Digital Investigation 24 (2018) S10–S17

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

DFRWS 2018 Europe — Proceedings of the Fifth Annual DFRWS Europe

The reliability of clocks as digital evidence under low voltage conditions

Jens-Petter Sandvik [a, b, *], André Årnes [a, c]

[a] Norwegian University of Science and Technology (NTNU), Norway
[b] National Criminal Investigation Service (Kripos), Norway
[c] Telenor ASA, Norway

Keywords:
Digital forensics
Mobile forensics
Clock
Clock documentation
Low voltage errors

A B S T R A C T

Battery powered electronic devices like mobile phones are abundant in the world today, and such devices are often subject to digital forensic examinations. In this paper, we show that the assumptions that clocks are close to correct can be misleading under some circumstances, especially with failing batteries. One of four tested devices showed the clock jumped 8 and 12 years into the future when the battery connector voltage was held at 2.030 V and 2.100 V for about 9 s. Other devices showed a more expected behavior, where the clocks were slowly lagging until it was reset. In addition to this, we tested the precision of some methods of documenting the clock settings, and found most timestamps to be within reasonable precision for forensic use. Finally, we describe a model for the variability of the timestamps examined.

Introduction

A forensic investigation often includes questions and hypotheses about the temporal domain, such as questions about when, and in which order certain events happened. It is an established practice in digital forensics to document the clock settings of digital equipment that will be used for evidence, as the trustworthiness of timestamps in the evidence is often questioned in court.

An ideal clock is an oscillator that increases a counter, in the same frequency as other clocks. A physical clock is not ideal, and will be affected by its physical properties, its environment, adjustments, etc. Wander, as the ntp version 4 specification calls it, is the average error over time a clock experiences which degrades the accuracy over time, and jitter is the small perturbations that limits the precision of the clock (Martin et al., 2010).

During normal operations with no external interference to the device, this is how the device works. During its lifetime, a device might be exposed to various conditions that can affect the correctness of operations. One such condition might be a failing battery.

A battery will power the phone until it reaches the lower limit for what the device needs for normal operations. At this point, the device will shut down, but the battery will continue to power the clock. In the end, the battery reaches a level where the energy required to power the low-power clock is insufficient, and the device will shut completely down. The intuitive understanding of the clock's behavior is that the clock will continue to stay close to correct until the memory doesn't have enough electric power to keep its data; then, the processor shuts down and the clock is reset to the device's epoch.

The background for these experiments comes from a case where the logs from a mobile phone indicated that the clock might have been adjusted 24 h forward right before or during the time it was powered off. Observation of the device three years later showed that removing the battery and reinserting it made the clock jump forward by up to 1 min compared to the original clock. The test was done using a power supply attached to the phone's battery pins instead of the battery, as the original battery had degraded to the point that it couldn't power the phone any more. The possibility that the clock had been automatically set into the future could therefore not be ruled out.[1]

* Corresponding author. National Criminal Investigation Service (Kripos), Norway.
E-mail addresses: jens.p.sandvik@ntnu.no, jens-petter.sandvik@politiet.no (J.-P. Sandvik), andrearn@pvv.ntnu.no (A. Årnes).

[1] The case is from the Norwegian court case LB-2016-112427. A timestamp analysis were presented in court and challenged, and a more thorough examination found the origin of the clock adjustments to be inconclusive.

https://doi.org/10.1016/j.diin.2018.01.003

A clock that can be adjusted back or forward in time by naturally occurring error situations, is not a common hypothesis that is considered during investigations, and the failure of considering this can be that an automatic adjustment of a clock is believed to be a manual, willed adjustment of the clock. A search for events at a particular time might return incorrect results because of erroneous timestamps.

While the focus in this paper is on mobile phones, the issues discussed here are also applicable to iot. The total number of future IoT devices vary greatly between estimates, but it is widely believed that the number will be greater than today. As the number of devices increases, the cost goes down, and more devices will operate without supervision. From that, we can conclude that the number of malfunctioning devices, such as devices with failing batteries, outside the supported operating temperature or in other unexpected states will also increase, leading to more errors.

In this paper we propose a hypothesis that the clock of a device can jump back or forward in time when the device experiences a low voltage state on the battery connectors. The alternative hypothesis is that the clock will either be close to correct, or be reset to the device's epoch, depending on the voltage applied. To test this, we first established the precision of various methods and timestamps that can be used for comparing clocks, then we continued to test 4 different mobile phones during low voltage states.

The rest of the paper is structured as follows: First related work is discussed, then a model for delays between the clock and measured timestamp is defined. The experimental setup is then described, followed by the results. Lastly, we round up with a discussion, conclusion, and suggest future work.

Related work

It is generally accepted that the data that makes up evidence can be uncertain and contain errors introduced either by system faults, or humans. A system might malfunction, thereby recording erroneous data, and humans can interfere and change data both willfully and by accident. Abstraction layers can hide the precision of the information, and the interpretation of the data can be uncertain. Casey (2002) described a system for assessing evidence based on its uncertainty by attaching certainty levels to each piece of evidence. Together with the uncertainty of origin, correctness of logs, loss of information, and errors, temporal uncertainty is one of the types of uncertainty that was described during interpretation and reconstruction. This experiment goes a step toward quantifying uncertainties in digital investigations. The fact that digital information might contain errors and uncertainties has highlighted a need for quantifying these possible errors and uncertainties (Erbacher, 2010).

Other research has focused on timestamps and how to detect temporal irregularities. The implications of not considering the timezone that the timestamp references can be serious when presented in court. Boyd and Forster (2004) showed by a case example in which misinterpretations influenced the hypotheses in a case. Kaart and Laraghy (2014) discussed how investigators can detect erroneously set time zones and which time zone the among various timestamps adheres to phones. They also described the configurations related to the clock and timestamps in Android phones.

The use of timestamps are important in investigations for many reasons: to search or carve for information within a certain period, to establish the order of events, or to find usage patterns (Årnes et al., 2017). Willassen (2008a) shows that by using a hypothesis-based approach, investigators can establish a hypothesis about how particular clocks have been adjusted, and test whether the timestamps support or refute the clock hypothesis. The clock hypothesis covering adjustments of a clock can be tested by looking at causally linked events and timestamps outside the possible set of timestamps for a particular clock. The formalism of the proposed method has been used for detecting clock adjustments using the Master File Table in the NTFS file system (Willassen, 2008b).

The memory cells in a processor can be affected by the supply voltages, the temperature, or other external sources like radiation. As the supply voltage to the cells are closing in to the threshold voltage of the transistors, the error rate of the memory cells increases many orders of magnitude (Dreslinski et al., 2010). CMOS circuit performance, among them memory cells, are dependent on many variables, and, e.g., aging processes degrade transistors and increase their threshold voltage (Santos et al., 2016).

To induce faults in processing hardware is not a new technique. Barenghi et al. (2009) exploited the faults happening during a constant low voltage state to attack an RSA software algorithm in an ARM-9 processor using three attacks. When keeping the voltage low on one of the power lines to the System-on-Chip (SoC), the core power line, the LOAD instructions were affected by bit failures. The result of the fault was either data corruption or an instruction swap, both of which could be exploited. Another method of manipulating the Trust Zone in an ARM processor was demonstrated by manipulating the software control of the Dynamic Voltage and Frequency Scaling system in the processor. By manipulating the processor voltage and frequency, cryptographic keys could be extracted from the Trust Zone (Tang et al., 2017).

Timestamp variability

There are many sources of variability in the process leading up to a timestamp or a documentation of the relationship between clocks. In this paper, we propose a model for these variable sources where the granularity of the model can be adjusted as needed. Here, we analyze at different scenarios that all have slightly different delay models. These scenarios are:

- Documenting the timestamp with a photo, using a camera clock for comparison
- Comparison of two clocks from two sources, typically a system clock and a external clock

These two scenarios consist of two basic models. These are:

- A timestamp set because of a particular event
- The update of a timestamp in a user interface

We can differentiate between a noise source, which can skew the resulting timestamp in either direction, and a delay that can only increase the difference forward in time between the clock and the resulting timestamp. Fig. 1(a) and (b) shows these two basic models for the source of the inaccuracy of the timestamps. Fig. 1(c) and (d) shows the two scenarios for documenting the time.

Each clock in the model has a noise source attached. In this model, this shows as a summary of all the noise affecting a clock source. These sources tend to be small, but might differ between clocks (Zhou and Nicholls, 2008). A processor can have multiple clock sources, and use the less precise, power saving clock during its sleep state, while it uses a more precise and power intensive clock during normal operations (Qualcomm Technologies, 2016).

In this paper, the formalism presented by Willassen (2008a) is utilized. It states that an event, $e \in E$, where E is the domain of events, can be mapped to the time domain, $t(e), E \rightarrow T$, and furthermore to a timestamp by a clock, c: $c(t(e)) = \tau_c(e), E \rightarrow V$, where V is the domain of time values. The clock function can then