Umsetzung starker Authentifizierung auf Basis von Passwort-Mechanismen

Heiko Rossnagel[1], Jan Zibuschka[2]

[1]Institut für Arbeitswissenschaft und Technologiemanagement
Univesität Stuttgart
heiko.rossnagel@iao.fhg.de

[2]Lehrstuhl für M-Business und Mehrseitige Sicherheit
Johann Wolfgang Goethe Universität Frankfurt
jan.zibuschka@m-lehrstuhl.de

Abstract: Eines der größten Probleme, mit denen Anwender bei der Verwendung von Authentifizierungssystemen konfrontiert werden, ist die Wahl eines sicheren Passworts. Anwender sind gezwungen, für eine Vielzahl von Diensten Passwörter zu verwenden. Es gibt verschiedene Authentisierungsfaktoren und -mechanismen, die gemeinhin in Bezug auf Sicherheit gegenüber Passwörtern als deutlich überlegen eingeschätzt werden. Die Akzeptanz dieser Systeme bleibt jedoch nach wie vor weit hinter der Stellung von Passwörtern zurück. Solche Systeme erfordern beispielsweise oftmals die Implementierung spezifischer Schnittstellen auf der Service-Seite. Dieser Beitrag präsentiert eine Lösung, die eine starke, bereits ausgerollte Authentifizierungsinfrastruktur, signaturfähige Smartcards, mit Passwort-basierten Authentisierungsmechanismen integriert. Sie kann dem Benutzer Single Sign On-Funktionalitäten bieten, ohne die Implementierung spezieller Schnittstellen durch die Diensteanbieter zu erfordern.

1 Einleitung

Eines der größten Probleme, mit denen Anwender bei der Verwendung von Authentifizierungssystemen konfrontiert werden, ist die Wahl sicherer Passwörter für die diversen Dienste, bei welchen Benutzer sich heute im Internet anmelden. Jedoch fällt es Benutzern sehr schwer, sich zahlreiche zufällig ausgewählte und voneinander unabhängige Passwörter zu merken, insbesondere, wenn solche Passwörter nur selten verwendet werden [ASL1997]. Daher neigen die Benutzer dazu, entweder schwache Passwörter zu verwenden [CM2006], wodurch das Authentifizierungssystem gegenüber dienstübergreifenden Attacken verwundbar wird [IWS2004]. Die Einführung einer neuen Authentifizierungsinfrastruktur ist jedoch mit einem teilweise erheblichen Aufwand und dadurch entstehenden Kosten verbunden. Auch ist nicht klar, ob ein von einem Diensteanbieter implementierter neuer Authentisierungsmechanismus von den Nutzern akzeptiert würde. Dies erstreckt sich sowohl auf die Einführung, als auch auf die Bedienung des Systems. Weiterhin kann es für den einzelnen Dienstanbieter unattraktiv sein, sich ausschließlich für ein bestimmtes Authentifizierungssystem zu entscheiden.

Die Angst vor Lock-In-Effekten gegenüber dem Anbieter des Authentifizierungssystems oder vor Fehlinvestitionen können eine erhebliche Rolle spielen [Wei2003]. Auch ein Gesamtinteresse an einem sicheren elektronischen Marktplatz wird durch Netzwerkexternalitäten nicht zu einer passenden Motivation. Jedoch legt die Betrachtung der Netzwerkeffekte Kompatibilität bzw. Interoperabilität als wichtigen Aspekt für den Gesamtwert des Netzes nahe [Eco1996]. Dieser Beitrag präsentiert eine Lösung, die eine starke, auf Nutzerseite bereits ausgerollte Authentifizierungsinfrastruktur – signaturfähige Smartcards – mit den auf Serviceseite weit verbreiteten Passwort-basierten Authentisierungsmechanismen integriert. Dadurch kann dem Benutzer eine relativ sichere Single Sign On-Funktionalität geboten werden, ohne dass eine Implementierung spezieller Schnittstellen durch die Diensteanbieter erforderlich wird.

2 Anforderungen

Neben der Möglichkeit, Passwörter verschlüsselt zu speichern, ist es auch möglich, Passwörter mit Hilfe kryptographischer Verfahren dynamisch zu generieren, wenn dies nötig wird. Solche Methoden sollten aber verschiedene Anforderungen erfüllen, um dem Nutzer und Diensteanbieter einen Nutzen zu ermöglichen [GGM+1997][RZ2006] [ZR2007].

- **Interoperabilität:** Durch die Integration bereits ausgerollter Authentifizierungsinfrastrukturenwerden Kosten gesenkt, außerdem können Komplementäreffekte realisiert werden [Eco1996].
- **Sicherheit der generierten Passwörter:** Sicherstellung eines geeigneten Entropiegehalts der generierten Passwörter, etwa über Länge, Alphabet und Verteilung.
- **Minimale Insider-Angriffe:** Weder sollte Vertrauen zu einem Dritten nötig sein, noch sollte das System gegen Angriffe anfällig sein, bei dem ein Administrator oder Hacker die mehrfache Verwendung desselben Passworts ausnutzt.
- **Beachtung der Passwortrichtlinien:** Generierte Passwörter müssen von den Diensteanbietern akzeptiert werden, und daher deren Richtlinien für akzeptable Nutzerpasswörter berücksichtigen.
- **Konsistenz:** Jeweilige Generierung eines deterministisch immer identischen Passworts bei jeder Nutzung eines bestimmten Diensts.
- **Mobilität:** Eine Anmeldung an einem Dienst sollte von überall und von jedem Gerät aus möglich sein, wie dies auch bei Passwörtern üblich ist.
- **Einfache Benutzbarkeit:** Eine niedrige wahrgenommene Benutzbarkeit wäre ein Hindernis für den Erfolg des Systems bei Benutzern [Dav1989].
- **Einzelnes Geheimnis:** Die Verwendung verschiedener Tokens, z.B. für verschiedene Dienste, sollte nicht ausgeschlossen, darf aber nicht Voraussetzung sein.
- **Minimale Server-Infrastruktur:** Minimiert Kosten für den Provider, Lock-In des Benutzers und Anfälligkeit des Systems

3 Implementierung

Um die Machbarkeit einer Passworterzeugung auf Basis bereits existierender Signatursysteme zu zeigen, wurde ein Prototyp in Java entwickelt, der einfache Portierungen auf unterschiedliche Plattformen (wie beispielsweise mobile Endgeräte) ermöglichen soll. Es wurde eine modulare Architektur implementiert, deren Grundstruktur das Hinzufügen neuer Smartcard APIs oder anderer Authentisierungs-Faktoren erleichtert. Der eigentliche Encoder bleibt dadurch schlank und portabel. Die grundsätzliche Idee des Algorithmus kann in vier Schritten zusammengefasst werden:

1. Definition einer Vorgehensweise, um Diensteidentifikatoren für unterschiedliche Diensteanbieter, gegenüber denen sich der Nutzer authentifizieren möchte, zu ermitteln. Dies kann dadurch erreicht werden, dass mehrere Attribute des Dienstes, wie beispielsweise Name des Dienstes, URL oder Benutzername, aneinandergehängt werden.
2. Kombination des Diensteidentifikators mit dem zentralen Authentifizierungsgeheimnis des Benutzers unter Verwendung starker kryptographischer Verfahren [ABM1997] [GGM+1997].
3. Transformation der resultierenden Daten in pseudozufällige Benutzerpasswörter.
4. Übertragung des Passworts in den entsprechenden Login-Dialog des Dienstes, z.B. ein Browser Plug-In [HWF2005] [RJM+2005].

Mehrere kryptographische Verfahren oder Kombinationen dieser [GGM+1997] sind für den 2. Schritt denkbar und möglich. Dieser Beitrag fokussiert sich auf Signaturen, aber sowohl Hash-Funktionen [ABM1997] und MACs [Fra2006] als auch verschiedene Verschlüsselungen können für diesen Schritt eingesetzt werden. Signaturen erscheinen aber im Kontext der bestehenden E-Government-Initiativen am relevantesten, und zumindest Hash-Funktionen sind für den Einsatz mit Smartcards suboptimal, da kein geheimer Schlüssel existiert und auf dem Token hinterlegt werden kann. Digitale Signaturen haben dagegen die Sicherheitseigenschaft der Unfälschbarkeit. Dies bedeutet, dass ein Angreifer nicht in der Lage ist, einen beliebigen Text mit der Signatur des Benutzers zu versehen, sofern er nicht im Besitz des geheimen Schlüssels des Benutzers ist. Dies gilt auch dann noch, wenn der Angreifer im Besitz des öffentlichen Schlüssels des Benutzers sowie mehrerer signierter Nachrichten ist. Ein wichtiger Schritt, der die explizite Beachtung von Passwortrichtlinien erst ermöglicht, ist dabei die komplexe Armierung digitaler Signaturdaten zu Passwörtern. Da es sich bei Signaturen um Pseudozufallswerte handelt, kann es bei Verwendung verbreiteter Verfahren wie Base64 mit hoher Frequenz zur Ablehnung des erzeugten Passworts durch den Service kommen [RJM+2005].

Allerdings liegen die Passwortrichtlinien üblicherweise nicht in von Dritten verarbeitbarer Form vor. Der Benutzer kann sie bei jedem Log-In von Hand konfigurieren, dies ist jedoch sehr aufwendig und fehleranfällig. Um die Benutzerinteraktion zu minimieren, gehen wir davon aus, dass Richtlinieninformationen auf einem Server hinterlegt sind. Ein detailliertes Beispiel findet sich in [Fra2006]. In [HWF2005] wird ein ähnlicher Ansatz vorgeschlagen, der jedoch nicht die Präsenz einer gegebenen Zeichenklasse garantieren kann, und eine signifikant größere Parametermenge verwendet.

4 Diskussion

Im Gegensatz zu herkömmlichen Vorgehensweisen beim Einsatz von Signaturen zur Authentifizierung setzt das System nicht auf Transaktionsebene an. Dies ist eine Folge des einfachen Aufbaus der üblichen Passwortmechanismen, die keine Authentifizierung pro Transaktion anbieten. Dementsprechend kann natürlich auch kein Challenge-Response realisiert werden, wenn man auf Passwortschnittstellen aufsetzen will. Dennoch konstatieren wir ein erheblich höhere Sicherheit und Portabilität, als dies heutige Passwortsysteme bieten können, bei sofortiger Kompatibilität mit einer hohen Zahl von Diensten. Im Gegensatz zu Smartcard-Lösungen, die verschlüsselte Passwörter auf dem Token speichern, kann die vorgestellte Lösung auf Basis einer bereits eingesetzten und verbreiteten Signaturkarteninfrastruktur eingesetzt werden, was die Kosten gegenüber herkömmlichen Token-Systemen deutlich reduziert und die Anzahl der vom Benutzer verwendeten Tokens nicht erhöht. Mithilfe eines Dienstes für die Verwaltung von Meta-Informationen, wie in [Fra2006] beschrieben, lässt sich die Benutzbarkeit noch mal deutlich verbessern. Wie in [ABM1997] und [GGM+1997] gezeigt, könnten auch unverkettbare Benutzerpseudonyme auf ähnliche Weise erzeugt werden, was besonders bei anonymer Kommunikation nützlich ist. Die Mobilität des Systems, und die Eigenschaft, dass es auf gespeicherte Passwörter verzichtet, machen es auch für einen Einsatz auf mobilen Endgeräten attraktiv. Nichtdeterministische Signaturalgorithmen benötigen weitere Anpassungen, da in Passwortauthentifizierungssystemen deterministisch stets dasselbe Passwort wieder verwendet wird. Dies sollte aber in der Praxis kein Hindernis darstellen, da die meisten verbreiteten Signaturerstellungseinheiten deterministische Signaturen wie RSA verwenden [ZR2007].

5 Zusammenfassung

Es wurde eine Methode zur sicheren Generierung von Passwörtern mittels digitaler Signaturen vorgestellt. Die Architektur könnte etwa mit eIDs [DWP2004] [Hva2004] im Rahmen von E-Government-Maßnahmen breiten Nutzergruppen zugänglich werden. Da der Benutzer diese Lösung für sein Passwortmanagement nutzen kann, schätzen wir die wahrgenommene Nützlichkeit [Dav1989] als recht hoch ein. Durch eine regelmäßige Nutzung dieses Verfahrens stiege auch die Vertrautheit der Nutzer mit der Signaturerstellungseinheit, was zu einer höheren Akzeptanz für elektronische Signaturen in der Bevölkerung führen könnte. Daher bietet sich eine solche Anwendung als eine flankierende Maßnahme für die Einführung von elektronischen Signaturen an [RZ2006] [Roß2007].

Literaturverzeichnis

[ABM1997] Abadi, M., Bharat, K. und Marais, J. (1997) System and method for generating unique passwords, United States Patent #6141760.
[ASL1997] Adams, A., Sasse, M. A. und Lunt, P. (1997) Making Passwords Secure and Usable, *Proceedings of HCI on People and Computers XII*, August, Bristol, Springer, 1-19.

[CM2006] Cazier, J. A. und Medlin, B. D. (2006) How Secure is Your Password?, *Journal of Information System Security*, 2, 3, 69-82.
[Dav1989] Davis, F. D. (1989) Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology, *MIS Quaterly*, 13, 3, 319-340.
[DWP2004] De Cock, D., Wouters, K. und Preneel, B. (2004) Introduction to the Belgian EID Card, in S. K. Katsikas, S. Gritzalis und J. Lopez (Hrsg.), *Public Key Infrastructures*, Springer, Berlin Heidelberg, 1-13.
[Eco1996] Economides, N. (1996) The Economics of networks, *International Journal of Industrial Organization*, 14, 673-699.
[Fra2006] Frauenhofer SIT (2006) Der PasswordSitter: Whitepaper.
[GGM+1997] Gabber, E., Gibbons, P., Matias, Y. und Mayer, A. (1997) How to Make Personalized Web Browsing Simple, Secure and Anonymous, *Proceedings of the First International Conference on Financial Cryptography*, Anguilla, British West Indies, Springer, 17-32.
[Hva2004] Hvarre, J. (2004) Electronic signatures in Denmark: free for all citizens, *e-Signature Law Journal*, 1, 1, 12-17.
[HWF2005] Halderman, J. A., Waters, B. und Felten, E. W. (2005) A convenient method for securely managing passwords, *WWW '05: Proceedings of the 14th international conference on World Wide Web*, Mai, Chiba, Japan, ACM Press, 471-479.
[IWS2004] Ives, B., Walsh, K. und Schneider, H. (2004) The Domino Effect of Password Reuse, *Communications of the ACM*, 47, 4, 75-78.
[RJM+2005] Ross, B., Jackson, C., Miyake, N., Boneh, D. und Mitchell, J. C. (2005) Stronger Password Authentication Using Browser Extensions, *Proceedings of the 14th USENIX Security Symposium*, 31.Juli-5.August, Baltimore, Maryland.
[Roß2007] Roßnagel, H. (2007) Mobile Qualifizierte Elektronische Signaturen: Analyse der Hemmnisfaktoren und Gestaltungsvorschläge zur Einführung, unpublished doctoral dissertation, Department of Business Administration and Economics, Johann Wolfgang Goethe University, Frankfurt am Main.
[RZ2006] Roßnagel, H. und Zibuschka, J. (2006) Single Sign On mit Signaturen: Integration von qualifizierten Signaturen und Passwortsystemen, *Datenschutz und Datensicherheit (DuD)*, 30, 12, 773-777.
[RZ2007] Roßnagel, H. und Zibuschka, J. (2007) Integrating Qualified Electronic Signatures with Password Legacy Systems, *Digital Evidence Journal*, 4, 1, 5-11.
[Wei2003] Weitzel, T. (2003) A Network ROI, Proceedings of the MISQ Academic Workshop on ICT standardization, ICIS 2003, Seattle WA, USA, AIS.
[ZR2007] Zibuschka, J. und Roßnagel, H. (2007) Implementing Strong Authentication Infrastructure Interoperability with Legacy Systems, Proceedings of the IFIP Conference on Policies & Research in Identity Management (IDMAN), Rotterdam, Springer.