



Abhörsicherheit von Mikrowellen-Richtfunksystemen

Einführung

Das Dokument beschreibt die Übertragungssicherheit bei Mikrowellen-Richtfunksystem (MRS) und die Hindernisse, die ein potentieller Lauscher überwinden muss, um das Signal zu empfangen und zu dekodieren. Vorausgesetzt ist, dass das zu übertragende Nutzsignal nicht zusätzlich mit externer Technik verschlüsselt ist.

Empfang und Dekodierung des Signals mit Systemen von Drittanbietern

Im Unterschied beispielsweise zur Lichtwellenleiter-Übertragung gibt es keine Richtlinien hinsichtlich der Freiraumübertragung. Daher arbeiten die MRS mit einer proprietären Übertragung, die von keiner anderen im Markt frei erhältlichen Hardware verarbeitet werden kann.

Um eine solche Hardware zu bauen, müsste der potentielle Lauscher folgende Größen genau kennen:

- das Modulationsverfahren: Kein anderer Hersteller verwendet das gleiche Verfahren und auch kein anderes System kann dahingehend geändert werden, diese Modulation zu verarbeiten.
- Verschlüsselung und Überlappung: Um eine hohe Performance zu erreichen, wird das Signal verschlüsselt und bei der Übertragung überlappt. Die genauen Algorithmen müssten für ein erfolgreiches Abhören dem Abhörenden bekannt sein.
- FEC und MUX-Rahmen: FEC steht für Forward Error Correction und ist eine Methode für die Identifizierung und Berichtigung von Fehler im Bit-Fluss in Echtzeit. Der MUX-Rahmen definiert die Größe der versandten Pakete und deren Beginn/Ende. Zur Entschlüsselung müssen beide Algorithmen und Variablen zur Verfügung stehen.

Aus diesen Gründen ist es ausgeschlossen, dass illegale Lauscher unter Verwendung von Ausrüstung von Drittanbietern Erfolg beim Empfang und der Entschlüsselung der zu übertragenden Nutzdaten haben.

Entschlüsselung mit baugleichen Systemen

Eine Option wäre der Einsatz baugleicher Systeme. Dies mag möglich sein, doch ist es mit hohen Kosten verbunden und hält weitere Hindernisse bereit:

So muss der potentielle Lauscher genau das gleiche Equipment einsetzen, mit gleicher Schnittstelle, der Übertragungsfrequenz, der Polarisierung und der genauen Einstellung Ihrer Systeme.

Weiterhin müsste das von der Inneneinheit aufbereitete Signal entschlüsselt werden. Am schwierigsten ist dies beim Datenverkehr des Ethernet-Interface. Da dort ein Switch integriert ist, sind alle Pakete an eine bestimmtes Netzwerkgerät adressiert. Daher müsste der Lauscher ein Programm oder eine Hardware konstruieren, die das abgehörte Netzwerk genau in MAC-Adressen und Struktur abbilden oder simulieren kann. Alternativ könnte auch die gesamte Ethernet-Schnittstelle in Hard- und Software eins zu eins nachgebaut werden, was nahezu unmöglich ist (MAC-Adressen sind weltweit einmalig!).

Die Sprachübertragung (E1) kann mit Hilfe eines PBX-Servers entschlüsselt werden, doch muss der Lauscher für jede Richtung ein komplettes System bereitstellen oder er erhält nur eine Hälfte der Information.

Eines der schwierigsten Hindernisse ist aber, das Signal überhaupt zu empfangen. Um ein qualitativ vernünftiges Signal zu erhalten, muss die Antenne des Lauschers innerhalb der Sendekäule oder ganz nahe beim Sender stehen. Da die Antenne einen extrem kleinen Abstrahlwinkel haben, heißt dies in der Praxis, dass die Abhöreinrichtung direkt in der direkten Sichtlinie zwischen den Endstellen platziert sein muss. Bei einer Montage auf dem Dach oder einem Mast führt dies zum Aufstellen eines hohen Mastes, um das abhörende System dort zu platzieren, oder die Montage auf dem gleichen Dach direkt neben dem abzuhörenden Empfänger. Unbemerkt kann dies nicht bei normalen Sicherheitseinrichtungen kaum geschehen.

Danach muss der Lauscher das Signal dekodieren. Dazu benötigt er folgende Daten:

- Frequenz;
- Bandbreite;
- Datentyp.

Danach müssen die in beide Richtungen gesendeten und gleichzeitig abgefangenen Informationen in einer bestimmten Weise zusammengefügt werden. Andernfalls fehlen dem Lauscher die Hälfte der gesendeten Daten und Informationen.

Die alles führt zu dem Schluss, dass es zwar theoretisch möglich ist, die Sprachsignale abzufangen und zu entschlüsseln, doch in der Praxis aufgrund des extrem hohen Aufwands und der damit verbundenen Kosten nahezu ausgeschlossen ist. Außerdem benötigt der Lauscher sehr hohes technisches Wissen. Bei der Datenübertragung kommen noch die Switch-Funktionen als weiteres Hindernis hinzu.

Verglichen mit anderen Technologien wie WLAN oder Leitungen ist die Übertragung mittels Mikrowellen-Richtfunksystemen abhörsicherer!

Folgt man den Regeln des Bundesamtes für Sicherheit in der Informationstechnik (BSI), so ist grundsätzlich dort eine Verschlüsselung vorzusehen, wo die vertraulichen Daten entstehen. Sie erst dort, wo sie ein Gebäude verlassen, zu verschlüsseln, ist nicht sinnvoll, da internen Lauschern der Zugriff leicht gemacht wird.