IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.co

ITP4849

Time Management in Information Security

Göran Pulkkis and Kaj Grahn
Arcada Polytechnic
Metsänpojankuja 3
02130 Espoo, Finland
tel. +358-9-525321, fax +358-9-52532222
goran.pulkkis@arcada.fi, kaj.grahn@arcada.fi

ABSTRACT

This paper surveys essential time management issues in information security. The generation and distribution of Coordinated Universal Time (UTC), the certified, reliable common international time source, is outlined. The theoretical and methodological foundations of secure time synchronization of computer network device clocks are presented. Necessary fault tolerant features in time synchronization protocols are pointed out. The Internet standard for time synchronization of network computer clocks, the Network Time Protocol (NTP) and the emerging security features of NTP are briefly described. Time stamping protocols, time stamping renewal protocols, time stamping technology, and time stamping services are shortly surveyed. The role of time stamping in implementing reliable digital archives with persistent information integrity is pointed out. A recently launched pilot project on processing and archiving PKI certified digital documents in the administration of Arcada Polytechnic is presented.

1 INTRODUCTION

Time management of authentication is essential in tracing and auditing usage patterns in information systems, time management of integrity is essential in information backup procedures, and time management of non-repudiation is essential in electronic administration processes as well as in e-commerce. For time management an exact, reliable and unconditionally accessible time reference is needed as well as tools and procedures to prove that an event has occurred before or after a specified moment of time. Time synchronization in peer-to-peer computer networks is dependent on an exact time reference. Key area examples where time synchronization is essential are: file time stamps, log file accuracy, auditing, monitoring, access security, authentication and scheduled operations. Time management security focuses on reliable time synchronization, time stamping and secure digital archiving.

2 RELIABLE TIME SOURCES

More than 30 years Coordinated Universal Time (UTC) has been the internationally accepted time standard. UTC follows exactly – except for some inserted leap seconds /12/ - the International Atomic Time (TAI) calculated by the Bureau International des Poids et Mesures (BIPM) /13/ from more than 200 atomic clocks in metrology institutes and observatories in more than 30 countries. Clock measurement data is compared using satellite communication with Global Positioning System (GPS) satellites and more recently with geostationary telecommunication satellites using Two-Way Satellite Time and Frequency Transfer (TWSTFT). BIPM estimates the TAI accuracy to about 0.1 ms/year /14/.

The task of the BIPM is to ensure world wide uniformity of measurements and their traceability to the International System of Units (SI). As provider of UTC, BIPM is an International Timing Authority. Metrology institutes and observatories, where atomic clocks deliver measurement data for TAI, are National Timing Authorities in their countries. A National Timing Authority delivers a reliable national time source based on UTC.

The Laboratory of Time and Frequency of the Centre for Metrology and Accreditation (MIKES) /15/ is the National Timing Authority in Finland. MIKES, which is an agency of the Ministry of Trade and Industry in Finland, delivers using Cs atomic clocks the UTC based official Finnish time with a present uncertainty of about 300 ns.

The Time & Frequency Division of the National Institute of Standards and Technology (NIST) /16/, an agency of the US Department of Commerce, is the US National Timing Authority. UTC(NIST) is presently the Cesium Fountain Atomic Clock NIST-F1. The uncertainty of UTC(NIST) in relation to UTC(BIPM) is presently about 0.1 ns/day.

The core of reliable time management is an IT infrastructure, in which all local time settings can be proved to be derived from clocks of Timing Authorities. Upper limits of the allowed deviation from UTC should be possible to define. Methods to check at any moment of time, that the difference between a local time source and UTC is less than a required upper limit, should also be available.

The time source of NIST is accessible

- using radio communication to clocks tied to UTC(NIST) in NIST radio stations /16/ or in GPS satellites /17/
- over Internet using the Network Time Protocol (NTP) and **stratum 1** NIST time servers /18/
- using dial-up modem lines via the NIST Automated Computer Time Service (ACTS) /18/.

The security of these access methods to a UTC(NIST) time source is assessed in /19/.

The time source of MIKES is accessible using NTP and Internet connected time servers with clocks tied to UTC(MIKES). Synchronization to GPS satellite clocks will also be possible in a near future /20/.

A draft on a PKI based implementation of a secure and trusted time infrastructure for supplying secure UTC time was proposed on an IETF conference in 1998 /21/. By now, no IETF RFC standard based on this proposal exists, but computer technology supporting this trusted time infrastructure is available /22/.

3 TIME SYNCHRONIZATION IN COMPUTER NETWORKS

3.1 Theoretical and Methodological Foundation

In *external time synchronization* the goal is to set local clocks as close as possible to an external time reference source like UTC. In *internal time synchronization* no external time reference is available and the goal is to minimize the maximum differences between readings of device clocks in a computer network /1/.

Basic time synchronization difficulties arise from

- local clock drift relative to a correct time
- unpredictable synchronization message delays in computer networks.

Worst case estimates of local clock drift define necessary refreshment rates for local time settings. Unpredictable synchronization message delays introduce timing uncertainty in a distributed computing infrastructure. A mathematical treatment of these difficulties is published in /1/. Algorithms for external time synchronization can also be used for internal time synchronization by choosing an arbitrary processor clock as time source /1/.

A structured implementation of time synchronization in a computer network is a layered client/server synchronization hierarchy, in which

- the top layer consists of synchronization servers
- the bottom layer consist of synchronization clients
- computers on all intermediate layers are servers to the computers on the next lower layer and clients to the computers on the next higher layer.

The clock of a server is a time source for a client on the next lower level. The time synchronization topology is of course independent of the computer network topology. A three layer structured implementation of a pure external time synchronization algorithm is illustrated in Fig. 1.

The basis of any clock synchronization algorithm for a distributed computing system is the order in which events occur. The scheme for ordering events in processes of a distributed computing system using logical clocks proposed by Lamport in /2/ has been the basis of many later proposals for time synchronization in distributed computing /3/. The event ordering scheme of Lamport is based on the assumption, that communication links and local clocks are functionally reliable, but synchronization message delays are unpredictable and local clocks have drift /1/. Lamport's scheme is a logical reasoning scheme based upon

- time stamps on events
- the temporal *happened before* relation
- some relation for total ordering of all processes in the distributed computing system.

The integrity of time in Lamport's scheme is in /3/ expressed as updating a vector clock consisting of all logical clocks in the distributed computing system, whenever a process receives a time stamped message. In /3/ is also presented an algorithm for preserving the causal ordering of synchronization messages by delaying incoming messages to processes until certain logical timing conditions are met. A causal ordering violation would occur, if

receive(message2) *happened before* receive(message1)

because of unpredictable message delays even if

send(message1) *happened before* send(message2).

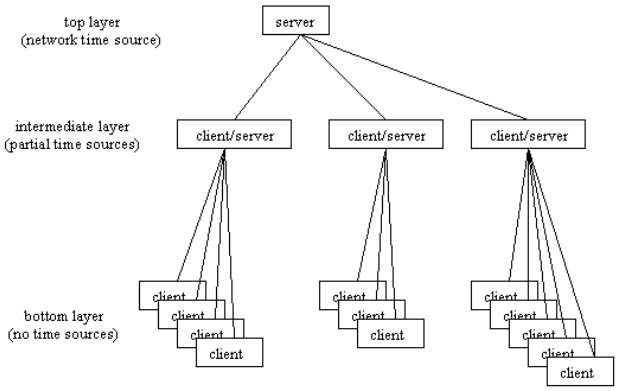

Fig. 1. A three layer structured implementation of a pure external time synchronization algorithm in a network of 16 computers. Network topology is independent of time synchronization topology.

3.2 Fault Tolerant Time Synchronization

Management of communication link unreliability and local clock failures also requires fault tolerance from time synchronization algorithms and protocols. The main weakness with a single common time reference source is unrecoverable time management failure if the common reference fails /4/. Even for a 100% reliable common time reference source in a distributed computing infrastructure fault compensation procedures are still needed for situations, where synchronization to the common reference fails in one or several network devices.

A basic fault tolerant time synchronization protocol for management of local clock failures and unreachable local clocks because of communication link failures in a distributed computing infrastructure is the Byzantine Clock Synchronization Protocol /4/.

Attempts to design a temporal logic - a formalism originally introduced in /5/ - for proving properties of fault tolerant time synchronization protocols have been made. Such a temporal logic should have the ability to /4/

- easily translate from local time to global time assertions
- treat faultiness as a time-varying property
- reason about the cardinalities of processors satisfying certain constraints.

3.3 Network Time Protocol

The Network Time Protocol (NTP) is a time synchronization standard in a TCP/IP network. It is used to synchronize computer time to some reference source, when the deviation from the reference is minimized in all computers. If two NTP servers are synchronized to each other as peers, the two clocks agree on the time reference. At the top of the NTP hierarchies one or more clocks are synchronized to a common time reference and to each other. The reference source can be another computer, a radio, a satellite receiver or a modem. The accuracy of other clocks depends on

- how close a clock is to the reference clock
- the network latency to the clock
- the claimed accuracy of the clock.

Typical accuracy values are within 1 ms on LANs and within some tens of milliseconds on WANs relative to UTC via a GPS receiver /23/.

Other time synchronization protocols, including Digital Time Synchronization Service (DTSS), have influenced NTP. This makes NTP a very robust and mature technology. NTP is useful also in other environments than TCP/IP because of flexible client/server relationship and implemented security /24/.

A NTP client communicates with one or more NTP servers. The system is set up as a hierarchy, where each level is called a **stratum**. Used reference clocks form **stratum 0**. Clients communicate through **stratum 1** servers synchronized to stratum 0. Compared to Figure 1 **stratum 1** is the top layer, **stratum 2** is the intermediate layer and **stratum 3** equals the bottom layer. The clients are potential servers to other clients on a higher stratum level. The UDP protocol is used for client/server communication.

NTP computers operate in different configuration modes with following client and server types: server, client, peer, broadcast/multicast server, and broadcast/multicast client. Clients and servers operate with or without cryptographic authentication. The operation requires little resource overhead. A single NTP server can serve hundreds of clients using only some percents of its CPU capacity. The length of unencrypted NTP Ethernet packets is 90 bytes /23/.

The adjustment of a system's time may take several minutes, because a combining algorithm computes weighted average of time offsets. This reduces the effects of variable latency. The system clock is disciplined to operate in frequency-lock, phase-lock and hybrid modes. An algorithm responsive to network time jitter and clock oscillator frequency wander is used /25/.

The network must be able to resist accidental or malicious attacks. NTPv3 uses symmetric key cryptography to authenticate individual servers, but without secure key distribution support. Also interaction between the authentication and synchronization functions is a problem.

Reliable key management requires secure timekeeping and vice versa. A revised security model and authentication scheme called Autokey has been implemented in NTPv4 /26/.

Autokey is based on a combination of PKI and a pseudo-random sequence generated by repeated hashes of a cryptographic value involving both public and private components. Symmetric key cryptography is supported using MD5 message digests to detect packet modification. Replay is avoided (source verified) by the use of time stamped RSA digital signatures and X.509 certificates. A private key is negotiated with the Diffie-Hellman protocol /26/.

The time stamped digital signature scheme does not provide protection against masquerade and middlemen. Every member of a closed group shares a secret group key in the included. The form could be a private certificate or another certification scheme. Four schemes are implemented in Autokey /26/:

- private certificates
- trusted certificates
- modified Schnorr algorithm
- modified Guillou-Quisquater

In the IETF stime Working Group /27/ published in February 2002 its latest draft on using PKI to secure the NTP protocol. *The purpose of this working group is to define the message formats and protocols – specifically modifications to the existing Network Time protocol (NTP) - which are necessary to support the authenticated distribution of time for the Internet. Work will concentrate on the Internet-based NTP, to be enhanced with the addition of public-key based authentication and security.*

4 TIME STAMPING

The concept *cryptographic time stamp (TS)* on a piece of digital information (a message, a document, a picture, a video sequence, etc.) was defined in /6/, patented /7/, and in a later patent /8/ concretized to

$$TS = Sign(hash(Info||X)||Time) \quad (1)$$

Sign denotes a cryptographic digital signature, *Info* denotes the time stamped piece of information, *X* is a data string used to identify *Info*, *hash* denotes a cryptographic hash function, *Time* denotes the creation date&time of the digital signature, and || denotes concatenation. Later verification of the signature with the public key on the PKI certificate of the signer is thus not only an integrity proof but also a proof that the time stamped piece of information existed at the date&time of the time stamp. Consequently, a time stamp on a digitally signed document proves the existence of the signature at the time&date of the time stamp. The signature is valid, if the PKI certificate of the signer was neither expired nor revoked at the date&time of the time stamp. The reliability of a cryptographic time stamp naturally requires confirmation, that the date&time are derived from a reliable time source.

Time stamp certificates can be revoked or they expire. The lifetime of time stamp certificates can be longer than the lifetime of ordinary signature certificates by increasing key lengths. A time stamp can no longer be verified, if the PKI certificate of the signer is expired/revoked. To prolong the validity of a cryptographic time stamp a time stamp renewal method was defined and also patented /8/ by the inventors of the original time stamping concept. The time stamp renewal method was defined as

$$TS_{i+1} = Sign(hash(TS_i||Info)||Time) \quad (2)$$

The significance of symbols is as in (1). TS_i denotes the original (i=0) or a renewed (i>0) time stamp on *Info* and the certificate to verify TS_i must still be valid at *Time* of the renewed time stamp TS_{i+1}. However, different digital signature protocols and/or different cryptographic hash functions can be user to create TS_i and TS_{i+1}.

The time stamping protocol in latest IETF draft standard /28/ is very similar to the original time stamping methods /6/, /7/ and /8/. Security improvements to the time stamp renewal protocol have recently been proposed /9/.

A commercial time stamping service (TSS) based on the time stamping protocol standard is presented in /29/. A TSS needs a hash of a piece of information for which a cryptographic time stamp is returned. To verify a timestamp the public key on the CA certificate for the private time stamp signing key of the TSS is needed. Such a certificate could be called a TSA (Time Stamping Authority) certificate. Software and computer technology for setting up a TSS is also available /30/. Time stamping software is also embedded in Internet Explorer /31/.

A collection of essential time stamping web links is published on the home page of Helger Lipmaa, professor of Cryptology in Helsinki University of Technology /32/.

An important electronic legal service, digital notarization, is based on cryptographic time stamping. A digital notarization service provider /29/ defines: "Digital notarization is a time stamping service that lets you prove the existence and state of an electronic document at a fixed point in time by creating a digital receipt" /33/. Also the digital trace of any electronic transaction can be notarized.

5 SECURE DIGITAL ARCHIVING

In PKI based information security an electronically signed document should be archived together with the signature certificate. Also the CA certificate needed to verify the ownership of the public key on the signature certificate must be available in the archive.

Digitally signed documents must also have valid time stamps when they are submitted to the archive /10/. Time stamp certificates proving the validity of signatures on the certified points of time must consequently be available in the archive. Also valid root certificates of time stamping authorities must also be available. Only then the authenticity of time stamp certificates can be proved.

To the archive must be added renewed time stamp certificates /8/, /9/ for time stamped documents and certificates already in the archive before the earlier time stamp certificates have expired or are revoked /11/.

Timed integrity control and timed backups of archived electronic information is a necessity since electronic archiving media like magnetic discs/tapes and optical discs are neither fault free nor persistent in the time dimension. Archived electronic documents must be migrated to new electronic archiving medium before media degeneration has spoiled both the archived piece of information itself and all archived backup copies. Archived information is unspoiled as long as its integrity can be checked by signature verification with a valid signature certificate. Otherwise this integrity check also requires a valid time stamp certificate or a chain of renewed time stamp certificates with a valid time stamp certificate in the end of this chain.

Since secure digital archives of signed documents require long term preservation of signature certificates. CA certificates, and TSA certificates and existing Certification and Time stamping Authorities may close their services and new Authorities will emerge. A global infrastructure – Procopius – for certificate archival proposed and simulated in /11/. Procopius is proposed to be not only a secure global write-once publication medium for certificates issued by Time Stamping Services and Certification Authorities but and also a Time Stamping Service to maintain the validity published certificates through renewed timestamps.

5.1 Pilot Project: Digital Processing and Archiving of Signed Documents

In Arcada Polytechnic a pilot project for electronic processing and archiving of invoices started in autumn 2002. Invoices will be attached to X-Sign /34/ based XML forms for electronic processing and archival. Incoming electronic invoices will be attached as such and paper invoices will be scanned. Necessary PKI signatures using Finnish electronic ID cards /35/ will certify the data filled into the XML form together with the attached invoice. Each PKI signature will be time stamped to ensure secure archival. Approved electronic invoices will be

- registered
- interfaced to other administrate software in the economy administration of Arcada
- archived for at least 10 years according to requirements of Finnish legislation.

The archiving period exceeds the lifetime of used signature certificates, and is long enough to require also media migration. For these reasons computerized integrity and backup control procedures will be worked out and simulated for possible future integration in the economic administration of Arcada.

6 CONCLUSIONS

Trusted reliable distributed services in a peer-to-peer network require, that local time is everywhere correct and reliable. Reliable reference time sources, fault tolerant time synchronization in the computer network and the use of secure authentication schemes are essential. Reliable cryptographic time stamping is a prerequisite for e-commerce and electronic administration. For secure electronic archiving integrity preservation is a key issue. PKI based integrity preservation requires a global support infrastructure with timestamp renewal of preserved certificates for archived digital information. Operational integrity preservation procedures must be worked out, evaluated, and tested also in small scale digital archiving, as in a presented pilot project on processing and archiving PKI secured administrative documents.

REFERENCES

Persistent References

/1/ Patt-Shamir, B. and Rajsbaum, S. "A Theory of Clock Synchronization." *Proceedings of the* 26th Symposium on Theory of Computing, May 1994

/2/ Lamport, L. "Time, Clocks and Ordering of Events in a Distributed System." *Communications of the ACM*, Vol. 21, No.7, 1978, pp. 558-565.

/3/ Ganguly, J. and Lemmon, M. D. *Theory of Clock Synchronization and Mutual Exclusion in Networked Control Systems*. Technical Report ISIS-99-007. University of Notre Dame, August 1999

/4/ Shankar, N. "Mechanical Verification of a Generalized Protocol for Byzantine Fault Tolerant Clock Synchronization." in Vytopil, J. (Ed) "Formal Techniques in Real-Time and Fault-Tolerant Systems." *Lecture Notes in Computer Science*, Vol. 571, Berlin: Springer Verlag, 1992, pp. 217-236

/5/ Pnueli, A. "The Temporal Logic of Programs." *Proceedings of the 18th Annual IEEE Symposium on Foundations of Computer Science*, 1977, pp. 46-57

/6/ Haber, S. and Stornetta, W. S. "How to Time-Stamp a Digital Document." *Journal of Cryptology*, Vol. 3, No. 2, 1991, pp. 99-111

/7/ Haber, S., Wakefield, S., and Stornetta Jr., W. S. *Method for Secure Time-Stamping of Digital Documents.* Bell Communications Research Inc., Livingston, N. J. United States Patent number 5,136,647, 1992

/8/ Haber, S., Wakefield, S., and Stornetta Jr., W. S. *Method of extending the validity of a cryptographic certificate.* Bell Communications Research Inc., Livingston, N. J. United States Patent number 5,373,561, 1994

/9/ Al-Riyami, S. and Mitchell, C. J. "Renewing Cryptographic Time Stamps." *Proceedings of the 6th IFIP Communications and Multimedia Security Conference*, Portoroz, Slovenia, September 2002

/10/ Wright, T., "Secure Digital Archiving of High-Value Data." In Temple, R. and Regnault, J. *Internet and Wireless Security.* UK: Btexact TECHNOLOGIES, ISBN 0 85296 197 9, 2002, pp. 133-145

/11/ Maniatis, P., Giuli, T. J., and Baker, M. *Enabling the Long-Term Archival of Signed Documents through Time Stamping*. arXiv:cs.DC/0106058, Department of Computer Science, Stanford University, USA, June 2001

WWW References

/12/ Portal of International Earth Rotation Service. http://hpiers.obspm.fr (Retrieved 23.9.2002)

/13/ English Portal of Bureau International des Poids et Mesures (BIPM). http://www.bipm.org/enus/ (Retrieved 23.9.2002)

/14/ BIPM UTC/TAI Time Server. http://www.bipm.org/enus/5_Scientific/c_time/time_server.html (Retrieved 23.9.2002)

/15/ Portal of Centre for Metrology and Accreditation (MIKES) in Finland. http://www.mikes.fi (Retrieved 24.9.2002)

/16/ Time & Frequency Division of NIST (National Institute of Standards and Technology). http://www.boulder.nist.gov/timefreq/ (Retrieved 30.9.2002)

/17/ Using a Global Positioning System (GPS) receiver as a NIST traceable frequency reference. http://www.boulder.nist.gov/timefreq/service/gpscal.htm (Retrieved 30.9.2002)

/18/ Set Your Computer Clock to NIST Time. http://www.boulder.nist.gov/timefreq/service/time-computer.html (Retrieved 30.9.2002)

/19/ Trusted Time White Paper, trustEra, Inc. July 2002. http://www.trustera.com/sys-tmpl/nss-folder/trustedtimewhitepaper (Retrieved 29.9.2002)

/20/ NTP Service of MIKES. http://www.mikes.fi/frameset.aspx?url=page.aspx%3fcontentID=257 (Retrieved 30.9.2002)

/21/ O. Paridaens: Report on 43rd IETF Meeting December 7th-11th, 1998, Orlando(US). http://www.ejeisa.com/nectar/scimitar/issue12/article007.htm (1.10.2002)

/22/ Trusted Time™Infrastructure. http://www.datum.com/tt/pages/trustedtime/infrastructure.html (retrieved 4.10.2002)

/23/ Deets, D. and Brunette, G. *Using NTP to Control and Synchronize System Clocks – Part II: Basic NTP Administration and Architecture*. July 2001. http://www.sun.com/solutions/blueprints/0701/NTP.pdf (Retrieved 2.10.2002)

/24/ Mills, D. *External Clock Discipline and the Local Clock Driver*. http://www.eecis.udel.edu/~ntp/ntp_spool/html/extern.htm (Retrieved 2.10.2002)

/25/ Mills, D. *NTP Architecture, Protocol and Algorithms*. http://www.eecis.udel.edu/~mills/database/brief/arch/arch.pdf (Retrieved 2.10.2002)

/26/ Mills, D. *Autonomous Authentication*. http://www.eecis.udel.edu/~mills/database/brief/arch/arch.pdf (Retrieved 2.10.2002)

/27/ Secure Network Time Protocol (stime) Charter. http://www.ietf.org/html.charters/stime-charter.html (Retrieved 2.10.2002)

/28/ Adams, C., Cain, P., Pinkas D., and Zuccerato, R. *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*, Request for Comments: 3161, IETF Network Working Group, August 2001, http://www.ietf.org/rfc/rfc3161.txt (Retrieved 16.9.2001)

/29/ VeriSign Authentic Document IDs. Build trust in your online documents. http://www.verisign.com/products/notarize (Retrieved 29.9.2002)

/30/ Trusted Time™ StampServer™. http://www.datum.com/tt/pages/trustedtime/stampserver.html (Retrieved 16.9.2002)

/31/ Signing and Checking Code with Authenticode. http://msdn.microsoft.com/workshop/security/authcode/signing.asp (Retrieved 4.10.2002)

/32/ Digital Time-Stamping. http://www.tcs.hut.fi/~helger/crypto/link/timestamping (Retrieved 10.1.2003)

/33/ FAQs About Authentic Document IDs. http://www.verisign.com/products/notarize/faq.html (Retrieved 4.10.2002)

/34/ Avain Technologies. http://www.avaintec.com (Retrieved 4.10.2002)

/35/ Web Portal of the Finnish Electronic Identity Card. http://www.fineid.fi. (Retrieved 4.10.2002)