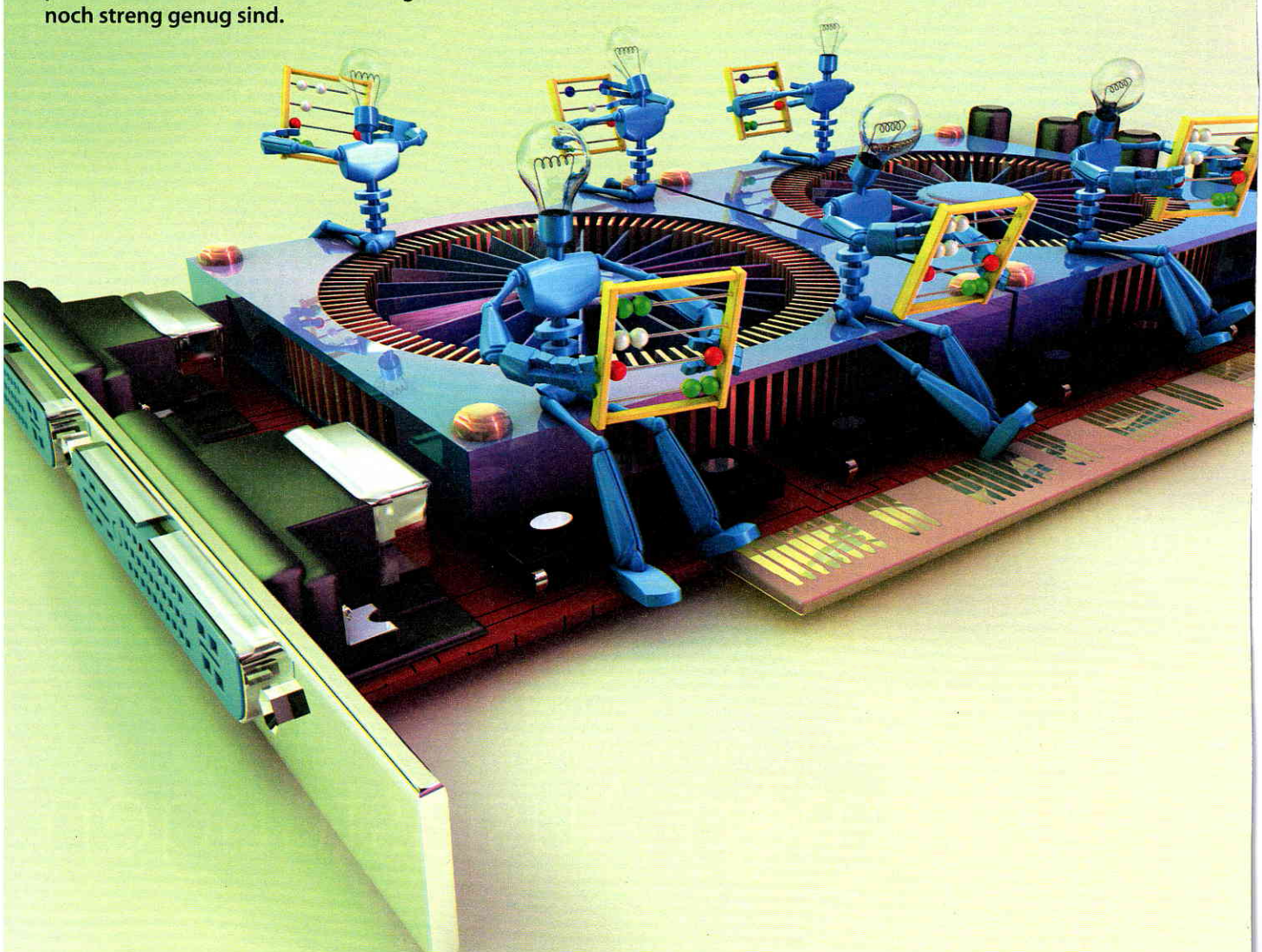
Stefan Arbeiter, Matthias Deeg

Bunte Rechenknechte

Grafikkarten beschleunigen Passwort-Cracker

Auch Passwortknacker profitieren von der hochgezüchteten Rechenleistung moderner Grafikprozessoren. Höchste Zeit zu prüfen, ob die Richtlinien für die Vergabe sicherer Passwörter noch streng genug sind.



Schon lange dienen Passwortknackprogramme nicht nur Kriminellen, sondern sind bei Gedächtnislücken, forensischen Analysen und in der Strafverfolgung oft die einzige Möglichkeit, an ein unbekanntes Passwort zu gelangen. Anders als die Passwörter von Verschlüsselungsprogrammen wie PGP oder TrueCrypt liegen Anmeldekennwörter und Passwörter zur Authentifizierung im Netzwerk in der Regel als Hash-Werte vor, aus denen sich die ursprünglichen Passwörter nicht wieder berechnen lassen.

Passwort-Cracker rücken den Hashes mit Hilfe verschiedener Verfahren auf den Leib. Ein Verfahren, das immer zum Erfolg führt, ist das Durchprobieren aller möglichen Passwörter mit einem Brute-Force-Angriff. Doch damit tun sich Passwort-Cracker schwer: Je nach Länge und Komplexität eines Passwortes rechnen sie Wochen, Jahre oder gar Jahrhunderte vor sich hin, bevor sie alle möglichen Zeichenkombinationen abgeklappert haben.

Mit schwachen Hash-Algorithmen wie etwa dem alten LM-Hash der Windows-Versionen vor XP SP3 machen die Passwortknacker allerdings kurzen Prozess. Selbst der als eher gemütlich bekannte Cracker „Cain & Abel" berechnet auf einem einzelnen Kern eines Intel Core 2 Quad Q9300 acht bis neun Millionen LM-Hashes pro Sekunde und kann damit aufgrund eines Designfehlers im LM-Algorithmus jedes noch so lange und komplexe Passwort innerhalb von neun Tagen aufdecken.

Bei Hash-Funktionen wie dem NTLM-Hash aktueller Windows-Versionen und -Netzwerkprotokolle ist allerdings schiere Rechenleistung gefragt. Moderne Cracker wie der kostenlose BarsWF für MD5-Hashes und ElcomSofts „Distributed Password Recovery" verteilen die Last auf nahezu beliebig viele Prozessorkerne und sorgen so auf Großrechnern für einen mächtigen Geschwindigkeitsschub. Das ElcomSoft-Programm kann die Aufgabe mit einer Client-Server-Architektur sogar auf einem skalierbaren Cluster bewältigen. Die Version für bis zu 20 Clients kostet

600 Euro und steht auch als kostenlose Testversion zum Download bereit.

Farbenfroh

Doch eine neuere Entwicklung sorgt nun auch auf Heim-PCs für einen beachtlichen Leistungszuwachs: die Nutzung der Rechenleistung moderner Grafikkarten. Die hochgezüchteten Grafikprozessoren (GPUs) sind besonders effizient darin, immer gleiche Rechenoperationen auf großen Datenmengen auszuführen und werden gern zur Beschleunigung wissenschaftlicher Simulationen eingesetzt. Diese Rechenleistung kommt nun auch modernen Passwort-Crackern zugute. Sowohl BarsWF als auch das unter anderem NTLM-fähige ElcomSoft-Programm können mit Hilfe des CUDA-Frameworks Grafikkarten von Nvidia für ihre Brute-Force-Berechnungen nutzen.

Um die Leistung der GPUs mit gewöhnlichen Prozessoren zu vergleichen, lassen wir zwei höchst ungleiche Systeme für einen Geschwindigkeitstest antreten. Der erste Kandidat ist ein 24-kerniger Windows-2008-Server mit vier Intel-Dunnington-Prozessoren mit jeweils sechs Kernen und 2,5 GHz. Mit einer solchen Hardware sind beispielsweise der HP Proliant DL580 G5 (ab 18 000 US-Dollar mit 8 GByte RAM) oder Dell PowerEdge R900 (31 000 US-Dollar mit 64 GByte RAM) ausgestattet.

Der Herausforderer ist ein typisches Gamer-System: ein Intel Core 2 Quad Q9300 mit einer GeForce-GTX-280-Karte von Nvidia unter Windows XP x64. Die Kosten belaufen sich auf rund 350 Euro für die Grafikkarte und 450 Euro für das Quad-Core-System. Auf beiden Rechnern kam die 64-Bit-Variante von BarsWF 0.8 zum Einsatz. Für das Passwort-Cracken mit Hilfe des „dummen" Brute-Forcing sind die Größe des Hauptspeichers und des Grafikkarten-RAM unerheblich.

Pro Core berechnet der 24-Kern-Server knapp 50 Millionen Hashes pro Sekunde und kommt auf einen Gesamtdurchsatz von stolzen 1,2 Milliarden Hashes in der Sekunde. Die Grafikkarte hingegen leistet zwar mit 720 Millionen Hashes in der Sekunde nur zwei Drittel davon, aber das für gerade einmal ein Zwanzigstel des Preises.

Zusammen mit dem Quad-Core kommt der Gamer-PC auf beachtliche 0,9 Milliarden Hashes pro Sekunde. Damit hat sich die Größenordnung der im PC-Bereich erzielbaren Rechenleistung deutlich verschoben. Je 1000 investierter Euro kann man bereits mit rund zwei Milliarden MD5-Hashes je Sekunde rechnen.

Farbattacke

Dieser beachtliche Leistungsschub für Heimrechner wirft freilich die Frage auf, ob gängige Passwort-Policies dem gewachsen sind oder einer Anpassung bedürfen. Um die Sicherheit einer Policiy einzuschätzen, muss man berücksichtigen, wie viel Geld ein Angreifer ausgeben würde, um – in diesem Fall – ein Passwort hinter einem NTLM-Hash durch Brute-Force aufzudecken.

Wie groß ist also die Gefahr, die von einer Einzelperson ausgeht, die bis zu 1000 Euro für Hardware investieren kann? Für diesen Preis bekommt man ein System mit zwei GeForce-9800-GTX-Karten, getaktet auf 1,6 GHz, und einem Dual-Core-Prozessor AMD Athlon X2 4850e mit 2,5 GHz. Wichtig ist auch ein starkes Netzteil sowie eine leistungsfähige Kühlung, denn anders als beim Spielen laufen die Komponenten beim Cracken permanent unter Volllast.

Auf dem Prüfstand stehen aktuelle Richtlinien (Policies) für sichere Passwörter, wie sie typischerweise Firmen verwenden. Hier sind nach Erfahrungen der SySS GmbH, für die die Autoren hauptberuflich tätig sind, sechs- bis achtstellige Passwörter üblich, die sich hauptsächlich in der Zahl der erforderlichen Sonderzeichen unterscheiden – durchschnittlich zwei. Policies, die längere Passwörter oder Passphrases erfordern, sowie Systeme, die keine klassischen Passwörter verwenden, sind immer noch die Ausnahme.

Der ElcomSoft-Cracker bewältigt auf unserem Testsystem durchschnittlich 850 Millionen NTLM-Berechnungen je Sekunde. Die Menge der durchzuprobierenden Sonderzeichen haben wir auf 22 typische Elemente reduziert: _@#$&+-=%*"~!?.,:;()<>. Dies sind die Sonderzeichen, die menschliche Nutzer bevorzugen.

Die Tabelle oben rechts zeigt die vom Programm anhand der Systemgeschwindigkeit vorausgesagte Zeitdauer zum Abklappern aller möglichen Passwörter innerhalb der spezifizierten Klasse. Im statistischen Mittel ist ein Passwort nach der Hälfte der angegebenen Maximalzeit ermittelt.

Maximale Crack-Dauer für Windows-Passwörter (NTLM)

Stellen	Zeichenraum	Dauer
6	A-Z, a-z, 0-9	1 Minute
6	A-Z, a-z, 0-9, typ. Sonderzeichen	6 Minuten
8	A-Z, a-z, 0-9	2 Tage und 17 Stunden
8	A-Z, a-z, 0-9, typ. Sonderzeichen	33 Tage
8	A-Z, a-z, 0-9, alle Sonderzeichen	82 Tage
11	A-Z, a-z	270 Jahre

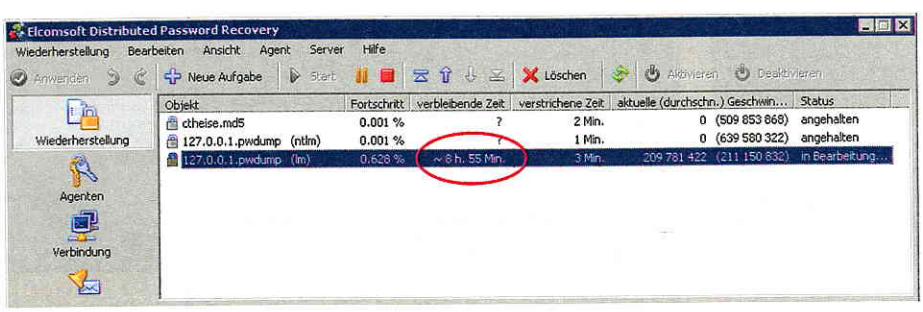
Angaben laut ElcomSoft-Cracker auf einem AMD Athlon X2 4850e mit zwei GeForce-9800-GTX-Karten

Sechsstellige Passwörter aus Groß- und Kleinbuchstaben sowie Ziffern sind schon für einen einfachen PC zu schwach: Die insgesamt 57 Milliarden möglichen Passwörter bewältigt die von uns gewählte AMD-CPU auch ohne GPU-Unterstützung in zehn Minuten.

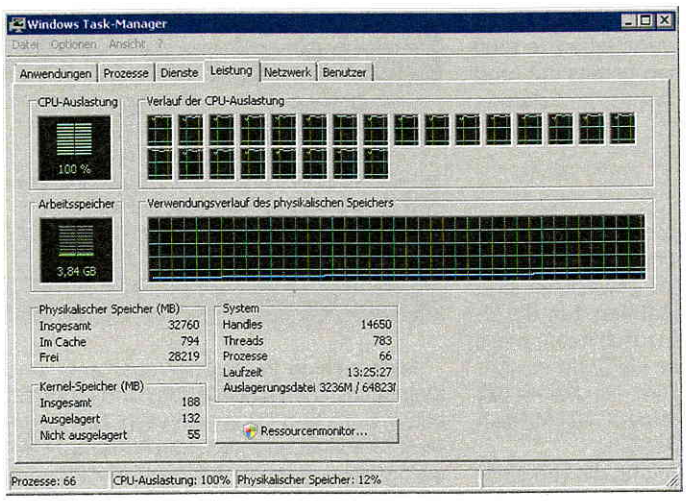
Mit Hilfe der beiden GPUs macht der Cracker innerhalb einer Minute kurzen Prozess. Auch wenn zusätzlich die 22 Sonderzeichen zu berücksichtigen sind, ist der Sicherheitsgewinn unerheblich: Die 355 Milliarden Kombinationen sind nach gerade einmal sechs Minuten vollständig durchprobiert. Erst bei achtstelligen Passwörtern erhöht sich die Dauer auf mehrere Tage und durch Hinzuziehen der Sonderzeichen immerhin auf einen Monat.

In der Praxis sind die meisten Anwender bei der Wahl der Sonderzeichen sehr vorsichtig, weil es mit Leerzeichen und anderen ungewöhnlichen Zeichen auf manchen Systemen zu Problemen kommen kann. Doch selbst wenn man alle möglichen Sonderzeichen mit in die Berechnung einfließen lässt, zeigt die vorausberechnete Maximaldauer von knapp 82 Tagen, dass es nur ein paar

Mit Hilfe der hochoptimierten Spezialprozessoren moderner Grafikkarten lassen sich bestimmte Algorithmen – darunter auch das Passwort-Cracking – enorm beschleunigen.



Der alte Windows-LM-Hash degeneriert zum Horror-Hash: Selbst komplizierteste Passwörter sind in wenigen Stunden geknackt.



Mit 24 Kernen geht der Intel-Dunnington-Server zu Werke. Schnell ist er allemal, aber auch teuer.

GPUs beziehungsweise Personen mit Gaming-PCs mehr braucht, um auf einen erträglichen Zeitrahmen zu kommen.

Statt Sonderzeichen sollte man einem Passwort folglich lieber zusätzliche Stellen spendieren. Immerhin ist unsere Testhardware bereits mit allen nichttrivialen elfstelligen Passwörtern hoffnungslos überfordert. Ausreichend komplexe Passwörter dieser Länge lassen sich allerdings nur mit besonderen Tricks merken. Eine weitverbreitete Möglichkeit sind die von Microsoft empfohlenen Passphrasen, doch auch besondere Passwortsysteme generieren nahezu beliebig viele sichere und dennoch merkbare Passwörter [1].

Preisfrage

Anders sieht es aus, wenn Angreifer größere Beträge investieren, um den Knackzeitraum auf ein vertretbares Maß zu reduzieren. Cracker wie der von ElcomSoft skalieren durch ihre Netzwerkfähigkeit problemlos auf ganze Rechnerfarmen. Möchte man selbst komplexeste achtstellige NTLM-Passwörter – also etwa 95^8 Möglichkeiten – innerhalb eines Tages bruteforcen können, ist eine Rechenleistung von 80 Milliarden Hashes pro Sekunde nötig.

Um solche Werte zu erzielen, sollte man – etwas Spielraum vorausgesetzt – von 180 Grafikkarten des Typs 9800 GTX oder der höher getakteten Version 9800 GTX+ ausgehen. Bei einem Preis von rund 150 Euro je Karte und zwei Karten je PC läge ein Cluster dieser Größe daher in der Preisregion von 50 000 Euro.

Hinzu kommen allerdings die Kosten für Unterbringung, Stromversorgung und Kühlung. Dennoch wird deutlich, dass Sicherheitsverantwortliche längst nicht mehr davon ausgehen können, dass eine typische Passwort-Policy mit mindestens acht Stellen ausreichend Sicherheit bietet, wenn die NTLM-Hashes in falsche Hände gelangen.

Die Zukunft

Das von einer Einzelperson beziehungsweise einem aufgerüsteten PC ausgehende Risiko ist nicht so hoch, wie man vielleicht vermutet. Schon bei acht Stellen ist man bereits bei Rechendauern von mehreren Wochen angelangt, sofern Sonderzeichen enthalten sind.

Aufgrund der Preisentwicklung bei Grafikkarten sind Vorhersagen über die künftige Evolution des GPU-basierten Crackings und das Performance-Wachstum schwierig, zudem auch ATI-Karten mit dem Brook-Framework laut erster Berichte sehr hohe Leistung bringen. Auch ist zurzeit die Zahl der unterstützen Hash-Typen durch Recovery-Software noch begrenzt. Beispielsweise die in Windows-Netzwerken verwendeten Hashes unterstützt noch kein GPU-beschleunigter Cracker.

Doch die GPU-Technologie bedeutet einen gewaltigen Sprung nach vorne, der es dem Einzelnen nicht nur ermöglicht, komplexe wissenschaftliche Simulationen durchzuführen, sondern auch mehrere Milliarden Passwörter pro Sekunde durchzuprobieren. Der Autor von BarsWF plant den Aufbau eines gemeinschaftlichen Rechenprojektes, an dem ähnlich wie Folding@home jeder Besitzer einer geeigneten Grafikkarte teilnehmen kann.

Auch der langwierigen Berechnung von Regenbogentabellen, mit denen sich bestimmte Passwort-Angriffe enorm beschleunigen lassen [2], sollen GPUs nun auf die Sprünge helfen. Es ist also höchste Zeit, die Passwort-Policies an den Stand der Technik anzupassen. (cr)

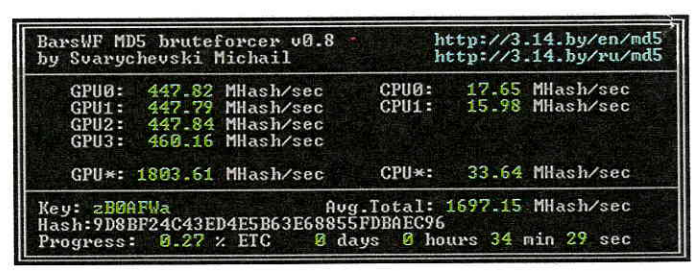
Literatur

[1] Christiane Rütten, Schön kompliziert, Passwörter mit Köpfchen, c't 2/09, S. 86

[2] Karsten Nohl, Kunterbuntes Schlüsselraten, Von Wörterbüchern und Regenbögen, c't 15/08, S. 190

[3] Vortrag zur GPU-Beschleunigung von MD5: www.troopers08.org/content/e6/e494/BELENKO_Andrej_-_Troopers08.pdf

Schon eine einzelne Nvidia-GPU vom Typ GTX 280 erreicht fast die Performance des 24-Kerners. BarsWF listet unter dem Durchsatz der Einzelkomponenten auch die Gesamtgeschwindigkeit.



Darfs auch ein wenig mehr sein? Zwei ältere High-End-Gamer-Karten wie Nvidias GeForce 9800 GX2 lassen selbst den 24-Kern-Server weit hinter sich. c't