PRIVACY FRIENDLY DEVICE IDENTIFICATION AND AUTHORIZATION FOR THE HOSPITALITY INDUSTRY

Overview

The Hospitality industry, like many others, is trying to balance consumer needs for digital privacy with convenience and a personalized, high-quality guest experience. For years, a variety of hotel systems have been able to rely on a device's MAC address as a method of positively identifying a device, and thus a guest, to deliver a more seamless, high quality, guest experience. However, over time, the MAC address has been used and abused in ways never considered when it was conceived. These unintended use cases have allowed consumer privacy to be compromised for the benefits of others, and in some cases, for more questionable purposes. As a result, device manufacturers have been taking actions to obfuscate device MAC addresses to reclaim consumer privacy, even though some of the steps will come at a very real cost to guests, properties and the supporting industry. To eliminate this tradeoff between privacy and function, LEVL is introducing a new device identity platform that can positively identify and authorize devices, without significant privacy compromise. It is the first such privacy friendly mechanism for device identification.

THE USE AND ABUSE OF MAC ADDRESSES

Every Wi-Fi device has a unique identifier, the MAC address, that is used to identify the sender and receiver radios during transmission. In wireless technologies, e.g., WiFi, messages are exchanged over the air, so they can be intercepted and decoded to extract the MAC address, specially so as the MAC Address is transmitted unencrypted (this is required for networking/functionality purposes). By 2012 the smart phone revolution was well under way and it was becoming apparent that the MAC address was being used for much more than just managing Wi-Fi Traffic. On the plus side, it was used to enable parental controls in Wi-Fi or used for a more seamless login experience on a hotel property. Pay-per-use network access was also made significantly easier with single login for the duration of a stay.

(c) LEVL Technologies Inc. 2020

On the other hand, app makers were using it to track user behaviors with other apps. Still others were using it to track the physical location of people and MAC addresses were increasing being linked to specific people. It was about this time that Apple took the first steps to protect privacy by randomizing MAC addresses prior to joining a network. Since then, device and OS makers have increased their privacy efforts by minimizing App access to MAC addresses and more recently, Android 10 introduced a randomized MAC address per SSID even after joining a network. These have all been great step forwards in privacy, with almost no impact to the guest experience. And yet the abuse continues in mid-2020 it was discovered that TikTok had collected 100s of millions of user MAC addresses by working around Android protections. Thus, the industry continues to strive to improve privacy protections. The most recent step forward is Apple's recent move to time-based MAC addresses in IOS14. This move would effectively handicap use MAC address within the hospitality industry for many of the current use cases. Privacy and user convenience are once again at odds.

THE IMPACT OF RANDOM MAC ADDRESSES

Apple's announcement is giving people in many industries significant reason to pause (or panic). It basically means that every day, a device has a new MAC address, with the goal to prevent linking the identity and activity from one day to another. Many services which rely on MAC address will be affected.

- Seamless guest Wi-Fi login ends each night and starts over on the new day, requiring guests to re login to the network every day – affecting the general user experience.
- Multi day billing becomes a challenge as well because there will be no record of what devices have paid for access – this means pay-per-use users will be asked to re-pay every day.
- Employees will also have to re-login each day onto the network, reducing productivity and employee satisfaction.
- Devices such streaming hubs and IoT devices may also be impacted because in many cases these are automatically allocated to specific VLANs, and their association with such VLAN is enforced using MAC filtering.
- Network optimization and support technologies using device MAC addresses to quickly diagnose, prevent or fix network performance problems are also affected.
- Personalization services which provide the user an individual experience at the property will be affected as well.

Without the MAC address as we know it, guest experience erodes, costs go up, and revenue will eventually go down.

(c) LEVL Technologies Inc. 2020

SO, WHAT ARE THE ALTERNATIVES TO MAC ADDRESSES?

To date, there are not any obvious alternatives to using MAC addresses to identify a device while maintaining user privacy. The most discussed is Hotspot 2.0, an industry standard with little acceptance to date. Hotspot 2.0 requires users to install a profile on their device for each hotel brand they use. The implementation has some variation depending on the device manufacturer and Apple, in particular, has not adopted the latest versions of the specification. While this approach may work for loyalty guests, it is relatively expensive and not consistent across all device types. To date, the Hotspot 2.0 user experience is, in the best case, a challenge and it would only apply to a subset of the hospitality use cases. Beyond Hotspot 2.0, the most common thoughts are to try to delay the implementation of better user privacy, building more authentication into brand Apps, or essentially just living with a degraded guest experience.

THE LEVL SOLUTION – PRIVACY FRIENDLY DEVICE IDENTIFICATION

At LEVL, we take a novel approach to device identification. LEVL uses a full-stack approach, leveraging data from all 7 layers of the OSI model. For examples of how this can be done with minimal risk to user privacy and for examples of features used by LEVL to construct a LEVL-ID please see Appendix A. This approach enables LEVL to create a unique identifier (LEVL-ID) for every individual device on a hotel property. The LEVL-ID is created passively using the information already present on every device and without the need to modify anything on the devices. A LEVL ID is a derived identifier, so it is not stored on the device where it can be stolen by a malicious App. The ID is never transmitted over the air directly, so it cannot be intercepted or “sniffed”. Instead, the LEVL-ID is derived from the network, the device radio waves, and the device behavior. Thus, a LEVL-ID is localized to a specific property and the network within that property, preventing 3rd parties to track devices.

(c) LEVL Technologies Inc. 2020

As a result, LEVL-IDs are privacy friendly, easy to implement, and cost effective. In terms of privacy, the IDs are constructed in a manner to intentionally localize them to a network. Getting a LEVL-ID from one network is not going to work at another network. Thus, not only can they not be extracted directly from a device, there is no value to bad actors to collect LEVL-IDs as they can not be used in another network. Implementing a LEVL-ID is dependent upon the use case and the existing network infrastructure. In most cases, it can be as easy as installing a lightweight appliance within the property network. The ease of implementation, the use of standard hardware and the flexibility to scale the use from simple identification to authentication allows LEVL to offer this technology in a very cost-effective manner.

In summary, the LEVL-ID ideal for enabling properties to maintain a high-quality digital guest experience, while at the same time respecting guest privacy. From seamless Wi-Fi access to maintaining a high performing network, the LEVL-ID can be employed to effectively counter the downsides of MAC address randomization without sacrificing a guest's digital privacy.

WHERE IS LEVL IN USE?

The initial adoption of LEVL's platform is in various European designed sedans and SUVs in model year 2021. LEVL's technology has been tested by leading Tier-1s and OEMs in the automotive industry and has been chosen by the biggest automotive companies to secure the next generation of vehicle access systems. LEVL has been chosen for its unique ability to defeat impersonation and relay attacks, for its ability to operate within strict automotive regulatory guidelines and for its ease of deployment.

WHO IS LEVL?

Founded in 2017 and backed by Silicon Valley VCs, LEVL currently has offices in Palo Alto, Denver and Tel Aviv. In 2022 LEVL was acquired by a joint venture between Comcast and Charter. The technical team includes engineers with experiences from places like the Israeli defense forces, Israeli intelligence, Google, Dell, Akamai, Qualcomm and more.

Contact us at: Sales@LevlTech.com

(c) LEVL Technologies Inc. 2020

Additional Details

LEVL uses data collected from all 7 layers of the OSI stack to create a LEVL-ID for every individual device. The data leveraged does not include private user information nor the data transmitted by the user over the network. LEVL's platform leverages management protocols and specific management packets/protocols transmitted by the network to create a LEVL-ID. Some examples are provided in the following table. Note that LEVL's platform does not require all these layers of information, in fact, even a subset of these can be used to create an ID.

Layers	Examples of features
1 - Physical	Channel Frequency Response (for wireless) voltage on the port (for wired, when available)
2 – Data Link	Timing behavior 802.11x Capabilities (for wireless) Beamforming sounding packets (for wireless)
3 - Network	ICMP Fingerprint List of open ports List of used protocols DHCP Fingerprints SNMP Fingerprints
4 - Transport	TCP headers fingerprint
5 - Session	NetBIOS fingerprint
6 - Presentation	SSL/TLS supported capabilities list
7 - Application	HTTP/FTP fingerprints

(c) LEVL Technologies Inc. 2020