All times are Pacific Time (GMT/UTC -7h)

ALL SESSIONS

SPEAKERS

RollBack - A New Time-Agnostic Replay Attack Against the Automotive Remote Keyless Entry Systems

Levente Csikor | Senior Research Scientist, NCS Group / Institute for Infocomm Research, A*STAR
Hoon Wei Lim | Director, Cybersecurity R&D, NCS Group
Jun Wen Wong | Researcher, DSBJ Pte. Ltd.
Soundarya Ramesh | PhD Student, National University of Singapore
Rohini Poolat Parameswarath | Researcher, National University of Singapore
Chan Mun Choon | Professor, National University of Singapore

Date: Thursday, August 11 | 1:30pm-2:10pm (Islander EI (Level 1))
Format: 40-Minute Briefings
Tracks: Cyber-Physical Systems, Hardware / Embedded

Automotive Remote Keyless Entry (RKE) systems implement disposable rolling codes, making every key fob button press unique, effectively preventing simple replay attacks. However, RollJam was proven to break all rolling code-based systems in general. By a careful sequence of signal jamming, capturing, and replaying, an attacker can become aware of the subsequent valid unlock signal that has not been used yet. RollJam, however, requires continuous deployment indefinitely until it is exploited. Otherwise, the captured signals become invalid if the key fob is used again without RollJam in place.

We introduce RollBack, a new replay-and-resynchronize attack against most of today's RKE systems. In particular, we show that even though the one-time code becomes invalid in rolling code systems, there is a way to utilize and replay previously captured signals that trigger a rollback-like mechanism in the RKE system. Put differently, the rolling codes can be resynchronized back to a previous code used in the past from where all subsequent yet already used signals work again. Moreover, the victim can still use the key fob without noticing any difference before and after the attack.

Unlike RollJam, RollBack does not necessitate jamming at all. Furthermore, it requires signal capturing only once and can be
exploited any time in the future as many times as desired. This time-agnostic property is particularly attractive to attackers, especially in car-sharing/renting scenarios where accessing the key fob is straightforward. However, while RollJam defeats virtually any rolling code-based system, vehicles might have additional anti-theft measures against malfunctioning key fobs, hence against RollBack. Our ongoing analysis (covering the Asian vehicle manufacturers for the time being) against different vehicle makes, models, and RKE manufacturers revealed that ~70% of them are vulnerable to RollBack. Since most of the RKE transceivers from three out of the four (identified) manufacturers were vulnerable, the impact is expected to be bigger worldwide.

PRESENTATION MATERIAL

- Slides
- Whitepaper