

Risk Management related to Privacy Policies of an Online Store

George Cristian Schin

george.schin@ugal.ro

Dunarea de Jos University of Galati, Romania

This paper seeks to explore the early warning alerts that NORSE system proposes to e-commerce merchants. The real time visibility to cyber-attacks empowers this intelligence tool with high capabilities to detect the threats that companies confront with. The fight against cyber-criminality should be reinforced globally, in the attempt to mitigate the risks and losses determined by attackers. By analysing two case studies, the article proposes a framework which can guide e-commerce merchants to integrate intelligent systems for threat detection. The managerial implications are obvious, equipping the leaders with tools to prevent both financial and knowledge loss.

Keywords: cyber-attack, risk management, privacy, e-commerce

JEL Code: K23, L43

1. Theoretical background: cyber-attacks and e-Commerce

E-commerce security strategies deal with two issues: protecting the integrity of the online business model and its internal systems; accomplishing transaction security between the customer and the e-commerce merchant (Marchany and Tront, 2002).

Security concern is one of the main reasons customers give for not purchasing over Internet. Consumer reluctance to e-commerce is partly due to the fact that the security issues related to shopping on the Internet are considerably high (Udo, 2001).

To the extent that e-commerce is novel to a consumer, disposition to trust will influence trust in the vendor (Harrison McKnight, 2001), but for repetitive buyers the online trust is approached differently. Whether the perceived risks were higher or lower in e-commerce differ from a customer to another, the real threat of third-party intrusion of personal information or financial information is actually less of a threat online than via the more traditional means (Miyazaki and Fernandez, 2001). In examining consumer trust in E-commerce, literature reveals two levels of treating overall online client trust: cognition-based trust (a low level of trust) and affect-based trust (a high level of trust) (Chen and Dhillon, 2003).

Creating procedures to deal with downtime, power outages, cyber attacks, and failure of technology assure competitive advantages for e-commerce merchants (Yasin et al., 2006). No organization connected to the Internet can assume it is safe from a cyber-attack or a criminal act against its business network, including its clients ().

The devastating impact of cyber-attacks to today's e-commerce environment has involved enormous interest in intrusion detection research, both from academic and e-commerce practitioners. In order to guarantee the requirement for continuous availability of products and services bought online, it is also important to consider how the system reacts once the intrusion is detected (Foo et al., 2005).

Hackers' power is constantly increasing and there are more attacks in the last years. Secure web applications for e-commerce stores are only possible when a Secure SDLC (Software Development Life Cycle) is applied (Kaur, 2016).

2. Peculiarities of cyber-attacks in E-Commerce – a case study on NORSE

As E-commerce sales continue to grow in the last decade, the rise in the sophistication of fraud represents a warning alert. Fraudsters have evolved their efforts by increasing automation and creating innovative solutions. With their immense distributed power due to collaborative fraud networks, they pose a significant threat to e-Commerce. Leveraging these technologies, fraudsters are able to instantly change IP locations to avoid being traced and initiate transactions from locations that seem to be legitimate or may even be the cardholder's actual compromised computer – a type of fraud

known as Clean Fraud. Thus, many fraudulent e-Commerce transactions might appear as being legitimate and are not identified by traditional anti-fraud methods.

Validation tools available through the Internet sites are not as effective for mobile devices and most e-commerce merchants have not yet established anti-fraud user-authentication for their customers on mobile devices. Because they involve less personal information, which can be analysed to ensure they correlate with a genuine customer, mobile devices can be an easier channel for fraudsters to be further exploit.

Determining if a transaction is legitimate or not and deciding whether to approve or reject it is a critical milestone in e-Commerce operations. There are envisaged measures that may trap fraudulent transactions, but may also block genuine customers, who will make complaints. Merchants use a variety of automated fraud management techniques, such as fraud-scoring calculators, device fingerprinting, order velocity, multi-merchant data, and analysis of anonymous or free email accounts. In addition, there are still many e-commerce merchants who review their orders in a personalized way. Despite these efforts, they remain challenged in their abilities to protect against fraud attacks, maintain a positive customer experience, and keep costs in line.

Cyber-criminals rapidly change the origin of their attacks and hide their true location and identity using virtualized servers, public cloud infrastructure, and anonymizing proxies. In short time, fraudsters set up connections for online shopping and place orders, and just as quickly bring them down — making it nearly impossible to accurately trace the activity back to its actual source. Detecting and stopping e-commerce fraud therefore requires an effective threat intelligence-based approach, which empowers online merchants to assess the risk level of any transaction in real time.

While existing technologies are in many cases a good pillar for a fraud prevention program, one critical element is missing: live attack intelligence. The most effective way to reduce e-Commerce fraud is to leverage a specialized tool - Norse live attack intelligence. Using a custom integration via a customized API, online merchants obtain a highly accurate live risk assessment of any e-Commerce transaction. Norse's ability to identify and block anonymized IP addresses and other fraud risk factors protects e-commerce merchants from the most advanced online fraud techniques, which quickly evolve.

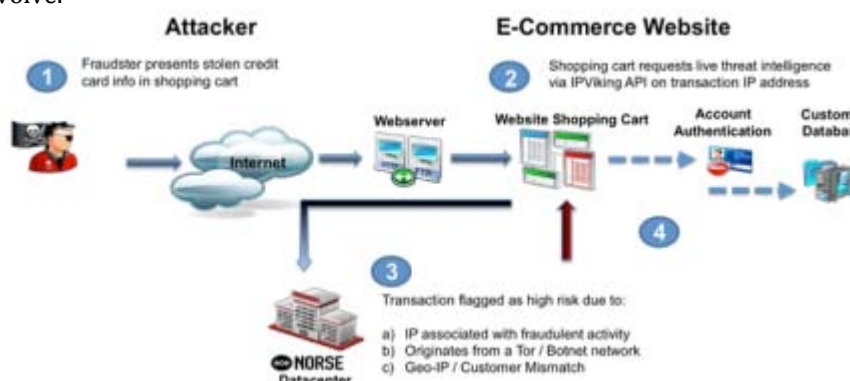


Figure 1 – Interconnections between attackers and e-commerce websites

Source: http://www.norse-corp.com/wp-content/uploads/2015/04/Norse-SB-eCommerce_Fraud1.pdf

For many enterprises, the website is the primary channel for communicating and transacting with prospects, customers, partners, suppliers, etc. Consequently, it is also one of the primary attack vectors used by cyber criminals when targeting an organization for ecommerce fraud as well as security compromise and breach. For companies that engage in ecommerce and store confidential personally identifiable customer information, the website represents an even greater source of potential business risk. Tor is a public peer-to-peer network, but unlike other peer-to-peer networks, its main function is anonymization of network traffic. With the rise in ecommerce over the past decade, fraudsters have evolved their efforts by increasing automation.

With their immense distributed power, attackers pose an increasing threat on the ecommerce landscape. In addition, the increasing use and popularity of Tor and other Internet anonymizing services has created a new security and fraud challenge for businesses and organizations that conduct business and process transactions online. Leveraging these technologies, fraudsters are able to rapidly change locations to avoid being traced and initiate transactions from locations that seem to be legitimate or may even be the cardholder's actual compromised computer. The result is that

many fraudulent ecommerce transactions appear to be legitimate and circumvent traditional anti-fraud methods.

The attack against the political fund raising site used sophisticated, automated scripts that were specifically designed to work with the target site's financial system. The attack was distinguished by the use of credit card account information that looked legitimate enough to spoof some typical forms of fraud detection. It also used 109 unique and undocumented Tor exit nodes to provide attack launch points from which the attackers could not be traced. Finally, the attackers use strategically placed botnet command and control points. While specific points of origin were obfuscated with Tor anonymization, the pattern of attack required a distributed, orchestrated effort.

E-commerce has changed the way people shop from the comfort of their place, in just a few clicks. Customers expect a more personalized experience which brought e-commerce retailers to develop their own apps and give them a highly convenient experience of shopping on the go.

With the proliferation of mobile apps, cyber threats have also increased, primarily because of the vulnerabilities found in these apps due to the inadequate technical controls and also due to the poor security practices of the mobile app owners.

Cybercrimes have posed a serious concern for e-commerce retailers leading to significant business implications and bad PR. E-commerce retailers should take proactive measures to protect their mobile apps from these malicious hackers and safeguard their customers' personal information that they leave while shopping on the app.

Here are two companies that got hacked:

1. **eBay** – The breach at eBay Inc was poised to be one of the biggest data breaches in history, based on the number of accounts compromised. Around 145 million records were accessed by hackers that contained passwords as well as email addresses, birth dates, mailing addresses and other personal information. The hackers got the login credentials of a small number of employees that allowed them to gain access to eBay's corporate network.
2. **Starbucks** – Last year Starbucks app was hacked twice in a gap of few months, where in hackers stole money from several Starbucks customers by gaining access to their credit card information through the app and using the auto-load function. Criminals were using Starbucks accounts to access consumers' linked credit cards. Taking advantage of the Starbucks auto-reload function, they could steal hundreds of dollars in a matter of minutes.

There are many threats to e-commerce security, such as acts of human error or failure, forces of nature, deliberate acts of theft or extortion, etc. Because technology and the internet at that are still such a new phenomenon there are many issues with websites and there is still no way to make your e-commerce site completely secure without certain threats always looming. With technology continually changing and new e-commerce sites entering the market using new and improved technology other e-commerce sites are always looking for a way to improve and become better than the next, creating a competitive advantage. With all this continuous change, this makes it hard to continually keep the current threats away while also staying relevant, keeping employees up to date and trained, keeping cost down, etc.

Below are some of the biggest and most current threats to e-commerce, divided into 2 categories: deliberate acts and human error.

Fraud-- E-commerce websites are vulnerable to fraud from external and internal sources. These incidents include credit card fraud, anything being entered into the system by rogue employees, hackers, trojan horses, etc.

Security-- These issues relate to internal business networks and interface between transactions done by the customer and the network. Hackers can gain access to internal systems via the e-commerce website.

Viruses-- Malicious software and computer viruses are two of the biggest threats. Viruses are normally from external sources and can corrupt files on website if introduced into the internal network. Viruses can completely destroy a computer system and disrupt the operations of the website. Trojan Horse is a malicious software that has the ability to capture the clients information, before any encryption software can take effect. They can also impersonate a customer and pass over bad and malicious codes into the server running the website.

E-commerce hackers are the main threat to the e-commerce environment, however they are responsible for unleashing potential sub-threats such as Man-in-the-Mobile(MITMO), Man-in-the-Browser(MITB) through Trojans(Zeus, Silion, Torpig, and Yaludle), and Man-in-the-Middle(MITM).

Phishing attacks can be used as part of the process with the previously mentioned attacks to steal financial information from consumers. The Man-in-the-Middle attack, also known as session hijacking is used by hackers to intrude into an existing connection to intercept the exchanged data and inject false information. It involves eavesdropping on a connection, intruding into a connection, intercepting messages, and modifying data. If a hacker were to capture the cookie that is used to maintain the session state between a consumer's browser and the genuine website they are logging into, the hacker could present that cookie to the web server and impersonate the connection. The consumer's financial information is now at risk of being compromised. Below is an example of a normal transmission and MITM attack: A normal transmission where the user logs on to an e-commerce website where the user's credentials are verified and user gains access to website.

The following security controls are recommended solutions for e-commerce companies as additional security to thwart any cyber-attacks. The recommended security controls are offered by Trusteer, a private held corporation. The security software offered by Trusteer such as Pinpoint, Mobile and Rapport will assist e-commerce companies in mitigating the discussed threats to ensure a safe online environment. According to Trusteer, Trusteer Cybercrime Prevention Architecture "is the technology foundation of Trusteer's sustainable security solution, enabling organizations to protect their employees and customers against malware and phishing attacks. It prevents credential theft, account takeover, and sensitive information theft. Trusteer Intelligence Center experts extract emerging Crime Logic from threat information gathered by tens of millions of protected endpoints. Trusteer's clientless and endpoint protection layers are constantly updated to secure users against the evolving threat landscape.

3. Conclusions

Today's cybercriminals have automated tools, new attack vectors, and a seemingly never-ending supply of zeroday vulnerabilities to exploit. Despite a wide range of available security and antifraud solutions, the fundamental architectures of traditional signature and policy-based solutions lack the intelligence and proactive adaptability needed to effectively protect against today's advanced attacks, APTs, and zero-day exploits. Given today's elevated threat environment, "businesses can no longer afford to play a game of chance.

They must prepare to play a new game, one that requires advanced levels of skill and strategy to win."5 The time is now for security vendors and IT security professionals to rise to this challenge together with new intelligence-based solutions and deployment strategies. Fortunately, innovative cloud-based solutions like Norse Live attack intelligence are available to enable organizations to quickly and cost effectively integrate live actionable threat intelligence at virtually any point in the IT infrastructure and web-based business processes. Integration via flexible RESTful API, enables organizations to transition to an intelligence-based strategy incrementally, prioritizing resources and efforts based on the organization's specific risk profile and attack surface, thereby raising their overall security posture and lowering business risk.

Norse Live attack intelligence opens up new possibilities for organizations in designing effective cyber security and fraud reduction strategies. With direct integrations to third-party solutions or simple integration via the flexible RESTful API, organizations can now add actionable threat intelligence virtually anywhere within their IT infrastructure and online business processes, enabling more informed and accurate decisions about what to block, what to allow, and what should be routed for additional analysis or verification.

Designed to support the requirements of high volume network infrastructure such as routers, firewalls, and load balancers, and to enable easy integration into critical business processes, websites, customer login forms, and ecommerce systems, the Norse Live attack Intelligence platform is features a highly redundant and scalable global high-speed delivery infrastructure that ensures extremely fast and reliable delivery of data with no latency from calculations. Response time against the Norse delivery platform is measured in microseconds with the ability to support hundreds of thousands of queries per second. Dynamic DNS ensures that customers connect to the geographically closest resource to minimize network latency.

And the end of this interesting and very captivating subject, I realised that the entire world is exposed to a very major threat and besides nuclear attacks, armed attacks, wars and so on, those cyberattacks are silent, imminent, precise and very harmful for every person that use a smartphone, a bank account, personal computer or laptop or everything that have a direct connection to internet.

References

1. Chen, S. C., & Dhillon, G. S. (2003). *Interpreting dimensions of consumer trust in e-commerce*. *Information Technology and Management*, 4(2-3), 303-318.
2. D Harrison McKnight, N. L. C. (2001). *What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology*. *International journal of electronic commerce*, 6(2), 35-59.
3. Foo, B., Wu, Y. S., Mao, Y. C., Bagchi, S., & Spafford, E. (2005, June). *ADEPTS: adaptive intrusion response using attack graphs in an e-commerce environment*. In *2005 International Conference on Dependable Systems and Networks (DSN'05)* (pp. 508-517). IEEE.
4. Kaur, D., & Kaur, P. (2016). *Empirical Analysis of Web Attacks*. *Procedia Computer Science*, 78, 298-306.
5. Marchany, R. C., & Tront, J. G. (2002, January). *E-commerce security issues*. In *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on System Sciences* (pp. 2500-2508). IEEE.
6. Miyazaki, A. D., & Fernandez, A. (2001). *Consumer perceptions of privacy and security risks for online shopping*. *Journal of Consumer affairs*, 35(1), 27-44.
7. Smith, G. S. (2004). *Recognizing and preparing loss estimates from cyber-attacks*. *Information Systems Security*, 12(6), 46-57.
8. Udo, G. J. (2001). *Privacy and security concerns as major barriers for e-commerce: a survey study*. *Information Management & Computer Security*, 9(4), 165-174.
9. Yasin, M. M., Czuchry, A. J., Gonzales, M., & Bayes, P. E. (2006). *E-commerce implementation challenges: small to medium-sized versus large organisations*. *International Journal of Business Information Systems*, 1(3), 256-275.