TIME GUIDANCE FOR NETWORK OPERATORS, CHIEF INFORMATION OFFICERS, AND CHIEF INFORMATION SECURITY OFFICERS

NOVEMBER 12, 2019

TABLE OF CONTENTS

TIME GUIDANCE FOR NETWORK OPERATORS, CHIEF INFORMATION OFFICERS, AND CHIEF INFORMATION SECURITY OFFICERS

SCOPE

This document is intended to provide guidance for network operators, Chief Information Officers (CIOs), and Chief Information Security Officers (CISOs). The goal of this document is to inform the reader on time **resilience** and security practices in enterprise systems. The guidance below attempts to address gaps in available time testing practices, increasing awareness of time-related issues within systems, and increasing awareness of the linkage between time and cybersecurity.

BACKGROUND

Every network operator must understand time and how it affects their network(s). Accurate, synchronized time is critical to many network functions and security, yet many users of time services know little about the source of their time. For example, in the United States, the principle sources of official time are the U.S. Naval Observatory UTC(USNO) and the National Institute of Standards and Technology UTC(NIST).

Additional guidance for C-Suite and the technical practitioner can be found here.[1,2]

INTRODUCTION

The recommendations in this document are intended to be incorporated into current test plans and regular systems maintenance. These recommendations can be integrated into any organization's master test plan.

Today, nearly all organizations rely on accurate time to sustain their daily network operations. Accurate time stamps are critical for banking and stock transactions, communications systems, system forensics, audits, and equipment maintenance. The ability of an organization's time infrastructure to deliver accurate and stable time while protecting the availability and integrity of time depends on the organization's function and requirements. Regardless of which timing protocol your organization uses to receive its time, **Network Time Protocol (**NTP), **Precision Time Protocol** (PTP), or via **Global Positioning System** (GPS), it is important to know the source of your time and to regularly monitor and test your time systems to ensure they are available and operating properly.

[1] CISA Fact Sheet on Time for C-Suite: https://ics-cert.us-cert.gov/sites/default/files/documents/Corporate_Leadership_Resilient_Timing_Overview-CISA_Fact_Sheet_508C.pdf

[2] CISA Fact Sheet on Time for Technical Practitioner: https://ics-cert.us-cert.gov/sites/default/files/documents/Technical-Level_Resilient_Timing_Overview-CISA_Fact_Sheet_508C.pdf

Despite the criticality of accurate and precise time, many organizations do not incorporate time hygiene basics into their routine network maintenance. What happens when your network's timing source is lost? How would you know? Do you have a documented recovery plan should your network lose valid time? Does your organization conduct regular testing related to time system outages and recovery to understand critical dependencies? Do you have a documented process for handling **leap seconds** and Daylight Savings Time adjustments? The last leap second event took place December 31, 2016; how did your organization prepare for this leap second adjustment and how do your systems handle leap seconds? Additional information on leap seconds and the December 2016 leap second event can be found here.[3]

This document aims to provide practical guidance for the management of time in enterprise systems and testing your time resilience.

USE CASES

Still not convinced? The use cases below are both real world and fictional, and exemplify the importance of comprehensive cybersecurity and cyber hygiene practices and the correlation of applying these best practices to reduce adverse impacts to your systems' time. The testing recommendations listed in this guidance document are intended to help you understand your time requirements and to preclude similar scenarios from happening to your organization.

SCENARIO ONE

GPS receiver firmware updates were not applied prior to and in preparation of the April 6, 2019, GPS Week Number Rollover event.[4] As a result, the New York City Wireless Network (NYCWiN), responsible for controlling traffic lights and other key functions within the city, was adversely impacted for 11 days in April 2019. A formal report concluded the outage could have been prevented had firmware updates been conducted in advance of the rollover event.[5, 6]

SCENARIO TWO

As a result of the April 6, 2019, GPS Week Number Rollover, a number of Boeing Dreamliner aircraft were grounded in China because of a glitch with their GPS systems. For most airlines, the rollover occurred without incident, but older devices onboard some aircraft

[3] https://www.us-cert.gov/sites/default/files/documents/Best_Practices_for_Leap_Second_Event_Occurring_on_31_December_2016_S508C.pdf
[4] https://www.dhs.gov/cisa/gps-week-number-roll-over
[5] https://statescoop.com/nyc-works-to-reboot-wireless-network-after-gps-update-crashed-it/
[6] https://www1.nyc.gov/assets/home/downloads/pdf/office-of-the-mayor/nycwin-incident-assessment.pdf

displayed an almost 20-year date discrepancy.[7] As many as 15 flights were delayed or canceled as they awaited GPS software updates.

SCENARIO THREE

Your IT network has been attacked causing financial losses and damaging the reputation of your company. Understanding how the attack took place will assist in preventing future incidents and potentially identifying the attacker. According to FBI cyber investigators timestamps are a crucial artifact when performing digital forensics analysis. When comparing events it can be difficult to determine what activity caused another when timestamps are incorrect. When investigating computer intrusions, the timing associated with malware artifacts being written to disk or in memory and any corresponding network traffic, is critical, as it can make the difference between correlating the network activity of the malicious attack, rather than introducing ambiguity from other causes. Determination of activity related to the user versus a malicious actor is heavily dependent upon the accuracy and consistence of time stamps across data sets. While timing itself is important, equally important is understanding the time offsets or time zones of the timestamp data. Only with accurate timestamps and properly correlated time offsets can accurate timelines of computer intrusions be retrieved.

RECOMMENDATIONS AND TEST PLAN

1. KNOW YOUR SYSTEM

The best way to manage and secure your network is to understand the nature of all the devices on your network. It is important to identify, verify, and document timing dependencies within your organization and create a timing topology (see Appendix A) to assist with identifying which devices rely on accurate time and what level of **accuracy** and **precision** they need.

The following is a real-world instance of why knowing your system is important. A recent Apple software update notice advised users to update specified devices prior to November 3, 2019, to maintain accurate GPS location and correct date and time functionality. These devices where not impacted by the April 6, 2019, GPS Week Rollover event as Apple programmed the update to occur on a date after the week rollover event. This exemplifies why knowing your system is critical to you and your users operations; it also directly correlates to item 1.a.i.3 below.[8]

a. Managing timing and synchronization devices used in your network.
    i. Testing Questions:
        1. Do you have policies governing the distribution of time of day on your network?

[7] https://simpleflying.com/boeing-787-china-grounding/
[8] https://support.apple.com/en-us/HT210239

2. Can you identify which servers provide time across your network? Do you have **traceability** from time servers to **Stratum** 1 clocks? Do those servers acquire time from a Stratum 1 time reference?
3. If a GPS receiver is providing time on your network, are you including the receiver in your standard IT inventory and providing regular software/firmware updates per manufacturer recommendations?
4. Do you scan your network regularly for time servers?

b. Identify the applications or systems that require time for operation within your organization.
    i. Testing Questions:
        1. Have you validated these systems and applications really need time?
        2. At what level of accuracy, with respect to UTC (NIST)/UTC (USNO), are the systems reliant on time?
        3. Do you have a time source and distribution method that meets the level of accuracy identified in item 2 above?

c. Maintain an inventory of your organization's time-dependent systems.
    i. Testing Questions:
        1. Does your organization have an inventory of time-dependent systems and their precision requirements?
        2. Does your organization have an inventory of timing and synchronization devices?
        3. Does your organization have a means of keeping this inventory current?
        4. Is time-reliance documented in your system architecture?

d. Is your system capable of detecting time anomalies?
    i. Testing Questions:
        1. Do you have a published Level of Service for timing?
        2. Do you have a way to identify or monitor the Level of Service (if defined)?
        3. Are you able to notify your users if your network is not performing to the published Level of Service agreement?
        4. Is your system capable of detecting anomalies? For example, if your time jumps backwards or forwards?

e. Know how long your system and critical applications can maintain nominal operation in the absence of synchronization to a primary time source?
    i. Testing Questions:
        1. Has your organization identified a **holdover** time for each time-reliant system and application in your inventory?
        2. Has the holdover time been approved by end users (have you validated that it meets business or mission requirements)?

3. Has regular preventative maintenance been performed to ensure holdover devices are operationally ready and maintain quality if reference source degrades?

f. Understand how the system reacts when time accuracy is degraded.
    i. Testing Questions:
        1. Are systems designed to inform critical time dependent applications that timing is degraded and may not be reliable?
        2. Do applications have error handling routines to address degraded or unreliable time?
        3. Are operators trained to respond to GPS receiver alarms/fault indications?
        4. Do you have an alternate/backup source of timing to go to should your primary time source be degraded?

2. KNOW YOUR TIMING SOURCE (S)

It is imperative to know your primary time source; do you utilize a time service, **NTP**, **PTP**, or **GPS** via antenna and receiver. Many organizations utilize a GPS receiver to obtain time and distribute that time through NTP. It is recommended to utilize at least two or more **traceable** time sources with the lowest possible **stratum** to minimize or eliminate timing errors.

a. Identify the primary source(s) of time for your organization.
    i. Testing Questions:
        1. What is your primary source of time?
        2. Do you have a secondary time source identified and configured?
        3. What level of accuracy (i.e., seconds, milliseconds or microseconds) is provided by your time source?
        4. Does that source meet your requirements for time?
        5. Are processes defined to resolve time source discrepancies?

b. Do you have a regulatory Level of Service requirement for your system or application? Determine the level of time performance needed for your system or application.
    i. Testing Questions:
        1. Can your systems tolerate degradation to Level of Service?
        2. Are your systems able to holdover for x hours/days until external time returns?
        3. Are your systems able to operate without your time source for any length of time? For example, does the system have a holdover capability (internal oscillator) that enables some Level of Service during a disruption of primary source(s)?

c. Are all GPS receivers in compliance with the latest Global Positioning System (GPS) Interface Control Document (ICD)? The latest version of the GPS ICD can be found on gps.gov (https://www.gps.gov/technical/icwg/).
    i. Testing Questions:
        1. Check for firmware updates to comply with ICD updates.

d. Do you have an authentication scheme to verify your time comes from a legitimate time server(s)?
    i. Testing Questions:
        1. Test time servers, validate authenticity.

3. KNOW YOUR USERS

a. Do your users have regulatory requirements for time on their system or application? Is this captured in your service-level agreement?

b. Do you know whether your customers depend on your systems/network as a source of accurate time?

c. Have you published a Level of Service for timing on your network?

4. REGULARLY UPDATE YOUR SYSTEM

a. Practice good cyber hygiene within your network as well as with special purpose time equipment. Regularly update your systems and firmware.
    i. Testing Questions:
        1. Do you deploy firewalls and use virus protection?
        2. Are software patches and system updates installed once available? Updates are located at: http://www.ntp.org/downloads.html. The network manager should maintain a file or log of NTP software/firmware versions of each client.
        3. The NTP Security Notice site can provide vulnerability and mitigation details and is located at: http://support.ntp.org/bin/view/Main/SecurityNotice
        4. Are timing and synchronization devices routinely patched?
        5. Do you receive push notifications from vendors when patches are available?
        6. Are GPS timing receivers installed in accordance with DHS best practices?[9]

b. When incorporating new timing sources or devices, consider full-lifecycle cyber security with best practices built-in at the time of product delivery.
    ii. Testing Questions:

[9] https://www.dhs.gov/sites/default/files/publications/GPS-PNT-Best-Practices-Time-Frequency-Sources-Fixed-Locations-508.pdf

1. Are timing and synchronization devices included in your lifecycle management plan?
2. If timing and synchronization devices are not upgradable are they scheduled for replacement?
3. Does the timing and synchronization equipment have strong default security settings?
4. Is the timing and synchronization device and its software/firmware adaptable and upgradeable?

c. Follow guidance provided by the manufacturer for maintenance and updates to hardware and software to ensure optimal operation of your equipment.

d. Regularly back up data and/or files (i.e., configuration files, settings, etc.).

5. DOCUMENT AND TEST YOUR SYSTEM AND SOURCES

a. Have processes in place to validate your internal and external time source(s).
   i. Testing Questions:
      1. For timing systems and devices have you documented processes for maintenance, testing, and validation?
      2. Do you have time maintenance, time anomaly, and time recovery procedures documented?
      3. Are these processes incorporated into your Standard Operating Procedures (SOPs)?
      4. Are employees familiar and trained on timing system, device maintenance, and testing protocols?
      5. Do you perform good cyber hygiene?

b. Test your time equipment to ensure it operates according to your accuracy and precision requirements.
   i. Testing Questions:
      1. Do you have clear timing protocol policies?
      2. What timeservers are master clocks and how do those clocks acquire their time?
      3. Are GPS/GNSS timing devices (receivers and antennas) installed and maintained in accordance with DHS best practices.[10]
      4. Do you have a documented process to establish time after an outage?
      5. Block non-authenticated ports at the firewall for network perimeter security?

[10] https://www.navcen.uscg.gov/pdf/gps/Best%20Practices%20for%20Improving%20the%20Operation%20and%20Development%20of%20GPS%20Equipment.pdf

c. Incorporate battery tests and replacement schedules as part of your maintenance schedule. Use Uninterruptable Power Source (UPS) and test regularly.

d. Using a test bed can be helpful prior to deployment of new or updated systems, but keep in mind there is no guarantee the test bed will operate like the actual network.

e. Identify testing intervals annually and before and after a known time event (i.e., leap second, daylight saving time).

6. DIVERSIFY YOUR TIMING SOURCES

a. Diversify receiver types (models and manufacturers) within your network; this provides resilience within your network.

b. Use multiple available timing sources (network-based, system clocks, two-way time transfer, etc.) to avoid single points of failure.

c. Understand the benefits, limitations, and risks associated with each timing source.

7. DETECT AND ADDRESS ANOMALIES IN YOUR TIMING SOURCES

a. Have a way to detect anomalies in your time source(s).
    i. Testing Questions:
        1. Do you have documented processes to follow should anomalies be detected? These may include audit logs, alerts, etc.
        2. Are operators/network staff/technical staff trained to respond to alarms, indicating timing issues?

b. Based on your time requirements, do you have equipment, processes and procedures in place to handle extended time source outages/anomalies?

c. If your primary time source becomes corrupted or unavailable, do you have a process for moving to an alternative time source? Is this external or internal?

REFERENCES

(1) Department of Homeland Security, *Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure*, https://www.us-cert.gov/sites/default/files/documents/Improving_the_Operation_and_Development_of_Global_Positioning_System_%28GPS%29_Equipment_Used_by_Critical_Infrastructure_S508C.pdf

(2) Global Positioning System (GPS) Interface Control Documents (ICDs) https://www.gps.gov/technical/icwg/

(3) U.S. Department of Homeland Security, United States Coast Guard Navigation Center, *Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations*, https://www.dhs.gov/sites/default/files/publications/GPS-PNT-Best-Practices-Time-Frequency-Sources-Fixed-Locations-508.pdf

(4) U.S. Department of Homeland Security, National Cybersecurity & Communications Integration Center, *Best Practices for Leap Second Event Occurring on 31 December 2016*, https://www.us-cert.gov/sites/default/files/documents/Best_Practices_for_Leap_Second_Event_Occurring_on_31_December_2016_S508C.pdf

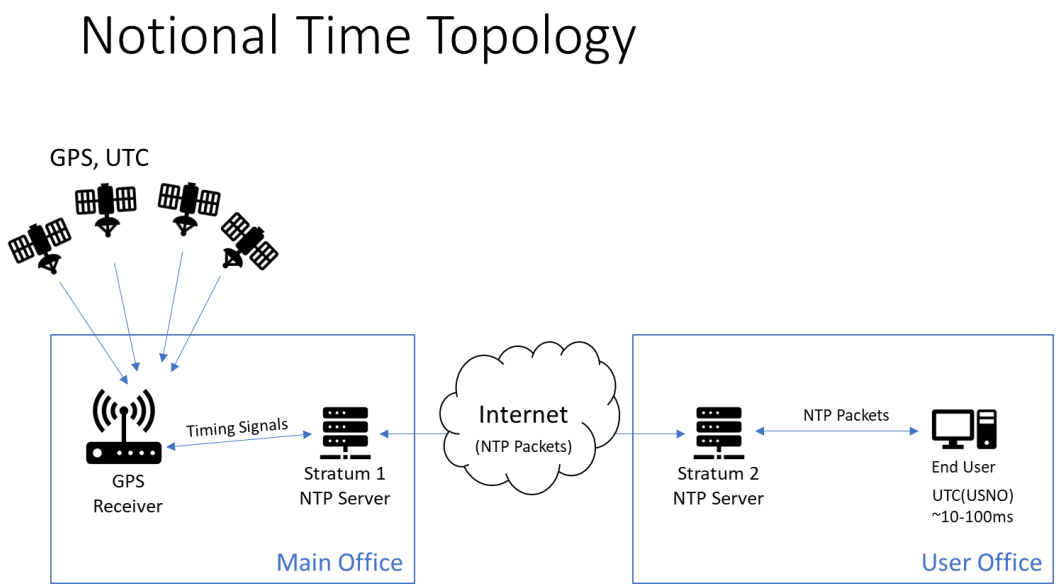
(5) Internet Engineering Task Force (IETF), Network Time Protocol Best Current Practices, https://www.rfc-editor.org/rfc/pdfrfc/rfc8633.txt.pdf

(6) Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations, 6 January 2015, https://www.us-cert.gov/sites/default/files/documents/Best%20Practices%20-%20Time%20and%20Frequency%20Sources%20in%20Fixed%20Locations_S508C.pdf

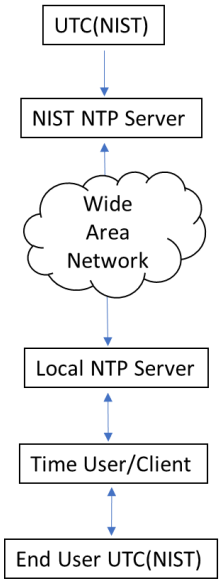
APPENDIX A

If your mission or business service requires accurate time to successfully operate, it is critical to understand and identify your organization's time dependencies and requirements. This can best be accomplished by maintaining an awareness of all the devices on your network via network topology diagrams.

The network topologies illustrated below provide examples of how your organization can document its timing dependencies.



Example Topology 1



Example Topology 2

In Example Topology 1, GPS and UTC are shown as primary timing sources. The timing information from either source is shown to propagate through the network to an end user device via three devices: a GPS receiver and Stratum 1 and 2 NTP Servers. All three devices, to include the primary sources, should be documented as time dependencies of the end user device.

Example Topology 2 shows a time user/client receiving timing information from NIST.

GLOSSARY

Accuracy – the degree of conformity of a measured or calculated value to its definition, related to the offset from an ideal value.*

Coordinated Universal Time (UTC) – the international atomic time scale that serves as the basis for timekeeping for most of the world. UTC is a 24-hour timekeeping system. The hours, minutes, and seconds expressed by UTC represent the time-of-day at the Earth's prime meridian (0^0 longitude) located near Greenwich, England. UTC is the ultimate standard for time-of-day, time interval, and frequency measures. Clocks synchronized to UTC display the same hour, minute, and second all over the world (and remain within one second of UT1). Oscillators synchronized to UTC generate signals that serve as reference standards for time interval and frequency.*

Global Positioning System (GPS) – is a U.S.-owned utility that provides users with positioning, navigation, and timing (PNT) services.**

GPS Time – the Global Positioning System (GPS) is a constellation of satellites each carrying multiple atomic clocks. The time on each satellite is derived by steering the on-board atomic clocks to the time scale at the GPS Master Control Station, which is monitored and compared to UTC(USNO). GPS time does not adjust for leap seconds, it is ahead of UTC(USNO) by the integer number of leap seconds that have occurred since January 6, 1980, plus or minus a small number of nanoseconds. However, the time offset from UTC is contained in the GPS broadcast message and is usually applied automatically by GPS receivers.***

Holdover – performance of an oscillator in the event of loss of synchronization

Leap Second – a second added to Coordinated Universal Time (UTC) to make it agree with astronomical time to within 0.9 second. UTC is an atomic time scale, based on the performance of atomic clocks. Astronomical time is based on the rotational rate of the Earth. Since atomic clocks are more stable than the rate at which the Earth rotates, leap seconds are needed to keep the two time scales in agreement.*

Network Time Protocol (NTP) – a standard protocol used to send a time code over packet-switched networks, such as the public internet. The Network Time Protocol (NTP) was created at the University of Delaware, and is defined by the RFC-1305 document. The NTP packet includes three 64-bit time stamps and contains the time in UTC seconds since January 1, 1900 with a resolution of 233 picoseconds. The NTP format is supported by the NIST Internet Time Service.*

NIST Time – UTC(NIST) is the coordinated universal time scale maintained at NIST. The UTC(NIST) time scale comprises an ensemble of cesium beam and hydrogen maser atomic clocks, which are regularly calibrated by the NIST primary frequency standard. The number of clocks in the time scale varies, but is typically around ten. The outputs of the clocks are combined into a single signal by using a weighted average. The most stable clocks are assigned the most weight. The clocks in the UTC(NIST) time scale also contribute to the International Atomic Time (TAI) and Coordinated Universal Time (UTC). UTC(NIST) serves

as a national standard for frequency, time interval, and time-of-day. It is distributed through the NIST time and frequency services and continuously compared to the time and frequency standards located around the world. ***

Oscillators – an electronic device used to generate an oscillating signal. The oscillation is based on a periodic event that repeats at a constant rate. The device that controls this event is called a resonator. The resonator needs an energy source so it can sustain oscillation. Taken together, the energy source and resonator form an oscillator. Although many simple types of oscillators (both mechanical and electronic) exist, the two types of oscillators primary used for time and frequency measurements are quartz oscillators and atomic oscillators.*

Precision – the ability of a device to produce, repeatedly and without adjustments, the same value or result, given the same input conditions and operating in the same environment.*

Precision Time Protocol (PTP) – a standard protocol defined by the IEEE-1588 standard for sending time over packet-switched networks. The Precision Time Protocol (PTP) can potentially obtain much lower uncertainties than the Network Time Protocol (NTP), often less than 1 μs. Unlike NTP, PTP is generally not implemented over the public Internet. It is typically utilized over private or local area networks where path delays can be better measured and estimated. The grandmaster clock is the time reference for all other clocks in a PTP system. The other clocks are designated as ordinary clocks, which have a single PTP port, and boundary clocks, which have multiple network connections and can bridge synchronization from one network segment to anther.***

Resilience – the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions; includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. (Presidential Policy Directive 21)

Stability – an inherent characteristic of an oscillator that determines how well it can produce the same frequency over a given time interval. Stability does not indicate whether the frequency is right or wrong, but only whether it stays the same.*

Stratum Clock – a clock in a telecommunications system or network that is assigned a number that indicates its quality and position in the timing hierarchy. The highest quality clocks, called stratum 1 clocks, have a frequency offset of 1×10^{-11} or less, which means that they can keep time to within about one microsecond per day. Only stratum 1 clocks may operate independently; other clocks are synchronized directly or indirectly to a stratum 1 clock.*

System architecture – fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution. (NIST SP 800-160)

Testing interval – the elapsed time between two events. Time interval is usually measured in small fractions of a second, such as milliseconds, microseconds, or nanoseconds.*

Traceability – the property of a measurement result whereby the result can be related to a reference through a documented unbroken chain of calibrations, each contributing to the measurement uncertainty.*

Two-way time transfer – a measurement technique used to compare two clocks or oscillators at remote locations. The two-way method involves signals that travel both ways between the two clocks or oscillators that are being compared.*

United States Naval Observatory (USNO) – established in 1830, the USNO is one of the oldest scientific agencies in the United States. The USNO determines and distributes the timing and astronomical data required for accurate navigation and fundamental astronomy. It maintains a UTC time scale that is typically within 20 nanoseconds of UTC(NIST). Both NIST and the USNO can be considered official sources of time and frequency in the United States.*

USNO Time – the USNO maintains the U.S. Department of Defense reference for time and time interval. USNO has an ensemble of atomic clocks, which is used to derive a time scale called UTC(USNO). The clocks in the ensemble contribute to International Atomic Time (TAI) and Coordinated Universal Time (UTC). UTC(USNO) and UTC(NIST) are kept in very close agreement, typically to within 20 nanoseconds, and both can be considered official sources for time in the United States.***

*https://www.nist.gov/pml/time-and-frequency-division/popular-links/time-frequency-z/time-and-frequency-z-z-index

** https://www.gps.gov/systems/gps/

*** https://www.nist.gov/pml/time-and-frequency-division/nist-time-frequently-asked-questions-faq