Poster: Understanding Free-riding Attacks in Internet Zero-rating Services

Zhiheng Liu, Zhen Zhang, Shihao Jing, Zhaohan Xi and Yinzhi Cao
Lehigh University
27 Memorial Dr W, Bethlehem, PA, USA
[zhl416][zhza16][shj316][zhx516][Yinzhi.cao]@lehigh.edu

I. INTRODUCTION

Network service provided by Internet service providers (ISPs) is often charged, e.g., via the amount of traffic in the cellular network like T-Mobile or via a one-time fee in aircraft cabin WiFi. In addition to the charged service, many ISPs also provide so-called zero-rating services for contracted or affiliated content providers (CPs). For example, T-Mobile offers a so-called BingeOn program with over 100 CPs, such as Youtube. T-Mobile users can access services provided by these CPs, e.g., watching Youtube videos, free of charge. Passengers of United Airlines can freely access United and its partners' website. China Mobile partners with Alibaba, a Chinese e-commerce company, and allows its users to purchase items via Alibaba's mobile app without data charge.

Although zero-rating services provide convenience for both users and CPs, some users with malicious intent can launch so-called free-riding attacks to bypass the pre-set zero-rating policies and visit normal websites beyond zero-rating service for free. Such new free-riding attacks are first documented by Kakhki et al. [1]: They show that an attacker can masquerade a non-zero-rating server to be BingeOn enabled, i.e., as zero-rated. Unlike traditional free-riding attacks [2] that exploit the bugs of the ISP via uncharged protocols such as network domain service (DNS) and TCP retransmission, these new free-riding attacks are even more challenging and hard to defend as three parties—the user, the ISP, and the CP—are involved. More importantly, these free-riding attacks are severe and cost ISPs much income: China Mobile loses half million of US dollars per month due to such free-riding attacks, such fraud traffic can reach 100TB volume every month with in the China Mobile Network.

To better understand such free-riding attacks, we conduct a survey study of the aforementioned free-riding attacks. Particularly, we show that such attacks not only exist for un-encrypted traffic but also apply to encrypted traffic, e.g., these transmitted via HTTPS protocols. A report from Sandvine [3] indicates that over 70% of global Internet traffic was encrypted in 2016 which enlarge the severity of the zero-rating vulnerability, because there is no perfect solution to identify packet and authenticate service in encrypted traffic. Furthermore, apart from the CP authentication vulnerability, we show that the communication integrity among the three parties can also be compromised. Even if the ISP authenticates the CP, i.e., fixing the vulnerability documented by Kakhki et al. [1], free-riding attacks still exist. We then perform our versions of the free-riding attacks on a variety of real-world ISPs—such as T-Mobile, China Mobile, and United Cabin WiFi—which span from the mobile cellular network provider to airplane cabin WiFi and from the U.S. to China. Our results show that all the surveyed ISPs are vulnerable to the free-riding attacks: Specifically, a malicious user can bypass the zero-rating policy and access to any websites for free.

Apart from these real-world ISPs adopting industry-level enforcements, academic researchers have also proposed solutions to enforce zero-rating policies. In particular, Y. Yiakoumis et al. proposed network cookies [4] in which an authentication token (called network cookie) serves as a ticket for the ISP to zero-rate corresponding traffic. However, this academic solution is also vulnerable to free-riding attacks. Notably, an attacker can bind a network cookie designated for zero-rating traffic to normal traffic and bypass the zero-rating policy.

Faced with the security problems as mentioned above in both industrial and academic solutions, we introduce the analyzers of current zero-rating threat and vulnerability. In addition, we present several free-riding attacks to real world mobile and WiFi operators.

II. Methodology of Free-riding Attack

Our zero-rating threat model for both unencrypted traffic (e.g., HTTP protocol) and encrypted traffic (e.g., HTTPs protocol) is discussed below. We successfully launch free-riding attacks on real-work operators, such as T-Mobile and China Mobile. This threat model also covers low bandwidth Wifi network operator, such as United airline cabin network. We introduce the methodology of the threat model based on the difference of the carrying network: unencrypted traffic network and encrypted traffic network.

For unencrypted traffic network, Because the traffic is in plain text, the ISP can use deep packet inspection (DPI) to examine the entire packet, determine the destination, and zero-rate corresponding traffic. Although undocumented, the zero-rating policy adopted by major ISPs, as shown by our experiments, is to inspect the 'Host' field of the HTTP header in the request from the user to the CP. Note that the reason for such inspection is that the 'Host' field is relatively stable comparing with others such as the IP address.

Because the ISP only inspects the traffic but does not contact the CP, an attacker can launch free-riding attacks to either subvert the authenticity of the CP or compromise the integrity of the packet between the user and the CP.

First, when the attacker, as a malicious user, connects to a non-zero-rating CP, the attacker can alter the 'Host' field in the HTTP request so that the ISP will mistakenly consider the connection as zero-rating traffic. That is, the attacker subverts the authenticity of the CP via mimicking zero-rating behavior. Second, when a packet, e.g., HTTP response, comes back from the CP to the user, a man-in-the-middle attacker between the CP and the ISP can modify the packet and insert unauthorized, third-party contents, thus violating the integrity of the connection.

For encrypted traffic network, the traffic between the user and the CP is encrypted, e.g., via the TLS/SSL protocol, meaning that the ISP cannot directly inspect the contents, e.g., the 'Host' field, as what it does for unencrypted one. Instead, the ISP inspects the TLS client hello message, which is unencrypted, and determine the destination of the connection. Particularly the ISP extracts the destination host name from the Server Name Indication (SNI) in Server Name Extension segment of the client hello message and uses it as the determining factor of the zero-rating policy.

Interestingly, both problems—i.e., CP authenticity and packet integrity—for unencrypted traffic still exist regardless of the fact that the communication is encrypted. First, the attacker can still masquerade a zero-rating CP by modifying the SNI field in TLS/SSL connection to be the host name of the zero-rating CP. Second, because the user is the attacker who has the private key and session key of the TLS connection, the attacker can setup a man-in-the-middle proxy that decrypts the traffic, inserts unauthorized, third-party contents, and encrypts the traffic again.

III. Real world Experiments

In this section, we describe how to launch the free-riding attacks against real-world ISPs. We deploy a test bed for launching the attack and analyzing traffic. This test bed contains client (e.g., zero-rating participated mobile phone or computer), a remote server (e.g., cloud server for redirecting traffic) and two man-in-the-middle proxies where a local proxy at client-side in between the application and the ISP to modify the client traffic and masquerade a real CP, and an external proxy in between the ISP and the CP to forward the traffic to the real CP and compromise the packet integrity from the real CP. Consider a normal connection: a client application, e.g., a browser or a mobile APP, connects to a CP via an ISP. The man-in-the-middle proxies interact with the connection and modify the packets with in the traffic.

Our ISP targets can be classified into two major categories: mobile network providers and airline WiFi network providers. Particularly, we include two mobile and one airline WiFI network ISPs and the overall results are shown in Table I. We have test Mobile network operators such as T-Mobile and Chian Mobile and WiFi network operator such as United airline cabin WiFi. All the tested ISPs are vulnerable to the free-riding attacks. Because of the page limitation, In this abstract, we use T-Mobile as an example to demonstrate the attack. T-Mobile provides a BingeOn program so that a user can visit many content providers, such as HBOgo.com and history.com, for free. We set up the environment in using our test bed. Both the application and the local proxy is located in a computer tethered to a mobile phone with the T-Mobile SIM card. The external proxy is a server located by Amazon web service. The amount of traffic is measured by the T-Mobile self-service code, which provides two values: one for the total amount of data and the other for charged amount of data.

TABLE I
Summary of the Attacks on Real-world ISPs

	Mobile Network		WiFi Network
	T-Mobile	China Mobile	United Airline
Unencrypted Traffic	✓	✓	✓
Encrypted Traffic	✓	✓	✗

The results show that the BingeOn program is vulnerable to free-riding attacks, i.e., the application at the client side can visit both encrypted and unencrypted version of an arbitrary website outside of the BingeOn program free of charge. Specifically, we have two conclusions. First, the local proxy can masquerade any unencrypted traffic as these from a website with unencrypted version, e.g., HBOgo.com, by modifying the "Host" field, and any encrypted traffic as these from a website with encrypted version, e.g., Youtube.com, by modifying the SNI field of the TLS handshake. Second, the external proxy can modify and inject arbitrary data into the packet coming from a zero-rating CP.

We also discover the academic approaches such as network cookie are vulnerable to free-riding attacks. We deploy the network cookie environment (e.g., cookie server, middlebox and client) based on the code provided by the author. We create a malicious client to get the cookie from the cookie server during the DNS request visiting a CP's server. This malicious client can override the networking and append it to any outgoing traffic. In this case, the ISP middlebox can not differentiate the zero-ride packet and free-riding packet. We also create a formal method of verification to prove the vulnerability of network cookie.

IV. Discussions

We discuss possible ethics concerns in this section. During all the experiments, we will pay corresponding ISPs for the amount of data that we downloaded for free. Specifically, for T-Mobile and China Mobile, we purchase corresponding data volume, and for United WiFi, we purchase a WiFi pass on the flight in which we perform the test.

V. CONCLUSIONS

This poster focuses on an analysis of the vulnerability of the mobile zero-rating network and introduces the demonstration of free-riding attack. In addition, we illustrate a survey of free-riding attack experiments on several real-world ISP via both unencrypted and encrypted traffic.

References

[1] A.M Kakhki, F. Li, D. Choffnes, E. Katz-Bassett, A. Mislove, BingeOn Under the Microscope: Understanding T-Mobiles Zero-Rating Implementation, workshop on QoE-based Analysis and Management of Data Communication Networks, p.43-48, August 22-26, 2016, Florianopolis, Brazil

[2] Y. Go, J. Won, D. Kune, E. Jeong, Y. Kim, K. Park, Gaining Control of Cellular Traffic Accounting by Spurious TCP Retransmission, INET NDSS, San Diego, CA, USA, Feb. 2014.

[3] Sandvine.co, Report: Encrypted Internet Traffic: A Global Internet Phenomena Spotlight, 2016.

[4] Y. Yiakoumis, S. Katti, and N. McKeown. Neutral Net Neutrality. In: Proceedings of the 2016 Conference on ACM SIGCOMM 2016 Conference. SIGCOMM 2016. Florianopolis, Brazil