And the Winner was...

Wie es mit dem besten studentischen Beitrag vom BSI-Kongress 2007 weiterging

In Kooperation mit dem Fraunhofer IGD und dem INI-Graphics-Net ist auf dem 10. Deutschen IT-Sicherheitskongress 2007 der beste Beitrag eines Studenten ausgezeichnet worden (vgl. <kes> 2007#3, S. 41). Der Gewinner Dominik Birk erhielt ein Stipendium für ein 6-monatiges Praktikum innerhalb des INI-GraphicsNet. Das Projekt des Gewinners hat mittlerweile Fortschritte gemacht, das Praktikum weitere Projekte nach sich gezogen.

Von Dominik Birk, VICOMTech

Im Mai 2007 haben sich Dominik Birk und Felix Gröbert gegen drei Mitstreiter im Rennen um den „Best Student Paper Award" des 10. Deutschen IT-Sicherheitskongresses des BSI durchsetzen können. Bei dem Beitrag über ein „Framework zur Identifikation von Identitätsbetrügern, Geldwäschern und Phishing-Simulanten" handelte es sich nicht um eine Abschlussarbeit, sondern um ein „freiwilliges" Paper, das in etlichen Nächten neben den universitären Pflichten ausgearbeitet wurde.

Rückblick: Das Framework

Die gängigen Ansätze gegen Phishing sind meist rein passiver Art wie beispielsweise Blacklisting, Anti-Phishing-Toolbars für Browser oder der Einsatz aktueller Virenscanner. Der „siegreiche" Vorschlag von 2007 ist hingegen aktiver Art und versucht, den Angreifer (Phisher) mit seinen eigenen Waffen zu schlagen: Dies geschieht dadurch, dass eigens für diesen Zweck erstellte, gefälschte Nutzerdaten, so genannte „Phoneytokens" (Phishing-Honey-Token), erstellt und in großer Menge an den Phisher übertragen werden. Bei der Auswertung gephishter Accounts lässt sich dann nicht mehr differenzieren, welche Zugangsdaten valide sind und bei welchen es sich um Phoneytokens handelt. Die einzige Möglichkeit für den Phisher wäre, alle Accounts automatisiert zu überprüfen, was jedoch der Betreiber der gephishten Site (Bank o. Ä.) durch den Einsatz von Turingtests (Captchas) unterbinden kann.

Der im prämierten Paper beschriebene Ansatz geht davon aus, dass der Phisher versuchen wird, Phoneytokens und gültige Zugangsdaten von Opfern zu unterscheiden und zwar anhand der Übertragung und einzelner Attribute der Phoneytokens selbst. Der „Phoneytokensender", also die Instanz, welche die Token an den Phishingserver überträgt, muss daher so arbeiten, dass keinerlei Unterschied zur Übertragung durch ein reales Opfer ersichtlich wird. Technisch gesehen ist der Phoneytokensender also ein virtuelles Opfer einer Phishingattacke.

Zunächst müssen dazu die Phoneytokens im Kontext der Phishingwebseite erstellt werden: Es ist beispielsweise nicht sinnvoll, deutsche Namen und Adressen auf eine Phishingwebseite zu übertragen, die den US-amerikanischen Raum fokussiert; des Weiteren müssen Loginname und Passwort wie auch gegebenenfalls PIN und TANs an die entsprechende Site (z. B. Kreditinstitut) angepasst werden.

Bei der Übertragung ist es wichtig, die jeweilige Zeitzone zu beachten: Es gab beispielsweise Studien, die besagten, dass die meisten Phishingopfer in den USA ihre persönlichen Informationen morgens zwischen 9 und 10 Uhr an den Phishingserver übertragen. Es wäre also verräterisch, die meisten Phoneytokens nachts zu übertragen. Zudem muss der Phoneytokensender neben der eigentlichen Phishingwebseite sämtliche zusätzliche Daten nachladen: Um nicht aufzufallen, müssen sämtliche Schritte eines realen Opfers nachgestellt werden. Dazu gehören auch alle Bilder, Stylesheets (CSS) und Javascript-Dateien und eine entsprechende zufällige „Wartezeit" bis zur Übermittlung der Phoneytokens: Diese sollte sich im Rahmen der Zeit bewegen, die ein reales Opfer für das Ausfüllen der Formulare benötigen würde. Anschließend sollten auch die Seiten nachgeladen werden, die ein Browser dem Opfer anzeigen würde.

Mit diesen Methoden lässt sich verhindern, dass ein Phisher mit einem Blick in die Logfiles Phoneytokens aussortieren kann, indem er den Phoneytokensender durch unvollständiges Verhalten identifiziert. Problematisch gestaltet sich dabei zudem eine hinreichende Divergenz benutzter IP-Adressen: Theoretisch würde zwar ein statischer Phoneytokensender ausreichen, allerdings könnte dann ein Angreifer mit einem Blick alle Phoneytokens dieses Senders aussortieren. Zur vollständigen Simulation von Phishingopfern wird also ein möglichst großer, authentischer Pool an IP-Adressen benötigt, der vor allem viele dynamische IPs großer Provider enthält.

Ausblick: Beta voraus!

Zur Lösung dieses Problems hatte das Paper eine Implementierung vorgeschlagen, die Teilnehmer im Internet in das Framework einbezieht. Mittlerweile steht der Autor

kurz vor der Veröffentlichung einer Beta-Version der Implementierung dieses Frameworks, die in den letzten Monaten parallel zu anderen Projekten vorangetrieben wurde. Angestrebt ist dazu eine offene Implementierung als Firefox-Erweiterung, die zum freien Download zur Verfügung steht. Sämtliche Firefox-Nutzer könnten damit am beschriebenen Anti-Phishing-Framework teilnehmen, indem sie einfach diese Erweiterung installieren.

Das Plug-in kommuniziert mithilfe kryptografischer Protokolle mit einem zentralen System, das Daten verifizierter Phishing-Webseiten an die verschiedenen Teilnehmer (Firefox-Erweiterungen) verteilt. Anschließend öffnen diese Clients eine Verbindung zum Phishing-Server und simulieren ein Phishingopfer.

Phisher, die anschließend versuchen, die gephishten Accounts zu missbrauchen, können derartige Phoneytokens nicht von gültigen, gephishten Datensätzen unterscheiden. Neben der Verhinderung illegaler Finanztransfers könnte dies auch helfen, Phisher dingfest zu machen, indem Banken oder andere Sitebetreiber mit dem Framework zusammenarbeiten: Denn Login-Versuche mit bekannten Phoneytokens lassen sich registrieren und gegebenenfalls an die Behörden weiterleiten. Dass heutige Phishing-Angriffe vermehrt auf Malware und größtenteils nicht mehr auf reinen E-Mails basieren, ist dabei kein Problem – das beschriebene Framework ist auch in diesem Szenario einsetzbar.

Einblick: Neue Projekte

Durch den Gewinn des Preises hatte der Autor die Möglichkeit, ein 6-monatiges Stipendium in einer internationalen Forschungseinrichtung der INI-GraphicsNet-Stiftung in Zusammenarbeit mit dem Fraunhofer-Institut für Graphische Datenverarbeitung IGD anzutreten. Die INI-GraphicsNet Stiftung ist ein internationales Netz von Institutionen zur Aus- und Fortbildung, Forschung und Entwicklung und seine Mitglieder beschäftigen sich hauptsächlich mit grafischer Datenverarbeitung. Für einen Studenten der IT-Sicherheit ergab sich damit eine gute Gelegenheit „über den Tellerrand“ hinauszublicken. Nach ausgiebigen Gesprächen fiel die Wahl auf das VICOMTech – Visual Communication and Interaction Technologies Centre in San Sebastian (Spanien), da es dort auch einen Bereich für IT-Sicherheit gibt. Seit Anfang Mai arbeitet der Autor nun in diesem Institut, das eines der angesehensten Technologiezentren in der Region ist und auf dem Gebiet der grafischen Datenverarbeitung und Multimedia jede Menge praxisnahe Forschungsthemen bietet.

Erschien zuvor die Relevanz der grafischen Datenverarbeitung für die IT-Sicherheit noch unklar, so änderte sich dies mit Beginn dieser Arbeit in Spanien schlagartig: Eine der herausragenden Eigenschaften der IT-Sicherheit ist die Möglichkeit, diverse andere Forschungsfelder mit ihr zu verbinden. Meist ergeben sich dann neue Möglichkeiten und Problemlösungen, die sich ansonsten nur schwer erarbeiten ließen. Konkret ergab sich eine Mitarbeit an einem Framework, das Multimediastreams eindeutig mit einem Wasserzeichen markiert und gleichzeitig den Sender über eine digitale Signatur authentifiziert.

So soll beispielsweise ein Anbieter von Broadcasts oder Multicast-Multimedia-Streams gegenüber einer dritten Partei beweisen können, wann und wie oft er täglich einen Stream abgespielt hat. Broadcastbetreiber für Radio und Fernsehen werden oft finanziell von Urheberrechtsvertretern für ihre Publikation belangt. Dabei kann es sein, dass der Broadcaster mehr bezahlt als er eigentlich müsste, da nicht genau nachzuweisen ist, wann welches Medium wie oft publiziert wurde. Das angestrebte Framework soll dieses Problem lösen, indem eine Agentur, die so genannte „Monitoring Agency“, ständig die gesendeten Broadcasting-Streams beobachtet und mithilfe des eingebetteten Wasserzeichens und der Authentifizierung genau feststellen kann, wann welcher Broadcaster welches Medium wie oft gesendet hat. Die Agentur erstattet dem Urheberrechtsvertreter anschließend Bericht, der nicht verfälscht werden kann, da auch der Vertreter Mitglied in der genutzten Sicherheitsinfrastruktur ist und die Datenübertragung gegebenenfalls verifizieren kann.

Dieses Thema erwies sich als sehr vielseitig, da es etliche verschiedene Gebiete wie Watermarking-Algorithmen, Public-Key-Infrastrukturen (PKIs) oder auch Next Generation Multimedia Networks (IPTV) verbindet. Darin liegt eine große Herausforderung, zumal es sich um eine praktische Anwendung handelt und nicht nur um theoretische Gedankenspielereien, wie man sie bisweilen im universitären Umfeld findet.

Zurzeit evaluiert der Autor hierzu bestehende Signaturschemata daraufhin, ob sie den Anforderungen dieser spezifischen Applikation gewachsen sind: Durch den sehr beschränkten Raum, der zur Einbettung eines Wasserzeichens in einen Multimediastream zur Verfügung steht, sind viele gängige Schemata wie RSA nicht geeignet, da die entstehenden Signaturen schlichtweg zu groß sind. Es müssen also alternative Verfahren gefunden werden, deren Signaturen in die verfügbaren „Slots“ passen.

Mein aufrichtiger Dank gilt der Jury des Best Student Awards anlässlich des BSI-Kongresses 2007 sowie Herrn Jorge Posada, dem Leiter von VICOMTech, für die Möglichkeiten, die er mir an seinem Institut bietet. Auch Herrn Alexander Nouak (Fraunhofer IGD) und Herrn Dr. Joachim Rix (INI-GraphicsNet) möchte ich herzlich für die Hilfsbereitschaft bei kleineren und größeren Problemen danken. – Dominik Birk ■