This ain't your dose: Sensor Spoofing Attack on Medical Infusion Pump

Youngseok Park[1,2], Yunmok Son[2], Hocheol Shin[2], Dohyun Kim[2], and Yongdae Kim[2]

[1]NAVER Labs
ys.park@navercorp.com
[2]Korea Advanced Institute of Science and Technology (KAIST)
{*yunmok00, h.c.shin, dohyunjk, yongdaek*}*@kaist.ac.kr*

Abstract

Sensors measure physical quantities of the environment for sensing and actuation systems, and are widely used in many commercial embedded systems such as smart devices, drones, and medical devices because they offer convenience and accuracy. As many sensing and actuation systems depend entirely on data from sensors, these systems are naturally vulnerable to sensor spoofing attacks that use fabricated physical stimuli. As a result, the systems become entirely insecure and unsafe.

In this paper, we propose a new type of sensor spoofing attack based on saturation. A sensor shows a linear characteristic between its input physical stimuli and output sensor values in a typical operating region. However, if the input exceeds the upper bound of the operating region, the output is saturated and does not change as much as the corresponding changes of the input. Using saturation, our attack can make a sensor to ignore legitimate inputs. To demonstrate our sensor spoofing attack, we target two medical infusion pumps equipped with infrared (IR) drop sensors to control precisely the amount of medicine injected into a patients' body. Our experiments based on analyses of the drop sensors show that the output of them could be manipulated by saturating the sensors using an additional IR source. In addition, by analyzing the infusion pumps' firmware, we figure out the vulnerability in the mechanism handling the output of the drop sensors, and implement a sensor spoofing attack that can bypass the alarm systems of the targets. As a result, we show that both over-infusion and under-infusion are possible: our spoofing attack can inject up to 3.33 times the intended amount of fluid or 0.65 times of it for a 10 minute period.

1 Introduction

Sensors measure physical quantities and convert those to electrical signals. Many critical systems such as medical devices, drones, and automotive systems are often built as sensing and actuation system, using those sensors to increase their safety and operational accuracy. Sensors also offer great convenience to users by supplying a variety of information in consumer devices such as smartphones and smart refrigerators.

However, sensors can be a threat in terms of security to their sensing and actuation systems because of spoofing attacks. Sensors are fundamentally vulnerable to spoofing attacks because they cannot inherently distinguish between legitimate and maliciously generated stimuli. Furthermore, many sensing and actuation systems are entirely dependent on sensor outputs. Therefore, such systems are vulnerable to sensor spoofing attacks.

In recent years, several attacks against sensors used in sensing and actuation systems have been proposed. Foo Kune et al. show that an attacker can inject a fake sensor signal into a wire in front of an Analog-to-Digital Converter (ADC) by applying an Electro-Magnetic Interference (EMI) [7]. This injection can induce defibrillation shocks in a Cardiac Implantable Electrical Device (CIED) or disable triggering them even in a situation where shocks are necessary. Shoukry et al. introduce a spoofing attack against a wheel speed sensor of an Anti-lock Braking System (ABS) by injecting a magnetic field that cancels out the original magnetic field and injects a fake one [22]. In addition, Son et al. show that a gyroscope in a drone can be abnormally disturbed by high-power sound noise with a specific (resonant) frequency [25]. This disturbance in the gyroscope can make the drone uncontrollable and crash it.

In this paper, we present a new type of a sensor spoofing attack using *saturation* in contrast with the three aforementioned works. Sensors have a typical operating region related to their input and show an unexpected output called *saturation* when operating beyond that region. Within the operating region, a sensor has a linear property where the output value is proportional to its

input stimuli. However, as the input exceeds the upper bound of the operating region, the sensor output is saturated, and does not change as much as the input changes, which makes the output nonlinear. Therefore, if an attacker injects an external high-power signal into a target sensor using the same physical quantity, the sensor will stop responding to any change of environment because of *saturation*. In this way, the attacker can bury the legitimate signal by injecting a spoofing signal into the sensor.

To find out the effects of *saturation* in sensing and actuation systems, we choose medical infusion pumps with a drop sensor as our target systems. Infusion pumps are devices used in hospitals to control precisely the amount of medicine injected into a patient's blood stream. Some infusion pumps use a drop sensor to count drops and thereby measure the exact volume of infused medicines for the patient's safety. The drop sensor detects an object between an infrared (IR) emitter and a receiver by sensing the change of intensity of the received IR ray. By counting drops flowing inside a tube, the infusion pump injects the exact volume accurately and safely.

We investigate two types of infusion pumps and two drop sensors for each for our spoofing attacks. First, we analyze the drop sensors based on the signal generated by the sensors. By tracing the signal, we study the behavior of the drop sensor's output signal. We also discover that the drop sensor is saturated with our IR source and stops sensing the real drops. Our second analysis is targeted on the hardware and software of the infusion pump. By tracing the sensor output signal, we locate the microcontroller unit (MCU) that receives the output from the sensor. On extracting the firmware of that MCU, we discover the drop detection mechanism of the target. We find a vulnerability that while sensing drops, the infusion pump recognizes drops of fluid with only a relative change of the sensor's output. Using this vulnerability, we can simulate fake drops in the drop sensor by changing the intensity of the IR spoofing signal. Finally, with a dynamic analysis using the IR ray, we discover that the infusion rate increases with saturation and decreases with fake drops simulated by spoofing. Using these results, we introduce two spoofing attacks: *over-infusion* and *under-infusion*. The term *over-infusion* means overdosing the patients and *under-infusion* means underdosing him or her. Although there exists an alarm system to sense malfunctions in the drop sensor, we bypass it by designing a proper spoofing pattern based on observations of the dynamic response of the target system. As a result, *over-infusion* allows the infusion pump infuse about 333 % of fluid as compared to the normal operation and *under-infusion* does infuse about 45 % less. In short, we can control the infusion rate of the pump to make it operate faster or slower to a limited degree and this can be a serious threat to a patient's life. We note that this spoofing attack is not easy to detect because the IR ray used for spoofing is invisible.

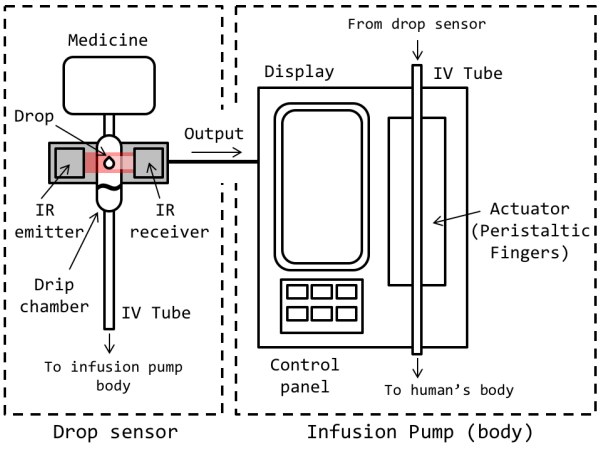


Figure 1: Components of the infusion pump and drop sensor (depicted as gray boxes)

The remainder of this paper is organized as follows. Section 2 provides the background information about the target systems and their sensors. Section 3 describes the hardware and software analyses of the targets. Section 4 explains a simple experiment necessary to design our spoofing attack. Section 5 presents the detailed spoofing attacks and their results. Discussions of this study are presented in Section 6. We summarize existing works related to attacks on medical devices and sensors in Section 7. We conclude this paper in Section 8.

2 Background

2.1 Infusion Pump

Infusion pumps are used to automatically infuse fluids, especially medicines. These pumps can control the rate of infusion to fine-grained levels which cannot be achievable manually, and continuously monitor the infusion without a pause. Though there are various types of infusion pumps, here, we restrict the term, only to pumps for continuous infusion, which can precisely maintain the infusion rate preset by users such as medical staffs.

Some infusion pumps control the infusion rate using only the pump body, but some pumps use an external drop sensor for greater accuracy [9]. Such infusion pumps have two parts: a drop sensor and the pump body (Figure 1). External drop sensor senses the fluid drops infused, and pass the output signal to the pump body. The pump body includes a display, a control panel, and peristaltic fingers operated by motors for pushing the fluid out.

Since its operation is directly related to the lives of pa-

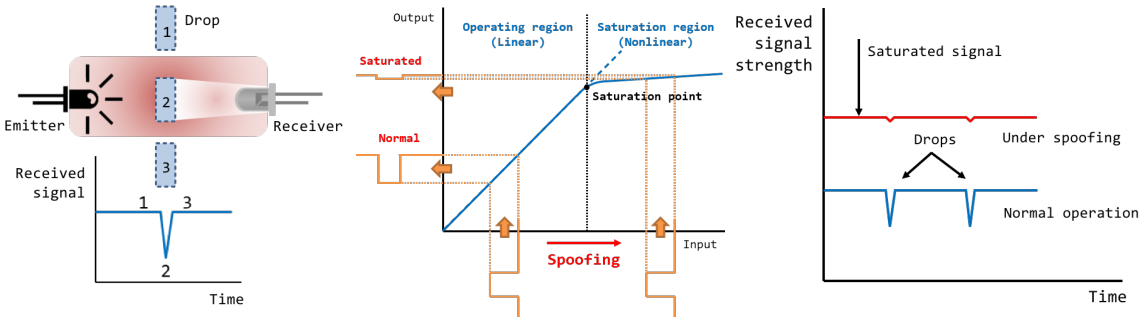


Figure 2: Illustration of (a) drop sensor operation principle, (b) *saturation* effect on the input and output of the sensor, and (c) sensor spoofing attack using *saturation* on the drop sensor. The drop sensor cannot perceive real drops because the signal of drops is buried in the saturated signal.

tients, FDA (the US Food and Drug Administration) has made guidance and recommendations for mitigating and managing the cybersecurity of medical devices [5, 6]. Additionally, there is Conformité Européenne Marking (CE Marking), which is a manufacturer's declaration that the product satisfies the requirements of the European health and safety directives [4, 18]. Safety-critical devices, especially medical devices, must have a CE Marking to be placed on the market in EU [21].

As a result, state of the art infusion pumps are equipped with various safety features to mitigate the threats on them. They are designed to minimize the number of single points of failure [28]. That means they try to cross-validate their operations as much as possible. A drop sensor can be one example for those trying to check an infusion rate, although that can be precisely inferred also by noting the speed of the rotating motors.

For example, Generic Infusion Pump Hazard Analysis and Safety Requirements [8] states that "if the pump is equipped with a flow rate sensor and the flow rate exceeds the programmed rate setting by more than 10% over a period of more than 15 minutes, or if the pump goes into free flow, the pump shall issue an alarm to indicate overinfusion of the patient." It also states about under-infusion as well. However, these statements completely ignore maliciously manipulating flow rate sensor itself, which is the main theme of this paper.

2.2 Drop Sensor

A drop sensor, also known as a drop counter, is used in various applications to measure the exact amount of fluid flowing. Although other measurement methods using an image or a piezoelectric sensor have been introduced [19, 26], most drop sensors usually use an IR ray [17, 27] to sense the drop of fluid because of its low cost and simple structure. In case of the infusion pump, with an IR emitter and a receiver facing each other, the drop sensor can help the infusion pump to calculate the exact volume of fluid passing through, by counting the number of drops between them. Because the volume of each drop varies according to the diameter of the tube of an intravenous (IV) set, the volume of each drop must be specified beforehand [11]. Figure 2a illustrates the basic operational mechanism and the output signal of the drop sensors. As a drop falls down in the drip chamber (marked as 1 in Figure 2a), it blocks and absorbs the IR ray between the emitter and the receiver (marked as 2 in Figure 2a). This causes a change in the light intensity as observed by the drop sensor. Although it is possible to perform infusion without it, a drop sensor is frequently used for a more accurate infusion.

2.3 Sensor Saturation

All sensors have a typical operating region corresponding to their input signal. As shown in Figure 2b, the output of a sensor is proportional to its input in the operating region, preserving linearity. However, if the input exceeds a certain point, i.e., *the saturation point*, the output signal cannot reflect the variation in the input any more, and that makes the output nonlinear. Using this nonlinearity, an attacker can virtually blind the target sensor by saturating it with the spoofing signal as shown in the Figure 2c. Here, an attacker can reduce the height of the notches generated by real drops with his or her signal to prevent the victim sensor from sensing existing drops. To do this when the victim sensor is not saturated, the attacker 1) must know the exact instant and the amount of the reduced intensity of the IR ray when the real drop passes through, and 2) fill that notch in that time with the exact intensity of the IR ray. Therefore, this is not trivial. However, when the attacker has once saturated the victim sensor, he or she can successfully disturb drop detection

(a) (b) (c) (d)

Figure 3: (a) One of target drop sensors used on Pump1 (installed), (b) Internal structure of the drop sensor, (c) IR filter used to block external optical interferences, and (d) Four wires connected between the drop sensor and the infusion pump body (the right side of the board). Note that drop sensors of Pump1 and Pump2 are mostly identical in their internal structures.

because the victim sensor is now blind to any external variations.

2.4 Sensor Spoofing Attack

Spoofing attack is a term usually used in network security which denotes masquerading as legitimate users with forged data like Internet Protocol (IP) address in TCP/IP and caller ID spoofing in voice over IP. In the context of sensors, a spoofing attack is the injection of a deceiving physical signal into a victim sensor. Without any defensive measures, the victim sensor accepts every received signal, trusting it as legitimate. This eventually leads to the malfunction of the systems connected to the victim sensor.

3 System Analysis

As target systems, we chose two off-the-shelf infusion pumps equipped with different drop sensors: JSB-1200 [20] and BYS-820 [3] manufactured by *JYM Medical Technology* and *Chansha Beyond Medical Devices*, respectively. Note that both infusion pumps have an ISO 13485:2012 [14] and CE 0197 certification [4] guaranteeing the safety of medical devices, while conforming to EU standards. We call the JSB-1200 as *Pump1* and the BYS-820 as *Pump2* in the rest of the paper.

To understand the operational mechanism of the drop sensor and the infusion pump, and to design our sensor spoofing attack, we analyzed the target systems, performing a hardware, software, and dynamic analysis. In this section, we focus on Pump1, analyzing the sensing mechanism of the target drop sensors and the mechanism the infusion pump use for precessing the sensor outputs, because these two pumps and drop sensors have a similar appearance and an operational mechanism. In addition, in Section 4, we show a dynamic analysis results for observing the reactions of both of the infusion pumps with an IR ray.

3.1 Hardware Analysis

Drop Sensor Analysis: Figure 3 shows the internal structures of the drop sensor of Pump1. To sense drops (i.e., to block the IR ray between the IR emitter and receiver by falling drops), a transparent drip chamber has to be clamped by the drop sensor as shown in Figure 3a. The IR ray generated by the IR emitter (on the left side in Figure 3b) is guided to the IR receiver (on the right side in Figure 3b) via two narrow slits facing each other. On the rear side of the receiver-side slit, a mirror-like IR filter (Figure 3c) is placed before the IR receiver. This IR filter helps to protect the IR receiver from external interferences such as from a visible ray of light. However, spoofing using additional IR source with the same wavelength is still possible and it remains undetected by the medical staffs or the patients because of the invisibility of the IR ray. Figure 3d shows an interface between the drop sensor and the infusion pump. Four wires marked as *GND*, *IN*, *LED*, and *VCC* comprise the interface. Among the four wires, *VCC* and *GND* are used for supplying power to the drop sensor, and *LED* provides a signal to make a green LED blink, which indicates that the sensor detects a falling drop. Lastly, *IN*, our main focus for analysis, is for transmitting the analog output signal of the drop sensor to the infusion pump. Therefore, we used an oscilloscope and analyzed the signal on the *IN* wire under various conditions.

Infusion Pump Analysis: To trace the signal transmitted on the *IN* wire, we tore down Pump1 and manually analyzed its mainboard. As a result, we could trace the main hardware structure related to the output of the drop sensor. This structure is described in Figure 4. On the mainboard, there are two MCUs: AT89S52 [1] and W78E516D [29] manufactured by *Atmel* and *Nuvoton*, respectively.

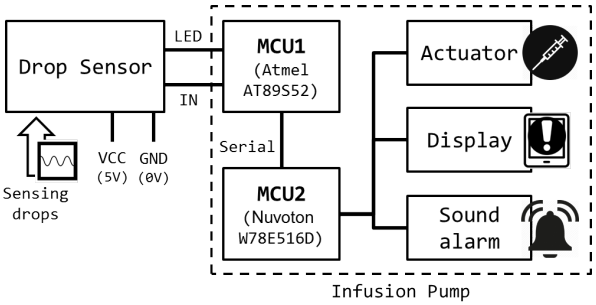


Figure 4: Main structure of Pump1 considering the sensor output (Output of the drop sensor is fed into MCU1. In MCU1, it is transformed into a serialized digital signal and transmitted to MCU2 which controls the infusing motor and alarm systems.)

The analog output from the drop sensor (i.e., the signal on the *IN* wire) is connected to an 8-bit ADC, which converts the analog signal to an 8-bit digital signal. In the ADC, the input voltage level from 0 V to 5 V is represented as 8-bit digital data from `0x00` to `0xFF`. By a simple test for input and output of this ADC, we found that the exact quantization level of this system is 0.02 V (e.g., 0.32 V of the analog input is digitized to `0x10`). The first MCU, AT89S52, interprets the quantized output from the drop sensor and detects drops based on a drop detection algorithm that we will explain in Section 3.2. When the algorithm detects a drop, the first MCU generates a specific 8-bit data (`0x11`) and transmits it to the second MCU, W78E516D. The second MCU is directly connected to and controls peripherals such as an infusing motor, display, and an alarm speaker.

Firmware Extraction: To know how the 8-bit digitized output of the drop sensor affects to the infusion pump, we tried to extract the firmware from the two MCUs. For the first MCU, we successfully dumped its firmware via the Serial Peripheral Interface (SPI) bus which is located nearby. We used a commercial USB-ISP device as a hardware interface and AVR Studio 4, a software tool provided by *Atmel* to develop firmware for *Atmel* processors. *Atmel* processors support a function for read protection by setting specific fuses at the end of development, but these fuses were not set in this case.

On the contrary, for the second MCU, the firmware extraction was failed because of the lack of an interface and a proper software tool. Therefore, we had to analyze the pump dynamically to deduce the operation of the second MCU when actuating the peripherals. We present the results of the dynamic analysis in Section 4.

Algorithm 1: Simplified drop detection algorithm in the 1st MCU, AT89S52, of Pump1

Input: The 8-bit digitized data of the drop sensor
Output: Two flags for drop detection and alarm
Output: The 8-bit data for the 2nd MCU, W78E516D

```
1  Initializing Maximum, Minimum, and Average;
   Loop For every 500 us
2      if No drop is detected for 60 ms then
3          if Input < Average − 0x10 then
               // When the voltage drop higher
                  than 0.32 V occurs
4              Set the drop detection flag
5              Send 0x11 to the 2nd MCU
6              break;
7          end
8      end
9      if Input < Minimum then
10         Minimum = Input;
11     end
12     if Input > Maximum then
13         Maximum = Input;
14     end
15     if Maximum − Minimum >= 0x05 then
           // Reset the minimum and maximum
              values when the voltage change
              is higher than 0.1 V
16         Maximum = Input;
17         Minimum = Input;
18         break;
19     else
20         Average = (Maximum + Minimum)/2;
21         if Average < 0x08 then
               // The average value is lower
                  than 0.16 V (i.e., the drop
                  sensor is blocked)
22             Set the blocking alarm flag
23             Send 0x41 to the 2nd MCU
24         end
25         break;
26     end
27 EndLoop
```

3.2 Software Analysis

The extracted firmware from the first MCU is based on the Intel HEX format [13]. This format uses a simple structure for transmitting a binary file through a serial communication channel without non-ASCII characters. After converting the firmware to its original format, we analyzed it using the IDA Pro. The firmware is composed of 8051 instruction sets, and we analyzed it by tracing the pin connected to the output of the ADC. The name of the

pin is specified in the datasheet of the first MCU, and the IDA Pro supports the naming for each pin by default. With manual analysis, we figured out the algorithm for sensing drops and this is described in Algorithm 1.

Algorithm 1 detects drops and sets two flags (the drop detection flag and the blocking alarm flag) based on the digitized output of the drop sensor. At the beginning of this algorithm, after initializing the *maximum*, *minimum*, and *average* values, a loop is executed every 500 us with the help of a timer interrupt. In the loop, if at least 60 ms is passed after the last drop, and the voltage decreases more than 0.32 V from the *average* (line 2, 3), the infusion pump regards this voltage variation as the presence of a drop. In other words, the pump just detects drops based on only the relative alteration of the sensor output. When a drop is detected, the first MCU sets the drop detection flag and sends `0x11` to the second MCU (line 4, 5). If the drop detecting condition is not met (line 2, 3), the *maximum* and *minimum* values are updated (line 9–14), and the *average* value is set as the arithmetic mean of the *maximum* and *minimum* (line 20). However, to detect the voltage drop, the *average* should be derived when the signal is stable. Therefore, the pump checks the signal stability before calculating the *average*, and resets the *maximum* and *minimum* when the signal is unstable (line 15–18). Additionally, if the *average* value is lower than 0.16 V, the system sets the alarm flag and sends a `0x41` to the second MCU (line 21–24), because this situation can be considered that a physical obstacle is blocking the IR ray inside the drop sensor.

3.3 Summary and Vulnerability

To sum up, the drop sensor transmits the output voltage signal to MCU1. The MCU1 detects the voltage drop caused by drops in the drip chamber and sends its data to MCU2. More importantly, the infusion pump detects drops based only on the relative changes of the drop sensor's output voltage. Moreover, there is no mechanism for detecting an external signal or sensor saturation in both the hardware and software of the target systems. Thus, an attacker will be able to affect the sensor output by injecting the IR ray into the drop sensor's receiver. Experimental results with the external IR ray will be presented in Section 4.

4 Experiment

As analyzed in the previous section, an infusion pump would be deceived by a sensor spoofing attack on the drop sensor because of its vulnerability in drop detection mechanism. In this section, we present the results of our preliminary experiments in investigating whether or not the target systems are affected by our spoofing attack.

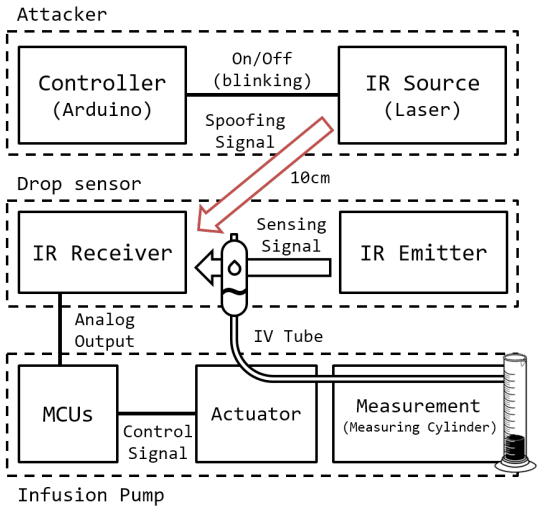


Figure 5: Setting for our experiments

4.1 Experimental Setup

The settings of our experiments (Section 4 and 5) are shown in Figure 5. Infusion pumps and drop sensors are generally installed with an IV set. An IR laser with wavelength of 905 nm and power of 30 mW [12] was aimed at the IR receiver of the drop sensor. In our experiments, the distance between the IR laser and the IR receiver of the drop sensor was about 10 cm for convenience, and a detailed discussion about the spoofing distance is available in Section 6. To turn on and off the IR source, we used an Arduino board as a controller. To see the effect of our spoofing attack, we measured the output voltage of the drop sensor (i.e., the *IN* wire) and the signal between the two MCUs using an oscilloscope. We also used a measuring cylinder at the end of the IV set for measuring and evaluating the amount of the fluid infused. Note that we used a low-cost IR laser and other devices available in online markets. Results of the experiments are summarized in Table 1.

4.2 Simple Spoofing

Saturation: As mentioned in Section 2, saturation is caused by a nonlinear characteristic of the sensor. When we injected IR rays into the receivers of the drop sensors, both drop sensors were saturated and could not sense drops any more. As the drop sensor is already saturated by the attacker's signal and the IR has a physically additive property, changes in IR intensity by real drops cannot make any difference to the output voltage of the drop sensor (Figure 6a). As a result, while the sensor remains saturated, the infusion pump lets fluid flow faster than the infusion speed set by a user because it perceives that

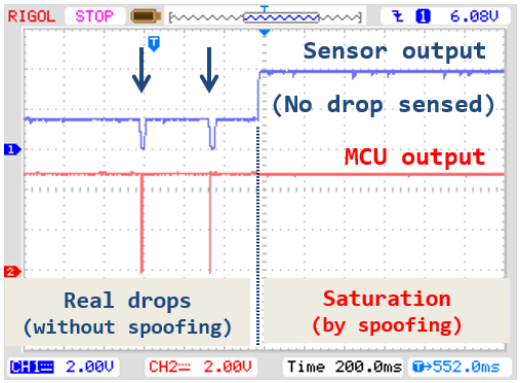
Table 1: Experimental findings of simple spoofing for two infusion pumps

Infusion pump	Experimental findings
Pump1 (JSB-1200)	• *Saturation* can be maintained for 13 seconds continuously without alarm. • *Saturation* occurs for preset infusion rates under 76.5 mL/h. • During *saturation*, the measured actual rate is about 180 mL/h. • The minimum interval of *fake drops* is 4.2 seconds without alarm.
Pump2 (BYS-820)	• *Saturation* affects only the drop sensor successfully (not the system). • Until the interval of *fake drops* decreased to 0.5 seconds, no alarm generated.

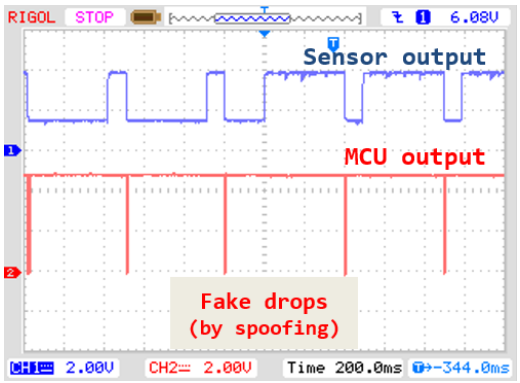
there is no drop in the drip chamber, resulting in *over-infusion*. From iterative experiments, we noticed that Pump1 infuses at the rate of 180 mL/h when its sensor is in saturation. However, this was applicable only to the rate below 76.5 mL/h and there was no change in the infusion rate over 76.5 mL/h. Additionally, in case of Pump1, the system detected the abnormal state and generated an alarm when we maintained saturation over 13 seconds. On the other hand, for Pump2, the drop sensor was saturated, but the infusion speed was not affected by saturation. As a result, both drop sensors were fooled by our spoofing attack, but the actuation of each infusion pump was different according to its operation or implementation.

Fake Drop: The result of our analysis in Section 3 shows that the infusion pump detects drops only by voltage drops in the output signal of the drop sensor. This means that if an attacker can generate falling edges in the drop sensor's output, fake drops could be introduced. As shown in Figure 6b, when we generated fake drops by injecting saturating signal and stopping it to generate fake drops, the MCU sends the signal meaning that the drop is detected. As a result of injecting fake drops, both infusion pumps slow down the speed of infusion because the pumps perceive sufficient drops are already falling, resulting in *under-infusion*. However, too many fake drops can be considered as an abnormal situation and this generates an alarm. When the interval of fake drops was less than 4.2 seconds, Pump1 generated an alarm. In the case of Pump2, we checked until the interval was down to 0.5 seconds, but there was no alarm.

Because some of the experiments caused alarms to be generated, this simple spoofing does not qualify for use as a spoofing attack in the real world. However, the results in Table 1 provide us a definite evidence of the possibility for a sensor spoofing attack. Moreover, by properly composing them, we can design patterns for a spoofing signal for *over-infusion* and *under-infusion* (caused by saturation and fake drops) that can avoid the target system's alarm mechanism.



(a)



(b)

Figure 6: Drop sensor's output after simple spoofing: (a) by saturation (For the duration of saturation, no drop is sensed.) and (b) fake drops (When falling edges are injected, fake drops are sensed.)

5 Spoofing Attack

In Section 4, we checked how the target infusion pump reacts to our spoofing attack. As a result, the drop sensor is saturated with our spoofing signal and does not sense drops anymore, while the MCU in the infusion pump detects spurious drops whenever we generate voltage drops in the output of the drop sensor. Additionally, there is an alarm system in the infusion pump which indicates an abnormal status of the drop sensor. In this section, we present a detailed implementation of our spoofing attack bypassing the alarm system and its results.

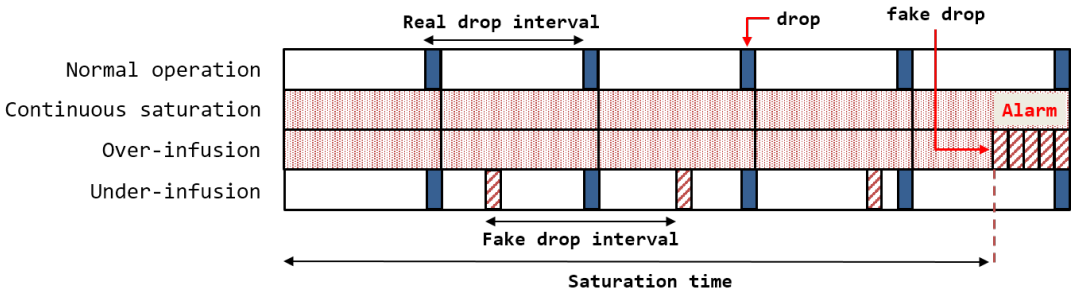


Figure 7: Spoofing attack pattern for bypassing alarm mechanism in the infusion rate of 60 mL/h. The alarm can be bypassed by mixing saturation and fake drops. The fake drops compensate for the drops that are not sensed during the saturation period.

5.1 Bypassing the Alarm

To bypass the alarm system of the infusion pumps, we designed a spoofing pattern causing saturation for a specific period and compensating an insufficient number of drops missed due to saturation by fake drops during the next short period immediately after. We hypothesized that the infusion pump senses abnormal states by counting the number of drops in a specific time interval and the following experimental results show that our hypothesis is true.

Figure 7 presents our spoofing attack pattern to bypass the alarm system. Note that we have used an IV set with a specification of 20 drops/mL which is commonly used in hospitals. This means that a drop falls every 3 seconds in a 60 mL/h setting. The first row in Figure 7 shows the normal operation of the infusion pump where a drop falls regularly. The second row indicates the situation of an alarm being generated by the persistent spoofing attack causing saturation. When saturation is sustained, the infusion pump senses the abnormal operation of the drop sensor and stops the infusion, while generating an alarm. Next, we experimentally figured out that the upper limit of the saturation time is 13 seconds, with no alarm being generated in this time, causing *over-infusion*. This is shown in the third row of Figure 7. Because there should be five drops in 15 seconds at the 60 mL/h infusion rate, we need to make the infusion pump perceive that there is no error by compensating with five drops for the next 2 seconds. For other infusion rates, we adjusted the number of compensative fake drops to be proportional to the rate. Additionally, we also succeeded *under-infusion* by introducing fake drops in a certain interval such as in the fourth row of Figure 7. By changing the saturation time or the interval of fake drops, we could as well control the injected volume to a limited degree.

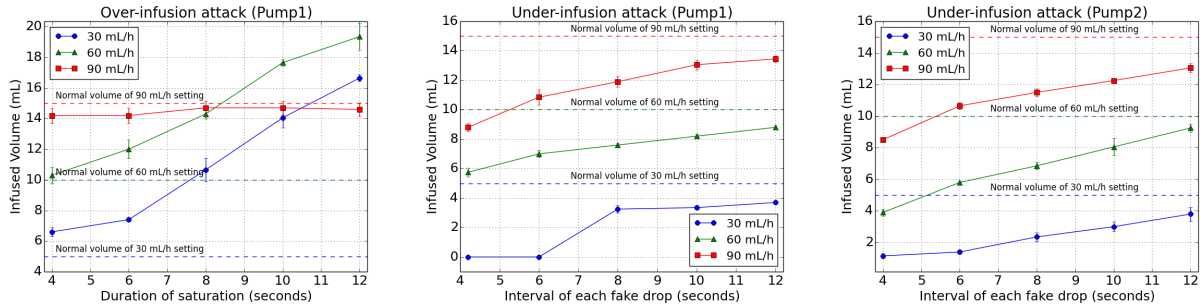
5.2 Over- and Under-infusion

Figure 8 shows the results of *over-* and *under-infusion* based on various infusion rates. Each experiment proceeded five times and data in the graph is an average and a standard deviation of them. Expected volumes for 30, 60, and 90 mL/h infusion rate in 10 minutes are 5, 10, and 15 mL, respectively. For Pump2, because the system did not react to saturation, only *under-infusion* attack was performed.

Over-infusion: As we mentioned in Section 4.2, the upper limit of the saturation time not trigerring the alarm is 13 seconds. Figure 8a shows the relationship between the infused volume and the saturation time for 10 minutes. For the 30 mL and 60 mL infusion rate, the infused volume proportionally increases with an increase in the saturation time. Because the infusion rate in the saturation time is 180 mL/h (Table 1), the longer saturation time leads to more infusion. For 30 mL, the infused volume increases up to about 18 mL compared to 5 mL in the normal operation. However, the spoofing attack did not work on the rate of 90 mL/h because Pump1 did not react to saturation for the rates above 76.5 mL/h.

Under-infusion: Generating fake drops in the drop sensor made the infusion pump inject less fluid. The results of spoofing attacks using *under-infusion* against two infusion pumps are displayed in Figure 8b and 8c. Contrary to Pump2, the spoofing attack against Pump1 at 30 mL/h failed in 4 and 6 seconds of intervals followed by the alarm. Except for these cases, both graphs show a similar relationship between the intervals of fake drops and the infused volume of fluid. Although the infused volume of the two infusion pumps is different, in both, a shorter interval between the fake drops results in reduced infusion. The result of Pump1 shows that the infused volume decreases to about 6 mL during the 60 mL/h infusion rate.

To conclude, we could control the infused volume for



(a) (b) (c)

Figure 8: Infused volume of fluid according to the saturation time or fake drop interval for different preset of infusion rates. By changing the saturation time and fake drop interval, the infused volume can be controlled. (a) and (b) shows the results of *over-* and *under-infusion* for Pump1, and (c) shows the result of *under-infusion* for Pump2. In all cases, the spoofing was maintained for 10 minutes.

both *over-* and *under-infusion* with a few limitations. In case of the 60 mL/h rate, fluid was over-infused to about twice and under-infused to about a half of the amount infused in normal operation.

6 Discussion

In this section, we discuss the possible range of our spoofing attack and mitigation methods against a sensor spoofing attack.

6.1 Spoofing Distance

In order to spoof a drop sensor, using an IR laser is appropriate because a laser maintains its intensity over a long distance. However, a laser also has a limited effective range called a near field when the laser beam is on focus [24, 16]. In the far field which is beyond the near field, the intensity of a laser beam decreases as a square of the distance from the near field. Additionally, the power of a laser maintains its intensity only to an effective distance and this distance is related to the power of a laser. If the laser power quadruples, the effective distance doubles. A laser with a 500 mW and above has an effective distance of a few hundred meters, and that can hazard to eyes [15].

We succeeded in spoofing from a range of 12 meters using a 30 mW, low-cost IR laser pointer. Although the distance presents a difficulty in aiming at the target because the beam diameter of the laser is too small, an attacker can spoof sensors at longer distances if he or she utilizes a powerful enough laser.

6.2 Mitigation

Existing mitigative approaches against sensor spoofing attacks can have two largely independent factors: detection and prevention capabilities. First, a drop sensor with only detection capability cannot prevent spoofing attacks from affecting its output. Instead, it detects spoofing attempts, so that the victim device can take available defensive measures such as generating an audible alarm. On the other hand, a drop sensor only with prevention capability cannot sense the existence of spoofing attempts targeting it. However, it is immune to such attacks to some extent, which make the sensor output remain unaltered even under spoofing. Here, we list several detection and prevention approaches drop sensors can take to mitigate sensor spoofing attacks against them.

Detection: Under its normal operating condition, the receiver on a drop sensor is exposed to a constant maximum light. The light intensity is at its maximum in the absence of any drops, because fluid drops reduce the light intensity by blocking or absorbing the light passing through them. Therefore, by checking whether the light intensity exceeds the preset maximum level, all attack attempts using saturation can be detected.

Another detection method named PyCRA was recently published [23]. PyCRA is a spoofing detection scheme for active sensors composed of an emitter and a receiver similar to the drop sensor. PyCRA detects spoofing attempts by turning off the transmitter at random instants. Without a spoofing signal, the receiver should receive nothing when the transmitter turns off. If there is a signal in the receiver when the transmitter is turned off, however, PyCRA regards it as a spoofing attack. Because the presented attack does not monitor the emitted signal from the target drop sensor, PyCRA can be applied to detect spoofing attempts against drop sen-

sors.

Prevention: Physical isolation can be the simplest solution for close range applications to prevent spoofing attacks, because it can completely block external stimulation. Therefore, a spoofing signal cannot affect the receiver as long as the physical isolation is well established. However, even if physical isolation can fundamentally protect the sensor inside against spoofing attempts, it increases production cost because it requires additional hardware for establishing the isolation.

7 Related Works

The method of sensor spoofing attack has been studied recently. As this study focuses on applying newer type of sensor spoofing attacks on medical devices, we categorized the related works into two groups; sensor spoofing attack and medical devices security.

Sensor Spoofing Attack: Sensors are devices to measure the ambient energy or a property of the target. Sensors generally have an open structure to accept signals or physical quantities from the outside and this enables attackers to manipulate the sensor's output. Work by Son et al. [25] focused on spoofing a MEMS gyroscope sensor using an intentional sound interference. As MEMS gyroscopes have a resonant frequency, attackers can abnormally disturb the gyroscope on drones, making them uncontrollable and crashing them. Moreover, Shoukry et al. introduced a study about spoofing an Anti-lock Braking System by injecting a magnetic field that cancels out the real signal and then injects the malicious signal [22]. By injecting the malicious signal, they showed that the ABS wheel speed sensor can be deceived by the spoofing signal. These works relate to spoofing the sensor by a side-channel or canceling the real signal and injecting the malicious signal. In contrast, our work focuses on a spoofing with physical quantity that cannot be canceled out. Instead of canceling the legitimate signal out, we saturate the sensor to blind it.

Medical Devices Security: Security threats on medical devices can be lethal because these devices are used for therapy on patients. Therefore, several works on security of medical devices have been introduced to decrease threats in medical devices. Barnaby Jack introduced the vulnerability of wireless insulin pumps, containing a tiny radio transmitter to allow users to adjust their functions without knowing the insulin pump ID [2]. He made a program to scan the insulin pumps' ID nearby, and exploited their vulnerabilities such as letting the pump repeatedly deliver its maximum dose. In addition, Halperin et al. exploited the vulnerabilities in the digital control channel used to communicate with implantable medical devices (IMDs), by implementing several software radio-based attacks that could compromise the patient's safety and privacy [10]. However, this work was related to intercepting and attacking the implantable cardioverter defibrillator (ICD) communication, and not to spoofing a specific sensor. Foo Kune et al. presented that CIED can be spoofed by injecting EMI into a wire in front of the ADC [7]. This injection could induce defibrillation shocks in a Cardiac Implantable Electrical Device (CIED) or disable its triggering even in a situation where shocks are necessary. Again, because malfunctioning medical devices can expose patients to danger, the security and safety on those devices must be considered.

8 Conclusion

In this paper, we performed a sensor spoofing attack against an IR drop sensor existing in medical infusion pumps. We statically analyzed the hardware and software and found that there are two vulnerabilities in the target system. The first is caused by a nonlinearity of the sensor itself, and the other is a fault in the drop detection algorithm. Because the drop sensor has an open structure to receive signals from the emitter, attackers can inject their signals externally. With this structural problem and the vulnerabilities, we succeeded in changing the dosage amounts by spoofing the drop sensor. Although there are alarm systems for the safety of the patient, we bypassed the alarms with specific spoofing patterns based on the dynamic analysis. As a result, we could control the infusion rate of the infusion pump to a certain degree by operating it faster or slower than its speed in normal operation. Because saturation is a natural characteristic of sensors, many other sensing and actuation systems may also have similar vulnerabilities which can create serious issues in the safety-critical systems. However, there has been no serious consideration to detect and prevent sensor spoofing attacks. We also discuss possible mitigation approaches as well.

Acknowledgements

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (No.B0717-16-0109, Building a Platform for Automated Reverse Engineering and Vulnerability Detection with Binary Code Analysis).

References

[1] AT89S52 Datasheet. `http://www.atmel.com/images/doc1919.pdf`. [Online; accessed 10-2016-May].

[2] Barnaby jack could hack your pacemaker and make your heart explode. http://www.vice.com/read/i-worked-out-how-to-remotely-weaponise-a-pacemaker, 2013. [Online; accessed 10-2016-May].

[3] BYS-820. http://en.csbeyond.com/products_detail/&productId=30.html#. [Online; accessed 10-2016-May].

[4] Committee European Marking. http://ec.europa.eu/growth/single-market/ce-marking/index_en.htm. [Online; accessed 10-2016-May].

[5] FDA Infusion Pumps. http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/GeneralHospitalDevicesandSupplies/InfusionPumps/default.htm. [Online; accessed 9-May-2016].

[6] FDA Medical Device Cybersecurity. http://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm. [Online; accessed 9-May-2016].

[7] FOO KUNE, D., BACKES, J., CLARK, S., KRAMER, D., REYNOLDS, M., FU, K., KIM, Y., AND XU, W. Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors. In *IEEE Symposium on Security and Privacy* (May 2013), pp. 145–159.

[8] Generic Infusion Pump Hazard Analysis and Safety Requirements Version 1.0. http://repository.upenn.edu/cgi/viewcontent.cgi?article=1938&context=cis_reports. [Online; accessed 16-2016-May].

[9] Generic PCA Infusion Pump Reference Implementation. https://rtg.cis.upenn.edu/medical/gpca/rtg_gpca_video_v1.html. [Online; accessed 10-2016-May].

[10] HALPERIN, D., HEYDT-BENJAMIN, T. S., RANSFORD, B., CLARK, S. S., DEFEND, B., MORGAN, W., FU, K., KOHNO, T., AND MAISEL, W. H. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In *Security and Privacy, 2008. SP 2008. IEEE Symposium on* (2008), IEEE, pp. 129–142.

[11] HILLMAN, M. R. The prediction of drop size from intravenous infusion controllers. *Journal of Medical Engineering & Technology 13*, 3 (1989), 166–176.

[12] Focusable Infrared Laser Diode Module with 905nm 30mw. http://www.ebay.com/itm/INDUSTRIAL-Focusable-905nm-30mW-Infrared-IR-Laser-DOT-Diode-Module-TTL-100khz-/120948669358?hash=item1c291a3bae:g:xSkAAOSw~oFXIy0-. [Online; accessed 9-May-2016].

[13] Hexadecimal object file format specification. http://microsym.com/editor/assets/intelhex.pdf, 1998. [Online; accessed 10-2016-May].

[14] ISO 13485. http://www.iso.org/iso/iso13485. [Online; accessed 15-2016-May].

[15] Laser hazard distance chart. http://www.lasersafetyfacts.com/hazard_distance_chart.html. [Online; accessed 9-May-2016].

[16] Laser systems for optical microscopy. http://www.olympusmicro.com/primer/techniques/microscopylasers.html. [Online; accessed 9-May-2016].

[17] LAWLER, C. Drop volume measurement system, Apr. 11 1989. US Patent 4,820,281.

[18] Medical Devices Guidance in EU. http://ec.europa.eu/growth/sectors/medical-devices/guidance/index_en.htm. [Online; accessed 15-2016-May].

[19] PEKKARINEN, M., WOLF, L., AND WOODWORTH, W. Indirect piezoelectric drop counter and method, Apr. 22 1986. US Patent 4,583,975.

[20] Peristaltic pump infusion pump (jsb-1200). http://www.made-in-china.com/showroom/jymp umplisha/product-detailEXAmZfvcHnWd/China-Peristaltic-Pump-Infusion-Pump-JSB-1200-.html. [Online; accessed 10-2016-May].

[21] Placing on the market of Medical Devices. http://ec.europa.eu/consumers/sectors/medical-devices/files/guide-stds-directives/placing_on_the_market_en.pdf. [Online; accessed 15-2016-May].

[22] SHOUKRY, Y., MARTIN, P., TABUADA, P., AND SRIVASTAVA, M. Non-invasive Spoofing Attacks for Anti-lock Braking Systems. In *Cryptographic Hardware and Embedded Systems*. Springer, 2013, pp. 55–72.

[23] SHOUKRY, Y., MARTIN, P., YONA, Y., DIGGAVI, S., AND SRIVASTAVA, M. PyCRA: Physical Challenge-Response Authentication For Active Sensors Under Spoofing Attacks. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (2015), ACM, pp. 1004–1015.

[24] SIEGMAN, A. Defining, Measuring, and Optimizing Laser Beam Quality. *Proc. SPIE 1868* (1993), 2–12.

[25] SON, Y., SHIN, H., KIM, D., PARK, Y., NOH, J., CHOI, K., CHOI, J., AND KIM, Y. Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors. In *24th USENIX Security Symposium* (2015), pp. 881–896.

[26] SONG, Q., ZHANG, G., AND QIU, Z. Drop growth monitoring and drop volume measurement based on image drop analysis with ccd. *Instrumentation Science & Technology 31*, 1 (2003), 1–13.

[27] SUGISAKI, Y., TAKADA, M., TOKUDA, K., SUZUKI, Y., OYA, T., TOMEBA, S., AND YOSHIDA, S. Device for controlling liquid dropping, May 9 1989. US Patent 4,827,970.

[28] US FOOD AND DRUG ADMINISTRATION. Infusion pumps total product life cycle: Guidance for industry and fda staff. *Food and Drug Administration Standard* (2014), 910–766.

[29] W78E516D Datasheet. http://www.nuvoton.com/opencms/system/modules/com.thesys.opencms.nuvoton/pages/download/download.jsp?file=http://www.nuvoton.com/hq/resource-download.jsp?tp_GUID=DA00-W78E516D-058D&version=1.9. [Online; accessed 10-2016-May].