Issued 3/11/17

A Massive Failure that Leaves iPhones & Android Mobiles Open to Tracking

To protect mobile devices from being tracked as they move through Wi-Fi-rich environments, there's a technique known as MAC address randomization. This replaces the number that uniquely identifies a device's wireless hardware with randomly generated values. In theory, this prevents criminals from tracking devices from network to network, and by extension the individuals using them, because the devices in question call out to these nearby networks using different hardware identifiers. It's a real issue because stores can buy Wi-Fi equipment that logs smartphones' MAC addresses, so that shoppers are recognized by their handheld when they next walk in, or walk into affiliate shop with the same creepy system present. This could be used to alert assistants, or to follow people from department to department, store to store, and then sell that data to marketers and ad companies. Public wireless hotspots can do the same. Transport for London in the UK, for instance, used these techniques to study Tube passengers.

Regularly changing a device's MAC address is supposed to defeat this tracking. But it turns out to be completely worthless, due to a combination of implementation flaws and vulnerabilities. That and the fact that MAC address randomization is not enabled on the majority of Android phones. In a paper published on Wednesday, US Naval Academy researchers report that they were able to "track 100 per cent of devices using randomization, regardless of manufacturer, by exploiting a previously unknown flaw in the way existing wireless chipsets handle low-level control frames." Beyond this one vulnerability, an active RTS (Request to Send) attack, the researchers also identify several alternative deanonymization techniques

that work against certain types of devices. Cellular radio hardware has its own set of security and privacy issues; these are not considered in the Naval Academy study, which focuses on Android and iOS devices. Each 802.11 network interface in a mobile phone has a 48-bit MAC address layer-2 hardware identifier, one that's supposed to be persistent and globally unique. Hardware makers can register with the Institute of Electrical and Electronics Engineers (IEEE) to buy a block of MAC addresses for their networking products: the manufacturer is assigned a three-byte Organizationally Unique Identifier, or OUI, with is combined with an additional three-byte identifier that can be set to any value. Put those six bytes together, and you've got a 48-bit MAC address that should be globally unique for each device.

The IEEE's registration system makes it easy to identify the maker of a particular piece of network hardware. The IEEE also provides the ability to purchase a private OUI that's not associated with a company name, but according to the researchers "this additional privacy feature is not currently used by any major manufacturers that we are aware of." Alternatively, the IEEE offers a Company Identifier, or CID, which is another three-byte prefix that can be combined with three additional bytes to form 48-bit MAC addresses. CID addresses can be used in situations where global uniqueness is not required. These CID numbers tend to be used for MAC address randomization and are usually transmitted when a device unassociated with a specific access point broadcasts 802.11 probe requests, the paper explains. The researchers focused on devices unassociated with a network access point – as might happen when walking down the street through various Wi-Fi networks – rather than those associated and authenticated with a specific access point, where the privacy concerns differ and unique global MAC addresses come into play. Previous security research has shown that flaws in the Wi-Fi Protected Setup (WPS) protocol can be used to reverse engineer a device's globally unique MAC address through a technique called Universally Unique IDentifier-Enrollee (UUID-E) reversal. The US Naval Academy study builds upon that work by focusing on randomized MAC address implementations. The researchers found that "the overwhelming majority of Android devices are not implementing the available randomization capabilities built into the Android OS," which makes such Android devices trivial to track. It's not clear why this is the case, but the researchers speculate that 802.11

chipset and firmware incompatibilities might be part of it. Surprisingly, Samsung devices, which accounted for 23 per cent of the researcher's Android data set, show no evidence of implementing MAC address randomization.

Apple, meanwhile, introduced MAC address randomization in iOS 8, only to break it in iOS 10. While the researchers were evaluating devices last year, Apple launched iOS 10 and changed its network probe broadcasts to include a distinct Information Element (IE), data added to Wi-Fi management frames to extend the Wi-Fi protocol. "Inexplicably the addition of an Apple vendor- specific IE was added to all transmitted probe requests," the paper explains. "This made identification of iOS 10 Apple devices trivial regardless of the use of MAC address randomization." This shortcoming aside, Apple handles randomization correctly, in the sense that it properly randomizes the full 48-bits available for MAC addresses (with the exception of the Universal/Local bit, set to distinguish between global MAC addresses and the local ones used for randomization, and the Unicast/Multicast Bit). The researchers find this interesting because the IEEE charges a fee for using the first three bytes of that space for CID prefixes, "meaning that Apple is freely making use of address space that other companies have paid for." In a phone interview with The Register, Travis Mayberry, assistant professor at the US Naval Academy and one of the paper's co-authors, expressed surprise that something like 70 per cent of Android phones tested did not implement MAC address randomization.

Apple fared better in terms of effort, though not results. "Apple is the closest to being pretty good," Mayberry said, but noted that Apple devices, despite the advantage of hardware consistency, are still vulnerable to an RTS (Request to Send) attack. Sending RTS frames to an Apple phone forces the device to reveal its global unique MAC address, rather than the randomized one normally presented to the hotspot. "No matter how hard you try, you can't defend against that because it's a property of the wireless chip itself," said Mayberry. There was single Android phone that fared well. "The one Android phone that was resistant to our passive attacks was the CAT S60 which is some kind of 'tough' phone used on construction sites and the like," Mayberry explained in an email. "It did not have a recognizable fingerprint and did not ever transmit its global MAC except when associating. It was still vulnerable to our active RTS attack though,

since like I said, that is a problem with the actual chips and effects every phone." Mayberry was at a loss to explain why Apple shot itself in the foot by adding a trackable identifier to a system that previously worked well. "I initially thought it might be to support some of the 'continuity' features where multiple apple devices can discover and exchange stuff like open browser tabs and clipboard contents but that came out in earlier versions of iOS," he said. "It also might be linked to the HomeKit features that they added in iOS to control IoT devices.

Basically it would have to be to purposefully identify and discover other Apple devices that are not associated, otherwise we wouldn't see it in probe requests. All of this is pure speculation though and we really don't have a strong reason for it."