RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **TECH-R02**

# The Time is Now: The Criticality of Time Synchronization & Information Security

**Ben Rothke CISSP, CISM**

Senior Information Security Manager
Tapad
@benrothke

# Disclaimer

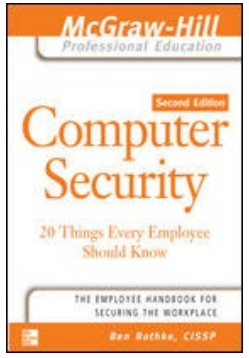
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

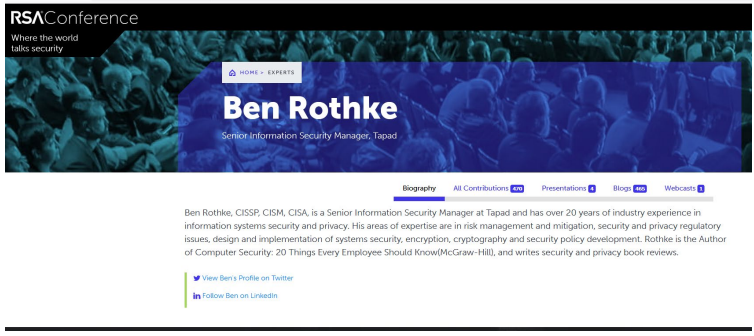
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

# About me

- Ben Rothke, CISSP, CISM, CISA
- Manager - Information Security at Tapad
- Author
  - *Computer Security: 20 Things Every Employee Should Know*
  - RSA Conference book reviews
  - Articles: https://medium.com/@brothke



# Agenda

- Session is:
  - An overview of the need for time synchronization
  - Why time synchronization is critical for security software and hardware to run effectively
  - An overview of NTP
- Session is not:
  - A comprehensive overview of setting up a corporate  time synchronization infrastructure
  - How to configure NTP
  - Which time synchronization product to purchase

# The problem

- Computer clocks aren’t designed for accuracy.
- A typical clock can drift more than one hour in a year.
- Without effective network time synchronization, effective time can’t be established.

# Doing things on time is a universal need


- Plane departures
- Self-driving cars
- Cron jobs
- Forensics
- GPS
- Network authentication
- Industrial processes
- Network logs
- Job shifts
  - *The only reason for time is so that everything doesn't happen at once* - Albert Einstein

# Importance of time synchronization

- Allows events to occur at the proper time - *event synchronization*
  - Schedule a process and ensure that it starts or stops on time or runs for a specified period regardless of when it starts or stops
- Provides proof when events occurred or did not occur - *digital forensics*
  - Ensure that cooperating processes can interoperate correctly, so that if one process hands a task off to another process, the second process will in fact be ready to accept the handoff

# Costs / ROI of time synchronization


- Enterprise-level time server costs
  - approximately $4,000 to $12,000 depending on the level of accuracy required, and if redundancy is needed.
- Can be installed and running in a few hours
- Benefits include:
  - prevent operational failure
  - improve security
  - mitigate legal exposure
- ROI
  - Time services ROI can often measured in weeks or months

# Practical Example

- Attacker illegally infiltrates your system on Sunday January 9, 2022 between 14:42:39 and 15:21:57
- Your system logs show that these events occurred starting at 19:49:12
- Attacker has witnesses stating that he was watching a NFL Game with them from about 18:00 – 22:00
- Prosecutor won't take the case as the logs can't be admitted as evidence
- *A snafu such as seriously unsynchronized logs would be regarded by a defense layer as a providential gift* - Ronald Coleman, Esq.

# Regulatory


- Time synchronization is part of numerous regulations and industry standards:
  - 21 CFR Part 11
  - PCI DSS
  - GLBA
  - Sarbanes-Oxley
  - HIPAA
  - National Emergency Number Association
  - Public Safety Answering Point Master Clock Standard
  - Standard #1221 - Installation, Maintenance and Use of Emergency Services Communication Systems

# Time synchronization - PCI DSS v4

| Requirements and Testing Procedures | | Guidance |
|---|---|---|
| **10.6** Time-synchronization mechanisms support consistent time settings across all systems. | | |
| **Defined Approach Requirements**<br>**10.6.1** System clocks and time are synchronized using time-synchronization technology.<br>**Customized Approach Objective**<br>Common time is established across all systems.<br>**Applicability Notes**<br>Keeping time-synchronization technology current includes managing vulnerabilities and patching the technology according to PCI DSS Requirements 6.3.1 and 6.3.3. | **Defined Approach Testing Procedures**<br>**10.6.1** Examine system configuration settings to verify that time-synchronization technology is implemented and kept current. | **Purpose**<br>Time synchronization technology is used to synchronize clocks on multiple systems. When clocks are not properly synchronized, it can be difficult, if not impossible, to compare log files from different systems and establish an exact sequence of events, which is crucial for forensic analysis following a breach.<br>For post-incident forensics teams, the accuracy and consistency of time across all systems and the time of each activity are critical in determining how the systems were compromised.<br>**Examples**<br>Network Time Protocol (NTP) is one example of time-synchronization technology. |
| **Defined Approach Requirements**<br>**10.6.2** Systems are configured to the correct and consistent time as follows:<br>• One or more designated time servers are in use.<br>• Only the designated central time server(s) receives time from external sources.<br>• Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC).<br>• The designated time server(s) accept time updates only from specific industry-accepted external sources.<br>• Where there is more than one designated time server, the time servers peer with one another to keep accurate time.<br>• Internal systems receive time information only from designated central time server(s).<br>**Customized Approach Objective**<br>The time on all systems is accurate and consistent. | **Defined Approach Testing Procedures**<br>**10.6.2** Examine system configuration settings for acquiring, distributing, and storing the correct time to verify the settings are configured in accordance with all elements specified in this requirement. | **Purpose**<br>Using reputable time servers is a critical component of the time synchronization process.<br>Accepting time updates from specific, industry-accepted external sources helps prevent a malicious individual from changing time settings on systems.<br>**Good Practice**<br>Another option to prevent unauthorized use of internal time servers is to encrypt updates with a symmetric key and create access control lists that specify the IP addresses of client machines that will be provided with the time updates. |
| **Defined Approach Requirements**<br>**10.6.3** Time synchronization settings and data are protected as follows:<br>• Access to time data is restricted to only personnel with a business need.<br>• Any changes to time settings on critical systems are logged, monitored, and reviewed.<br>**Customized Approach Objective**<br>System time settings cannot be modified by unauthorized personnel. | **Defined Approach Testing Procedures**<br>**10.6.3.a** Examine system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need.<br>**10.6.3.b** Examine system configurations and time synchronization settings and logs and observe processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed. | **Purpose**<br>Attackers will try to change time configurations to hide their activity. Therefore, restricting the ability to change or modify time synchronization configurations or the system time to administrators will lessen the probability of an attacker successfully changing time configurations. |

PCI Security Standards Council

TAPAD A part of experian.

# Incorrect timing adds to conspiracy theories

# Absolute vs. Relative Time

- Since the 17th century time has been measured astronomically
  - The event of the sun reaching the highest point in the sky is called the transit of the sun
  - The interval between two consecutive transits of the sun is called a solar day
- In the 1940s, it was established that the earth's rotation is not constant
  - The earth is spinning slower
  - 300 million years ago, there were about 400 days per year

# Absolute vs. Relative Time

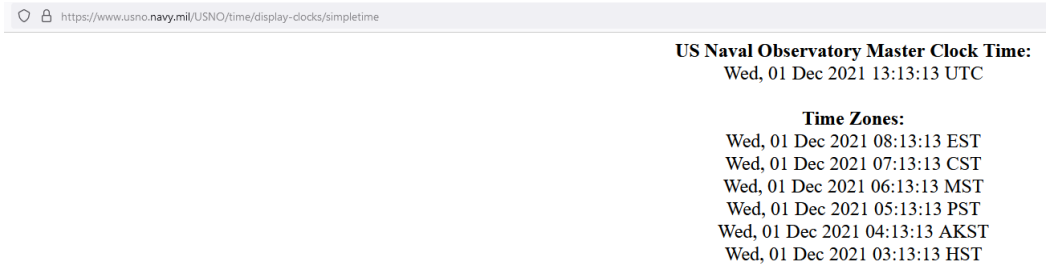
- Relative or astronomic time is based on the earths rotation.
- Earth's rotation is not absolute, leap seconds are added to keep UTC synchronized with the astronomical timescale.
- 1967 - 13th General Conference on Weights and Measures defined the International System unit of time, the *second*, in terms of atomic, rather than motion of the Earth.
  - https://www.bipm.org/en/home
- Defines the *second* as duration of 9,192,631,770 cycles of microwave light absorbed via transition of cesium-133 atoms in their ground state.

# Atomic Clocks

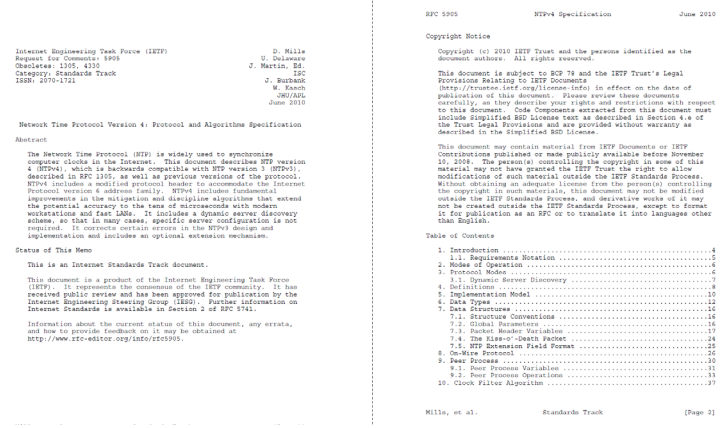
- Atomic clock was invented in 1948
  - Thousands of worldwide cesium-133 clocks
  - Periodically they are averaged to produce international atomic time (TAI)
  - The Bureau International de l'Heure (BIH) maintains the official clock
  - Accurate to roughly one second every million years

# USNO Master Clock

- USNO Time Service Department atomic clock timescale is based on an ensemble of cesium-beam frequency standards, hydrogen masers, and rubidium fountains.
- UTC (USNO) is usually kept within 10 nanoseconds of UTC (BIPM)
  - https://www.usno.navy.mil/USNO/time/master-clock



# Network Time Protocol (NTP)



Internet Engineering Task Force (IETF)
Request for Comments: 5905
Obsoletes: 1305, 4330
Category: Standards Track
ISSN: 2070-1721

D. Mills
U. Delaware
J. Martin, Ed.
ISC
J. Burbank
W. Kasch
JHU/APL
June 2010

Network Time Protocol Version 4: Protocol and Algorithms Specification

Abstract

The Network Time Protocol (NTP) is widely used to synchronize computer clocks in the Internet. This document describes NTP version 4 (NTPv4), which is backwards compatible with NTP version 3 (NTPv3), described in RFC 1305, as well as previous versions of the protocol. NTPv4 includes a modified protocol header to accommodate the Internet Protocol version 6 address family. NTPv4 includes fundamental improvements in the mitigation and discipline algorithms that extend the potential accuracy to the tens of microseconds with modern workstations and fast LANs. It includes a dynamic server discovery scheme, so that in many cases, specific server configuration is not required. It corrects certain errors in the NTPv3 design and implementation and includes an optional extension mechanism.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5905.

RFC 5905 NTPv4 Specification June 2010

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

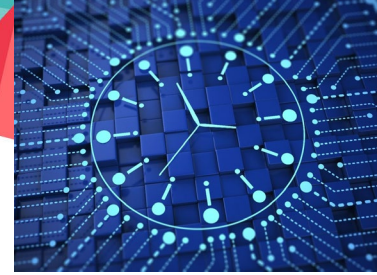
Table of Contents



Mills, et al. Standards Track [Page 1]

- RFC 5905 – NTP - Version 4
  - https://datatracker.ietf.org/doc/html/rfc5905
- UDP port 123
- Accurate to within 10 - 100 milliseconds
- UDP is an unreliable protocol, but NTP has been architected to sustain levels of accuracy and robustness; even when used over numerous gateways and delays.
- In use over 40 years and remains the longest running, continuously operating Internet application protocol.

# Network Time Protocol (NTP)

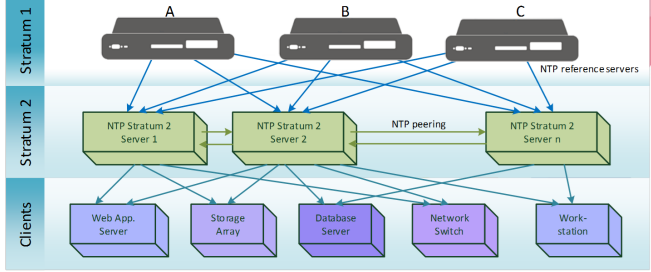


- NTP is only the protocol – not an application
- Implementing NTP requires separate client and server applications
- Developed at Univ. of Delaware by David Mills
  - 1985 – version 1 – RFC 1059
  - 1989 – version 2 – RFC 1119
  - 1992 – version 3 – RFC 1305
  - 2010 – version 4 - adds secure authentication features
  - 2022 – current production version: 4.2.8p15 – June 2020
  - https://www.ntp.org/downloads.html

# NTP Time Sources

- Dedicated NTP server with access to an external UTC time source
  - Stratum-1 GPS-based hardware device
- Public server with or without direct access to UTC time
  - Internet-based stratum 1,2 or 3
- Local master clock time source on a local network
  - Set by a local network administrator

# NTP Design




- Choose your NTP time source
  - Internal – More control, more management
  - External – Less control, less management
- Time source will impact topology, configuration, and management aspect of the entire NTP infrastructure.
- Possible time sources include:
  - Dedicated internal stratum-1 hardware appliance
  - Public stratum-1 server
  - Public stratum-2 NTP server
  - Local master

# Public vs. Private time servers


- If your desired accuracy is in:
  - **Microseconds** – Don't rely on public time servers. Purchase a stratum-1 primary time server.
  - **Milliseconds** - you can likely rely on public time servers
  - **Seconds** - you can rely on public time servers.
- Public time servers are administered on a voluntary basis and there is no guarantee of server availability, accuracy or security.
- NTP Pool - huge virtual cluster of timeservers providing reliable easy to use NTP services.
  - https://www.ntppool.org

# NTP Time server feature comparison

| Time Source | Availability | Accuracy | Security | Costs |
|---|---|---|---|---|
| Dedicated server | High | High | High | High |
| Public server | Medium | Medium | Low | Low |
| Local master | High | Low | High | Low |

# NTP design - topology

- Determine the desired level of time accuracy
- Number of NTP clients
- Network infrastructure redundancy
- Network physical topology and geography
  - How are the sites connected?
  - Round trip delays can impact NTP and negatively affect time accuracy

# NTP design - features

- Determine which NTP features to use
  - Basic
  - Security
    - Authentication
    - Access control
  - Redundancy
    - Redundancy between peers
    - Redundancy configuration on clients

# NTP design - management

- How much you need to manage your NTP infrastructure is dependent on how important synchronized time is to your organization
  - SNMP
  - Ping
  - Vendor tools
- Metrics and statistics
  - Averages
  - Clock skew
  - Clock drift

# Apply time synchronization to your org

1. Ensure that firewalls, routers, critical servers, etc. have correct time.
2. Identify all critical network devices that require accurate time.
3. Appoint a responsible technical staff member to be the time services liaison and to manage time services.
4. Meet with vendors of time synchronization equipment to determine the solution that best fits your organization and specific needs.
5. Advise management of the security risk of non-synchronized time
6. Management approval for purchase of time synchronization equipment
7. Ensure that time synchronization is an enterprise policy

# Network time distribution stratum levels

- Stratum 0 - Reference clock source
  - NPL, NIST, USNO, GPS
- Stratum 1 - Primary Time Servers
- Stratum 2 - Secondary Time Servers; generally application servers, NOS servers, routers
- Stratum 3 - Workstations, servers, Controlled Timed Device (CTD)
- Stratum 4 - x – Deeper into other workstations, servers, and CTD

# Policy

- Time synchronization must be made part of the corporate IT systems and security policies
- Example:
  - “Time synchronization to an accurate time source is required on all enterprise network devices”.
- Without a policy, there will be no impetus for staff to achieve the goal of accurate, synchronized time.

# GPS as a trusted time source

- GPS is unique in that it offers a direct, accurate and secure connection from UTC to inside the security of the organization's network firewall.
- No WAN or router delays
- No need to keep NTP port 123 open on the firewall
- European Space Agency Galileo navigation satellite systems provides same services as GPS.

# Audit

- Infrastructure must be able to prove that the time on any monitored system was correctly synchronized at a particular time and date with a specified time source.
- Often required by industry specific regulations
- Audit logs must be used within the context of digital forensics.
  - Follow the rules of evidence

# Time synchronization in the cloud

- Most cloud providers will perform time synchronization
  - Customer is responsible for the logging and monitoring
- Amazon Time Sync Service
  - Accessible from all EC2 instances
  - https://aws.amazon.com/about-aws/whats-new/2017/11/introducing-the-amazon-time-sync-service/
  - https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/set-time.html
- Google Cloud Services (GCP)
  - https://cloud.google.com/container-optimized-os/docs/how-to/create-configure-instance#time_synchronization

# Products

- Orolia
  - https://www.orolia.com
- EndRun Technologies
  - https://endruntechnologies.com
- Microsemi
  - https://www.microsemi.com



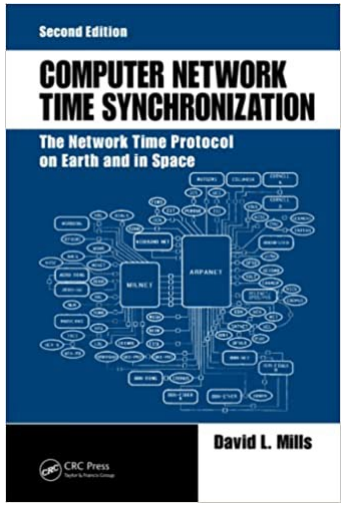

- Product should have security features, including VLAN support, account / access management, authentication, encryption, security event logs, firmware updates, and more.

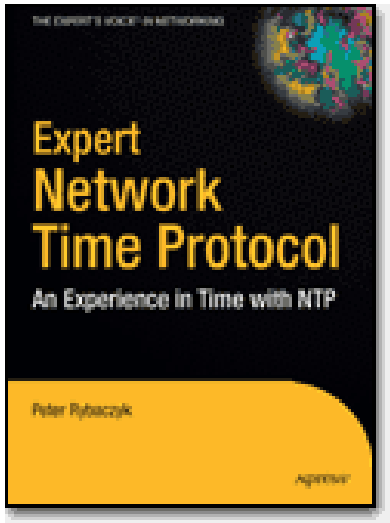
# International organizations

- Physikalisch-Technische Bundesanstalt (PTB)
  - https://www.ptb.de/cms/en.html
- National Physical Laboratory NPL, UK
  - https://www.npl.co.uk/
- Royal Observatory
  - https://www.rmg.co.uk/royal-observatory
- Federal Office of Metrology (METAS)
  - https://www.metas.ch/metas/de/home.html
- Bureau International des Poids et Mesures
  - https://www.bipm.org/en/home

# Books

- Expert Network Time Protocol: An Experience in Time with NTP - Peter Rybaczyk
- Computer Network Time Synchronization: The Network Time Protocol - David Mills
  - NTP documentation repository https://support.ntp.org/bin/view/Main/DocumentationIndex



# Apply

- Today
  - Understand the criticality of network time synchronization
- Next 90 days
  - Commence the corporate initiatives for correct network time
  - Identify all critical network devices that require accurate time.
- Within six months
  - Ensure that time synchronization is an enterprise policy
  - Create project plans to remediate any time synchronization gaps

# Conclusion

- Need for synchronized time is a crucial  business and technology need.
- Synchronized time is an integral part of an effective network and security architecture.
- Information security hardware and software is highly dependent on synchronized time.
- Ensuring accurate time is relatively inexpensive and offers a significant ROI.

# Q/A

- Any questions?
- Please remember to fill out the evaluation forms