HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Kurzfassung der Semersterarbeit

Abteilung	**Informatik**
Name der Studenten	**René Herrmann** **Christian Bernet**
Semester	**SS 2002**
Titel der Semesterarbeit	**Distributed Wireless Honeypot**
Examinatorin / Examinator	**Ivan Bütler / Christoph Schnidrig**

Kurzfassung der Diplomarbeit

Der Wechsel von den üblichen Netzwerken zu den Wireless Local Area Networks (WLAN) birgt auch neue Gefahren in sich. Betreibt eine Firma einen WLAN Zugangspunkt (Access Point), kommt eine neue Angriffsmöglichkeit hinzu, wie das interne Netzwerk der Firma angegriffen werden kann. Angreifer, sogenannte Wardriver, die mit Laptop, Wireless-Karte und entsprechenden Tools ausgerüstet sind, versuchen Access Points auszuspionieren. Der Distributed Wireless Honeypot (DWHP) konzentriert sich in erster Linie darauf den Einsatz solcher Wardriving-Tools zu erkennen und Daten über den Angriff in einer zentralen Datenbank zu speichern.

Der DWHP beinhaltet einen Access Point der als Lockvogel (Honeypot) fungiert, einen Master der die gesammelten Informationen auf einer Webseite publiziert und einem oder mehreren Agents die den WLAN-Datenverkehr überwachen. Einerseits ist es dem DWHP möglich zu registrieren wie oft, von welcher MAC-Adresse aus und in manchen Fällen auch mit welchem Programm ein Access Point angegriffen wird, anderseits kann er auch alle WLAN-Pakete zur späteren Analyse aufzeichnen. Der aufgezeichnete Datenverkehr wird im Dateiformat der gängigen Netzwerkanalyse Tool Ethereal und TcpDump gespeichert. Beim Starten eines Agents kann ihm auch eine bereits aufgezeichnete Datei zur Analyse übergeben werden.

Erkennt ein Agent einen Angriff, sendet er dem Master einen sogenannten Alert. In einem Alert steht die MAC Adresse des Angreifers, von welcher Art der Angriff war und zu welchem Zeitpunkt der Angriff stattfand.

Die Erkennungsmuster (Patterns) auf die ein Agent reagiert sind in einer XML-Datei konfigurierbar. In der XML-Datei wird beschrieben, welche Abfolge von Paketen einen Alert auslösen. Dabei können die Werte aller Felder eines Frames des 802.11 MAC Layers mittels Regulären Ausdrücken spezifiziert werden. Somit ist gewährleistet, dass der DWHP auch für die Erkennung von zukünftigen Angriffstools eingesetzt werden kann.