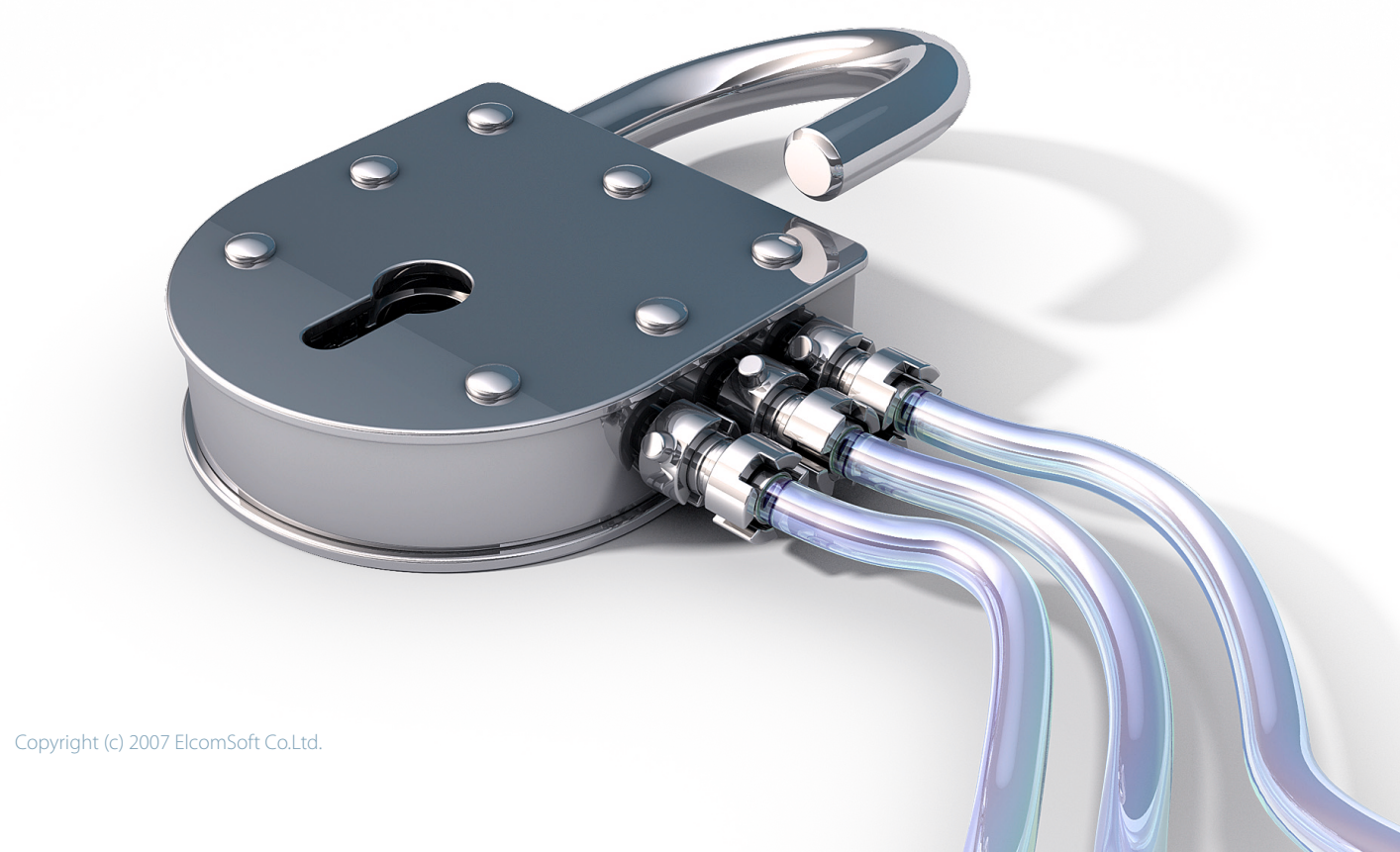
ELCOMSOFT
PROACTIVE SOFTWARE

DIE GRÖSSE HAT BEDEUTUNG

VORTEILE DER VERTEILTEN PASSWORT-WIEDERHERSTELLUNG



ELCOMSOFT
PROACTIVE SOFTWARE

INHALTE

INFORMATION IST EIN SCHLÜSSEL ZU RICHTIGEN ENTSCHEIDUNGEN

Die Wörter, wie "Informationsalter", "Informationstechnologien", "Der, der Informationen besitzt, regiert die Welt" haben sich längst in unseren Gedächtnissen eingeprägt. Jeder weiss, daß Informationen eine der wertvollsten Ressourcen sind.

Haben Informationen selbst einen Wert? Nein. Informationen sind beim Treffen der Entscheidungen äußerst wichtig. Dies ist wichtig. Eine richtige Entscheidung ist ein Schlüssel zum Erfolg in jedem Feld. Der Informationsbesitz ist vom entscheidenden Wettbewerbsvorteil in der heutigen Geschäftswelt.

Kein Wunder, daß dem Informationsschutz so viel Beachtung geschenkt wird. Das größte Teil der Informationen wird digital erstellt und gespeichert (Microsoft Office - Dokumente, verschiedene Datenbanken und Finanzdaten in Intuit Quicken etc). Demnach sind die Leistungen bei der Software und Hardware, Informationen zu schützen, als erstes auszudiskutieren.

SCHUTZMASSNAHMEN HABEN VORRANG

IT – Sicherheit ist eine sich rasch entwickelnde Branche der Informationstechnologie-Industrie. Der Markt strotzt von Software-Produkten, die dafür entwickelt wurden, den Zugriff auf die Informationen einzuschränken und Informations-Leckstellen zu vermeiden (zum Beispiel, Tools für die Zugriffskontrolle und Authentifizierung, Firewalls, Backup-Systeme, Antivirus-Pakete und so weiter).

Wenn man allerdings von den einfachsten Maßnahmen des Informationsschutzes spricht, ist der Passwort-Schutz die einfachste Maßnahme unter den Nutzern.

Verkaufsdaten und finanzielle Umsätze, Kunden-Datenbanken, Buchhaltung und internes Rechnungswesen, analytische Berichte und Prognosen – all diese Informationen werden gebraucht, um eine Firma erfolgreich zu bedienen und strategische Entscheidungen zu machen, deren Einfluss immer weiter wächst. Ungeschützte Zugänge zu den Informationen dieses Artes sind unmöglich. Dies ist eine simple Basis der Sicherheitspolitik einer Firma.

VERLUST DES ZUGRIFFS – TÄGLICHE ANGELEGENHEITEN

Offensichtlich ist die schwache Stelle eines Informationssystems der menschliche Faktor. Passwortschutz ist dem Mangel unterworfen.

Trotz mehrerer Maßnahmen, die unternommen werden, um ein Passwort zu schützen (wie, zum Beispiel, das Eingrenzen der minimalen Passwort-Länge und –komplexität, Passwort-Überprüfungen, reguläre Änderungen des Passwortes), kann nichts das Hauptproblem lösen - Passwortverlust. Es ist schwer, einen Menschen zu finden, der auf einem PC gearbeitet und diese Situation nicht erlebt hat.

Sie können leicht das Passwort vergessen. Sie sind ein vernünftiger Mensch und haben es nicht in einem Notizblock festgehalten, sondern sich einfach dank einer Eselsbrücke gemerkt. Sie sind sich über das Geburtsjahr sicher, doch Ihr Lieblingsgericht hat sich geändert – und Sie können sich nicht mehr daran erinnern!

Oder hat vielleicht ein Verkaufsmanager gekündigt, ohne das Passwort für den Lieferungsbericht zu hinterlassen? Sie können keinen Kontakt mit ihm aufnehmen, Gegenseite droht mit einem Vertragsbruch, falls Sie die Rechnungen nicht sofort bezahlen, doch Sie haben keinen Zugang zu den Daten.

Falls die Mitarbeiter-Kündigung Gründe, wie finanzieller Betrug oder Arbeit für die konkurrierende Firma, hat, sollten Sie wirklich nicht darauf zählen, dass er das Passwort übergibt. Doch Sie brauchen immernoch den Zugang. So schnell wie möglich.

Dennoch ist das Problem der Passwort-Wiederherstellung verschlüsselter Daten zu lösen. Die Absurdität der Situation ist: je komplizierter das Passwort ist, desto weniger sind die Chancen, es aufzudecken. Strenge Passwort-Schutzpolitik ist schwer zu knacken. Es gibt aber auch gute Nachrichten – in den meisten Fällen kann der Zugang wiederhergestellt werden.

PAAR WÖRTER ÜBER… PASSWÖRTER

Seit der Passwortschutz erfunden und somit das Problem eines Passwort-Verlustes allgegenwärtig wurde, haben die Software-Entwickler nach einer Möglichkeit gesucht, dieses Problem zu lösen. Als Ergebnis bietet der Markt heutzutage eine weite Reihe der Passwort-Wiederherstellungs-Technologien.

Lasst uns erstmal die Informationen über die Passwort-Wiederherstellungs-Methoden zur Seite legen und die Grundinfos über Passwörter, Passwort-Typen und Infos, die Sie brauchen, um ein Passwort zu finden, ausdiskutieren.

Englischsprachige Passwörter nutzen generell folgende Symbole: 26 Kleinbuchstaben (a…z), 26 Grossbuchstaben (A…Z), 10 Zahlen (0…9) und 33 Sonderzeichen (!@#$%^ etc); somit ergeben sich 95 Symbole für beliebige Kombinationen. Manchmal werden die Sonderzeichen aus der Gruppe ausgeschlossen, was die Anzahl der möglichen Kombinationen erhöht. Außerdem kann ein Passwort lang oder kurz sein, was von großer Wichtigkeit ist, wenn jemand ein Passwort nicht abrufen oder rücksetzen kann und Brute-Force-Angriff auszuführen hat.

Trotz mehrerer Aufrufe, das Passwort sicher zu verwalten, vermeiden viele Nutzer die einfachsten Schutztricks. Solche Erscheinung erweist, daß ein Mensch ein schwaches Glied in der Kette ist und eine gefährliche Lücke im Sicherheitssystem.

Die Mehrheit der populären Passwörter sind einfach nur Wörter, aus der Muttersprache des Nutzers abgeleitet. Manchmal können die Wörter, die als Passwörter benutzt werden, im Alltagsleben gefunden werden: Geburtsjahr, Telefonnummer, Tiername, Kreditkarten-Nummer etc. Ein neues Passwort kann eine leicht modifizierte Variante des vorherigen Passwortes sein. Dies ist ein Weg, wie die meisten Nutzer die Situation mit regelmäßiger Passwort-Änderung lösen, die von den Sicherheitsvorschriften vorgegeben wird. Doch die offensichtlichste Spur ist, dass die Menschen dazu tendieren, das Passwort auf dem Arbeitsplatz zu behalten oder in der PC-Datei zu speichern. Solch eine Situation untergräbt die Idee des Passwortschutzes komplett.

Demnach kann ein Passwort leicht gefunden werden, wenn man, zum Beispiel, die Passwort-Stuktur oder –länge kennt oder einige Informationen über den Nutzer hat. Technologien, die spezifische Software zur Passwort-Wiederherstellung benutzen, ermöglichen die Nutzung solcher Informationen.

WEGE ZUR PASSWORT-WIEDERHERSTELLUNG

Die automatischen Grundmethoden der Passwort-Wiederherstellung sind Brute-Force, Masken-Angriff, Wörterbuch-Suche, verschlüsselte Begriffssuche (weniger möglichen Kombinationen im Vergleich mit Brute-Force) und so genannter Rainbow-Table-Angriff. Manchmal werden andere Methoden zur Zugriffs-Wiederherstellung auf die Datei benutzt, wie zum Beispiel Known-Plaintext-Angriff. Lasst uns einige Methoden ausführlicher betrachten.

BRUTE-FORCE

Brute-Force-Angriff ist einfach: bei der Suche nach einem Passwort probiert ein Programm jede mögliche Symbolkombination aus. Die Suche kann auf bestimmte Länge, Symboltyp (Buchstaben, Zahlen oder anderes) eingeschränkt werden, beziehungsweise auf Symbole, die als erstes ausprobiert werden müssen.

Wie viel Zeit ist jedoch nötig, damit eine Brute-Force-Attacke ein Passwort wiederherstellt? Es hängt von der Passwort-Länge, Symbolreihe und PC-Leistung, sowohl dem passwortgeschützten Dateityp ab.

Natürlich kann ein Passwort sehr schnell gefunden werden, und das Programm muss nicht alle möglichen Kombinationen ausführen. Jedoch sollten Sie darauf nicht zählen. Die Aufgabe kann Jahre dauern, falls sie auf einem Durchschnitts-PC ausgeführt wird. Da die Brute-Force-Technologie die zeitaufwendigste Methode ist, kann darauf nur dann zurückgegriffen werden, wenn keine anderen Methoden vorhanden sind.

MASKEN-ANGRIFF

Falls Sie das Passwort selbst erstellt haben, können Sie es mithilfe der Masken-Attacke wiederherstellen, indem Sie die Suchreihe eingrenzen. Vielleicht wissen Sie noch die Länge des Passwortes oder einiger Symbole? Jede Information könnte vom Nutzen sein.

Sie wissen, zum Beispiel, dass Sie nur Zahlen und kleingeschriebene lateinische Buchstaben benutzt haben. Somit können Sie bei der Suche bestimmte Symbole und Großbuchstaben ausschließen. Es ist auch günstig, wenn Sie eine bestimmte Reihenfolge eines Zeichens im Passwort wissen. Falls zum Beispiel, ein Passwort aus 10 Zeichen besteht, mit „a" anfängt und mit „2007" endet, können Sie die Suchvorlage "a?????2007" nutzen. Unbekannte Zeichen werden in der Vorlage mit Fragezeichen markiert.

Masken-Angriff macht Sinn: ein Programm muss weniger Kombinationen ausprobieren, so dass das Passwort in kürzerer Zeit gefunden wird.

Wenn allerdings keine Details über ein Passwort bekannt sind, kann die Masken-Attacke generell nicht ausgeführt werden. Es gibt aber zum Glück noch eine weitere effiziente Passwort-Wiederherstellungs-Methode.

WÖRTERBUCH-SUCHE

Lasst uns annhemen, Sie kennen die Wörter und Namen, die im Passwort vorkommen könnten. In diesem Fall können Sie die Wörterbuch-Suche benutzen.

Die Nutzer neigen oft zur Benutzung allgemeiner Wörter bei der Erstellung der Passwörter. Allgemein könnten es Wörter, wie "öffnen", "Zugriff" oder "Passwort" sein. Im Vergleich zu den chaotischen Kombinationen der Zeichen und Zahlen sind solche Passwörter schneller einzuprägen. Tatsächlich sind solche Passwörter genauso leicht, wie die anderen, zu vergessen, doch leichter wiederherzustellen.

Woher nimmt man aber das Wörterbuch (oder die Wortliste)? Als erstes könnte es in das Passwort-Wiederherstellungs-Programm eingeschlossen sein. Als zweites können Sie danach im Internet suchen. Verschiedene Listen allgemeiner Wörter, thematische Listen (Natur, Fussball-Teams etc), Kurzwort-Listen sind allgegenwärtig. Als drittes können Sie solches Wörterbuch selbst erstellen.

Diese Methode hat offensichtliche Vorteile. Die Liste der allgemeinen Wörter, die in den Passwörtern benutzt werden, ist begrenzt; sie enthaltet nie mehr als 100 000 Wörter. Das Ausprobieren von 100 000 Kombinationen ist eine leichte Aufgabe für die modernen PCs. Somit ist es ratsam, diese Suchmethode als erste anzuwenden. Es könnte funktionieren.

RAINBOW-ANGRIFF

Offensichtlich ist das wichtigste Kriterium bei der Passwortsuche die Zeit, die man für die Suche braucht. Brute-Force-Angriff probiert alle möglichen Kombinationen aus, und die Wiederherstellung komplexer Passwörter braucht zu viel Zeit. Falls die Suche Monate oder Jahre dauert, ist der praktische Wert gleich Null.

Die Methode der Rainbow-Tabellen (Rainbow-Attacke) kann das Problem eliminieren. Der Grundgedanke dieser Methode ist die Nutzung der Vorberechnung von Passwort-Varianten für eine bestimmte Symbolreihe.

Die Idee des Ersetzens der ressourcenintensiven Berechnungen durch eine Nachschlagetabelle, die zuvor vorbereitet wurde, ist nicht neu. Nachschlagetabellen werden benutzt, wenn es leichter ist, die Daten aus dem Speicher zu extrahieren, als zu erstellen. Das einzige Manko an der Nachschlagetabelle ist deren Größe: nicht jedes Unternehmen kann sich erlauben, Terabytes von Daten zu speichern. Deswegen wurden die 'Regenbogen'-Tabellen (oder optimierte Nachschlagetabellen) ins Leben gerufen. Die Größe der Rainbow-Tabelle ist viel kleiner, als die von der Nachschlagetabelle.

Generieren der Rainbow-Tabelle bestimmt die Wahrscheinlichkeit der Passwort- oder Schlüssel – Wiederherstellung, vorgeschlagene Angriffszeit und Zeit für die Tabellengenerierung im Voraus. Das Abstimmen der Einstellungen und Finden der passenden Balance zwischen der Angriffszeit und Wahrscheinlichkeit der Passwort-/Schlüssel-Wiederherstellung müsste separat behandelt werden. Als Ergebnis werden die Tabellen, die helfen, schnell das Passwort/den Schlüssel aus einer bestimmten Reihe mit hoher Wahrscheinlichkeit zu finden, in einer angemessenen Zeit erstellt.

Im Vergleich zu den einfachen Nachschlagetabellen ist die Wahrscheinlichkeit der Passwort-Wiederherstellung mithilfe der Rainbow-Entschlüsselung niedriger als 100%, doch das Ergebnis ist es wert. So ermöglicht, zum Beispiel, der Rainbow-Angriff, der auf der Tabelle mit 7 alphanumerischen Symbolen (innerhalb einer Woche aufgebaut) basiert, die Wiederherstellung eines Passwortes mit 7 alphanumerischen Symbolen innerhalb der 20-30 Sekunden. Bei der Brute-Force-Attackef würden Sie dafür über 24 Stunden brauchen. Der Vorteil ist offensichtlich.

ZEIT IST GELD

Nachdem wir ausdiskutiert haben, was die Passwörter sind und wie die Grundmethoden zur Passwort-Wiederherstellung aussehen, können wir nun voraussehen, wie schwer es ist, den Zugriff auf die Daten wiederherzustellen: die Wahrscheinlichkeit, ein Passwort zu finden und die Zeit, die man dafür braucht.

Der Aufwand bei Passwort-Wiederherstellung hängt von vielen Faktoren ab, wie die Passwort-Länge, Zeichenreihe, geschützter Dokumententyp, Verschlüsselungs- Algorithmus und PC-Leistung. Als Allgemeinregel gilt, dass die Wahrscheinlichkeit zeitabhängig ist: ein Passwort kann 100%-tig wiederhergestellt werden, wenn die Suchzeit nicht eingeschränkt ist.

Die Nutzer heutzutage sind der Passwort-Benutzung mehr bewusst: Passwörter wurden länger und komplexer. Zum Beispiel, nutzen über 60% der MySpace[1] - Nutzer Passwörter, die 8 oder mehr Symbole enthalten, während nur 1% der Nutzer 5-stellige Passwörter ergreift. 80% der Passwörter enthalten Buchstaben und Zahlen; Passwörter, die ein Wort enthalten, das leicht im Wörterbuch zu finden sind, betragen 3.8%.

Wie zuvor gesagt, kann ein Passwort schnell gefunden werden, so daß es nicht nötig ist, alle möglichen Passwort-Kombinationen auszuprobieren. Seien Sie jedoch für das schlimmste gefasst – manchmal dauert die Passwortsuche Jahre. Werden Sie nach so langer Zeit immer noch das Passwort brauchen?

Zeitfaktor ist entscheidend, wenn ein Problem der Wiederherstellung des Passwortes gelöst wird, weil Informationen unrelevant werden und veralten. Wie kann man die Passwort-Suchzeit verkürzen?

Entschlüsselungs-Algorithmus, Passwortlänge und –komplexität, sowohl der Dokumenttyp sind beständig; diese Parameter können nicht geändert werden. Die einzige Sache, die wir zur Verfügung haben, ist Rechenleistung.

[1] http://www.wired.com/politics/security/commentary/securitymatters/2006/12/72300

PASSWÖRTER SCHNELLER FINDEN

VERTEILTE DATENVERABEITUNG

Trotz moderner PCs, die Daten mit großer Geschwindigkeit verarbeiten, dauert die Passwort-Wiederherstellung mit dem Brute-Force-Angriff zu lange, da es eine schwierige Aufgabe für einzelnen PC ist.

Das Erstellen riesiger Datenverarbeitungs-Ressourcen für das Lösen der Aufgaben, die viele PC-Jahre einnehmen, sind auf der Tagesordnung (zum Beispiel, Protein-Untersuchungen, mathematische Gesetze, Untersuchungen der Humangenome, Wettervorhersagen). Nur die Super-PCs mit beispielloser Performance können diese Berechnungen abwickeln. Die Anzahl der Super-PCs wächst, doch die Preise sind immer noch sehr hoch: nicht jedes Unternehmen und noch nicht mal jeder Staat kann sich so ein Super-PC[2] erlauben.

Was ist mit dem Verbinden mehrerer PCs? Was ist, wenn es nicht nur einige sind, sondern Dutzend oder sogar hunderte? Dann bekommen wir einen völlig anderen Ressourcentyp. So kam die Idee der verteilten Datenverarbeitung auf die Welt. Verteilte Datenverarbeitung bedeutet die Ausführung der zeitintensiven Berechnungen mithilfe von zwei oder mehr PCs, die als Netzwerk agieren. Diese Aufgabe sollte in Teile aufgeteilt werden, die auf verschiedenen PCs gleichzeitig agieren. Demnach trägt ein PC dazu bei, ein Teil des Datenaufbaus zu verarbeiten.

Ein PC kann leicht solches Problem in der Freizeit lösen. Kein Wunder, denn wenn Sie mit Anwendungen (Internet-Browser, Office-Anwendungen) in Windows arbeiten, bleibt der Prozessor für 99% der Arbeitszeit außer Betrieb; er erwartet einfach neue Daten oder Aufgaben, die eingegeben werden müssen, und verbraucht dafür umsonst den Strom.

Spezielle Software, die in den Projekten der verteilten Datenverarbeitung benutzt wird, kann den stilliegenden Prozessor effektiv laden. Solche Software läuft im Hintergrund-Modus oder startet, wenn der Prozessor außer Betrieb ist, und bestimmt sofort, wenn der Prozessor durch den Nutzer geladen wird, um später neu zu starten; das Ausführen der Software ist für den Nutzer unsichtbar.

[2] Laut http://www.top500.org/ vom Juni 2007, 8 von 10 Super-PCs, die auf der Liste der 500 leistungsstärksten PCs oben stehen, in den USA platziert.

VORTEILE DER NUTZUNG SOLCHER METHODE FÜR PASSWORT-WIEDERHERSTELLUNG

Die Aufgabe ist das Ausprobieren aller möglichen Passwort-Kombinationen, um das verlorene Passwort zu finden oder Zugriff auf das Dokument zu bekommen. Solch eine Aufgabe kann leicht mit verteilter Datenverarbeitung gelöst werden.

Zugang zu einigen Dokumenten oder Anwendungen kann in kurzer Zeit mithilfe eines einzelnen PCs wiederhergestellt werden (Zum Beispiel, für IBM® Lotus®- SmartSuite®-, Corel® WordPerfect® - und Office – Dokumente, egal wie komplex das Passwort ist, oder ein Passwort für ICQ oder Google-Talk, das lokal gespeichert wurde). Doch andere Passwörter verlangen nach größeren Ressourcen, selbst wenn es keine Zeiteinschränkung gibt. Hochgeschwindigkeits-Suche kann für bestimmte Dokumenttypen oder Verschlüsselungs-Algorithmen nicht garantiert werden. Zum Beispiel kann Intel® Core™2 Duo ein Microsoft Office 2007 - Dokument mit garantierter Geschwindigkeit von 100 Passwörter pro Sekunde durchsuchen; oder es kann die RAR-Datei mit Geschwindigkeit von nicht mehr als 100 Passwörter pro Sekunde durchsuchen. RGP – Passwortsuche ist zeitintensiv: Suchgeschwindigkeit kann von Dutzend bis Tausende Passwörter variieren, je nach Format und Algorithmus. Selbst wenn die Suchgeschwindigkeit hoch ist (zum Beispiel, wenn standardmäßige 40-Bit-Verschlüsselung in Word/Excel 97/2000/XP/2003 oder Adobe Acrobat PDF-Dokumenten benutzt wird), hat die verteilte Datenverarbeitung mehrere Vorteile. Mit einem einzelnen PC (selbst wenn er leistungsstark ist) dauert es einige Tage um das Problem zu lösen; im Netzwerk kann die Aufgabe innerhalb weniger Stunden oder selbst Minuten gelöst werden. Mehr noch – verteilte Datenverarbeitung ist unabdingbar bei der Suche mehrerer Dokumente.

Zeitvorteil ist nicht der einzige Vorteil der verteilten Datenverarbeitung. Hier sind einige gute Argumente:

- Kein Bedarf, einen PC (oder PCs) zu beantragen, bestimmte Aufgabe zur Passwort-Wiederherstellung auszuführen;
- Verarbeiten mehrerer Dokumente;
- Nutzung der PCs in der Arbeitszeit oder Freizeit (Nutzer werden nicht gestört);
- Nutzung selbst eines leistungsschwachen PCs im Netzwerk – alle PCs tragen zur Aufgabenlösung bei;
- Abändern der Anzahl beschäftigter PCs, abhängig von Dokumenten-Anzahl, angenommener Passwort-Komplexität und Aufgaben-Dringlichkeit.

LÖSUNG AUSWÄHLEN

Somit bestehen nun keine Zweifel, ob das Passwort-Wiederherstellungs-Tool gekauft werden müsste. Es ist offensichtlich, dass jeder Systemadministrator solch ein Tool bei sich haben müsste. Die Ausgaben sind spätestens dann zurückgezahlt, wenn das erste Passwort verloren ist.

Was muss in diesem Fall betrachtet werden?

Als Erstes, die Wahrscheinlichkeit der Passwort-Wiederherstellung, die vom Software-Anbieter angegeben wird. Das Kriterium ist für die Bewertung der Lösungs-Effizienz entscheidend. Deswegen kaufen Sie es doch, oder? Natürlich kann die 100%-tige Wahrscheinlichkeit nur in Abwesenheit der Zeiteinschränkungen garantiert werden, doch dieses Bild ist nicht gut genug für Sie. Als Allgemeinregel muss der Zugriff auf das Dokument so schnell wie möglich wiederhergestellt werden: die Zeit geht.

Zweitens ist die Reihe der unterstützten Betriebssysteme, Anwendungs-Versionen, Dateiformate, Sprachen und Dekodierungen zu beachten. Es ist schwer zu sagen, mit welcher Adobe Acrobat – Version Sie sich befassen werden, wenn Sie das Passwort wiederherstellen. Erkundigen Sie sich, wie man die neuere Versionen bekommt, sowohl über die Zeitspanne, in der dieses Upgrade vorhanden sein wird.

Der letzte Punkt ist, ob die verteilte Datenverarbeitung überhaupt möglich ist. Diese Methode zur Lösung komplexer (CPU-hungriger) Probleme verlangt nach der Arbeitsleistung einer PC-Gruppe, zum Beispiel, PCs, die lokal oder entfernt miteinander verbunden sind. Die Methode wird beim Passwort-Hacken benutzt. Einige Passwörter für Dokumente und Anwendungen können mithilfe eines einzelnen PCs in kurzer Zeit wiederhergestellt werden (zum Beispiel, lokal gespeichertes ICQ-Passwort oder Passwort für das WordPerfect - Dokument). Doch für viele anderen verlangt die Wiederherstellung größere Ressourcen. So sind, zum Beispiel, die PGP-Passwörter so sicher, daß das Passwort-Hacken nur mithilfe der verteilten Datenverarbeitung möglich ist.

Es gibt Grundkriterien beim Wählen der Lösung für die Passwort-Wiederherstellung.

ELCOMSOFT DISTRIBUTED PASSWORD RECOVERY – PASSWORT SOFORT

Elcomsoft Distributed Password Recovery ermöglicht die Inbetriebnahme der PC-Leistung aller Netzwerk-PCs, egal ob das Netzwerk global oder lokal ist.

Dieses Produkt kann ein Passwort für beliebiges Microsoft Office-Dokument wiederherstellen – Word, Excel, PowerPoint (beliebige Ausgabe), Passwörter für Microsoft Money, Microsoft OneNote, Adobe Acrobat, Intuit Quicken, Lotus Notes (ID-Dateien), Anmeldungs-Passwörter für Windows 2000/XP/2003/Vista, PGP Secret Keys (*.skr), PGP Disk (*.pgd), PGP - Diskverschlüsselung, PGP ZIP-Archive (*.pgp), PKCS #12-Zertifikate (*.pfx), MD5-Hashes.

100% Wiederherstellung ist für Word 97-2003- und Excel 97-2003 – Dokumente garantiert, falls 40-Bit-Verschlüsselungsschlüssel benutzt wurde (standardmäßiger Microsoft Office-Verschlüsselungsschlüssel). Entschlüsselung der Adobe Acrobat PDF – Dateien mit 40-Bit-Verschlüsselung ist auch garantiert (in den früheren Adobe Acrobat-Versionen benutzt oder manuell in Acrobat 6/7/8 gewählt). Elcomsoft Distributed Password Recovery kann auch sowohl die "Nutzer"-, als auch die "Inhaber"-Passwörter für PDF-Dateien mit 40-Bit- oder 128-Bit- Verschlüsselung finden.

Gut strukturierte Architektur von Elcomsoft Distributed Password Recovery ermöglicht das ständige Ausweiten der Liste mit unterstützten Formaten.

Das Programm hat eine "Client-Server"-Struktur und beinhaltet drei Komponente: Server, Agent und Konsole (siehe Bild 1).

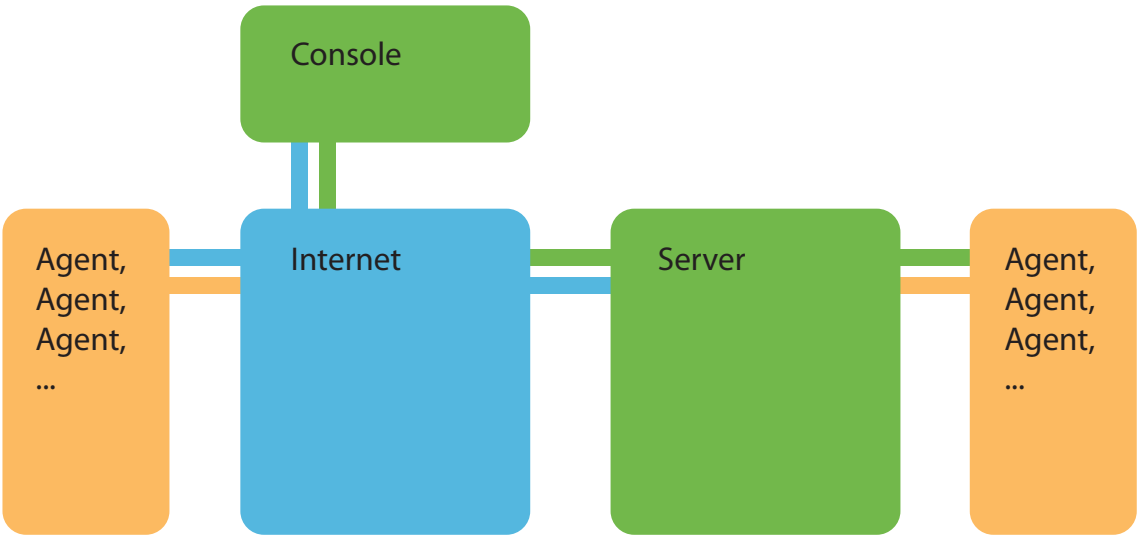


Bild 1. Struktur von Elcomsoft Distributed Password Recovery.

Der Server auf einem der PCs im Netzwerk wird in Gang gesetzt. Dann verbinden sich vorher installierte und in Gang gesetzte Agente (auf den Arbeitsstationen) mit den Servern, liefern die gemachte Arbeit (falls sie eine hatten) und erhalten den nächsten Arbeitsteil. Die Daten werden im archivierten Format übermittelt, so dass es die Netzwerk-Performance nicht beeinflusst.

Die Konsole kann von jedem PC im Netz gestartet werden. Die Kontrolle des Servers ist möglich, genauso wie das Hinzufügen der neuen Aufgaben und Betrachten der Statistiken. Passwort-Suchserver können entweder lokal oder entfernt kontrolliert werden. Dauer der Arbeitszeit (Wochentage, Arbeitsstunden) und Aufgaben-Rangfolge können für Agente festgelegt werden.

Die Methode der Passwort-Wiederherstellung kann bei der Aufgabenerstellung gewählt werden: Suche nach Passwort-Länge (setzen Sie die minimale und maximale Länge des Passwortes), Maskensuche (suchen Sie mit kleinen bekannten Passwort-Teilen nach dem Passwort) oder garantierte Wiederherstellungs-Schlüsselsuche. Die Symbolreihe kann auch eingeschränkt werden (gross- und kleingeschriebene Buchstaben, Zahlen, Sondersymbole etc). Der Administrator kann die Aufgabe jeden Augenblick bestimmen oder starten.

Einer der Produktvorteile ist die bequeme Arbeit mit mehreren Dokumenten. Elcomsoft Distributed Password Recovery ermöglicht das Erstellen der Dokumentenliste; die Suchreihenfolge kann in jedem Moment bearbeitet werden. Demnach hilft die ElcomSoft – Lösung beim Sparen der PC-Ressourcen und Arbeitszeit der Sicherheitsdienste.

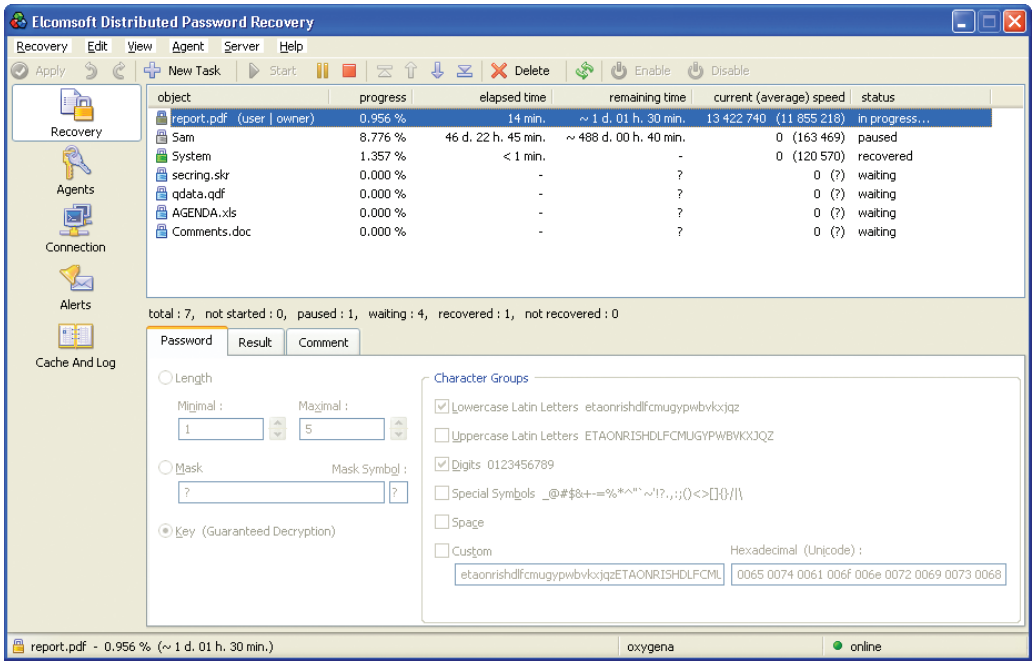


Bild 2. Hauptfenster von Elcomsoft Distributed Password Recovery (Komponent «Server»).

Zusätzlich zu den Vorteilen der Nutzung verteilter Datenverarbeitung für die Passwort- und Schlüssel - Wiederherstellung (siehe oben) lasst uns einige Vorteile von Elcomsoft Distributed Password Recovery zusammenfassen:

- **Unterstützung vieler Anwendungen.** Elcomsoft Distributed Password Recovery kann den Zugriff auf beliebige Dokumente schnell und effizient wiederherstellen.
- **Skalierbarkeit.** Das Produkt kann innerhalb des Netzwerkes jeder beliebigen Größe benutzt werden.
- **Minimale Netzwerk-Überlastung.** Archivierter Datenwechsel und minimierter Netzverkehr garantieren minimierte Überlastung des Netzwerkes.
- **Gründliche Abstimmung der Agent-Leistung.** Dauer der Arbeitszeit (Wochentage, Arbeitsstunden) und Aufgaben-Rangfolge können für die Agenten festgelegt werden.
- **Alle vorhandenen PCs nutzen.** Selbst die leistungsschwachen PCs im Netzwerk können hinsichtlich der Festlegung der Aufgaben-Reihenfolge, der Arbeitszeit für Agente und Software- und Hardware-Anforderungen benutzt werden.
- **Arbeit mit mehreren Dokumenten.** Beliebige Anzahl der Dokumente kann für die Passwort-Suche benutzt werden.
- **Reihenfolge der Dokumentenbearbeitung wählen.** Jeder Datei wird die Verarbeitungs-Rangfolge zugeteilt, die jederzeit verändert werden kann.

Server und Agent haben die Testversionen.

ÜBER ELCOMSOFT

Der 1990 gegründete russische Software-Entwickler ElcomSoft Co. Ltd. zählt zu den führenden Experten im Bereich Software zur Sicherheitsprüfung und Wiederherstellung von Passwörtern und Kennungen, mit denen sie Windows-Netzwerke sichern bzw. auf wichtige Dokumente zugreifen können. Dank der einzigartigen Technologien genießen die Produkte des Unternehmens weltweite Anerkennung.

Zu den Kunden von ElcomSoft zählen weltbekannte Unternehmen aus folgenden Branchen:

High Tech: Microsoft, Adobe, IBM, Cisco
Regierungseinrichtungen: FBI, CIA, US Army, US Navy, Department of Defence
Consulting-Unternehmen: Andersen Consulting, Deloitte & Touche, Ernst and Young, KPMG, PricewaterhouseCoopers
Finanzdienstleistungen: Bank of America, Citibank, Equifax, HSBC, Wells Fargo, J.P.Morgan, Credit Suisse
Telekommunikation: France Telecom, BT, AT&T
Versicherungen: Allianz, Mitsui Sumitomo
Handel: Wal-Mart, Best Buy, Woolworth
Medien & Unterhaltung: Sony Entertainment
Hersteller: Volkswagen, Siemens, Boeing
Energie: Lukoil, Statoil
Pharmazie: Johnson&Johnson, Pfizer, GlaxoSmithKline, Novartis

Das Unternehmen ist Microsoft Gold Certified Partner, Intel Software Partner, Mitglied der Russian Cryptologie Association (RCA), des Computer Security Institute (CSI) und der Association of Shareware Professionals (ASP).

Auf die technologischen Errungenschaften von Elcomsoft wird in vielen bekannten Büchern Bezug genommen, beispielsweise, in der Microsoft-Enzyklopädie „Microsoft Encyclopedia of Security", „The art of deception" (Kevin Mitnick), „IT Auditing: Using Controls to Protect Information Assets" (Chris Davis) und „Hacking exposed" (Stuart McClure).

Mehr über Elcomsoft können Sie auf der Webseite des Unternehmens erfahren.

ADRESSE:

ElcomSoft Co. Ltd.
Zvezdnyi blvd. 21, Office 541
129085 Moskau

FAX:

USA (toll-free): +1 (866) 448-2703
Großbritannien: +44 (870) 831-2983
Deutschland: +49 18054820050734

WEBSEITEN:

http://www.elcomsoft.ru
http://www.elcomsoft.com
http://www.elcomsoft.de
http://www.elcomsoft.jp
http://www.elcomsoft.fr