Kleiner Lauschangriff gegen Windows-Fernwartung

[26.07.2005 11:04]

Dirk Knop

Kleiner Lauschangriff gegen Windows-Fernwartung

Designschwäche im Remote-Desktop-Protokoll

Ein Designfehler in dem Remote-Desktop-Protokoll bietet jedem Mitarbeiter im Netzwerk die Möglichkeit, die Zugangsdaten zu fernadministrierten Windows-Servern auszuhorchen. Das Tool "Cain&Abel" verhilft selbst ohne Fachkenntnisse mit wenigen Mausklicks zum Administrator-Passwort.

Hinter Microsoft Windows Terminal Server und Remote-Desktop-Verbindungen in Windows XP stecken Dienste, die entferntes Anmelden und Arbeiten auf dem Rechner ermöglichen. Ursprünglich von Citrix entwickelt, um eine begrenzte Anzahl an Softwarelizenzen für viele Benutzer auf einem Server zugänglich zu machen, ergaben sich nach Lizenzierung durch Microsoft für die daraus entwickelten Terminal Services weitere logische Einsatzszenarien. Endlich ist auch ein Windows-Server vollständig aus der Ferne zu administrieren, die Fernwartung und Support von Benutzerrechnern fordert dem Administrator nicht mehr in jedem Fall eine Marathon-Strecke im Hause ab.

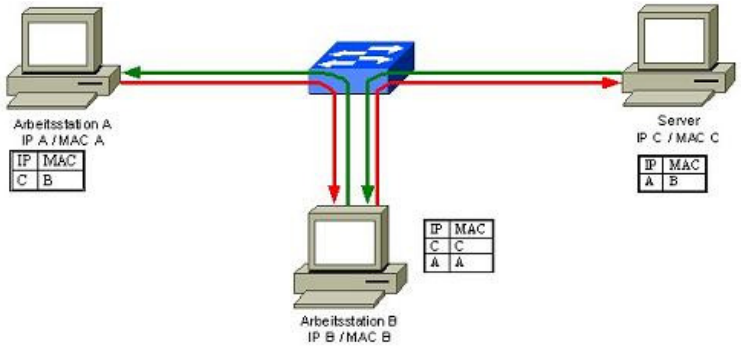
Selbst für den Privatgebrauch kommen die Terminal Services in Form des kleinen Bruders namens Remote Desktop zum Einsatz. So kann der begabte Enkel seinem weit entfernt lebenden Großvater dank der in Windows XP eingebauten Remote-Desktop-Unterstützung bei seinen Rechnerproblemen helfen.

Terminal Services und Remote Desktop setzen auf das Remote-Desktop-Protokoll (**RDP[1]**) auf. Für Unix und Linux gibt es mit **rdesktop[2]** einen RDP-Client, der das entfernte Windows auch auf den lokalen KDE- oder Gnome-Desktop holt.

Designfehler

Allerdings weist RDP eine gravierende Design-Schwäche auf: Client und Server müssen sich nicht gegenseitig authentifizieren. Aller Verschlüsselungsaufwand ist vergebens, wenn sich ein nicht vorgesehener Rechner in die Kommunikation unbemerkt einklinken kann. Schon im April 2003 zeigte Erik Forsberg in einem **Advisory[3]** einen erfolgreichen Man-In-The-Middle-Angriff (MITM) gegen RDP-Sitzungen.

Der Verkehr zwischen Client und Server ließ sich unbemerkt über eine dritte Station mittels ARP-Spoofing umleiten und mitprotokollieren (siehe [1]). So konnte er die **RC4[4]**-Schlüssel, mit denen die RDP-Verbindungen gesichert werden, erschnüffeln und zum Entschlüsseln des Traffics nutzen. Nach diesem MITM-Angriff lagen die Passwörter für den Serverzugriff dann im Klartext vor.



Arbeitststation B kann durch Manipulieren der ARP-Caches die Verbindung zwischen Arbeitsstation A und dem Server über sich umleiten.

[page_break]

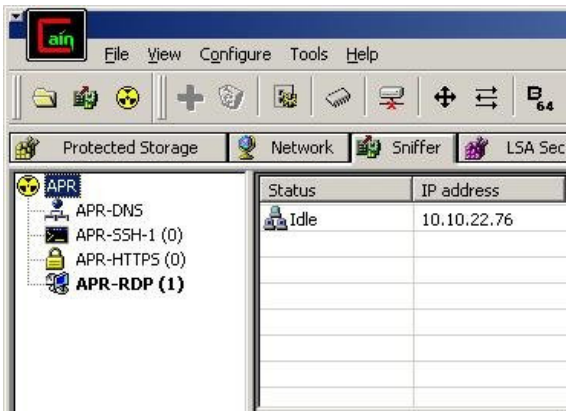
Nachschlüssel vom Schlüsseldienst

Mit den aktuelleren Versionen der Clients basierend auf RDP v5.2 gab es eine kleine Änderung gegenüber der Vorgängerversion: Der Server weist sich nun mit einem Zertifikat gegenüber dem Client aus. Damit ist der ursprüngliche MITM-Angriff so nicht mehr durchführbar. Wie Massimiliano Montoro feststellte, hat Microsoft seine Hausaufgaben aber leider nicht gründlich genug gemacht [2].

Der Server erstellt dieses Zertifikat, indem er seinen öffentlichen Schlüssel mit einem privaten Schlüssel signiert. Dieser private Schlüssel ist allerdings fest in die Datei `mstlsapi.dll` einprogrammiert. Diese DLL ist auf jedem Windows XP, Windows 2000 Server und Windows 2003 Server vorhanden -- der Schlüssel ist dabei immer derselbe.

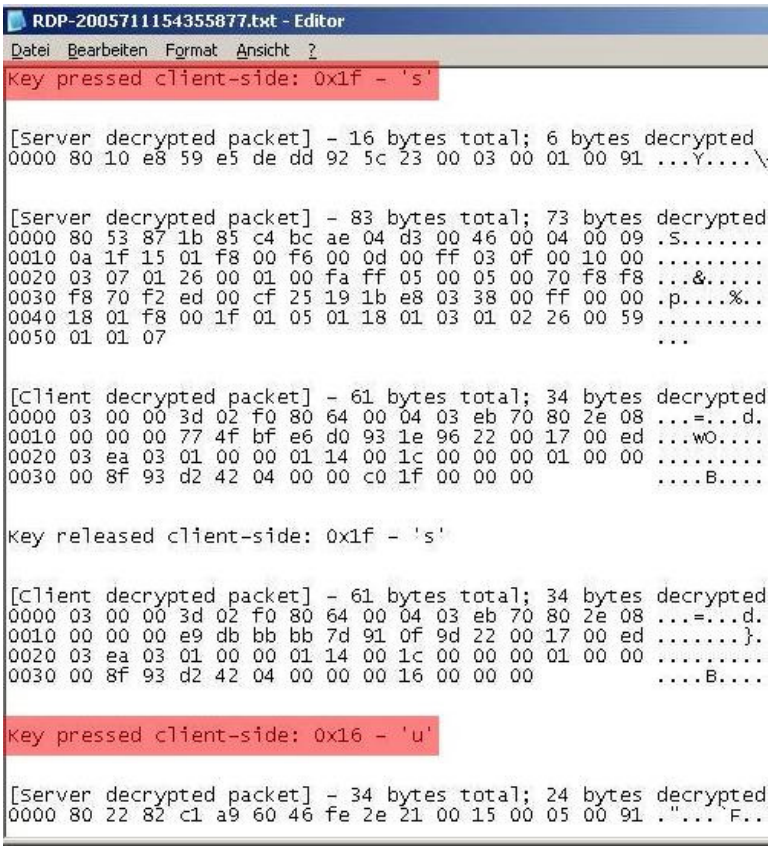
Daher ist es ein Leichtes, die "alte" Attacke mit kleinen Modifikationen weiterhin durchzuführen. Der Rechner in der MITM-Position muss

hierfür lediglich ein eigenes Zertifikat mit dem Schlüssel aus seiner DLL signieren und an den Client schicken. Dieser akzeptiert es ohne weitere Rückmeldung auf Client- oder Server-Seite.



[5]
Nach wenigen Mausklicks leitet Cain & Abel den RDP-Verkehr über sich um.

Das Security-Audit-Tool "Cain&Abel" unterstützt seit der Version 2.7 diese MITM-Attacke [3]. Mit wenigen Mausklicks lassen sich komfortabel die zu belauschenden Rechner auswählen, den Verkehr schneidet das Tool automatisch mit und entschlüsselt ihn auch gleich. In der Protokoll-Datei fanden sich bei unseren Tests dann die Tastenanschläge des sich anmeldenden Administrators. Damit ließ sich das Passwort sehr einfach rekonstruieren.



In der Log-Datei werden alle Tastendrücke mitprotokolliert -- auch die Passworteingabe.

[page_break]

Fazit

Microsoft ist dieser Sachverhalt sehr wohl bekannt. In einem Technet-Artikel vom Januar 2005 dokumentiert das Unternehmen die Problematik mit dem Satz: "Remote Desktop Protocol (RDP) provides data encryption, but it does not provide authentication to verify the identity of a terminal server." Deshalb schlagen die Redmonder vor, RDP-Verbindungen mittels Transport Layer Security (TLS) zusätzlich abzusichern [4].

Damit werden dann zwar die bereits verschlüsselten RDP-Pakete nochmals verschlüsselt. Aber dank der in TLS vorgesehenen Authentifizierung ist dann wenigstens sichergestellt, dass sich ein Angreifer nicht unbemerkt dazwischenmogeln kann. Laut Microsoft muss dafür allerdings der Terminal Server auf Windows Server 2003 laufen und der Client mit Windows 2000 oder XP.

Aufgrund der für das Opfer unsichtbaren Angriffsmöglichkeit verbietet sich der ungesicherte Einsatz von Terminal Services und Remote Desktop in Firmennetzen. Befindet sich der Angreifer nicht im selben Netz wie der RDP-Client oder -Server, fällt das Risiko geringer aus. Er müsste dann schon einen der Router auf dem Weg unter seine Kontrolle bringen, um einen MITM-Angriff durchzuführen.

Nach diversen Studien erfolgt jedoch die Mehrzahl aller Angriffe in Netzwerken nicht durch externe Hacker, sondern von innen. Unzufriedene oder einfach nur neugierige Mitarbeiter können sich auf diesem Weg auch ohne großes technisches Wissen kritische Zugangsdaten verschaffen. Arbeitsplätze mit eingeschränkten Benutzerrechten reduzieren dieses Risiko zwar, aber wenn der Mitarbeiter von einer CD booten oder ein mitgebrachtes Laptop ans Netz anschließen kann, hält ihn das nicht wirklich auf.

Wer als Administrator seine RDP-Verbindungen zur Wartung eines Benutzerrechners nutzt und sie nicht beispielsweise über TLS absichert, riskiert ein kompromittiertes Administrator-Kennwort. Ebenso ist die RDP-Sitzung zu Windows-Servern durch geeignete Maßnahmen abzusichern, auch hier ist der Zugriff ohne zusätzliche Authentifizierung tabu. (**dmk[6]**)

Literatur

[1] Gereon Ruetten, Oliver Stutzke; Angriff von innen, Technik und Abwehr von ARP-Spoofing-Angriffen; **heise Security[7]**
[2] Advisory von Massimiliano Montoro: **Microsoft RDP Man in the Middle Vulnerability[8]**
[3] Homepage von **Cain&Abel[9]**
[4] Technet-Artikel zu RDP: **Configuring authentication and encryption[10]**

URL dieses Artikels:
http://www.heise.de/security/artikel/61945

Links in diesem Artikel:
[1] http://www.microsoft.com/windows2000/techinfo/howitworks/terminal/ rdpfandp.asp
[2] http://rdesktop.sourceforge.net/
[3] http://seclists.org/lists/bugtraq/2003/Apr/0038.html
[4] http://de.wikipedia.org/wiki/RC4
[5] /bilder/61945/0/1
[6] mailto:dmk@heisec.de
[7] http://www.heise.de/security/artikel/55269/0
[8] http://www.securiteam.com/windowsntfocus/5EP010KG0G.html
[9] http://oxid.it/cain.html
[10] http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/a92d8eb9-f53d-4e86-ac9b-29fd6146977b.mspx