Winking Router: A Side Channel Attack Survey

Rohit Aich[1], Prabuddha Kumar[2] and Divyansh Upreti[3]

***Abstract*— Side channel attacks provide an effective means for gauging usage patterns over a network. These can reveal information like the websites accessed over a network, time when machines are active etc. Our project aims to address the feasibility of a side channel attack by observing the router blinking pattern to estimate the website being accessed. This is a potential threat because modern day smartphones have high frame-rate cameras that can be used to observe the blink pattern of a router. Through the course of the project, we will try and model the signature pattern of each website and use this model to predict the website being accessed.**

I. RELATED WORK AND STUDIES : A LITERATURE SURVEY

There has been a lot of related work to analyze the threat side channel attacks pose for various devices in a network. Below, we have tried to see how a study of network packet traffic would be potentially able to predict the web-activity of a user.

Xun Gong et al. [1] analyze the web traffic. They have shown that traffic patterns leaked through side channels can be used to gain sensitive information. Attackers can find out which website, or webpage a user is accessing simply by monitoring the packet size distribution. The attacker sends frequent probes and measures the sizes, timings and counts of packets arriving. If the training and test data collected is from the same location, large fraction of sites can be accurately detected. They study on how traffic analysis can be a serious threat to Internet privacy as it can be carried out remotely, without access to the analyzed traffic, thus greatly increasing the scope of attack. There was some accuracy loss due to differences in test and training environments but overall It was found that despite working with noisier information source than previous related works, this website detection attack nevertheless showed that remote traffic analysis is a serious threat to Internet privacy. The study done by Kadloor et al. [2] shows that a low-rate sequence of probes sent to a DSL router can give out essential information about the traffic timing and volume information, if only the router is connected to a public domain, like the internet. The low rate of probes would not cause a significant delay in the router response, and hence the user would also be oblivious of such nefarious attempts. The attackers would be easily able to measure the round trip times of the packets they sent through the router, and based on the scheduling algorithm, FCFS or round-robin, they could almost accurately predict the user-activity by 90%. Earlier, it was assumed that in these attacks, the attacker should require access to the victim's traffic, i.e., it should be able to access the victim's router. However, new research proves that no such linkage is necessary, and indeed any one who could send messages to the victim's router could pull this off by studying the network packets. Coull et al. [3], examine the extent of privacy of data in encrypted messaging services by examining Apple iMessage, which is an end to end encrypted service. They find out that it is possible to extract some information from the packets such as the language of the message, the size of the content, some operating system information among others. They also suggest a countermeasure by inserting random padding to the packets. This is relevant to our project in that they provide remedies to mitigate snooping by side channel attacks.

Several studies have also been done to use side-channel attacks to create specific fingerprints of different websites, based on the traffic of network packets or round-trip-timing of network packets (RTT). Research conducted by Ling et al [4] shows that it is possible to predict the websites the victim has visited by measuring the round-trip-times (RTT) from the victims machine to destination websites. They derive a model by fingerprinting the websites based on the RTT, and then conduct a side-channel attack where they try to predict the websites visited by users based on the RTT-s recorded, with a specific probability factor. They also give out possible solutions to counteract the attack, like using the k-means clustering and the K-anonymity algorithm to achieve similar RTT-s for different websites, so that they cannot be distinguished. Hermann et al. [5] use a Multinomial Nave Bayes Classifier to detect websites with an accuracy of 97%. They use website fingerprinting to learn the packet distribution of a website, and use the fingerprint of websites for classification. They mention that this technique is extremely effective against single hop techniques under closed world assumptions. They do, however concede that if the closed world assumptions are left out, the accuracy is so far not great, but getting better. Conducting a bit different study on profiling attacks, Liberatore, et al. [6] examine the effectiveness of network analysis techniques for identifying encrypted HTTP streams. They use classification algorithms to identify encrypted traffic on the basis of similarities of features when compared to known profiles. They show that these techniques can work at significant scale. The paper also

*This work is an ongoing research project at the Computer Science Department of Stony Brook University

[1]R. Aich is a PhD Student, Department of Computer Science, Stony Brook University, NY 11790, USA. raich at cs.stonybrook.edu

[2]P. Kumar is an MS Student, Department of Computer Science, Stony Brook University, NY 11790, USA. prabkumar at cs.stonybrook.edu

[3]D. Upreti is an MS Student, Department of Computer Science, Stony Brook University, NY 11790, USA. dupreti at cs.stonybrook.edu

suggests countermeasures to prevent unwarranted snooping. The key highlight is that the authors claim that traces of websites from packets can be identified 66-90% of times, under a set of assumptions.

In specific cases, side channel analyses on network packet lengths have also revealed information about encrypted Voice-over-Internet (VoIP) calls. Wright et al [7] shows that even the encrypted VoIP calls are not safe against side-channel attacks with network packets. As the VoIP calls are encrypted with variable bit rate (VBR) and length-preserving encryption to save bandwidth, the researchers have been able to analyze the length and demographics of the output VoIP packets to identify the phrases spoken within the call with an accuracy of 50%. In certain cases, they have been even able to achieve an accuracy of 90%. They constitute a model by considering the constitution of phonemes, and predict how the length of network packets varied over different phrases. They later fit this model to the output packets to predict the encrypted phrases. This shows that the side-channel attacks involving network packets are so efficient that the encryption efforts to secure the data have become useless.

In general, side-channel attacks to determine users online activity is a novel topic for the researchers. The study done by Qing Yang et al [8] shows that public USB charging stations pose a significant privacy risk to smartphone users even when no data communication is possible between the station and the users mobile device. Their results show that the attack is highly successful and they were able to achieve over 90% webpage identification accuracy. This work is studies side channel attack on smartphones under phone constraints demonstrates that websites can be correctly identified within a short timespan of two to six seconds. The researchers use machine learning algorithms to identify the web-pages the user visited, and exploits smartphones factors such as user interaction with touchscreen, WiFi and LTE connectivity, training and testing device mismatch, type of connection (HTTP or HTTPS) and relative location of the host serving the webpages to the smartphone. They present a side channel attack allowing a charging station to identify which web-pages are loaded while smartphone is charging. They collect power traces of Alexa top 50 websites on multiple smartphones under several conditions, including battery charger level, browser cache enabled/disabled, taps on the screen, WiFi/LTE, TLS encryption enabled/disabled and time elapsed between collection of training and testing data, website location and were able to achieve identification accuracies as high as 98.8 % with 2 second traces. Attacks using other websites to infer the victims online activity from browser caches and history have also been common. Edward W. Felten et al [9] studied the attacks that allow a malicious web site to determine whether or not the user has recently visited some other, unrelated web page. This malicious page can determine this by measuring the time the users browser requires to perform certain operations. As browsers perform various forms of caching, the time required for operations depends on users browsing history. By measuring the time required to access an element, malicious program can tell if the element is in a nearby cache and thus learn that element has been accessed recently. For example, an insurance-company site could determine whether the user has recently visited Web sites relating to a particular medical condition. This is a dangerous side attack to conceal users browsing history and figure out his general browsing patterns.

REFERENCES

[1] X. Gong, N. Borisov, N. Kiyavash, N. Schear, Website Detection Using Remote Traffic Analysis. "http://publish.illinois.edu/science-of-security-lablet/files/2017/03/Website-Detection-Using-Remote-Traffic-Analysis.pdf"

[2] S. Kadloor, X. Gong, N. Kiyavash, T. Tezcan, N. Borisov, Low-Cost Side Channel Remote Traffic Analysis Attack in Packet Networks. "https://ieeexplore.ieee.org/document/5501972"

[3] S. E. Coull, K. P. Dyer, Traffic Analysis of Encrypted Messaging Services: Apple iMessage and Beyond.

[4] Z. Ling, J. Luo, Y. Zhang, M. Yang, X. Fu, W. Yu, A Novel Network Delay Based Side-Channel Attack: Modeling and Defense. "https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6195628"

[5] Dominik Herrmann, Rolf Wendolsky, Hannes Federrath, Website Fingerprinting: Attacking Popular Privacy Enhancing Technologies with the Multinomial Nave-Bayes Classifier.

[6] M. Liberatore, B. N. Levine, Inferring the source of encrypted HTTP connections. "https://dl.acm.org/citation.cfm?id=1180437"

[7] C. V. Wright, L. Ballard, S. E. Coull, F. Monrose, G. M. Masson, Spot me if you can: Uncovering spoken phrases in encrypted VoIP conversations. "http://cs.jhu.edu/ cwright/oakland08.pdf"

[8] Q. Yang, P. Gasti, G. Zhou, A. Farajidavar, K. S. Balagani, On Inferring Browsing Activity on Smartphones via USB Power Analysis Side-Channel. "https://ieeexplore.ieee.org/document/7782756"

[9] ,E. W. Felten, M. A. Schneider, Timing Attacks on Web Privacy.