, and loses their money. In most cases, the virus can be safely removed without damaging the user's data.

Another well-known form of ransomware is what is commonly referred to as a crypto-locker virus. Crypto-locker viruses can be much more costly if an infection occurs, as most data on the infected machine is usually lost. When crypto-locker is executed on a machine, it encrypts the user's files, and displays a message informing the user that they must pay to regain access to their data. The user may choose to pay the ransom, but there is no way to be sure that the data will be decrypted, and in most casual user scenarios, the data is never restored.

Tech Support Fraud

Tech support fraud is another form of electronic scam that is becoming more and more prevalent in consumer computing. A consumer will typically be drawn into this scam in one of two ways, either by receiving a phone call from a bogus support company, or by calling a number after being prompted by a popup warning on a web page. In either case, once the call is established, the consumer is convinced to allow a remote user access to their computer. If access is granted, the remote user will display an array of "problems" and system warnings in an effort to convince the unsuspecting consumer that an urgent fix is needed, and then offers to sign the consumer up for technical support service. Once the consumer pays, the remote user will either "fix" the problem, often by clearing system logs and emptying the recycle bin, or infect the machine with some other form of malware to further victimize the consumer.

Due to increased awareness of this type of internet fraud, cyber criminals have developed a new approach called a refund scam. According to FTC.gov, "If you paid for tech support services, and you later get a call about a refund, don't give out any personal information, like your credit card or bank account number. The call is almost certainly another trick to take your money" (FTC, 2014). Essentially, the same criminals that originally victimized a consumer make a second attempt to defraud the consumer by obtaining credit card information through false pretenses. They offer a refund, but instead end up making withdrawals on the account (FTC, 2014).

Vendor Verification in Electronic Transactions

Consumers face an overwhelming challenge in protecting both their financial and data assets, and because e-commerce is becoming such a substantial component of a successful economy, ensuring consumer confidence in e-commerce has become critical to continued economic success. A critical component of that confidence in e-commerce deals with the consumer being able to trust the vendor that they're dealing with. Many consumers fail to investigate the products and services that they purchase online, and those that do investigate these buying decisions often face conflicting reviews and fraudulent information. It can be nearly impossible for the casual user to find accurate information on a given product, and if they do, they can't be sure who or what to trust.

In light of this issue, the potential exists to provide consumers with an additional line of defense against these types of internet fraud. One possibility would require slight modifications to the secure electronic transaction protocol (SET), a protocol used in card-not-present (CNP)

transactions on the internet using public key infrastructure. The primary purpose of SET is to securely encrypt the details of an electronic transaction so that none of the parties involved may access any consumer data that isn't needed to complete the transaction. The parties involved in an SET transaction include the consumer, the vendor or merchant, the receiving (merchant's) bank, and the card-issuing (consumer's) bank.

An SET transaction begins with the consumer browsing a merchant's site and making a product selection. Once the consumer is ready to complete the purchase, credit card information that is pre-loaded in a digital wallet application or plug-in is selected to use for the purchase. The browser then requests both the merchant's and receiving bank's digital certificates, and checks them for authenticity. Once the check passes, the payment information is encrypted using the receiving bank's public key, and the remaining transaction information is encrypted using the merchant's public key. This ensures that the merchant never has access to the consumer's credit card information. The entire package is then forwarded to the merchant, who then verifies the consumer's digital certificate, decrypts the merchant data relating to the transaction, and then forwards the encrypted payment package to the receiving bank. Upon receipt, the receiving bank decrypts the payment package, and forwards the payment request to the card-issuing bank. If the balance is available, an approval is transmitted to the merchant so that the merchant can fulfill the order (Ramakrishnan, 2000).

In order to implement vendor verification within the SET protocol, a few subtle changes could be made. To begin with, the digital wallet application, which stores the consumer's digital certificate, could be modified to also store the card-issuing bank's digital certificate. As part of the initial encryption process, the merchant's digital certificate could be encrypted using the card-issuing bank's public key, and then included in the encrypted payment package. Once the

receiving bank receives and decrypts the payment package, the encrypted merchant credentials would then be forwarded to the card-issuing bank. After decryption, the card-issuing bank could cross-reference the merchant credentials against a central database of known and reported fraudulent vendors. If the card-issuing bank receives a hit on the merchant credentials, an automated email could be sent to the consumer warning of the merchant's reputation, but allowing the consumer to proceed with the transaction by clicking a verification link and accepting the risk. If the merchant credentials check out, the transaction would proceed as normal.

Implementation of vendor verification in SET will require some initial back-end setup, particularly in establishing a central database for card-issuing banks to query. Current models do exist, however, that can facilitate the database's creation. Operating in a similar manner to the way virus definitions are updated in antivirus applications, the merchant reputation database would be made available to card-issuing banks that choose to provide the service. Initial data obtained from participating banks on reversed charges relating to specific electronic merchants could serve as a starting point for populating the database, and records could be updated based on new reports made to card-issuers regarding electronic fraud. Additionally, vendor verification in SET will create increased network traffic, particularly for the card-issuing bank.

Implications

Vendor verification in SET can provide consumers with the ability to safely participate in e-commerce while providing the assurance that they're spending their money with a trusted merchant. It also has the potential to reduce the incidence of internet fraud by making it more difficult for cyber criminals to achieve a payoff. Reducing the criminal segment in e-commerce

will open the door for legitimate businesses to join the electronic marketplace, boosting the economy and encouraging new merchants to throw their hats into the ring. Additionally, there is the potential for card-issuing banks to achieve increased profits based on premium services relating to vendor verification, or at the least, save precious time and money resulting from the cost of issuing and reversing fraudulent charges.

The downsides to vendor verification are few, but tangible. Consumers in the electronic marketplace don't like to wait, and the added steps in vendor verification could prove burdensome, particularly as it relates to vendor warnings. Some consumers may be aggravated by having to approve a transaction through email before it completes, but most consumers would appreciate the added security. Additionally, SET has not yet been adopted on a global scale, but the consumer benefits of vendor verification could easily push SET into the spotlight. Implementation of SET with vendor verification will take some time and will create some cost, but the ends more than justify the means. Increased profit potential, cost savings, and rising consumer confidence will make it well worth it.

Conclusion

Consumer confidence is crucial to the continued growth and success of e-commerce. The internet has become a jungle full of traps and pitfalls waiting to snag the unsuspecting consumer. Purely electronic transactions present a special concern for wary consumers, as no reliable means exist for consumers to effectively research the overwhelming number of products and services available on the internet. Security measures have been developed to address many concerns in e-

commerce, including transaction security, consumer privacy, and payment integrity, but few if any solutions exist to address consumer confidence in electronic merchants.

Vendor verification can provide consumers the reassurance that their privacy and interests are protected in the electronic marketplace. Secure electronic transaction protocol provides one potential platform for the implementation of vendor verification, but other options are just as viable. Whatever the vehicle may be, vendor verification has the potential to boost consumer confidence, to increase profits for merchants and banks, and to save banks the costs of reversing charges associated with this type of electronic fraud.

Works Cited

"Driver Support." *download.cnet.com*. CNET.com, n.d. Web. 12 April 2015. <http://download.cnet.com/Driver-Support/3000-18513_4-76026725.html>

"Driver Support." *driversupport.com*. Driver Support, n.d. Web. 12 April 2015. <http://www.driversupport.com/>

"Internet Crime Schemes." *ic3.gov*. Internet Crime Complaint Center, FBI, n.d. Web. 12 April 2015. <http://www.ic3.gov/crimeschemes.aspx>

Kostadinov, Dimitar. *Cyber Extortion*. InfoSecInstitute.com, 2014. Web. 12 April 2015. <http://resources.infosecinstitute.com/cyber-extortion/>

Maggie61. (2014, August 18). Removing Driver Support Virus. Message posted to http://forum.kaspersky.com/index.php?s=06658b4c79e07a2b86eeb03756cb247e&showtopic=303400

MartinT. (2014, May 30). Is driversupport.com a useful/honest site? Message posted to http://answers.microsoft.com/en-us/windows/forum/windows_7-security/is-driversupportcom-a-usefulhonest-site/9f7ee417-b095-4447-b0c4-b26f3953598f

Rabbit28. (2014, August 16). Malware 'Driver Support" "My PC Backup" "Sync Folder" "Cut the Rope" (url shortcut). Message posted to https://forums.malwarebytes.org/index.php?/topic/155243-malware-driver-support-my-pc-backup-sync-folder-cut-the-rope-url-shortcut/

Ramakrishnan, Ganesh. "Secure Electronic Transaction (SET) Protocol." ISACA, 2000. Web. 12 April 2015. <http://www.isaca.org/Journal/archives/2000/Volume-6/Pages/Secure-Electronic-Transaction-SET-Protocol.aspx>

"Tech Support Scams." *consumer.ftc.gov*. Federal Trade Commission, 2014. Web. 12 April 2015. <http://www.consumer.ftc.gov/articles/0346-tech-support-scams>

Total and E-commerce Value of U.S. Retail Trade Sales from 2000 to 2013. (2014). [Graph details total yearly economic sales numbers for as well as e-commerce figures for the years 2000-2013]. Statista: The Statistics Portal. Retrieved from http://www.statista.com/statistics/185283/total-and-e-commerce-us-retail-trade-sales-since-2000/