Passwörter taugen nichts

mrmcd100b, 21. - 23.7.06

Hanno Böck, http://www.hboeck.de/

Passwörter?

- geheim
- gott
- linux
- Name von Freundin, Mutter, Kind

flirtlife.de

• 123456	1375	1.4
• ficken	404	0.4
• 12345	367	0.4
• hallo	362	0.4
• 123456789	260	0.3
• schatz	253	0.3
• 12345678	215	0.2
• daniel	215	0.2

Gute Passwörter

- c@|4(aj.:*
- jgx.~0=:"2
- $%@gvg`4$!
- |x-$d"m1uz
- fm9m,5e9v#

- pwgen -cAnys 10 5

Je Zugang ein Passwort?

- Linux-Login, GPG-Passwort, Crypto-Partition
- Webmail auf gmx.de, web.de
- >10 schlecht administrierte phpBB-Foren
- Wikipedia, icq, jabber, Google, flickr
- Mein Blog, mein Wiki, meine Bildergalerie
- ssh-Accounts, Freenode-Registrierung
- Cisco-VPN an der Uni

Phishing

Sparkasse

Sparkasse

Sehr geehrte Kundin, sehr geehrter Kunde,

wir freuen uns Ihnen mitzuteilen, dass Online-Banking der Sparkasse jetzt noch sicherer ist!

Weltweit gilt das TAN-Verfahren als eines der sichersten Legitimations-Verfahren für Online-Bankgeschäfte. Dennoch gab es in letzter Zeit immer wieder Versuche, auf betrügerische Art und Weise TAN-Nummern von Kunden zu erhalten und das Geld ins Ausland zu überweisen.

Zur Zeit ist uns das Verfahren, die die Betrüger für die Entwendung der TAN-Listen benutzen, nicht bekannt.

Um Ihre Online-Geschäfte noch besser zu schützen, führt die Sparkasse zusätzliche Schutzmassnahmen ein.

Fuer den gewöhnlichen Schutz durch nicht nummerierte TAN-Liste haben Sie zwei gültige TAN einzugeben. Wenn sie den neuen iTAN Verfahren benutzen, müssen Sie 20 iTAN eingeben.

Nutzer, die den iTAN-Schutz verwenden, gehen Sie bitte auf diesen Link: https://www.sparkasse.de/verify/itan.do

Kunden, die den gewöhnlichen Schutz durch TAN-Liste verwenden, gehen Sie bitte auf diesen Link: https://www.sparkasse.de/verify/tan-listen.do

Achtung! Wir bitten unsere Kunden um Verständnis für diese Überprüfung.

Alle Sparkassenkonten, die nicht innerhalb eines Tages authentifiziert werden, werden gesperrt!

Passwort-Hashes

- Rainbow-Tables
  Lösung: Salt
- Brute Force-Angriffe, bspw. John the Ripper

Passwort Policy

- Mindestens 10 Zeichen
- Jeweils mind. 10% Buchstaben, Zahlen und Sonderzeichen
- Keine zwei gleichen Zeichen hintereinander

Beispiele?

- a1#a1#a1#a1#
- g3#3img3#3im
- 1q“W3e$R5t
- 1234abcd!“§$

Sicherheitsparameter

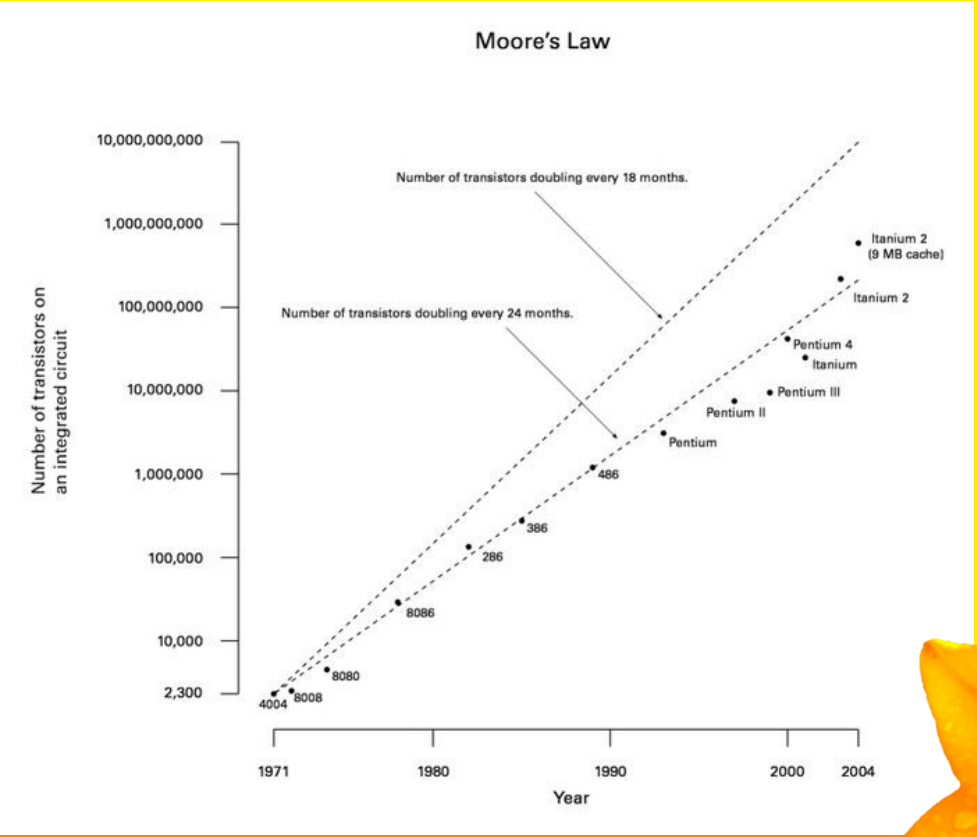
- Szenario Schlüssellängen
- Annahme: Angreifer (NSA o. ä.) hat deutlich höhere Rechenkapazitäten
- Skalierung der Sicherheitsparameter

Sicherheitsparameter

- Beispiel: RSA-1024 evtl. angreifbar, Umstieg auf RSA-2048/4096 machbar.
- SHA-1 durch SHA-256/512 ersetzbar.

Moore's Law

- The complexity for minimum component costs has increased at a rate of roughly a factor of two per year



Thesen

- Nicht skalierbare Sicherheits-parameter schlechte Idee
- Evolution hält sich nicht an Moore's Law
- Skalierbarkeit von Passwörtern stark begrenzt, Skalierbarkeit von Angriffen nicht

Alternativen?

- Client-Zertifikate
- ssh-Public-Keys
- ssl-Client-Zertifikate
- HBCI mit Keyfile, Chipkarte
- Smartcards generell

SSL/TLS-Clientzertifikate

- Authentifizierung in Webanwendungen möglich
- Kaum genutzt
- Login bei CAcert möglich

HBCI

- HBCI ist keine so schlechte Idee, insb. mit Chipkarte
- Freie Implementierungen: aqbanking, moneypenny
- HBCI mit PIN/TAN, iTAN: Grausamer Unfug!

Crypto-Cards

- FSF-Fellowship: 1024-Bit
- 2048/4096-Bit-Karten teuer
- Prinzipiell GPG, SSH, SSL/X.509 problemlos möglich

Cardreader

- Schonmal im Saturn einen Cardreader gekauft?
- Treiber?
- Cardreader kaum per default erhältlich

Chipkarte passwortgeschützt?

- These: Eine Chipkarte ohne Passwort ist besser als ein Passwort alleine
- Jeder Angriff auf Chipkarte erfordert physischen Zugriff, Angriffe auf Passwörter meist passiv und virtuell

Beyond Chipcards

- Biometrie
- RFID
- Trusted Computing
- ?

Biometrie

- Vollständig neuartige Probleme („Schlüsselklau“)
- Massive Privacy-Implikationen
- Sicherheit ebenfalls nicht beliebig skalierbar
- Schlüsselspuren

RFID

- Neue Probleme (Auslesbarkeit)
- Privacy
- Kaum Sicherheitsvorteile
- Vorteile nur im Anwendungskomfort

Trusted Computing

- Bekannte Probleme, Privatsphäre, Kontrollierbarkeit
- Praktisch alle für den Nutzer sinnvollen Anwendungen von TCG sind auch mit Chipkarten lösbar

Fragen?

Hanno Böck

http://www.hboeck.de