Eine vorläufige Version erscheint auf der D·A·CH Security 2007.

Verwendet Ihre Bank Sichere TANs?

Marc Fischlin*

Darmstadt University of Technology, Germany
marc.fischlin@gmail.com www.fischlin.de

Zusammenfassung. Wir stellen im folgenden die statistische Auswertung einiger (i)TAN-Listen zweier Banken vor. Dabei stellt sich heraus, dass die Listen einer Bank starke statistische Auffälligkeiten zeigen, die zu einer signifikanten Verbesserung der Vorhersagewahrscheinlichkeit solcher TANs führt.

1 Einleitung

Online-Banking wird heutzutage oft durch PIN/TAN-Verfahren abgesichert, bei denen dem Kunden neben seiner geheimen PIN auch noch eine Liste von Transaktionsnummern zum Schutz einzelner Vorgänge vorliegt. Die TAN ist dabei eine meist sechsstellige, von der Bank erzeugte Dezimalzahl, die dem Kunden zuvor per Post in einer Liste von ca. 100 TANs zugeht.

Die Sicherheit PIN/TAN-basierter Verfahren beruht insbesondere auf der Qualität der PIN —in der Regel vom Kunden gewählt— und der Unvorhersagbarkeit der TANs. Idealerweise sollten diese TANs zufällig erzeugt werden, so dass die Ratewahrscheinlichkeit einer einzelnen, sechsstelligen TAN nur 10^{-6} beträgt. Eine erste Analyse einiger vorliegender TAN-Listen einer mitteldeutschen Bank mit Filial- und Online-Betrieb für ca. 250.000 Privatkunden zeigt allerdings, dass die Vorhersagewahrscheinlichkeit für solche Listen teilweise bis zu 18-mal so hoch ist (experimentell ermittelt). Somit können diese TANs mit einer Wahrscheinlichkeit von ca. 1/55.555 vorhergesagt werden und liegen daher unter dem Sicherheitsniveau fünfstelliger TANs.

Wir stellen im folgenden unsere ermittelten Vorhersagewahrscheinlichkeiten vor. Dazu präsentieren wir die grundlegenden statistischen Auswertungen der vorliegenden TAN-Listen und die Auffälligkeiten, die zu Verbesserungen der Ratewahrscheinlichkeiten führen. Wir betonen, dass sich die vorgestellten Ergebnisse auf *indizierte* TANs (iTANs) beziehen, bei denen die TANs numeriert werden und für jede Aktion eine bestimmte TAN abgefragt wird. Solche iTANs werden von den Banken oft als sicherheitsverstärkend angepriesen. Wie unsere Experimente zeigen, gilt dies allerdings nicht, wenn die TANs selbst nicht gut gewählt werden.

2 Angriffsmodell

Unser Angriffsmodell lässt sich durch folgendes Beispiel motivieren: Auf dem Computer des Kunden wurde ein Torjaner installiert, der die verbrauchten, in der Regel indizierten TANs

*Diese Arbeit wurde im Rahmen des Emmy Noether Programms Fi 940/2-1 der Deutschen Forschungsgemeinschaft (DFG) unterstützt.

(und eventuell die PIN) während der Aktionen des Kunden protokolliert. Nachdem einige (i)TANs vom Kunden verwendet wurden, sendet der Trojaner die protokollierten Daten an einen Angreifer. Der Angreifer meldet sich dann bei der Bank unter dem Namen des Kunden an, führt eine Aktion aus und versucht dazu, aus den erhaltenen Daten eine Vorhersage für die entsprechende (i)TAN zu generieren.

Bei qualitativ guten (i)TANs sollte der Angreifer im obigen Beispiel selbst bei Kenntnis der PIN nur eine geringe Erfolgswahrscheinlichkeit besitzen. Anders dagegen bei schwach erzeugten (i)TANs, bei denen das Erraten eventuell möglich ist. Im Unterschied zu Man-in-the-Middle-Angriffen auf iTAN-Verfahren [News05], bei denen der Angriff nur zu dem Zeitpunkt erfolgen kann, in dem auch der Kunde online ist, kann der Angriff hier auch "offline" erfolgen: Nach der Übertragung der Daten des Trojaners kann der Angreifer den Versuch ohne Unterstützung des Kunden ausführen.

3 Statistische Auswertung der TAN-Listen

Unsere Experimente wurden ohne Unterstützung der Banken ausgeführt und beruhen auf fünf vorliegenden (i)TAN-Listen des Autors für zwei Banken. Um die Qualität der Listen zu ermitteln, haben wir zunächst einfache statistische Auswertungen durchgeführt. Die dabei gefundenden Auffälligkeiten treten für echt zufällig erzeugte TAN-Listen nur sehr selten auf, teilweise können wir solches statistisches Rauschen im Wahrscheinlichkeitsbereich von ca. 10^{-5} bis 10^{-6} quantifizieren.

Bei der Beschreibung der statistischen Merkmale konzentrieren wir uns zunächst auf *eine* iTAN-Liste *einer* Bank A; die Resultate für die anderen Listen werden in Abschnitt 3.5 skizziert. Zunächst fällt auf, dass die 96 iTANs dieser Liste von Bank A nur aus den Dezimalzahlen 1 bis 9 bestehen, während die 0 nie auftritt. Dadurch erhöht sich die Ratewahrscheinlichkeit für Dezimal-TANs von 10^{-6} unmittelbar auf $9^{-6} \approx 1,88 \cdot 10^{-6}$, also fast um den Faktor 2.

3.1 Relative Häufigkeit von Ziffern

Bei einer echt zufällig erzeugten Liste aus Ziffern zwischen 1 und 9 —und damit auch annähernd bei einer durch einen starken Pseudozufallsgenerator erzeugten Liste— sollte jede Ziffer etwa gleich häufig in der kompletten Liste (gemittelt über alle $96 \cdot 6$ Stellen) auftreten, also mit relativer Häufigkeit von $1/9 = 11,11\%$. Bei denen uns vorliegenden TAN-Listen schienen allerdings oberflächlich betrachtet einige Ziffern häufiger aufzutreten als andere, so dass wir zunächst die relative Häufigkeit untersuchten.

In Abbildung 1 ist die Verteilung der Ziffern für die vorliegende iTAN-Liste dargestellt. Offensichtlich tritt die Ziffer 4 dabei doppelt so oft wie erwartet auf ($23,61\%$ vs. $11,11\%$), während beispielsweise die Ziffer 1 nur in ca. $7,11\%$ der Stellen vorkommt. Einen ähnlichen Fall gab es bereits einmal bei EC-Karten-PINs [Club97], bei denen manche Ziffern wegen der Umwandlung der Hexadazimalzahlen in Dezimalziffern häufiger auftraten; wir können allerdings keine Aussage machen, ob hier ein vergleichbarer Grund vorliegt.

Solche Abweichungen können übrigens auch bei echt zufällig erzeugten TAN-Listen auftreten. Jedoch lässt sich die Wahrscheinlichkeit, dass in einer solchen TAN-Liste aus $6 \cdot 96$ echt zufällig gewählten Ziffern zwischen 1 und 9 beispielsweise eine Ziffer mehr als doppelt so häufig wie erwartet auftritt, mittels der Chernoff-Schranken (siehe Anhang B) nach oben durch $10^{-5,22}$ abschätzen. Die Wahrscheinlichkeit, dass dies in zwei TAN-Listen (so wie hier in zwei der drei vorliegenden Listen der Bank A) jeweils passiert, sinkt somit deutlich unter die Chance auf einen Sechser im Lotto.

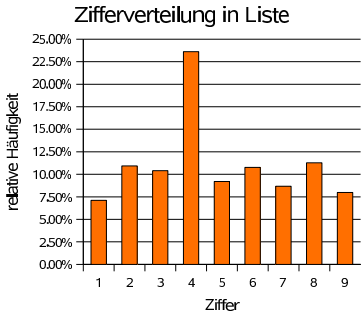

Abbildung 1: Statistische Verteilung der Ziffern (erwartet: $11,11\%$)

Ein weiteres Merkmal zur Messung der (Nicht)-Uniformität und Ermittlung möglicher Angriffe ist die sogenannte Renyi-Entropie. Sie gibt im wesentlichen die Kollisionswahrscheinlichkeit von Zufallsvariablen wider. In unserem Zusammenhang ist sie daher relevant bezüglich der Fragestellung, wie oft die durch die Bank erzeugten (i)TANs mit unseren Vorhersagen kollidieren. Dieser und weitere Entropie-Begriffe werden ausführlicher im Abschnitt A diskutiert.

Für eine echt zufällig erzeugte TAN (aus den Ziffern 1 bis 9) ist die Renyi-Entropie für die Zifferverteilung gleich $-\log_2 11,11\%$. Für die vorliegende iTAN-Liste beträgt sie dagegen $-\log_2 12,98\%$, liegt also höher und kann daher für die Vorhersage herangezogen werden.

3.2 Relative Häufigkeiten bezüglich Positionen

Eine weitere Auffälligkeit der Listen schien die Häufigkeiten bezüglich der sechs Positionen zu betreffen. Eine Aufstellung der relativen Häufigkeiten der Ziffern unterteilt nach Positionen bestätigte diese Vermutung. Insbesondere die letzte Stelle der TANs zeigte starke Schwankungen. So tritt die Ziffer 4 hier in ca. 40% aller Fälle auf (statt mit Häufigkeit $11,11\%$ bzw. mit Häufigkeit $23,61\%$, wenn man die Zifferverteilung der kompletten Liste zugrundelegt). Dagegen kommen die Ziffern 1, 3, 7 und 9 nur selten an dieser Position vor (jeweils maximal $4,16\%$). Siehe Abbildung 2.

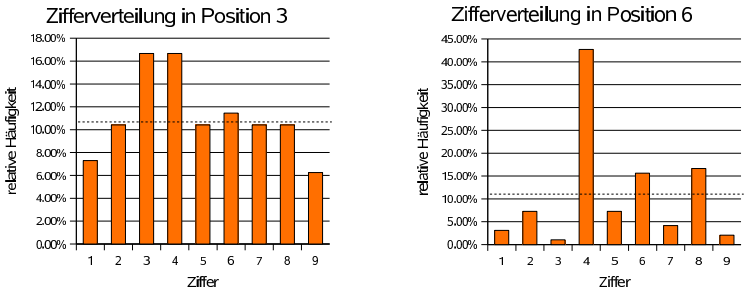

Abbildung 2: Statistische Verteilung der Ziffern bezüglich der Positionen 3 und 6 (erwartet: jeweils $11,11\%$). Bemerkung: Die Grafiken sind unterschiedlich skaliert.

Dabei ist anzumerken, dass hier bei jeder Position nur 96 Daten vorliegen, also im Durchschnitt jede Ziffer $96/9 = 10,66$ Mal auftreten sollte. Daher sind statistische Abweichungen aufgrund des geringen Stichprobenumfangs möglich. Allerdings zeigt auch hier wieder eine Anwendung der Chernoff-Schranke, dass bei echt zufällig gewählten Ziffern zwischen 1 und 9 folgende Abschätzung gilt: Die Wahrscheinlichkeit, dass es irgendeine Position und irgendeine Gruppe von 4 Ziffern in der Liste gibt, so dass diese Ziffern in dieser Position insgesamt in nur ca. 10% der Fälle getroffen werden (so wie hier die Werte 1, 3, 7 und 9 zusammen in Position 6), beträgt höchsten 10^{-6}.

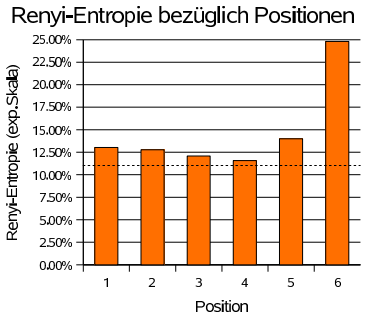

Abbildung 3: Statistische ermittelte Renyi-Entropie der einzelnen Positionen (erwartet: $-\log_2 11,11\%$). Bemerkung: Grafik ist gemäß $y \mapsto 2^{-y}$ skaliert.

Die Renyi-Entropien der Zifferverteilung bezüglich der einzelnen Positionen sind in Abbildung 3 dargestellt. Sie liegen alle über dem erwarteten Wert $-\log_2 11,11\%$. Dies legt eine verbesserte Vorhersagestrategie nahe (siehe Anhang A), wenn auch hier wieder der geringe Stichprobenumfang angemerkt sei.

3.3 Ziffernverteilung bezüglich Positionen

Als nächste Statistik betrachten wir die Verteilung einer Ziffer bezüglich der sechs Positionen. Unter optimaler Verteilung sollte jede Ziffer gleich häufig in den Positionen auftreten, also in jeder Stelle in $1/6 = 16,66\%$ der Fälle. Exemplarisch haben wir die Verteilungen der Ziffern 3 und 5 in Abbildung 4 dargestellt. Dabei zeigt sich, dass die 3 am häufigsten an Position 3 vorkommt $(26,66\%)$, aber fast nie an der letzten Position $(1,81\%)$. Genauso ist Ziffer 5, wenn sie in einer TAN auftritt, in mehr als einem Viertel aller Fälle an der ersten Position zu finden $(29,16\%)$.

3.4 Korrelationen

Ein weiterer wichtiger Aspekt sind die Abhängigkeiten zwischen Ziffern. Treten beispielsweise bestimmte Paare von Ziffern zu häufig in einer TAN auf? Wenn, treten dann diese Paare auch oft an bestimmten Positionen auf?

Wir ermittelten deshalb für alle Ziffern x, mit welcher Häufigkeit dann auch eine Ziffer y auftritt, sowie für alle Paare von Ziffern x, y, mit welcher relativen Häufigkeit in einer TAN eine dritte Ziffer z vorkommt, gegeben dass x, y auftreten. Auch hier zeigten sich starke Abweichungen vom erwarteten Wert. Da man hier die Liste der wenigen TANs noch zusätzlich

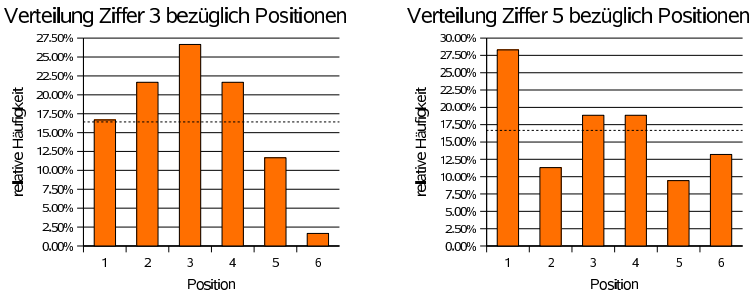

Abbildung 4: Statistische Verteilung der Positionen der Ziffern 3 bzw. 5 (erwartet: jeweils $16,66\%$). Bemerkung: Die Grafiken sind unterschiedlich skaliert.

einschränkt, lässt sich allerdings nicht ermitteln, ob diese Abweichungen durch die Erzeugung oder statistisches Rauschen entstanden sind. Inbesondere für solche Korrelationsstatistiken sind daher weitere TAN-Listen oder mehr Informationen über den Erzeugungsalgorithmus notwendig.

3.5 Statistiken für andere Listen

Bisher haben wir lediglich die statistischen Merkmale der iTAN-Liste einer Bank A vorgestellt. In Abbildung 5 sind examplarisch Statistiken für weitere TAN-Listen angegeben. Darunter sind drei iTAN-Listen von Bank A (inklusive der bereits ausführlich betrachteten Liste), bestehend aus zwei Listen für einen Kunden 1 und einer Liste für einen anderen Kunden 2. Die Listen umfassen jeweils 96 sechsstellige iTANs aus den Ziffern 1 bis 9. Dazu kommen zwei Listen des Autors für eine Direkt-Bank B, jeweils 100 sechsstellige TANs aus den Ziffern 0 (!) bis 9. Bei den Listen für Bank B handelt es sich um eine iTAN-Liste und eine TAN-Liste; die Bank hat vor kurzem auf indizierte TANs umgestellt.

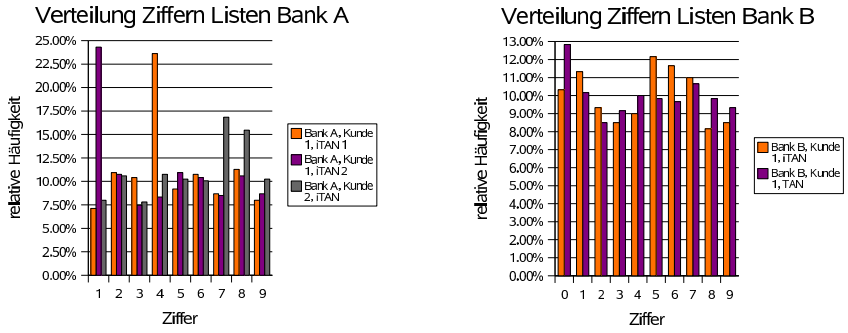

Abbildung 5: Statistische Verteilung von Ziffern in Listen. Bemerkung: Die Grafiken sind unterschiedlich skaliert.

Bemerkenswert bei der relativen Häufigkeit für die Listen von Bank A ist, dass jede der vorliegenden TAN-Listen der Bank "Ausreißer"-Ziffern mit deutlich höhere Trefferquoten

besitzt. Bei den Listen von Kunde 1 wird jeweils eine Ziffer mit annähernd doppelter relativer Häufigkeit gewählt, die konkrete Ziffer variiert allerdings mit den Listen. Wir konnten keinen Zusammenhang zwischen dieser Ziffer und anderen Merkmalen der Listen (Kundennamme, Listennummer etc.) herstellen.

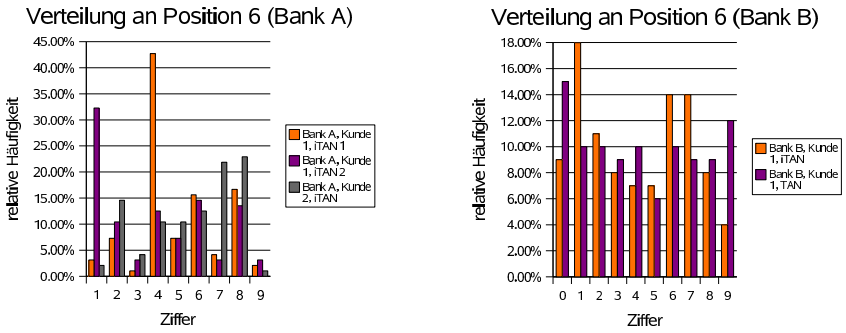

Abbildung 6: Statistische Verteilung der Ziffern in Position 6. Bemerkung: Die Grafiken sind unterschiedlich skaliert.

In Abbildung 6 sind die Verteilungen der Ziffern in Position 6 für die Listen dargestellt. Statistisch auffällig —außer der Verteilungen der Listen von Bank A— erscheint die Schwankung der Werte für die iTAN-Liste von Bank B (linker Balken), beispielsweise wird die Ziffer 1 an Position 6 in 18% aller Fälle getroffen. Dies kann aber noch im Rahmen von statistischem Rauschen liegen.

4 Experimente

Wir haben obige Überlegungen zu den statistischen Merkmalen in ein Programm zur Vorhersage der (i)TANs umgewandelt. Dieses Programm haben wir gegen die fünf vorliegende (i)TAN-Listen getestet.

4.1 Versuchsdurchführung

Zur Approximation der Vorhersagewahrscheinlichkeit für die gegebenen (i)TAN-Listen bestehend aus $n \in \{96, 100\}$ (i)TANs wiederholen wir folgende Schritte 100-mal:

1. Wir wählen 3 TANs aus der Liste aus, die als “Challenge”-Kandidaten dienen. Dies entspricht der allgemein üblichen Begrenzung der Fehlversuche bei solchen Online-Banking-Verfahren, bevor der Zugang gesperrt wird. Die Wahl erfolgt uniform aus der Menge aller n Zahlen (wobei wir somit zu Gunsten der Banken annehmen, dass die TANs —wie bei indizierten Verfahren wünschenswert— in echt zufälliger Reihenfolge abgefragt werden).

2. Die übrigen $n - 3$ TANs dienen als Quelle für den Angriff. Aus diesen Daten wird zunächst eine Statistik für die relativen Häufigkeiten, Renyi-Entopien, Korrelationen etc. berechnet.

3. Zur Approximation der Erfolgswahrscheinlichkeit unseres Verfahrens wiederholen wir nun ebenfalls 100-mal folgenden Versuch (so dass wir insgesamt $100 \cdot 100 = 10.000$ Iterationen ausführen):

   (a) Unser Algorithmus berechnet aufgrund der Statistik —und in jeder Iteration unabhängig— einen TAN-Vorhersageversuch, bestehend allerdings nur aus 4 Ziffern und zwei "Jokern" (die Wahl der Positionen der Joker kann variieren). Durch die beiden Joker-Positionen können wir die Erfolgswahrscheinlichkeit leichter approximieren (siehe unten).

   (b) Wir vergleichen die 3 Challenge-TANs mit der Vorhersage und werten einen Erfolg für den Angreifer, wenn mindest eine der Challenge-TANs mit dem Rateversuch an den 4 Zifferpositionen übereinstimmt (also 4 der 6 Ziffern korrekt geraten wurden).

   Wir bestimmen aus den Ergebnissen in Schritt 3b eine Approximation p für die Vorhersagewahrscheinlichkeit: Sei E die Anzahl der Erfolge in den 100 Wiederholungen in Schritt 3b. Dann approximiert $E/100$ die Erfolgswahrscheinlichkeit des Angreifers, 4 der 6 Ziffern vorherzusagen. Dann ist aber dieser Wert $E/100$ dividiert durch $(\#\text{Ziffern})^2 \in \{81, 100\}$ eine Approximation p für die Erfolgswahrscheinlichkeit, *alle* Ziffern vorherzusagen, wenn die beiden verbleibenden Ziffern zwischen 1 und 9 bzw. 0 und 9 an den Joker-Positionen mit Wahrscheinlichkeit $\frac{1}{9^2} = \frac{1}{81}$ bzw. $\frac{1}{10^2} = \frac{1}{100}$ einfach geraten werden.

Als Vorhersagewahrscheinlichkeit berechnen wir nun den Durchschnitt über alle ermittelten Erfolgswahrscheinlichkeiten p in den 100 Wiederholungen der Schritte 1 bis 3. Insbesondere wird der Angreifer in jeder dieser Wiederholungen zurückgesetzt, und ihm liegen damit keine Ergebnisse der bisherigen Wiederholungen und auch nicht die 3 jeweils verwendeten Challenge-TANs vor; dies entspricht dem Szenario in unserem Trojaner-Beispiel.

Durch die beiden Joker-Positionen erhalten wir trotz der relativ geringen Anzahl Wiederholungen der Schleife in Schritt 3 eine statistisch stabile Aussage über die Erfolgswahrscheinlichkeit zur Vorhersage der 6 Ziffern. Verbesserte Angriffe, die auch die beiden letzten Ziffern noch aus der Statistik der Stichprobe vorherbestimmen statt zu raten, könnten eventuell eine noch höhere Wahrscheinlichkeit erzielen.

4.2 Auswertung

Die triviale —und für echt zufällig erzeugte TANs aus 10 Ziffern auch beste— Angriffsmethode, durch reines Raten eine der 3 Challenge-TANs zu bestimmen, hat die Erfolgswahrscheinlichkeit

$$p_{\text{rnd}} = \sum_{i=1}^{3} \binom{3}{i} (10^{-6})^i (1 - 10^{-6})^{3-i} \approx 3 \cdot 10^{-6}.$$

Daher sind wir an der Qualität unseres Angriffs im Vergleich zu diesem maximalen Sicherheitsniveau interessiert. Mit den Experimenten erhielten wir die in Abbildung 7 angebenenen Approximationen für die Vorhersagewahrscheinlichkeiten und den erhöhten Faktor im Vergleich zur echt zufällig erzeugten TANs.

Der Verbesserungsfaktor für die iTAN-Liste 1 von Bank A ergibt sich anscheinend nicht nur aus der auffälligen Verteilung an Position 6 (Ziffer 4 mit ca. 40%). Zum Vergleich betrachte man die Strategie, als letzte Ziffer an Position 6 immer die 4 zu raten, und die restlichen

Beschreibung	Erfolgswahrscheinlichkeit (experimentell)			Faktor		
Bank A, Kunde 1, iTAN 1	$p_{A,1,1}$	$=$	$54,32 \cdot 10^{-6}$	$\frac{p_{A,1,1}}{p_{\text{rnd}}}$	$\approx$	**18,10**
Bank A, Kunde 1, iTAN 2	$p_{A,1,2}$	$=$	$22,22 \cdot 10^{-6}$	$\frac{p_{A,1,2}}{p_{\text{rnd}}}$	$\approx$	**7,40**
Bank A, Kunde 2, iTAN	$p_{A,2}$	$=$	$11,11 \cdot 10^{-6}$	$\frac{p_{A,2}}{p_{\text{rnd}}}$	$\approx$	**3,70**
Bank B, Kunde 1, iTAN	$p_{B,1,i}$	$=$	$2 \cdot 10^{-6}$	$\frac{p_{B,1,i}}{p_{\text{rnd}}}$	$\approx$	**0,66**
Bank B, Kunde 1, TAN	$p_{B,1}$	$=$	$5 \cdot 10^{-6}$	$\frac{p_{B,1}}{p_{\text{rnd}}}$	$\approx$	**1,66**

Abbildung 7: Experimentell ermittelte Erfolgwahrscheinlichkeit des Programms. Faktor gibt an, wieviel häufiger die Vorhersage im Vergleich zum optimalen Sicherheitsniveau (Faktor **1**) gelingt.

5 Ziffern uniform zwischen 1 und 9 zu wählen. Diese Strategie hätte eine Erfolgswahrscheinlichkeit von

$$p \approx 3 \cdot \tfrac{2}{5} \cdot 9^{-5} = 20,32 \cdot 10^{-6}$$

und wäre damit nur den Faktor ca. $6,77$ besser als p_{rnd}, während das Programm hier (experimentell) einen Faktor von ca. $18,10$ erzielt.

Die Faktoren $0,66$ und $1,66$ für Bank B zeigen, dass hier die erfolgreichen Angriffe auf Bank A nicht greifen. Im Fall $0,66$ ist der Angriff sogar schlechter als der triviale Angreifer, der einfach alle Ziffern rät. Beide Faktoren liegen allerdings unseres Erachtens nach im Bereich der insignifikanten Abweichung.

5 Fazit

Der geringe Stichprobenumfang lässt streng genommen keine verlässliche Aussage über die allgemeine Qualität der (i)TAN-Listen der betreffenden Banken zu. Die statistischen Auffälligkeiten lassen sich jedoch nur mit sehr kleiner Wahrscheinlichkeit durch zufällige Störungen erklären. Wir weisen ferner darauf hin, dass hier nur eine "Black-Box-Analyse" vorliegt: uns waren keine Informationen über die Algorithmen zur Erzeugung der TANs bekannt. Da wir zusätzlich die Angriffe nicht optimiert haben, könnten die tatsächlichen Vorhersagewahrscheinlichkeiten daher insgesamt noch höher ausfallen.

Unabhängig von unseren Resultaten hat Felix "FX" Lindner vergleichbare Auffälligkeiten für TAN-Listen der Citibank festgestellt [Lind06].[1] Bemerkenswert in diesen Fällen ist, dass die Generierung der TAN-Listen vollständig in der Verantwortung der Banken liegt. Folglich sind selbst für einen gut informierten Benutzer, der sich beispielsweise geeignet gegen Phishing-Angriffe schützt, solche schwachen TAN-Listen außerhalb seiner Kontrolle.

Literatur

[Club97] Chaos Computer Club: EC-Karten Unsicherheit. *In: Datenschleuder #59*, siehe `http://ds.ccc.de/` (Juni 1997).

[Lind06] F. Lindner: Citibank wuerfelt nicht. *In: Heise Security*, siehe `http://www.heise.de/security/artikel/78939` (Oktober 2006).

[1] Wir danken den Gutachtern der D·A·CH Security 2007 für diesen Hinweis.

[News05] Heise News: iTAN-Verfahren unsicherer als von Banken behauptet. *In: Heise News*, siehe `http://www.heise.de/newsticker/meldung/63249` (August 2005).

A Shannon-, Renyi-, und Min-Entropie

Zur besseren Verständlichkeit der statistischen Analyse wiederholen wir zunächst einige elementare Fakten über die mathematische Präzisierung des Zufälligkeitsbegriffs, der Entropie.

Entropie ist ein Maß für die Ungewissheit oder auch die Zufälligkeit von Zufallsvariablen. Es gibt verschiedene Entropie-Skalen, die unterschiedliche Maße für die Zufälligkeit ausdrücken. Die drei relavantesten Entropien für uns sind die Shannon-Entropie, die Renyi-Entropie und die Min-Entropie.

Die *Shannon-Entropie* einer Zufallsvariablen X, definiert als $H(X) = -\sum_x (\mathrm{Prob}\,[X = x] \cdot \log_2 \mathrm{Prob}\,[X = x])$, misst, wieviel Bits zur Beschreibung eines Ausgangs eines Zufallsexperiments benötigt werden. Sie ist maximal, wenn X uniform verteilt ist. Eine optimales Verfahren zur Erzeugung von TAN-Listen sollte daher möglichst hohe Shannon-Entropie haben. Eine rein zufällig gewählte TAN von sechs Ziffern hat die Shannon-Entropie $-\log_2 10^{-6} \approx 19,93$, so dass zur Vorhersage ca. 20 Bits erraten werden müssen. Durch die Beschränkung auf die Dezimalzahlen zwischen 1 und 9 sinkt die maximale Shannon-Entropie auf $-\log_2 9^{-6} \approx 19,02$, also ca. 19 Bits.

Die *Renyi-Entropie* von X, $H_2(X) = -\log_2 \sum_x \mathrm{Prob}\,[X = x]^2$, ist ein Maß für die Kollisionswahrscheinlichkeit der Zufallsvariablen X. Sie misst, wie groß die Wahrscheinlichkeit ist, beim zweimaligen Ziehen den selben Wert zu erhalten. In unserem Zusammenhang sind wir an Kollisionen zwischen einer von der Bank erzeugten TAN und einer von uns geratenen TAN interessiert. Da für die Renyi-Entropie im Vergleich zur Shannon-Entropie stets $H_2(X) \leq H(X)$ gilt, mit Gleichheit genau dann, wenn X uniform verteilt ist, ist die Ungewissheit gemäß Renyi-Entropie für nicht uniform verteilte X kleiner als die der Shannon-Entropie.

Die *Min-Entropie* von X, $H_\infty = -\log \max_x \mathrm{Prob}\,[X = x]$, beschreibt die optimale Vorhersagestrategie für eine Zufallsvariable: Man rate den Wert, der mit der größten Wahrscheinlichkeit von X getroffen wird. In unserem Zusammenhang ist die Min-Entropie also ein Maß für den besten Rateversuch einer TAN. Es gilt stets $H_\infty(X) \leq H_2(X)$ mit Gleichheit nur für uniform verteilte Zufallsvariablen X.

Die Min-Entropie und die Renyi-Entropie sind in userem Angriffsmodell allerdings nicht unmittelbar geeignet. Da wir die Verteilung einer *kompletten* TAN $T \in \{1, 2, \ldots, 9\}^6$ aus sechs Ziffern nicht kennen, können wir den Wert mit höchster Wahrscheinlichkeit nicht bestimmen. Für die untersuchte TAN-Liste von Bank A beispielsweise kennen wir zwar die (statistische Approximation der) Min-Entropie der Zufallsvariablen $X \in \{1, 2, \ldots, 9\}$, die die Verteilung einer *einzelnen* Ziffer beschreibt. Diese beträgt nämlich $H_\infty = -\log \mathrm{Prob}\,[X = 4] = -\log 23,61\% \approx 2$, da die Ziffer 4 am häufigsten getroffen wird.[2] Allerdings tritt beispielsweise die TAN 444 444 (bestehend aus den besten Rateversuchen für die einzelnen Ziffern) nie auf.

Die Renyi- und Min-Entropie für die einzelnen Ziffern oder auch für einzelne Positionen —so wie in Abbildung 3 dargestellt— vernachlässigen Abhängigkeiten zwischen den Ziffern. Deren Bestimmung liefert uns daher zunächst nur eine Aussage über die Zufälligkeit der TAN-Zahlen: Für sehr gut erzeugte Zahlen sollte diese Entropie dicht an der Shannon-Entropie liegen; sonst signalisiert eine abweichende Min- oder Renyi-Entropie die Nicht-Uniformität der Verteilung. Werden solche Abweichungen für einzelne Ziffern oder Positionen dann für

[2] Zum Vergleich: für echt zufällige Dezimalzahlen ist die Min-Entropie $\log 10 \approx 3,32$.

konkrete Angriffe ausgenutzt, muss der Erfolg solcher Heuristiken daher experimentell verifiziert werden.

B Chernoff-Schranke

Mittels der Chernoff-Schranken kann man bei einer Reihe von Experimenten die zufällige Abweichung vom erwarteten Wert abschätzen. Wirft man beispielsweise m-mal eine faire Münze, so erwartet man im Durchschnitt $\frac{1}{2}m$-mal den Ausgang "Kopf". Die Chernoff-Schranke liefert nun die Wahrscheinlichkeit, beispielsweise $\frac{3}{4}m$-mal "Kopf" zu erhalten. Dabei zeigt sich, dass starke Abweichungen vom Erwartungswert sehr unwahrscheinlich sind:

> **Chernoff-Schranke:** Seien $X_1, X_2, \ldots, X_m$ unabhängige Zufallsvariablen mit $\text{Prob}\,[X_i = 1] = p$ und $\text{Prob}\,[X_i = 0] = 1 - p$ für $i = 1, 2, \ldots, m$. Dann gilt für alle Konstanten $c \in (0, 1]$:
>
> $$\text{Prob}\left[\sum_{i=1}^{m} X_i \geq pm + cm\right] \leq e^{-2c^2 m}.$$

Betrachten wir als Beispiel die Abschätzung $10^{-5,22}$ aus Abschnitt 3.1, dass in einer TAN-Liste aus $6 \cdot 96 = 576$ echt zufällig gewählten Ziffern zwischen 1 und 9 eine Ziffer mehr als doppelt so häufig wie erwartet auftritt. Wir betrachten zunächst die Wahrscheinlichkeit für eine feste Ziffer (also z.B. dass die 5 doppelt so oft vorkommt). In diesem Fall sei X_i die Zufallsvariable, die 1 ist, wenn die i-te der $m = 576$ Ziffern gleich unser vorgegebenen Ziffer ist, und 0 sonst. Somit ist $p = \text{Prob}\,[X_i = 1] = \frac{1}{9}$. Im Erwartungswert treffen wir daher diese Ziffer $\sum X_i = pm = 64$ mal.

Um die Wahrscheinlichkeit zu messen, dass unsere Ziffer doppelt so häufig wie erwartet auftritt, setzen wir in der Chernoff-Schranke $c = p = \frac{1}{9}$ und vergleichen somit $\sum X_i$ mit $pm + cm = 2pm$. Damit ergibt sich:

$$\text{Prob}\left[\sum_{i=1}^{m} X_i \geq pm + cm\right] \leq e^{-2c^2 m} \leq e^{-14,22}.$$

Die Wahrscheinlichkeit, dass *irgendeine* der 9 Ziffern doppelt so oft auftritt, beträgt daher maximal $9 \cdot e^{-14,22} \leq 10^{-5,22}$.