HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Kurzfassung der Semesterarbeit

Abteilung	**Informatik**
Name der Studentin / des Studenten	**Marius Müller** **Alexander Hitz**
Diplomjahr	**WS 2004/2005**
Titel der Studienarbeit	**WLAN Intrusion Detection System**
Examinatorin / Examinator	**Prof. Beat Stettler**

Kurzfassung der Diplomarbeit

In dieser Arbeit geht es um Sicherheit bei WLAN Hot-Spots. In einem solchen öffentlichen Umfeld muss meist auf eine WEP Verschlüsselung verzichtet werden, da ein "geheimer" Kanal zum Benutzer fehlt, um ihm den WEP Schlüssel sicher mitzuteilen. Ohne WEP Verschlüsselung ist ein Benutzer nun aber fast beliebig attackierbar. Beispiele sind Man-in-the-middle Attacken, ARP-Spoofing, MAC-Spoofing etc.
Unsere Arbeit besteht nun darin, ein Intrusion Detection System auf einen Accesspoint von der Firma ASCOM zu implementieren. Auf diesem Accesspoint läuft BusyBox, ein embedded Linux. Das Wireless-Interface kann in den Monitor Mode gesetzt werden, und kann somit alle Pakete aus der WLAN Umgebung sniffen.
Dieses eingesetzte Intrusion Detection System soll Attacken in einer WLAN Umgebung detektieren und Alarmmeldungen an einen Administrator senden. Ein solcher Accesspoint kann in einer Hot-Spot Umgebung (z.B. Flughafen Zürich) installiert werden.
Wir haben begonnen, uns über Wireless-Attacken und den Aufbau eines Intrusion Detection System zu informieren. Nach einer Einarbeitungsphase schauten wir uns um, was für bestehende Intrusion Detection System Produkte schon vorhanden sind und was deren Stärken und Schwächen sind. Wir haben uns dann für das Open Source Projekt Snort-Wireless entschieden, da dieses die meisten nützlichen Features enthält. Snort-Wireless erkennt MAC-Spoofing, Authentication- sowie Deauthentication flooding, gefälschte Accesspoints sowie aktives Accesspoint Scanning. Zusätzlich besitzt es verschiedene Outputmöglichkeiten, wie Meldungen an den Syslogdeamon. Dieser sendet die Meldung an den angegebenen Syslogclient (Administrator), oder die Log-Meldung mit Hilfe eines dazuinstallierten Outputplugin an eine Datenbank (z.B MySQL, PostgreSQL, Oracle, SQL Server sowie unixODBC). Wir verwenden das Versenden über Syslog.
Ein weiterer wichtiger Vorteil von Snort-Wireless ist, dass es über eine riesige Community verfügt und stehts weiterentwickelt wird. Wird also eine neue Angriffsart entdeckt, ist innerhalb kürzester Zeit eine Signatur, die diese Attacke erkennt, auf dem Internet verfügbar.
Da der ASCOM Accesspoint jedoch eine MIPS Architektur besitzt, der mit Big Endian arbeitet, mussten wir einige Teile des vorhandenen Sourcecodes anpassen, damit Snort-Wireless auch auf dem Accesspoint richtig funktioniert. Dieser angepasste Sourcecode wird dann mit einem Crosscompiler kompiliert. Es müssen dazu jedoch noch bestimmte Libraries eingebunden werden. Danach kann das kompilierte Binary über das Ethernet Interface, das der Accesspoint besitzt, heraufgeladen und gestartet werden.