Protecting COVID-19 Vaccine Transportation and Storage from Analog Cybersecurity Threats

Yan Long, Sara Rampazzi, Takeshi Sugawara, and Kevin Fu

Protecting the global human population against COVID-19 depends on complex logistics and transportation of vaccines, often at unusually low, cryogenic temperatures. Moreover, malicious cybersecurity actors, both individuals and nation states, exist and have disrupted the vaccine supply chain.[1,2]

In January 2021,a large U.S. healthcare system asked for help to protect its refrigeration systems from radiofrequency (RF)-based analog cybersecurity threats against the temperature sensors used in COVID-19 vaccine cold chain transportation and storage. It is well known in the security research community that intentional electromagnetic interference (EMI) can not only disrupt but also control the output of temperature sensors.[3,4]

With the goal of assessing potential RF-based risks facing COVID-19 vaccine cold chain and deriving accessible methods for protection, the authors conducted experimental and theoretical analyses that led to the following lessons learned:

1. The experiments confirmed that EMI can disturb temperature sensors in cryogenic freezers.
2. Precautions of simple physical and administrative controls can considerably reduce the risk of electronic tampering of the vaccine cold chain transportation and storage to ensure safety and effectiveness.
3. Interdisciplinary research between the fields of biomedical engineering and embedded security results in discoveries that protect the health and safety of patients.

Multiple reports indicated that the U.S. quarantined more than 3,000 doses from Pfizer and 16,000 doses from Moderna vaccine shipments after the sensors reported unexplained anomalies in temperature readings.[5–7] During this event, which at the time of this writing remained under investigation, a question arose of how to defend sensors from potential analog cybersecurity threats.

Cybersecurity exploits can cause sensors monitoring the vaccine temperatures to detect falsely higher and/or lower readings, leading to deceptively incorrect excursions from critical temperature ranges. To ensure public confidence in the efficacy of the vaccines, it's important that cooling and monitoring systems operate within correct temperature ranges, even when sensors are malfunctioning or subjected to the threats. Moreover, automated regulatory compliance based on sensor readings could cause unintended, self-inflicted disruptions to the supply chain: Vaccines with temperature excursions in sensor readings are required to be recalled and analyzed by the manufacturer,[5,8] causing further disruption to a vaccine in short supply.

The Threat

Intentional EMI used against off-chip temperature sensors has been shown to affect sensor readings and thus disrupt the temperature monitoring and control of commercial devices that use such sensors. For example, research has shown that intentional EMI can be used to change the temperature readings of an infant incubator from a distance of 5 m or induce a temperature excursion of up to 40°C in a shielded hybridization oven used in laboratories.[3]

The susceptibility of these devices depends on various factors, including the signal-conditioning circuit used to process the sensor signal and convert it into readable values for the users, the electronic components and materials used to fabricate the sensors, and the control system that regulates the behavior of the device in the case of closed-loop systems. These types of vulnerable temperature sensors also are widely used in vaccine

***Yan Long**, BSc, is a doctoral student and graduate student research assistant in the Department of Electrical Engineering and Computer Science at the University of Michigan in Ann Arbor, MI. Email: yanlong@umich.edu*

***Sara Rampazzi**, PhD, is an assistant professor in the Department of Computer and Information Science and Engineering at the University of Florida in Gainesville, FL. Email: srampazzi@ufl.edu*

***Takeshi Sugawara**, PhD, is an associate professor in the Department of Informatics at the University of Electro-Communications in Tokyo, Japan. Email: sugawara@uec.ac.jp*

***Kevin Fu**, PhD, is an associate professor in the Department of Electrical Engineering and Computer Science at the University of Michigan in Ann Arbor, MI. Email: kevinfu@umich.edu*
Corresponding author

cold chain transportation and storage.[9,10] Digital temperature loggers, which contain such sensors, are suggested by the Centers for Disease Control and Prevention (CDC) for COVID-19 vaccine handling.[8]

These sensors consist of sensing units made of thermocouples, resistance temperature devices, or thermistors that transduce temperatures to electric signals. Subsequent signal conditioning circuits then convert the electric signals (voltages) into digital temperature readings (numbers). The threat arises because EMI can cause electric distortions on the wires between temperature sensors and embedded computer systems.

Today, embedded systems cannot distinguish between the authentic electric signals generated by the temperature and those by intentional EMI. Thus, the embedded computer systems will unknowingly accept false temperature readings from sensors fooled by intentional EMI. In other words, a malicious party can use EMI to drive the temperature readings for the vaccines higher or lower than its real value and cause false temperature excursions. Because EMI essentially refers to radio waves that can penetrate walls, malicious parties may launch this attack stealthily by generating EMI even in a different room from where vaccines are kept.

Sensor device manufacturers typically use methods such as metal shielding of the circuits and sensor probes to reduce the susceptibility to the interference. However, the real-world effectiveness of these practices is difficult to predict. The authors conducted preliminary tests of popular digital temperature loggers from two manufacturers that meet manufacturing practices and guidelines for cold chain transportation (one compliant with the EN 12830 standard and the other compliant with the 21 CFR part 11 standard). We found that both devices were susceptible to intentional EMI. In addition, we found that a real-time temperature monitor used in hospital settings can be attacked, causing the sensors to falsely report both higher and lower temperatures.

Effective EMI frequencies range from 350 to 1,100 MHz, which can be easily generated with commercially available radio devices. With a maximum EMI output intensity of just 30 dBm (close to the maximum intensity of 3G mobile phones) and a distance of 0.1 m between the EMI output device and the target temperature sensors, the maximum temperature reading increase of the temperature-monitoring devices was +6°C and the maximum decrease was –38°C. In comparison, the EN 12830 standard enforces a ±1°C measurement error tolerance for temperature-monitoring devices and the CDC recommends ±0.5°C or less.[8]

This degree of change in temperature readings can cause a critical temperature excursion and compromise vaccine shipments and storage. Because the EMI output intensity decides how large the electric distortion will be in the target sensor and how far the EMI signal can travel, a higher degree of change in temperature readings or a longer attack distance also can be achieved by a malicious party via use of higher-power radio devices. In an extreme case, previous research has shown that a high-power microwave generated with civilian equipment has the potential to perform a kilometer-range sabotage.[11]

To show the impact of intentional EMI, we conducted a demonstrative experiment using the real-time temperature monitor used in hospital settings to measure the cryogenic temperature generated by dry ice in a foam box (Figure 1). Figure 2 shows how a malicious attacker can control the temperature readings of the real-time temperature monitor. In the tests, the malicious attacker causes controlled positive and negative temperature offsets by using different EMI frequencies and increases the offsets by using higher EMI intensity.

Threat Mitigation Analysis

The difficulty of mitigating intentional EMI threats against off-chip temperature sensors is threefold:

1. Engineering efforts (e.g., RF shielding, EMI filters, twisted-pair cables) that make devices pass the standard industrial electromagnetic compatibility tests have been shown to be insufficient for preventing an intentional EMI attack.[3,12,13]
2. Temperature sensors that already are designed, manufactured, and deployed

cannot be easily modified in a timely manner to mitigate intentional EMI threats because this often requires sophisticated hardware/circuit component modifications (e.g. modifying the signal conditioning circuit).

3. Other countermeasures (e.g., sensor redundancy) might not effectively mitigate EMI threats because closely located sensors (e.g., as found with small refrigerators or vaccine transport boxes) can suffer from intentional EMI disruption during the attack[14] and distantly located sensors cannot measure the accurate temperature in the vicinity of the vaccines.[8] In addition, no standard technique currently exists for using redundant temperature sensors to prevent sensor attacks.

As a result of conventional countermeasures being insufficient, a substantial gap exists for mitigating intentional EMI threats against the vaccine cold chains in accessible and nonintrusive ways. In the current analysis, we address this gap by proposing a few simple measures that can effectively reduce the risk of malicious tampering with intentional EMI to near zero through approaches such as physical administrative controls.

The effort that the attacker needs to exert and the type of attack model are the two key points to consider when designing mitigation schemes. A malicious party needs to find certain frequencies for the EMI signals that can most successfully affect the target temperature sensor. Some frequencies may increase the temperature reading, whereas others may decrease it; this depends on the specific sensor device model and the deployment scenario, which affects the electrical

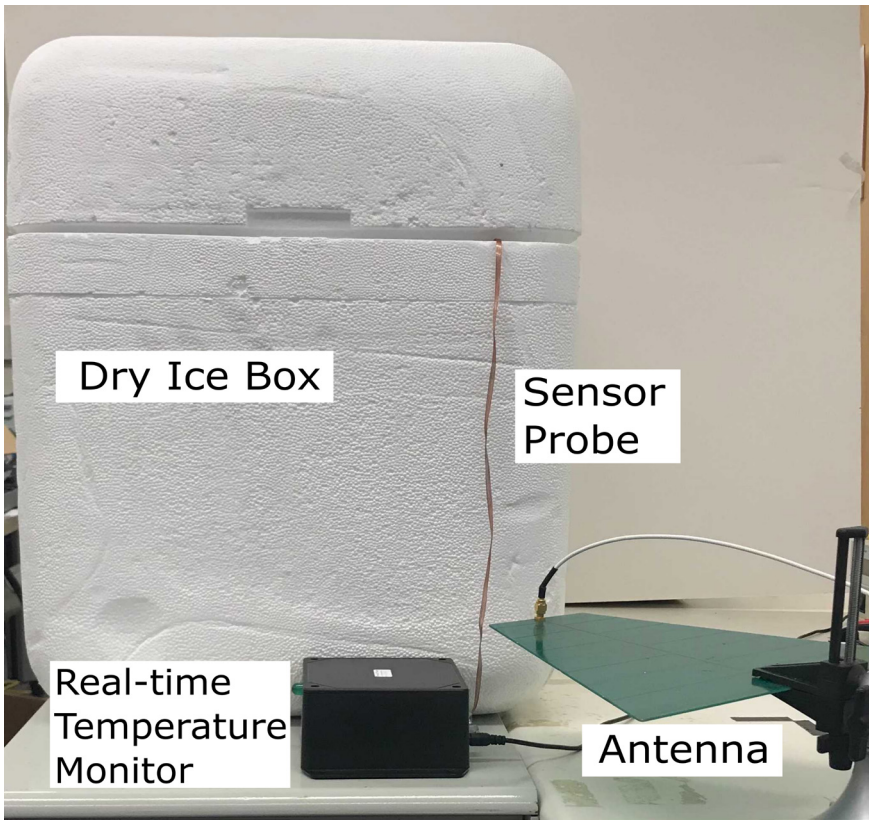

Figure 1. Experimental setup for measuring the temperature variation under intentional electromagnetic interference attack with a foam box filled with dry ice.

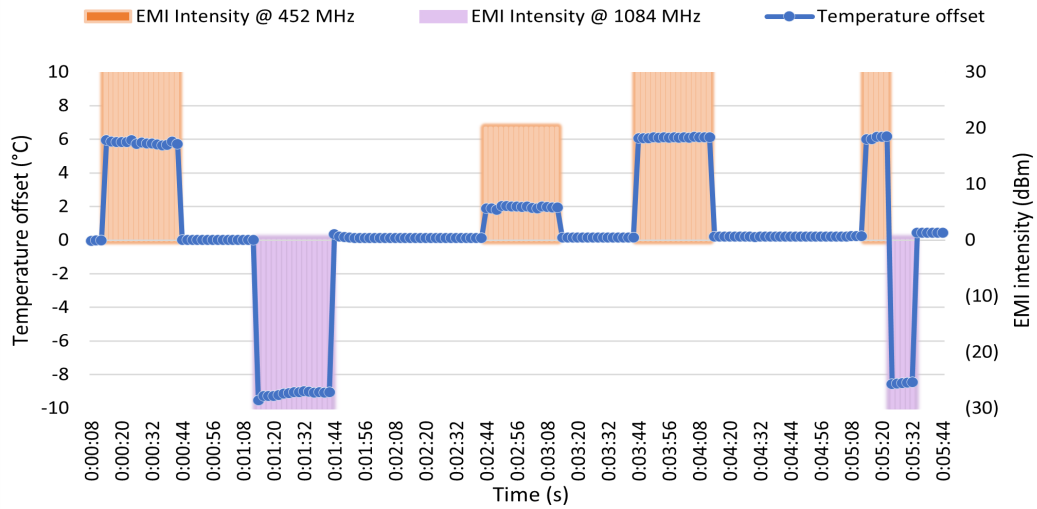

Figure 2. Real-time temperature monitor readings offsets under intentional electromagnetic interference (EMI) attack with dry ice (at –77°C) in three different scenarios. Test 1 (*left*): controlled positive and negative offsets resulting from 30 dBm EMI for 30 seconds; test 2 (*center*): controlled offset with increasing EMI intensity (20 and 30 dBm, respectively); test 3 (*right*): controlled rapidly changing offset.

coupling path between the EMI source and target sensor.

To find the vulnerable frequencies for a particular temperature sensor, the malicious party needs to attempt different frequencies and observe corresponding changes in temperature readings. Without a feedback system, adversaries will have a difficult time guessing how their EMI is affecting a sensor's output. An adversary may consider a brute-force, wide-spectrum attack in an effort to eliminate the need for finding the vulnerable frequencies, but it comes at the cost of using considerably more expensive and rarer radio equipment that supports a very wide band (hundreds of megahertz) of RF.

Because only certain vulnerable frequencies (e.g., the resonant frequencies of a target device's circuit) can be exploited by the adversary to cause traceable changes in temperature readings, previous research on intentional EMI has focused primarily on vulnerable-frequency attacks.[3,12] In the current analysis, we also address mitigation of vulnerable-frequency attacks.

Generally speaking, two types of threat models exist: off-site and on-site exploitation. In off-site exploitation, the attacker would know in advance the model of sensor devices being used. The attacker could acquire the same equipment and find the vulnerable frequencies in an off-site setting, then bring portable devices (e.g., walkie talkies, which are widely known to emit strong EMI) customized at these vulnerable frequencies to the proximity of vaccines and change temperature readings.

On-site exploitation, on the other hand, does not require prior knowledge of the sensor device model. The attacker can set up a laptop with radio antennas and software-defined radio devices, then tune the frequencies and observe corresponding temperature reading changes on the spot. Of course, on-site exploitation requires more risk by the adversary, who might be noticed to be in possession of radio equipment.

Finally, if an attacker does not know the exact model of the sensor device used, they may use a combined approach in which they guess and buy similar products and obtain a list of the vulnerable frequencies of these devices via off-site testing. Then, they can perform an on-site exploitation by first trying those frequencies and observing whether the target device has the same vulnerable frequencies. However, no guarantee exists that the devices will share a similar range of vulnerable frequencies and, depending on the devices' complexity, the approach will require greater time and effort on the part of the adversary.

Defensive Strategy: Deterrence via Adversary Time and Effort

The key to mitigating such threats is to increase the effort and time the attacker needs to exert in order to find the devices' vulnerable EMI frequencies and the appropriate EMI output intensity. Several precautions can be easily taken to reduce the risks to a minimal level: (1) cutting off the feedback, (2) keeping the sensor device model confidential, (3) hiding/randomizing the location of the temperature-monitoring devices, (4) carefully selecting sensors with a desired sampling rate, and (5) using temperature indicators that are less or not susceptible to EMI.

Cutting Off the Feedback

The attackers cannot easily know if the EMI frequencies used are the vulnerable frequencies if they cannot observe the change in temperature readings. The feedback cutoff can be achieved by eliminating easily snooped monitor screens and real-time temperature display on the temperature-monitoring devices. For instance, a small blinder on the temperature display (similar to a gas station payment pump or voting machine) can make snooping more difficult.

If easily snooped visual feedback cannot be eliminated, stand-off distances from the monitoring devices should be enforced to prevent nonauthorized people from observing the readings. A larger stand-off distance will also require a higher-power EMI output device in order to affect the sensor, which increases the cost incurred by the malicious party.

Further, the temperature data should only be accessible to trustworthy parties when necessary. Some temperature-monitoring systems also provide wireless communication functionality and monitoring software, which expose additional attack surfaces for

the attacker to acquire the temperature-reading feedback. In this case, enforcing strong passwords and authentication schemes is crucial.

Of note, although feedback cutoff is the most effective method to prevent on-site exploitation, technically it cannot prevent off-site exploitation, in which case the attacker is the administrator of the duplicate target device that was acquired and therefore has unlimited access to sensor readings. However, avoiding temperature sensor devices with real-time temperature display can also greatly increase the effort of an attacker conducting an off-site exploitation due to the burden of reading the data repeatedly in an asynchronous fashion.

Keeping the Sensor Device Model Confidential

Keeping the sensor device model confidential is the most effective way to prevent off-site exploitation because, in this case, the attacker cannot acquire a duplicate device to find the vulnerable frequencies in advance. But similarly, this strategy alone cannot defend against on-site exploitation where the attacker can test the real device on the spot if the device's temperature-reading feedback is not cut off or well protected.

Hiding/Randomizing the Location of Temperature-Monitoring Devices

Hiding/randomizing the location of the temperature-monitoring devices can reduce risk. After the attacker finds the vulnerable frequencies, the degree of change in temperature readings depends on the output intensity of the EMI source, as well as the distance and coupling path between the EMI source and target sensors. The attacker faces the risks of using too low intensity (so that no temperature excursions are caused) or too high intensity (so that the temperature excursions appear as artificial, which could reveal the attacker's existence). Hiding/randomizing the sensor locations can prevent attackers from knowing the distance and coupling paths, greatly increasing the effort of the attackers for deciding the appropriate output intensity and thus lowering risks of this threat.

Carefully Selecting Sensors with a Desired Sampling Rate

Carefully selecting sensors with a desired sampling rate will reduce risk. The sample rate of a temperature sensor is the frequency of updating the temperature readings. The lower the sample rate, the slower the attacker will be able to identify the vulnerable frequencies because of the slow feedback update. To maximize the effort the attacker needs to put forth, it is advisable to select a temperature sensor/device whose maximal supported sample rate is closest to the minimal sample rate necessary to effectively monitor vaccine conditions and ensure vaccine safety.

For example, if the vaccine monitoring requires reading the temperature every 10 minutes, choosing a sensor/device with the highest supported sample rate of one sample per 10 minutes is recommended over using one that supports one sample per second and setting the device to read the temperature every 10 minutes. Otherwise, the attacker could easily conduct an off-site attack in which they set the duplicate device acquired to the highest supported sample rate and thus find the vulnerable frequencies quickly. In the above example, the time that the attacker needs to find the vulnerable frequencies can be in creased 600 times (10 min/1 s) by selecting the right sensor device.

Using Temperature Indicators that Are Less or Not Susceptible to EMI

Using temperature indicators that are less or not susceptible to EMI will reduce risk. On-chip integrated temperature sensors (e.g., using silicon-based microelectromechanical system [MEMS] technologies) are less susceptible to EMI due to the smaller dimension of their electric paths. Commercially available MEMS temperature sensors, however, rarely are able to operate at a temperature lower than –40°C and therefore are not applicable to monitoring COVID-19 vaccines, many of which require storage at ultra-cold temperatures (–80°C to –60°C). Further, because the on-chip sensor does not have a sensor probe, it's relatively less flexible for deployment in cold chain cooling systems.

In addition to on-chip electronic sensors, nonelectronic temperature indicators (e.g., chemical-based indicators) also may be used

for secondary temperature verification. However, to the authors' knowledge, few models can be used for monitoring COVID-19 vaccines, which require ultra-low temperature storage.

Conclusion

Analog cybersecurity threats in the form of EMI can fool temperature sensors used in the cold chain transportation and storage of COVID-19 vaccines. The best way to prevent sensor-based disruption to the supply chain is to design sensor circuits to resist deliberate EMI. As a temporary measure to defend the supply chain from EMI threats, simple administrative controls, such as controlling physical access to visual displays of temperature, can prevent adversaries from causing disruption.

Acknowledgments

This work is supported by the National Science Foundation (NSF) under grant no. CNS-2031077, by the Japan Society for the Promotion of Science (JSPS) KAKENHI under grant no. 21K11884, and by a gift from Facebook. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the NSF, JSPS, or Facebook.

References

1. Dewan S, Nolan K. Pharmacist accused of tampering with vaccine was conspiracy theorist, police say. www.nytimes.com/2021/01/04/us/pharmacist-accused-of-tampering-with-vaccine-was-conspiracy-theorist-police-say.html. Accessed Jan. 4, 2021.
2. Fox C, Kelion L. Coronavirus: Russian spies target Covid-19 vaccine research. www.bbc.com/news/technology-53429506. Accessed Jul. 16, 2020.
3. Yazhou T. Trick or heat? Manipulating critical temperature-based control systems using rectification attacks. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, Nov. 6, 2019, London, UK*. New York, NY: Association for Computing Machinery.
4. Fu K, Xu W. Risks of trusting the physics of sensors. *Communications of the ACM*. 2018;61(2):20–3.
5. Lovelave B Jr. U.S. quarantines Pfizer vaccine shipments in California and Alabama after transit 'anomaly' left vials too cold. www.cnbc.com/2020/12/16/covid-vaccine-us-quarantines-pfizer-shipments-in-california-alabama-after-transit-anomaly.html. Accessed Dec. 16, 2020.
6. Salcedo A. More than 16,000 vaccine doses potentially spoiled in Maine and Michigan by temperature problems. www.washingtonpost.com/nation/2021/01/20/moderna-vaccine-spoiled-maine-michigan. Accessed Jan. 20, 2021.
7. Jordan Shamus K. Nearly 12,000 doses of Moderna COVID-19 vaccines spoiled en route to Michigan. www.freep.com/story/news/health/2021/01/19/moderna-covid-19-vaccines-spoiled-michigan/4219827001. Accessed Jan. 21, 2021.
8. Centers for Disease Control and Prevention. *Vaccine Storage and Handling Toolkit: 2021*. www.cdc.gov/vaccines/hcp/admin/storage/toolkit/index.html. Accessed Aug. 6, 2021.
9. Chojnacky MJ, Strouse GF, Wyatt Miller W. Methods for accurate cold-chain temperature monitoring using digital data-logger thermometers. www.nist.gov/publications/methods-accurate-cold-chain-temperature-monitoring-using-digital-data-logger. Accessed Aug. 6, 2021.
10. Chojnacky MJ, Chaves Santacruz LF, Wyatt Miller W, Strouse GF. Optimizing data logger setup and use for refrigerated vaccine temperature monitoring. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=916348. Accessed Aug. 6, 2021.
11. Backstrom MG, Lovstrand KG. Susceptibility of electronic systems to high-power microwaves: summary of test experience. *IEEE Transactions on Electromagnetic Compatibility*. 2004;46(3):396–403.
12. Shoukry Y, Martin P, Tabuada P, Srivastava M. Non-invasive spoofing attacks for anti-lock braking systems. In: Bertoni G, Coron JS, Eds. *Cryptographic Hardware and Embedded Systems: CHES 2013*. Berlin, Germany: Springer; 2013.
13. Foo Kune D, Backes J, Clark SS. Ghost talk: mitigating EMI signal injection attacks against analog sensors. https://ieeexplore.ieee.org/document/6547107?arnumber=6547107. Accessed Aug. 6, 2021.
14. Hongjun C. Software-based realtime recovery from sensor attacks on robotic vehicles. International Symposium on Research in Attacks, Intrusions and Defenses, 2020. Berkeley, US. USENIX.