THE ASPECTS OF PROBING INTO THE ONLINE FRAUD OF 'SALAMI SLICING ATTACK'

Tapasya B., School of Law, Christ University

ABSTRACT

This paper shall focus on the emerging trend of online malware, revolving mainly around the "Salami Slicing Attack", its rampancy in recent times, strategies brought forward to lure factions of consumers who fall prey without any realization. The axis of this study will be to analyze the trends noticed throughout India which have to lead to the strengthening of cyber security walls in the last decade. The out-turn of such an attack is to be so small that it goes unnoticed by each of the victims, but when conglomerated, the combined output is great. There has been made provisions to safeguard the target consumers as well as their faction, by both legal and protective means, but these are not exhaustive. The need for such a malicious online threat may either be to steal a great amount of money or resources by means of minute modifications which tend to remain unseen, causing only negligible losses. This paper shall suggest possible amendments to existing legislation and newer areas to build laws on, to ensure the all-round protection of internet users in this day and age of digitalization and globalization. This paper shall recite certain recent cases of law pertaining to cyberspace mishaps over the recent times.

Introduction

What is the inherent cause and effect of small volume online frauds done on large scale? The rationale of the online fraud technique discussed is the factor of indistinct subtraction of resources, which, either done repeatedly to the same person over a long duration of time; such as the amalgamation of scraps to form a whole salami, or finished at once through multiple persons; such as collecting slices of various meats to form a whole salami, this is basically the 'Salami Analogy'. This recent weed in online frauds has received little to no light through exclusive legal measures, owing to the negligence of the victim.

In an effort to probe into the act of fraud, it is necessary to answer the following questions:

(1) What is a Salami-slicing Attack?

(2) How is it accomplished by the perpetrator?

(3) What are the means to identify and prevent such attacks?

Cybercrimes may involve traditionally unlawful activities like defamation, forgery, fraud, mischief and theft, all of which are punishable by the Indian Penal Code; the power of modernization has given rise to evolved crimes which are subject to the Information Technology Act, 2000. The IT act,2000 categorizes cybercrime by two heads, one where the computer is the target and the other where the computer is the weapon.

What is a Salami-slicing attack?

The phrase 'Salami-slicing' as defined by the Oxford dictionary is the process of gradually reducing the size of something by a series of small incremental steps. It was coined in the 1940's by the Hungarian Communist leader, Mátyás Rákosi[1] in his speech describing his strategy to demonize his opposition by gradual change.

In the digital realm, it translates to the stealthy process of "penny-shaving". The crime is closely associated with net banking and electronic data interchange (EDI).

[1] Lendvai, Paul (2003). *The Hungarians: 1000 Years of Victory in Defeat*. London: C. Hurst and Co, Ltd. p. 430. ISBN 1-85065-6827.

> "*Salami attacks take place when small, almost immaterial, amounts of assets are systematically acquired from many sources. In such minuscule denominations, they frequently exist just below the threshold of perception (and detection, for that matter). The result is an ongoing accumulation of assets in such a manner that the victims, whose assets are vanishing, fail to even notice*".[2] (Hale 2012)

As mentioned earlier, there are essentially two formats of salami-slicing which are recognized as fraudulent activity online. The slicing strategy extends its arms over personal data in the form of information from websites that collect user details, online surveys, deposit sites which collect trash information, witness reports and reviews, borrowed or stolen documents, banking and transaction details, which include the targets' contact details and whereabouts, yielding abundant factual information regarding the individual.

The attack process

There exist several variations in the method of approach in the process of salami-slicing. Rounding vulnerabilities[3], embezzlement, exploiting loopholes in automated manuscripts[4], overcharging on prices[5], underpaying the company, logic bombs, are few to be named from notable cases of the past.

(I) ROUNDING VULNERABILITIES

Rounding means to make a number simpler, keeping it closest to its actual value, the result is easier to use, even though it is less accurate. Rounding vulnerabilities translate to a value, mostly decimal, being rounded-off to an amount minutely larger than it actually is, thereby initiating gains for the receiver.

It is commonly seen over internet banking applications, where the amounts are specified only up to two decimals, the transaction of any sum with a greater number of decimal digits to it

[2] Hale, Michael. 2012, *'Salami attacks'*

[3] Furtuna, Adriana, 2013. *'Practical exploitation of rounding vulnerabilities in internet banking applications'*

[4] Constatin, L, Sep 19, 2009 11:08 GMT. *'E-Trade Salami-Slice Fraudster Sentenced to Jail'. Sep 19, 2018. https://news.softpedia.com/news/E-Trade-Salami-Slice-Fraudster-Sentenced-to-Jail-122150.shtml*

[5] Jan 10, 1993, *'Car- Rental Company's Ex-Owners Charged with Cheating Customers '*, national edn, p 1001024. https://www.nytimes.com/1993/01/10/us/car-rental-company-s-ex-owners-charged-with-cheating- customers.html

[5] Jan 10, 1993, *'Car- Rental Company's Ex-Owners Charged with Cheating Customers '*, national edn, p 1001024. https://www.nytimes.com/1993/01/10/us/car-rental-company-s-ex-owners-charged-with-cheating- customers.html

would be rounded off to the nearest whole number. This could be either in favour of the bank or the consumer.[6] [7]

Illustration:

Current account balance: A

Transfer 1: +€7.4545 = +€7.45 (bank gains +€0.0045)

Transfer 2: +€7.4575 = +€7.46 (bank loses +€0.0025)

Protective strategy:

It is possible for a consumer to protect oneself by making transactions which are rounded-off to a larger amount than that is actually paid forth, transferring foreign currencies between accounts shall also minimize loss by decimals.

The bank can minimize its losses by reducing the number of foreign exchange transactions and levy a fee on them. The bank should also monitor suspicious activity which shall be deemed against the banking policies.

(II) EMBEZZLEMENT

To embezzle means to thieve or misappropriate funds in one's trust or that which belongs to one's employer.[8]

The rapid transition from conventional bookkeeping methods to computerized consumer-tracking systems, banking has evolved and reached the palms of consumers and crooks, making it easier for both to remain in contact with each other. Misappropriation of funds via online transactions is common by fraudsters who direct large amounts of money to their accounts and go untraceable on accomplishing their feat. But, the uncommon case of embezzlement through salami-attacks was first seen in **the Tesco Bank case [9] in 2016**, where amounts ranging from €50 to €800 were transferred from each account in order to avoid being detected by fraud-check alarms.

[6] Furtuna, Adriana, 2013. *'Practical exploitation of rounding vulnerabilities in internet banking applications'*

[7] Taber, John.K. *'A Survey of Computer Crime Studies',* 2 Computer L.J. 275 (1980)

[8] https://en.oxforddictionaries.com/definition/embezzlement

[9]D'souza, Hamlin. Nov 8th, 2016. '*Salami Attack at Tesco Bank'*
https://www.linkedin.com/pulse/tesco-bank-breach-story-hamlin-dsouza

The Information Commissioner's Office scrutinised the situation and fined telecom company which provides the service for the website, a record £400,000 in October for failing to stop the personal data of 157,000 customers being misused.

Illustration:

The embezzler transfers minute denominations of money at a given time from hundreds of accounts into a dummy account, ensuring that the same set of accounts stolen from are not repeated more than two to three times a year. Thereby ensuring discrepancy, since, in most cases, the victim shall not notice the loss nor file a complaint, the reason being the pettiness of value.

Protective strategy:

The bank reacted within two days on seeing suspicious activities backed by customer complaints that their accounts had been emptied over a short span of time, by freezing all transactions via online media and promised to restore the lost amounts back into the victimised customer accounts as soon as they could.

The customers using online banking facilities are to lookout for e-mails and SMS's which instruct customer to validate bank account details or request to transfer money to any other account. The consumer is required to double-check with the bank before undertaking any transactions of that sort.

Banks request customers to update and keep a check on their bank details and account balance regularly, to ensure that no mishap goes unnoticed either by the user or the banker.

The "Zwana" case is a combination of Rounding-off and Embezzlement

The programmer of a mail-order company rounded-off odd cents in the company's sales-commission accounts and placed them as the last record amongst commission files under the dummy account name of "Zwana", (accounts were processed alphabetically). The excess sub-commission has been collected for three years, until the company decided to honour the holders of the first and last accounts, thereby unraveling the crime[10].

(III) EXPLOITATION OF LOOPHOLES

[10] Taber, John.K,*' A Survey of Computer Crime Studies'*, 2 Computer L.J. 275 (1980)

The efficiency and effectiveness of computerized actions owe its efficiency to coding and programming operations. Any code developed by man or machine is bound to have an error, which in turn gives rise to loopholes. In most cases, the erroneous codes are a part of exhaustive programs, which go unidentified by code-reviewers.

In the point of view of the perpetrator, the existing error is meant to be exploited for personal benefit; and the company entertaining such errors is bound to pay for it; finding ground in the fact that several laws do not punish exploitation of loopholes.

(II) The "Plumas Lake Man" case [11]renders cognisance to this attack strategy.

In 2007, Michael Largent wrote a supplementary computer program which allowed him to defraud Charles Schwab & Co., Google and E-trade by opening and attempting to open over 58,000 brokerage accounts using false identities, in pursuit of stealing the micro-deposits of $0.01 to $2.00 which were deposited to consumer account in order to check operative functionality of the course of transaction through the website. The perpetrator gained a large sum over a period of one year, but his cover was undone in mid-2008 and imprisoned for a period of 15 months with $200,073.44 fine and a three-year restriction from using any computing devices.

Illustration:

Besides the online attack for pilferage of resources and information, salami attack strategies have also been used to promote sales.

A jury in Fort Lauderdale claimed that the executives of a rental-car company revised a computerized billing program to add five gallons to the actual gas tank capacity of their vehicles. Over three years, 47,000 customers who returned a car without topping it off ended up paying an extra $2 to $15 for gasoline.[12]

The artifice employed in this attack is subtle **over-charging** for the commodities provided. The consumer shall fall prey for the same, simply for the reason that he is tricked to do so

[11] 08-236 - USA V. LARGENT

[12] Jan 10, 1993, *'Car- Rental Company's Ex-Owners Charged with Cheating Customers ',* national edn, p 1001024. https://www.nytimes.com/1993/01/10/us/car-rental-company-s-ex-owners-charged-with-cheating-customers.html

by the false advertising.

Protective strategy:

The consumer is required to employ individualistic judgement while entertaining any transaction and purchase.

All interactions must remain between parties to the transaction, not entertaining any middlemen.

Even the slightest of discrepancies noticed by the consumer or the company must be brought to the notice of appropriate authority; since the loss for one may be negligible, but the collective loss is detrimental to the entire cyber ecosystem.

The law should streamline the sales ethics that are to be followed by companies and salesmen.

A body designated to fix prices of goods and services is recommended to monitor pricing by evaluation of all products that circulate on sales.

(IV) SIPHONING OF RESOURCES

This exercise of unlawfully liquidating money or information over a period of time from consumer SIM cards by repeatedly calling them from untraceable devices, automated to make blank calls is an emerging trend in the slicing field.

Illustration:

An individual was charged nearly Rs.180.00 out of his phone billing, after receiving calls from an unknown number. Even though the incoming remained unattended, the sufferer was charged Rs.60.00 for each of the three calls made to him. The victim, in an attempt to return these calls, found that they could not be delivered to the very same contact number.

A complaint was lodged with the Cyber Crime Cell, but the number still remains untraced. It is believed that the privacy policies of mobile SIM companies prove as a hurdle in tracking the perpetrator and that Phishers who professionally indulge in penny-shaving from multiple individuals shall be working with several numbers.[13]

[13] Chavan, Vijay. Aug 19th. 2013. *'Salami attacks are latest phishing hack'* https://punemirror.indiatimes.com/pune/cover-story//articleshow/31278235.cms

Protective strategy:

Consumers need to refrain from answering calls from unknown numbers, especially from those which seem atypical.

It is best advised to block the number or disconnect such calls immediately, to prevent loss with each consecutive phone call.

The privacy policies governing the service provider should ensure that the consumer number remains protected at all times from anti-social elements.

SIM card companies should have streamlined policies, permitting access to judicial and defence bodies to probe into civilian complaints.

(V) UNDERPAYING THE COMPANY

As the title suggests, it is a strategy undertaken by an employee of the company to profit more than the company could through a series of transactions. In this attack, the consumer is not the victim; it is the company which is the sufferer.

Illustration:

In 1997, the perpetrator reprogrammed the computerised cash registry at the *Taco Bell* he worked so that a taco costing $2.99 was only charged at 1 cent on the food chain's internal computer. The customer pays full price, the registry receives its allotted balance and the perpetrator got to keep the difference.[14]

This cycle of long con took years for the mother company to notice since it was an enormous food chain and the profits from any one joint among hundreds would be negligible in comparison to the total revenue.

Protective strategy:

All institutions which are branching out are at risk of being underpaid. Such companies require conducting regular audits at all levels to ensure that no amount of profit is siphoned by any of the middlemen before it reaches the company accounts.

[14] Neumann, Peter.G. '*RISKS*', 18, 76.

Prevention of the Attack

The most effective way to identify a salami-attack is checking each line of the code. This exhaustive process is called **Glass-box testing**[15]since it results in the utmost transparency of the coding. The aim of glass-box testing is to find errors and rectify the internal structures and working of any code or its resulting application. The process involves the programmer to design test cases, which include a pre-designed output, and the codes are run through it.

This exhaustive method is test design can unravel errors, bugs and other problems which are potential loopholes. But it may also miss correction of certain 'unimplemented parts' of the specification or fail to accomplish incomplete codes.

-*"Cybersecurity is a shared responsibility, and it boils down to this: in cybersecurity, the more systems we secure, the more secure we all are."* (Jeh Johnson)

The institutions, banks and companies which are susceptible to attacks are required to **update their security systems** and strengthen their firewalls regularly, to ward off any attacks. The basal idea of any unauthorised users to any account or system is to either gain the existing resources or to employ them for anti-social purposes. Applying proper digital security shall ensure that the user shall be notified in case of all types of suspicious activities in the system. There exist numerous variations of online security advice, i.e., updating of anti-virus software and anti-spyware software, password protection guidance, constant application of the latest updates and patches which are evolved to secure the system from the newest of threats, and a firewall.

Coders are required to **minimise errors** in programs to prevent attackers from taking advantage of loopholes in the system. Erroneous codes are those that provide a welcome gate for hackers and programmers who can find them at ease. By employing techniques like Black- box (behavioural), White-box (internal), Gray-box (debugging) testing, it is possible to eradicate the errors to a great extent; as a result of which, both the user and the service provider are protected from any losses.

The consumer and company should have a cordial relationship, such that both are willing to notify each other on any deduction or addition of resources or theft of personal data,

[15]'ET Workshop v.120- *Management and techniques*'

irrespective of the quantity and quality.

This professional closure shall ensure the safety of both bodies and prevent any further loss. In addition to that, the cyberspace would be bettered and safer to access, without the fear of being injured and left unnoticed.

Conclusion

The cynosure of this paper boils down to the following propositions with regard to protection from and prevention of salami-slicing attack throughout all computed operations:

The programming operations carried out by all companies which work by online means should have the concerned codes regularly audited and updated by an administrative authority, void of loopholes and bugs of any kind.

The tribunal for consumer protection should assess and fix appropriate prices for goods sold multiple times online, in order to prevent overpricing.

There have been numerous attempts to put an end to phishing, but with the growth of networking, the tactics employed in crime have evolved as well, giving rise to Salami-slicing, the least known crime. This paper is an attempt to shine light on the topic and provide knowledge of the same.