Vermeintliche Sicherheit

Der Digitalfunk hat keine Firewall

Klemens Wangen

Eine alte Weisheit lautet: Es gibt keine sicheren Systeme. Doch gilt das auch für die Systeme des digitalen professionellen Mobilfunks? Sind diese nicht per se sicher? Keineswegs. Verschiedene Szenarien, Verfahren und Techniken sind denkbar, die diese Systeme kompromittieren können. Eine Kontrolle ist immer besser.

Die Gefahr kommt aus der Luft

Im Jahr 2011 veröffentlichte die internationale Gruppe von Programmierern Osmocom einen öffentlich zugänglichen Code, mit dem es einem von ihnen möglich war, das Tetra-Signal zu demodulieren. Damit wurde den Hackern Tür und Tor geöffnet, denn zum Abhören digitalisierter Sprache bedarf es einer Demodulation der Signale.

Mit dem von Osmocom veröffentlichten Code war das nun möglich geworden. Ein damals 25-jähriger Student machte es sich zur Aufgabe, das Tetra-Netz von Slovenien auf Sicherheitslücken zu untersuchen und stellte dabei sehr schnell fest, dass die meisten Tetra-Benutzer (auch in Deutschland) ihr System gar nicht verschlüsseln (http://osmocom.org/projects/tetra).

Von jedem Studenten der Nachrichtentechnik, Physik oder Informatik können solche Tools, wie das von Osmocom, eingesetzt und mit anderen trickreichen Programmen ganz leicht kombiniert werden. Noch schlimmer: Man kann alle Tools im Internet (oder besser: Darknet) kaufen.

Kriminelle Energien

Und nun stellen Sie sich vor, in einem Gefängnis plant ein Insasse seinen Ausbruch und lässt jemanden draußen kriminelle Tools einsetzen. Dieser stiftet dann von außen Verwirrung mit falschen Nachrichten, realisiert Ablenkungsmanöver mit z.B. einem vermeintlichen Feuerausbruch – ein Notruf hier, eine Manipulation der Funkgeräte dort –, so dass plötzlich gar keine Kommunikation mehr möglich ist.

Oder Sie sind Lagerflächenbetreiber in einem Hafen und beschäftigen sich mit Containerumschlag. Was passiert eigentlich, wenn Sie die Schiffe nicht schnell genug löschen können, weil die Kommunikation gestört ist. Kostet das nur Geld? Oder was ist, wenn es aufgrund von bewusst manipulierten Meldungen zu falsch abgestellten Containern kommt, beispielsweise genau neben einem Zaun. Und am nächsten Tag hat der Zaun ein großes Loch, und der Container ist leer?

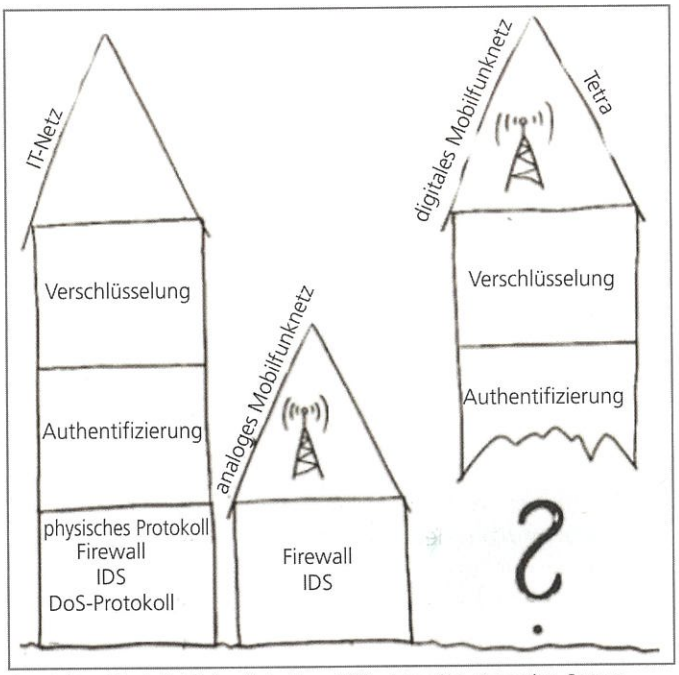
Oder stellen Sie sich eine Demonstration vor, bei der die Polizei mit einem

Klemens Wangen ist Geschäftsführer von Wangen Communication Consulting in Duppach

Großaufgebot an Personal für Ordnung sorgen muss. Was passiert, wenn deren BOS-Netz (BOS – Behörden und Organisationen mit Sicherheitsaufgaben) mithilfe verschiedener Methoden und unterschiedlicher Strategien gleichzeitig angegriffen wird. Oder wenn nun ein Überfall bei der Kreissparkasse mit Geiselnahme fälschlicherweise ins Tetra-System geschleust wird, kann die Polizei dann noch im Juweliergeschäft helfen, in dem auch gerade ein Raub geschieht? Kann eine Umweltkatastrophe vermieden werden, wenn die BOS-nahen Truppen von THW oder ähnlichen Organisationen auf dem Tetra-System nicht mehr kommunizieren können?
Sind diese Fragen und Vorstellungen realitätsfremd? Ganz und gar nicht. Eine einzelne Störung kann die Nutzer eines Tetra-Systems sicherlich nerven, hat aber sonst keine großen Auswirkungen. Eine raffinierte, kombinierte Vielzahl an Störungen aber legt auch ein Tetra-System mit Sicherheit so lange lahm, bis das eigentliche Verbrechen begangen worden ist.

Digitalfunk hat keine Firewall

Der Analogfunk (100 % physikalische Sprachmodulation) hat eine intrinsische Firewall (FW) und ein Intrusion-Detection-System (IDS) – und zwar in Form seiner Benutzer. Hört der Benutzer im analogen Signal etwas Merkwürdiges, sonderbare Geräusche, Rauschen, wo eigentlich kein Rauschen sein sollte, kann er aktiv werden. Das ist schnell, treffsicher und preiswert.
Beim Digitalfunk (100 % digitale Metadaten) fehlt dieser Schutzfaktor vollkommen. Er hat keine Firewall oder IDS-Logik direkt an der Luftschnittstelle, d.h. am Base Radio (BR) bzw. Base Controller (BC). Eine externe Firewall, wie sie Kabelnetze ihr eigen nennen, die zwischen Systemen und Netzen sitzt und Innen von Außen separiert, kann es über Funk aus physikalischen Gründen nicht geben.
Oder etwa doch? Wenn Funkmodems eingesetzt werden, gibt es eine Firewall. Diese sitzt aber erst tief in der Infrastruktur – beim Packet-Data-Gateway – und schützt dort das lokale Netz (Local Area Network – LAN) des Betreibers gegen Hacker, die Zugriff auf irgendein reguläres Funkgerät haben, das als Modem (SNDCP) konfiguriert ist. Umgekehrt verhindert die Firewall auch unkontrollierten Zugriff aus dem Betreiber-LAN auf das Tetra-eigene Netz aller Modems. Aber wie hilft das gegen Denial-of-Service- oder andere Angriffe aus der Luft? Dem eigentlich sehr sicheren Digitalfunk fehlt etwas Elementares – dem Tetra-Stack fehlt der Unterbau (*Grafik*). Sicher haben die Hersteller alles dafür getan, um sichere Systeme zu entwickeln. Aber es gibt Fälle, allesamt leider Realität, die dem entgegen sprechen. Mit einer kleinen Hardware, z.B. dem SDR-Shack (SDR-IQ-Sender), blockiert man mit wenigen geschickt platzierten Call-Setups alle drei Traffic-Channels einer Basisstation für 5 min. Und diese Call-Setups sind nicht unterbrechbar, weil sie mit Priorität 15 versehen sind.



Dem Tetra-Stack fehlt der Unterbau (IDS – Intrusion Detection System, DoS – Denial of Service) *(Quelle: Dr. Reckenfelderbäumer)*

Oder der Notruf von einem Standard-Handfunkgerät. Mit ein wenig Kreativität kann mithilfe der PEI-Schnittstelle z.B. alle 20 s ein Notruf abgesetzt werden – und schon sind alle Traffic-Channels einer Basisstation dauerhaft blockiert und auch nicht unterbrechbar. Auf dem Funkgerät erscheint für den Nutzer die Meldung „Calling…".
Oder, wenn man mit einem Standard-Handfunkgerät über die PEI-Schnittstelle unauffällig 50 % oder sogar mehr Auslastung auf dem Organisationskanal einer Basisstation generieren kann.
Richtig gemein wird es, wenn sich ein Nutzer mit einem Standard-Handfunkgerät in eine Basisstationssimulation (10 Frame Replay) einbucht anstatt in seiner eigenen Homebase. Mit dem Befehl Group-Attach.PTT erhält der Nutzer dann Call Setup Failed – und ist nicht mehr erreichbar, merkt es zunächst aber nicht. Erst wenn er versucht, mit anderen Kollegen zu sprechen und die mit einem Mal nicht mehr erreichbar sind, fällt ihm auf, dass hier irgendetwas nicht stimmen kann.
Diese Szenarien sind nicht an den Haaren herbeigezogen, sie können allesamt Wirklichkeit werden. In unserem Labor konnten wir folgendes nachstellen:

Random-Access
Ein einzelner Uplink-Subslot-Burst mit irregulärer SSI blockiert 68 Slots, d.h., für ca. 4 s ist der gesamte MCCH Organisationskanal einer Basisstation blockiert. Das hat zur Folge, dass in den Logs der Anlage kein Event gespeichert wird. Wenn sich dann jemand in der Analyse versucht, wird er vermutlich sagen: „Das wird wahrscheinlich ein Effekt von Empfängerrauschen oder gar Höhenstrahlung sein" – und das ganze als einen „Nadelimpuls" abtun.

Broadcast-Attacke via BSIP (Base Station Interchange Protocol) mit LLC-Ack-Request
Bei dieser Attacke wird das Netz mit einer Unzahl von Antwortmeldungen

belastet. So etwas ähnliches kennt man von Scada-Netzen.

BOOTA (Buffer Overflow over the Air)
Beim BOOTA fällt der HF-Träger nach Call-Setups mit einer Standard-MS (via PEI-Schnittstelle) einfach aus. Bei einer Analyse könnte man auch meinen, dass es sich nur um einen Call of Death (CoD) gehandelt hat.

Es gibt eine Vielzahl weiterer Fälle. Alle führen dazu, dass das vorhandene Tetra-System sehr stark belastet wird, teilweise ausfällt oder gar komplett lahm gelegt wird. Die wirtschaftlichen Folgen kann man sich für ein Industrieunternehmen schnell ausrechnen.

Ist Tetra sicher?

Alle Betreiber des professionellen Mobilfunks wähnen sich in (vermeintlich) großer Sicherheit, weil sie Tetra nutzen. Tetra ist sicher, heißt es und wird es von den Herstellern propagiert.
Die Betreiber von kritischen Infrastrukturen nutzen Tetra, um eine sichere Kommunikation zu gewährleisten. Zu nennen sind neben sicherheitskritischen Einrichtungen und Institutionen wie die BOS und alle BOS-ähnlichen Einrichtungen wie z.B. Justizvollzugsanstalten und Flughäfen, auch die großen Industrieanlagen, Umschlagplätze wie Häfen und Bahnhöfe oder öffentliche Verkehrsbetriebe, Energieversorger oder Stadtwerke. Hinzu kommen z.B. noch die Objektfunkversorgung und militärische Anwendungen.
Von einem guten Tetra-System wünscht man sich Schutz vor:

Denial-of-Service-Attacken (DoS)
DoS bezeichnet in der Informationstechnik die Nichtverfügbarkeit eines Internetdienstes. Die häufigste Spielart ist die Überlastung eines spezifischen Servers oder Datennetzes. Durch eine Unmenge von verteilten Anfragen wird eine Dienstblockade erzielt (Distributed Denial of Service – DDoS). Cyberkriminelle bieten diese DDoS als Tools zum Kauf an. Es gibt Fälle von Erpressung mit Geldzahlungen, damit das System wieder funktioniert

Gezielte Angriffe auf das Tetra-System:

- Jammer gegen das ganze Downlink-Band – laut, breit, permanent (bekannt aus der analogen Welt);
- Tetra-konformes Uplink-Jamming gegen einzelne Carrier oder gegen genau ein Netz – leise, normgerecht und nur bei Netzaktivität;
- fremde Standard-Mobilfunkstation (via PEI-Schnittstelle) gegen Organisations- und Sprachkanäle;
- NC-MS (nichtkooperativ, realisiert durch SDR) gegen das Random-Access-Protokoll (Slotted Aloha) und beliebig kreativ gegen höhere Protokollschichten.

Tetra Security

Um bei Fragen zur Tetra-Security helfen zu können, bedarf es Spezialisten. Eine mögliche Form sind Audits, die von der passiven Beobachtung des Tetra-Systems über Penetrationstest bis zu tiefem Hacking reichen können. Mit vielen Fragen im Gepäck (siehe die *Textkästen*) sollte ein Experte prüfen, ob das Tetra-System so eingestellt ist, dass es mit den vorhandenen Bordmitteln als brauchbares und verhältnismäßig sicheres Netz betrieben werden kann. Hierbei wird unterschieden zwischen Blackbox-, Whitebox- und Greybox-Untersuchungen.

Bei einer Blackbox-Untersuchung ist über das System gar nichts bekannt. Mithilfe einer relativ einfachen Software werden die Funksignale mitgeschnitten. Dafür wird mit einer DVB-T-Antenne (bessere Antennen liefern bessere Werte) und einer speziellen Software das Tetra-Signal an der Luftschnittstelle aufgezeichnet. Dieser Traffic in the Air wird dann im Labor analysiert. Das Ergebnis gibt bereits Aufschluss darüber, ob die vom Hersteller versprochenen Leistungsmerkmale eingehalten werden, zum Beispiel ob die Authentifizierung auch wirklich aktiv ist und korrekt funktioniert oder ob die Verschlüsselung richtig arbeitet. Erste Sicherheitslücken werden sichtbar.

Während man bei der Blackbox-Methode raten muss, ob die aufgezeichnete Frequenz die richtige war (das stellt man erst im Labor fest), weiß man bei einer Greybox-Untersuchung ganz genau, welche Frequenzen dem Betreiber zugeteilt wurden. Außerdem ist bekannt, welches System der Betreiber nutzt, aber noch nicht, welche Parameter gesetzt sind. Mit gezielten Frequenzaufzeichnungen wird das System wie bei der Blackbox-Methode untersucht, mit dem Unterschied, dass gezielt Versuche angestellt werden können, um deutlich mehr über das System zu erfahren, als der Betreiber mitteilen wollte.

Bei der Whitebox-Untersuchung wird anders vorgegangen. Dazu liegen bereits alle Informationen des Betreibers vor. Untersucht wird nun, ob einerseits die Versprechen des Lieferanten gehalten wurden und ob es andererseits gelingen wird, in das System von außen einzudringen, es zu manipulieren oder gar zum Stillstand zu bringen.

Während das Whitebox-Verfahren starke Penetration und tiefes Hacking erfordert, sind bei den Blackbox- und Greybox-Verfahren eher moderate Audits erforderlich, was sich letztendlich auch im Preis des Dienstleisters niederschlägt. Das Whitebox-Verfahren ist viel aufwendiger, da man hierbei einerseits versucht, das eigene System so „wasserfest" wie möglich zu machen und andererseits mit immer raffinierteren Methoden versucht, das System zu kapern.

Fragen, die sich der Betreiber eines Tetra-Systems stellen sollte

- Ist unser System sicher gegen Angriffe?
- Bemerken wir es, wenn uns ein Jammer stört?
- Bemerken wir überhaupt etwas, wenn ein Non-Cooperative Terminal Equipment versucht, in unser System einzudringen?
- Oder eine der Mobile Stations geklont wird?
- Haben wir Service Level Agreements (SLAs) für unser Funksystem?
- Wie lange braucht es, um einen Störer zu erkennen, ihn zu finden und die Folgen der Störung zu beheben?
- Befinden sich Funkgeräte als „Aktoren" im Netz, die auf SDS/Statusdaten selbstständig eine Aktion ausführen können?
- Befinden sich Sensoren im Netz, die ohne manuellen Eingriff permanent Daten liefern?
- Würden Sie unter Fake-Daten leiden?
- Wie ist eigentlich der Ausfall einer Basisstation oder der Komplettausfall des ganzen Netzes zu verkraften?
- Wurden Systemkomponten schon einmal gecrackt?
- Wurde das alles jemals getestet?
- Werden Angriffe dieser Art überhaupt bemerkt?

Jedes Verfahren liefert knallharte Fakten und konfrontiert Betreiber und Hersteller mit der vorgefundenen Situation. So kann bereits mit der Blackbox-Methode festgestellt werden, ob der Hersteller des Systems die Authentifizierung aktiviert hat und ob diese richtig funktioniert. Hat der Hersteller diese Funktion dem Betreiber verkauft, aber nicht korrekt konfiguriert, wird das in der Analyse sofort sichtbar.

Im gemeinsamen Gespräch zwischen Betreiber und Dienstleister werden dann Lösungsvorschläge und Strategien erarbeitet. Im günstigsten Fall ist alles in Ordnung. Oft sind es auch nur Kleinigkeiten, die nachträglich eingestellt werden müssen und bei denen man mit Bordmitteln bereits die Lücken schließen kann. Das kann die geringfügige Veränderungen von Parametern oder auch die Aktivierung einer wichtigen Funktion sein.

Wenn der Betreiber die aufgedeckten Sicherheitslücken nicht hinnehmen möchte, der Hersteller diese aber nicht schließen kann, müssen Lösungsmöglichkeiten überlegt und entsprechend gesucht werden – notfalls durch Austausch des ganzen Systems.

Tetra Security Monitor

Ideal wäre ein systemneutraler Tetra Securiy Monitor, der mithilfe künstlicher Intelligenz (KI) frühzeitig erkennen kann, wenn am Tetra-System manipulative Eingriffe vorgenommen werden, und entsprechend rechtzeitig warnt.

Ein solcher Tetra Security Monitor (TSM) steht quasi neben der Basisstation und überwacht, was gerade im Bündelfunksystem passiert. Er sollte mehrere HF- und Netzeingänge zur Protokollierung besitzen und Angriffsmuster automatisch erkennen. Dazu kann er sich beispielsweise der Fuzzy-Logik und KI-Methoden bedienen.

Überwacht werden sollten bei einem Tetra-System:

- Luftschnittstelle Downlink/Uplink;
- TMV-Port (o.ä.) des Base Radios (ungern, da dies eine zusätzliche Last für das Base Radio darstellt);
- NetworkTap-Kommunikation BR-BC;

- NetworkTap-Kommunikation BC-Switch (bzw. BC/Switch-AuC);
- ggf. auch Anlagen/SwMI-Logs;
- Meldungen via Alarmkontakten, E-Mail, SIEM-API.

Um ein solches System zu entwickeln, ist die Kooperation mit namhaften Universitäten sinnvoll, an denen Fragen zur Tetra-Sicherheit wissenschaftlich untersucht und Fuzzy-Logik- und KI-Methoden entwickelt werden können.

Fazit

Die alte Weisheit lautet, das es keine sicheren Systeme gibt – also auch keine sicheren Tetra-Systeme. Eine sehr gute Empfehlung sind daher Tetra Security Audits, die sehr schnell Aufschluss darüber geben, ob das eingesetzte System zumindest den Leistungsmerkmalen entspricht, die man beim Lieferanten bestellt hat. Sie liefern außerdem Erkenntnisse über mögliche Sicherheitslecks. Tiefer gehende Analysen wie die Whitebox-Methode sind sehr aufwendig und naturgemäß nicht preiswert, liefern dafür aber sehr sichere Systeme.

Sofern ein System Encryption und Authentifizierung nutzen kann, sollten diese Leistungsmerkmale eingesetzt werden, um das Tetra-System erheblich sicherer vor Angriffen zu machen. Das wird allerdings bisher von den meisten Anwendern nur sehr selten genutzt, von den BOS in Deutschland einmal abgesehen.

Es mag sein, dass das System mit einer Authentifizierung und Verschlüsselung einer stärkeren Belastung ausgesetzt ist und daher von den Lieferanten nicht empfohlen wird. Der Hersteller aber sollte in der Lage sein, entsprechend bessere Hardware anbieten zu können, damit die erforderlichen sicheren Funktionen auch leistungsfähig ausgeführt werden können.

Oder die aufgedeckten Sicherheitslücken werden bewusst in Kauf genommen, in der Organisation entsprechend implementiert und sicherheitstechnisch bewertet. In jedem Fall sollte der Geschäftsführer alles tun, damit ihm kein Organisationsverschulden nachgewiesen werden kann. *(bk)*

PMR-Expo 2018: Sicherheit im Blick

Vom 27. zum 29. November wird die Koelnmesse wieder Gastgeber der PMR-Expo sein (www.pmrexpo.de). Die europäische Leitmesse für das Netzwerk Sichere Kommunikation gibt bereits zum 18. Mal einer großen Zahl nationaler und internationaler Aussteller, Herstellern, Anwendern und Betreibern von PMR-Systemen eine gute Gelegenheit zum Informationsaustausch und zu Diskussionen. Dabei wird sich in diesem Jahr der Sicherheitsaspekt wie ein roter Faden durch das Vortragsprogramm ziehen. Zum Beispiel wird man diesem Thema mit einem neuen Format gerecht, dem Summit Sichere Kommunikation. Zum Auftakt führt PMeV-Geschäftsführer Uwe Jakob mit dem Vortrag „Sicherheitskritische Kommunikation – gestern, heute und morgen" in das Thema ein. Weitere hochkarätige Vorträge schließen sich an. Beispielsweise referiert Klaus Gräser von Schnoor Industrieelektronik über schwarzfallsichere Kommunikation, und Michael Fertig von Hytera Mobilfunk berichtet über sichere Kommunikation mit Virtualisierung.

In der Konferenzebene steht die sichere Kommunikation für die Energiewirtschaft im Mittelpunkt. Ihr kommt insbesondere für die schnelle Wiederherstellung der Stromversorgung im Schwarzfall bei Energieversorgern eine enorme Bedeutung zu.

Der dritte Tag des Summit steht wie gewohnt im Zeichen aller relevanten Leitstellenthemen.

Vervollständigt wird die PMR-Expo wie in jedem Jahr durch das PMR-Expo Career Programm, zahlreiche themenspezifische Fachforen und die bewährte Ausstellung. Letztere bietet mit 4.800 m² noch mehr Platz als im Vorjahr zum Austausch mit Entscheidern und Experten der Branche. Rund 230 Aussteller, darunter 73 internationale, haben bereits einen Stand gebucht.

PMR-News

+++ Am 15. August wurden die ersten beiden von insgesamt zehn **satellitengebundenen mobilen Basisstationen** (Sat-mBS) an die Bereitschaftspolizeien der Länder Berlin und Brandenburg übergeben. Sie bestehen aus einem Zugfahrzeug und einem Anhänger, der die Systemtechnik für den Betrieb der Sat-mBS enthält.

+++ Das Schweizer Bundesamt für Bauten und Logistik (BBL) und die Eidgenössische Zollverwaltung (EZV) beauftragten **Kapsch Trafficcom** mit der selektiven **Modernisierung der straßenseitigen Mautsystemeinrichtungen**, d.h. der Grenzbaken- und Kontrollanlagen, Kontrollfahrzeuge sowie der zentralen Rechenzentren. Zuvor schloss Kapsch Trafficcom die Modernisierung des österreichischen GO Maut Systems Ende Juni planmäßig ab.

+++ Motorola Solutions integriert die **Videomanagementsoftware Avigilon Control Center** (ACC) in

(Foto: Motorola)

seine CommandCentral-Aware-Plattform für Leitstellen (*Bild*). Damit erhalten Leitstellenmitarbeiter und Einsatzleiter Echtzeitinformationen über eine zentrale Datenquelle und können dort auch Videofeeds, Einzelheiten zum Vorfall, Benachrichtigungen, Karten oder die Standorte ihrer Ersthelfer abrufen.

+++ Siemens und **Damm** implementierten und testeten zusammen erfolgreich eine offene und interoperable **Tetra-Paketdatenlösung**, die den Forderungen von ETCS Level 2 (European Train Control System) entspricht. Die Tests fokussierten hauptsächlich Bandbreitenforderungen sowie die verlässliche Übertragung von Daten.