Defending Wi-Fi Network Discovery from Time Correlation Tracking

The Problem

MAC address randomization alone doesn't work to hide devices.

Devices can be tracked based on **patterns in Wi-Fi discovery events** to defeat MAC address randomization:

- Timing between probe request transmissions
- MAC randomization deployment inconsistencies
- Consistent delays between each probe request
- # of packet bursts to appear on a channel
- # of probe requests in each burst

Our Solution

Configure probe request transmissions
- Randomize the *ProbeDelay* parameter for random jitter
- Choose the channel(s) to scan – default to all channels
- Optional, choose number of probes to scan per burst

↓

Randomize the MAC address on each packet
A per-packet basis makes a stronger defense

↓

Transmit the probe request
Frames wait a random *ProbeDelay* during network discovery

↓

Evaluate with a Time-based Tracking Algorithm
Collect stats on IFAT metrics to identify devices

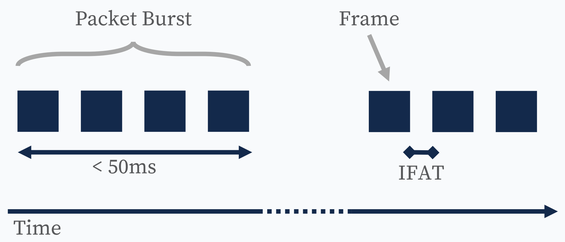
References

E. Fenske et al. Three Years Later: A Study of MAC Address Randomization in Mobile Devices And When It Succeeds. In *PoPETs '21*. DOI: 10.2478/popets-2021-0042

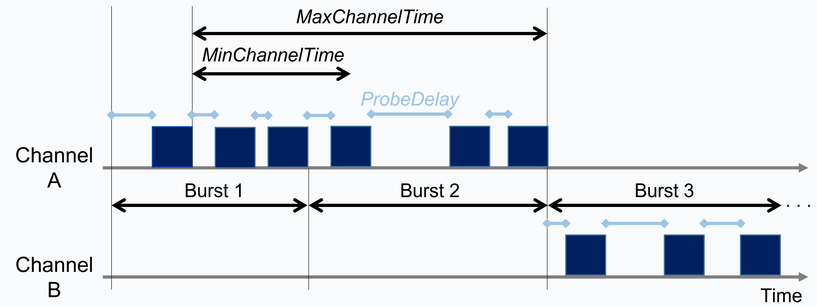
C. Matte et al. Defeating MAC Address Randomization Through Timing Attacks. In *WiSec '16*. DOI: 10.1145/2939918.2939930

M. Vanhoef et al. Why MAC Address Randomization is Not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms. In *ASIA CCS '16*. DOI: 10.1145/2897845.2897883

We defended against tracking Wi-Fi devices with breaking temporal patterns in wireless transmissions.



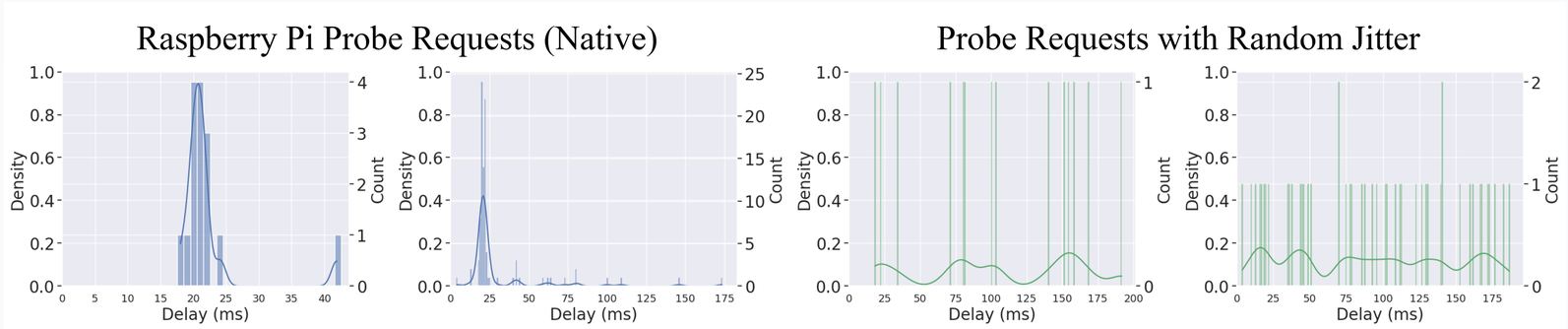
Probe request transmissions have a predictable *Inter-frame Arrival Time (IFAT)*. This leaks a traceable transmission behavior for the device.



Our solution randomizes *ProbeDelay* on each frame to change IFATs between transmissions and break native temporal patterns.

Native IFATs have predictable timing

IFATs from random jitter have a more uniform distribution



1min capture, Peak at 21ms | 20min capture, Peak at 21ms | 1min capture from Netlink | 20min capture from Netlink

Identifying the Raspberry Pi with Native Probes
- 88% of the time in the 1min capture, and
- 75% of the time in the 20min capture

Identifying the Modified Probing
- No match from jittered frames for both time windows

Federico Cifuentes-Urtubey, Robin Kravets, and Deepak Vasisht
Department of Computer Science, University of Illinois at Urbana-Champaign

CS @ ILLINOIS COMPUTER SCIENCE