CBL Communication by light

Gesellschaft für optische Kommunikationssysteme mbH

Stellungnahme zur BSI Zertifizierung von CBL-Richtfunkkomponenten

In der Broschüre „Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte“ schreibt das BSI sinngemäß wie folgt:

Mikrowellen- und FSO-Richtfunksysteme haben ihren Ursprung im Bereich der Telekommunikation auf der Ebene der physikalischen Übertragung. In diesem Sinne wird eine Richtfunkstrecke wie ein Kabel behandelt.

Eine Verschlüsselung der Luftschnittstelle ist bei allen Richtfunktechniken, also dem optischen und dem Mikrowellen-Richtfunk weder vorgeschrieben noch standardisiert.

Obwohl beim Mikrowellen-Richtfunk stark bündelnde Parabolantennen eingesetzt werden, kann eine absolute Parallelität der Strahlen bedingt durch äußere Störeinflüsse nicht sichergestellt werden. Allerdings müßte ein potenzieller Lauscher zum Abhören neben der Sende- und Empfangsfrequenz auch die Polarisation, das Modulationsverfahren sowie Gerätetyp und Rahmenkodierung kennen.

Bei allen Richtfunk-Systemen benötigt man eine uneingeschränkte Sichtverbindung zwischen den beiden Standorten. Im Falle einer Nutzung von mikrowellenbasierten Techniken ist zusätzlich die Abwesenheit von Hindernissen innerhalb der sogenannten Fresnel-Zone gefordert.

Mikrowellen-Richtfunksysteme werden auch künftig eingesetzt werden, wenn ein Bedarf nach hohen Datenraten und/oder der Überbrückung größerer Entfernungen besteht. Da diese Richtfunksysteme rein auf der physikalischen Übertragungsebene arbeiten, sind standardisierte Sicherheitsmechanismen zwischen den Sende- und Empfangseinheiten nicht zu erwarten. Die Hersteller von Richtfunksystemen werden auch in Zukunft wahrscheinlich eher selten eine Verschlüsselung auf Ebene der Richtfunksysteme anbieten und der Nutzer bleibt für die Absicherung selbst verantwortlich.

Abhörsicherheit von Mikrowellen-Richtfunksystemen (MRS)

Empfang und Dekodierung des Signals mit Systemen von Drittanbietern

Im Unterschied beispielsweise zur Lichtwellenleiter-Übertragung gibt es keinen Standart bei der Freiraumübertragung. Daher arbeiten die MRS mit properitären Übertragungsverfahren, die nicht von anderer 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.

- Die Mikrowellen-Richtfunkkomponenten sind ab Werk standardmäßig mit einem Scrambling (fest eingestellter Hardwareschlüssel) versehen, um eine hohe Datensicherheit zu erreichen. Das Nutzsignal wird damit 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 Fehlern 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 gleichem Hard- und Softwarestand, gleicher Schnittstelle, gleicher Übertragungsfrequenz, Polarisation und der detailierten Systemeinstellung. Weiterhin müsste das von der Inneneinheit aufbereitete Signal entschlüsselt werden. Am schwierigsten ist dies beim Datenverkehr des Ethernet-Interfaces. Da dort ein Switch integriert ist, sind alle Pakete an ein bestimmtes Netzwerkgerät adressiert. Daher müsste der Lauscher ein Programm oder eine Hardware konstruieren, die das abgehörte Netzwerk genau in MACAdressen 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, denn MAC-Adressen sind weltweit einmalig!

Die Sprachübertragung (S2m/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 übertragenen 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 Sendekeule 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 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 geeignet auf zu stellen, oder die Montage auf dem gleichen Dach direkt neben dem abzuhörenden Empfänger. Unbemerkt kann dies bei normalen Sicherheitseinrichtungen wohl kaum geschehen. Somit kann man bereits bei der Planung der Standorte für die Richtfunk-Endstellen das Risiko eines unbefugten Zugriffs durch Zugangssicherungen erheblich reduzieren.

Dies 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 verbunden Kosten nahezu ausgeschlossen ist. Außerdem benötigt der Lauscher sehr hohes technisches Wissen. Bei der Datenübertragung kommen noch die Switch-Funktionen als weiteres Hindernis hinzu.

Grundsätzlich wird die Mikrowellen-Übertragungstechnik als sicherste Methode im Sinne des Signaltransfers im Vergleich zu terrestrischen Übertragungen angesehen. Kupfer- oder LWL-Standleitungen sind an den Knotenpunkten meist zugänglich und somit leichter abhörbar.

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 zu verschlüsseln, wo sie ein Gebäude verlassen, ist nicht sinnvoll, da **internen** Lauschern der Zugriff leicht gemacht wird.

CBL GmbH
Münster, im März 2010 Dr.-Ing. Hermann Lentke, GF