"Sampling Race: Bypassing Timing-based Analog Active Sensor Spoofing Detection on Analog-digital Systems"

Target system & service

- an active sensor system composed of an emitter and a receiver
- neither the emitter nor the receiver can be shielded from the external environment to ensure correct operation
- although the sensor output is analog, it will be sampled and quantized into digital form
- the victim system may adopt a regular-channel spoofing detection system (e.g., PyCRA) to detect spoofing attacks against it
- location of the measured entity relative to the sensor is not fixed (e.g. radars, sonars)

Vulnerability

- in PyCRA, the only private information shared between the emitter and the receiver is the timing of the emitter signal level changes.If this information is leaked, the attacker can defeat the challenge-response authentication.
- Since victim system also has a physical delay, it may not notice spoofing signal if an attacker can react faster than the victim can notice. (the delays in victim and attacker systems are in competition)
- If attackers have a sufficiently faster ADC sampling rate than the victim, and the victim's time precision is insufficient to cover the minimal physical delay of the attacker, they can win the competition.
- because PyCRA's authentication is based on the sudden drop of signal levels, attackers can sense the falling edge in challenges issued by the victim and react before the signal level reaches the LOW state.

Exploitation (attacks)

* Simple Detector and the Confusion Phase)

- condition 1: the attacker's physical delay is shorter than the victim's sampling interval
- condition 2: the attacker can detect the falling edge of the challenge
- result: the attacker can react to the challenge before the victim's next sampling moment, bypassing the authentication

* Kai-square detector)

- also can be bypassed for applications where the transition time of the attacker can be reduced below the victim's sampling interval

Evaluation and experimental method

- victim sensor: an IR drop counter installed on a commercial infusion pump
- attacking emitter and receiver: an IR light emitting diode (LED) and an IR phototransistor
- target wavelength: 850 nm ~ 950 nm
- victim and attacker processors: 2 Arduino UNO boards (attacker only: comparator)
- the attacker receives the IR signal from the emitter via optical channel and performs spoofing attack
- the attacker delay can be reduced to 2.8 μs, which is much less than 5 μs, the sampling period corresponding to the 200 kHz sampling rate (taken from the original PyCRA paper)

Defense (potential solutions for the attacks)

- introducing redundancy (adopting not only an identical type of sensors, but also multiple types of sensors)
- tightly shield the actuator, the receiver, and the measured entity so that the measured physical media cannot be penetrated from the outside

Future work

- work on sensor fusion techniques to accommodate the acquired multiple sensor output streams when using redundancy
- design robust and generalizable defense mechanism for active sensors
- since this work showed that there is no generalized and robust authentication, specific security solution is required for each active sensor systems before any new generalizable prevention