Schach dem Spion

Immer mehr Spieler nutzen das Internet als Schachplattform. Kein Wunder, denn die Vorteile liegen auf der Hand: Zum einen findet sich dort für jeden, vom Anfänger bis zum Großmeister, ein passender Gegner. Zum anderen besteht keine Notwendigkeit, durch Sprühregen und Schneematsch zum Schachklub zu stapfen, man kann bequem zu Hause im Sessel sitzend spielen. Server-Schach gegen Gegner aus aller Welt macht sogar ein kleines bisschen süchtig. Doch das Schachspiel im Internet hat auch seine Schattenseiten – während man bei einer "realen" Partie seinem Gegner von Angesicht zu Angesicht gegenübersitzt, ist das im Internet eben nicht so. Das bedeutet, dass man über die Identität des Schachpartners normalerweise nichts weiß. Die Spieler identifizieren sich ausschließlich über ihre Nicknamen und ihre erspielte Spielstärke. Aber wer garantiert, dass man tatsächlich gegen den Hobbyspieler mit einer Elo-Wertung von 1300 spielt und nicht etwa gegen dessen Nachbarn, der zufällig Schachgroßmeister ist und weit über 2500 Elo liegt?

Zwar hat nicht jeder einen Großmeister in der Nachbarwohnung, aber das größere Problem besteht ohnehin in der Verwendung von Schachsoftware. Auf heutiger Hardware reichen auch bei frei verfügbaren Engines wie Crafty wenige Sekunden Bedenkzeit, um selbst Meister gegen die Wand zu spielen.

Die meisten Spieler, die sich mit Hilfe einer Schach-Engine Vorteile verschaffen, tun dies wohl, um sich mit einer höheren Elo-Wertung auszuzeichnen als sie spielerisch verdienen. Die Verlockung zu schummeln steigt besonders dann, wenn innerhalb eines Internet-Turniers Preisgelder vergeben werden – das ist mittlerweile durchaus üblich und macht das Cheaten daher besonders prekär. Doch die Motive fürs Schummeln sind letztlich irrelevant; Fakt ist, dass es Cheater auf jeder Schach-Plattform gibt, die ehrlichen Spielern zunehmend den Spielspaß verderben. Es gibt verschiedene Mechanismen, um gegen solche regelwidrigen Verstöße vorzugehen.

Technische Kontrolle

Die drei großen Plattformen – Playchess, ICC und FICS – schlagen dabei grundsätzlich unterschiedliche Wege ein. Playchess, der kostenpflichtige Schachserver von ChessBase, geht dabei am schärfsten vor: Zum einen überprüft der Client den Rechner des Nutzers auf so genanntes Task-Switching, also ob der Spieler während einer Schachpartie zu anderen Programmen wechselt. Geschieht dies zu häufig, besteht ein grundlegender Cheat-Verdacht; der Spieler wird markiert und seine Elo-Wertung gelöscht.

ChessBase hat einen Cheater erwischt

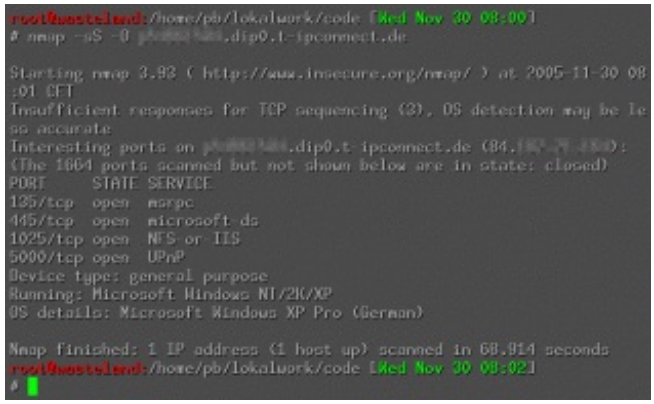
Es leuchtet ein, dass bei dieser Methode auch Spieler zu Unrecht unter Verdacht geraten. Etwa dann, wenn der Gegner in längeren Partien etwas träge spielt und man sich daher die Zeit mit Surfen im Internet vertreibt oder nebenbei per Instant Messenger chattet. Daher setzt Playchess zusätzlich noch auf andere Schutzmechanismen. So überwacht der Schach-Client außerdem die Prozessliste des Rechners und blickt sogar in die Fenstertitel anderer Programme, um nebenher laufende Schachsoftware zu erkennen. Diese Methode ist äußerst strittig, Sicherheitsexperten läuft es dabei eiskalt den Rücken runter, denn das sind Mechanismen, die ebenso von klassischer Spyware genutzt werden. Da der Datenverkehr zum ChessBase-Server verschlüsselt stattfindet, kann der Anwender nicht überprüfen, welche Daten der Client tatsächlich an den Server übermittelt. Aus datenschutzrechtlicher Sicht ist dieses Verhalten höchst bedenklich.

Der Internet Chess Club

Und die Effektivität solcher Maßnahmen darf zurecht angezweifelt werden: Die Titelzeile eines Programms lässt sich sehr leicht manipulieren, und auch ein Fenster vor der Taskwechselerkennung zu verstecken kostet einen halbwegs talentierten Programmierer keine zehn Minuten. Sobald der Cheater seine Analyse-Software auf einem Zweitrechner einsetzt, laufen ohnehin alle technischen Überwachungsmaßnahmen ins Leere. Letztlich dürfte mit solch fragwürdigen Methoden nur ein kleiner Teil der Schach-Schummler entlarvt werden, zumal es neben dem Einsatz von Schachsoftware noch ganz andere Möglichkeiten des Cheatens gibt.

Die Tragweite des Problems wurde bei ICC (Internet Chess Club), der mit über 30.000 Spielern größten Schach-Plattform, deutlich: Dort prüfen die Clients zwar nicht die Prozessliste des Rechners, dafür aber kann die Bezahlung der Accounts über den Client stattfinden – per Paypal oder Kreditkarte. Die Amerikaner John Black, Martin Cochran und Ryan Gardner haben im Dezember 2004 ein Paper veröffentlicht, das zeigt, dass die Verschlüsselung von ICC diverse Schwachstellen aufweist. Es war den Autoren ohne größere Schwierigkeiten möglich, als so genannter Man-in-the-middle sensitive Daten wie Paypal-Passwörter und Kreditkarteninformationen abzugreifen. Nebenbei gelang es ihnen dabei auch, die Zeitkontrolle auszuhebeln und Züge quasi ohne Bedenkzeit zu übermitteln – eine ganz andere Form des Cheatens.

Neben den Einsatz von Schachsoftware gibt es ohnehin noch ganz andere Methoden, um sich in einer virtuellen Schachpartie einen Vorteil zu erschleichen. Ein nahe liegender Hebel ist der Datenverkehr an sich. Sowohl ICC als auch ChessBase verschlüsseln den Netzverkehr, damit Manipulation nicht allzu einfach möglich ist. Wie aber Black, Cochran und Gardner zeigten, ist dies auch kein unüberwindliches Hindernis. Im Rahmen ihrer Studie gelang es ihnen auch, durch Aushebelung der Verschlüsselung ungültige Züge an den Schach-Server zu übermitteln – die der Schachclient normalerweise verhindert.



Den Portscanner NMAP gibt es gratis für fast alle Betriebssysteme

Bei ChessBase kommt hinzu, dass die Clients standardmäßig eine Direktverbindung (DCC, Direct Client to Client) aufbauen – das heißt, dass die Rechner der Schachspieler direkt kommunizieren, ohne dazwischengeschalteten Schachserver. Das vermindert den so genannten Netlag – also die Latenz zwischen den Zügen, birgt aber ein weiteres Risiko, denn zwangsläufig muss den beiden Clients jeweils die IP-Adresse des Gegners bekannt sein. Das ermöglicht beispielsweise einen direkten Denial-of-service-Angriff auf den Rechner des Gegners: Durch das massenhafte Senden von SYN-Paketen ließe sich beispielsweise die Verbindung des Gegners unterbrechen, wodurch man sich zumindest einen Zeitvorteil erschleichen kann. Durch die Übermittlung der IP-Adresse können aber noch ganz andere Probleme entstehen. Denn im Unterschied zu Chat-Protokollen wie IRC sind sich die meisten Schachspieler wohl nicht einmal bewusst, dass ihre IP-Adresse übertragen wird. Und man kann auch nicht davon ausgehen, dass jeder Internet-Schachspieler hinter einer wasserdichten Firewall sitzt, sondern eher auf einer mehr oder weniger geschützten Windows-Kiste arbeitet und spielt.

Ein Angreifer hat mit Kenntnis der IP-Adresse die Möglichkeit, gezielt über Schwachstellen in den Rechner einzubrechen. Oft reißen Anwender auch erst selbst Sicherheitslücken auf, indem sie fragwürdige Security-Software einsetzen – eine Funktion vieler "Personal Firewalls" besteht etwa darin, IP-Adressen zu sperren, von denen ein echter oder vermeintlicher

Angriff kam. Solcher Software einen Angriff von der IP des Schachservers vorzugaukeln ist eine Leichtigkeit für jeden, der den Portscanner NMAP kennt. Die Folge: Die IP des Schachservers wird gesperrt. Dieser nimmt an, die Verbindung wäre unterbrochen, weil er keine Antwort auf seine Anfragen erhält – und der Cheater gewinnt per Zeitüberschreitung. Vor allem ältere Personal Firewalls, die sich oft auf Heft-CDs diverser Computerzeitschriften finden, aktivieren diese Funktion nach der Installation automatisch; neuere Versionen tun dies meist nicht, doch kann ein paranoider Anwender das selbst tun – wovon unbedingt abzuraten ist, denn diese Funktion schafft ein Problem, wo keins ist und stuft selbst harmlose Portscans als gefährliche Angriffe ein. Von all den Buffer-Overflows, die in solch vermeintlicher Sicherheitssoftware lauern und die wöchentlich in der Fachpresse gemeldet werden, erst gar nicht zu reden. Besser ist es daher, die Einfallstore zu schließen, wie hier beschrieben. Gegen die Möglichkeit, dass die Schachclients selbst Schwachstellen aufweisen können, hilft das freilich ebensowenig wie alle Firewalls dieser Welt.

Das soll nicht heißen, dass bei jeder DCC-Verbindung gleich ein Angriff erfolgt – das dürfte vielmehr eine Ausnahme sein. Es zeigt aber, dass bei jedem technischen Verfahren, mehrere Angriffsvektoren existieren, mehrere Möglichkeiten, das Verfahren auszuhebeln – bei der Übertragung von Daten im Internet gibt es keine hundertprozentige Sicherheit. Für den Schutz vor Cheatern gilt das genauso, wer wirklich schummeln will, findet meistens auch einen Weg, und das nicht nur beim Schach. Bei allen Multiplayer-Spielen wird geschummelt, und welche Maßnahmen sich die Hersteller und Betreiber auch ausdenken, die Cheater finden immer wieder einen Weg drumherum. Bei Quake oder Enemy Territory wird beispielsweise die technische Kontrollsoftware Punkbuster eingesetzt, aber auch hier findet ein ständiger Wettlauf zwischen Cheatern und Punkbuster-Entwicklern statt, da immer neue Tricks auftauchen.

Fazit

Technische Maßnahmen greifen erfahrungsgemäß am wenigsten, das ist beim Schach nicht anders als bei Quake. Der vielversprechendste Ansatz zur Überführung von Schummlern besteht in einem analytischen Verfahren, dass ChessBase zusätzlich anwendet: Hierbei werden die verdächtigen Partien anhand von ausgeklügelten Algorithmen überprüft, um den potenziellen Einsatz von Software aufzudecken. Nach Angaben der ChessBase-Entwickler ist dieses Verfahren so zuverlässig, dass sogar Großmeister beim Schummeln entlarvt werden können – was in der Vergangenheit wohl auch vorgekommen ist. Der Nachteil des analytischen Verfahrens besteht darin, dass mehrere Partien untersucht werden müssen, um halbwegs zuverlässige Aussagen zu treffen; dennoch bleibt auch dann ein Rest Unsicherheit, denn die Analyse wirft nur eine Schummelwahrscheinlichkeit aus, kann den Cheat aber nicht beweisen. Auf die vielen tausend täglich gespielten Partien kann ChessBase dieses Verfahren mangels Rechenkapazität nicht anwenden.

Der kostenlose Schachserver FICS

Beim kostenlosen Schachportal FICS verzichten die Betreiber komplett auf eine technische Kontrolle, weder Taskswitching noch Prozesslisten werden überwacht, stattdessen findet eine rein menschliche Überprüfung statt. Bei Cheat-Verdacht können sich die Spieler an spezielle Administratoren wenden, die die verdächtigen Partien analytisch kontrollieren. Bestätigt sich der Cheat-Verdacht, kann die Partie nachträglich annuliert, beziehungsweise für den Cheater als verloren gewertet werden.

Auch die ChessBase-Entwickler räumen ein, dass das analytische Verfahren am erfolgversprechendsten ist. Zumal mit den technischen Mitteln nur die Dummbrote und Cheat-Anfänger entlarvt werden können. Hier sollte der Respekt vor dem Datenschutz höhere Priorität haben. Aufgrund des Zeitaufwands und beschränkter Rechenkapazitäten werden normalerweise nur Turnierspiele auf Schummeln analysiert, für die Tausenden von spontanen Schachpartien findet das meistens nicht statt. Aber auch für diese Spieler gibt es einen vielversprechenden Schutz vor Cheatern, der übrigens auch auf jedes andere Multiplayer-Spiel angewandt werden kann: Spielen Sie bevorzugt mit Spielern, von denen sie wissen, dass sie nicht schummeln und wärmen Sie Leuten, gegen die Sie Verdacht hegen, ein hübsches Plätzchen auf Ihrer Ignore-Liste. – Vertrauen ist nach wie vor die beste Garantie für ein optimales Spielvergnügen. *(Patrick Brauch)*