Cybersecurity

Latest BLE vulnerability might be a deal-breaker

10-minute Insight

UK-based NCC Group says it found security flaws in Bluetooth Low Energy (BLE). The vulnerability involves using a link layer relay attack on a BLE system. This attack is effective to gain access and start a Tesla model 3 and a Tesla model Y.

BLE is broadly used as a communication protocol in several industries, including automotive. One of the use cases involves using BLE as communication protocol between the key (either smart key or digital key) and the vehicle to allow entry and start.

In this insight we explore the potential impact of such vulnerability and how it might affect the selection of future communication technologies for OEMs.

Target audience

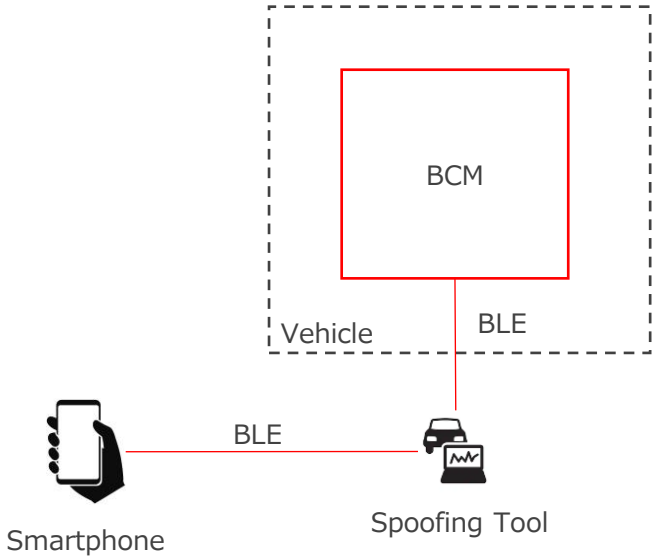
Product planning Strategy Cybersecurity Engineering

Focus market(s)

Global

What is happening?

NCC Group finds vulnerability on Bluetooth*



NCC Group researchers demonstrated a new way to do a man-in-the-middle attack in BLE communications between the Tesla vehicle and the user's smartphone.

The attack appears to be effective at 25 meters range from the vehicle and allows attackers to unlock and operate the vehicle. NCC Group successfully tried this attack on a Tesla model 3 and a Tesla model Y.

Brands shown to be affected by vulnerability (brand uses a BLE-only system for vehicle access)

TESLA

Brands that could be affected by vulnerability (brand using a BLE-only system for vehicle access)**

长安汽车 CHANGAN
HONDA
LINCOLN
ROEWE 荣威
VAUXHALL
WEY
WELTMEISTER 威马汽车

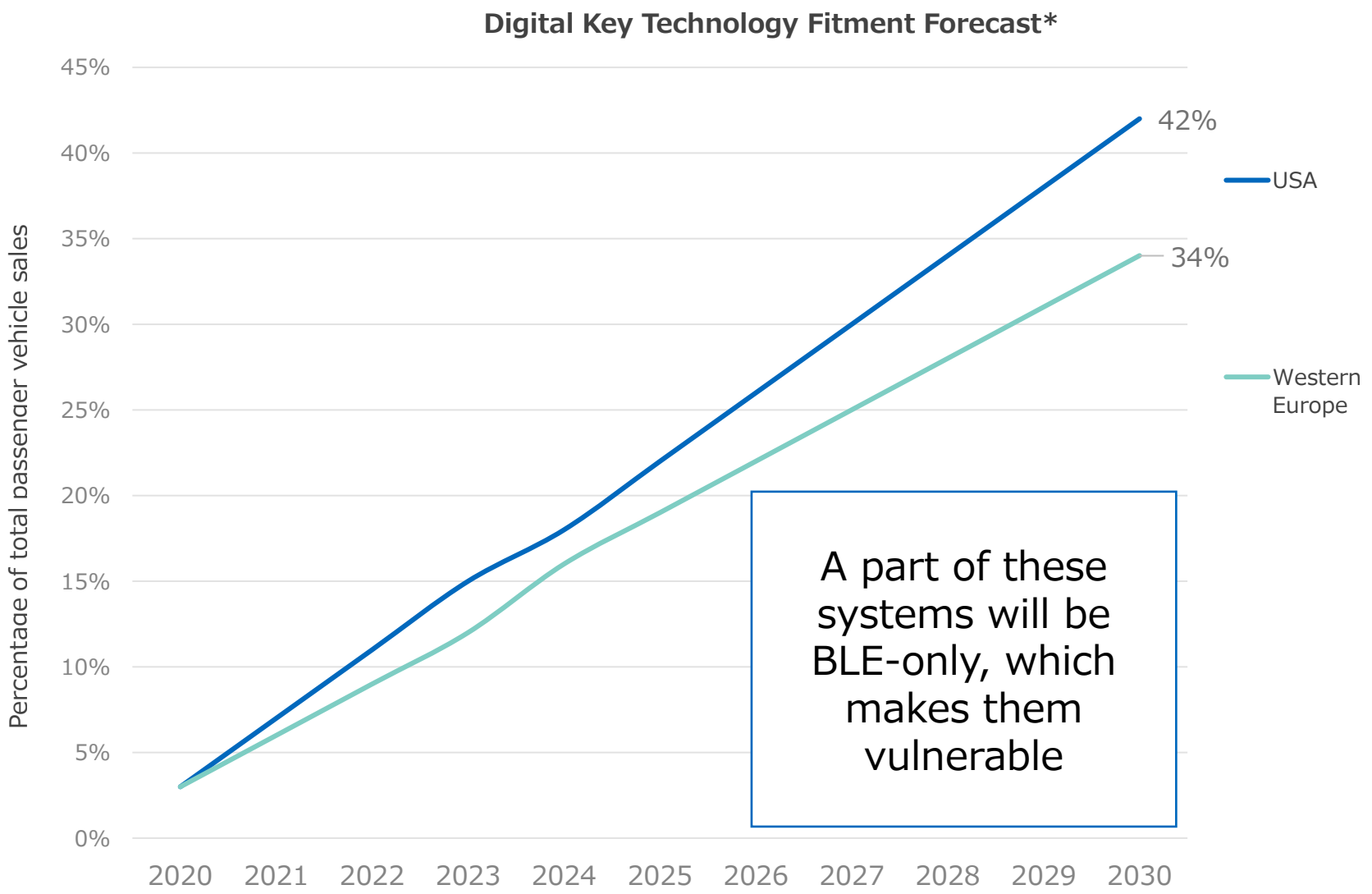
* Initial press release made by NCC
** Based on SBD's Digital Key Guide (Ref 711)

Key takeaway

If what NCC states is accurate this is an important vulnerability, affecting anything that relies on BLE as a communication protocol for proximity base use cases (including access control, such as door locks)

- Based on the available data, it seems there are no directly deployable mitigations on the Bluetooth layer.
- For an automotive access control case this means the only direct solution would be disabling the passive entry function that uses BLE.
- There are indirect mitigations like 2-factor authentication that could mitigate the issue (e.g. Tesla's Pin to Drive) however, this does not solve the inherent vulnerability, it just adds another layer of security.
- This is the first time that this type of attack is publicly known, based on SBD's Cybersecurity Intelligence (link here).

Why does it matter?



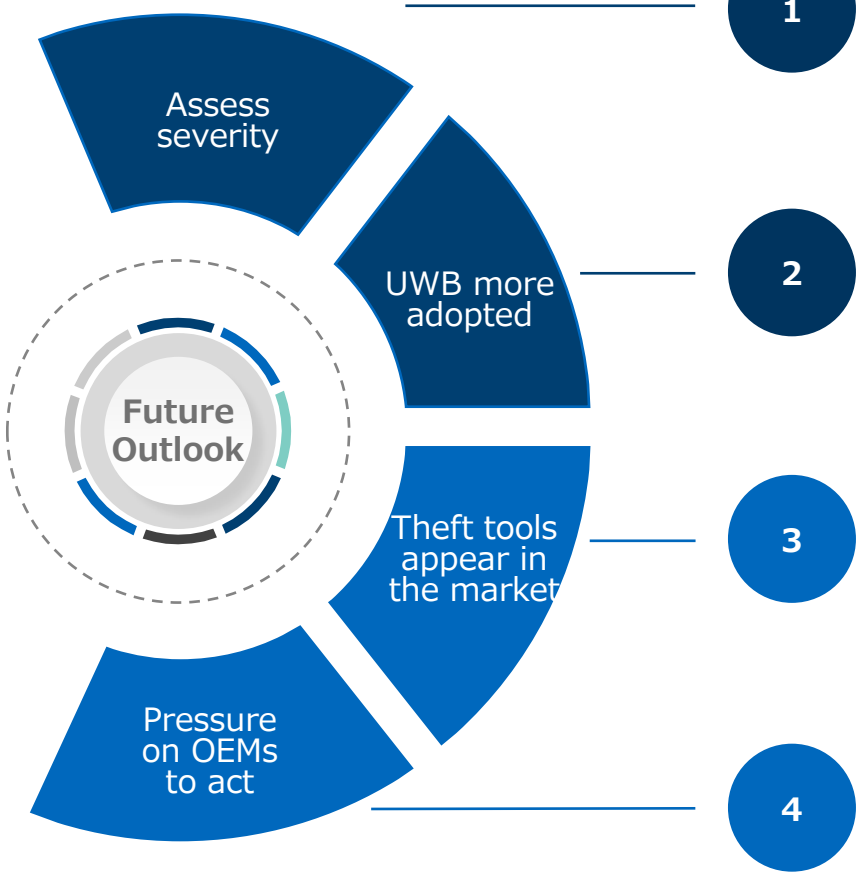
Key takeaway

The vulnerability presented by NCC affects vehicles with smart or digital key systems that use only BLE. This presents an opportunity for thieves to gain entry to such vehicles.

- Using BLE in combination with other communication technology, like Ultra-Wide Band (UWB), will further enhance the overall security of the system.
- Future Smart key systems are likely to adopt BLE+UWB communication technologies used by the digital key systems, eliminating the need for 2 separate communication platforms.
- A vulnerability for car access will not only affect brand perception. If thefts on certain models increase due to thieves exploiting the vulnerability, insurance premiums will increase, making total cost of ownership higher for consumers.

* Forecast based on SBD's Digital Key Guide (Ref 711)

Where next?



1. Cyber security experts need to assess the impact, severity and replicability of this attack.
2. An inherent vulnerability on BLE will accelerate the consideration and adoption of UWB or UWB+BLE for vehicle access systems
3. Theft tools that use this vulnerability will start being used by OCGs to access vehicles
4. As mainstream media reports the new theft method, there will be pressure on OEMs to address the vulnerability

1-3yrs | 3-5yrs | >5yrs

Key takeaway

There is a race between making secure systems and creating tools to exploit underlying vulnerabilities. Depending on the severity and feasibility of this vulnerability, a BLE-only system might be discarded for sensitive use cases, such as vehicle access.

- There is currently not enough public information to assess the impact of the attack. The NCC security group will not release the full details of the attack until the affected parties can address or patch the vulnerability (which is common practice that follows the path of responsible disclosure).
- However, if this vulnerability is not easy to solve, other actors will try to replicate the vulnerability for their own means (e.g. illegally accessing a vehicle).

Who to watch out for?

Trend-setters within our industry

CAR CONNECTIVITY consortium®

> The CCC brings together an incredibly unique group of like-minded companies, many of which are natural competitors, in order to deliver a universal digital key capability to the world's transportation industry. The strength of this digital key ecosystem rests with our member companies who are sustaining and advancing this interoperable digital key for the future of mobility. I'm confident of their commitment to our mission.
>
> **Daniel Knobloch – President, Car Connectivity Consortium, CCC**

Trend-setters outside our industry

Bluetooth® SPECIAL INTEREST GROUP

> The arrival of channel sounding to provide high-accuracy distance measurement using Bluetooth technology is expected to ship in products in 2023. This will bring significant enhancements for positioning applications, improving the accuracy over existing systems, as well as the security, and is expected to be widely supported by the chipset ecosystem without the need for a new chip or advanced antenna designs.
>
> **Bluetooth SIG webinar**

Key takeaway

Different bodies are pushing certain technologies to become mainstream in automotive. Given the industry-wide support CCC is getting, it is likely that future communication protocols will be based on their specification.

- The CCC issued its digital key specification release 3 early. The specification covers passive entry and passive start use cases. By doing so, the CCC have considered the secure ranging aspect of those use cases which made them select a combination of BLE+UWB technology.
- It is expected that most OEMs will follow CCC specifications in the future when adopting digital key systems.
- On the other hand, Bluetooth SIG thinks that BLE alongside channel sounding will enhance the accuracy of positioning applications, e.g. vehicle access systems.

How should you react?

1 Select

Select the appropriate technology for each use case. In its current state, Bluetooth cannot ensure a secure distance bounding. Hence, it should not be used to ensure a precise distance measurement (e.g. for passive entry systems).

2 Balance

Evaluate use cases and provide the best balance between security and user functionality. Put in place best practices for both security and functionality.

3 Secure

Including security by design on systems is paramount. Critical use cases should have further failsafe in place.

Authors

Edward Paez
Specialist

Jithesh Joshy
Domain Principal

Related SBD Reports

Ref:711
Digital Key Guide

Ref:905
Cybersecurity Intelligence

Related SBD Consultancy

- Penetration testing
- Design reviews
- Security benchmarking
- Strategic advisory

Interested in finding out more?

Most of our work is helping clients go deeper into new challenges and opportunities through custom projects. If you would like to discuss recent projects we've completed relating to **Cybersecurity**, please contact us.