

# Aplicaciones forenses del NTP: En busca del tiempo perdido

Juan G. Lalinde-Pulido\*, Carlos E. Urrego-Moreno\*, Juan D. Pineda\* and Santiago Toro\*

\*Departamento de Informática y Sistemas

Universidad EAFIT

Medellín, Colombia

email: {jlalinde, curregom, jpineda2, storooace}@eafit.edu.co

**Resumen**—El NTP es un protocolo de comunicaciones cuya finalidad es sincronizar el reloj de las diferentes máquinas de una red con la hora universal. Actualmente se reconoce la importancia de la sincronización de los relojes en las investigaciones forenses, pues de esta manera se permite la reconstrucción de los hechos. Sin embargo, no siempre los relojes de las máquinas involucradas están sincronizados. En el presente trabajo se propone una técnica basada en el uso NTP para ajustar los tiempos de los logs de máquinas que no están previamente sincronizadas permitiendo reconstruir, al menos parcialmente, la secuencia de ocurrencia de los eventos objeto de la investigación.

## I. INTRODUCCIÓN

El principio fundamental de las ciencias forenses es el principio de intercambio (*exchange principle*), también conocido como el principio Locard en honor del Dr. Edmon Locard quien lo formuló. De hecho, Locard fundó el primer laboratorio forense en 1910 en Lyon [1]. El principio de intercambio dice que cuando dos objetos entran en contacto, ocurre una transferencia de material [2]. En el ciberespacio, debido a su naturaleza intangible, el principio de intercambio no aplica a no ser que los sistemas sean preparados adecuadamente. Para que se puedan aplicar los principios de la computación forense se debe garantizar que el sistema está configurado de tal manera que se cumple el principio de Locard. El principal mecanismo para implementar dicho principio es llevar un registro (bitácora o *log*) de toda la actividad del sistema. Con el fin de facilitar la actividad forense, en el *log* las actividades registradas se acompañan con *estampas de tiempo*. De esa manera se puede organizar una cronología de los eventos.

Es importante que un sistema esté configurado de manera que facilite el análisis forense pues “*La complejidad del entorno demanda que se definan los detalles de tiempo. El fallo de la preservación de los datos, en el sistema víctima o atacante, reducirá la usabilidad que pueda tener la evidencia*” [3]. Para poder establecer una relación de orden entre los eventos en una sola máquina basta con utilizar el reloj local como fuente para generar las *estampas de tiempo*. Sin embargo, cuando se requiere establecer una base de tiempo común para correlacionar la actividad de la máquina con eventos ocurridos en otras máquinas o en el mundo real, es necesario utilizar una base común de tiempos.

El NTP (*Network Time Protocol*), protocolo desarrollado por D. Mills en la Universidad de Delaware y cuya primera versión se definió en el RCF1059 [4], es el estándar adoptado a nivel mundial para sincronizar los relojes de las máquinas con una base común. En sistemas aislados esta base se puede elegir arbitrariamente, pero en los sistemas conectados a internet la base es el estándar UTC [5].

Este trabajo explora el uso del NTP como mecanismo para reestablecer una base de tiempo común en investigaciones de computación forense. Para esto se propone una técnica que permite estimar la hora real de ocurrencia de los eventos registrados aún cuando las máquinas no estaban sincronizadas. Este proceso, aunque no es 100 % preciso, permite tener una buena estimación del orden de ocurrencia de los eventos.

El trabajo se organiza de la siguiente manera: En la sección II presentamos el NTP. La sección III analiza como se debe configurar el NTP para uso forense. La sección IV presenta cómo se puede

aprovechar la información que entrega el NTP para tratar de determinar la hora real de ocurrencia de los eventos en una máquina que no estaba sincronizada y la sección V presenta las conclusiones.

## II. *Network Time Protocol*

El NTP es el protocolo de sincronización de relojes más utilizado en Internet. La última versión oficial se define en [6] y fue desarrollado inicialmente por David Mills. Actualmente está funcionando la versión 4 pero no ha sido estandarizada. Su funcionamiento se basa en conformar un árbol de distribución del tiempo de manera que todas las máquinas puedan tener acceso al tiempo universal. La raíz del árbol es el tiempo universal UTC y las máquinas del primer nivel, conocido como estrato 1, se sincronizan con él utilizando algún mecanismo externo como puede ser un receptor GPS, un reloj atómico calibrado, etc. Las máquinas del siguiente nivel, denominado estrato 2, utilizan como sincronizador (tiempo de referencia) a la máquina de estrato 1 y, en general, las máquinas del estrato  $n$  utilizan como sincronizador a la máquina del estrato  $n - 1$ .

Cada máquina puede tener varios maestros, pero sólo se sincroniza con uno de ellos. Para seleccionarlo, estima para cada uno de ellos cuál es el error máximo en que puede incurrir por utilizarlo como sincronizador y selecciona el menor. El valor estimado se conoce como distancia a la raíz. En el funcionamiento normal, las máquinas se comunican con todos los posibles maestros en cada período de resincronización y seleccionan el reloj que van a tomar como base a partir de los datos obtenidos en las últimas ocho lecturas. El proceso de selección del maestro es realmente un algoritmo que se encarga de construir el árbol tratando de minimizar la distancia a la raíz.

Para estimar el tiempo de cada uno de los maestros, utiliza un filtro de mínima. La idea es simple. Periódicamente envía una solicitud al maestro quien le responde con el valor de su tiempo. Con la información recibida calcula dos valores: un desplazamiento  $o$  y un retardo  $d$ . El desplazamiento es un estimador de la diferencia de fase que tienen los relojes en ese momento y el retardo es un estimador del tiempo que toma la transmisión de los mensajes en la red. Se guardan los últimos ocho pares de valores calculados y se selecciona como estimación del tiempo en el maestro aquel que tenga el menor

desplazamiento. El tiempo en el maestro se obtiene como la suma del tiempo local y el desplazamiento estimado.

Adicionalmente, tiene varios modos de funcionamiento que especifican como se establecen las relaciones entre sincronizador y sincronizado. Lo único que determinan los diferentes modos es quién va a ser la fuente de tiempo y si la relación puede ser simétrica o no.

La principal fortaleza está en la técnica que utiliza para controlar el funcionamiento del reloj lógico de las máquinas. Inicialmente estaba basada en un PLL (*Phase Lock Loop*) y posteriormente se agregó un FLL (*Frequency Lock Loop*) para manejar los casos particulares cuando los períodos de resincronización son muy grandes [7], [8]. Esta técnica garantiza una gran estabilidad del reloj aún cuando se pierda comunicación con la fuente de frecuencia de referencia.

## III. USO DEL NTP PARA CREAR AMBIENTES QUE FACILITEN EL ANÁLISIS FORENSE

En las organizaciones se presenta un escenario en el cual tenemos una serie de máquinas que, incluso siendo homogéneas, requieren un mecanismo de sincronización pues los relojes tienen desviaciones debidas a diferencias físicas (de fabricación) y de entorno. Para esto, es necesario establecer un tiempo de referencia común que les permita periódicamente sincronizar sus relojes y así establecer una base temporal común. El protocolo NTP puede ser utilizado para crear ambientes que facilitan el análisis forense, pues con la configuración adecuada da ventajas tanto administrativas como de seguridad.

Una buena práctica es configurar un servidor NTP interno en la organización, que esté encargado de sincronizar a los usuarios de la misma y además de mantenerse sincronizado con respecto a un servidor de mucha mayor precisión en el caso en que sea deseado.

En este escenario cliente/servidor, es importante identificar explícitamente quién es el servidor, bien sea con nombres DNS o por direcciones IP. Este proceso puede ser realizado automáticamente utilizando el modo *NTP multicast*, u otro esquema basado en DNS conocido como *NTP pool* [9]. También es posible llevar a cabo este proceso de descubrimiento y el de configuración manualmente.

Dependiendo de la cantidad de clientes que se desee tener en la red interna y del nivel de dispo-

nibilidad del servicio de tiempo, es posible utilizar más de un servidor NTP interno. En este caso, los distintos servidores deben estar sincronizados entre ellos para que cada uno de sus respectivos clientes queden sincronizados.

Cada uno de los servidores primarios puede ofrecer tres tipos de sincronización, el primer tipo es aquel en el cual el servidor NTP no se encuentra sincronizado en este tipo de sincronización, todos los clientes de la subred quedan sincronizados entre sí, a pesar de que el tiempo del servidor con el que se sincronizan no es necesariamente el correcto. Desde la perspectiva forense, el principal problema de dicho modo es que carece de una base que permita correlacionar los eventos con el tiempo real de ocurrencia, pero de todas maneras tiene la ventaja de que permite establecer una relación de orden entre ellos.

El segundo tipo de sincronización que puede proveer el servidor NTP, es sincronización externa, basándose en la utilización de un receptor GPS, que es, en si, una fuente de sincronización muy aproximada al tiempo real. Este receptor GPS esta permanentemente recibiendo información de los satélites y la utiliza para calcular la posición y el tiempo. Este tipo de sincronización externa, ofrecida por el servidor, es poco costosa debido a que no se necesitan componentes de altos precios para poder recibir información GPS [10]. Es el tipo de funcionamiento más adecuado para facilitar la actividad forense porque posee una fuente de tiempo que se ajusta al tiempo real y que garantiza alta disponibilidad y precisión.

El tercer tipo de sincronización ofrecida por el servidor NTP, también es una sincronización externa, que se basa en la utilización de un servidor estrato 2, mucho más exacto que los servidores de estratos más bajos ( $n > 2$ ). No se utilizan servidores estrato 1, pues los servidores de este estrato, a pesar de ser los más exactos, tienen cargas muy pesadas que van siempre en incremento [9].

En ambientes seguros se recomienda tener un servidor NTP que sincronice todas las máquinas internas de manera que tengan una hora en común. Así, en caso de ocurrir un siniestro, se puede reconstruir la secuencia exacta de los acontecimientos. Cuando el incidente ocurre en una red que no ha tenido este tipo de sincronización, sea por descuido o por ubicación en distintos husos horarios, se procede a sincronizar los relojes con respecto a un servidor

común y de esta manera se establece una línea de tiempo común calculando los tiempos equivalentes en cada una de las máquinas implicadas.

#### IV. CÓMO DETERMINAR LA HORA REAL DE UN EVENTO EN UNA MÁQUINA NO SINCRONIZADA

Según estudios sobre investigación digital forense realizados en 2007, aproximadamente el 74 % de los relojes de los *hosts* observados estuvieron desfasados en un rango de 10 segundos en comparación con tiempo de UTC [11]. El 26 % restante estaban con rangos de desfase mayores, solo alrededor del 50 % de las máquinas analizadas presentaron desfases inferiores a 1 segundo. Este análisis se realizó a partir de los experimentos realizados en 8149 computadores en un período de 6 meses. Esto pone en evidencia la necesidad de proponer técnicas para determinar la hora real de ocurrencia de los eventos aún cuando los sistemas no estén sincronizados, ya que una diferencia de segundos podría ser significativa en la reconstrucción de los hechos en un análisis forense de un incidente informático.

Uno de los retos más grandes que hay dentro de la investigación por medio de la computación forense, es el ordenar temporalmente los hechos, cuando los tiempos en cada una de las máquinas comprometidas carecen de una base común. En [12] se propone una técnica para compatibilizar las estampas de tiempo de las máquinas ubicadas en husos horarios diferentes siempre y cuando se conozca en detalle el comportamiento del reloj durante el periodo de tiempo de interés. En este trabajo damos un paso adicional al utilizar el NTP para estimar las características de los relojes de manera que aún sin conocer el comportamiento de los relojes durante el periodo de interés, se pueda obtener una aproximación adecuada.

La técnica que se presenta a continuación sirve para establecer el orden de ocurrencia de los eventos independiente de la diferencia que puede existir entre la hora de referencia y la hora del incidente. Para esto se propone un análisis *post-mortem* de los logs ajustando las estampas de tiempo a partir de los parámetros del reloj estimados con NTP y así determinar el orden de ocurrencia de los sucesos. A continuación se describe la metodología para solucionar este problema por medio de algunos métodos que hacen uso de los factores que afectan la sincronización de relojes, como el desfase en el tiempo y la diferencia de frecuencias.

Teniendo en cuenta que en un ataque pueden estar comprometidas muchas máquinas y que se desea reconstruir la secuencia de eventos, se debe establecer un reloj de referencia que sirva como guía a la hora de encontrar la secuencia de los hechos independientemente de que las máquinas involucradas tengan sus relojes sincronizados o no.

Para establecer una línea de tiempo en la cual se ubiquen correctamente cada uno de los acontecimientos durante el incidente es necesario conocer los factores que generan la diferencia entre los distintos relojes. El primer factor es el *desfase*, la diferencia de tiempo entre el reloj local y el de referencia, esta diferencia puede ser positiva o negativa. El segundo factor proviene de diferencias físicas y ambientales y es la deriva (*drift*) de la frecuencia. Ésta hace que el reloj local se atrase o se adelante con respecto al reloj de referencia y se modela como una diferencia de frecuencia de funcionamiento entre ambos relojes.

El protocolo NTP calcula tanto el desfase como la deriva de frecuencia del reloj local con respecto al reloj de referencia y realiza correcciones a la forma como se calcula la hora en la máquina [7]. La técnica propuesta utiliza estos parámetros para obtener una hora común a todas las máquinas implicadas recalculando las estampas de tiempo de todos los logs y de esta manera llegar a una secuencia de eventos consistente. Debe tenerse en cuenta que la relación de eventos es parcial. Esto no es problema porque como lo muestra Lamport en [13], debido a que la granularidad de las unidades de medida del reloj no es suficiente para expresar el tiempo continuo, los retardos en las comunicaciones y la cantidad de procesos que se están ejecutando en la máquina, no hay forma de detectar el orden real de los eventos ocurridos concurrentemente, es decir aquellos eventos cuya diferencia en tiempo es inferior a la mínima unidad de medida disponible. Aunque es claro que la simultaneidad absoluta no puede darse, sí es posible que con las capacidades de medida de los relojes actualmente disponibles dos eventos sean clasificados como simultáneos, motivo por el cual no puede tenerse un ordenamiento total de los eventos ocurridos, y sólo puede usarse uno parcial.

El modelamiento de los relojes se hace a través de líneas rectas donde la abscisa se refiere al tiempo en el reloj local y la ordenada al tiempo en el reloj de referencia, como podemos observar en la figura

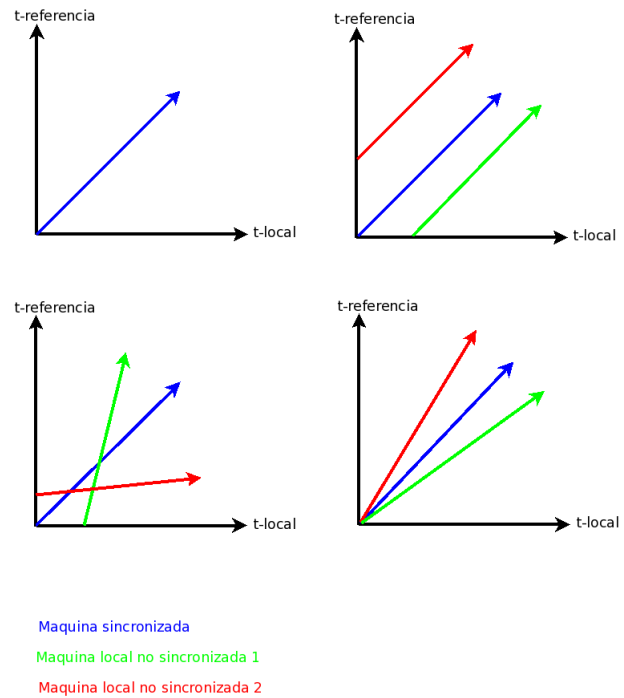


Figura 1. Casos de los relojes

1 un reloj perfectamente sincronizado será una recta  $y = x$  (Línea azul), el tiempo local y el tiempo de referencia son exactamente el mismo. Sin embargo como se ha planteado existirán máquinas que se alejarán tanto de la hora del reloj de referencia como de su frecuencia. Dado esto se pueden presentar los siguientes casos.

- El reloj local está perfectamente sincronizado con el reloj de referencia y por lo tanto el comportamiento se ajusta a la ecuación  $y = x$ .
- El reloj local está desfasado en tiempo con respecto al reloj de referencia pero ambos tienen la misma frecuencia y por lo tanto se ajusta a la ecuación  $y = x + b$ , donde  $b$  es el desfase entre los dos relojes.
- El reloj local está desfasado en tiempo y en frecuencia con respecto al reloj de referencia y se ajusta a la ecuación  $y = mx + b$  con  $b \neq 0$  y  $m \neq 1$
- El reloj local no tenía desfase en el instante inicial pero hay diferencia de frecuencia y por lo tanto se ajusta a la ecuación  $y = mx$  donde  $m \neq 1$

Dado que buscamos dar una equivalencia de los tiempos en cada una de las máquinas a través de NTP hallamos el desfase de tiempo y de frecuencia a partir de las diferencias con el reloj de referencia.

Para realizar esto basta con configurar el cliente de NTP en la máquina, utilizar el comando `ntpdate` para obtener el desplazamiento que es estimado como la corrección instantánea de la hora que hace dicho comando. Para obtener la deriva de la frecuencia, la recomendación oficial [14] es:

1. ejecutar el comando `ntptime -f 0` para garantizar que se comienza a estimar
2. configurar el NTP para que sincronice la hora del servidor local con respecto a la hora de un servidor confiable
3. eliminar el archivo `ntp.drift`<sup>1</sup>
4. ejecutar el `daemon` y esperar por lo menos 15 minutos hasta que el comando `ntpq -c rv` presente `status=4`. La deriva de la frecuencia se obtiene del campo `frequency=` y debe estar del orden de 1ppm.

Dado que el reloj se representa con la recta  $y = mx + b$ , la situación ideal es cuando no hay desfase y por lo tanto  $y = x$ . En este estado ideal del reloj tanto el reloj de la máquina local como el reloj de referencia tienen la misma hora y trabajan a la misma frecuencia. Sin embargo, se parte del hecho de que todas las máquinas comprometidas pueden tener horas y frecuencias diferentes y por lo tanto la recta se ajusta a la ecuación  $y = mx + b$  donde  $b$  es el desfase en la hora cero del reloj de referencia y la pendiente de la recta  $m$  es la frecuencia en la que está trabajando el reloj. Si  $f$  es la deriva de frecuencia calculada con el NTP, entonces  $m \approx 1 + f$ . Para calcular  $b$  se procede de la siguiente manera: sea  $o$  el desplazamiento obtenido con `ntpdate` en el instante  $x = t$ , por lo tanto el valor de  $y$  en el reloj no sincronizado en ese momento es  $y = tm + b$ . Pero adicionalmente,  $y = t + o$  y por lo tanto  $t + o = tm + b$ . De aquí concluimos que  $b = t(1 - m) + o$  y por lo tanto

$$b = t(-f) + o \quad (1)$$

Una vez calculados  $m$  y  $b$  a partir de  $f$  y  $o$ , se normaliza el tiempo de la máquina local con respecto a la hora de referencia, de la siguiente manera: Sea  $t_n$  una estampa de tiempo en el log de la máquina no sincronizada y se desea calcular  $t'_n$  que es la estampa de tiempo corregida. Como en el reloj de referencia  $y = x$  y en el reloj a

corregir  $y = mx + b$ , entonces debemos analizar  $t_n = mt'_n + b$ . En esta expresión todos los valores son conocidos con excepción de  $t'_n$  y por lo tanto

$$t'_n = \frac{t_n - b}{m} = \frac{t_n - t(-f) - o}{1 + f} \quad (2)$$

De esta manera las estampas de tiempo  $t_n$  se pueden corregir utilizando la deriva de la frecuencia  $f$ , el desplazamiento  $o$  y el valor  $t$  del reloj de referencia al hacer la corrección con `ntpdate`.

Finalmente, el resultado no es exacto porque la frecuencia de los relojes no permanece constante. Ésta puede variar y se identifican dos factores. El primero se denomina envejecimiento, actúa a largo plazo y se debe al desgaste del cristal de cuarzo. El segundo se denomina ambiental, actúa a corto plazo y depende de la temperatura y del ruido eléctrico [15]. Sin embargo, estos valores no son significativos especialmente si no ha transcurrido demasiado tiempo entre los eventos y la estimación de los parámetros y las condiciones ambientales son similares.

## V. CONCLUSIONES

La técnica presentada permite reconstruir la secuencia de eventos, al menos de manera aproximada, aún cuando los relojes de las máquinas no estuvieran sincronizados, permitiendo al investigador establecer el orden temporal de los eventos. El único supuesto es el uso de un reloj con oscilador de cuarzo que es la norma en las máquinas actuales. De esta manera se da un paso adicional para permitir a los investigadores forenses, y especialmente a las fuerzas del orden, la investigación de incidentes informáticos en ambientes que originalmente no estaban bajo el control del investigador y no están preparados para este tipo de investigaciones.

## REFERENCIAS

- [1] K. Higgins, "Nist & law enforcement: Technical partnerships for public safety and security," [http://www.eeel.nist.gov/oles/NIST-Law\\_Enforcement\\_Tech\\_Partnerships.pdf](http://www.eeel.nist.gov/oles/NIST-Law_Enforcement_Tech_Partnerships.pdf). [Online]. Available: [http://www.eeel.nist.gov/oles/NIST-Law\\_Enforcement\\_Tech\\_Partnerships.pdf](http://www.eeel.nist.gov/oles/NIST-Law_Enforcement_Tech_Partnerships.pdf)
- [2] S. W. G. o. M. A. S. E. Committee, "Trace evidence recovery guidelines," <http://www.fbi.gov/hq/lab/fsc/backissu/oct1999/trace.htm>, FBI, Oct. 1999. [Online]. Available: <http://www.fbi.gov/hq/lab/fsc/backissu/oct1999/trace.htm>
- [3] J. Tan, "Forensic readiness," @stake, Inc., Tech. Rep., July 2001.

<sup>1</sup>En algunas distribuciones de Linux es el archivo `/var/lib/ntp/drift`

- [4] D. Mills, "Network time protocol (version 1) specification and implementation," <http://www.eecis.udel.edu/~mills/database/rfc/rfc1004.txt>, May 1998. [Online]. Available: <http://www.eecis.udel.edu/~mills/database/rfc/rfc1004.txt>
- [5] U.S. Naval Observatory, "What is universal time?" <http://aa.usno.navy.mil/faq/docs/UT.html>, Oct 2003. [Online]. Available: <http://aa.usno.navy.mil/faq/docs/UT.html>
- [6] D. L. Mills, "Network time protocol (version 3) specification, implementation and analysis," Network Working Group Request for Comments: 1305, March 1992, (Obsoletes RFC 1119, RFC 1059, RFC 958).
- [7] D. Mills, "A kernel model for precision timekeeping," <http://rfc.net/rfc1589.html>, March 1994. [Online]. Available: <http://rfc.net/rfc1589.html>
- [8] "The kernel discipline," <http://www.ntp.org/ntpfaq/NTP-s-algo-kernel.htm>. [Online]. Available: <http://www.ntp.org/ntpfaq/NTP-s-algo-kernel.htm>
- [9] D. L. Mills, *Computer Network Time Synchronization. The Network Time Protocol*, T. F. Group, Ed. Taylor & Francis Group, 2006.
- [10] "Synchronizing ntp servers to the gps system," <http://www.publicwarehouse.co.uk/computertutorials.php?tutorial=247.php>. [Online]. Available: <http://www.publicwarehouse.co.uk/computertutorials.php?tutorial=247.php>
- [11] B. Buchholz, Florian. Tjaden, "A brief study of time," Tech. Rep., 2007. [Online]. Available: <http://www.sciencedirect.com/science/article/B7CW4-4NYJ0W6-2/2/7c1d8a4edafac174a8711b7eef6c5b4c>
- [12] M. Stevens, "Unification of relative time frames for digital forensics," Defence Science and Technology Organisation - Australia [<http://dSPACE.dsto.defence.gov.au/dSPACE-oai/request>] (Australia), Tech. Rep., 2004. [Online]. Available: <http://hdl.handle.net/1947/1917>
- [13] L. Lamport, "Time, clocks, and the ordering of events in a distributed system," *Commun. ACM*, vol. 21, no. 7, pp. 558–565, 1978.
- [14] D. Kabs, "How to calibrate system clock using ntp," <http://support.ntp.org/bin/view/Support/HowToCalibrateSystemClockUsingNTP>, March 2006.
- [15] NIST, *NIST Frequency Measurement and Analysis System: Operator's Manual*. NIST, August 2001, no. NISTIR 6610. [Online]. Available: <http://tf.nist.gov/general/pdf/1469.pdf>