Hans-Joachim Knobloch

Formale Sicherheitsanalyse von Online-Banking-Protokollen

Für die Verifikation kryptographischer Protokolle hat sich die von Burrows, Abadi und Needham 1989 entwickelte BAN-Logik bewährt [1]. Der Beitrag unterzieht die Online-Banking-Protokolle mit iTAN und Token einer solchen semi-formalen Analyse mit BAN-Logik – und kommt zu interessanten Ergebnissen.

1 Modell zur Sicherheitsanalyse

In einem abstrahierten Modell zur semiformalen Analyse von Sicherheit und Bedrohungen beim Online-Banking sind die folgenden mit unterschiedlicher Motivation handelnden Parteien zu betrachten:

- Alice (die Kundin) will Bob (der Bank) eine unverfälschte Nachricht (den Transaktionsauftrag) schicken.
- Bob (die Bank) will zwischen Nachrichten von Alice (der Kundin) und Paul (dem Angreifer) unterscheiden.
- Paul (der Angreifer, z. B. per Phishing) will Bob eine Nachricht im Namen von Alice schicken oder – äquivalent dazu – eine Nachricht von Alice gezielt verfälschen.

Hinsichtlich der Kommunikation gilt nach den obigen Grundüberlegungen:

- Paul kann unter beliebigem Namen mit Alice und Bob kommunizieren
- Alice und Bob können nur unter Einfluss von Paul kommunizieren

Während Bob über ein vertrauenswürdiges Gerät (nämlich die bankseitigen Server-Systeme) verfügt, das mit hoher Bandbreite kommunizieren kann und in der Lage ist, Schlüssel vertraulich zu speichern, sind die Fähigkeiten von Alice relativ eingeschränkt:

Hans-Joachim Knobloch

Security Consultant bei der Secorvo Security Consulting GmbH

E-Mail: hans-joachim.knobloch@secorvo.de

- Alice verfügt über ein vertrauenswürdiges Gerät (z. B. ein Handheld-Device mit Chipkarte), das zwar in der Lage ist, Schlüssel sicher zu speichern, aber von der Kommunikationsbandbreite her nicht ohne weiteres in der Lage ist, die gesamte Nachricht zu empfangen oder zu übermitteln (manuelle Tasteneingabe und Ablesen vom Display).
- Die Kommunikation mit Alice muss über ein nicht vertrauenswürdiges Gerät (den PC) vermittelt werden.

Dem Angreifer Paul müssen weitreichende Fähigkeiten unterstellt werden:

- Paul kann die Kommunikation zwischen Alice und Bob manipulieren (als „Man-in-the-middle", z. B. über einen Phishing-Server).
- Paul kann das nicht vertrauenswürdige Gerät von Alice (den PC) manipulieren (z. B. durch ein Trojanisches Pferd).
- Paul kann die Kommunikation zwischen den Geräten von Alice manipulieren (z. B. im Fall, dass die Chipkarte in einen an den PC angeschlossenen Kartenleser eingelegt ist).
- Paul kann Alice (z. B. durch Phishing und ähnliche Maßnahmen) zu nahezu beliebigen Handlungen veranlassen, d. h. den von Alice befolgten Algorithmus bzw. Protokollablauf manipulieren.

Bei einer weiten Interpretation der letztgenannten Angreiferfähigkeit könnte Paul Alice dazu veranlassen, eine von ihm gewünschte Nachricht in ihrem Namen an Bob zu schicken (z. B. eine vom Phisher vorgegebene Überweisung selbst vorzunehmen). Dies ist in der Praxis zwar nicht ausgeschlossen, entspricht jedoch einem Trickbetrug, gegen den ein technischer Schutz grundsätzlich nicht möglich ist.

Für die weitere Betrachtung möglicher technischer Schutzmaßnahmen sind daher sinnvolle Einschränkungen zu treffen, zu welchen Handlungen Paul Alice veranlassen kann.

Plausibel erscheinen zunächst die folgenden Einschränkungen:

- Paul kann Alice nicht dazu veranlassen, geheime Schlüssel preis zu geben (da diese z. B. in der Chipkarte gespeichert sind).
- Paul ist ein Programm, das zur Laufzeit des Protokolls nach einem vorgegeben Algorithmus agieren muss.

2 Analyse mittels BAN-Logik

Um die realistischen Angriffsszenarien zu systematisieren und die Wirksamkeit der gewählten Schutzmechanismen bewerten zu können, wurden zwei Online-Banking-Protokolle einer Analyse mit der von Burrows, Abadi und Needham entwickelten BAN-Logik [1, 2, 3] zur (semi-) formalen Analyse von kryptographischen Authentifikationsprotokollen unterzogen.

Die BAN-Logik wurde bereits mit leichten Erweiterungen zur Analyse des Bezahlverfahrens für eine Smartcard-basierte Geldbörse angewandt [4].

Die Grundelemente der BAN-Logik sind die folgenden Ausdrücke (1) bis (8), wobei *A*, *B*, *C* handelnde Parteien des zu untersuchenden Protokolls, *K, L* kryptographische Schlüssel und *X*, *Y* Protokollnachrichten (ggf. auch Schlüssel) oder Aussagen bzw. Ausdrücke über Protokollnachrichten bezeichnen:

(1) $A \mid\equiv X$

A glaubt *X* ist gültig (jenseits berechtigter Zweifel, ob evtl. eine Täuschung vorliegt).

(2) $A \mid\sim X$

A sagte einmal *X* (diese Aussage oder Nachricht könnte aber z. B. aus einem früheren Protokollablauf stammen oder per Phishing provoziert sein).

(3) $A \mid\Rightarrow X$

A ist zuständig für *X* (d. h. *A* ist kompetent, vertrauenswürdige Aussagen zu *X* zu treffen).

(4) $A \triangleleft X$

A sieht *X*.

(5) $\#X$

X ist frisch (d. h. *X* enthält z. B. einen aktuellen Zeitstempel oder eine Information, die vor dem aktuellen Protokollablauf noch nie verwendet wurde, eine sogenannte „Nonce").

(6) $\{X\}_K$

X ist verschlüsselt mit *K*.

(7) $A \overset{K}{\leftrightarrow} B$

A und *B* teilen den geheimen Schlüssel *K* miteinander (und darüber hinaus allenfalls noch mit absolut vertrauenswürdigen Dritten); u. U. wird dieser für A und B vorgesehene Schlüssel erst im Verlauf des Protokolls generiert – d. h. in der Sprechweise der BAN-Logik von einer Partei, die dafür zuständig ist, gesagt – und verteilt.

(8) (X, Y)

X konkateniert mit *Y* (sofern aufgrund des umgebenden Ausdrucks die Klammerung klar ist, können die Klammern auch entfallen, z. B. bei $\{X, Y\}_K$).

Zur Analyse von Online-Banking-Protokollen mit TAN müssen wir noch einen weiteren Ausdruck ergänzen:

(9) $\langle X \rangle_K$

X ist integritätsgeschützt mit *K* (also per MAC-Prüfsumme o.ä. gesichert, aber nicht verschlüsselt; dieser Ausdruck kann im wesentlichen wie $\{X\}_K$ verwendet werden, schützt aber z. B. eine Nonce nicht gegen die Verwendung durch Dritte im laufenden Protokollablauf).

Um ein kryptographisches Protokoll in der Sprache der BAN-Logik idealisiert darzustellen, wird folgende Notation für die einzelnen Protokollschritte verwendet:

(10) $A \rightarrow B : X$

A sendet *X* an *B*. Nach einem solchen Protokollschritt gilt stets $B \triangleleft X$.

Die wesentlichen Schlussregeln der BAN-Logik sind:

- Die Regel über *Vertrauen in die Autorität*: Wenn *A* glaubt, dass *B* für eine Aussage *X* zuständig ist und glaubt, dass *B* die Aussage *X* glaubt, dann glaubt auch *A* die Aussage *X*.

(11) $$\frac{A \mid\equiv B \mid\Rightarrow X,\ A \mid\equiv B \mid\equiv X}{A \mid\equiv X}$$

- Die Regel über *Verbindlichkeit frischer Aussagen*: Wenn *A* glaubt, dass *X* frisch ist und glaubt, dass *B* die Aussage *X* gesagt hat, dann glaubt *A* auch, dass *B* immer noch *X* glaubt.

(12) $$\frac{A \mid\equiv \#X,\ A \mid\equiv B \mid\sim X}{A \mid\equiv B \mid\equiv X}$$

- Die Regel über *Absenderintegrität durch Kryptographie*: Wenn *A* glaubt, den Schlüssel *K* mit *B* zu teilen und sieht, dass *X* mit *K* verschlüsselt bzw. integritätsgeschützt wurde, dann glaubt *A*, dass *X* tatsächlich von *B* gesagt wurde.

(13) $$\frac{A \mid\equiv A \overset{K}{\leftrightarrow} B,\ A \triangleleft \{X\}_K}{A \mid\equiv B \mid\sim X}$$

bzw. $$\frac{A \mid\equiv A \overset{K}{\leftrightarrow} B,\ A \triangleleft \langle X \rangle_K}{A \mid\equiv B \mid\sim X}$$

- Die Regel über *Nachrichtenintegrität durch Kryptographie*: Wenn *A* glaubt, dass *X* frisch ist, und sieht, dass (*X*, *Y*) mit *K* verschlüsselt bzw. integritätsgeschützt wurde, dann glaubt *A*, dass auch *Y* frisch ist.

(14) $$\frac{A \mid\equiv \#X,\ A \triangleleft \{X, Y\}_K}{A \mid\equiv \#Y}$$

bzw. $$\frac{A \mid\equiv \#X,\ A \triangleleft \langle X, Y \rangle_K}{A \mid\equiv \#Y}$$

Daneben gibt es noch weitere Schlussregeln zu konkatenierten Aussagen. Diese Regeln beschreiben intuitiv verständliche Sachverhalte, z. B. dass *A* auch jeden einzelnen Teil einer für *A* sichtbaren konkatierten Nachricht sieht, und werden unten an der Stelle eingeführt, an der sie zum ersten Mal benötigt werden.

3 Analyse des iTAN-Protokolls

Zunächst untersuchen wir nun das hinlänglich bekannte iTAN-Verfahren zur Legitimation von Transaktionen im Online-Banking.

Das in der Sprache der BAN-Logik idealisierte iTAN-Protokoll betrachtet als beteiligte Parteien die Bank *B*(ob) und die Kundin *A*(lice) und geht von folgenden Voraussetzungen aus:

(15) $$A \mid\equiv A \overset{K}{\leftrightarrow} B$$
$$B \mid\equiv A \overset{K}{\leftrightarrow} B$$

A und *B* teilen den geheimen Schlüssel K. Da A nicht wirklich einen geheimen Schlüssel vorliegen hat, darf *K* nur eingeschränkt verwendet werden, um $I \in \{0,\ldots,100\}$ zu verschlüsseln, was die verfügbaren iTANs modelliert.

Implizit ist damit angenommen, dass kein Dritter *K* kennt und *K* gemäß der grundsätzlichen Einschränkung des Angreifermodells auch weder von *A* noch von *B* weitergegeben wird. Ebenfalls wird implizit angenommen, dass die Zusendung der iTAN-Liste von *B* an *A* unverfälscht und vertraulich gelingt.

(16) $B \mid\equiv A \mid\Rightarrow T$

B glaubt, dass *A* für Transaktionsnachrichten T zuständig ist.

(17) $A \mid\equiv T$

A beabsichtigt Transaktion *T*.

(18) $A \mid\equiv B \mid\Rightarrow I$

A glaubt, dass *B* für TAN-Ordnungsnummern *I* zuständig ist.

(19) $B \mid\equiv I,\ B \mid\equiv \#I$

B verwendet eine frische TAN-Ordnungsnummer *I*.

Diese Annahme ist angesichts des möglichen Umfangs von 100 Ordnungsnummern, die ein Angreifer alle bereits verwenden könnte, in der Praxis eher etwas zu optimistisch und bliebe als Voraussetzung für einen erfolgreiche formale Herleitung des Sicherheitsziels zu hinterfragen, wenn nicht, wie unten dargestellt, die Herleitung aus anderen Gründen ohnehin scheitern würde.

Auf die Modellierung der SSL-Verbindung, über welche die Protokollnachrichten verschlüsselt und integritätsgeschützt übertragen werden, wird verzichtet, da nach der Bedrohungslage ein Angreifer z. B. in Gestalt eines Trojaners den Schutz durch die SSL-Verbindung aushebeln könnte.

Ziel der Protokollanalyse ist die Ableitung der Aussage:

(20) $B \mid\equiv T$

B glaubt die Transaktionsnachricht *T*. Darin ist impliziert, dass die Transaktionsnach-

richt auch unverfälscht ist, d. h. *B* berechtigt an die Gültigkeit der Nachricht glaubt.

Die idealisierten Protokollschritte sind:

(21) $$A \rightarrow B : T$$

A sendet *B* die gewünschte Transaktion.

(22) $$B \rightarrow A : I$$

B sendet die TAN-Ordnungsnummer *I*. Wenn die Kundin *A* aufmerksam genug ist, zu prüfen, ob sie diese Ordnungsnummer bereits abgestrichen hat und ggf. das Protokoll abbricht, kann man ab diesem Protokollschritt weiterhin voraussetzen, dass gilt: $A|\equiv \# I$.

(23) $$A \rightarrow B : \{I\}_K$$

A sendet die passende iTAN.

Der Versuch einer formalen Herleitung von $B|\equiv T$ scheitert daran, dass *T* weder in eine Verschlüsselung noch in eine MAC-Prüfsumme eingeht, so dass *B* nicht über die Regeln zur Absender- und Nachrichtenintegrität $B|\equiv \# T$ und $B|\equiv A|\sim T$ herleiten kann, was wiederum benötigt würde, um über Verbindlichkeits- und Autoritätsregel zum Ziel zu kommen.

Dies ist die formale Konsequenz der bekannten Sicherheitsschwächen des iTAN-Verfahrens (kein Integritätsschutz der Transaktion, d. h. *T* kann vom Angreifer unerkannt modifiziert werden).

4 Analyse eines Token-TAN-Protokolls

Als Alterantive zu dem – im betrachteten Angreifermodell – unsicheren iTANProtokoll untersuchen wir nun eine Protokoll-Variante, bei der den Kunden von ihrer Bank ein Hardware-Token bzw. eine Chipkarte personalisiert, d. h. mit einem geheimen Schlüssel bestückt, zur Verfügung gestellt wird. Die TAN wird dann abhängig von einer Nonce der Bank (die den Index der iTAN ersetzt) und den eingegebenen Transaktionsdaten in diesem Token errechnet.

4.1 Ohne Eingriff in die Benutzerführung

Das in der Sprache der BAN-Logik idealisierte Token-TAN Sicherheitsprotokoll betrachtet das sichere Gerät *C*(hipkarte) der Kundin *A* als weitere beteiligte Partei und geht von folgenden Voraussetzungen aus:

(24) $$B|\equiv B \overset{K}{\leftrightarrow} C$$
$$C|\equiv B \overset{K}{\leftrightarrow} C$$

B und *C* teilen den geheimen Schlüssel *K*. Die in der Praxis mögliche bankseitige Ableitung von *K* aus einem Masterkey wird an dieser Stelle nicht weiter betrachtet, d. h. wir nehmen implizit an, dass eine solche Ableitung kryptographisch ebenso stark ist wie eine zufällige und vertrauliche Wahl.

(25) $$A|\equiv A \overset{L}{\leftrightarrow} C$$
$$C|\equiv A \overset{L}{\leftrightarrow} C$$

A und *C* teilen den geheimen Schlüssel *L*. Dieser Schlüssel existiert nicht tatsächlich. Die Verschlüsselung mit *L* modelliert jedoch den sicheren Kanal zwischen *A* und *C*, d. h. die (offline) Tastatureingaben und Ablesen, ggf. nach vorheriger Authentisierung durch eine Karten-PIN.

(26) $$B|\equiv A|\Rightarrow T$$

B glaubt, dass *A* für Transaktionsnachrichten *T* zuständig ist.

(27) $$A|\equiv T$$

A beabsichtigt Transaktion *T*.

(28) $$A|\equiv B|\Rightarrow Y$$

A glaubt, dass *B* für die von ihr gesendeten Nonces *Y* zuständig ist.

(29) $$B|\equiv Y, B|\equiv \# Y$$

B verwendet eine frische Nonce *Y*.

(30) $$B|\equiv C|\Rightarrow A|\equiv T$$

B glaubt, dass *C* zuständig dafür ist, ob *A* Transaktionsnachrichten *T* glaubt. Mit anderen Worten: *B* glaubt, dass *C* im Namen von *A* spricht, wenn es um *T* geht. Diese Annahme erscheint plausibel, sofern *C* ein offline betriebenes, persönliches Gerät von *A* ist, dessen Verlust *A* bemerken und melden würde und auf das ein Dritter (PIN-Schutz) keinen Zugriff hat. Auf die Modellierung der SSL-Verbindung wird aus den oben genannten Gründen wieder verzichtet.

Ziel der Protokollanalyse ist wiederum die Ableitung der Aussage:

(31) $$B|\equiv T$$

B glaubt die Transaktionsnachricht *T*.
Die idealisierten Protokollschritte sind:

(32) $$A \rightarrow B : T$$

A sendet *B* die gewünschte Transaktion. Dieser Schritt wäre nach strenger Auslegung des idealisierten Protokolls überflüssig. In der Praxis wird er jedoch benötigt, um die später nicht mehr explizit übertragene Nachricht *T* auf Bankseite zu rekonstruieren.

(33) $$B \rightarrow A : Y$$

B sendet die Nonce *Y*.

(34) $$A \rightarrow C : \{Y, T\}_L$$

A gibt per Tastatur die Nonce und die Transaktionsnachricht in *C* ein. Dies ist eine Idealisierung, da je nach Transaktionstyp nur mehr oder minder große nur Teile von *T* in die dynamische TAN eingehen können, ohne den Anwender mit der fehlerfreien Übertragung zu überfordern.

Als zusätzliche Annahme können wir nach diesem Schritt von $C|\equiv \#(Y,T)$ ausgehen, da es sich um eine unmittelbare Benutzereingabe handelt.

(35) $$C \rightarrow A : \left\{\left\langle Y, T, A|= T\right\rangle_K\right\}_L$$

C gibt über die Anzeige die TAN aus. Dieser Schritt ist in zweifacher Hinsicht eine gewisse Idealisierung: Einerseits werden *Y* und *T* nicht übertragen, sondern liegen *A* und *B* bereits vor. Zum anderen ist $A|\equiv T$ implizit in der Tatsache enthalten, dass eine TAN ausgegeben wird. Im Rahmen der nachfolgenden Analyse ist daher nachzuweisen, dass $C|\equiv A|\equiv T$ gilt, wenn *C* eine TAN ausgibt.

(36) $$A \rightarrow B : \left\langle Y, T, A|= T\right\rangle_K$$

A überträgt die angezeigte TAN. Auch hierbei werden *Y* und *T* nicht tatsächlich übertragen, sondern liegen *B* bereits vor.

Die formale Herleitung des Sicherheitsziels kann in zwei Schritten erfolgen. Zunächst wird als Zwischenschritt $C|\equiv A|\equiv T$ hergeleitet:

(37) $$\frac{C|\equiv A \overset{L}{\leftrightarrow} C, C \triangleleft \{Y,T\}_L}{C|\equiv A|\sim (Y,T)}$$

ergibt sich durch Regel (13) angewandt auf (25) und (34).

(38) $$\frac{C|\equiv A|\sim (Y,T)}{C|\equiv A|\sim T}$$

ergibt sich durch eine intuitive Konkatenationsregel angewandt auf (37).

(39) $$\frac{C|\equiv \#(Y,T)}{C|\equiv \# T}$$

ergibt sich durch eine intuitive Konkatenationsregel angewandt auf (34).

(40) $$\frac{C|\equiv \# T, C|\equiv A|\sim T}{C|\equiv A|\equiv T}$$

ergibt sich durch Regel (12) angewandt auf (38) und (39). Diesem Zwischenergebnis folgend kann *C* in Schritt (35) tatsächlich

(implizit mit Anzeige der TAN) aus berechtigter Überzeugung $A|\equiv T$ sagen. Nun bleibt im zweiten Schritt das eigentliche Sicherheitsziel abzuleiten:

(41) $$\frac{B|\equiv B \overset{K}{\leftrightarrow} C, B \triangleleft \langle Y, T, A|\equiv T\rangle_K}{B|\equiv C|\sim (Y, T, A|\equiv T)}$$

ergibt sich durch Regel (13) angewandt auf (24) und (36).

(42) $$\frac{B|\equiv C|\sim (Y, T, A|\equiv T)}{B|\equiv C|\sim A|\equiv T}$$

ergibt sich durch eine intuitive Konkatenationsregel angewandt auf (41).

(43) $$\frac{B|\equiv \#Y, B \triangleleft \langle Y, T, A|\equiv T\rangle_K}{B|\equiv \#(T, A|\equiv T)}$$

ergibt sich durch Regel (14) angewandt auf (29) und (36).

(44) $$\frac{B|\equiv \#(T, A|\equiv T)}{B|\equiv \#T, B|\equiv \#A|\equiv T}$$

ergibt sich durch eine intuitive Konkatenationsregel angewandt auf (43).

(45) $$\frac{B|\equiv \#A|\equiv T, B|\equiv C|\sim A|\equiv T}{B|\equiv C|\equiv A|\equiv T}$$

ergibt sich durch Regel (12) angewandt auf (42) und (44).

(46) $$\frac{B|\equiv C|\Rightarrow A|\equiv T, B|\equiv C|\equiv A|\equiv T}{B|\equiv A|\equiv T}$$

ergibt sich durch Regel (11) angewandt auf (30) und (45).

(47) $$\frac{B|\equiv A|\Rightarrow T, B|\equiv A|\equiv T}{B|\equiv T}$$

ergibt sich durch Regel (11) angewandt auf (26) und (46).

Damit ist die formale Herleitung erfolgreich abgeschlossen.

Unter der Annahme, dass *A* sich an das Protokoll hält und das Gerät *C* für einen Dritten nicht nutzbar ist, ist das Verfahren also sicher gegen Angriffe im betrachteten Angreifermodell.

4.2 Mit Eingriff des Angreifers in die Benutzerführung

Unter der Annahme des erweiterten Angreifermodells, dass *P*aul *A*lice zu weitgehend beliebigen Handlungen veranlassen kann, sind die in Abschnitt 4.1 angenommenen Voraussetzungen (26) und (30) nicht mehr haltbar. Die Bank kann in diesem Angreifermodell nicht mehr sicher wissen, ob Kunde *A* eine Transaktionsnachricht vertrauenswürdig und aus eigenem Willen so geäußert hat, oder ob *A* von einem Angreifer per Phishing o. ä. zu dieser Nachricht verleitet wurde. Auch das Gerät *C* kann dies per se nicht realistisch unterscheiden.

Da aber die beiden Voraussetzungen (26) und (30) als wesentlicher Bestandteil in die abschließenden Analyseschritte (46) bzw. (47) eingehen, ist die obige formale Herleitung der Sicherheit des Token-TAN-Protokolls unter den erweiterten Bedrohungsannahmen in dieser Form nicht möglich.

Das legt nahe, dass die getroffenen Annahmen für die Wirksamkeit der Schutzmaßnahme (TAN-Erzeugung per Token) essentiell sind; fallen sie weg, gilt die Sicherheit des Verfahrens möglicherweise nicht mehr uneingeschränkt.

Ganz wesentlich ist dabei auch Schritt (34) des Verfahrens: Dessen Sicherheit hängt davon ab, dass *A* die unter Risikoaspekten relevanten Teile der Transaktionsdaten ohne fremde Hilfe – die in Wirklichkeit von *P* vorgegaukelt sein könnte – leicht ermitteln und fehlerfrei eingeben kann. Damit sind beispielsweise summarische Werte oder Teile von „fremd" vorberechneten Prüfsummen an dieser Stelle ungeeignet.

An eben dieser Stelle sind, wie von Drimer, Murdoch und Anderson [5] beschrieben, auch reale Implementierungen von Token-TAN-Verfahren mit CAP (Chip Authentication Programme) Handheld-Kartenlesern in Großbritannien anfällig gegen in Phishing-Manier vorgetragenes Social Engineering.

5 Fazit

Die (semi-) formalen Analysen der Online-Banking-Protokolle mit iTAN und mit Token-basierter TAN legen die sicherheitskritischen Punkte der Verfahren offen:

- Das iTAN-Verfahren bietet keinen Authentizitätsschutz der Transaktion und ist daher bekanntermaßen anfällig für Man-in-the-Middle-Angriffe (z. B. über einen Trojaner).
- Token-TAN-Verfahren besitzen diese Schwäche nicht, sofern ein Angreifer den Token nicht manipulieren kann.
- Essentiell ist dabei, dass die Nutzerin *A*lice sich durch eine möglichst intuitive Benutzerführung, die nur schwer durch *P*aul missbräuchlich umgedeutet werden kann, stets im Klaren darüber ist, welche Aktion sie gerade durchführt bzw. freigibt. Angelehnt an die Sprache der BAN-Logik: „*A* muss wissen, was *A* tut".
- Die Sicherheitsbeweise lassen sich nur unter der Voraussetzung führen, dass ein Angreifer *P*aul die Nutzerin *A*lice nicht zu beliebigem Handeln verleiten kann.

Der Einsatz eines Tokens (Chipkarte, TAN-Generator o. ä.) sorgt also nachweislich für einen deutlichen Sicherheitsgewinn gegenüber dem iTAN-Verfahren. Allerdings hat auch die Sicherheit token-basierter Verfahren Grenzen: Gegen einen Angreifer, dem es gelingt, *A*lice z. B. durch eine Fälschung der Benutzeroberfläche („Testbetrieb") dazu zu bewegen, gutgläubig und unbeabsichtigt selbst eine falsche Transaktion zu veranlassen, ist auch dieses Verfahren nicht gefeit.

Dank

Der Autor dankt Dr. Kai Buchholz-Stepputtis und Dr. Boris Hemkemeier (beide Commerzbank AG) sowie Dirk Fox (Secorvo) für zahlreiche Diskussionen, Anregungen und konstruktive Kommentare.

Literatur

[1] M. Burrows, M. Abadi, R. M. Needham, *A Logic of Authentication*, in: Proceedings of the Royal Society of London A v 426 (1989), pp. 233-271.

[2] M. Burrows, M. Abadi, R. M. Needham, A Logic of Authentication, in: ACM Transaction on Computer Systems, Vol. 8, No. 1, Feb. 1990, pp. 18-36. http://www.stanford.edu/class/cs259/WWW06/papers/ban1990.pdf

[3] Neumann, Heike; Kessler, Volker: *Formale Analyse von kryptographischen Protokollen mit BAN-Logik*. DuD 2/1999, S. 90-93.

[4] R. J. Anderson, *The Formal Verification of a Payment System*, Technical report, Computer Lab, Univ. of Cambridge, UK, 1997. http://www.cl.cam.ac.uk/~rja14/Pape rs/uepsbook.pdf

[5] S. Drimer, S. J. Murdoch, R. J. Anderson, *Optimised to fail: Card readers for online banking, Financial Cryptography and Data Security*, Rockley, Barbados, 23–26 February 2009. http://www.cl.cam.ac.uk/~sjm217/papers/fc09optimised.pdf