Poster: Passive Device Identification with Packet Timing Analysis

Federico Cifuentes-Urtubey, Deepak Vasisht, and Robin Kravets
University of Illinois at Urbana-Champaign
{fc8,deepakv,rhk}@illinois.edu

ABSTRACT

We present preliminary results on identifying unique devices using an attack exploiting temporal patterns on packet bursts during Wi-Fi network discovery. The attack achieves a 94.1% success rate in detecting unique mobile devices.

CCS CONCEPTS

• **Networks** → *Network privacy and anonymity*.

1 EXPLOITING INTER-BURST TIMING

With a pervasive Wi-Fi network infrastructure, people are equipped with devices that allow them to easily be tracked. To obtain connectivity, Wi-Fi devices must search for nearby access points (APs) to connect with, in which they broadcast probe request packets that contain their unique factory-assigned MAC address, allowing a nearby attacker to easily identify them. As a defense, mobile devices adopted MAC address randomization to prevent leaking devices' globally unique address while removing the link between sequential packets. Since the MAC address is not the only explicit identifier while probing, *MAC randomization alone fails to protect other identifiers that can be used to track users.*

Even without a unique identifier, Wi-Fi traffic from a given device demonstrates temporal patterns that can be exploited to track it [1, 2]. In this work, we conduct a preliminary analysis on a new attack that exploits temporal patterns between bursts of probe requests transmitted by a device during network discovery. Our attack's intuition lies in how Wi-Fi devices configure scanning for APs on a predictable interval. We refer to this as the *burst interval*. By measuring burst intervals, similar measurements can be used to identify a device with high probability as it uses MAC randomization.

Attack Design: Using the above intuition, the attack's goal is to find repeating patterns from a sequence of probes. Given a trace of probe request transmissions, we create a time-domain matched filter where if there is a probe at time t, then the value of the sequence $S(t)$ is 1, otherwise 0. A base pattern $b_{k,T}$ representing a sequence of k bursts spaced by time T is then used to find probes matching the sequence from the capture. At time index i, $b_{k,T}(i)$ is set to 1 if $i = \{1, ...k\}T$. To find the pattern $b_{k,T}$ in $S(t)$, we correlate time-shifted copies of the base pattern with the captured sequence. If the correlation results above a threshold, probes from the positive results are considered belonging to the same device.

Device	Detection Rate	Burst Interval
Windows 10 Laptop	85.7%	59.7s ± 20ms
Raspberry Pi 3B+	96.8%	60.0s ± 25ms
Ubuntu 20.04 Laptop	100%	63.0s ± 30ms

Table 1: Detection Rates and Observed Burst Intervals from the burst interval attack against deployed devices.

Implementation: In a sparse network (i.e., <20 devices), a Windows 10 laptop, a Raspberry Pi 3B+ running the *brcmfmac* WLAN driver, and an Ubuntu 20.04 laptop running the *ath10k* WLAN driver are deployed with MAC randomization enabled. A MacBook Air captures packets on Channel 1 for 30 minutes, then the packet capture is analyzed using the recorded random MAC addresses as ground truth.

Results: A successful result of the burst interval attack correctly identifies the MAC addresses used by a given deployed device. This is measured as precision, where the number of correct matches is divided by the number of matches made. From our analysis, the burst interval attack identifies the deployed devices with an average true positive rate of 94.1%. Detection rates for each device are summarized in Table 1. Burst intervals account for variation from channel contention on the medium.

Based on experimental results, our burst interval attack can identify unique devices by exploiting predictable transmission timing during Wi-Fi network discovery.

REFERENCES

[1] Célestin Matte, Mathieu Cunche, Franck Rousseau, and Mathy Vanhoef. 2016. Defeating MAC Address Randomization Through Timing Attacks. In *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec '16)*. 15–20. https://doi.org/10.1145/2939918.2939930

[2] Jeffrey Pang, Ben Greenstein, Ramakrishna Gummadi, Srinivasan Seshan, and David Wetherall. 2007. 802.11 User Fingerprinting. In *Proceedings of the 13th Annual ACM International Conference on Mobile Computing and Networking (MobiCom '07)*. 99–110. https://doi.org/10.1145/1287853.1287866

S3 '23, October 6, 2023, Madrid, Spain

ACM ISBN 979-8-4007-0342-3/23/10.
https://doi.org/10.1145/3615591.3615675