Schutzmöglichkeiten gegen Phishing

Klaus Plößl, Hannes Federrath, Thomas Nowey
Universität Regensburg
{klaus.ploessl,hannes.federrath,thomas.nowey}@wiwi.uni-regensburg.de

Abstract: Dieses Papier stellt einen neuen Lösungsvorschlag zur Eindämmung von Phishing vor. Der Vorschlag baut auf dem Prinzip der Challenge-Response-Authentikation auf und kommt ohne Hardware beim Kunden aus. Dadurch kann er ohne größere Kosten insbesondere von Banken und gegebenenfalls von Websitebetreibern umgesetzt werden, und stellt somit einen guten Kompromiss gegenüber anderen Verfahren dar. Der größte Nachteil besteht darin, dass er nicht gegen man-in-the-middle-Angriffe schützt.

1 Bekannte Gegenmaßnahmen

Phishing ist eine relativ neue Form des Betrugs, die mit Methoden des Social Engineering arbeitet. Das Opfer wird dazu gebracht, persönliche Daten (z.B. Passwörter, Kreditkarteninformationen oder Onlinebanking-Daten) zu verraten [Gro03].

Mittlerweile gibt es eine Vielzahl von Vorschlägen, wie man sich vor Online-Betrügern im Allgemeinen und Phishing im Besonderen schützen kann. Im Folgenden werden einige Maßnahmen kurz genannt, ausführlichere Informationen sind auf unserer Webseite (http://www-sec.uni-regensburg.de/phishing/) zu finden.

Eine Gruppe von Vorschlägen lässt das bisherige PIN/TAN-Verfahren unverändert. Im Wesentlichen wird vorgeschlagen, diese Gruppe in nutzerabhängige Verfahren (z.B. „Leitfaden“ für richtiges Verhalten, Filter, Browser-Plug-ins) und nutzerunabhängige Verfahren (Spam-Trap, Domain-Watch, Validierung von Absenderdaten, Fraud Detection Systeme) einzuteilen.

Als nachhaltige Lösung des Problems kommen allerdings nur Verfahren in Frage, die das bisherige PIN/TAN-Verfahren zur Authentifizierung bzw. Autorisierung ändern. Bei den meisten dieser Verfahren ist weitere Hardware in Form von Kartenlesern, Chipkarten und/oder Token nötig.

Die sicherste Gegenmaßnahme ist der Einsatz von digitalen Signaturen. Dabei werden alle Aufträge vom Nutzer signiert und können nicht mehr unerkannt verändert werden. Nachteilig ist, dass eine entsprechende Public-Key-Infrastruktur existieren muss.

2 Neuer Lösungsvorschlag

Im Prinzip handelt es sich bei dem neuen Verfahren um die Verknüpfung des PIN/TAN-Verfahrens mit einem papierbasierten Challenge-Response-Verfahren. Es unterscheidet sich vom herkömmlichen PIN/TAN-Verfahren darin, dass der Nutzer anstelle der TANs eine Liste erhält, in der Zahlenpaare aufgeführt sind. Diese Zahlenpaare sind Challenge-Response-Paare, d.h. dem Nutzer wird beim Abschließen einer Transaktion eine Zahl (die Challenge) präsentiert und er muss die zugehörige Zahl (Response) des Zahlenpaares eingeben. Nur wenn er die richtige Response eingegeben hat, wird die Transaktion ausgeführt.

Soll anstelle einer Transaktion (auch) der Zugang zu einem System geschützt werden, gibt der Nutzer bei der Anmeldung seine Kennung an und bekommt daraufhin eine Challenge präsentiert, auf die er mit der richtigen Response antworten muss. Dem Nutzer wird der Zugang nur gewährt, wenn die Response richtig ist. Will der Nutzer nun eine Transaktion durchführen, wird ihm eine weitere Challenge der Liste präsentiert, auf die er wieder mit der zugehörigen Response antworten muss.

Eine Challenge wird immer nur ein einziges Mal an den Nutzer geschickt, egal ob die eingegebene Response richtig oder falsch war. Sind die Challenges auf der Liste verbraucht, bekommt der Nutzer eine neue Liste. Außerdem sollte nach einer bestimmten Anzahl von Fehlversuchen (z.B. drei) der Nutzer benachrichtigt und der Account zumindest für eine bestimmte Zeit gesperrt werden.

Es ist sinnvoll, zusätzlich die Gültigkeit der Challenge auf einen kurzen Zeitraum zu beschränken, um man-in-the-middle-Angriffe zu erschweren, d.h. es steht dem Angreifer nur ein eng begrenzter Zeitraum zur Verfügung.

Werden Challenge und Response (z.B. durch die Verwendung einer Buchstabenfolge als Challenge und einer Zahlenfolge als Response) besser unterscheidbar gemacht, verbessert dies die Usability.

3 Bewertung

Der neue Vorschlag wird anhand der für die Phishing-Problematik relevanten Kriterien in [ELP+01] bewertet. In Tabelle 1 auf S. 3 werden die Ergebnisse der Bewertung zusammengefasst. ++ bedeutet sehr gut, + gut, $\sim$ mittelmäßig, - schlecht und - - sehr schlecht.

Die momentan eingesetzten Passwörter und TANs bieten keinen Schutz vor Phishing. Im Gegensatz dazu macht der Einsatz von PKI und digitaler Signatur Phishing unmöglich, da die signierten (Auftrags-) Daten nicht unbemerkt geändert werden können.

Werden Hardware-Token eingesetzt, gibt es geringe Unterschiede beim Schutz vor Phishing je nach konkreter Ausprägung. Werden die Einmalpasswörter periodisch gewechselt, muss der Betrüger einen man-in-the-middle-Angriff durchführen, um Nutzen aus den abgefangenen Passwörtern zu ziehen. Handelt es sich um Token, die auf Anforderung ein zeitunabhängiges Passwort generieren, hat es der Betrüger leichter. Er kann die ergaunerten Passwörter solange benutzen, bis das Opfer sich erneut beim Dienstleister anmeldet.

	Sicherheit		Nutzerakzeptanz				Kosten				
Verfahren	*Schutz vor Phishing*	Zuverlässigkeit	Installationsaufwand	Anwendbarkeit	Wiederverwendbarkeit	Transparenz des Ablaufs	Software-Kosten	Hardware-Kosten	Schulungs-Kosten	Administrations-Kosten	Weitere Einsatzmögl.
Passwort	- -	$\sim$	+	+	+	+	+	+	+	-	+
Neues Verfahren	+	++	++	++	+	++	+	+	+	+	+
Token: Einmal-PW periodisch	+	+	++	+	+	++	+	-	$\sim$	+	+
Token: Einmal-PW auf Anforderung	$\sim$	+	++	+	+	++	+	-	$\sim$	+	+
PKI mit Smartcard-Unterstützung	++	+	+	++	++	++	-	-	$\sim$	$\sim$	++

Tabelle 1: Bewertung der Alternativen aus [ELP$^+$01], eigene Bewertungen *kursiv*

Die neu vorgeschlagene Lösung bietet einen höheren Schutz gegen Phishing als Token, die ihre Passwörter auf Anforderung generieren, da der Betrüger die richtige Response auf eine Challenge benötigt. Da jede Challenge dem Nutzer aber nur einmal präsentiert wird, kann sich der Betrüger keine Challenges auf Vorrat holen. Maximal ist es für den Betrüger möglich, einen man-in-the-middle-Angriff durchzuführen, wodurch das neue Verfahren annähernd den Schutz vor Phishing bietet wie Token, die periodisch neue Einmalpasswörter generieren.

Papierlisten, wie sie in dem neuen Verfahren verwendet werden, sind sehr zuverlässig. Die einzige Gefahr besteht darin, dass sie verlegt oder gestohlen werden könnten. Bei Hardware-Token besteht zusätzlich die Gefahr, dass die Stromversorgung nicht sichergestellt ist oder durch Krafteinwirkung Defekte auftreten.

Ein Installationsaufwand für den Benutzer ist weder beim Einsatz von Token noch bei der Verwendung papierbasierter Challenge-Response-Listen gegeben. Alle Varianten sind sehr einfach anwendbar. Die neu vorgeschlagene Variante ist dem bisherigem PIN/TAN-Verfahren aber ähnlicher als die Verwendung von Token.

Beim Punkt Wiederverwendbarkeit für andere Zwecke sind die Methoden gleich gut wie die herkömmlichen Passwörter. Für jeden Dienst wird ein eigenes Token bzw. eine eigene Liste benötigt, jede der Methoden kann aber auch für andere Anwendungen wie die Authentifizierung an Bankautomaten usw. benutzt werden. Die Transparenz beim Ablauf der Authentifizierung bzw. Autorisierung ist sehr hoch, da der Nutzer immer genau weiss, was er tun muss und warum. Er hat volle Kontrolle darüber, was er eingibt und was nicht.

Die Software-Kosten sind bei allen Varianten ähnlich niedrig. Beim neuen Vorschlag muss das bisherige PIN/TAN-Verfahren erweitert werden, was vergleichsweise geringen Aufwand verursacht. Beim Einsatz von Token muss ebenfalls ein neues Authentifizierungsmodul benutzt werden, das aber meist vom Token-Hersteller zur Verfügung gestellt wird.

Beim neuen Verfahren fallen keine zusätzlichen Hardwarekosten an. Lediglich die Papierlisten müssen erstellt werden. Dies unterscheidet sich aber nicht vom PIN/TAN-Verfahren. Die Schulungskosten sind gering, da das Verfahren dem bekannten PIN/TAN-Verfahren sehr stark ähnelt. Da die Nutzer ihr Passwort nicht mehr vergessen können, fallen die Administrationskosten sogar geringer aus, als beim normalen Passwortverfahren.

Die Token-basierten Verfahren verursachen bei großen Nutzerzahlen nicht zu vernachlässigende Hardware-Kosten, da jeder Nutzer mit einem Token ausgestattet werden muss. Auch die Kosten für Schulung und Administration sind höher als bei der Verwendung von Passwörtern, da die Bedienung der Token vielen Nutzern erst beigebracht werden muss.

4 Zusammenfassung

Zuverlässiger Schutz vor Phishing ist nicht durch die existierenden Passwort und PIN/TAN-Verfahren möglich. Der Einsatz von digitalen Signaturen ist in Bezug auf Sicherheit die beste verfügbare Lösung. Diese bringt allerdings viele Kosten in Form von zusätzlich benötigter Hardware, Benutzerschulungen, Support, Betrieb der PKI usw. mit sich. Auch ist der Nutzer nicht mehr uneingeschränkt mobil, da bei den meisten Lösungen ein Kartenleser an den PC angeschlossen und Treiber dafür installiert werden müssen. Dies ist z.B. auf Reisen in einem Internet-Cafe nahezu unmöglich.

Die Verwendung von Hardware-Token mit zeitlich begrenzt gültigen Passwörtern schützt ebenfalls relativ zuverlässig vor Phishing-Attacken. Allerdings ist auch diese Alternative mit zusätzlichen Kosten für Hardware, Benutzerschulungen und Support verbunden. Diese sind zwar geringer als beim Einsatz von PKI und digitaler Signatur, aber dennoch bei großen Nutzerzahlen nicht zu vernachlässigen. Auch werden die Nutzer nicht gewillt sein, für jede Anwendung einen eigenen Hardware-Token zu benutzen und ggf. immer bei sich zu haben.

Das neu vorgeschlagene papierbasierte Challenge-Response-Verfahren könnte ein guter Kompromiss zwischen Sicherheit und Kosten sein, da es annähernd so zuverlässig vor Phishing-Attacken schützt wie der Einsatz von Hardware-Token, jedoch wesentlich weniger zusätzliche Kosten verursacht, da z.B. keine Hardware beim Nutzer benötigt wird. Es existiert lediglich kein Schutz vor man-in-the-middle-Angriffen, was aber auch beim Einsatz von Hardware-Token nicht der Fall ist.

Aufgrund der Nähe des Verfahrens zum bisher eingesetzten Passwort- bzw. PIN/TAN-Verfahren, halten sich auch die (zusätzlichen) Kosten für Benutzerschulungen und Support in Grenzen. Die Mobilität des Nutzers bleibt größtenteils erhalten, da er im schlechtesten Fall für jede benötigte Anwendung ein Blatt Papier bei sich haben muss, auf dem die Challenge-Response-Paare abgedruckt sind.

Literatur

[ELP+01] W. Essmayr, H. Leonhardsberger, S. Probst, W. Stockner und E. Weippl. Qualitative Evaluation of Authentication Approaches for eBanking. Bericht SCCH-TR-0215, Software Competence Center Hagenberg, Hagenberg, 2001.

[Gro03] The Anti-Phishing Working Group. *Proposed Solutions to Address the Threat of Email Spoofing Scams*, Dezember 2003.