HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Kurzfassung der Studienarbeit

Abteilung	**Informatik**
Name der Studentin / des Studenten	**Andreas Hofmann** **David Brüllmann**
Studienjahr	**2004**
Titel der Studienarbeit	**WLAN Hot Spot Usertracking**
Examinatorin / Examinator	**Beat Stettler**

Kurzfassung der Studienarbeit

Wie der Name es bereits sagt, geht es darum die User zu tracken. Tracken bedeutet soviel wie den User zu verfolgen damit er in seiner „Spur“ bleibt. Er soll dabei auch nicht von etwaigen Angreifern beeinträchtigt werden. Eine weitere Vorgabe betraf die Installation von zusätzlicher Software. Kein Kunde soll spezielle Software installieren müssen. WLAN benutzt man spontan und mit einer Installation wäre die Spontaneität drastisch eingeschränkt. Geschäftskunden ohne lokale Administratorenrechte könnten das WLAN gar nicht benutzen.
Auf der Suche nach solchen Methoden mussten wir feststellen, dass es eine vollständige und sichere Lösung nur auf der Hardwareebene gibt. Leider können wir aber die WLAN Spezifikationen nicht ändern. Wir fanden dennoch einen Weg, wie wir auf Softwareebene die Benutzer beobachten und dabei Unregelmässigkeiten festhalten können. Ein allfälliger Angreifer wird also von unserer Software erkannt. Diese Erkennung können wir durch zusätzliches Verschicken von ARP Requests bestätigen. Entstehen aufgrund unserer ARP Request zwei ARP Responses wissen wir mit 100%iger Sicherheit, dass zwei Computer mit gleicher MAC Adresse im Netz sind. Da eine MAC Adresse aber eindeutig einer Netzwerkkarte zugeordnet ist, bedeutet dies einen Angriff. Die MAC Adresse kann mit gewissem Fachwissen gefälscht werden.
Unser Programm funktioniert folgendermassen: Jedes IP Paket enthält eine so genannte IP ID. Diese IP ID ist theoretisch aufsteigend von 0 bis 65535 anzutreffen. Wir stellten eine Kontinuität bei den Betriebssystemen Windows 2000, Windows XP und MAC OS 10 fest. Diese Kontinuität erlaubt uns, den Surfer anhand dieser IP ID zu verfolgen. Stimmt nun diese Kontinuität nicht mehr, registriert dies unser Programm. Wenn der Benutzer sich abmeldet oder fünf Minuten nicht mehr reagiert, gilt seine Verbindung als unterbrochen und das Programm erstellt einen Logeintrag mit allen gesammelten Daten über den User. Ein zusätzlicher Knackpunkt war für uns die VPN Verbindung. Oft bauen Geschäftsleute eine sichere Verbindung zu ihrem Unternehmen auf. Aber auch diese IP ID können wir mit unserer Software verfolgen. VPN Aktivität registrieren wir ebenfalls im Logfile.
Im Logfile finden wir also eine Zusammenfassung, was alles für Fehler auftreten und ob Attacken ausgeübt wurden. Anhand dieser Aufstellung kann ein Hot Spot Betreiber feststellen ob in seinem Netz Angriffe stattfinden. Gegebenenfalls könnte er direkt intervenieren, die unrechtmässigen Benutzer stellen und Schadenersatz fordern.