**Paper -** [**Ghost Peak: Practical Distance Reduction Attacks Against HRP UWB Ranging**](https://www.usenix.org/system/files/sec22fall_leu.pdf)

**Summary**

This paper is about attacks on High-Rate Pulse Repetition Frequency (HRP) Ultra-Wide Band (UWB) distance measurement systems. Attacks are conducted on chips like Apple U1, NXP, and Qorvo. Authors were able to spoof a 12m distance to 0m with a success probability of up to 4%. Security vs latency is an important factor that the author is trying to emphasize especially in security-critical applications using UWB HRP devices. These attacks are conducted using a technique called selective overshadowing where the power level is independently adjusted thereby deceiving the receiver as not an additional packet or a jamming packet to the legitimate one. In this technique, the attacker observes and analyzes the sequence of packets transmitted and then interjects signals over selected packet components to trick the receiver into mistaking noise as a legitimate signal.

**Strengths**

* Secure-ranging protocols used in cars and other access systems have to be secure for a long time since these can't be changed once installed in the systems. So this paper is a step in that direction to make sure that these protocols are secure and future-proof before they are widely adopted.
* Attacks are conducted without the knowledge of cryptographic material shared between the devices or access to randomized message content thereby making it a serious and legitimate threat to the protocols and systems using these protocols.
* The cost of the attacks is as low as 65 USD and devices used for the attack can be purchased off the shelf. This reduces the barrier for attacks and many attackers from script kiddies to experience attackers can use these techniques to compromise the distance measurement.
* A clear call to action on updating the security of HRP-UWB systems is described in the paper and also possible countermeasures are also discussed with the pros and cons of changing receiver complexity on battery-powered devices such as Air tags

**Weaknesses**

* Attacks are conducted on proprietary chips such as Apple, NXP, and Qorvo. The security configurations of these chips are not known and it is not possible to determine if they can be changed. It also brings up the question of how would these attacks fare against those changed configurations.
* One other limitation of these attacks is attacker doesn't have fine control over the amount of distance reduction. Although this doesn't necessarily stop attackers from just reducing the distance to less than the threshold to gain access to systems.
* The probability of the success of the attacks can be reduced if the receiver is able to identify outliers as a distance reduction attack but when this is done it might affect the user experience by causing false positives.