

Warum ich keine „digitale Signatur“ will

Benedikt Stockebrand

GUUG UpTimes, Mai 2005

In den letzten Monaten ist viel darüber diskutiert worden, warum digitale Signaturen solche Akzeptanzprobleme haben. Die Diskussionen drehen sich meistens darum, wer welche Vorteile von der Verwendung digitaler Signaturen hat und wer auf der anderen Seite die Kosten trägt.

Die Frage nach der Sicherheit digitaler Signaturen wird dagegen in einigen wichtigen Punkten systematisch vernachlässigt: Zwar werden die benutzten Algorithmen und die Sicherheit von Karten und Kartenlesern genauso diskutiert wie die rechtliche Verbindlichkeit von Signaturen, aber ein viel entscheidenderer Aspekt bleibt aussen vor: die Frage, welche Nachteile und Risiken mir als potentielltem Signatur-Benutzer zugemutet werden.

Denn es wird jedem Benutzer einiges zugemutet: Die digitale Signatur ist rechtlich im wesentlichen mit der handschriftlichen Unterschrift gleichgestellt. Bei einem Missbrauch des Signaturschlüssels trägt der Eigentümer des Schlüssels die Beweislast, weil §17 Signaturgesetz (SigG) [1] axiomatisch die Sicherheit der verwendeten Verfahren impliziert. Wenn eine digitale Signatur in der Praxis die gleiche rechtliche Bedeutung wie eine Unterschrift haben soll, ist dieser Anspruch auch zwingend nötig.

Im gleichen Paragraphen wird aber auch mein grosses Problem mit digitalen Signaturen deutlich:

(1) Für die Speicherung von Signaturschlüsseln sowie für die Erzeugung qualifizierter elektronischer Signaturen sind sichere Signaturerstellungseinheiten einzusetzen, die Fälschungen der Signaturen und Verfälschungen signierter Daten zuverlässig erkennbar machen und gegen unberechtigte Nutzung der Signaturschlüssel schützen. [...]

(2) [...] Die Signaturschlüssel-Inhaber sollen solche Signaturanwendungskomponenten einsetzen oder andere geeignete Maßnahmen zur Sicherheit qualifizierter elektronischer Signaturen treffen.

Was heisst das für mich? Wenn ich einen Signaturschlüssel habe und einem Rechner anvertraue, dann bin ich dafür verantwortlich, dass dieser Rechner sicher ist.

In einem nach meiner Erfahrung normalen Unternehmensumfeld gibt es einen (Windows-)Arbeitsplatzrechner, der von professionellen Systemadministratoren betreut wird. Sobald ich also eine SmartCard mit meinem Schlüssel in den Kartenleser eines solchen Rechners stecke und mit einer PIN oder ähnlichem freischalte, erteile ich implizit allen diesen Administratoren eine Blankounterschrift und hoffe, dass kein Administrator sie eigenmächtig benutzt.

Das setzt voraus, dass die Administratoren saubere Arbeit geleistet haben und der Rechner sicher ist. Nachdem mindestens ein namhafter Antiviren-Hersteller inzwischen dazu übergegangen ist, stündlich Updates seiner Viren-Signaturen bereitzustellen [2], ist das Zeitfenster, in dem ein Bürorechner vor einem neuen Virus ungeschützt ist, offensichtlich genau wie das damit verbundene „Restrisiko“ für einen Windows-Benutzer alles andere als „vernachlässigbar klein“.

Noch schlimmer sieht es mit dem heimatlichen Windows-Rechner des „durchschnittlichen Privat-Users“ aus; mehrere hundert Mails täglich dokumentieren alleine in meiner Inbox, dass eine ernstzunehmende Zahl von Usern es nicht schafft, den eigenen Rechner zu schützen.

Und auch Unix löst das Problem nicht. Selbst wenn alle Windows-Rechner

dieser Welt mit Linux neu installiert würden, wäre die Situation nicht besser. Nicht nur, dass Linux wie jedes andere Unix seine gelegentlichen Sicherheitslücken hat; der grossflächige Einsatz von Linux würde ihm die gleiche „Aufmerksamkeit“ zukommen lassen, wie Windows heute von organisierten Kriminellen erfährt, während die durchschnittliche Kompetenz der Benutzer exponentiell fallen würde.

Dass diese organisierten Kriminellen ernstzunehmen sind, zeigt nicht nur die ständig zunehmende Spam-Flut, sondern auch die immer ausgefeilteren Phishing-Angriffe, die zum guten Teil auch für Profis nicht auf Anhieb zu erkennen sind. Wer Sebastian Gajeks Vortrag [3] beim Frühjahrsfachgespräch gehört hat, wird die Machbarkeit solcher Angriffe wohl kaum in Frage stellen. Und ein Blick in das Archiv des Heise-Newstickers zeigt schnell, dass es einerseits genug kriminelle Energie gibt [4, 5], um Sicherheitslücken und die Unwissenheit der Nutzer im grossen Stil auszunutzen, und andererseits auch namhafte Online-Angebote gelegentlich wenig Rücksicht auf die Sicherheit der Rechner ihrer Kunden nehmen [6, 7].

In dem Mass, wie sich digitale Signaturen etablieren, werden sie zur lukrativen Zielscheibe solcher Kriminellen.

Damit steckt die digitale Signatur in einem Dilemma: Erhebt sie, wie bisher im Signaturgesetz verlangt, den Anspruch auf rechtliche Verbindlichkeit, wird sie für jeden Benutzer zu einem langfristig unkalkulierbaren Risiko. Wird ihre rechtliche Verbindlichkeit aber auf ein Niveau herabgesetzt, das der Sicherheit heutiger Rechner angemessen ist, wird sie nutzlos.

Diesem Dilemma kann sie sich nicht entziehen. Auch der Versuch,

mit „qualifizierten Signaturen“, das heisst mit zweckgebundenen Signaturschlüsseln, den möglichen Schaden zu begrenzen, ist wohl kaum angemessen: Solche zweckgebundenen Schlüssel werden wohl nur für ausreichend wichtige, und damit riskante, Zwecke ausgestellt und eingesetzt. Damit sind sie aber trotz ihrer Einschränkung ein lohnenswertes Angriffsziel; möglicherweise werden sie gerade durch diese Einschränkung einfach als lohnenswertes Ziel identifizierbar.

Schliesslich bleibt noch das Argument, dass eine handschriftliche Unterschrift ja auch kaum fälschungssicher ist. Das stimmt, aber erstens ist auch dem letzten Provinzrichter vermutlich bekannt, dass sich Unterschriften fälschen lassen, zweitens gibt es eine Reihe altbewährter Mittel, um gefälschte Unterschriften in vielen Fällen zu erkennen und drittens muss ich mich bei einer Unterschrift zwar auf einen Kugelschreiber verlassen, aber nicht auf einen Rechner, dessen Integrität ich

blind voraussetzen muss.

Auch wenn sich die Argumentation vieler Laien zu dem Thema auf ein fachlich wenig fundiertes „ich traue dem Rechner nicht, ich mache das lieber mit der Hand“ beschränkt, ist diese Sichtweise am Ende völlig korrekt. Mit allem Wissen um Rechner, Kryptographie und die rechtlichen Rolle digitaler Signaturen kann ich zu keinem anderen Ergebnis kommen. Und deshalb werde ich mich so lange es geht dagegen wehren, dass mir eine digitale Signatur aufgezwungen wird.

Aber etwas Gutes hat diese Entwicklung vielleicht doch: Wenn die ersten spektakulären Prozesse wegen gestohlenen Signaturschlüsseln durch die Presse gehen, dann werden vielleicht, ganz vielleicht, die Software-Hersteller zu einem angemessenen Umgang mit Sicherheitsproblemen gezwungen werden, wenn sie Marktanteile behalten und Schadensersatzforderungen vermeiden wollen. Man soll ja versuchen, in allem das Gute zu sehen...

Literatur

- [1] http://bundesrecht.juris.de/bundesrecht/sigg_2001/gesamt.pdf
- [2] <http://www.kaspersky.com/de/avupdates>
- [3] Sebastian Gajek, „Eine Neue Generation von Angriffen gegen SSL/TLS-geschützte Webapplikationen“, GUUG Frühjahrsfachgespräch 2005 Proceedings, pp. 147–158.
- [4] <http://www.heise.de/newsticker/search.shtml?T=phishing>
- [5] <http://www.heise.de/newsticker/meldung/57762>
- [6] <http://www.heise.de/newsticker/meldung/50334/>
- [7] <http://www.heise.de/newsticker/meldung/57759/>