Deep Freezing Attacks on Capacitors and Electronic Circuits

Jalil Morris, Obi Nnorom Jr., Anisul Abedin,
Ferhat Erata, and Jakub Szefer

Yale University, New Haven, CT 06511, USA
{firstname.lastname}@yale.edu

Abstract. This paper introduces new deep freezing attacks on capacitors and electronic circuits that use them. The new attacks leverage liquid nitrogen to rapidly freeze electrolytic capacitors and supercapacitors to temperatures approaching −195 °C (−320 °F or 77 K). Due to the quick freezing to the extremely low temperatures, overall capacitance of the capacitors rapidly drops towards zero. Change of the capacitance can affect reliability and security of electronic circuits that these capacitors are used to build, and this work in particular evaluates electronic filters, as well as capacitor-powered microcontrollers, and their response to the deep freezing attacks. This work presents disruptive attacks that affect the operation of the target device, but then return device to normal operation after short amount of time when the components warm up. In addition to the disruptive attacks, this work also demonstrates destructive attacks where the target device is damaged due to the extreme freezing. Both types of attacks leave no trace as the liquid nitrogen evaporates after the attack is finished. This paper highlights new threats that designers should be aware of and defend against.

Keywords: electrolytic capacitors, supercapacitors, high-pass filters, low-pass filters, microcrontrollers, liquid nitrogen, freezing attacks, security

1 Introduction

Computer and embedded systems depend on capacitors as the very basic building blocks of many electronic circuits that make them up. Two particular types of capacitors often used in electronic circuits are the electrolytic capacitors and supercapacitors. Electrolytic capacitors are polarized capacitors, which leverage wet or dry electrolytic, and can be made from aluminum, tantalum, or niobium. Wet aluminum capacitors tend to be widely used and are the focus of this work. Another type of widely used capacitors are supercapacitors, which have very high capacitance values, but tend to have lower voltage ratings compared to electrolytic capacitors. They can be polarized or non-polarized, although they are more commonly polarized, and use an electrolytic between the electrodes of the capacitor.

These capacitors are not entirely stable over all possible operating temperatures. Generally, Equivalent Series Resistance (ESR) increases as the temperature decreases, and this effect is particularly pronounced for aluminum electrolytic capacitors, "due to the limitation of wet electrolyte conductivity at low temperatures" [1]. Similar effects also exist in supercapacitors. Consequently, rapidly freezing such capacitors can have a significant effect on their capacitance, which is leveraged by our deep freezing attacks using liquid nitrogen (LN_2).

By using liquid nitrogen we can rapidly freeze electrolytic capacitors and supercapacitors to temperatures approaching −195 °C (−320 °F or 77 K). When the electrolyte in the capacitors freezes to these temperatures, the electrons or ions within the electrolyte no longer have much freedom to move, an electric field is not formed between the plates of the capacitor, and the overall capacitance of the capacitor rapidly drops towards zero. Rapid reduction of the capacitance has direct impact on the circuits that utilize these capacitors as we show in this work. This in particular leads to the new non-invasive and trace-free LN_2 attacks. LN_2can be obtained easily from chemical or scientific supply companies and, in small quantities, is easy to transport and deploy. The attacks are further very low-cost. Vendors such as Airgas charge about $0.28 per liter when LN_2 is purchased in bulk, while academic cleanroom at our institution charges about $0.10 per liter for bulk LN_2. Each individual attack instance uses no more than few liters, costing at most $0.50 per attack.

To evaluate the new physical LN_2 attacks, we investigate how the aluminum electrolytic capacitors respond to temperatures well below their operable range by dousing or dipping them in the liquid nitrogen. We also investigate how a capacitor's physical size, volume, composition, and electrical properties (i.e. capacitance and voltage rating) influence how effective liquid nitrogen is in changing a capacitor's characteristics. We further study the impact of the freezing duration on the measured capacitance changes. The main take-away is that even with short attack time on order of 10-30 s, a capacitor's capacitance drops towards zero. Further, capacitance quickly returns to normal when LN_2 is no-longer applied and the target allowed to warm up, leaving no trace of the attack. This is thus a new type of a disruptive attack, where device briefly operates abnormally during the attack, but then returns to normal operation when attack finishes. Although permanent damage was not observed when freezing individual capacitors, we did observe permanent damage of a microcontroller board when it was frozen while attacking on-board capacitors, leading to a possible new type of a destructive attack as well.

Many circuits' functionality depends on capacitors for their correct operation. A simple, but important class of circuits are electronic filters, such as high-pass and low-pass filters. Their cut-off frequency, i.e. frequency above which the high-pass filter passes signals or equivalently the frequency at which a low-pass filter attenuates signals, depends on the time constant, which is the product of the resistance (R) and capacitance (C). Affecting the capacitance of the capacitors in the filters, through the freezing attacks, directly affects the resistance and capacitance product, effectively changing the time constant and the behavior

of the filter. Consequently, we investigate the deep freezing attacks and their effects on the cut-off frequency. We observe the high-pass filters begin to attenuate some signals that were passed before, and, conversely, low-pass filters allow some signals to pass which were attenuated before. This can in the least cause wrong sensor readings, or at worst cause unexpected faults in the system using the filters.

Capacitors are not only used in sensing circuits, but can also be used for energy storage. In particular electrolytic capacitors and supercapacitors can be used to power intermittent-computing devices, such as MSP430-class microcontrollers (MCUs). We evaluate how affecting the capacitance of these capacitors used to power microcontrollers can lead to a device crash or an inconsistent operation of the device.

For all the different types of devices and circuits that we consider, once the freezing effect wears off, the circuits usually return to their normal operation, without leaving any traces of the freezing attack. These are new types of disruptive attacks that temporarily modify behavior of the device, but then return the device to normal operation. In one case, a destructive attack was also observed, when a microcontroller board failed to operate after repeated freezing. The fact that circuits are not physically modified and that no easily observable traces persist after the freezing is finished (for the disruptive attacks) make these attacks very stealthy. For destructive attacks, even though the device is damaged, analyzing the source of the damage is difficult if all the traces of the LN_2 freezing are gone.

Based on our findings, we propose a set of defenses. Some of the different possible passive defenses can be easily deployed, such as switching away from using aluminum electrolytic capacitors or by adding insulation. In addition, active defenses can use temperature sensors deployed near critical capacitors or circuits to detect the freezing attack and take evasive action.

1.1 Paper Organization

The remainder of the paper is organized as follows. Section 2 presents background on capacitor temperature characteristics and cooling-related attacks. Section 3 gives the threat model. Section 4 overviews setup used for the experiments. Section 5 presents the evaluation results. Discussion of the results and potential defenses is given in Section 8 and the paper concludes in Section 9

2 Background

This section provides background on thermal characteristics of capacitors, and on existing work on security effects of cooling or freezing of electronic components.

2.1 Temperature Characteristics of Capacitors

Capacitors are passive electronic components that are used to store energy. Their capacitance is affected by temperature, and, for polarized aluminum electrolytic

capacitors, the capacitance can decrease by almost 40% when exposed to low temperatures of −55 °C [1,?]. Supercapacitors are also susceptible to temperature variations, and are typically not designed to work below −20 °C or −40 °C, as their capacitance is significantly reduced.

While the temperature effects on capacitors are known when the discrete capacitors are exposed to temperatures reaching −55 °C, how the capacitors behave when frozen by an attacker using liquid nitrogen and reaching −195 °C has not been evaluated from security perspective before. As will be explained in the threat model, Section 3, it is relatively easy to freeze the electronics with liquid nitrogen, without leaving a trace of an attack. It is in this context that we are especially interested in evaluating the impact of the freezing effects on different types of capacitors and circuits as a function of the freezing time of the capacitors.

2.2 Cold Boot and Chill Out Attacks

Security attacks based on rapidly cooling computer components are perhaps best exemplified by the Cold Boot attack [2], which focused on the internal capacitors found in the data cells of Dynamic Random Access Memory (DRAM) modules. The authors showed that by cooling DRAM chips (and thus the capacitors that they contain), the decay rate of the capacitors used to store data bits in DRAMs is reduced. This extends the time for which data persists in a powered-off chip, and allows malicious adversaries to transfer the cooled DRAM to a different computer to read the DRAM cells before the data is lost. The Cold Boot attacks focused on using up-side-down compressed air cans which leak compressed gas when used up-side-down and cool the DRAM. Authors also showed dipping DRAM chips in liquid nitrogen as a means to extend the time of the Cold Boot attack. Follow-up work, among others, showed similar security attacks by, for example, cooling smartphones in a refrigerator to extract keys stored in DRAM and break Android Full-Disk Encryption [4]. More recent work [6] showed that Cold Boot attacks still work in new DDR4 memories that use scrambling. The existing Cold Boot related work thus has focused on computer memories only, and did not consider electrolytic capacitors or supercapacitors, which we do in this work.

More recent work demonstrated the Chill Out attack [3], which focused on evaluation of behavior of capacitors and DC/DC converters when exposed to cooling sprays. The authors showed that there is a decrease in capacitance when electrolytic capacitors are cooled to about −55 °C, and that DC/DC converter behavior changes if the cooling is applied to the output electrolytic capacitors used in the converters. The authors used off-the-shelf electronic cooling sprays and, similar to prior work, up-side-down compressed air cans.

Our work differs from such prior research by considering the security implications of freezing capacitors individually, and also freezing capacitors inside electronic filters and energy-storage capacitors in microcontrollers. Neither did the existing work evaluate using liquid nitrogen to bring these devices to extreme temperatures approaching −195 °C.

3 Threat Model

This work assumes a malicious attacker who has physical access to the target device, but cannot modify or probe the target device, which could be easily noticed or detected by on-board circuitry. Instead, the attacker has a brief time window to make changes to the environment in which the device operates, such as by pouring liquid nitrogen or dipping it in liquid nitrogen. We assume the attacker can control the time of the LN_2 pouring or time of dipping in the LN_2. We assume the attacker has access to device for no more than about 30-60 s, making this a very fast attack.

While the attack could be detected by use of thermal sensors, to best of our knowledge, existing circuits targeted in this work do not contain thermal sensors or other defenses. Section 8 has a more detailed discussion of the potential defenses and other considerations. We further assume the defenders could analyze the device after the attack for any traces of the attack, but this type of attack leaves no trace of the freezing once the liquid nitrogen evaporates, allowing the attack to go undetected.

4 Experimental Setup

In this work, we use three basic setups: one to observe changes to capacitor behavior in response to freezing, one to test impact of capacitor freezing on a high-pass and low-pass filters, and one to test impact of capacitor freezing on capacitor-powered MCUs.

The *capacitor testing* setup uses the ADALM2000 power supply and oscilloscope module[1] to drive the capacitors with 3-5 V inputs by applying a step function input and captures the voltage across the capacitor as it is charging and discharging, under different freezing conditions. When step function is applied and input becomes one, the time to go from zero to full charge can be observed, and when the input goes to zero at the end of the step function, the time to go from full charge to zero can be observed. Both charging and discharging characteristics are measured using the ADALM2000 module.

The *high-pass and low-pass filter testing* setup uses a Keithley 2231A power supply to provide input voltages, the ADALM2000 to provide sine wave input to the filters with 5 V peak-to-peak voltage and frequency in the 1 kHz range, and captures the output of the high-pass filter and low-pass filter using a Tektronix MDO3104 Mixed Domain Oscilloscope with TPP1000 1 GHz passive probes.

The *microcontroller and supercapacitor testing* setup uses multiple MSP430-class microcontroller boards, especially `MSP430FR5994` and `MSP430FR5969` development boards. These can be powered through a USB cable, or a `P2110-EVB` harvester kit board can be used to power the microcontroller boards from an RF transmitter. All the boards are described in detail in Section 7. The capacitors

[1] ADALM2000: Advanced Active Learning Module, https://www.analog.com/en/design-center/evaluation-hardware-and-software/evaluation-boards-kits/ADALM2000.html

Table 1. Aluminum electrolytic capacitors of different types, physical dimensions, and voltage ratings used in the capacitor freezing tests. The capacitors are cylindrical in shape and their volume is $\pi(\frac{D}{2})^2 H$, where H is the height and D is the diameter. The times are rounded to the closest 15 second interval due to the experimental setup and the time measurement method.

Brand	**Value**	**Rating**	H	D	T_{zero}	T_{normal}
Capacitor Freezing Tests						
Panasonic	220 µF	6.3 V	11 mm	5 mm	15 s	120 s
Panasonic	220 µF	25.0 V	12 mm	8 mm	30 s	150 s
Panasonic	220 µF	63.0 V	22 mm	10 mm	45 s	210 s
Panasonic	470 µF	16.0 V	12 mm	8 mm	15 s	165 s
Panasonic	680 µF	35.0 V	20 mm	13 mm	45 s	210 s
Panasonic	1,500 µF	50.0 V	36 mm	16 mm	120 s	360 s

on these boards are subjected to the freezing attacks and the time before boards crash due to lack of stored energy as the capacitors are frozen is measured. Time is measured by observing an output LED which stops blinking when the test program crashes.

4.1 Liquid Nitrogen Freezing Approach

Liquid Nitrogen (LN_2) is used to gauge the effects of freezing the capacitors. When used to freeze a device, it is expected to freeze down to approximately −195 °C or −320 °F. To freeze the capacitors, they are either dipped or doused with LN_2. Liquid nitrogen is non-conducting, thus making it safe for pouring over electronics, or dipping electronics in it. For the capacitor-only tests, the capacitors are connected to the target circuit by long wires so that the capacitor is frozen, but the rest of the circuit is not affected. For dipping, the capacitors are lowered into a container filled with LN_2 and held inside LN_2 for the specified mount of time. For dousing, the capacitors are placed on a styrofoam surface and LN_2 is poured over for the specified amount of time. For other tests, if the capacitor is permanently attached to another device and cannot be removed, e.g., to the MCU board, the liquid nitrogen is poured on the capacitor for the specified amount of time, and it may also spill over onto adjacent components during pouring.

5 Capacitor Freezing Attacks

To understand impact of freezing on capacitors, we first perform a set of experiments to determine how the capacitance is affected by the freezing. This *capacitor testing* can give insights into attacks discussed in later sections. Table 1 shows capacitors of different types, physical dimensions, and voltage ratings used in the capacitor freezing tests.

Table 2. Aluminum electrolytic capacitors used in electronic filter tests. H is the height and D is the diameter of the cylindrical-shaped capacitors used in high-pass and low-pass filter tests.

Brand	**Value**	**Rating**	H	D
High-Pass Filter Tests				
Kemet	47 µF	25.0 V	13 mm	5 mm
Panasonic	220 µF	25.0 V	12 mm	8 mm
Nichicon	470 µF	16.0 V	13 mm	10 mm
Low-Pass Filter Tests				
Kemet	47 µF	25.0 V	13 mm	5 mm
Panasonic	220 µF	25.0 V	12 mm	8 mm
Nichicon	470 µF	16.0 V	13 mm	10 mm

The table in particular shows T_{zero} and T_{normal} which are the freezing time taken for freezing to cause an aluminum electrolytic capacitor's capacitance to approach zero and thawing time taken for capacitor to return to its normal capacitance, respectively. It can be seen from the table that in general T_{zero} is correlated with the physical volume of the capacitor. For same capacitance values, capacitors with bigger voltage rating in general have bigger volume. Thus for same capacitance values, capacitors with bigger voltage rating tend to take longer to cool down. T_{normal} is also related to the capacitor size and volume, and it can be seen that once frozen, the bigger the capacitor, the longer it takes for it to regain normal operation. For most of capacitors freezing of less than 60 s is sufficient to bring the aluminum electrolytic capacitors' capacitance down to zero, and these deep freezing times will be used to study effects on filters and capacitor-powered microcontrollers in the next sections.

6 Electronic Filter Freezing Attacks

In this section we evaluate effects of deep freezing on high-pass and low-pass filter circuits. Table 2 shows capacitors evaluated with these electronic filters. As we demonstrate in this section, the deep freezing is able to be used to non-invasively shift the cutoff frequency of these filters. We also call this a new Cutoff Frequency Shifting Attack (CFSA). By affecting the cutoff frequency, wrong operation of the filters can be induced.

6.1 Attacks on High-Pass Filters

The frequency above which the high-pass filter passes signals, i.e. the cutoff frequency, depends on the time constant $\frac{1}{RC}$, where R is the resistance and C is the capacitance. Freezing capacitors brings down value of C, effectively changing the time constant of the circuit, and increasing the cutoff frequency. For a fixed

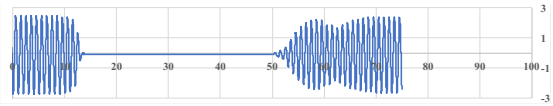

Fig. 1. Example of high-pass filter's response to 30 s of LN_2 pouring. The filter used 47 µF electrolytic capacitor. The x-axis is in seconds, and the y-axis is the output signal amplitude. The experiment was stopped at 75 s.

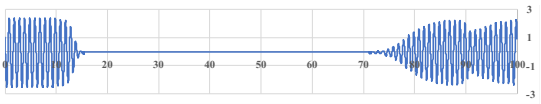

Fig. 2. Example of high-pass filter's response to 30 s of LN_2 pouring. The filter used 220 µF electrolytic capacitor. The x-axis is in seconds, and the y-axis is the output signal amplitude.

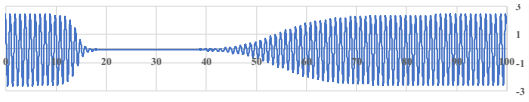

Fig. 3. Example of high-pass filter's response to 30 s of LN_2 pouring. The filter used 470 µF electrolytic capacitor. The x-axis is in seconds, and the y-axis is the output signal amplitude.

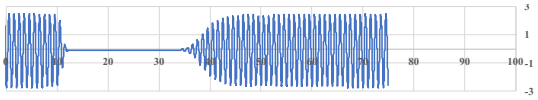

Fig. 4. Example of high-pass filter's response to 10 s of LN_2 pouring. The filter used 47 µF electrolytic capacitor. The x-axis is in seconds, and the y-axis is the output signal amplitude. The experiment was stopped at 75 s.

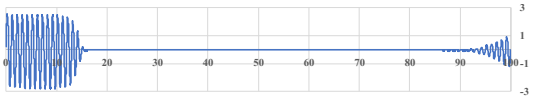

Fig. 5. Example of high-pass filter's response to 30 s of dipping in LN_2. The filter used 220 µF electrolytic capacitor. The x-axis is in seconds, and the y-axis is the output signal amplitude.

input frequency, as the capacitors freeze, the signal begins to be attenuated. For fixed size capacitor, this happens at approximately same time, regardless of the pouring duration. Once the pouring stops, the capacitors slowly start to warm up, which means the time constant changes back towards its original value, and the filter begins to pass the input signal again.

Figures 1 and 4 show an example of a high-pass filter's response to 30 s and 10 s of LN_2 pouring, respectively. A 47 µF and 15.6 kΩ were connected in series to create a high-pass filter with a cutoff frequency of 0.7 Hz. A 5 V peak-to-peak 1 Hz signal was passed through the filter and the output was observed as shown on the figures. The figures demonstrate that longer freezing results in longer time when filter attenuates frequency it should not. Figure 1 shows attenuation between approximately 10 s and 50 s marks, while Figure 4, where freezing was shorter, shows attenuation between approximately 10 s and 35 s marks. In all cases the effect lasts past the end of the freezing.

Figures 2 and 5 compare effect of pouring LN_2 over the capacitors vs. dipping capacitors in LN_2, both for 30 s, respectively. A 220 µF and 3.3 kΩ were connected in series to create a high-pass filter with a cutoff frequency of 0.7 Hz. Again a 5 V peak-to-peak 1 Hz signal was passed through the filter and the output was observed as shown on the figures. It can be seen from the figures that dipping creates a longer-lasting freezing effect, and it takes longer for the filter to regain its original behavior.

Figures 1, 2, and 3 show filters with 47 µF, 220 µF, and 470 µF capacitors, respectively. For all three, the freezing effect takes place before the pouring finishes. The 47 µF capacitor recovers faster compared to 220 µF. For the 470 µF, although the input frequency is no-longer passed as seen from the figure, it may not be fully frozen, and starts to recover sooner. Due to biggest physical volume, the recovery rate is slowest as can be seen between 40 s and 80 s mark.

6.2 Attacks on Low-Pass Filters

The cutoff frequency of the low-pass filter likewise depends on the time constant of the circuit, which is the $\frac{1}{RC}$, where R is the resistance and C is the capacitance. As the capacitor freezes, the value of C is reduced, which increases the cutoff frequency. As a result, when low-pass filter is frozen, the previously attenuated signals begin to be passed through.

Figure 6 shows an example of low-pass filter's response to 30 s of LN_2 pouring. A 220 µF and 3.3 kΩ were connected in series to create a low-pass filter with a cutoff frequency of 0.7 Hz. A 5 V peak-to-peak 1 Hz was inputted to the filter, and the output was observed as shown in the figure. Our results indeed confirm the expectation that during the attack the input signal is not attenuated as much (between 20 s and 70 s mark), while once the capacitor begins to warm up the signal is again attenuated (after 70 s mark).

6.3 Attacks on Higher-Order Filters

Attacks in the previous section targeted first-order filters. In addition, we have tested second-order filters. We used same 47 µF, 220 µF, and 470 µF electrolytic capacitors. Each filter used only one type of capacitor. Since the higher-order filters use multiple capacitors, we tested LN_2 dipping attack on individual capacitors (where only one of the capacitors was frozen at a time), and on all

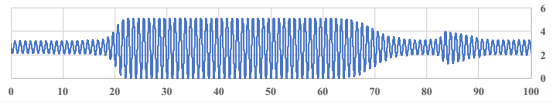

Fig. 6. Example of low-pass filter's response to 30 s of LN_2 pouring. The filter used 220 µF electrolytic capacitor. The x-axis is in seconds, and the y-axis is the output signal amplitude.

capacitors (where all capacitors used in the filter were frozen at once). In particular, we tested "Vin", "Vout," and a "Vin + Vout" capacitors. "Vin" indicates the test done on the capacitor closest to the input, "Vout" indicates the freezing test done on the capacitor closest to the output, and "Vin + Vout" indicates that both capacitors were dipped in LN_2 at the same time. The capacitors were dipped in LN_2 for 10 s, 30 s, and 60 s for different tests.

In all cases we observed similar results to the first-order filter tests. Regardless of which capacitor or capacitors were frozen, the filters behaved the same, e.g., high-pass filter is made to attenuate signals during freezing. Freezing the "Vin" capacitor causes high-pass filter to attenuate the inputs, and the second stage cannot recover this input. Freezing of the "Vout" capacitor attenuates the signal at the output, which unfrozen first stage cannot correct. Freezing of both capacitors simply combines the effects. Based on the results, we conclude that higher-order filters do not help mitigate the new freezing attacks.

6.4 Comparison to Freezing with Cooling Sprays

In addition to using liquid nitrogen, we used electronics cooling spray, similar to the Chill Out attack [3], but in our case we cooled the capacitors in the filters. The capacitors in the filters were sprayed for up to 30 s with the cooling spray. However, no significant effect was observed on the filters. This seems consistent with the existing work [3], where cooling capacitors with the cooling spray caused capacitance changes to be 10% or less. Thus, the time constant of the filter will be changed minimally when cooling spray is applied, while with the liquid nitrogen there is significant time constant change as the capacitance goes to zero.

7 Energy Storage Freezing Attacks

In addition to being able to modify behavior of circuits such as electronic filters, the freezing attacks can directly impact operation of devices that depend on them for energy storage. In particular, we have explored the MSP430-class microcontrollers (MCUs) which are a representative of transiently-powered computing devices, also called intermittent-computing devices. The intermittent-computing devices are used to run computations on limited amount of energy stored in the capacitors. The code running on intermittent-computing devices is designed to work with the specified capacitor by, for example, using checkpointing [5] to ensure forward progress between each discharge of the capacitor.

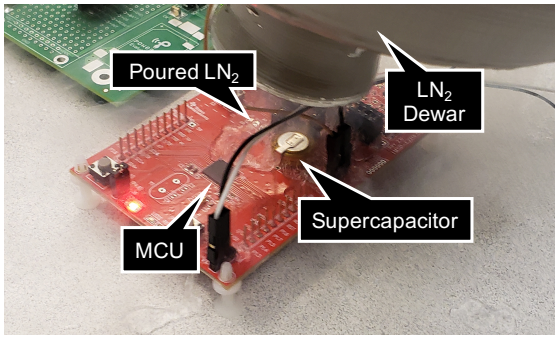

Fig. 7. Example of freezing attack via pouring LN_2 on the supercapacitor on the `MSP430FR5994` board.

However, as we demonstrate in this section, freezing of the capacitors used for energy storage effectively cuts down, or even fully eliminates, the stored energy available to run computation. Freezing thus can be used to stop computation from progressing, or to introduce faults if the checkpoint is not reached. Because frozen capacitor stores less, or even zero, energy than what is assumed when selecting checkpoint locations, code that works correctly under normal conditions, will not work with frozen capacitors where energy storage is not sufficient to reach the checkpoints. The repeated deep freezing attacks may even permanently damage the boards, as we observe.

7.1 Capacitor-Powered MSP430-class MCUs

The freezing tests were conducted on the `MSP430FR5994` development board with a 0.22 F supercapacitor and on the `MSP430FR5969` development board with a 0.10 F supercapacitor. The boards can be powered via USB to charge the devices, and when USB cable is disconnected, they run on the energy stored in the on-board capacitors until the device runs out of energy.

In addition, a `P2110-EVB` harvester kit board was tested, which has a 0.05 F AVX BestCap supercapacitor, a 0.001 F electrolytic capacitor, or can be used with user-installed capacitor. The harvester kit board can be used to power the MPS430 boards, bypassing the capacitor on these boards. The harvester kit board is charged when a remote radio-frequency (RF) transmitter transmits power, when the transmitter is turned-off, or out of range, the harvester kit board powers the MSP430 boards from its capacitor. The `P2110-EVB` harvester kit board is optimized for operation in the 902-928 MHz band, but will operate outside this band with reduced efficiency. RF transmitter used transmits in at 915 MHz.

Table 3. MSP430-class MCUs and capacitors tested. FR5994 refers to the `MSP430FR5994` board, FR5969 refers to the `MSP430FR5969` board, and P2110 refers to the `P2110-EVB` harvester kit board. If harvester was used, the pre-installed or user-installed capacitor on the harvester was used, otherwise the MCU board's capacitor was used.

Board	Harvester Used?	Capacitor	Volt Rating	Type
Electrolytic Capacitor Tests				
FR5969	P2110	330 µF	25.0 V	Electrolytic
FR5969	P2110	470 µF	16.0 V	Electrolytic
FR5969	P2110	3,300 µF	16.0 V	Electrolytic
Supercapacitor Tests				
FR5994	P2110	0.05 F	—	Supercap.
FR5969	—	0.10 F	—	Supercap.
FR5994	—	0.22 F	—	Supercap.

7.2 Setup for Microcrontroller Freezing Attacks

The freezing attacks on microcontrollers were done similar to attacks on capacitors and electronic filters discussed in prior sections: by dipping the capacitors in LN_2 or by pouring LN_2 over the capacitor. Figure 7 shows example of attack by pouring LN_2 over the supercapacitor on the `MSP430FR5994` board. Table 3 shows the boards and capacitors tested.

7.3 Freezing Attacks on Energy Storage in Electrolytic Capacitors

The `P2110-EVB` harvester kit board allows for installation of user-provided capacitor, and we tested three different types of electrolytic capacitors by installing them on the harvester kit board. The pre-installed 0.05 F AVX BestCap supercapacitor and 0.001 F electrolytic capacitor where both disabled by use of select jumpers. Auxiliary eZ-FET module on the `MSP430FR5994` board was disabled by removing jumpers to reduce energy consumption of the board.

The software running on the microcontroller was a simple code loop which is used to blink an LED following a predefined delay. Energy is consumed by the microcontroller as it is running the code as well as by the LED. Since the run-time on the electrolytic capacitors is very short, the oscilloscope was used to observe the VCC voltage and measure how long the device ran using the capacitor before energy ran out and VCC dropped below a threshold.

We evaluated effects of freezing before vs. after charging when dipping capacitors in LN_2. In the *freezing before and after charging* approach, the freezing starts before the energy-storage capacitor is charged. The total freezing time before device starts running in this approach is 50s (20s before charging plus 30s while charging). In the *freezing after charging only* approach, the energy-storage capacitor is first charged, and freezing is then applied. The total freezing time before device starts running in this approach is also 50s (all after charging). In

Table 4. Freezing tests for 50s of freezing of capacitors on MSP430-class MCUs tested on FR5969 with P2110 harvester for two freezing approaches. The run times are average of three runs. The control run time was measured when no freezing was performed. With freezing, the run time is indeed 0s for both approaches.

Capacitor	Control	With Freezing
Freezing Before and After Charging Approach		
330 µF	0.009s	0.000s
470 µF	0.020s	0.000s
3,300 µF	0.180s	0.000s
Freezing After Charging Only Approach		
330 µF	0.009s	0.000s
470 µF	0.020s	0.000s
3,300 µF	0.180s	0.000s

Table 5. Freezing test for checking varying amount of freezing of capacitors before charging on MSP430-class MCUs tested on FR5969 with P2110 harvester. The control run time was measured when no freezing was performed.

Capacitor	Control	10s Freezing	20s Freezing
Freezing Before Charging Only Approach			
330 µF	0.010s	0.000s	0.000s
470 µF	0.020s	0.000s	0.000s
3,300 µF	0.160s	0.080s	0.016s

both approaches the total charging time is 30s and on-board switches are used to enable or disable connection to the energy-storage capacitor to ensure fixed charging time and that device only starts running (and thus consuming energy) after the charging and 50s of freezing are completed. For both approaches the capacitors were dipped in LN_2 and remained in LN_2 for the duration of the test. The results are shown in Table 4. As can be seen, with freezing the run time for both approaches is 0s.

Since the extended freezing of the capacitors resulted in run time approaching zero, we also evaluated different freezing times. In a modified *freezing before charging only* approach, the capacitors are frozen for different amounts of time before they are charged, then they are removed from LN_2 and charged for 30s and then the device is allowed to execute to measure run time. The results are shown in Table 5. As can be seen, for smallest capacitors, the devices still are not able to run. For largest capacitor, the run-time is cut by 50% with 10s of freezing, and cut by almost 90% with 20s of freezing.

Table 6. Example results of pouring LN_2 to perform a freezing attack on microcontroller when different supercapacitors were used for energy storage. The freezing time refers to how long the LN_2 was being poured over the supercapacitor.

Capacitor	Freezing Time	Run-time before Crash
0.22 F (FR5994 board)	0 s	204 s
	30 s	15 s
0.10 F (FR5969 board)	0 s	192 s
	30 s	27 s
0.05 F (P2110 board)	0 s	*device*
	30 s	*damaged*

7.4 Freezing Attacks on Energy Storage in Supercapacitors

In addition to electrolytic capacitors, we have evaluated three supercapacitors. The 0.22 F supercapacitor pre-installed on the `MSP430FR5994` development board, the 0.10 F supercapacitor pre-installed on the `MSP430FR5969` development board, and the 0.05 F AVX BestCap supercapacitor pre-installed on the `P2110-EVB` harvester kit board. For supercapacitor tests, the same testing software was used as in electrolytic capacitor tests. However, since the supercapacitors allow the device to run for hundreds of seconds, a stopwatch application was used to measure the run-time until the LED stopped blinking and device runs out of energy.

Table 6 shows the results of pouring LN_2 over the supercapacitors. It can be seen the freezing effect is also significant on the supercapacitors. Especially, with 30 s of pouring of LN_2, the code run-time before energy runs out is cut by over 85% for the capacitors. The exact run-time available depends on number of factors, such as how the LN_2 is poured. Also, note that the `MSP430FR5994` and `MSP430FR5969` boards have different power management circuitry and extensions (i.e. there are other differences than just the capacitor size), this can explain the similar run times, despite different capacitor values. However, the freezing effect has the same magnitude in stored energy reduction.

In addition to significantly reducing energy storage and causing premature crashes, we further observed that following multiple freezing attacks permanent damage can occur. In particular, the `P2110-EVB` harvester kit board was damaged following LN_2 pouring. While we leave analysis of destructive attacks as future work, one possible explanation of the damage are excess currents generated during the freezing that affected the harvester kit's logic and charging circuits. Thus deep freezing can not only produce transient effects, but also lasting device damage.

8 Discussion

To detect or defend the deep freezing attacks, different possible defenses can be deployed, as discussed below.

8.1 Alternative Polarized Capacitors

One potential passive defense for attacks on aluminum electrolytic capacitors includes switching to other types of capacitors, such as capacitors based on tantalum or niobium. Tantalum capacitors have added benefit of high capacitance per volume, but tend to be more expensive, about 4× more expensive compared to aluminum electrolytic capacitors. Niobium capacitors are an alternative to tantalum and have lower cost, but still are about 3× more expensive compared to aluminum electrolytic capacitors. Both types, however, are significantly less impacted by temperature changes.

8.2 Larger Capacitors

Based on our experiments, large capacitor sizes (larger volume) require longer freezing time for the attack to take effect. Consequently, a different passive mitigation, but not a full defense, is to use physically larger capacitors, e.g., use capacitors for larger voltage ratings, than what the target circuit requires.

8.3 Added Insulation

Alternatively, dedicated insulation can be added around capacitors or whole circuits as a passive defense. Freezing attacks would now require removal of the insulation, which would make the attack noticeable. However, insulation may cause circuits to overheat during normal operation.

8.4 Temperature Sensitive Packaging

Key to the attacks is that they are difficult to notice after the attack is finished since the packaging of the electronic components is mostly unchanged by the freezing. To allow for better detection of the attack after the attack has happened, temperature sensitive packaging or labeling could be used. Sample passive indicators could include labels that peel off due to extreme freezing, or paint that changes colors permanently after the freezing.

8.5 Temperature Sensors

As an active defense, temperature sensors can be deployed near critical electrolytic capacitors or circuits that use them, to detect the freezing attack. The system detection and response would have to happen within the short attack time, so that defensive action takes place before circuit is frozen. The filters could output an error signal if they detect unusual temperatures, or for the microcontroller scenario, additional checkpoints could be activated at run-time. However, in all cases, the freezing my affect the sensors themselves. Study of freezing impacts on sensors is orthogonal and future work.

9 Conclusion

This paper presented new deep freezing attacks on capacitors and electronic circuits that use them. This work demonstrated that liquid nitrogen can be leveraged to rapidly freeze electrolytic capacitors and supercapacitors to temperatures approaching −195 °C (−320 °F or 77 K). At these temperatures, electrolytic capacitors and supercapacitors cease to operate within their specification. As a proof-of-concept of real attacks, this work demonstrated that operation of electronic filters is affected by the freezing attacks and that filters can be made to attenuate (for high-pass filters) or pass (for low-pass filters) undesired frequencies when frozen. Meanwhile, for capacitor-power microcontrollers, this work demonstrated that the microcontrollers can be made to crash as energy storage is significantly reduced due to the deep freezing attacks. This paper thus highlighted a number of new threats that designers of electronic circuits should be aware of and also presented number of potential defenses that can be considered to mitigate the new threats.

Acknowledgment

This work was supported in part by NSF grant 1901901. The authors would like to thank Kelly Woods and the Yale University Cleanroom for assistance in obtaining liquid nitrogen used in the experiments.

References

1. Faltus, R., Flegr, Z., Šponar, R., Jáně, M., Zedníček, T.: DC/DC converter output capacitor benchmark. In: Annual Passive Components Symposium. CARTS Europe (2008)
2. Halderman, J.A., Schoen, S.D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J.A., Feldman, A.J., Appelbaum, J., Felten, E.W.: Lest we remember: cold-boot attacks on encryption keys. Communications of the ACM **52**(5), 91–98 (2009)
3. Jr., O.N., Morris, J., Giechaskiel, I., Szefer, J.: Chill out: Freezing attacks on capacitors and dc/dc converters. In: Proceedings of the European Test Symposium. ETS (2021)
4. Müller, T., Spreitzenbarth, M.: FROST: Forensic recovery of scrambled telephones. In: International Conference on Applied Cryptography and Network Security. ACNS (2013)
5. Ransford, B., Sorber, J., Fu, K.: Mementos: System support for long-running computation on RFID-scale devices. In: International Conference on Architectural Support for Programming Languages and Operating Systems. ASPLOS (2011)
6. Yitbarek, S.F., Aga, M.T., Das, R., Austin, T.: Cold boot attacks are still hot: Security analysis of memory scramblers in modern processors. In: International Symposium on High Performance Computer Architecture. HPCA (2017)