Off-path Man-in-the-Middle Attack on Tor Hidden Services

Amirali Sanatinia, Guevara Noubir
Northeastern University
{amirali, noubir}@ccs.neu.edu

Abstract—**In the last decade, Tor proved to be a very successful and widely popular system to protect users' anonymity. However, Tor remains a practical system with a variety of limitations, some of which were indeed exploited in the recent past. Previous work showed the existence of malicious participating Tor relays. In this work, we show that an adversary who compromises the Hidden Service private key can mount a man-in-the-middle attack on hidden services. One characteristic of this attack is that the adversary does not need to be in the communication path between the client and the server. We demonstrate a proof-of-concept (POC) for this attack. Furthermore, we provide a tool that can be used to detect such attempts. We also discuss possible detection and mitigation mechanism and the implication of the certificate systems for hidden services.**

I. Introduction

Over the last decade, Tor emerged as a popular tool and infrastructure that protects users' anonymity and defends against tracking and censorship. It is used today by millions of ordinary users to protect their privacy against corporations and governmental agencies, but also by activists, journalists, businesses, law enforcements and military [1].

The success and popularity of Tor makes it a prime target for adversaries as indicated by recent revelations. Despite its careful design, that significantly improved users privacy against typical adversaries, Tor remains a practical system with a variety of limitations and design vulnerabilities, some of which were indeed exploited in the past [2], [3]. Due to the perceived security that Tor provides, its popularity, and potential implication on its users, it is important that the research community continues analyzing and strengthening its security.

Recent incidents revealed that the Tor network is continuously being attacked by a variety of organizations from universities to governmental agencies, with difficult to predict ramifications [2]. Existence of tools such as OnionScan [4] allows easy scanning of hidden services for vulnerabilities and misconfiguration. Previous research have confirmed the attack on hidden service [5], such attempts by different entities with varied level of sophistication and persistence.

In this work, we show that an adversary who compromises a Hidden Service's private key can mount a man-in-the-middle attack on the targeted hidden service. One characteristic of this attack is that the adversary does not need to be in the communication path between the client and the server. We provide a proof-of-concept (POC) for this attack. Given there is no revocation mechanism in hidden service, compared to the certificate system used by regular domains, limits the hidden services options of mitigation. This problem is innate to Tor's current design. We discuss possible detection and mitigation mechanism and the implication of the certificate systems for hidden services.

II. MITM Attack Setup

After acquiring the private key of a hidden service, to perform a successful stealthy MITM attack, the adversary needs to setup two relays. One that works as an impostor hidden service and another modified tor client that establishes and maintain a circuit with the "real" hidden service to relay the traffic from the user. Figure 1 shows the diagram of the attack architecture and connection setup.

In the first step the "real" hidden service, choose the corresponding HSDirs, to uploaded its descriptors (1). Then the adversary retrieves this information from the HSDirs (2) and establishes a circuit to the hidden services and maintains this connections (3). We modified the Tor client so that it would keep the connections. In the next step the adversary creates a new hidden service (using the compromised private key), and uploads the new descriptors to the HSDirs (4). Note that the same HSDirs will be used, since the hash of the public key (`.onion` address) is the same. The HSDirs will overwrite the previous "real" descriptor with the new one. Now, when the client wants of visit the targeted `.onion` address, he retrieves the descriptors from the HSDirs (5). Note, these descriptors were uploaded by the adversary. Next the client connects to the adversary's hidden service, under impression of connecting to the "real" hidden service (6). Since the adversary is sill connected to the "real" hidden service he can relay the traffic (7). Since the connections to the hidden services are not additionally encrypted, the traffic is visible to the adversary and is susceptible to interception.

III. Mitigation and Detection Strategies

As mentioned earlier, the hidden servers have no additional end-to-end encryption, since they provide an authenticated service baked in [6]. However, unlike regular domains that use SSL/TLS if the key is compromised there is no way to revoke the certificate. The only option is to abandon the `.onion` address and use a new one. It might be possible in case of personal hidden services, but for any public hidden service it is not desirable and optimal. Currently, DigiCert provides certificates for `.onion` domains. For example, Facebook uses such certificate for it's domain. However, only Extended Validation (EV) certificates are available for `.onion` domains.

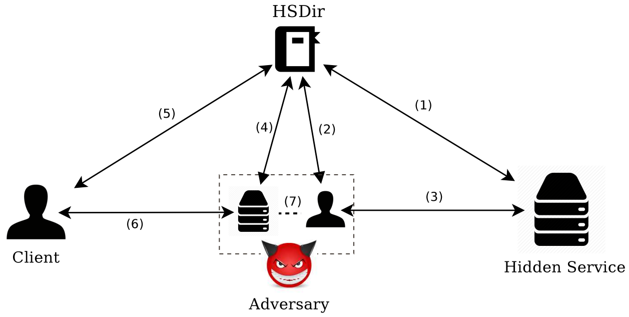

Fig. 1: Flow diagram of Tor hidden service MITM architecture and connection setup. We omit to show the circuits for clarity of the attack.

One the concerns raised by the CA/Browser Forum is the use SHA-1, RSA-1024 in the current hidden services architecture, however, the new design solves this problem by using SHA-256 and Ed25519 [6]. Given the anonymous nature of most hidden services, use of EV certificates is clearly not a viable solution. Please note that the certificates can also be susceptible to attacks [7], [8]

We implemented a mechanism to detect MITM attacks by comparing the descriptors at two levels. One level can be used by any entity to check if a MITM attempts is being made, but it is less accurate. The other approach can only be used by the entity who is running the hidden services and provides a more definitive conclusion. The first level at the HSDirs, meaning all the descriptors between the HSDirs should be the same and if there is a discrepancy it can a MITM attempt. In this approach we also consider the delay in the syncing process between HSDirs to reduce the false positives. The next level is at the hidden service. We log and compare the descriptors that the "real" hidden service has created and initially uploaded to the HSDirs, with the descriptors that the HSDirs serve to the users. If there is a discrepancy between this descriptors it is an indication of MITM attack. The POC video demo of the attack is available at `https://www.youtube.com/watch?v=nnlS4rMXp8M` The source code of the POC is also available at `https://ares.ccs.neu.edu/tor_mitm/`

IV. Related Work

Different aspects of the dark web and hidden services have been studied previously. For example Sanatinia and Noubir [9] look at the next generation of peer to peer onion botnets that rely on Tor to hide their source, destination and the content of the traffic. Other studies look at the content and attack surface of the hidden services and dark web [10]. In another work [3], the authors discover and exploit a flaw in the design and implementation of hidden services in Tor, which allows an adversary to measure the popularity of any hidden service, block access to hidden services, and ultimately deanonymize hidden services. Other works investigate the malicious behavior of the Tor relays. Winter et al. [11] study the behavior of Tor exit nodes, and expose such malicious nodes. Sanatinia and Noubir [12]design a novel framework to expose the snooping HSDris. Furthermore, they provide a classification of the snoopers and investigate their attack signatures. Syverson and Boyce [6] discuss the website authentication capabilities of hidden services and the future of hidden services.

V. Conclusion

Tor is a widely popular system for protecting users anonymity. Because of its anonymous nature, Tor attracts a large variety of users with different intentions and attacks. In this work, we showed that an adversary who compromises a Hidden Service's private key can mount a man-in-the-middle attack on the targeted hidden service. Furthermore, We discussed possible detection and mitigation mechanism and the implication of the certificate system for hidden services. We also provided a tool that can be used to detect MITM attack attempts.

References

[1] "Tor metrics," https://metrics.torproject.org/userstats-relay-country.html.

[2] "Confirmed: Carnegie mellon university attacked tor, was subpoenaed by feds," http://motherboard.vice.com/read/carnegie-mellon-university-attacked-tor-was-subpoenaed-by-feds, February 2016.

[3] A. Biryukov, I. Pustogarov, and R. Weinmann, "Trawling for tor hidden services: Detection, measurement, deanonymization," in *Security and Privacy (SP), 2013 IEEE Symposium on*, 2013.

[4] "Scan onion services for security issues," https://github.com/s-rah/onionscan/, April 2016.

[5] G. Noubir and A. Sanatinia, "Honey onions: Exposing snooping tor HSDir relays," in *DEFCON 24*, 2016.

[6] P. Syverson and G. Boyce, "Bake in .onion for tear-free and stronger website authentication," *IEEE Security Privacy*, 2016.

[7] "Let's encrypt issues certs to 'paypal' phishing sites: how to protect yourself," https://nakedsecurity.sophos.com/2017/03/30/lets-encrypt-issues-certs-to-paypal-phishing-sites-how-to-protect-yourself/, March 2017.

[8] L. S. Huang, A. Rice, E. Ellingsen, and C. Jackson, "Analyzing forged ssl certificates in the wild," in *2014 IEEE Symposium on Security and Privacy*, 2014.

[9] A. Sanatinia and G. Noubir, "Onionbots: Subverting privacy infrastructure for cyber attacks," in *The Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2015.

[10] A. Biryukov, I. Pustogarov, F. Thill, and R. P. Weinmann, "Content and popularity analysis of tor hidden services," in *ICDCSW*, 2014.

[11] P. Winter, R. Köwer, M. Mulazzani, M. Huber, S. Schrittwieser, S. Lindskog, and E. Weippl, "Spoiled onions: Exposing malicious tor exit relays," in *Privacy Enhancing Technologies*, 2014.

[12] A. Sanatinia and G. Noubir, "Honey onions: a framework for characterizing and identifying misbehaving tor HSDirs," in *Proceedings of IEEE Conference on Communication Networks Security (CNS)*, 2016.