TimeTravel: Real-time Timing Drift Attack on System Time Using Acoustic Waves

Jianshuo Liu[1,2], *Hong Li*[1,2]*, *Haining Wang*[3], *Mengjie Sun*[1,2], *Hui Wen*[1,2], *Jinfa Wang*[1,2], *Limin Sun*[1,2]
[1] *Institute of Information Engineering, Chinese Academy of Sciences*
[2] *School of Cyber Security, University of Chinese Academy of Sciences*
[3] *Department of Electrical and Computer Engineering, Virginia Tech*
{liujianshuo,lihong,sunmengjie,wenhui,wangjinfa,sunlimin}@iie.ac.cn,hnw@vt.edu

Abstract

Real-time Clock (RTC) has been widely used in various real-time systems to provide precise system time. In this paper, we reveal a new security vulnerability of the RTC circuit, where the internal storage time or timestamp can be arbitrarily modified forward or backward. The security threat of dynamic modifications of system time caused by this vulnerability is called *TimeTravel*. Based on acoustic resonance and piezoelectric effects, TimeTravel applies acoustic guide waves to the quartz crystal, thereby adjusting the characteristics of the oscillating signal transmitted into the RTC circuit. By manipulating the parameters of acoustic waves, TimeTravel can accelerate or decelerate the timing speed of system time at an adjustable rate, resulting in the relative drift of the timing, which can pose serious safety threats. To assess the severity of TimeTravel, we examine nine modules and seven commercial devices under the RTC circuit. The experimental results show that TimeTravel can drift system time forward and backward at a chosen speed with a maximum 93% accuracy. Our analysis further shows that TimeTravel can maintain an attack success rate of no less than 77% under environments with typical obstacle items.

1 Introduction

Maintaining the stability of the internal clock is crucial in real-time digital systems. In these systems, the system time-based signal plays an important role in keeping the clock accurate. The real-time clock (RTC) is a kind of simple, low-power circuit consisting of several counters widely used in electronic devices to provide time base signals [1]. Due to its low power consumption, easy-integrated, and precise timing characteristics, RTC has become a necessity for upholding the rhythm of timing in many low-speed applications, such as scheduling tasks in industrial automation, health measuring by healthcare devices, providing interruption for smart vehicle devices, and ensuring transaction accuracy in financial systems.

*Hong Li is the corresponding author.

Typically, RTC is usually soldered onto a PCB board as an independent module or is embedded inside a microcontroller as an integrated timing unit [2]. For clock timing applications, RTC requires users to manually set the initial time (or use the NTP protocol [3] to obtain the time) and then store it in the counter. Afterward, RTC generates 1-second time base signals (calendar mode) and communicates with other components through the system bus. For timestamp timing applications, RTC generates millisecond-level timestamp signals (32-bit mode) through the collaboration of frequency dividers and counters, providing more accurate timing functionality. When the microcontroller receives the time or timestamp, it will forward the time to higher-level applications or smart devices for further processing. Although obtaining system time is simple, the process may lack the necessary verification mechanism, making the time vulnerable to manipulation. Previous research has demonstrated that time synchronization request packages sent by clients can be hijacked, which in turn tampers with the client's local time [4, 5]. Attackers can also slow down or speed up a Bitcoin node's network timestamp counter by connecting as multiple peers and reporting inaccurate timestamps, which may increase the chances of a successful double-spending.

While there has been extensive exploration into malicious modification of system time or timestamp, these explorations often remain at the network layer and only work under certain assumptions. One previous work [4] assumes that NTP servers fragment packets to a 68-byte MTU; however, many OSes (e.g., Windows and Linux) already avoid this trait. Internet of Things (IoT) devices are commonly not configured with NTP, due to the limitations of timer and network performance. Bitcoin transactions nowadays rely on authoritative timestamp servers, which can generate timestamps with digital signatures to prevent malicious tampering [6]. In addition, some devices are not connected to the Internet, and they only rely on local timestamps or relative variances in timestamps to maintain their work logic. If the system time is maliciously changed, it may have serious consequences, such as property damage to the organization due to incorrect execution of equipment

operations or even timing failure of medical equipment that threatens human lives. However, timing attacks under these scenarios without NTP support have not yet been well studied.

On one hand, attackers usually have limited privileges to access a target device, and thus it is challenging to modify the time or timestamp saved by RTC counters. For devices that use millisecond timestamps to maintain work logic, it is almost impossible for attackers to dynamically tamper with such fine-grained timestamps because of the inaccessibility of related interfaces. On the other hand, many devices are often exposed in public areas that attackers can access, which inspires us to explore from a different angle. Can attackers modify the system time or timestamp solely through physical channels without requiring additional privileges, while maintaining a certain physical distance from the target device?

In this paper, we explore the vulnerability of RTC concerning time modification from a new perspective. Specifically, we reveal that attackers can modify the time or timestamp inside the RTC without privileges to compromise the device or the network where the device is connected, thereby triggering a series of severe consequences. The attack vector is to apply acoustic vibrations to the medium surface (e.g., a desk) where the target device is placed. This kind of acoustic wave may cause additional resonance in the quartz crystal oscillator in the RTC circuit, and then stimulate additional electrical responses. Any interference to the signal output by the oscillator may affect the accuracy of the time-base signal, thereby affecting the timing accuracy. We discover that by applying specific carefully crafted acoustic signals and propagating them to the oscillator, an attacker could instantly adjust the device's time forward or backward at different speeds. We call such a security threat *TimeTravel*. To the best of our knowledge, this is the first work to explore the feasibility of modifying the internal system time or timestamp in RTC directly via physical interference, which may disrupt the operational logic of various devices. We assess the security risks of TimeTravel on nine off-the-shelf modules with the configuration of an RTC circuit, as well as seven commercial devices for real-life attack scenarios. Our experimental results show that TimeTravel can successfully adjust the system time at different drifting rates with a maximum 93% success rate, and achieves desired robustness under environments with physical obstacles.

The main contributions of this work are summarized below:

1. We reveal a new security threat TimeTravel, which is the first real-time system time modification attack via a physical interference channel. TimeTravel is capable of arbitrarily drifting the time or timestamp in RTC at different speeds.

2. We analyze the electrical response characteristics of a quartz crystal oscillator to acoustic vibration both theoretically and experimentally. We observe that the phase and amplitude of the time-based signal output by the crystal oscillator vary for acoustic signals with different phases and amplitudes. Based on the response analyses, we design the principles for modifying the RTC time.

3. We conduct a set of experiments to assess the security risk posed by TimeTravel on nine off-the-shelf modules and seven commercial devices and propose countermeasures against this security threat.

The remainder of the paper is organized as follows. Section 2 describes the background of a quartz crystal oscillator and sound propagation module. Section 3 presents the threat model, including the attack goal, common attack scenarios, and attack assumptions. Section 4 presents the detailed methods to modify the RTC time. Section 5 details the attack steps. Section 6 evaluates the performance of TimeTravel. Section 7 discusses countermeasures, safety recommendations, and the impact of NTP synchronization. Section 8 surveys the related work on acoustic attacks, and finally, Section 9 concludes the work.

2 Background

In this section, we present the characteristics and operational logic of a quartz crystal oscillator, as well as the principle of Lamb waves.

2.1 Quartz Crystal Oscillator

A quartz crystal oscillator is a kind of circuit featured by frequency selection, with a quartz crystal as its principal element [7]. The quartz crystal oscillator works under *Piezoelectric* effect [8], characterized by the crystal's periodic expansion and contraction in response to an applied alternating electric field. Such changes in the crystal's volume generate surface charges to offset the structural changes, thereby generating alternating electrical signals within the circuit.

The quartz crystal oscillator displays an exceptionally high-quality factor [9], resulting in reduced mechanical energy loss near its resonance frequency. This quality especially enables the crystal responsive to external vibrations close to this frequency, showcasing a swift piezoelectric response, typically in the microsecond range or less [7]. By contrast, at off-resonance frequencies, the crystal shows increased mechanical energy dissipation [7]. Therefore, the quartz crystal oscillator is distinguished by its enhanced precision and stability when compared to alternative oscillation devices like CMOS oscillators.

The type of crystal oscillator usually adopted in RTC circuits is called a Tuning-fork-shaped oscillator. The surfaces of the crystal are attached by electrode plating, which extends outward from the pins to the external circuit. The entire quartz crystal and electrodes are wrapped by a metal cover. In common oscillator designs, the quartz crystal plays the

role of the inductive component. The Pierce oscillator [9] is often preferred for quartz crystal oscillator circuits. This configuration employs two capacitors, which are connected to the ground and the quartz crystal, respectively, forming a π-shaped inductor-capacitor (LC) frequency-selective network. The inverting amplifier within a microcontroller unit (MCU) is used for providing positive gain to the circuit and introducing additional phase shifts to the signal, ensuring the oscillation signal's stability. With specific configurations of crystal properties and capacitance, the oscillator is designed to have a predetermined resonant frequency. Signals matching this frequency encounter the lowest impedance, facilitating their passage through the crystal [10].

The RTC circuit typically utilizes a quartz crystal oscillator, resonating at 32.768 kHz, to generate periodic timing signals. The signal emitted by the oscillator is fed into the counters within the RTC circuit to create a base signal. RTC supports second-level timing (calendar mode), and some RTCs support millisecond-level timing (32-bit mode). For the former, the built-in frequency divider uses a 16-bit counter to divide the crystal oscillator clock pulse into 1 second and output the second-level clock pulses. The latter will be divided into millisecond or microsecond-level clock pulses for accurate timestamp counting. When the rising edge of the oscillation signal exceeds the threshold, the frequency division counter will decrease its stored value by 1, until the counter value drops to 0, and then the counter will trigger a clock pulse and reset. The triggered pulse should be the time-base signal after frequency division.

2.2 Propagation of Sound in Solid Medium

Sound is a vibrational disturbance that travels as an acoustic wave through mediums, such as fluids and solids. In a solid medium, sound waves can cause both volume deformation (the change in the overall volume of a solid) and tangential deformation (relative displacement or rotation of particles within a solid). In an isotropic medium, the direction of vibration indicated by this shear is perpendicular to the direction of wave propagation [11].

Sound waves propagate in different forms inside and on the surface of a solid medium. Inside a solid medium, sound waves mainly propagate as longitudinal waves. By contrast, sound waves propagate as guide waves - surface waves (e.g., Rayleigh waves [12]) or Lamb waves on the surface. When the thickness of the solid medium is at least several times larger than the wavelength of the sound wave, surface waves become the dominant form of propagation. Surface acoustic waves attenuate quickly after leaving on one side of the solid surface, usually not exceeding a few wavelengths of depth. However, when the solid medium is relatively thin (usually no larger than several times the wavelength), Lamb waves should be the main waveform, and both the top and bottom of the solid surfaces will propagate vibrations [11]. Since most devices are placed on a table no more than a few centimeters thick, we focus mainly on Lamb waves.

Lamb waves propagate on solid surfaces with two different modes: Symmetric and Anti-symmetric [13]. These two sets of waves with different modes can propagate independently on the same surface of the solid. Assuming that the Lamb wave propagates in the XZ-plane in the Z-direction. Anti-symmetric Lamb wave components primarily displace the solid media in the X-direction, whereas symmetric Lamb waves mainly cause displacements in the Z-direction [13].

For most kinds of solid medium, driven by low-frequency acoustic excitation signals (usually less than 100 kHz) [14], they will excite the first-order Lamb wave pattern with the same natural angular frequency as those of excitation signals (see Appendix B). Since TimeTravel focuses on the displacement of the medium along the X-direction, the equation for the displacement of the medium along the X-direction for a specific location z can be expressed as:

$$\xi = \gamma + \lambda \sin(\omega t + \Phi), \tag{1}$$

where ω represents the angular frequency of the excitation sound wave, and t represents the time. The detailed definition of the coefficient γ, λ, and Φ can be found in Appendix B.

3 Threat Model

In this section, we introduce the attack goals and assumptions.

3.1 Attack Goal

This work reveals a serious security risk: time data stored within the RTC circuit can be affected by external acoustic disturbances. Specifically, if a device relies on system time for specific tasks, it may experience a time drift. This drift can be either forward or backward, triggered by well-designed acoustic vibrations. The operational logic and states of these devices can be altered, leading to several potentially severe consequences. Such a vulnerability widely exists in our daily lives. As illustrative examples, we consider real-life scenarios where patients measure and record their basic vital signs, such as blood pressure and heart rate via a digital blood pressure (BP) monitor at a clinic's front desk, before their consultation with doctors (Fig. 1(a)); customers use POS machines to check out at self-service restaurants or shops (Fig. 1(b)). All of these devices use the RTC to accomplish specific tasks: the RTC 32-bit mode counters in a BP monitor generate millisecond timestamps to the microcontroller to process the measured pressure signals and control the deflating of the cuff; POS machines use the RTC to read the time and create the records of operations with specific timestamps.

The adversaries' goal is to intentionally emit acoustic wave sequences with specific frequencies for certain purposes. The wave sequence is transmitted to a target device through a

(a) Digital blood pressure monitor.

(b) Commercial portable POS machine.

(c) Traffic light controller.

Figure 1: IoT devices containing real-time clock.

solid surface (e.g., a table), and then it can modify the timestamps generated by the device. For example, attackers can maliciously adjust the measurement data of a blood pressure monitor by adjusting internal timestamp, causing the measurement data to be either too high or too low, which will pose a serious health threat even a life threat to a patient as doctors would be misled to take wrong medical treatments to the patient (e.g., issuing anti-hypertensive drugs, but the actual patient's complaint symptoms are not caused by high blood pressure). For a POS machine scenario, attackers can deliberately adjust the timestamp forward or backward to fall into the promotion time of some commodities, and purchase them with much lower price, resulting in substantial financial gains to themselves but losses to merchants. Furthermore, RTC timestamp also plays a key role in many daily scenarios, like traffic light controlling (Fig. 1(c)), industrial automation, autonomous driving, and networking systems. The timing drift in those mission-critical systems will pose serious threats to the society.

3.2 Attack Assumptions

We make the following assumptions when mounting the aforementioned attacks.

Attack Requirements. TimeTravel is a close-proximity attack; however, attackers only need to modify the time or timestamp of a target device in a controllable way by using acoustic guide waves. Attackers can carefully select the attack parameters to ensure the interference during the attack only affects the crystal oscillator and will not cause any human-perceived abnormalities in the surrounding environment.

Attacker's Prior Knowledge. We assume that attackers can test the target device on similar mediums under different amplitudes and initial phases of excitation signals, and can verify the corresponding front-end behaviors in advance. This allows attackers to establish the $\varphi \rightarrow \beta_1$ phase mapping (see Section 4.2). Attackers can purchase devices of the same models to conduct the testing.

Attack Equipment Setup. We assume that attackers place a piezoelectric transducer and a magnetic probe in proximity to the target device, for emitting guided waves and analyzing the EM signals leaked from the target device, respectively. In end-to-end attack scenarios, attackers can access the area surrounding the target device (e.g., a table) in advance and position a transducer either in front of or behind the device. A magnetic probe must be strategically placed beneath the device to capture leaked electromagnetic (EM) signals. Attackers can test the target device while it is left unattended in the actual attack environment, to establish the $\varphi \rightarrow \beta_1$ mapping. Based on the mapping and the actual distance between the transducer and the device, attackers select the phase of the oscillating signal detected by the probe. Then they attempt to emit an excitation signal that corresponds to the lowest amplitude of the superimposed oscillating signals. If the phase amplitude of the oscillator decreases and stabilizes during testing, the attack setup is confirmed to be calibrated and ready for use. To enhance concealment, attackers can attach adhesive tape to the surface of the magnetic probe and transducer, or cover them with camouflage materials. To generate and amplify attack signals, attackers need to use a USRP and a signal amplifier, but they can place/hide them far away from the attack plane.

4 Attack Mechanism Exploration

In this section, we theoretically explore the injection of attack signals into the RTC circuit for affecting its timing. We then discuss how to design the signal parameters to cause the RTC timestamp to drift forward or backward, followed by simple experimental validations.

4.1 Principle of Attack Signal Injection

TimeTravel leverages the sensitivity of the crystal oscillator to resonant frequency by applying additional mechanical vibrations. These vibrations may generate extra electrical signals, thereby altering the characteristics of the original oscillation signal in the circuit, with the intent of influencing the RTC's timing.

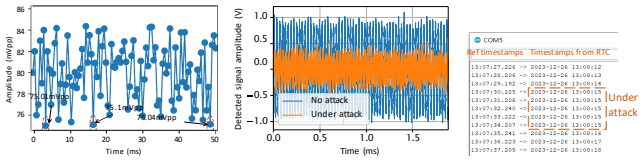
To introduce mechanical resonance interference in the crystal oscillator, TimeTravel utilizes a solid medium with the aid of acoustic mechanical displacement, instead of directly emitting ultrasonic waves in the air (see details in Appendix A). This method propagates emitted mechanical energy into the crystal oscillator. Driven by the vertical displacement of a mass at a specific location on the surface of a solid medium, the rigid object attached to the surface at that location moves vertically with the same acceleration as a whole. Given that the electrodes are affixed to both ends of the quartz chip and their extended pins are soldered onto the PCB, the quartz crystal oscillator as a whole is thus compelled to undergo the same accelerated mechanical movements as part of the motherboard to which it is attached. When the frequency of the mechanical vibrations applied to the crystal matches its resonant frequency, the crystal induces an additional resonant electrical response. The frequency of this electrical response

should be consistent with the frequency of the imported mechanical vibrations.

4.2 Principle of Time Drifting Backward

The influence of resonance response on the crystal's vibration is determined by the phase and amplitude difference between the response of imported vibration and the original resonant signal in the circuit. To achieve a backward drift of time relative to the current time, the key is to slow down the rate at which the time counter updates as much as possible. Based on signal superposition principle, attackers need to ensure that the phase of the injected electrical signals into the oscillator β_1 and the phase of the original oscillation signal β_2 differ by as close to π as possible. This way, $\cos(\beta_1 - \beta_2)$ approaches -1, and ϕ reaches its minimum value.

As mentioned in Section 4.1, attackers generate mechanical vibrations from a certain distance to the target device, inducing the crystal oscillator to produce additional electrical responses. The mechanical vibration of the crystal oscillator can be summarized as a cantilever beam vibration system under dynamic loads. Given the overall acceleration caused by external mechanical excitation $a(t) = A\sin(\omega t + \varphi)$, there is a proportional relationship between the stress and electric displacement vector caused by mechanical deformation: $D \sim \sigma \sim \sin(\omega t)$. Thus, the initial phase of the electrical response signal β_1 typically does usually not match the initial phase of the mechanical acceleration experienced by the crystal oscillator. This discrepancy is affected by the intrinsic properties of the quartz crystal (e.g., damping and stiffness). Additionally, other nonlinear components in the oscillation circuit may introduce a constant phase shift in the signal. These factors make it challenging to directly calculate the initial phase of the electrical response signal β_1, which is excited by the crystal's mechanical resonance when a specific phase of the electrical signal is applied to the transducer and propagated via mechanical vibration. Instead, we propose an experimental method to determine the mapping relationship between the phase of the excitation signal to the transducer φ and the injected electrical response signal β_1. Attackers can choose the horizontal distance z between the transducer and the crystal, as well as the initial phase φ of the excitation signal, and use a magnetic probe placed below the crystal oscillator to record the current oscillation signal phase β_2 in the circuit, and then immediately emit the signal. The excitation signal will reach the crystal after the propagation delay time t_T, leading to the possible amplitude and phase changes of emanated signals from the crystal oscillator. Attackers can keep $\{z, \varphi\}$ the same and emit signals at different times, after collecting sufficient samples, attackers then obtain values of z, φ, and β_2 that result in the relatively lowest observed EM signal amplitude. At this point, $\beta_1 - \beta_2$ should approach π, then attackers can further establish a mapping table $\{z, \varphi\} \rightarrow \beta_1$(note that $\beta_1 = \beta_2 + \pi$). Meanwhile, if φ changes x (i.e., $\varphi \leftarrow \varphi + x$), β_1 will change x accordingly.



(a) (b) (c)

Figure 2: Experimental results on the backward drift of time.

In the subsequent attack, attackers can select the phase φ and the attack distance z, mapping it to β_1. After observing that the phase of the signal emitted by the oscillation circuit reaches $\beta_2 = \beta_1 - \pi$, attackers immediately transmit and maintain the attack signal, so that the signal amplitude outputted from the oscillator will remain stable at a relatively low value after interference. The value k_a in Eq. 1 can be determined by solving Eq. 2 [15], which refers to the characteristic equation of Lamb waves:

$$\frac{\tan(\sqrt{\frac{\omega^2}{c_L^2} - k_a^2}\,d)}{\tan(\sqrt{\frac{\omega^2}{c_T^2} - k_a^2}\,d)} = -\frac{4\sqrt{(\frac{\omega^2}{c_T^2} - k_a^2)(\frac{\omega^2}{c_L^2} - k_a^2)}\,k_a^2}{(\frac{\omega^2}{c_L^2} - 2k_a^2)^2}, \quad (2)$$

where the angular frequency $\omega = 2\pi f$, d represents the thickness of the solid medium, and c_L and c_T represent the velocities of longitudinal and transverse waves inside the medium, respectively, which can be found in Table 3.

To verify the feasibility of time drifting backward, we conduct a sample experiment by employing a USRP N210 equipped with an amplifier to generate sinusoidal signals at a frequency of 32.768 kHz, an initial phase $\varphi = 0$ and an amplitude of 20Vpp. Other experimental apparatus includes an acrylic glass plate with a 5 mm thickness and a piezoelectric ceramic transducer with 3 cm in diameter and 2 mm in thickness. This transducer is connected to the amplifier, facilitating the transmission of Lamb waves to the glass plate. We integrate a DS1302 RTC module with an Arduino Uno Rev3 board using DuPont wires for further experimentation. The ceramic transducer is positioned roughly 5.5 cm from the RTC module's quartz oscillator, with a magnetic field probe placed directly behind the glass plate beneath the module, as depicted in Fig. 17. We emit pulses of 0.3ms duration at 0.5ms intervals, measuring the signal amplitude at the crystal oscillator both before and during these emissions over a 50ms period. We observe that the detected amplitudes of oscillating signals, as presented in Fig. 2(a), have significant reductions at 3.2 ms, 16.3 ms, and 48 ms, with recorded values of 75.01mVpp, 75.1mVpp, and 75.04mVpp, respectively; the phase of oscillating signals β_2 at these timestamps is around 0.56 deg. These values represent approximately 93.8% of the baseline amplitude of 80mVpp, suggesting that the initial phase of the electrical signal injected into the crystal oscillator

should be $\beta_1 = (3.14 + 0.56)$ deg. We further observe that the peak-to-peak amplitude of the superimposed signals remains consistently low during the attack. We increase the amplitude of the excitation signal and observe that as the amplitude increases, the detected oscillation signal amplitude gradually decreases. When the applied signal amplitude reaches 65Vpp, we notice that the oscillation signal's maximum amplitude decreases and then stabilizes at 36mV (Fig. 2(b)). Additionally, we observe that the RTC module's timing stops (Fig. 2(c)), but it resumes to normal once the attack ceases.

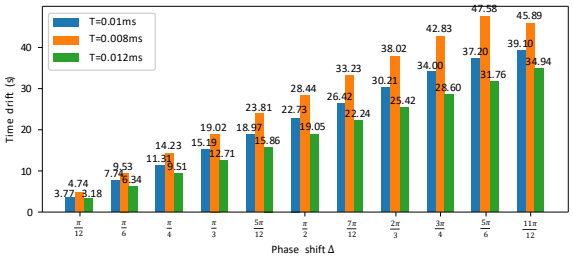
4.3 Principle of Time Drifting Forward

To expedite clock timing, attackers should design attack signal sequences to alter the phase of oscillation signals, thereby ensuring that the amplitude of oscillation signals exceeds the edge-triggering threshold more frequently. Assume that the initial phase of the electrical interference sinusoidal signal caused by the acoustic vibration is β_1, and the phase of the oscillation signal in the oscillator is β_2. We denote β_1 as $\beta_1 = \beta_2 + \Delta$. According to signal superposition principle, the phase of the superimposed signal can be expressed as:

$$\begin{aligned}\beta_2' &= \frac{\beta_1+\beta_2}{2} + \arctan\left(\frac{A-B}{A+B}\cdot\tan\left(\frac{\beta_1-\beta_2}{2}\right)\right) \\ &= \beta_2 + \frac{\Delta}{2} + \arctan\left(\frac{A-B}{A+B}\cdot\tan\left(\frac{\Delta}{2}\right)\right), \end{aligned} \tag{3}$$

where A, B refer to the amplitude of attack electrical signal and oscillation signal, respectively. The superimposed oscillation signal will have a new phase $\beta_2'(0 < \beta_1 - \beta_2' < \Delta)$, and will be immediately amplified by the feedback network and then sent back to the quartz crystal. The oscillation signal with phase β_2' will further overlap with the interference signal applied by attackers. After a period of time, the phase difference between the electric resonance signal of the crystal oscillator and the attack signal will gradually decrease until the phase remains consistent. Finally, the phase of the oscillation signal will be Δ earlier than before being attacked. Afterward, attackers can continue to emit attack signals with a phase difference of Δ from the current oscillation signal, causing the phase in the oscillation signal to continuously drift forward.

Using the superposition of signals of the same frequency to change the phase is equivalent to phase modulation, which broadens the signal spectrum in the frequency domain [16]. When the attack lasts for a period of time (usually not exceeding a dozen microseconds), the frequency band around the 32.768 kHz should gradually narrow and coincide with the central frequency. Then, it can be assumed that the phase of the oscillation signal in the circuit converges to the injected attack signal. Attackers can observe the phase of the oscillation signal at an appropriate time based on the phase mapping $\{z, \varphi\} \to \beta_1$ obtained in Section 4.2, causing β_2 to move Δ forward. After the phase of the oscillation signal converges and stabilizes, attackers can continue to shift the attack signal



(a)

Figure 3: Experimental results on forward drift of time.

phase forward by Δ, to induce β_2 to shift forward by Δ. After each attack, attackers will force the next rising/falling edge level trigger time to arrive $\frac{\Delta}{2\pi}$ earlier, as shown in Fig. 15. Considering that the interval between the rising and falling edge trigger points equates to half an oscillation cycle, attackers can establish $0 < \Delta < \pi$ to ensure the integrity of the edge triggering.

To validate the feasibility of time drifting forward, we use a 5 mm-thick acrylic glass plate and place the transducer 3 cm next to the DS1302 RTC crystal, and then when we observe that the oscillation signal emitted by the oscillator has a phase of $\frac{\pi}{2}$, we begin to emit excitation signals of 32.768 kHz that cause the oscillation signal phase to shift forward Δ. After every T ms of attack, attackers shift the phase of the excitation signal forward by Δ. We set the amplitude of the excitation signal to 65Vpp, the phase shift offset $\Delta = \frac{n\pi}{12}(n = 1, 2, ..., 11)$, and $T = 0.008, 0.01, 0.012$ ms. For each phase offset, we emit attack signal sequences 30 s and repeat the test 50 times. For each selected phase offset, we record the average offset of the time change read by RTC relative to the reference time change, as shown in Fig. 3(a).

Overall, the time drift of RTC increases with the increase of phase drift in a single attack. When the phase drift is $\frac{\pi}{12}$, the cumulative time drift under the three attack durations does not exceed 5 s. When the phase drift is $\frac{11\pi}{12}$, the timing rate of RTC is at least doubled. Meanwhile, the duration of the excitation signal emission also affects the final time drift. When the duration of signal transmission attacks is shortened, the overall time drift will increase accordingly. Under the phase shift $\Delta = \frac{11\pi}{12}$, the change in attack time from 0.012 ms to 0.008 ms will result in an additional time drift of approximately 13.75 s. This is because when the duration of the attack signal is shortened, the phase of the oscillation signal will shift forward more frequently, causing the oscillation signal to cross the edge trigger level more frequently. Under relatively long attack signal duration, the phase of the oscillating signal will change synchronously with the attack signal after converging to be consistent with the attack signal, without causing any additional phase shift and time forward drift. However, if the attack duration is too short ($T = 0.008$ ms), we observe that under a large phase drift $\frac{11\pi}{12}$, the crystal does not fully respond to the vibration mode of the attack signal, resulting

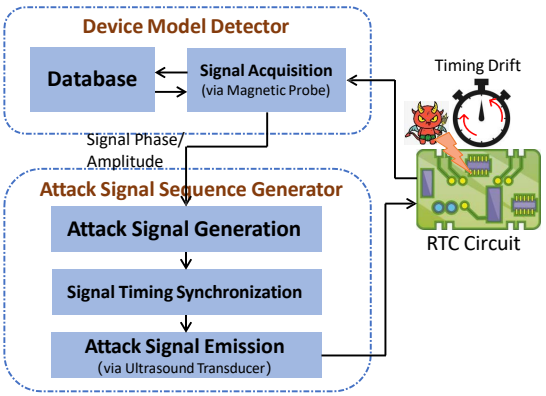


Figure 4: The general design of the TimeTravel attack scheme.

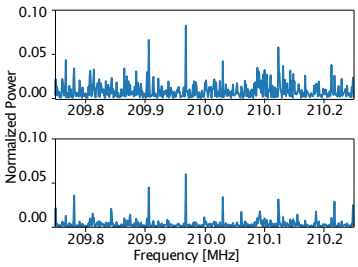


Figure 5: Undenoised signal FFT result (top) and denoised signal FFT result (bottom).

in the oscillation signal bandwidth still not approaching 0 at the end of a single attack, that is, the oscillation signal phase does not converge to the attack signal. Therefore, time does not drift forward steadily at a specific rate, resulting in an unexpected increase in time drift.

5 Attack Design

After exploring the feasibility of transmitting sound waves through acoustic transducers to affect the accuracy of clock timing within RTC, we now present the design principles for TimeTravel to achieve controllable and quantitative time drift attacks. To mount a successful attack, attackers should address the following two key challenges: (1) How to identify device models to match appropriate attack parameters? (2) How to configure the parameters of the attack signal (e.g., attack distance, phase, interval, and amplitude) to achieve the desired timing rate? Specifically, we elaborate on the design of the TimeTravel attack scheme, including the methods for identifying the model of devices, as well as attack signal configuration, as shown in Fig. 4.

5.1 Detection of the Target Device's Model

Different devices typically use distinct PCB materials, layouts, and RTC crystal oscillator models, resulting in varied stress distributions and vibration response characteristics under mechanical vibration. Detecting the model of the target device allows attackers to choose an appropriate attack strategy. One method is to leverage the frequency uniqueness of MCU clock signal components to recognize device models.

Attackers can use a magnetic probe to collect electromagnetic signals leaked near the device's MCU chip over a fixed period. After acquiring the raw EM signals, TimeTravel scales and normalizes the signal to balance the impact of detection distance on signal strength. Assume that the original signal sequence is $x = \{x_0, x_1, ..., x_n\}$, TimeTravel maps the original signal amplitude to $-a$ to b mV $(a, b > 0)$ through a linear transformation according to Eq. 4:

$$x_{scaled} = -a + (\frac{x - x_{min}}{x_{max} - x_{min}} \cdot (b + a)), \tag{4}$$

where x represents the original sample value, and x_{min} and x_{max} represent the minimum and maximum values in the original sample data, respectively.

Manufacturers typically use spread spectrum clocks (SSC) to generate the MCU clock signal, distributing the clock signal energy over a unique frequency band for electromagnetic compatibility. The SSC signal can be expressed as $V(t) = A\sin(2\pi f_0 t + \Delta f \frac{f_0}{f_m}\sin(2\pi f_m t))$, where f_0 is the center clock frequency, and f_m and Δf are the modulation frequency and frequency offset, respectively. These parameters are determined by the MCU's hardware configuration and manufacturing process differences. Attackers can investigate the MTU clock center frequencies f_0 of the target device in advance and add them to the collection G_0. After capturing a fixed length of the electromagnetic signal, TimeTravel iteratively selects f_0 in G_0 as the center frequency and uses a band-pass filter with f_0 as the center frequency and a preset bandwidth M to reduce the overall signal bandwidth. Furthermore, TimeTravel uses wavelet denoising to filter out noise unrelated to the spread spectrum clock signals. For instance, the denoised probing signal from the core MCU of the Omron HEM-7132, as shown in Fig. 5, demonstrates that after normalization and denoising, the detection of clock frequency components in the distance of 2 cm from the device's bottom can be enhanced with higher SNR.

To further identify subtle differences in f_0, f_m, and Δf among different device models, we use a CNN to classify one-dimensional signal sequences. The network consists of alternating convolution and pooling layers, followed by a softmax layer that classifies the input signal fragments into the device models in the database and outputs the classification confidence for each model. The detailed structure of the model is shown in Table 7. If the confidence level for all models is low in the output layer, it indicates that the target device model is not in the attacker's database, and TimeTravel will not proceed with the classification step.

5.2 Attack Acoustic Sequence Generation

Once attackers determine the model of the target device, they can design attack signal sequences to drift the target device's system time/timestamp at a certain rate. For time drifting forward and backward, there are different signal sequence generation strategies.

5.2.1 Time Drifting Backwards

The backward drift of time is achieved by utilizing the static logic characteristics of the RTC time counter. However, some RTC time counters may freeze if they do not detect an edge trigger for an extended period, remaining frozen until the device is restarted. To prevent time freezing, it is necessary to distribute the expected time drift length as evenly as possible throughout the entire attack period for accumulation. Assume that attackers expect the internal time in RTC to drift backward by b time units within a time units ($a > b$). If b exceeds the time threshold that causes RTC to freeze, they can design the sequence of attacks by continuously emitting attack signals for t, then stopping the attack for $\frac{a-b}{\frac{b}{t}-1}$. Here t should be less than the maximum attack duration that causes RTC to freeze. Attackers should repeatedly send the attack sequence $\lceil \frac{b}{t} \rceil$ times so that the time drift of b time units is evenly distributed across the attack duration of a time units.

After launching an attack, attackers need to calculate the phase of the oscillation signal after $t + \frac{a-b}{\frac{b}{t}-1}$ units, and then send an excitation signal corresponding to the attack phase at $t + \frac{a-b}{\frac{b}{t}-1} - t_T$, where t_T represents the time required for Lamb waves to propagate from the transducer to the crystal oscillator, as mentioned in Appendix B.

5.2.2 Time Drifting Forward

The forward drift of time is achieved by accelerating the time interval of the oscillation signal reaching the edge trigger threshold.

Assuming that attackers expect the time to drift forward by b time units within a time units, under the maximum time drift range allowed by the attack parameters. To evenly distribute the time drift throughout the entire attack, attackers can choose the duration $t_1 > 0$ of a single attack signal transmission and the interval $t_2 > 0$ between two consecutive attack signals. Throughout the entire attack, attackers need to emit k attack signals, where k and t_2 satisfy:

$$\begin{cases} k = \lceil \frac{2\pi b}{\Delta} \rceil \\ t_2 = \frac{a - t_1 \lceil \frac{2\pi b}{\Delta} \rceil}{\lceil \frac{2\pi b}{\Delta} \rceil - 1}, \end{cases} \tag{5}$$

where Δ refers to the amount of the oscillation signal phase to drift forward. Due to $t_2 > 0$, the time drift assumed by attackers should satisfy $a > \lceil \frac{2\pi b}{\Delta} \rceil t_1$.

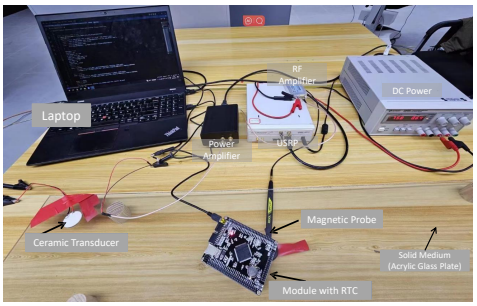


Figure 6: Experimental setup of the TimeTravel evaluation.

6 Experiment

In this section, we first elaborate on our experimental setup and then evaluate the overall performance of TimeTravel.

6.1 Experimental Setup

6.1.1 Attack Device

We use a RIGOL NFP-3 magnetic field probe set to sense the magnetic field emanating from the crystal oscillator. The probe is connected to an RF probe amplifier (frequency from 10 kHz to 1 GHz) to increase the amplitude of the sensing signal and filter noise. The received signal is transferred to a laptop by ETTUS USRP N210 for signal analysis and synchronization. For Lamb wave transmission, we adopt a Taimi ultrasonic piezoelectric ceramic transducer (resonance frequency band $15 \sim 35$kHz, maximum supporting voltage 240Vpp) and connect to FPA101A power amplifier as well as USRP to emit the Lamb wave acoustic signals.

6.1.2 Device Under Testing

We use four standalone RTC timing modules to test the attack performance of TimeTravel without any irrelevant circuit components, and five types of ARM development boards to test the attack on the RTC circuit under a general IC layout configuration. These boards/modules are listed in Table 1. For testing standalone RTC modules, we use the Arduino UNO R3 development board, connecting it to the modules to send commands and analyze returned time responses. The experimental setup is shown in Fig. 6. To verify in real scenarios, we test one commercial POS machine (Kaidianbao POS) and six commercial electronic blood pressure monitors (Omron HEM-7132, HEM-7124, HEM-7121; Xiaomi MI-BPX1; HYNAUT AXD-808; Yuwell YE660D). For the testing environment, we use aluminum, wood, acrylic glass, and hard plastic plates of different thicknesses as the solid medium for sound propagation. We set up the layout of our testing environment into two scenarios: In the first scenario, we position the module subjected to the attack on the surface of the solid medium. In the second scenario, besides placing the module on the medium's surface, we also place extraneous

Table 1: The Success Rates under Different Modules/Boards with RTC and Parameter Configurations.

#	Module	Pw.↑	Pw.↓	↓5s	↓25s	↓5.5s	↓20.05s	↑25s	↑45s	↑20.5s	↑40.05s
1	DS1302	68.2V	75V	89%/ 2.519[1]	87%/ 2.519	—	—	88%/ 1.009	90%/ 1.979	—	—
2	DS1307	67.1V	76V	88%/ 2.515	90%/ 2.515	—	—	88%/ 1.005	85%/ 1.975	—	—
3	PCF8563T	66.9V	73V	89%/ 2.521	85%/ 2.521	—	—	91%/ 1.011	86%/ 1.981	—	—
4	DS3231	64.6V	75V	91%/ 2.527	89%/ 2.527	—	—	88%/ 1.017	87%/ 1.987	—	—
5	STM STM32-F103ZET6	71.8V	79V	**93%**/ 2.535	89%/ 2.535	87%/ 2.535	86%/ 2.535	87%/ 1.025	86%/ 1.995	85%/ 0.844	87%/ 1.922
6	Alientek XC6-C6SLX16	71.1V	95V	84%/ 2.518	85%/ 2.518	85%/ 2.518	86%/ 2.518	84%/ 2.79	85%/ 2.395	84%/ 0.827	82%/ 1.905
7	Alientek STM32-F103ZGT6	72.3V	94V	85%/ 2.519	**83%**/ 2.519	86%/ 2.519	84%/ 2.519	84%/ 2.791	84%/ 2.399	**81%**/ 0.828	**78%**/ 1.906
8	Alientek STM32-F407ZGT6	71.9V	86V	89%/ 2.536	88%/ 2.536	90%/ 2.536	85%/ 2.536	85%/ 2.809	87%/ 2.413	86%/ 0.845	81%/ 1.923
9	DINGCHANG DC-A566	73.2V	88V	89%/ 2.921	91%/ 2.921	**92%**/ 2.921	89%/ 2.921	**83%**/ 2.801	85%/ 2.396	89%/ 0.83	**90%**/ 1.908

* The initial phase of the excitation signal applied by attackers to the transducer, expressed in radian (rad); Pw.↑ and Pw. ↓ refer to the minimum power transmitted to transducer, to cause the desired forward and backward timing drift, respectively.

items around the module (see Fig. 18). The second scenario is specifically designed to assess the robustness of TimeTravel.

6.1.3 Evaluating Metrics

Our evaluation is based on the following metrics. (1) **Success rate** is defined as the average probability of reaching the expected time drift within a specified time, under different configuration conditions. (2) **Processing delay** is the time interval when the target phase signal is captured from the oscillator circuit to the beginning of the emission of the acoustic attack signal from USRP. (3) **Robustness** assesses the ability to maintain a successful attack when there are some unrelated objects on the surface of the solid medium, where the attack target is located.

6.2 Performance Evaluation

In the experiment, we send commands to ARM/Arduino development boards to record the time from RTC counters. During the testing, we continuously adjust the vertical distance between the magnetic field probe and the oscillator, as well as the amplitude of the excitation signal to the transducer, to determine the maximum effective distance for detecting the phase of the oscillation signal and the minimum signal energy required to cause all desired time drift speeds. For the analysis on commercial devices, due to the inability to directly access the RTC time data, we evaluate the impact of TimeTravel on RTC through the relevant data output from the device (e.g., blood pressure, pulse, and transaction time).

6.2.1 Success Rate

A. General Attack Accuracy. (1) Evaluation on RTC modules/development boards: We utilize a 5 mm-thick acrylic glass plate as a medium for the experimental setup. The transducer is placed on the top surface of the plate, about 20 cm horizontally from the RTC crystal. We place a magnetic probe on the reverse side of the plate, aligning it with the location of the crystal. We conduct over a 30-second attack for each test and set the single attack duration of 0.009 ms for time forward drift scenarios. We carefully calibrate the amplitude and initial phase of the excitation signal to align with the expected time drift. For each module under test, we standardize the phase of the oscillating signal, observed at the onset of the attack, to zero. Table 1 shows the efficacy of attacks across nine modules, delineating different attack parameters and expected time drift scenarios. The results demonstrate that TimeTravel can effectively induce time drift in RTC across all modules, albeit at different drift speeds. Specifically, the success rate of mounting time modification attacks at a coarse granularity of 1 s varies from 83 % to 93 %. For a granularity of 0.1 s, this rate ranges between 81 % and 92 %, and for 0.01 s, it ranges from 78 % to 90 %. Note that since the selected standalone RTC modules lack the capability of outputting the time at the fine-grained millisecond level, we exclude these modules from the attack tests at the 0.1 s and 0.01 s granularities. The results indicate that no obvious correlation exists between the attack complexity and the precision of the desired time drift.

(2) Evaluation on representative commercial devices: Any changes in the timing rate of the BP monitor timing counter

(a) (b)

Figure 7: A commercial BP monitor setup in a real clinic environment.

can cause measurement errors in systolic and diastolic blood pressure (see Appendix D for details). We conduct the experiment in a real clinic environment, in which an Omron HEM-7132 BP monitor is placed on a table in the waiting area outside the clinic diagnosis room. The table is made of polyethylene with a thickness of 1.5cm. We position the transducer 10cm horizontally from the center of the backend enclosure of the monitor and place the magnetic field probe below the RTC crystal oscillator. The volunteer sits at the table like a regular patient, placing the arm on the table to measure blood pressure. The real clinic experiment scenario is shown in Fig. 7(a).

Before launching the attack, the volunteer's blood pressure is measured at 122/74 mmHg (Fig. 7(b)). When the EM signal phase is observed to be $\pi/2$, we transmit an excitation signal of 98V, 2.16 rads with an interval of 0.014 ms, and repeat the test five times. We observe that the average measured blood pressure of the volunteer decreases to 101/57 mmHg (Fig. 8(c)), with systolic and diastolic pressures decreasing by 17% and 23%, respectively, and the cuff deflation speed slows down. When we emit continuous attack signals, the cuff nearly stops deflating, and the screen displays an E1 error (Fig. 8(d)). Meanwhile, we observe that the amplitude of the oscillating signal decreases from approximately 100 mVpp to 77 mVpp and remains stable, indicating that the phase of the induced electrical signal is π out of the phase with the oscillating signal, causing the timing rate f decreasing nearly to 0Hz and the valve then stops deflating (i.e, $v' \to 0$). Based on the established $\varphi \to \beta_1$ mapping, we fix the excitation signal voltage at 100V and adjust the signal phase to 2.3 and 2.31 rads, while maintaining a transmission interval of 0.01 ms. We report that the cuff deflation speed gradually increases, and the measured blood pressures are 142/96 mmHg (Fig. 8(a)) and 158/105 mmHg (Fig. 8(b)), respectively. For every 0.01 rads increase in phase, the systolic and diastolic pressures increase by approximately 11% and 9%, respectively.

We further follow the same testing procedures and attack device setup on a real Kaidianbao POS machine scenario. We observe that when an excitation signal with a phase difference of π relative to the oscillating signal is transmitted, the timestamps recorded in the database for two consecutive card

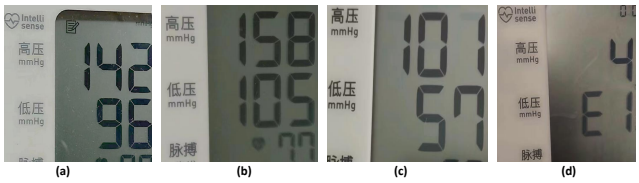
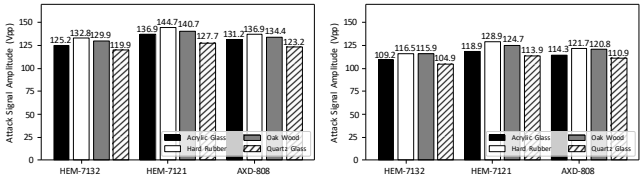


Figure 8: Experiment results on HEM-7132.

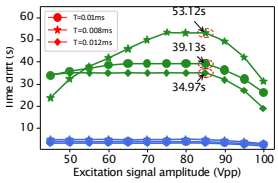


(a) Blood Pressure to 180mmHg. (b) Blood Pressure to 90mmHg.

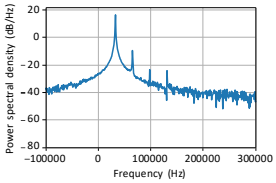
Figure 9: The minimum energy required for different BP monitors to attack under different solid materials.

swipes within a few seconds are identical. With a constant transmission interval, a phase shift of 0.005 radians in the attack signal results in a forward time drift of approximately 5 seconds. Since both kinds of devices leverage timestamps to sense physical signals/perform operations, we envision that any device with those sensing/operating mechanisms will be vulnerable to TimeTravel, posing severe security risks.

B. Impact of Medium Materials. The material of the solid medium plays a crucial role in the dispersion characteristics of waves and the amplitude of vibrations perpendicular to the medium's surface. To investigate the correlation between the minimum amplitude of the excitation signal and a successful attack, we first employ three representative modules/development boards listed in Table 1 and place them respectively on four different mediums of 5 mm-thickness, including acrylic glass, hard rubber, oak wood, and quartz glass. We place the transducer 20 cm away from the RTC crystal, set the corresponding initial phase of the excitation signal for the backward drift of 25 s and the forward drift of 45 s, then quantify the minimum amplitude of the excitation signal necessary for successful attacks. For each experimental setting, we test and identify the attack signal phase that reduces the oscillation signal amplitude to its lowest level in advance, thereby establishing an $\varphi \to \beta_1$ mapping relationship. The results are listed in Table 2, showing that for different boards, the average energy required for successful implementation of time forward and backward drift attacks on the surface of the quartz glass medium is the smallest; the energy required for attacks on the surface of the hard rubber plastic is relatively the highest. Meanwhile, we adopt three representative BP monitors placed on the surface with the same attack environment configuration, and then record the minimum attack signal amplitude required to modify the high pressure to 180 and 90mmHg. The blood pressure of the tested volunteer in the resting state is 121/80mmHg. As the results in Fig. 9 show,



(a) $\Delta = \frac{\pi}{12}$ (blue line) and $\frac{11\pi}{12}$(green line).



(b)

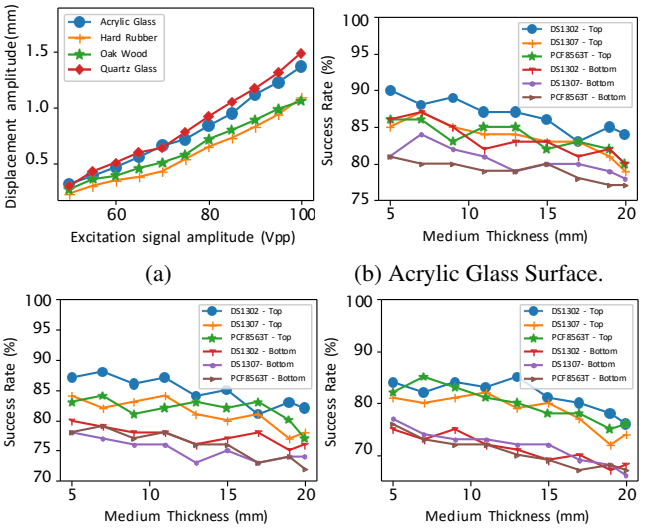
Figure 10: Experimental results on forward drift of time.

Material	↓25s	Phase	↑45s	Phase
RTC Module: DS1302				
Acrylic Glass	75V	2.519	68.2V	1.979
Hard Rubber	86V	2.018	79.1V	1.471
Oak Wood	80V	1.972	75.3V	1.426
Quartz Glass	69V	2.299	66.1V	1.753
Development Board: XC6C6SLX16				
Acrylic Glass	95V	2.518	75.1V	2.395
Hard Rubber	104.2V	2.132	85V	1.613
Oak Wood	99V	2.213	81.6V	1.728
Quartz Glass	87.5V	2.302	71V	1.897
Development Board: STM32-F407ZGT6				
Acrylic Glass	86V	2.536	71.9V	2.413
Hard Rubber	94.9V	1.947	81.2V	1.563
Oak Wood	90V	2.119	77V	1.718
Quartz Glass	79.8V	2.387	68.5V	2.012

Table 2: The minimum amplitude of the excitation signal, as well as corresponding initial phases (deg) necessary for successful attacks, under different expected time drift.

the energy required to launch a successful attack does not differ much among different mediums in general, even though different mediums exhibit different velocities of transverse and longitudinal waves (see Table 3).

To further evaluate the relationship between the amplitude of the excitation signal and the surface vibration response of the medium, we apply excitation signals of different amplitudes to the transducer and place the GFL-Z30N-RS485 vibration meter close to the surface of the selected medium to measure the vibration amplitude at which the crystal located. The variation of the vibration amplitude on the surface of the medium is shown in Fig. 11(a). The results show that as the amplitude of the excitation signal increases, the mechanical vibration amplitude on the surface of the medium follows an overall upward trend. When the excitation voltage increases to 50V, the vibration amplitude of different mediums at the selected positions increases by more than 400%. The difference in the vibration amplitude of different mediums under the same excitation signal may be caused by different structural characteristics (e.g., density and elasticity). For a medium with low density and high elasticity, attackers may need a larger signal amplitude to achieve successful attacks.



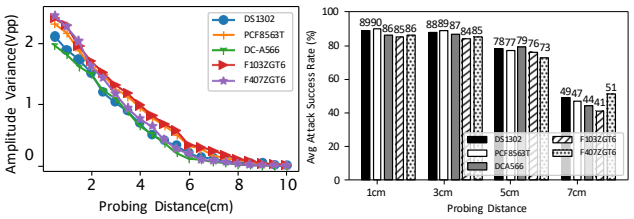
(a) (b) Acrylic Glass Surface.

(c) Hard Rubber Surface. (d) Oak Wood Surface.

Figure 11: The variation of surface vibration amplitude of the medium with the amplitude of the excitation signal (a); The success rate of attacks under different thicknesses of the medium and the positions of the transducer (b)-(d).

C. Impact of Attack Energy on Time Drifting Forward. According to Eq. 3, apart from the phase of the superimposed electric signal, the variation in the intensity of the excitation signal can affect the amount of time drift. To validate this effect, we integrate a DS1302 RTC module with a 5 mm-thick acrylic glass plate, place the transducer 3 cm next to the DS1302 RTC crystal, and set the amplitude of the signal driving the transducer to various levels (45, 50, 55, 60, 65, 70, 75, 80, 85, 90, 95, 100Vpp). The phase shift offset Δ is set to $\frac{\pi}{12}$ and $\frac{11\pi}{12}$. We start emitting the signal when the oscillation signal from the oscillator has a phase of $\frac{\pi}{2}$ and then record the average amount of time-forward drift, as shown in Fig. 3(a). Under the setting of a single attack duration of 0.008 ms, when the attack signal energy increased from 65Vpp to 75Vpp, the time drift increased from 45.89 s to 53.12 s, approximately 15.8%. At attack signal amplitudes of 75∼85Vpp, we observe no significant change in time drift. Simultaneously, we use the probe to detect the oscillation signal and observe that the frequency band overlaps with the center frequency at the end of a single attack of different durations, proving that the oscillation signal can converge within the duration of a single attack. Therefore, increasing the amplitude to accelerate the phase drift speed cannot help obtain more drift time.

With the increase of the energy of the excitation signal, the forward drift time starts to decrease at 90Vpp. Fig. 3(b) shows the power spectral density of the amplitude normalized oscillation signal at the excitation signal amplitude of 100Vpp. We observe a Lorentz-shaped spectrum broadening near the frequency of 32.768 kHz, with several harmonics based on 32.768 kHz occurring in the power spectrum. We believe that it is due to the excessive excitation amplitude on



(a) (b)

Figure 12: The variation in the peak-to-peak amplitude of the detected oscillation signal and the average attack success rate at different detection distances.

the crystal oscillator, resulting in its nonlinear behavior: the harmonic out-of-band components in the circuit will reduce the amplification gain of the amplifier in the feedback circuit for the 32.768 kHz in-band signal [17], making it difficult for the amplitude of the oscillator output signal to stably exceed the threshold of decreasing excitation counter values, which will lead the time not to drift forward as expected.

D. Impact of Medium Thickness. The intensity of Lamb waves decreases rapidly with an increase in the thickness of the medium, affecting the efficiency of energy transfer. We use acrylic glass, hard rubber, and oak wood materials with thicknesses ranging from 5∼20 mm. Placing the transducer on both sides of the board at the same position, we fix the distance between the transducer and the crystal oscillator at 20 cm. For each attack setting, we first establish $\varphi \rightarrow \beta_1$ through testing the phase response of oscillation signal, and find the attack signal phase that reduces the oscillation signal amplitude to its lowest level. Then, we adjust the phase of the excitation signal for a forward drift of 45 seconds and a backward drift of 25 seconds, maintaining the amplitude of the excitation voltage at 80Vpp and 85Vpp, respectively. The attack success rates with varying thicknesses of the plate are shown in Fig. 11(b), (c), and (d). As the thickness increases, the attack efficiency slightly decreases. When the thickness increases by 15 mm, the average success rate decreases by 7% across different materials. Additionally, placing the transducer on the back of the board results in an average success rate decrease of about 6% compared to placing it on the front. This is due to energy loss when sound waves transmit from the lower to the upper surface, reducing the mechanical energy that reaches the crystal oscillator.

E. Impact of the Magnetic Sensing Distance. We select five representative modules listed in Table 1 and place them respectively on a 5 mm-thickness acrylic glass plate. We then place the transducer 20 cm away from the RTC crystal, set the corresponding initial phase of the excitation signal for the backward drift of 25 s and the forward drift of 45 s. We position the magnetic probe at various distances below the RTC crystal oscillator and automatically track the moments when TimeTravel recognizes the phase of an oscillation signal as $\pi/2$, at which point the corresponding excitation signal is emitted. For each module, we repeat the attack for 100 times, and the observed peak amplitude of the oscillation signal and the average attack success rates are shown in Fig. 12(a) and (b), respectively. As the probing distance increases, the amplitude variation of the signal gradually decreases, until at a distance of approximately 7.5 cm, the amplitude changes of the magnetic signal all decrease to below 0.2Vpp, and we can hardly recognize a clear trend of amplitude changes under the presence of electromagnetic noise. Meanwhile, when the probe distance from the crystal oscillator is greater than 5cm, we observe that the attack success rate decreases significantly. At a distance of 7cm, the average success rate is only 46%. Due to the small amplitude change of the detected oscillating signal, when the attack distance is 7cm, TimeTravel wrongly misjudges other phases as $\pi/2$ for many times, resulting in the wrong time drift amount.

6.2.2 EM Side-channel Quality

To assess the quality of the electromagnetic side-channel, we use commercial BP monitors described in Section 6.1.2 with enclosures, as well as all modules and development boards listed in Table 1. We place each device under test on a 5mm thick acrylic glass surface, positioning the magnetic field probe 1∼4 cm below the MCU on the device's PCB board. We collect electromagnetic signal sequences of 100ms per data sample for the training set. For the testing set, we place the probe at distances of 1∼7 cm directly below the MCU of another batch of devices, collect 100ms electromagnetic signal sequences, and conduct classification tasks. For the parameter settings, we set $a = b = 50$ and $M = 5$MHz. The accuracy, recall rate, and F1 score of the model for the six BP monitors are shown in Table 6. Generally, for time series samples with a detection distance of 1∼4 cm, TimeTravel achieves a classification accuracy of more than 92% across different solid material surfaces. However, as the detection distance increases, the classification accuracy significantly decreases accordingly. At a 7 cm detection distance, the average classification accuracy for the three solid materials drops to below 40%. We observe that this decline corresponds with the average SNR of the test data decreasing from 21dB at a 1 cm detection distance to 6dB at a 7 cm detection distance, making it harder for the neural network to accurately capture spectral features and correctly classify the device model.

6.2.3 Processing Delay

TimeTravel captures and analyzes the signals emanating from the oscillator circuit in order to launch the attack at the appropriate times, which introduces additional processing delay, spanning from the moment the target phase signal is captured from the oscillator circuit to the beginning of the emission of the acoustic attack signal. We use modules listed in Table 1 and a laptop equipped with a 13th generation Core i7-1355U

processor and 32 GB of RAM, running on the Debian 12 operating system, to measure the processing delay. We keep the attack settings consistent with Section 6.2.1 (A) and then repeat the attack 100 times with the time drift backward by 5 s and 25 s, as well as forward by 25 s and 45 s. We record the hardware timestamps at which USRP begins to perceive the target phase of the oscillation signal and begins to transmit the signal. We then calculate the average delay, which is listed in Table 5. The average delay for different modules ranges from 0.77 µs to 0.87 µs, meaning that under normal circumstances, attackers can mount attacks with a processing delay of no more than approximately 2.9% of oscillation cycles (the oscillation cycle is around 30.52 µs).

6.2.4 Robustness

In real-world scenarios, a target device may be placed with extraneous items nearby. To evaluate the attack robustness of TimeTravel in the presence of extraneous items, we use a polyethylene plastic table with a thickness of 1.5 cm (covered with spray paint), place the transducer about 50 cm away from the RTC crystal, and adjust the amplitude and phase based on the excitation signal. We set up two scenarios, and in each scenario, we have different item layouts around the module, as shown in Fig. 18.

For setting 1, we place a digital camera, an electronic fan, a cup, a box, wood bricks, and a gateway on the table. For setting 2, we place a lamp, an electronic fan, a cup, and wood bricks on the table. Moreover, we set up a baseline without placing any extraneous items on the table to compare changes in attack efficiency. During the test, we keep the fan, digital camera, gateway, and lamp running, to maintain the presence of noise from other devices. We set the transducer 30 cm away from the RTC crystal, the amplitude of the excitation signal to 86V, and repeat the attack 100 times with forward drift by 45 s and then measure the average success rate under each representative module, which is shown in Table 4. We observe that when extraneous items are placed around the module, there is no significant change in the success rate of the attack compared to the baseline. The vibration waves of different frequencies propagate independently in the medium and do not interfere with each other, and only the acoustic vibration waves emitted by attackers will affect RTC timing. However, since TimeTravel relies on the conduction of mechanical energy between solid mediums, placing extraneous items beneath the target module may reduce the efficiency of the energy transfer, resulting in a lower attack success rate. The thicker the items, the lower the energy transfer.

7 Discussion

In this section, we discuss potential countermeasures and safety recommendations, as well as the impact of NTP synchronization.

7.1 Countermeasures

The key to defend against TimeTravel attacks lies in preventing acoustic vibrations from generating or propagating disruptive electrical signals in an RTC. Different from the potential hardware and software-based methods proposed in [18], we propose two kinds of countermeasures and have disclosed them along with the security threats to BP monitor vendors, including Omron, HYNAUT, Yuwell, and Xiaomi:

A. Replacing Oscillating Source. Apart from crystal, manufacturers can use frequency synthesizers [19] or MEMS oscillators to generate f_{output}=32.768 kHz oscillation signals. For instance, Silicon Labs Si5351 clock generator can generate specific frequency clock signals by using a 25MHz crystal oscillator that provides reference signals. Once powered with a 2.5V or 3.3V supply, the PLL and Multisynth divider parameters can be configured via the I_2C interface according to Eq. 6:

$$\begin{aligned} f_{PLL} &= \Delta_{PLL} \times 25\text{MHz} \\ f_{output} &= \frac{f_{PLL}}{\Delta_{multisynth}}, \end{aligned} \tag{6}$$

where Δ_{PLL} and $\Delta_{multisynth}$ can be determined as 36 and 27465.82 (fractional division), respectively, resulting in f_{output} as 32.768kHz. Finally, Si5351 outputs the generated clock signal through the CLK0 pin to the clock input pin of the RTC MCU. Generating 25MHz ultrasonic waves is challenging because of their weak diffraction ability. These waves typically propagate only a few millimeters in most solids, making it highly unlikely for a 25MHz crystal oscillator to be disturbed by acoustic signals.

B. Applying Shock-absorbing Materials. To reduce interference from potential resonance signals on the oscillator's vibration mode, manufacturers can use shock-absorbing materials to cover the timing circuit PCB containing the 32.768 kHz crystal oscillator. For RTC circuits and mechanical vibrations perpendicular to the plane, this scenario can be modeled as a mass-spring-damper system. As the damping coefficient in the system increases, the damping material's response becomes more even across a range of frequencies. Therefore, shock-absorbing materials with a higher damping coefficient results in less energy reaching the RTC crystal oscillator, providing more effective protection against mechanical vibration interference.

In addition, since mechanical vibrations are transmitted perpendicularly to the surface, placing the damping material perpendicular to the direction of vibration allows it to directly dissipate vibrational energy. However, when the damping material is placed at an angle, the vibrational energy is partially converted into shear force and partially into compressive force, reducing the effectiveness of energy absorption. Manufacturers can use damping materials with relatively high damping coefficients, such as Polyurethane Foam and Polymeric Viscoelastic Materials, and place the damping material parallel

to the solid plane to maximize the absorption of mechanical vibrational energy.

7.2 Safety Recommendations

When launching the attack, the electrical signal amplitude applied to the transducer often exceeds the maximum safe voltage for human exposure (36V). Therefore, it is strongly recommended that researchers wear insulating gloves during testing to prevent electric shock and use insulating tape to secure the transducer and its connected wires.

Lamb waves propagating in solids do not directly impact the human body as they are primarily confined within the material. However, these waves can interact with the air at the material boundaries, generating sound waves with the same or similar frequencies. Fortunately, such a process shows low energy conversion efficiency, due to the significant acoustic impedance difference at the solid-liquid interface. In our experiments, the detected sound pressure level at the material surface is no higher than 26 dB, comparable to ambient noise levels. However, to avoid potential health risks, researchers are advised to control the intensity of Lamb waves, ensuring that they remain within safe sound pressure levels for human exposure, especially when using powerful electrical signals to drive the transducers. For the testing experiment of the blood pressure monitor, we have obtained approval from the Institutional Review Board (IRB) before the test, and the participant is aware of the entire process of the experiment and is informed of the potential impact upon human subjects.

7.3 Impact of NTP Synchronization

The commercial POS machine we test uses NTP only to get the current time at startup, updates the RTC timing, and then works only with the RTC internal timestamp. Therefore, the POS machine does not rely on NTP after a successful startup. Moreover, there are some devices whose RTCs are not synchronized via NTP, e.g., Industrial PLCs, smart electricity/gas/water meters, and medical devices. NTP synchronizes system time periodically, often at intervals of minutes or hours based on device accuracy needs [20]. Altering RTC timing within a short span does not prompt NTP synchronization. However, in many scenarios, especially in real-time computing and communication systems, even temporary timestamp modifications can cause severe damages like service interruptions or cascade failures. Even if NTP syncs after or during the attack, damages are already done and irreversible.

8 Related Work

We survey previous research that utilizes acoustic signals to interfere with the operating logic of devices, which can be divided into two categories: (1) acoustic command attacks using sensors' nonlinear interpretation of acoustic signals and (2) acoustic signal resonance jamming attacks.

Prior work on the first type of attack targets voice control systems by using speech recognition algorithms to exploit microphone hardware's nonlinear response to ultrasound, injecting inaudible commands. Zhang et al. [21] first exploited a hardware loophole in the nonlinear response of a microphone, to convert ultrasound waves into valid voice commands and manipulate several brands of voice assistants. Roy et al. [22] utilized speaker arrays to effectively increase the acoustic stealth attack distance by sending narrow-band ultrasound waves. Yan et al. [23] proposed to inject ultrasonic commands into voice assistants through ultrasound waves propagating in a solid medium to bypass physical spatial obstacles. Ji et al. [24] utilized the feature that a capacitor emits a high-frequency noise when it is being charged or discharged, and configured specific voltages to the two sides of the capacitor to make the noise propagate to a cell phone's microphone to control the voice assistant to execute commands. Yang et al. [25] controlled the voice assistant by manipulating MEMS switching power supply to make noise.

For the second type of attack, attackers exploit the resonant frequency of electronic components to affect the normal operation of specific equipment or modules. Son et al. [26] emitted acoustic signals that are close to the resonance frequency of the gyroscope inside a drone, causing the gyroscope to resonate and then making the drone's flight trajectory change. Bolton et al. [18] emit acoustic resonance signals to the the magnetic head of a mechanical hard disk to make it positioned incorrectly, leading to the denial of service attack. Other methods are also proposed to perform acoustic signal injection attacks [27–29]. In this study, TimeTravel first utilizes a ceramic transducer to emit sound vibration signals to the RTC crystal oscillator, causing the shift of the signal's phase and amplitude. Then, TimeTravel is able to modify the system time stored in the RTC counter, posing a serious threat to the reliability of devices that utilize system time for real-time execution.

9 Conclusion

This paper presents a new security threat posed by a real-time RTC clock timing rate drift attack called TimeTravel. As a technique target for various real-time computing and communicating devices, TimeTravel leverages acoustic interference to modify the timing rate of the device's internal RTC clock, leading to the system timestamps drift. By analyzing the response characteristics of quartz crystals to acoustic resonance signals of different amplitudes and phases, we reveal a quantitative relationship between the parameter settings of the acoustic resonance signals and the amount of RTC time drift. We validate the efficacy of TimeTravel on nine off-the-shelf modules with RTC circuits and seven commercial devices, and evaluate the robustness under two realistic placement settings. Finally, we propose countermeasures against TimeTravel.

Acknowledgments

We would like to thank anonymous reviewers and our shepherd for their valuable feedback. This research was supported by the China National Key Research and Development Program under Grant No. 2022YFB3103904.

References

[1] Steve Goldband. Real-time clocks for microcomputers in behavioral research. *Behavior Research Methods & Instrumentation*, 11(2), 1979.

[2] Sadeque Reza Khan, Alvir Kabir, and Dilshad Ara Hossain. Designing smart multipurpose digital clock using real time clock (RTC) and PIC microcontroller. *International Journal of Computer Applications*, 41(9), 2012.

[3] Teemu Rytilahti, Dennis Tatang, Janosch Köpper, and Thorsten Holz. Masters of time: An overview of the NTP ecosystem. In *IEEE European Symposium on Security and Privacy (EuroS&P)*, 2018.

[4] Aanchal Malhotra, Isaac E Cohen, Erik Brakke, and Sharon Goldberg. Attacking the network time protocol. In *Network and Distributed System Security Symposium (NDSS)*, 2016.

[5] Yarin Perry, Neta Rozen Schiff, and Michael Schapira. A devil of a time: How vulnerable is NTP to malicious timeservers? In *Network and Distributed System Security Symposium (NDSS)*, 2021.

[6] Guangkai Ma, Chunpeng Ge, and Lu Zhou. Achieving reliable timestamp in the bitcoin platform. *Peer-to-Peer Networking and Applications*, 13, 2020.

[7] Robert J Matthys. Crystal oscillator circuits. *New York*, 1983.

[8] Shaul Katzir. The discovery of the piezoelectric effect. In *The Beginnings of Piezoelectricity: A Study in Mundane Physics*. Springer, 2006.

[9] Brian Ellis. Electronic circuits, fundamentals and applications. *Soldering & Surface Mount Technology*, 18(4), 2006.

[10] Eric A Vittoz, Marc GR Degrauwe, and Serge Bitz. High-performance crystal oscillator circuits: Theory and application. *IEEE Journal of Solid-state Circuits*, 23(3), 1988.

[11] Manohar Lal Munjal, Michael Vorländer, Peter Költzsch, Martin Ochmann, A Cummings, W Maysenhölder, and Walter Arnold. *Formulas of acoustics*. Springer Science & Business Media, 2008.

[12] John W Strutt and Lord Rayleigh. On waves propagated along the plane surface of an elastic solid. 2007.

[13] En Hong Ling and Ruzairi Hj Abdul Rahim. A review on ultrasonic guided wave technology. *Australian Journal of Mechanical Engineering*, 2017.

[14] Petr Hora and Olga Červená. Determination of lamb wave dispersion curves by means of fourier transform. *Applied and Computational Mechanics*, 6(1), 2012.

[15] Joseph L. Rose. *Ultrasonic waves in solid media*. Acoustical Society of America, 2000.

[16] Hans Roder. Amplitude, phase, and frequency modulation. In *Proceedings of the IEEE Institute of Radio Engineers*, 1931.

[17] Jianshuo Liu, Hong Li, Mengjie Sun, Haining Wang, Hui Wen, Zhi Li, and Limin Sun. NFCEraser: A security threat of NFC message modification caused by quartz crystal oscillator. In *IEEE Symposium on Security and Privacy (S&P)*, 2024.

[18] Connor Bolton, Sara Rampazzi, Chaohao Li, Andrew Kwong, Wenyuan Xu, and Kevin Fu. Blue note: How intentional acoustic interference damages availability and integrity in hard disk drives and operating systems. In *IEEE Symposium on Security and Privacy (S&P)*, 2018.

[19] Vadim Manassewitsch. Frequency synthesizers: Theory and design. 1987.

[20] David L Mills. A brief history of ntp time: Memoirs of an internet timekeeper. *ACM SIGCOMM Computer Communication Review*, 33(2), 2003.

[21] Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, and Wenyuan Xu. Dolphinattack: Inaudible voice commands. In *ACM Conference on Computer and Communications Security (CCS)*, 2017.

[22] Nirupam Roy, Sheng Shen, Haitham Hassanieh, and Romit Roy Choudhury. Inaudible voice commands: The Long-range attack and defense. In *Networked Systems Design and Implementation (NSDI)*, 2018.

[23] Qiben Yan, Kehai Liu, Qin Zhou, Hanqing Guo, and Ning Zhang. Surfingattack: Interactive hidden attack on voice assistants using ultrasonic guided waves. In *Network and Distributed System Security Symposium (NSDI)*, 2020.

[24] Xiaoyu Ji, Juchuan Zhang, Shui Jiang, Jishen Li, and Wenyuan Xu. Capspeaker: Injecting voices to microphones via capacitors. In *ACM Conference on Computer and Communications Security (CCS)*, 2021.

[25] Lanqing Yang, Xinqi Chen, Xiangyong Jian, Leping Yang, Yijie Li, Qianfei Ren, Yi-Chao Chen, Guangtao Xue, and Xiaoyu Ji. Remote attacks on speech recognition systems using sound from power supply. In *USENIX Security Symposium*, 2023.

[26] Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, and Yongdae Kim. Rocking drones with intentional sound noise on gyroscopic sensors. In *USENIX Security Symposium*, 2015.

[27] Yazhou Tu, Zhiqiang Lin, Insup Lee, and Xiali Hei. Injected and delivered: Fabricating implicit control over actuation systems by spoofing inertial sensors. In *USENIX Security Symposium*, 2018.

[28] Nicholas Carlini, Pratyush Mishra, Tavish Vaidya, Yuankai Zhang, Micah Sherr, Clay Shields, David Wagner, and Wenchao Zhou. Hidden voice commands. In *USENIX Security Symposium*, 2016.

[29] Liwei Song and Prateek Mittal. Poster: Inaudible voice commands. In *ACM Conference on Computer and Communications Security (CCS)*, 2017.

Appendices

A Verify the Feasibility of Transmitting Acoustic Waves in the Air to Interfere with Crystal Oscillator

To verify the possibility of transmitting ultrasonic waves through the air to change the speed of RTC timing, we use the DS1302 RTC module and connect it to the Arduino UNO Rev3 development board through Dupont wire. Moreover, we use a pair of XHXDZ-5140 and XHXDZ-4140 ultrasonic speakers respectively, and place them approximately 1.5 cm on both sides of the RTC module. The optimal operating frequency band of XHXDZ-5140 is 10∼30 kHz, and the optimal operating frequency band of XHXDZ-4140 speaker is 26∼46 kHz. Through these two speakers, we are able to verify the sensitivity of the RTC module to interference from 20∼46 kHz ultrasonic acoustic signals. We use alligator clips to connect the ultrasonic speakers to the signal source and excite 20Vpp, 20∼46 kHz sinusoidal signals. We observe that the RTC time is still increasing forward at 1-second intervals. The oscillation signal emitted by the quartz crystal oscillator before and after the attack detected by the magnetic field probe is shown in Fig. 14 (a), and it can be seen that there is no significant change in the amplitude and frequency of the oscillation signal. We then adjust the transmission voltage and the distance between the speaker and the RTC module, varying between 20∼50Vpp and 0.5∼1.5 cm, respectively. We observe that the oscillation signal during the attack is

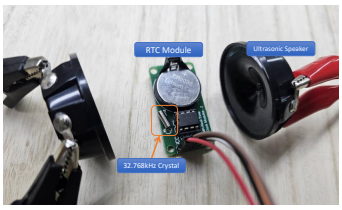
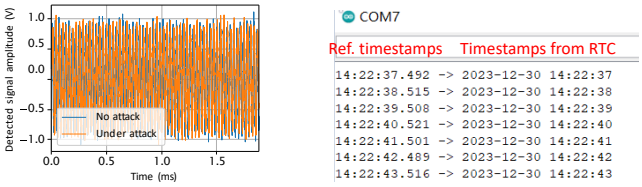


Figure 13: Experimental setup.



(a) (b)

Figure 14: Time domain of oscillation signal detected after sending 32.768kHz ultrasonic wave through the air(left); Serial output from development board (right).

still similar to that shown in Fig. 14(a), and the RTC module maintains normal timing (Fig. 14(b)). The failure of injecting attack signals over the air is due to the significant acoustic impedance and medium density disparity between fluids and solids. This inefficiency is compounded by the fact that ultrasound waves at the resonance frequency of 32.768 kHz have short wavelengths, making it difficult for them to penetrate the metal casing that encases quartz chips.

B The Propagation Characteristics of Lamb Waves

Lamb waves are elastic waves that propagate on the surface of a solid flat plate, consisting mainly first-order symmetric Lamb waves and first-order anti-symmetric Lamb waves. The speed of Lamb wave propagation mainly depends on the frequency of the propagating wave and thickness of the solid medium. Suppose the excitation signals from transducer $f(t) = p\sin(\omega t + \varphi)$ successfully excites a Lamb wave with a frequency of ω. When the first-order anti-symmetric wave component u propagates along the Z direction should be:

$$\xi = \mathrm{Re}\{u_x(t)\} = \lambda \sin(\omega t + \Phi), \tag{7}$$

where

$$\begin{aligned} \lambda &= \sqrt{[\alpha A p \cos(\alpha x)]^2 + [k_a B p \cos(\beta x)]^2} \\ \Phi &= -\omega t_T + \varphi - k_a z + \arctan\left(\frac{\alpha A \cos(\alpha x)}{k_a B \cos(\beta x)}\right), \end{aligned} \tag{8}$$

$t_T = \frac{d}{c_s}$ is the time required for the wave to propagate to (x,z); d is the distance between the sound source and the location (x,z); $k_a = \frac{\omega}{c_s}$ is the wave number of first-order anti-symmetric Lamb wave; c_s is the phase velocity, which can be calculated

by Eq. 2; $\alpha = \sqrt{(\frac{\omega^2}{c_L})^2 - k_a^2}$,$\beta = \sqrt{(\frac{\omega^2}{c_T})^2 - k_a^2}$, c_L and c_T represent the longitudinal and transverse wave speed (See Table 3). In practice, the propagation of sound waves in solids results in energy loss, which is reflected in a decrease in the amplitude of the waves. Therefore, V should be multiplied by an energy loss ratio $\varepsilon_{\Delta z}$: $V' = \varepsilon_{\Delta z} V$, which can be determined by experimental testing. For a certain solid medium, when z is determined, t_T is also determined, so attackers only need to determine z and φ to determine the phase of the displacement equation at a certain time. Since we focus on the particle displacement on the surface of the medium, so x can be set to 0. Additionally, when Lamb waves are not applied and the plate, there may exist prestress in the surface of a plate, representing the deformation of the plate in steady state, so a constant γ may be applied to ξ (i.e., $\xi' = \gamma + \xi$).

C Schematic Diagram and Explanation of the Principle of Time Drift Forwards

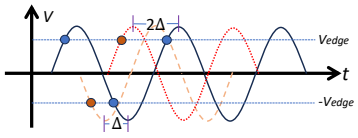


Figure 15: Schematic diagram of the principle of time drift forward.

Under Fig. 15, the black curve represents the initial oscillation signal in the circuit. The yellow curve shows a forward phase shift of Δ caused by a single attack, while the red curve shows a cumulative phase shift of 2Δ after two attacks. Blue dots indicate the moments the oscillation signal crosses the trigger levels (rising and falling edges) without attacks, while the orange dots represent the moment when the oscillation signal crosses the triggering level of the falling and rising edges during the implementation of two attacks. It can be seen that under the consecutive attack signals, the time when the oscillation signal crosses the edge trigger level is advanced.

D Modeling How Timing Drift of the Counter in a BP Monitor Affects the Accuracy of Blood Pressure Measurements

The BP monitor uses a solenoid valve to apply and release cuff pressure linearly, with a pressure sensor detecting oscillatory wave amplitudes during deflation. The solenoid valve's deflation rate, typically 2-3 mmHg/s, is controlled by periodic signals from clock circuit counters. The monitor's main controller records oscillation amplitudes from the pressure sensor over time. The systolic pressure is determined by identifying the cuff pressure corresponding to 40-45% of the peak

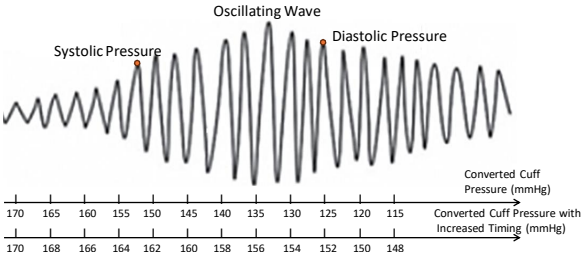


Figure 16: Accelerating the rate of cuff deflation causes the oscillation wave to pass through the points corresponding to systolic and diastolic blood pressure in a relatively short period of time, resulting in an overestimation of the cuff pressure value converted at the corresponding time.

amplitude during the amplitude-increasing phase, while diastolic pressure corresponds to 60-75% of the peak amplitude during the amplitude-decreasing phase (see Fig. 16). These ratios depend on the manufacturer's design. If the counter timing frequency is f (Hz), the valve's actual deflation rate is v (mmHg/s), ΔP is the pressure released per clock cycle (mmHg), and the initial cuff pressure and deflation rate are P_0 and V_0, respectively, then we have:

$$v = \Delta P \cdot f,$$

if the timing frequency changes Δf, the derived systolic pressure error can be denoted as:

$$\Delta S = (P_0 - S) \cdot \frac{\Delta P \Delta f}{V_0}. \tag{9}$$

Similarly, the error in diastolic pressure should be $\Delta D = (P_0 - D) \cdot \frac{\Delta P \Delta f}{V_0}$. Thus, when the timing rate increases, the accelerated rate of the cuff deflation causes the peak amplitude of the oscillation wave occurring earlier, leading to an overestimation of the cuff pressure values and, consequently, higher measurements of systolic and diastolic pressures (see Fig. 16). Conversely, a slower timing frequency delays the peak amplitude occurrence, resulting in underestimations of both systolic and diastolic pressures.

E Illustrations and Tables

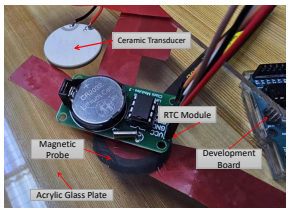
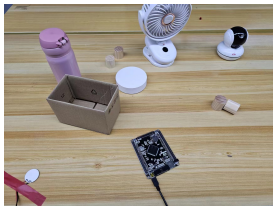


Figure 17: Experimental setup for time drifting backward.



(a) Experimental setting 1.

(b) Experimental setting 2.

Figure 18: Experimental setups on robustness performance test.

Medium	Wave Speed($10^3 m/s$)		Density
	Longitudinal	Transverse	(g/cm^3)
Aluminum	6.26	3.08	2.7
Stainless steel	6.10	3.30	7.85
Quartz glass	5.57	3.52	2.2
Acrylic glass	2.70	1.30	1.18
Hard rubber plastic	2.30	0.94	1.22
Oak wood	3.31	1.55	0.85
Polyethylene	2.14	0.72	0.94

Table 3: Acoustic transverse and longitudinal wave data in representative solid medium.

Module	Setting 1	Setting 2	Baseline
DS1302	89%	90%	89%
DS3231	85%	87%	86%
STM32F10-3ZGT6	82%	83%	83%
STM32F40-7ZGT6	87%	85%	87%

Table 4: The average attack success rate of representative modules under different environmental background settings.

Module	↓5s	↓25s	↑25s	↑45s
DS1302	0.81μs	0.82μs	0.82μs	0.8μs
DS1307	0.79μs	0.8μs	0.83μs	0.81μs
PCF8563T	0.81μs	0.82μs	0.79μs	0.83μs
DS3231	0.84μs	0.78μs	0.85μs	0.83μs
STM32F103ZET6	0.8μs	0.79μs	0.84μs	0.77μs
XC6C6SLX16	0.78μs	0.85μs	0.8μs	0.84μs
STM32F103ZGT6	0.83μs	0.81μs	0.78μs	0.85μs
STM32F407ZGT6	0.86μs	0.83μs	0.81μs	0.78μs
DC-A566	0.87μs	0.85μs	0.84μs	0.82μs

Table 5: Processing delay under different modules with RTC crystal.

Probing Distance	Accuracy	Recall	F1 Score
Solid Material: Acrylic Glass			
1cm	99.43%	99.24%	99.33%
2cm	99.41%	99.22%	99.31%
3cm	99.38%	99.16%	99.27%
4cm	93.29%	91.48%	92.38%
5cm	82.43%	77.38%	79.83%
6cm	54.69%	50.25%	52.38%
7cm	38.74%	33.62%	36%
Solid Material: Polyethylene			
1cm	99.37%	99.26%	99.31%
2cm	99.31%	99.24%	99.27%
3cm	99.3%	99.21%	99.25%
4cm	92.76%	90.74%	91.74%
5cm	79.66%	72.8%	76.08%
6cm	49.97%	47.82%	48.87%
7cm	31.08%	26.65%	28.7%
Solid Material: Hard Rubber Plastic			
1cm	99.46%	99.4%	99.43%
2cm	99.41%	99.38%	99.39%
3cm	99.22%	98.92%	99.07%
4cm	93.02%	91.47%	92.24%
5cm	82.43%	80.06%	81.23%
6cm	56.12%	52.98%	54.5%
7cm	33.96%	29.93%	31.82%

Table 6: Testing results of classification performance of device models under different detection distances and solid materials.

Layer	Operation	Kernel Size
1	Input	100000×1
2	Conv1D	16×64
3	MaxPool	4
4	Conv1D	8×128
5	MaxPool	4
6	Conv1D	8×256
7	MaxPool	4
8	Flatten	-
9	FC1	1024
10	Dropout	0.2
11	Output+Softmax	16*

Table 7: Neural network structure for model classification. The output classification labels include 15 device models as well as an “unidentified" label.