Das Paßwort ist tot …

Lang lebe das Paßwort!

- *Neue Gedanken zu einem alten Thema*
- **GUUG FFG 2008**
- Thomas Maus

thomas.maus alumni.uni-karlsruhe.de

Ein Streifzug durch den Märchenwald der Authentifikation

- Es waren einmal drei Authentifikationsprinzipien
- Der Host ist tot, das Paßwort ist tot und ...
- Paßwort-Qualität? Überraschung!
- Theorie und Praxis – Ein Feldtest
- Ergebnisse und Interpretationen
- Einführung der Paßwortqualitätsmessung
- Und die Moral aus der Geschicht' ...
- Diskussion

Es waren einmal drei Authentifikationsprinzipien

- Gängige Taxonomie der Authentifikation:
  - Wissen – Paßworte, PINs, ...
  - Gegenstände – Schlüssel, SmartCards, ...
  - Biometrie – Fingerabdruck, Iris, Gesicht, ...
- → „Wer bist Du?“ ersetzt durch:
  - „Was weißt Du?“
  - „Was besitzt Du?“
  - „Wie erscheinst Du mir?“
- Eigentliche Kernfrage „Was erlaube ich Dir?“

Wozu Authentifikation?

Namen sind Schall und Rauch ...

- Identifizieren – Sich Vorstellen:
  - *„Macht mir auf, Kinder, euer liebes Mütterchen ist da und hat jedem aus dem Walde etwas mitgebracht.“*
- Authentifizieren – die Identität prüfen:
  - *Die Geißlein riefen: „Zeig' uns erst deine Pfote, damit wir wissen, daß du wirklich unser liebes Mütterchen bist.“ Da legte er die mehlbestäubte Pfote ins Fenster.*
- Autorisieren – Rechte einräumen:
  - *So glaubten sie es wäre wahr und öffneten die Tür …*

„Zeig‘ uns erst Deine Pfote ...“

Authentisieren mit Biometrie

- Biometrie nicht mit Haushaltsmitteln überwindbar?
  - starbug (www.ccc.de)






„Zeig‘ uns erst Deine Pfote ...“

Authentisieren mit Biometrie

- Sicherheitsaspekte des Sensors
  - erfaßt nur kleinen Ausschnitt der Realität
  - Sensor-Arbeitsweise bekannt und manipulierbar

    ➜ Faksimile, Attrappe mit Virus oder Buffer-Overflow ;-)
  - Erfassung systemimmanent unscharf
    - False Negatives / Positives (Fehlabweisung und -annahme)
    - Maximum-Likelihood-Schätzung ➜ FPR und FNR gekoppelt
    - ehrlicher wäre „Grauzone der Ungewißheit“!
    - ergänzende Authentifikationsverfahren zwingend notwendig
  - Sensor liefert Bit-Folge ➜ Standard-Angriffsstrategien

„Zeig‘ uns erst Deine Pfote ...“

Authentisieren mit Biometrie

- Sicherheitsaspekte der Merkmale
  - nicht geheim (vor allem bei breiter Biometrie-Nutzung!)
  - nicht austauschbar (Kompromittierg, Stellenwechsel, …)
  - nur in begrenzter Anzahl je Merkmalsträger verfügbar
  - nicht ablegbar (Urlaub, Zwang, ...)
  - nicht Jeder hat technisch verwertbare Merkmale

    z.B. durch Alter, Beruf, Rasse, Versehrtheit ➜

    Ersatzverfahren zwingend notwendig! Sicherheit?

„Zeig‘ uns erst Deine Pfote ...“

Authentisieren mit Biometrie

- verlagert Risiken in den Personenschutzbereich:
  - Kuala Lumpur, 31.3.2005, Geschäftsmann überfallen
  - Kreditkarten und PINs abgepresst ...
  - Limousinenschlüssel verlangt (Hehlerwert ≈ 75.000$)
  - Problem: Wegfahrsperre biometrisch gesichert ...
  - Zeigefinger mit Machete abgehackt …
  - Quellen:
    - http://news.bbc.co.uk/go/pr/fr/-/2/hi/asia-pacific/4396831.stm
    - 4 weitere Artikel in der New Strait Times & Malay Mail

„Darauf stickte er »7 auf einen Streich«“

Authentisieren mit Gegenständen

- Verfahren sehr unterschiedlicher Stärke
  - RFID-Tags
  - Magnetstreifenkarten
  - TAN-Listen
  - Speicher-Chip-Karten
  - Einmal-Paßwort-Generatoren (unterschiedlicher Stärke)
  - Krypto-Prozessor-Chipkarten
- Gegenstände sind wehr- und hilflos
  - ergänzende Authentifikation zwingend notwendig

„Darauf stickte er »7 auf einen Streich«“

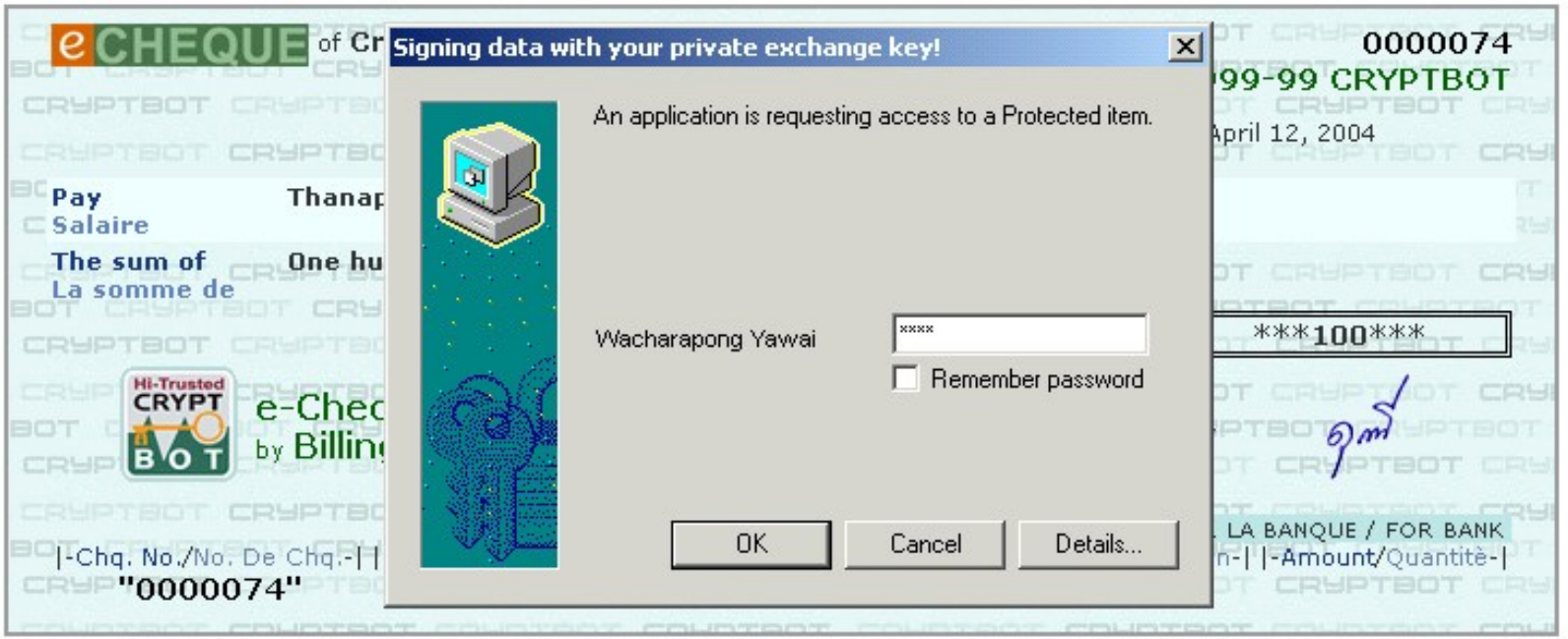
Authentisieren mit Gegenständen

- Krypto-Prozessor-Chipkarten deutlich das stärkste der Verfahren, aber …
  - Anlaß zur Sorge?
  - Welchem Gerät trauen Sie?
  - Warum?
  - Wohin geht die PIN?
  - Wie oft?
  - Computer sind so schnell, schneller als das Auge …

„Darauf stickte er »7 auf einen Streich«“

Authentisieren mit Gegenständen

- Zertifizierte Krypto-Prozessor-Chipkarten sicherlich sehr stark, aber …
  - Sie signieren, was Sie sehen?
  - Die Chipkarte signiert, was Sie sehen?



„Ach, wie gut, daß niemand weiß, daß …“

Authentisieren durch Wissen

- Mythos: Paßworte sind einfache & billige Lösung
  - „jeder kann sich ein Paßwort merken“, oder zwei, oder ein dutzend, oder etliche dutzend – alle 30 Tage neu …
  - korrekte Implementierung nicht trivial: LanMan-Hash
- Wahl guter Paßworte knifflig*
- Paßworte können ausgespäht werden
  - Paßwort/Hash wird (fremden) Systemen mit**geteilt**
  - Social-Engineering, Phishing, Zwang, …
  - Kibitzen, Zuhören, Key-logging, ...

* Hilfe naht

…

„Ach, wie gut, daß niemand weiß, daß ...“

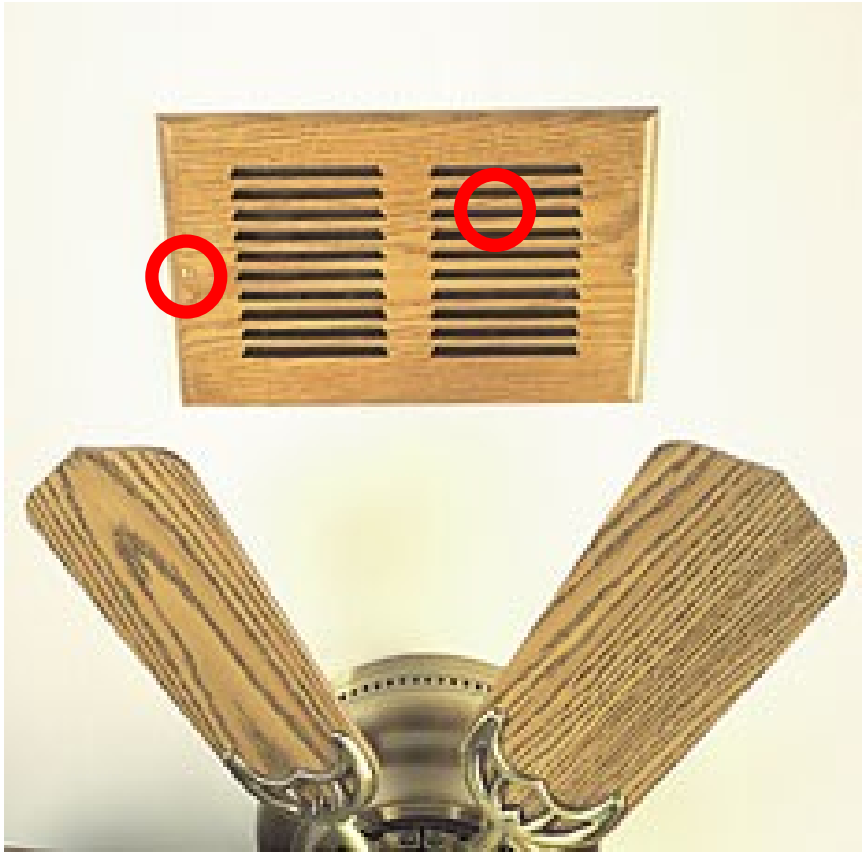
Authentisieren durch Wissen

- Ist dieser Computer eine Gefahr für Ihr Paßwort?

„Ach, wie gut, daß niemand weiß, daß ...“

Authentisieren durch Wissen

- Ist diese Decke eine Gefahr für Ihr Paßwort?



Es waren also einmal drei Authentifikationsprinzipien ...

- Information Kernmoment jeder IT-Authentifikation:
  - Wissen – Information im Gedächtnis
  - Gegenstände – Information in einem Gegenstand
  - Biometrie – Information über den Körper
- Überraschend bei Authentisierung gegenüber IT?
- Entscheidender für das Authentifikationsniveau:
  - Einsatz & Handhabung der Authentisierungsinformation
    - *„Aber Deine Stimme ist rau, du bist der Wolf!“* ≠ Zero-Knowledge
  - Bilaterale Authentifikation

Es waren also einmal drei Authentifikationsprinzipien ...

- Ergänzende Authentifikationsmethoden
  - Kontext – „Wo bist Du, und wann?“
    - gute physische Sicherheit: etwa durch den Werkschutz
    - soziale Kontrolle: Mitarbeitern fällt ungewöhnliches Verhalten auf
    - man kann nicht gleichzeitig an verschiedenen Orten sein
  - Verläßliche Technik – „Welchen Zugang nutzt Du?“
    - beeinflußt Bedrohungslage & Authentizitätsniveau, LAN↔WLAN
  - Gewährsleute – „Wer kennt Dich?“
    - eh‘ unverzichtbar für Initialisierung von Authentifikationmethoden

Der Host ist tot, das Paßwort ist tot und ...

- Paßworte kritischer denn je:
  - Biometrie* und Authentifikationsobjekte bedürfen zwingend der Ergänzung durch Wissen!
  - Authentifikationsmittel wie SSH- oder PGP-Private-Keys sowie Client-Certificates benötigen „Pass-Phrases“
  - Festplatten- und Dateisystemverschlüsselungen breiten sich aus und benötigen meist „Pass-Phrases“

→ intensiveren Angriffen länger widerstehen!

*Biometrie ist tot (IMHO) …

Paßwort-Qualität?
Überraschung!

- Schutz Dictionary-, Rainbow-, Brute-Force-Angriff?
  - Paßwort schwierig zu raten, also unvorhersagbar
  - Informationstheoretisches Maß: Entropie
- Was ist Entropie?
  - $H=-\sum p_i \cdot \log_2(p_i)$
- Jeder kennt und nutzt sie ...
  - Nachnamen dieses Zuhörers da raten, 3 Versuche
  - Warum nicht „Boltzmann“, „Shannon“ und „Wiener“?

Paßwort-Qualität?

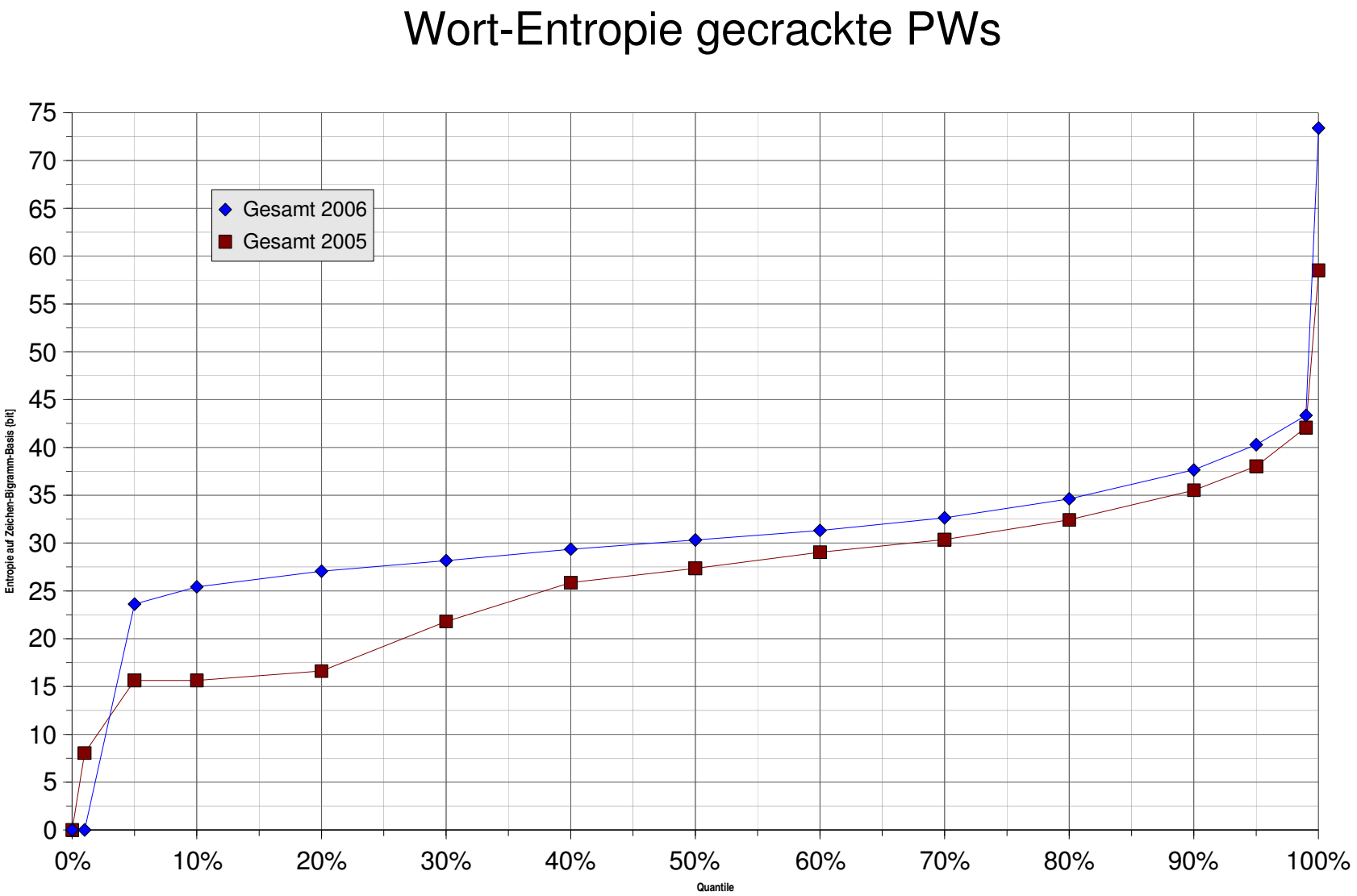
Entropie und Sprache

- Welche Buchstaben bei „Hangman“ zuerst?
- Die Entropie natürlicher Sprache?
  - 4,7 bit/Zeichen – gleichverteiltes Alphabet
  - ≈4 bit/Zeichen – Schriftsprache zeichenweise betrachtet
  - ≈3,9 bit/Zeichen, Basis Zeichenpaare
  - ≈1,9 bit/Zeichen, Basis Wort
  - ≈0,6 bit/Zeichen, Basis kompletter Kontext
  - N Bit Entropie ≙ so zufällig wie N Münzwürfe
- Überraschung: Entropie hängt vom Modell ab!

Theorie und Praxis – Ein Feldtest

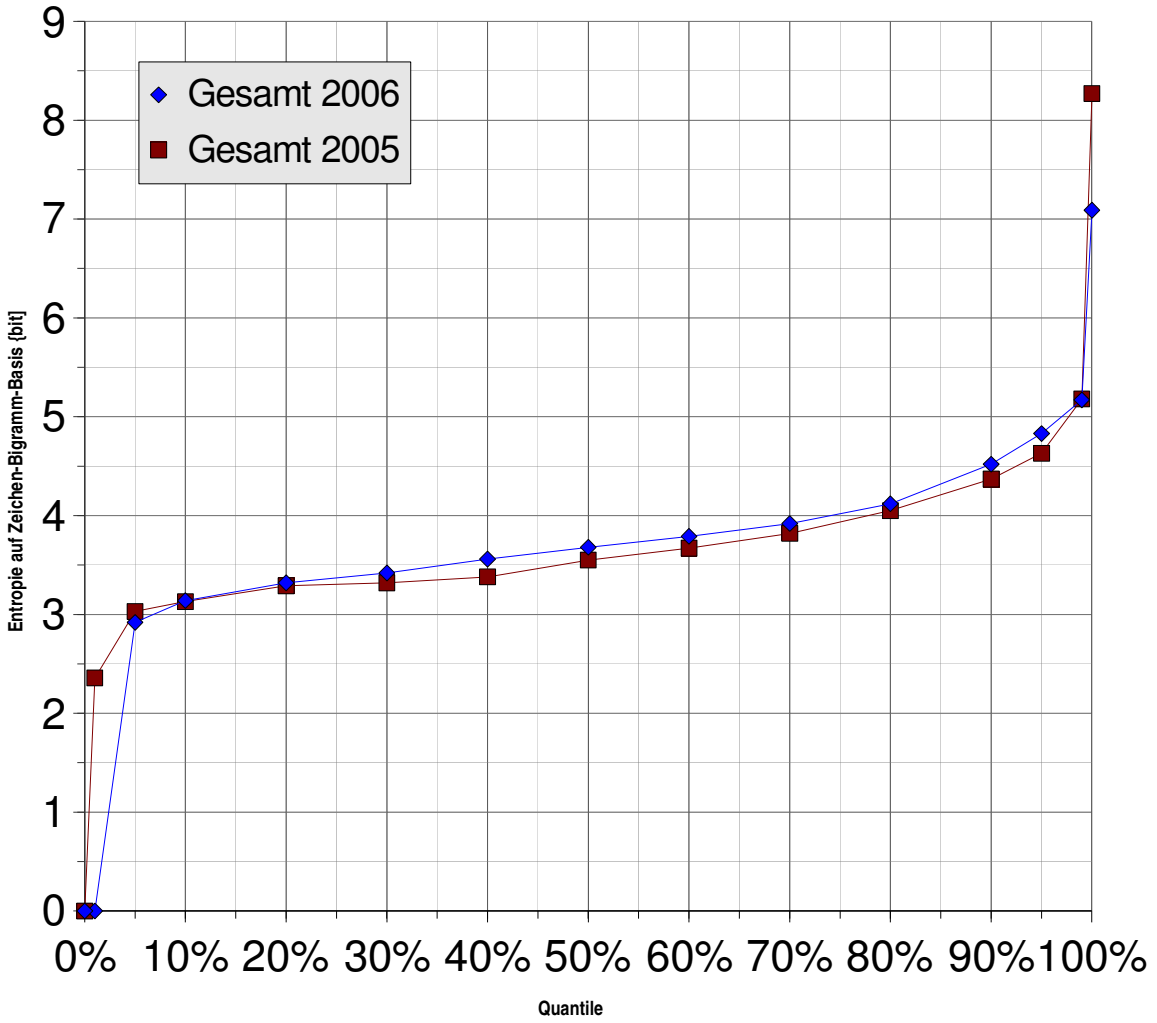
- 2 Paßwort-Audits gegen PW-Hashes (>200.000)
  - Audit 2005 **vor** Durchsetzung Password-Policy
  - Audit 2006 **nach** Durchsetzung Password-Policy
  - Glücksfall: Auswirkung Password-Policy prüfbar!
- typische Password-Policy
  - mindestens 8 Zeichen
  - mindestens je 1 Groß-, Klein-, Nicht-Buchstaben*
  - maximal 30 Tage Lebensdauer

Ergebnisse und Interpretationen

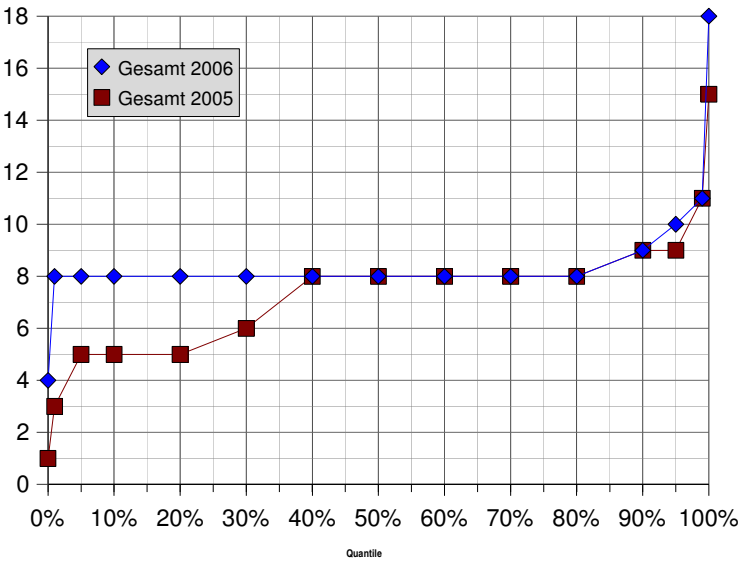


Ergebnisse und Interpretationen

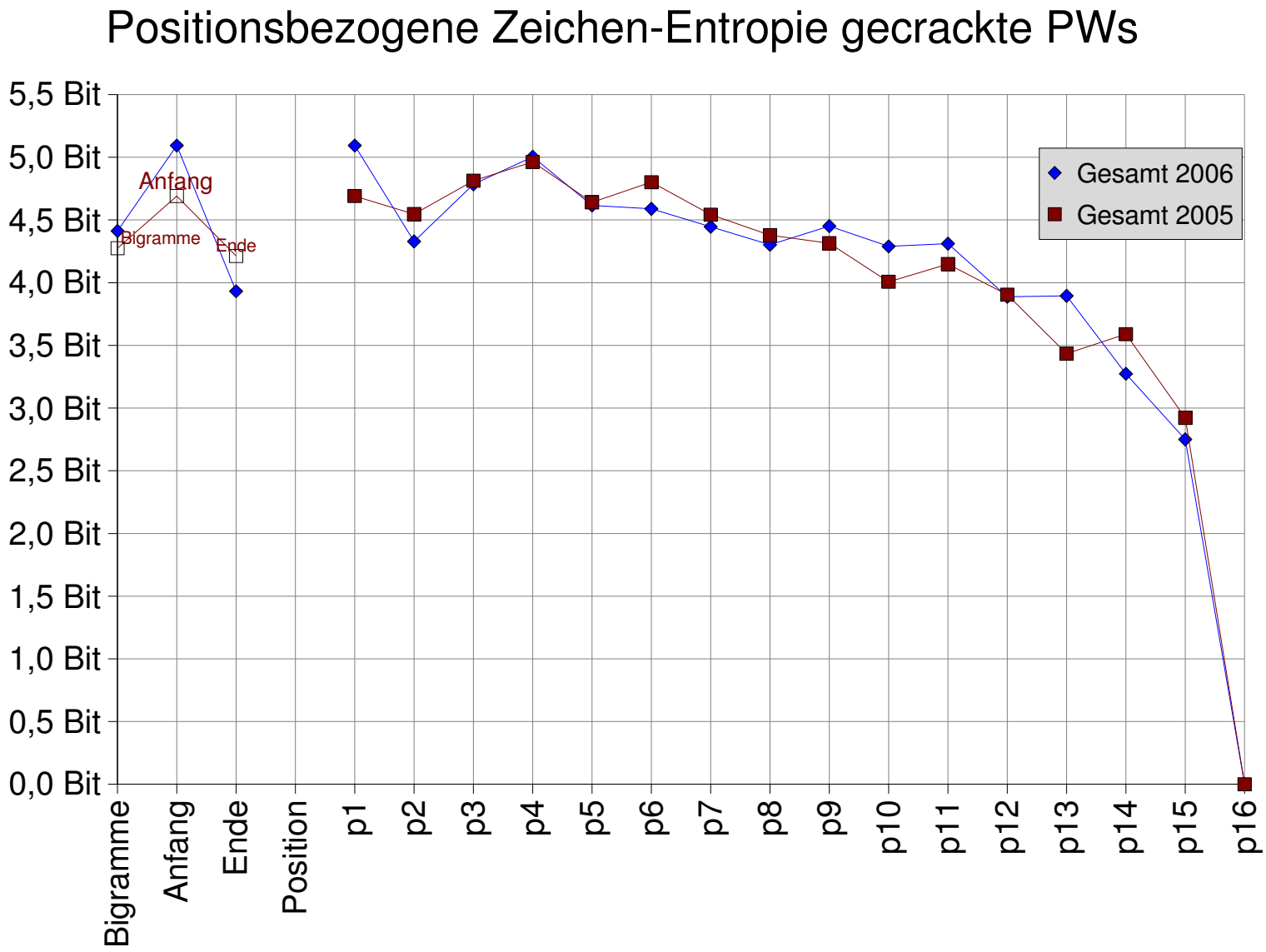
Zeichen-Entropie gecrackte PWs



Längenverteilung gecrackte PWs



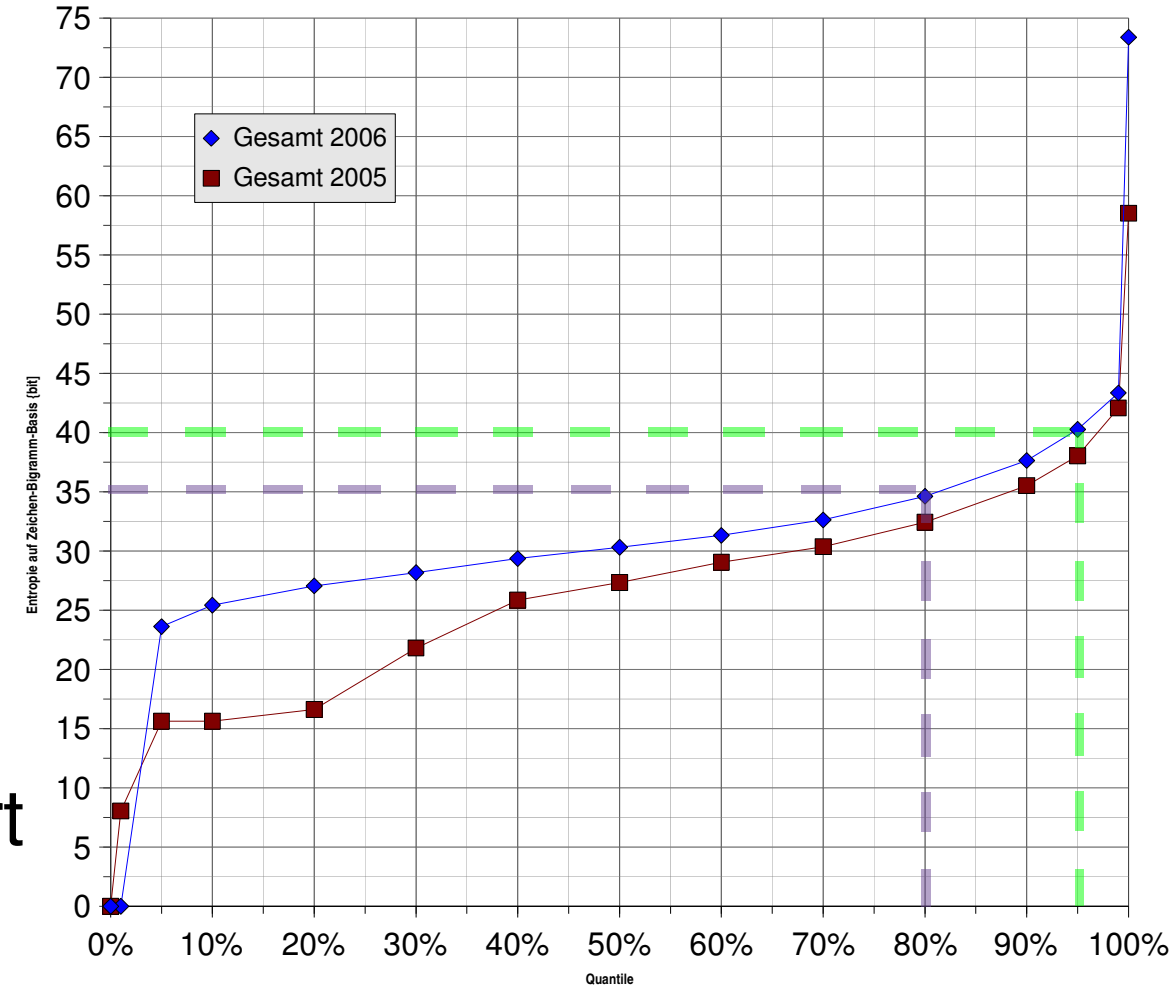
Ergebnisse und Interpretationen



Einführung der Paßwortqualitätsmessung

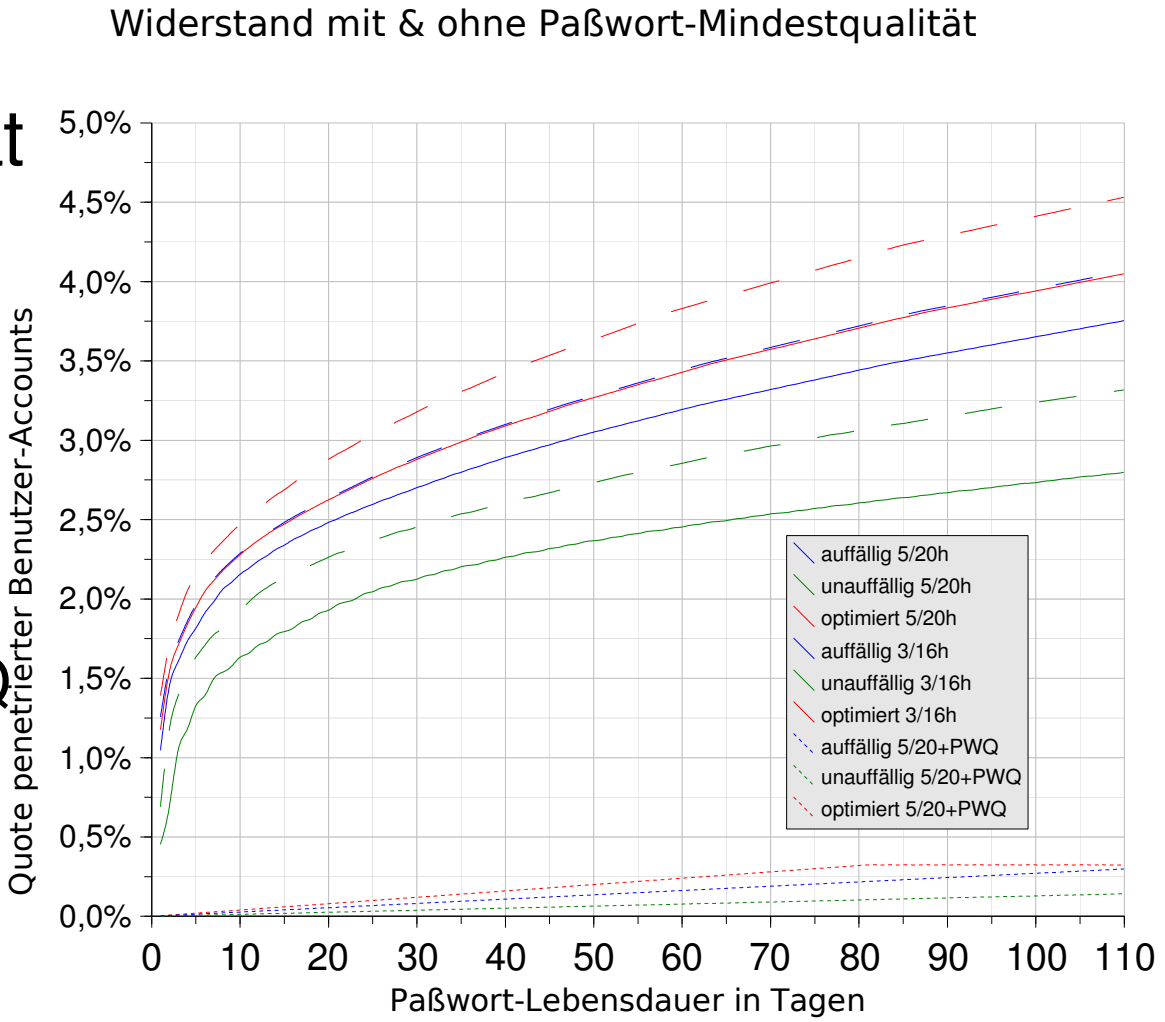
- Mindestqualität
  - statt
    - Mindestlänge
    - Komplexitätsregel
  - 35 Bit vermeidet
    - 80% Cracks
  - 40 Bit vermeidet
    - 95% Cracks
  - maßgeschneidert für Krypto-Keys!

Wort-Entropie gecrackte PWs



Einführung der Paßwortqualitätsmessung

- Lebensdauer
  - ohne PW-Qualität
    - 5 Tage zuviel ...
    - ob 30 oder 100 ...
  - mit PW-Qualität
    - fast frei gestaltbar
    - Idee: je nach PWQ
  - definierbare Schutzdauer für Krypto-Keys!



Ein Prototyp zur Paßwortqualitätsmessung

- Derzeit rein Web-Browser-basierte Client-Lösung
- Erfolgreicher Testlauf mit Blue- und White-Collars
- Verprobt für verschiedene europäische Sprachen
- Berücksichtigung von Key-Board-Patterns
- Berücksichtigung von Kontextinformationen

Ein Prototyp zur Paßwortqualitätsmessung

Geben Sie Ihr Test-Paßwort unten an:

Verdeckte Paßwort-Eingabe

Offene Paßwort-Eingabe

MiesesBeispiel

Optionale Kontext-Informationen

Hiermit kann beispielweise gegen die Benutzerkennung, Standortdaten, persönliche Daten oder auch das vorangegange Passwort korreliert werden ...

Verdeckte Kontext-Eingabe

Offene Kontext-Eingabe

Schätzung der Paßwort-Qualität

39.51 Bit

2.82 Bit/Zeichen

14 Paßwortlänge

Entropie-Schätzungen auf Basis verschiedener Modelle

46.71 Bit – Paßwort, Zeichenpaare, von links nach rechts

49.52 Bit – Paßwort, Zeichenpaare, von rechts nach links

51.17 Bit – Paßwort rückwärts, Zeichenpaare, von links nach rechts

58.93 Bit – Paßwort rückwärts, Zeichenpaare, von rechts nach links

67.04 Bit – als Anfangsbuchstaben

79.25 Bit – Tastaturmuster

Mali für Kontext- und Auto-Korrelation

7.20 Bit – Malus für Kontext- oder Auto-Korrelation

Gewichte zur Berechnung der Korrelationsmali

0.2 linearer Faktor für Korrelationslänge (0.1)

0.1 quadratischer Faktor für Korrelationslänge (0.1)

„Und die Moral aus der Geschicht' ...“

Fazit

- Kein Authentifikationsallheilmittel in Sicht
- Paßworte bleiben uns wohl noch lange erhalten
- Wertdichte von Paßworten steigt eher
- Einige tradierte Paßwortregeln fragwürdig
- → Paßwortsicherheit muß sich der Realität stellen
- Widerstandskraft der Paßworte steigern
- Vorhersagbare und messbare Sicherheit
- Werkzeuge, z.B. Password-Quality-Checker

Vielen Dank für Ihre Aufmerksamkeit!

- **Fragen?**
- **Diskussion …**

- Kontakt für Ihre Kritik & Fragen

thomas.maus alumni.uni-karlsruhe.de