TrustedAP: Using the Ethereum Blockchain to Mitigate the Evil Twin Attack

PHIL FOX, SUNY University at Buffalo, USA

The wireless network Evil Twin Attack (ETA) is still only partially mitigated decades after the advent of wireless networking. An ETA is a spoofing attack wherein a malicious actor creates a convincing copy of a wireless network Access Point (AP) by duplicating a Service Set ID (SSID) and/or hardware Message Access Control (MAC) address.

We introduce TrustedAP: A blockchain-based solution that provides means for clients to verify AP ownership as trustworthy using minimal (if any) connected time. We intend to use the blockchain and smart contracts as a medium for an end-user to challenge an AP's trustworthiness. Next, the AP or (AP trust-manager) delivers a sound, unique response to the blockchain and the requesting end user by extension. The response is validated by its ownership chain, and cryptographic integrity-preserving tools. Once validated, clients have a very strong reason to believe that their connection is trustworthy, genuine, and under positive control of the intended public WiFi provider.

Additional Key Words and Phrases: wireless network security, evil twin attack, cybersecurity, trust

ACM Reference Format:
Phil Fox. 2020. TrustedAP: Using the Ethereum Blockchain to Mitigate the Evil Twin Attack. In *SIGCSE TS 2021, ACM Student Research Competition.* ACM, New York, NY, USA, 3 pages.

1 PROBLEM AND MOTIVATION

Today, tools exist that enable novice-skilled malicious actors' problematic network proximity to devices and eavesdropping on unencrypted communications from unwitting, connected victims. The risk incurred from these attacks is especially adverse in environments with robust public WiFi on-offer such as airports, hotels, and on-the-go food service providers. ETAs can be very difficult to detect by an end-user since real-time internet connections can be properly routed. Further, auditing or forensics of ETA attack outcomes are difficult since important hardware stays within an attackers physical control.

TrustedAP is duly motivated by residual ETA risk even in the face of optimism regarding existing countermeasures. We recognize that ETAs are partially mitigated by encrypted communications. Emerging technology makes the availability of encryption fairly abundant through Secure Sockets Layer (SSL), Transport Layer Security (TLS), and general-purpose Virtual Private Networks (VPNs). The risk incurred from ETAs diminishes when 100% of a victim's incoming/outgoing network traffic is encrypted. However, problematic network proximity between malicious actors and victims leaves opportunities for network or hardware level exploits that can yield arbitrary remote code execution. Further, attacks against the network availability of victim wireless devices that operate with matching protocol cannot be mitigated by encryption alone and TrustedAP can help fill in the remaining cybersecurity gap.

2 BACKGROUND AND RELATED WORK

The ETA is (was) particularly effective when default operating system wireless network configurations store AP SSIDs and auto-connect when a saved SSID is within range. Public and device-default WiFi SSIDs (e.g., “Starbucks", “linksys") facilitate ETAs under those conditions due to their ubiquity as saved previous connections across devices in the wild. This paper’s author has experience with exploiting ETA vulnerabilities using these bases in a Red Team capacity during the SP1 and SP2 Windows XP patch era. Today, clients often confirm public WiFi APs per-use, prior to connection, but a lingering issue remains that plaintext, easily duplicated SSIDs (and MAC addresses, unfortunately) give clients zero basis for trust when creating and maintaining a connection.

Matos et al. propose a Near Field Communication (NFC) protocol for client devices to validate not yet trusted APs. This approach is sound, but limited by the physical NFC access constraints, and the need for non-traditional hardware implementation [1]. Nakhila et al. propose extending certificate validation for APs using similar protocols that facilitate HTTPS secure (and trusted) communication via the web. This approach is also sound, but limited by the need for strong *centralized* certificate-handling infrastructure [2]. We explain how these and similar limitations may be avoided given our unique approach in the next section.

3 APPROACH AND UNIQUENESS

Previous research findings and proposals on mitigating ETAs are often challenged on the basis of affordable, swift, wide implementation given the above mitigation structures in-place. TrustedAP potentially operates with minimal to zero additional hardware and leverages cryptographically strong, public, distributed resources for its operation. We aim to meet an implementation cost threshold for TrustedAP that overcomes existing cost-benefit obstacles that impede wide adoption of legacy solutions to the ‘ETA problem’.

TrustedAP client devices and AP webservers can interact using free Metamask, Node.js, and similar software platforms to handle information exchange. APs will be marked as trusted through a manager interface which requires near trivial input per AP thanks to the immutable trust handed down from the smart contact deployer to designated AP managers. A naive proof-of-concept implementation may require an AP-connected server/AP manager device, but future work may leverage a best-case, *native* on-AP/router/gateway platform. Future work may also yield minimal client impact from simple, portable installation. Lastly, we predict that maximal efficacy of TrustedAP is possible through operating system or other Wireless Connection Manager integration.

4 RESULTS AND CONTRIBUTIONS

TrustedAP aims to further (or perhaps completely) close the door on longstanding ETA cybersecurity vulnerabilities. In the best case, clients will identify an untrustworthy AP prior to connection time. In a naive proof-of-concept implementation, client devices will spend minimal connected time defeating prospective attacks before most malicious scans can complete. TrustedAP’s success is not contingent on effectiveness alone, as other strong solutions exist. Rather, TrustedAP further aims to take good advantage of the Etherium blockchain trust infrastructure and robust decentralized resources creating an affordable and (eventually) easy-to-implement solution that is attractive to both frequent public WiFi users and providers.

REFERENCES

[1] A. Matos, D. Romão, and P. Trezentos. 2012. Secure hotspot authentication through a Near Field Communication side-channel. In *2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. 807–814. https://doi.org/10.1109/WiMOB.

2012.6379169

[2] O. Nakhila, E. Dondyk, M. F. Amjad, and C. Zou. 2015. User-side Wi-Fi Evil Twin Attack detection using SSL/TCP protocols. In *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*. 239–244. https://doi.org/10.1109/CCNC.2015.7157983