Ein hybrides Zeitstempelsystem

Cristian Marinescu
Fakultät für Automatik und Computer Science
Universität "Politehnica" Bukarest
Splaiul Independenţei 313, Sektor 6, Bukarest, Rumänien
cristian.marinescu@omicron.at

Abstract: Eines der größten Probleme, mit denen digitale Beweisstücke und Dokumente konfrontiert werden, ist das Feststellen der exakten Herstellungszeit. Viele Sicherheitsdienste bauen auf der Fähigkeit auf, die Zeit verschiedener Operationen feststellen zu können. Einfache, verknüpfte und verteilte Schemen sind die heute verbreitetsten Methoden digitale Zeitstempel herzustellen. Sind diese aber dazu geeignet, sichere TSA Lösungen zu gewährleisten? Gibt es andere Ansätze, die Probleme der existierenden Methoden zu bewältigen und eine Software-Architektur zu schaffen, die einen sicheren Zeitstempeldienst zur Verfügung stellt? Folgender *State-of-the-Art*-Bericht setzt sich mit den Problemen der Zeitstempelschemen auseinander, versucht diese kurz zu analysieren und ein hybrides Zeitstempelsystem als neuen Lösungsansatz zu erforschen.
Stichwörter: digitale Signaturen, hybrides Zeitstempelschema, Sicherheit, Zeitstempel, TSA.

1 Zeitstempelschemen und ihre Probleme

Daten im elektronischen Format unterscheiden sich grundsätzlich von den herkömmlichen Papierdokumenten. Es gibt keine Unterschiede zwischen Original und Kopie und die Herstellungszeit kann leider nicht über traditionelle Methoden festgestellt werden. Um die Frage der Herstellungszeit zu beantworten, wurden die digitalen Zeitstempel erfunden. Sie gelten als elektronisches Beweismittel für den Zeitpunkt, an dem gewisse Daten existierten, und stellen eine Verbindung zwischen einem Zeitparameter und einer Darstellung der Daten dar [Me00]. Zeitstempel werden von einer Zeitstempelautorität (*Time-Stamping Authority – TSA*) erstellt, die die Echtheit des Zeitstempels und gegebenfalls des Zeitparameters garantiert.
Die Zeitstempelprotokolle werden in einfache, verknüpfte und verteilte Schemen klassifiziert [Wo04]. Die einfachen Schemen bestehen meistens aus synchronen Protokollen, in denen der Klient nach einem *request-response*-Modell mit dem Server kommuniziert. Das Resultat sind unabhängige Zeitstempel, die man anhand der inkludierten Zeitinformation und Genauigkeit vergleichen kann. Die Dokumente können anhand dieser Zeitinformation auf einer Zeitachse angeordnet werden. Die zentrale Schwäche dieser Architektur ist die Tatsache, dass man der TSA uneingeschränkt vertrauen muss [MŢ05].
Einfache Schemen können die Richtigkeit des Zeitparameters nicht garantieren. Es gibt keine Möglichkeit einen "Betrug" des Servers zu erkennen oder den Zeitparameter zu ve-

rifizieren. Im Falle eines unentdeckten Verlustes des privaten Schlüssels, kann man davon ausgehen, dass die ganze Sicherheit des Schemas kompromittiert wurde. Typische Beispiele für einfache Schemen sind RFC3161 [Ad02] und ISO/IEC 18014-2 [Is02].
Verknüpfte Schemen sind komplizierter als die einfachen Protokolle, dafür ist es aber schwieriger, falsche Zeitstempel zu generieren. Der Server verknüpft alle existierenden Stempel miteinander, sodass eine Verkettung aller Zeitstempel entsteht, die durch die TSA erzeugt wurden. Im Falle des Versuches, einen Stempel nachträglich zu verändern, müsste die Zeitstempelautorität die ganze Stempelverkettung verändern. Diese Methode bringt Vorteile gegenüber den einfachen Schemen, hat aber auch den Nachteil, dass sie viel komplizierter zu implementieren ist. Das Verifizieren der Zeitstempel kann in den meisten Fällen nur mithilfe des Servers gemacht werden. Zeitstempel, die in einem solchen System generiert wurden, können einen Zeitparameter enthalten, müssen aber nicht. Die TSA produziert in diesem Fall eine Zeitlinie durch das Aufreihen der Zeitstempel. Die Sicherheit ist unabhängig vom Schlüssel, mit dem man die Daten signiert, dafür sind aber Zeitstempel, die von unterschiedlichen Servern erzeugt wurden, schwer auf der temporalen Achse anzuordnen [MŢ07a].
Auch die verknüpften Schemen weisen Probleme auf: zwischen zwei Publikationsschritten gibt es die Möglichkeit die Zeitstempel zu fälschen. Obwohl dieses Problem nach dem Publizieren nicht mehr existiert, muss der Klient bis zu diesem Zeitpunkt der TSA voll vertrauen. Ein anderes Problem stellt auch die Überprüfung der Stempel dar, da es schwierig ist, ohne die Hilfe des Servers, die ganzen Zeitstempelverknüpfungen zu überprüfen. Die Operation gestaltet sich als sehr schwierig, da man während der Kontrolle eine Menge Zeitstempel verifizieren muss. Dieses Problem kann man teilweise durch die Einführung von *Merkle* oder binären Bäumen lösen, diese Ansätze haben aber negative Auswirkungen auf die Effizienz und auf die Leichtigkeit, mit der das Schema implementiert wird. [Ju98] präsentiert verschiedene Möglichkeiten des Angriffs auf verknüpfte Schemen wie die von Haber und Stornetta [HS91] und die von Benaloh und de Mare [BM91].
Die verteilten Schemen bestehen aus zwei oder mehreren Servern, die nach dem einfachen oder verknüpften Modell aufgebaut sind und die gemeinsam für das Generieren der Zeitstempel verantwortlich sind [Bo05]. Die Sicherheit wird erhöht, indem das "Geheimnis" (der Schlüssel der verwendet wird, um die Daten zu verschlüsseln), auf die unterschiedlichen Server verteilt wird. Um falsche Zeitstempel zu erzeugen, müssten alle Server an der Fälschung teilnehmen, was das ganze Schema sicherer macht. Trotz der größeren Sicherheit dieses Ansatzes leiden die meisten verteilten Schemen an denselben Problemen wie die einfachen und verknüpften Protokolle, auf denen sie aufbauen [Un01].
Ein großes Problem für die heutigen Zeitstempelschemen stellt die Vergleichsmöglichkeit zwischen den Zeitstempeln unterschiedlicher TSAs dar. Ist diese Vergleichsmöglichkeit nicht gewährleistet, können die Zeitstempel nicht auf der Zeitachse aufgereiht werden. Man hat auch versucht, die Einschränkungen der digitalen Signaturen, und dadurch auch die der *Public Key Infrastructures (PKI)*, mithilfe der digitalen Zeitstempel zu beseitigen [HP01]. Die Probleme sind eindeutig, wenn man den Zertifikatswiderruf oder den Augenblick, an dem eine Signatur entstanden ist, betrachtet. Durch die Einführung der Zeitstempel verändert man aber das Funktionsmodell der PKI. Eigenschaften, die zum Erfolg der PKI beigetragen haben, wie die direkte Kommunikation ohne einen vertrauten Vermittler oder die Möglichkeit ohne Serververbindung (im *offline*-Modus) die Weiterführung

der Prozesse zu gewährleisten, gehen praktisch verloren. Deshalb ist es fraglich, ob Zeitstempel wirklich die perfekte Lösung in diesem Fall darstellen [Ma04]. Zeitstempel sind tatsächlich nicht sehr nützlich, wenn die Sicherheitskriterien nicht erfüllt sind, und sie stellen auch nicht die perfekte Lösung für PKI-Strukturen dar. Sie sind aber im Alltag unabdingbar aufgrund ihrer vielen praktischen Anwendungen [MŢ07b], [PF96], und aufgrund ihrer vom Gesetzgeber verlangten Benutzung.

2 Ein neuer Ansatz: ein hybrides Zeitstempelschema

Die heute existierenden Zeitstempelstandards entfernen sich leider sehr stark von den Eigenschaften, die sie haben sollten. Aus unserer Analyse geht hervor, dass die heutigen Methoden, Zeitstempel zu erzeugen, nicht geeignet sind, sichere Lösungen zu gewährleisten. Man muss aber unterstreichen, dass jede Methode auch ihre Vorteile hat. Das Filtern der Nachteile und die Verknüpfung der Vorteile kann eine neue, hybride Methode hervorbringen, die die Eigenschaften der einfachen, der verknüpften und der verteilten Systeme miteinander vereint. Das hybride Schema, das im Folgenden vorgestellt wird, baut auf diesem Lösungsansatz auf.
Das hybride System besteht aus einer Gruppe von mindestens zwei Servern, die unabhängig voneinander Zeitstempel erzeugen können. Es muss ein *Hash* der Daten verschlüsselt werden und nicht die Daten selbst. Die signierten Daten müssen auch einen zufallsgenerierten Anteil besitzen, um *Hash*-Kollisionen vorzubeugen. Jeder Server muss ein eigenes Zertifikat besitzen, der private Schlüssel dient ausschließlich zum Signieren der Zeitstempel. Das ermöglicht eine einfache Überprüfung der Zeitstempel wie bei den einfachen Schemen. Weiters werden die Informationen aus den Zeitstempeln miteinander verkettet und zwar durch mehrere Methoden:

- durch den inkludierten Zeitparameter (und die damit verbundene Genauigkeit) entsteht eine Zeitachse, auf der die Zeitstempel aufgereiht werden. Die TSA muss sicherstellen, dass jeder Zeitparameter einmalig generiert wird. Diese Eigenschaft wird durch die Anordnung der Anträge beim Server sichergestellt;
- anhand eines eindeutigen Index, der mit jedem Stempel erhöht wird. Der Server muss sicherstellen, dass es keine zwei Zeitstempel gibt, die die gleiche Identifizierungsinformation besitzen;
- durch das gegenseitige Zeitstempeln einer gewissen Anzahl von generierten Stempeln bei einem anderen Server aus derselben Gruppe (Abbildung 1). Diese speziellen Zeitstempel bilden die Gruppe der Kontrollstempel.

Zu den wichtigsten Schritten beim Aufbau des hybriden Zeitstempeldienstes zählt die Definition entsprechender Überprüfungsmethoden, sowohl für die generierten Zeitstempel als auch für das Verhalten der Zeitstempelautorität. Man definiert mehrere Methoden um diese Überprüfungen durchführen zu können, hier nur die wichtigsten:

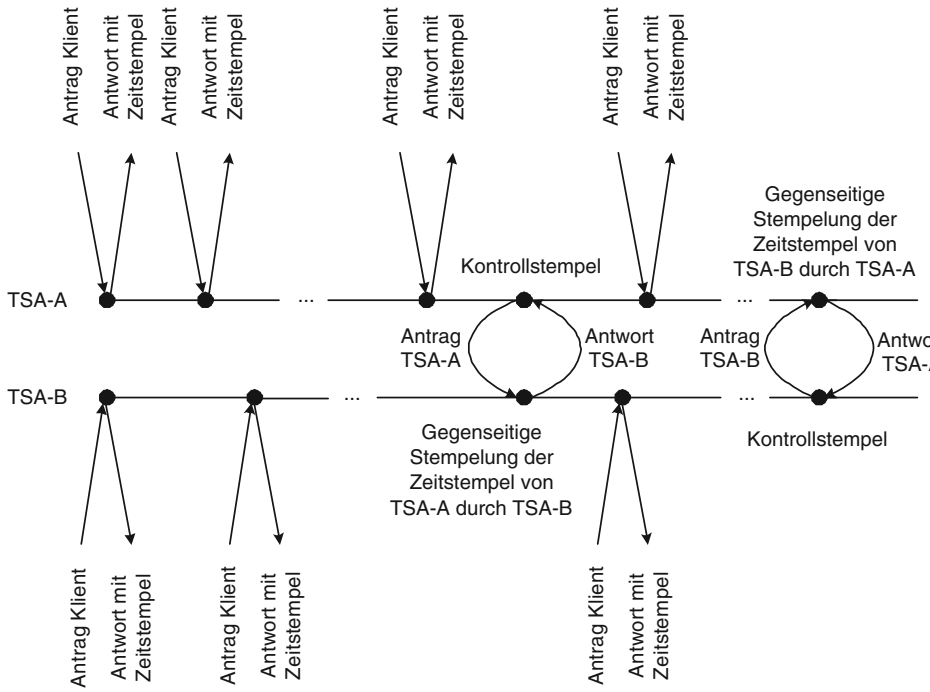

Abbildung 1: Die Erzeugung der Zeitstempel im hybriden Zeitstempelsystem

- eine einfache Methode, bei der nur die Signatur und der Name des Zeitstempelservers überprüft werden;
- eine komplexe Überprüfungsmethode, bei der die dreifach verketteten Informationen der Zeitstempel zwischen zwei Kontrollstempeln überprüft werden. Neben den Signaturen der Zeitstempel werden die drei Verkettungen (Aufreihung der Zeit, der Indizes, und Aufreihung des vom vorhergehenden Stempel inkludierten *Hashs*) überprüft. Die Zeitparameter aller Stempel müssen sich im Zeitintervall, das durch die zwei Kontrollstempel entsteht, befinden;
- eine Methode, die nur die Kontrollstempel einer Zeitstempelautorität überprüft.

Durch die Kombination des zweiten mit dem dritten Überprüfungsverfahren entsteht eine mächtige Methode das Verhalten des Zeitstempelsystems zu kontrollieren. Je nach Anwendung und Sicherheitsanforderung ist es möglich nur die Signatur des gefragten Zeitstempels, eine ganze Reihe verketteter Zeitstempel oder die ganze Serie, die von einer Gruppe von Servern generiert wurde, zu überprüfen.
Alle Uhren der Server, die das hybride Zeitstempelsystem bilden, müssen miteinander synchronisiert werden – mit mindestens derselben Genauigkeit wie die der generierten Zeitstempel. Das hybride System ermöglicht dadurch das Beantragen zweier Zeitstempel

bei zwei unterschiedlichen Servern aus derselben Gruppe: der erste wird als eigentlicher Zeitstempel verwendet, der zweite dient nur zur Kontrolle des Zeitparameters aus dem ersten Stempel und kann hinterher vom Klient verworfen werden. Auf diese Art und Weise hat der Klient die Möglichkeit den Zeitparameter mithilfe eines zweiten Servers zu überprüfen [Ma08].
Das hybride Schema hat folgende Vorteile:

- es ist nicht möglich nachträglich Zeitstempel zu modifizieren, da diese durch ihre digitale Signatur geschützt werden;
- es ist auch nicht möglich Serien von Zeitstempeln zu verändern, da das gegenseitige Zeitstempeln durch TSAs aus derselben Gruppe solche Versuche verhindert;
- der mitgelieferte Zeitparameter kann anhand einer Anfrage (für einen zweiten Zeitstempel) bei einem anderen Server derselben Gruppe überprüft werden – es wird dadurch dem Klient eine einfache Möglichkeit angeboten, die Richtigkeit der mitgelieferten Zeitinformation zu überprüfen;
- es gibt eine einfache, direkte Möglichkeit Zeitstempel zu verifizieren – sowohl beim Antragsteller als auch bei einer *Third Party*;
- das Schema lässt das Erzeugen von falschen Zeitstempeln nicht zu.

3 Schlussfolgerungen

Ohne die vorgestellten Probleme zu lösen, sind Zeitstempeldienste von Sicherheitslücken befallen und werden sich nicht als brauchbare Lösung durchsetzen können. Zeitstempeldienste sind nicht nur eine Möglichkeit, gewisse Probleme der PKI anzugehen, sie sind auch aus juristischen und notariellen Gründen nützlich, sobald sie vom Gesetzgeber verlangt werden und haben generell eine Menge Anwendungen – unter der Voraussetzung, dass die sicherheitsrelevanten Kriterien erfüllt werden.
Das hybride Schema vereint die Eigenschaften der einfachen, verknüpften und verteilten Systeme, in dem Versuch eine generell gültige Lösung für die vorgestellten Probleme der digitalen Zeitstempel zu finden. Die wichtigste Eigenschaft, die das hybride Schema mit sich bringt, ist die dem Klient angebotene Möglichkeit, den Zeitparameter, mit der angegebenen Genauigkeit zu überprüfen. Nur ein solcher Ansatz kann die Voraussetzungen für einen sicheren Zeitstempeldienst erfüllen.

Literatur

[Ad02] Adams, C. et. al.: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), 2002; ftp://ftp.rfc-editor.org/in-notes/rfc3161.txt

[BM91] Benaloh, J.; de-Mare, M.: Efficient Broadcast Time-Stamping, Technical Report TR-MCS-91-1, Clarkson University, Department of Mathematics and Computer Science, 1991.

[Bo05] Bonnecaze, A. et. al.: A Distributed Time Stamping Scheme, Proceedings of the IEEE Conference on Signal and Image Technology and Internet Based Systems, Cameroon, 2005.

[HP01] Housley, R.; Polk, T.: Planning for PKI – Best Practices Guide for Deploying Public Key Infrastructure, John Wiley & Sons, 2001.

[HS91] Haber, S.; Stornetta, W.S.: How to Time-Stamp a Digital Document, Journal of Cryptology, Vol. 3, No. 2, 1991; S. 99-111.

[Is02] ISO/IEC FDIS 18014-2, Information technology. Security techniques. Time-stamping services. Part 2: Mechanisms producing independent tokens, 2002; http://oberon.postech.ac.kr/kiisc-sis/timestamp

[Ju98] Just, M.: Some Timestamping Protocol Failures, Proceedings of the Symposium on Network and Distributed Security (NDSS 98), San Diego, CA, USA, 1998; S. 89-96.

[Ma04] Maurer, U.: New approaches to digital evidence, Proceedings of the IEEE, Volume 92, Issue 6, 2004; S. 933-947.

[Ma08] Marinescu, C.: Semnarea electronică a datelor. Schemă hibrid de realizare a ştampilelor digitale de timp, Teză de doctorat, Facultatea de Automatică şi Calculatoare, Universitatea "Politehnica" Bucureşti, Romania, 2008.

[Me00] Merrill, C.R.: Time is of the Essence: Electronic Documents Will Stand Up in Court Only If the Who, What and When They Represent are Unassailable, CIO Magazine, March 15, 2000, http://www.cio.com/archive/031500_fine.html

[MŢ05] Marinescu, C.; Ţăpuş, N.: Some Critical Aspects of the PKIX TSP, Lecture Notes in Computer Science, Vol. 3677, Conference on Communications and Multimedia Security 2005 (CMS2005), Salzburg, Austria, 2005.

[MŢ07a] Marinescu, C.; Ţăpuş, N.: A Survey of the Problems of Time-Stamping or Why It Is Necessary to Have Another Time-Stamping Scheme, Proceedings of the IASTED International Conference on Software Engineering 2007 (SE2007), Innsbruck, Austria, 2007.

[MŢ07b] Marinescu, C.; Ţăpuş, N.: The Problems of Time-Stamping Revisited, Proceedings of the 16th International Conference on Control Systems and Computer Science (CSCS16), Bucharest, Romania, 2007.

[PF96] Pinto, F.; Freitas, V.: Digital Time-stamping to Support Non Repudation in Electronic Communications, Proceedings of the SECURICOM'96, ed. MCI, CNIT, Paris, France, 1996; p. 397-406.

[Un01] Une, M.: The Security Evaluation of Time Stamping Schemes: The Present Situation and Studies, 2001, http://www.imes.boj.or.jp/english/publication/edps/2001/01-E-18.pdf

[Wo04] Wouters, K.: Time-Stamping: a survey, Seminars on COmputer Security and Industrial Cryptography (COSIC), K. U. Leuven, Department of Electrical Engineering, 2004; http://www.esat.kuleuven.ac.be/cosic/seminars/slides/Time-Stamping.pdf