Intrusion Detection in 802.11 Wireless Networks

Andreas Grosse

Inhaltsverzeichnis

Einführung / Momentane Situation

So wie sich das Mobiltelefon im Kommunikationsmarkt in den letzten Jahren durch seine Flexibilität und den daraus resultierenden Komfortgewinn etabliert hat, finden im Netzwerkbereich kabellose Netzwerke immer größeren Zuspruch. Trotz verschiedener physikalischer Übertragungstechniken haben sich mittlerweile einige Schnittstellen etabliert. Schon längere Zeit werden Infrarotschnittstellen (IrDA) zur Kommunikation zwischen Mobiltelefonen, PDAs und PCs eingesetzt. Für Personal Area Networks (PAN), ein Netzwerk zur Verbindung direkt am Körper getragener Geräte, ist der Funkstandard Bluetooth auf dem Vormarsch. Für größere Entfernungen und höhere Bandbreiten sind die erwähnten Medien nicht geeignet und andere Übertragungstechniken notwendig. Besonders interessant ist die Entwicklung im Wireless LAN Bereich. Die erzielten Reichweiten ermöglichen eine raumübergreifende Mobilität mit einer Übertragungsgeschwindigkeit, welche einem Vielfachen von ISDN entspricht und damit für viele Anwendungsfälle wie beispielsweise Informationsbeschaffung im Internet und das Überprüfen von E-Mail-Konten ausreicht. Während Technologien wie Infrarot und Bluetooth aufgrund ihrer vorrangigen Verwendung in Freizeitgeräten noch selten Bedeutung für Geschäftsprozesse haben, sind Wireless LANs in vielen Firmen bereits fest integriert. Besonders interessant für Firmen sind Infrastruktur-Netzwerke, da sie zentral verwaltet, administriert und vergleichsweise einfach im kompletten Gebäude verfügbar gemacht werden können. Für Intrusion Detection Systeme sind Infrastruktur-Netzwerke vorteilhaft, da sich an den Access Points der Netzwerkverkehr konzentriert. Damit bieten sie die Möglichkeit, ähnlich wie bei Switches und Routern in kabelgebundenen LANs, eine maximale Anzahl an Datenpaketen untersuchen zu können.

Sicherheit in 802.11 Netzwerken

Das grundlegende Sicherheitsproblem bei drahtlosen Netzwerken ergibt sich aus den physikalischen Eigenschaften des Mediums. Wie eingangs genannt, bringen drahtlose Netzwerke viele Vorteile mit sich, darunter natürlich vor allem die Mobilität und Flexibilität. Als großen Nachteil hat die Verwendung dieses Mediums allerdings zur Folge, dass die Grenzen zwischen dem internen Netzwerk, welches nur über fest definierte Verbindungen erreicht werden kann, und dem externen Netzwerk, bei dem jedes Element von außen erreichbar ist, verschwinden. Während bei einem klassischen, kabelgebundenen Netzwerk zuerst physikalische Sicherheitsvorkehrungen, Gateways und Firewalls überwunden werden müssen, um Zugriff auf ein Netzwerk zu erlangen, sind Elemente des drahtlosen Netzwerks Angriffen direkt ausgesetzt. Jedes Gerät muss auf einen Angriff direkter oder indirekter Art vorbereitet sein. Obwohl dieses Problem schon bei der Konzeption des 802.11- Standards bekannt war, ist dieser für einen kooperativen Betrieb konzipiert. Während bei klassischen Netzwerken ein Angriff auf die OSI-Schichten 1 und 2 sehr schwierig durchzuführen ist, da sie durch Firewalls und Gateways auf höheren Schichten von der Außenwelt abgetrennt sind, kann jedes Gerät im drahtlosen Netzwerk auf diese Art angegriffen werden.

Angriffsmöglichkeiten auf ein Wireless-Netzwerk

Man kann die Angriffsmöglichkeiten in folgende Kategorien zusammenfassen:

- Passive Angriffe

  Ein passiver Angriff ist das Belauschen eines Netzwerks nach interessanten Paketen. Darunter fällt jeglicher unverschlüsselte Traffic sowie 802.11 Management- und Control-Frames, die weitere Informationen über das Netzwerk enthalten können. Interessante Informationen sind hierbei beispielsweise die verwendeten SSIDs oder Hinweise auf die Präsenz von Access Points und anderen Stationen. Bei einem passiven Angriff werden keine eigenen Pakete verschickt, so dass die Gegenwart eines Angreifers nicht unmittelbar festzustellen ist. Passive Angriffe dienen der Aufklärung und gehen oft aktiven Angriffen voraus.

- Probing und Scanning

  Hierbei wird das Netzwerk aktiv erforscht. Es werden beispielsweise Probe Requests verschickt, um die Gegenwart von Access Points festzustellen; normalerweise werden hierbei eine leere SSID, die SSID *any* und von den Herstellern werkseitig eingestellte Standard-SSIDs getestet, was bei nicht abgesicherten Netzen zu einem Erfolg führen kann. Der bekannteste Vertreter der aktiven Scan-Technik ist das Programm NetStumbler [NSTR]. Mittlerweile gibt es Software, die durch charakteristische Merkmale einen Angriff von NetStumbler und anderen bekannten Programmen erkennen kann.

- Vorspielen einer falschen Identität

  Da bei 802.11-Netzwerken keine Überprüfung der Authentizität und Integrität von Datenpaketen stattfindet, sind sie anfällig für so genannte Identity Theft-Angriffe. Die Authentifizierung eines Clients erfolgt meist nur mittels der Netzwerk-SSID oder mittels SSID und MAC-Adresse. Die MAC-Adresse eines Clients kann jedem von dem Client stammenden oder an den Client gerichteten Frame entnommen werden, und die SSID kann von einem Angreifer spätestens bei der Assoziation eines berechtigten Clients mitgehört werden. Da sich eine Assoziation aufgrund der Anfälligkeit des Mediums für Packet Injection und DoS-Angriffe erzwingen lässt und das Einstellen einer anderen MAC-Adresse auch keine Schwierigkeiten bereitet, kann sich ein Angreifer schon nach kurzer Zeit als berechtigter Client ausgeben. Ein Angreifer kann auch die Identität eines APs annehmen, indem er Beacons aussendet und auf Probe Requests antwortet; damit ergeben sich ideale Voraussetzungen für einen *Man in the Middle*-Angriff. Da das Protokoll keine gegenseitige Authentifizierung vorsieht, kann der Client nicht feststellen, ob ein Access Point zur Firma gehört oder sich möglicherweise sogar außerhalb des Gebäudes befindet.

- Denial of Service

  Prinzipbedingt ist es bei Funknetzwerken einfach, die Funktion durch Störsignale zu beeinträchtigen. Aufgrund der Verwendung des ISM-Frequenzbereichs gibt es eine Vielzahl von Geräten, die auf demselben Frequenzband operieren, beispielsweise Funktelefone und Mikrowellenherde. Auch mit konventioneller Hardware für 802.11b-Netzwerke kann man den Betrieb stören, indem man den Kanal einfach mit Paketen flutet, welche mit den Paketen anderer Teilnehmer kollidieren und eine Neuübertragung verursachen. Durch das Versenden spezieller Management-Frames mit der Absenderadresse des Access Points können Stationen wiederholt deassoziiert werden. Wenn der Angreifer es schafft, sich als Access Point auszugeben und Stationen an sich zu binden, kann er den Datenverkehr komplett unterbinden. Durch das vergleichsweise geringe Alter der Technik und des Protokolls ist mit einer sehr unterschiedlichen Reaktion der Implementierungen verschiedener Hersteller auf Management-Frames zu rechnen, welche sich nicht an die Spezifikationen halten. Bisher haben sich die Angriffe größtenteils auf das Ausnutzen der vorhandenen Lücken und Schwächen bei 802.11b und WEP beschränkt. Zunehmend werden aber auch Berichte über Probleme bei Access Points bekannt (siehe [BTRAQ]), meist in Form von fehlerhaften Implementierungen, unsicheren Voreinstellungen oder Schwachstellen, die für DoS-Angriffe genutzt werden können.

- Ungenehmigte Hardware

  Weiteres Gefahrenpotenzial birgt ungenehmigte Hardware, welche ohne das Wissen und die Genehmigung der IT-Abteilung mitgebracht und eingesetzt wird. Dies kann ohne böse Absicht geschehen: Privat wird ein Funknetzwerk eingesetzt, die IT-Abteilung der Firma hat sich aber gegen den Einsatz von Wireless-Netzwerken entschieden oder berät noch über den Einsatz. Um die tägliche Arbeit zu erleichtern, wird privat angeschaffte Hardware in der Firma verwendet und damit die Sicherheitsmechanismen des Firmennetzwerks ausgehebelt. Laut einer Analyse der Gartner-Group [GRTNR] sind bei 20% aller Firmen ungenehmigte Access Points an die Firmennetzwerke angeschlossen. Dabei ist davon auszugehen, dass die meisten dieser APs ohne Firewall direkt an das Firmennetzwerk angeschlossen sind und damit einem Angreifer den vollen Zugriff auf das interne LAN über das drahtlose Netz ermöglichen.

Die integrierten Sicherheitsmechanismen der 802.11-Standards sind momentan nicht ausreichend. Durch zusätzlichen Einsatz von Programmen auf höheren Protokollschichten können die größten Schwächen und Probleme bei Integrität, Authentizität und Datensicherheit kompensiert werden. Dennoch bleiben Stationen im Funknetz anfällig für DoS-Angriffe und passives Mithören. Durch die fehlende Standardisierung wirksamer Sicherheitsmaßnahmen auf niederen Protokollschichten sind die Hardware-Hersteller gezwungen, eigene Sicherheitslösungen einzubringen, wodurch eine Interoperabilität mit Produkten anderer Hersteller nicht durchgängig möglich ist. Eine Verbesserung versprechen die Standardisierungsbemühungen um 802.1x und 802.11i. Leider können auch diese Standards die vielfältigen Angriffsmöglichkeiten auf Wireless-Netzwerke nur teilweise kompensieren. Die Sicherheitsprobleme werden auch in der Zukunft bei der Entscheidung über den Einsatz von Wireless-Netzwerken in Firmen eine gewichtige Rolle spielen. Für Firmen mit hohem Sicherheitsbedarf ist der Einsatz von Funknetzwerken zur Zeit nicht ratsam.

Konzeption eines Wireless-Sensors

Augrund der bestehenden Sicherheitslücken und Schwächen ist es offensichtlich, dass ein Sicherheitsbedarf, wie er für Firmen und Privatanwender notwendig ist, nur über zusätzliche Absicherung erfüllt werden kann. Neben dem Einsatz starker Verschlüsselung auf höheren Protokollschichten ist es für die Administratoren von Netzwerken unumgänglich, sich einen Einblick in ihr Netzwerk zu verschaffen. Dabei werden sie durch Intrusion Detection Systeme unterstützt. Um gezielt auf die Besonderheiten eines Wireless-Netzwerks eingehen zu können, ist ein spezieller Wireless-Sensor zur Integration in Intrusion Detection Systeme notwendig.

Was kann ein Wireless-Sensor erkennen?

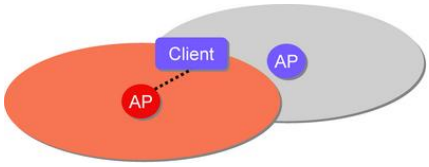
Anhand der Pakettypen, der in den Headern gesetzten Flags und Werte sowie des Inhalts der empfangenen Pakete lassen sich Rückschlüsse ziehen, die eine Kategorisierung und Priorisierung ermöglichen. In der Analysis Engine muss die Logik integriert werden, die aufgrund von Hinweisen auf das Ereignis schließen kann, welches diese Pakete verursacht hat. Diese Ereignisse lassen sich in Kategorien einteilen:

- Fremde Geräte

  Offensichtlich ist die Einteilung der Geräte in fremde und bekannte Stationen. Dies kann beispielsweise anhand der MAC-Adresse der Station erfolgen, die in den 802.11-Frames übertragen wird. Aufgrund weiterer Daten kann dann eine genauere Einteilung erfolgen:

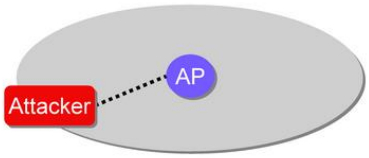
- Fremder Access Point

  Ein fremder Access Point kann aufgrund von Frames erkannt werden, die ausschließlich von Access Points versandt werden, beispielsweise Beacon Frames, Probe Responses, Association Responses und IAPP-Traffic, der zwischen zwei Access Points erfolgt und Roaming und Handover von Clients ermöglicht. Zum Aufbau siehe auch die folgende Abbildung:



  Fremder Client

  Fremde Clients können unter anderem anhand von Requests, wie beispielsweise Probe Requests und Association Requests, erkannt werden. Bei Verwendung von Programmen wie NetStumbler oder Kismet kann ein Angreifer an speziellen Flags, bestimmten SSIDs oder einer eindeutigen Signatur in den Nutzdaten der Pakete identifiziert werden. Die folgende Abbildung zeigt ein grafisches Modell hierzu:



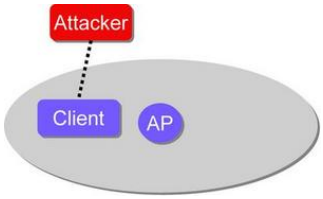
  Da bei 802.11-Frames weder Integrität noch Authentizität der übertragenen Pakete sichergestellt werden können, muss wie auch im konventionellen Ethernet damit gerechnet werden, dass die MAC-Adresse von Angreifern gefälscht wird. Hier ist beispielsweise der Fall denkbar, dass ein Access Point mittels einer positiven Ausschlussliste nur Clients mit bestimmter MAC-Adresse zulässt. Der Angreifer nimmt daher die MAC-Adresse eines berechtigten Clients an, um Zugriff auf das Netzwerk zu erhalten. In diesem Fall kann der Angriff beispielsweise daran erkannt werden, dass Pakete mit derselben MAC-Adresse ungewöhnlich stark in der Signalstärke variieren, wiederholt eine Bindung an den AP mit falschen SSIDs oder WEP-Schlüsseln versuchen oder durch anderweitig nicht zusammenpassende Parameter auffallen.

- Fremde Netzwerke

  Fremde Netzwerke lassen sich beispielsweise daran erkennen, dass der Absender von Datenpaketen zwar bekannt ist, diese aber nicht an einen bekannten Access Point gerichtet sind. Da in einem Infrastruktur-Netzwerk der gesamte Datenverkehr über einen Access Point laufen muss, sind alle anders gerichteten Pakete nicht Teil des Netzwerks. Hier existieren folgende Spezialfälle:

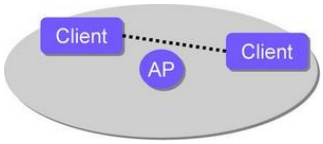
  - Kommunikationspartner bekannt, aber nicht AP

    In diesem Fall haben die Pakete als Ziel eine bekannte MACAdresse, welche aber nicht als Adresse eines genehmigten Access Points hinterlegt ist. Auch hier gibt es mehrere Möglichkeiten, Schlussfolgerungen zu ziehen. Falls die MAC-Adresse nicht von einem Angreifer übernommen wurde, weist diese Kombination auf ein Ad-Hoc-Netzwerk hin, was meist einen Verstoß gegen die Security Policy darstellt. Möglicherweise ist das Ziel der Kommunikation aber ein Angreifer, welcher die Identität einer autorisierten Station annimmt und deren MAC-Adresse fälscht, um dadurch Zugang zum Netzwerk zu erhalten. Dies wird auf folgender Abbildung deutlich:



Kommunikationspartner unbekannt

Ein unbekannter Kommunikationspartner ist eine Station, deren MAC-Adresse nicht bekannt ist, an die aber dennoch Pakete von einer bekannten Station gerichtet sind. Dies kann auf ein Ad-Hoc-Netzwerk hinweisen, bei dem eine bekannte Station mit einem fremden Client kommuniziert. Es kann aber auch auf ein Infrastruktur-Netzwerk deuten, bei dem sich ein Angreifer als Access Point ausgibt, um autorisierte Clients an sich zu binden. Wie bereits genannt, wählen einige Client-Implementierungen automatisch den signalstärksten Access Point zur Assoziation. Daher droht hier die Gefahr eines Man In The Middle-Angriffs. Ein unbekannter Kommunikationspartner kann auch aus dem Einsatz ungenehmigter, privat angeschaffter Hardware resultieren. Die Abbildung zeigt diesen Fall:



- • Auffälliger Traffic

Ungewöhnlicher Netzwerkverkehr kann auf Konfigurationsfehler oder Angriffe hinweisen. Bei den übertragenen Paketen werden die Paket- Header und die Nutzdaten nach ungültigen oder ungewöhnlichen Kombinationen sowie nach kritischen Inhalten untersucht. Im folgenden werden einige häufiger auftretende Fälle genannt:

-

Unverschlüsselter Datenverkehr

Von besonderem Interesse für den Netzwerkadministrator ist unverschlüsselter Datenverkehr, da dieser einen Verstoß gegen die Security Policy darstellt. Er versetzt jeden Passanten mit der entsprechenden technischen Ausrüstung in die Lage, den Netzwerkverkehr im Wireless LAN mitzulesen. In einem typischen Firmennetzwerk beinhaltet dies den Austausch von Dokumenten und EMails, die möglicherweise vertrauliche Daten enthalten.

Anmeldeversuche

Anmeldeversuche liefern Informationen über einen versuchten beziehungsweise erfolgreichen Zugang zum drahtlosen Netzwerk. Dazu dienen vor allem Probe Request- und Response- Pakete sowie Association Request und Response-Pakete. In diese Kategorie fällt auch eine aktive Suche nach Wireless-Netzwerken, wie sie beispielsweise von Tools wie NetStumbler oder dem Windows XP Scanning Service durchgeführt wird, da hierbei ebenfalls Probe Requests zum Einsatz kommen.

Unbekannte SSID/ESSID

Anhand der übertragenen SSID beziehungsweise ESSID kann man den Ursprung der Pakete schlussfolgern. Unbekannte SSIDs deuten auf Clients hin, die für andere Netze konfiguriert sind, also beispielsweise Besucher oder Passanten; ein typischer Angreifer testet bekannte Hersteller-SSIDs, um sich Zugang zum Netzwerk zu verschaffen. Bei einem Bürogebäude mit mehreren Firmen, die eigeneWireless LANs besitzen, kann man beispielsweise anhand bestimmter SSIDs auf Clients einer anderen Firma schließen. Anmeldeversuche mit deren SSID weisen nicht zwangsläufig auf einen Angriff hin, sind aber dennoch von Interesse.

Beacon propagating SSID

Um den Zugriff für nicht autorisierte Stationen zu erschweren, wurden Access Points um die Funktion erweitert, das Broadcasting der SSID zu unterdrücken. Als Folge davon muss ein Client die richtige SSID für eine erfolgreiche Authentifizierung kennen; eine Anmeldung mit leerer SSID oder der SSID *any* wird nicht mehr akzeptiert. Diese Option wird von den meisten Herstellern als *Closed Network* bezeichnet.

Bekannte Tools

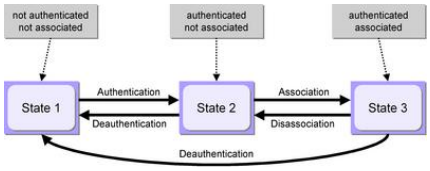
Anhand bestimmer Signaturen kann man verschiedeneWerkzeuge zum Scannen und Angreifen von Wireless-Netzwerken erkennen. So besitzen einige Programme bestimmte Zeichenketten in den Nutzdaten der Pakete oder eine eindeutige Kombination von gesetzten Flags in den Headern der Pakete. Mittels dieser Signaturen lassen sich beispielsweise wavemon, NetStumbler, DStumbler, Wellenreiter und der XP Network Scanning Service erkennen.

Unexpected Frame Type / Bits set

Für die Header-Felder *Control Type* und *Subtype* werden bei 802.11 zwei Bytes verwendet, mit denen die Frames in Management, Daten- und Kontrollframes eingeteilt werden. Die meisten Frames haben die Byte-Kombination 00/0100 (Probe Request), 00/0101 (Probe Response), 00/1000 (Beacon) und 10/0000 (Data). Da viele der möglichen Kombination noch für zukünftige Verwendung reserviert sind, ist es sehr wahrscheinlich, dass bisher ungenutzte Kombinationen verwendet werden, um Reaktionen auf undefinierte Frames zu provozieren, mit denen Access Points verschiedener Hersteller identifiziert werden können.

Unzulässiger Frame Type

Eine Station in einem drahtlosen Netzwerk kann sich in drei Phasen befinden. Zu Anfang befindet sich eine Station, die in die Reichweite eines Access Points betritt, in Phase 1: Sie ist nicht authentifiziert und nicht assoziiert. Nach einer erfolgreichen Authentifizierung befindet die Station sich in Phase 2; sie ist authentifiziert, aber nicht assoziiert. Daraufhin kann die Station eine Assoziation beginnen; im Erfolgsfall befindet sie sich dann in Phase 3, sie ist authentifiziert und assoziiert.



In Abhängigkeit der Phase, in dem sich eine Station befindet, sind nur bestimmte Frames zulässig. Zu den erlaubten Frames für eine Station in Phase 1 zählen beispielsweise die Management-Frames Beacon, Probe Request/Response, Authentication und Deauthentication. In Phase 1 können die meisten Control-Frames versandt werden, da diese für die Funktion des Netzwerkes notwendig sind. Data-Frames sind in dieser Phase nur in einem IBSS zulässig, da in Infrastruktur-Netzwerken jedes Datenpaket über einen Access Point gesendet werden muss. Dies ist einer Station aber erst nach der Assoziation mit einem Access Point erlaubt. In Phase 2 stehen einer Station zusätzlich die Management-Frames Association Request/Response, Reassociation Request/Response und Disassociation zur Verfügung. Nach einer erfolgreichen Assoziation befindet sich eine Station in Phase 3 und kann jegliche Data- Frames, Power-Save Control-Frames und Management-Frames zur Deauthentifizierung von Stationen versenden. Ein Wireless- Sensor, der eine interne Tabelle über die Phase von Stationen des Wireless-Netzwerkes führt, kann anhand dieser Tabelle erkennen, ob die versandten Pakete in der jeweiligen Phase zulässig sind.

MAC Address Spoofing

Viele Access Points bieten als zusätzliche Sicherheitsfunktion Zugriffskontrolle anhand der MAC-Adressen der Clients. Da diese Adressen in den meisten Fällen problemlos manuell eingestellt werden können, besteht die Gefahr einer Übernahme einer zulässigen Adresse durch einen Angreifer. Durch einfaches Mithören auf dem Funknetz lassen sich die MAC-Adresse und die verwendete SSID feststellen. Ein autorisierter Client kann beispielsweise durch DoS-Angriffe temporär behindert werden, worauf der Angreifer die Chance hat, seine Identität zu übernehmen. Eine Erkennung dieses Angriffs ist beispielsweise durch die Sequenznummern der Wireless-Frames möglich. Die Sequenznummern werden für das Zusammensetzen fragmentierter Frames benötigt. Laut 802.11-Spezifikation wird die Sequenznummer fortlaufend inkrementiert. Sprünge innerhalb dieser Sequenz können daher auf eine Übernahme der

MAC-Adresse hindeuten. Weitere Informationen zur Erkennung von MAC-Spoofing finden sich unter [JHWT].

Erkennung passiven Monitorings

Bei der Konzeption eines Wireless-Sensors stößt man zwangsläufig auf einen Sonderfall: Was passiert, wenn ein Angreifer sich wie der Wireless-Sensor im Monitor Mode befindet? Aufgrund der besonderen Problemstellung wird nachfolgend speziell auf dieses Thema eingegangen. Ein Angreifer, der sich wie ein Wireless-Sensor im passiven RFMON-Modus befindet, versendet keine Pakete. Aus diesem Grund ist es mit konventionellen Sensoren nicht möglich, die Gegenwart eines solchen Angreifers festzustellen, da diese auf dem Empfangen und Analysieren von 802.11-Frames basieren. Es gibt momentan zwei Alternativen, die jedoch nicht unter Intrusion Detection im klassischen Sinne fallen:

- Physikalische Ortung von Empfängern

  Unter Verwendung einer Antenne mit einer entsprechend hohen Verstärkung ist es möglich, einen Empfänger zu orten. Diese Technik wurde bereits zur Ortung unlizensierter Kurzwellenempfänger angewandt; eine Portierung auf Wireless-Netzwerke ist technisch machbar. Problematisch ist hierbei hauptsächlich, dass keine omnidirektionalen Antennen mit entsprechender Verstärkungsleistung verfügbar sind. Aus diesem Grund muss eine solche Lösung aus einer Anordnung mehrerer gerichteter Antennen bestehen. Da der Betriebsaufwand einer solchen Anlage den Aufwand für eine Absicherung des Wireless LANs übersteigt, wird dieses Verfahren kaum zum Einsatz kommen.

- Honeypot-Ansatz

  Da der Sensor nur passiv ist, kann er nicht überprüfen, ob der Datenverkehr, den er empfängt, reeller Datenverkehr ist. Aus diesem Grund kann man den Angreifer mit zusätzlich eingefügten Datenpaketen in die Irre führen. Bei einem Angriff basierend auf solchen Fehlinformationen ist eine Erkennung möglich. In diesem Zusammenhang interessant ist die Software [FKAP], die das Vorhandensein nicht existenter Access Points vorgibt. Jede Antwort an einen dieser APs deutet auf ein vorheriges Mithören im Funknetz hin. Eine weitere Alternative ist, dem Angreifer Informationen zu geben, die auf die Verfügbarkeit eines bestimmten Dienstes schließen lassen. Dazu prädestiniert sind beispielsweise gefälschte DHCP- oder SNMP-Pakete. Bei dem Versuch einer Nutzung eines dieser Dienste wird der Angriff erkannt, da diese Dienste von regulären Benutzern nicht in Anspruch genommen werden. Dieser Ansatz zur Erkennung eines Angreifers im Monitor Mode ähnelt dem eines Honeypots und fällt daher nicht in den Themenbereich. Weitere Informationen zu Honeypots finden sich unter [HYNT].

- Das Problem, einen passiven Angreifer erkennen zu können, ist nicht nur für Wireless-Netzwerke charakteristisch. Auch im konventionellen LAN ist es technisch komplex, dies zu erkennen, und die wenigen existierenden Ansätze befinden sich noch in einem frühen Stadium.

Fazit

Sicherheit in 802.11-Netzwerken ist ein Problem - ein Problem, für das es in absehbarer Zeit keine Patentlösungen geben wird. Bestehende Standards sind nicht ausgereift, proprietäre Implementierungen erzielen nicht die gewünschte Sicherheit, und die Vielfalt der Angriffe ist immens. Laut dem genannten Ansatz *Security = Visibility + Control* ergibt sich die Sicherheit durch die Kombination von Kontrolle und Transparenz. Kann die Zugriffskontrolle nicht garantiert werden, so erweist sich die Integration eines Intrusion Detection Systems an dieser Stelle um so wichtiger, um die Transparenz des Netzwerks und damit die Sicherheit zu erhöhen. Trotz des offensichtlichen Bedarfs an Intrusion Detection Systemen für Wireless-Netzwerke sind freie Produkte bisher kaum erhältlich. Verfügbare Produkte gehen meist nicht auf die Besonderheiten des Mediums ein und versuchen, konventionelle Intrusion Detection auf Wireless- Netzwerke zu übertragen. Dabei werden Angriffe, die in einem kabelgebundenen Netzwerk nicht anwendbar sind, selten in Betracht gezogen. Die Konzeption eines Sensors mit dem Fokus auf Ereignisse der unteren Protokollschichten bildet den zentralen Punkt. Durch eine Überwachung des Funknetzwerks im Monitor Mode und eine Analyse der empfangenen 802.11-Frames kann ein Sensor implementiert werden, welcher die speziellen Anforderungen erfüllt. Um den Bedarf an

Integrität, Authentizität und Datensicherheit zu erfüllen, ist starke Verschlüsselung auf möglichst niedrigen Protokollschichten notwendig. Ein herkömmliches Intrusion Detection System ist in diesem Fall nicht mehr in der Lage, Datenpakete auszuwerten. Zukünftige Intrusion Detection Systeme für Wireless- Netzwerke müssen die genannten Schwächen kompensieren. Dazu wird eine verstärkte Fokussierung auf den Layer 2 notwendig, um für die Betreiber des Netzwerkes wichtige Daten liefern zu können.

Die Positionierung eines Sensors ist in einem Wireless-Netzwerk problematischer als bei kabelgebundenen Netzwerken. Die optimale Position für einen einzelnen Sensor ist möglichst nahe an einem Access Point, da an dieser Stelle Angriffe auf den AP selbst und jegliche Kommunikationsversuche in das kabelgebundene Netzwerk entdeckt werden können. Damit kann jedoch nicht die Sicherheit jeder Station gewährleistet werden. Alternativ ist auch eine Positionierung mehrerer Sensoren entlang des Umfangs eines Funknetzwerkes möglich, was eine komplette Abdeckung aller Stationen des Funknetzwerkes erlaubt. Wie zu Anfangs genannt, muss der Sensor über die Fähigkeit verfügen, Daten im Monitor Mode aufzunehmen. Dies hat zur Folge, dass nur spezielle Funknetzwerkkarten verwendet werden können. Eine Beeinträchtigung eines Sensors durch die Menge an Datenpaketen ist aufgrund der Leistungsfähigkeit heutiger Hardware in Verbindung mit dem geringen Datenaufkommen in Wireless-Netzwerken auch in näherer Zukunft unwahrscheinlich.

References

[8SEC] Borisov, N., Goldberg, I., Wagner, D.: Intercepting Mobile Communications: The Insecurity of 802.11 Online im Internet (12/02/2003): http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

[8KEY] Fluhrer, S., Mantin, I., Shamir, A.: Weaknesses in Key Scheduling of RC4 Eighth Annual Workshop on Selected Areas in Cryptography, August 2001 Online im Internet (12/02/2003): http://downloads.securityfocus.com/library/rc4_ksaproc.pdf

[8WG] IEEE 802.11Working Group The Working Group for WLAN Standards Online im Internet (12/02/2003): http://grouper.ieee.org/groups/802/11/index.html

[ASVL] AbsoluteValue Systems The linux-wlan Company Online im Internet (12/02/2003): http://www.linux-wlan.com/

[ACSAC] Annual Computer Security Applications Conference Application Intrusion Detection using Language Library Calls Online im Internet (12/02/2003): http://www.acsac.org/2001/papers/21.pdf

[ACERT] The CERT Coordination Center AirCERT Project Homepage Online im Internet (21/02/2003): http://www.cert.org/kb/aircert/

[ARPK] WildPackets Inc. Airopeek NX Online im Internet (30/10/2002): http://www.wildpackets.org/products/airopeek_nx/

[ASNORT] AirSnort AirSnort - WLAN tool to recover encryption keys Online im Internet (06/02/2003): http://airsnort.shmoo.com/

[BTRAQ] Sicherheitslücken in Access Points: D-Link DWL-900AP+ Security Hole Online im Internet (12/02/2003): http://online.securityfocus.com/archive/1/306766 Longshine WLAN Access-Point LCS-883R VU#310201 Online im Internet (12/02/2003): http://online.securityfocus.com/archive/1/305344 DoS Vulnerability in Linksys Cable/DSL Routers Online im Internet (12/02/2003): http://online.securityfocus.com/archive/1/300754

[CIDF] Stuart Staniford-Chen et. al.: The Common Intrusion Detection Framework Architecture Online im Internet (12/02/2003): http://www.isi.edu/gost/cidf/drafts/architecture.txt

[CIDS] Cisco Systems, Inc.: Cisco IDS Host Sensor Data Sheet Online im Internet (12/02/2003): http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/prodlit/ hid25_ds.htm

[DSSID] The wi2600 Crew Liste von Default SSIDs Online im Internet (31/02/2003): http://mediawhore.wi2600.org/nf0/wireless/ssi

[ETHRL] The Ethereal Network Analyzer Online im Internet (12/02/2003): http://www.ethereal.com/

[FKAP] Black Alchemy Enterprises Fake AP Online im Internet (12/02/2003): http://www.blackalchemy.to/project/fakeap/

[GRTNR] The Gartner Group Gartner Advises on Security, August 2001 Online im Internet (12/02/2003): http://www.gartner.com/5_about/press_releases/2001/ pr20010809b.html

[GRPHA] Stuart Staniford-Chen et. al.: GrIDS - A GraphBased Intrusion Detection System for Large Networks In The 19th National Information Systems Security Conference, 1996 Online im Internet (18/10/2002): http://seclab.cs.ucdavis.edu/arpa/grids/welcome.html

[HSEC] Herwart Holland-Moritz, alias Wau Holland, 1951-2001, Mitbegründer des Chaos Computer Clubs In einem Interview im Zuge des Hamburger Dialog Online im Internet (13/01/2003): http://www.heise.de/newsticker/data/jk-10.05.00-000/

[HSNT] Heise Online Funknetze: Nachbesserung für mehr Sicherheit verspätet sich Online im Internet (25/02/2003): http://www.heise.de/newsticker/data/ea-25.02.03-000/

[HSTP] Jouni Malinen HostAP-Treiber Online im Internet (12/02/2003): http://hostap.epitest.fi/

[HYNT] The Honeynet Project To learn the tools, tactics, and motives of the blackhat community Online im Internet (12/02/2003): http://project.honeynet.org/

[IDWG] The Internet Engineering Task Force Intrusion Detection Working Group Online im Internet (12/02/2003): http://www.ietf.org/html.charters/idwg-charter.html

[ICOM] Intrusion, Inc. Why Firewalls Arent Enough Online im Internet (12/02/2003): https://www.intrusion.com/products/downloads/ WhyFirewallsArentEnough.pdf

[JHWT] Joshua Wright Detecting Wireless LAN MAC Address Spoofing Online im Internet (12/02/2003): http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf

[LMF] Joe McAlerney, Adam Migus libidmef - IDMEF Implementation Online im Internet (12/02/2003): http://www.silicondefense.com/idwg/libidmef/

[LXP] Defcom AB, CodeFactory AB libidxp - An IDXP/BEEP Protocol Implementation Online im Internet (12/02/2003): http://idxp.codefactory.se/

[NSTR] NetStumbler 802.11b based Wireless Network Auditing Online im Internet (31/01/2003): http://www.netstumbler.com/

[ORWN] Gast Matthew S.: 802.11 Wireless Networks: The Definitive Guide OReilly and Associates, Inc., Sebastopol, CA 2002

[PRLD] The Prelude Team Prelude - A Hybrid Intrusion Detection System Online im Internet (12/02/2003): http://www.prelude-ids.org/

[RLSC] Internet Security Systems RealSecure Network Protection Online im Internet (24/02/2003): http://www.iss.net/products_services/enterprise_protection/rsnetwork/

[RFC1] Point-To-Point Protocol (PPP) Online im Internet (12/02/2003): http://www.ietf.org/rfc/rfc1661.txt

[RFC2] PPP Extensible Authentication Protocol (EAP) Online im Internet (12/02/2003): http://www.ietf.org/rfc/rfc2284.txt

[RFC3] Remote Authentication Dial In User Service (RADIUS) Online im Internet (12/02/2003): http://www.faqs.org/rfcs/rfc2865.html

[SHBID] The SANS Institute What is host-based intrusion detection? Online im Internet (12/02/2003): http://www.sans.org/resources/idfaq/host_based.php

[SLATS] The SANS (SysAdmin, Audit, Network, Security) Institute Layered Approach to Security Online im Internet (13/01/2003): http://www.sans.org/resources/idfaq/layered_defense.php

[SCNT] Thomas H. Ptacek, Timothy N. Newsham Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection Online im Internet (05/02/2003): http://www.insecure.org/stf/secnet_ids/secnet_ids.html

[SNRT] The Snort Team Snort - The Open Source Network Intrusion Detection System Online im Internet (12/02/2003): http://www.snort.org/

[SNRTX] CERT Knowledgebase Snort XML Plugin Online im Internet (12/02/2003): http://www.cert.org/kb/snortxml/index.html

[TWRE] Tripwire, Inc. Tripwire Open Source, Linux Edition Online im Internet (12/02/2003): http://www.tripwire.org/

[VIDR] University of Virginia Intrusion Detection Research Online im Internet (30/10/2002): http://www.cs.virginia.edu/~jones/IDS-research/

[WSEC] Bernard Aboba Bernard Aboba's analysis of WEP2 security Online im Internet (16/01/2003): http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/1-253.zip

[WFAQ] Research Group Internet Security, Applications, Authentication and Cryptography, Abteilung Computer Science der University of California, Berkeley Security of the WEP algorithm Online im Internet (12/02/2003): http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html