Merkelphone unter der Lupe

Im Rahmen einer journalistischen Anfrage durch die ComputerBild hatte die Antago GmbH, vertreten durch MSc. Alexander Dörsam, die Chance das aktuelle „Merkelphone“ im Hinblick auf seine Abhörbarkeit zu prüfen. Bei den uns vorliegenden Geräten handelte es sich um das Modell Z10 der Marke BlackBerry mit funktionsfähiger Installation der SecuSmart Software. Die Handys wurden nicht durch die Antago eingerichtet oder geprüft. Alle folgenden Erkenntnisse beziehen sich auf bereits konfigurierte Maschinen.

Verfolgt ein Angreifer das Ziel, Handy Kommunikation abzuhören, bieten sich ihm rudimentär die folgenden drei Szenarien:

Szenario 1: Angriffe gegen das Mobiltelefon

Hierbei versucht ein Angreifer, dass Telefon selbst zu infizieren. Dazu wird in der Regel Schadsoftware verwendet um das Gerät zu verwanzen. Wie diese Schadsoftware auf die Endgeräte gelangt, hängt von den Möglichkeiten des Angreifers ab. Dies kann über temporären physischen Zugriff passieren, weil das Gerät beispielsweise unbeaufsichtigt ist oder zum „Aufladen“ per USB-Port mit fremden Computern verbunden wird, oder auch über infizierte Software in digitalen Shops. Denkbar sind auch Angriffe via stillen SMS an das Mobiltelefon. Letzteres wird von deutschen Behörden tausendfach pro Jahr durchgeführt, ist aber nur einem sehr kleinem Kreis von Personen im vollen Umfang möglich.

Szenario 2: Angriffe gegen das Telefonnetz selbst

Selten besprochen doch absolut realistisch sind Angriffe gegen die hinter dem Funknetzwerk stehende Infrastruktur des Providers. Bei dieser Infrastruktur gelten die gängigen Probleme der IT-Sicherheit und entsprechend auch die typischen Angriffs-Vektoren. Ein erfolgreicher Angriff auf solche Kernsysteme ermöglicht es dem Angreifer, auf ungleich mehr Informationen Zugriff zu erhalten als bei allen anderen Szenarien. Dieses Szenario wird bei der folgenden Betrachtung nicht berücksichtigt.

Szenario 3: Angriffe auf dem Funkweg

Der aktuell am intensivsten besprochene Angriffs-Vektor ist der Funkweg. Zur Kommunikation verwenden die Mobilgeräte in der Regel den GSM-Standard. Dieser hat eine Verschlüsselung implementiert (A5.1), welche seit geraumer Zeit als gebrochen gilt. Möchte ein Angreifer also die Kommunikation einer Partei abhören, gibt es in diesem Szenario weitere 2 grundlegende Möglichkeiten:

- Mitschneiden

  Entscheidet ein Angreifer sich für diese Option, muss er zunächst in der Lage sein, den Funkverkehr seines Zieles physisch erfassen zu können. Dies bedeutet, sich in der Nähe seines Zielobjektes zu befinden. Kann ein Angreifer in der räumlichen Nähe zu seinem Ziel dessen A5.1 verschlüsselte Kommunikation unter der Verwendung von bspw. dem OsmocomBB-Projekt mitschneiden, kann er diese danach „offline“ entschlüsseln.

Antago GmbH | Heinrichstrasse 10 | D 64283 Darmstadt Sitz der Gesellschaft: Darmstadt | Registergericht: Darmstadt
Tel.: +49 . 6151 . 428568 . 0 | Fax: +49 . 6151 . 428568 . 1 Steuer-Nr.: 07 228 03 20 3 | Ust-IDNr.: DE 27 237 9849
E-Mail: sicherheit@antago.info | Web: http://www.antago.info Konto-Nr.: 0133 106 971 | BLZ: 508 526 51 | Sparkasse Dieburg
HRB: 89141| Geschäftsführerin: Silke Thielmann IBAN: DE07 5085 2651 0133 1069 71 | BIC: HELADEF1DIE

- IMSI-Catcher

  Bei einem IMSI-Catcher muss sich ein Angreifer ebenfalls in der Nähe seines Zieles befinden und würde sich dort als Mobilfunknetzwerk-Basisstation ausgeben. Dazu könnte die folgende Hardware eingesetzt werden:

Gibt sich ein Angreifer als Mobilfunknetzwerk-Basisstation aus, muss er gleichzeitig den Benutzer auf seine eigene Zelle „locken“. Dazu kann entweder mit höherer Sendeleistung oder Störung der echten Zelle gearbeitet werden. Ist das Ziel einmal bei dem IMSI-Catcher eingebucht, kann der Angreifer alle Gespräche aufzeichnen. Wichtig hierbei ist, dass dieser „öffentlich verfügbare“ IMSI-Catcher sich gegenüber dem echten Mobilfunknetzwerk nicht im Namen des Ziels authentifizieren kann. Entsprechend sind keine eingehenden Anrufe mehr auf das Ziel möglich.Ausgehende Anrufe werden durch den Angreifer üblicherweise durch ausländische VoIP-Provider auf das normale Telefonnetzwerk gebracht. Dies ermöglicht es dem Angreifer, auch die echte Telefonnummer des Zieles als Anrufende zu verwenden.

Antago GmbH | Heinrichstrasse 10 | D 64283 Darmstadt Sitz der Gesellschaft: Darmstadt | Registergericht: Darmstadt
Tel.: +49 . 6151 . 428568 . 0 | Fax: +49 . 6151 . 428568 . 1 Steuer-Nr.: 07 228 03 20 3 | Ust-IDNr.: DE 27 237 9849
E-Mail: sicherheit@antago.info | Web: http://www.antago.info Konto-Nr.: 0133 106 971 | BLZ: 508 526 51 | Sparkasse Dieburg
HRB: 89141| Geschäftsführerin: Silke Thielmann IBAN: DE07 5085 2651 0133 1069 71 | BIC: HELADEF1DIE

Angriff gegen das Merkelphone

Bei der Untersuchung der uns vorliegenden Cryptophones im Rahmen der journalistischen Anfrage wurde nun versucht, mit einem stark begrenzten Aufwand die Machbarkeit des Szenarios 3 zu prüfen. Dabei gibt es, wie oben näher beschrieben, die Möglichkeit des Mitlauschens bzw. die Verwendung des IMSI-Catchers. Die Funktion der installierten SecuSmart Software adressiert zunächst die Schwäche des durch GSM verwendeten A5.1 Algorithmus. SecuSmart legt eine weitere Verschlüsselung zusätzlich zu GSM an und macht ein einfaches „mit lauschen“ im Rahmen unserer Möglichkeiten unmöglich. Dies hilft auch, Szenario 2 zu vermeiden.

Der Einsatz eines IMSI-Catchers brachte aber ein eher unerwartetes Verhalten zu Tage. Zunächst ist es so, dass SecuSmart die Anrufe ebenfalls per VoIP verarbeitet und darauf basierend verschlüsselt. Ist eine Kommunikation auf Datenpaket-Ebene aber nicht möglich, kann eine Verschlüsselung basierend auf VoIP nicht durchgeführt werden.

Im Rahmen unserer Untersuchung wurden zwei Merkelphones eingesetzt, welche bereits verschlüsselt mit einander kommuniziert hatten, sich also „kennen“. Danach wurde eines dieser Telefone manuell auf unsere Basisstation eingebucht. Wichtig dabei ist: ohne gültige Lizenz der Bundesnetzagentur ist das Betreiben einer Basisstation nicht erlaubt. Über selbige Lizenz verfügt die Antago GmbH. Weiter ist es nicht erlaubt, Netze wie bspw. das von T-Mobile zu imitieren. Daraus leitete sich die Notwendigkeit ab, das Telefon manuell auf die Basisstation der Antago GmbH einzubuchen, dies hat allerdings keinen Einfluss auf die Ergebnisse des Tests.

Nachdem das Telefon mit der Basistation der Antago verbunden war, bestand keine Möglichkeit mehr eine Datenverbindung herzustellen und damit war auch keine verschlüsselte Kommunikation über SecuSmart mehr möglich. Das zweite Telefon war weiterhin in einer regulären Funkzelle eingebucht und könnte damit auch verschlüsseln. Mit der Intention, ein vertrauliches Gespräch zu führen, wurde dann die SecuSmart-App auf dem „angegriffenen“ Handy gestartet und der Anruf zu dem zweiten Cryptophone wiederholt. Dieses mal hat die App allerdings festgestellt, dass keine verschlüsselte Kommunikation hergestellt werden kann und direkt an die Telefoneinheit des BlackBerrys übergeben. Dieses Verlassen der sicheren Umgebung wurde ausschließlich mit „*Telefonnummer* anrufen Ok?“ kund getan. Entsprechend gering schätzen wir die Chancen ein, dass ein Benutzer dies als Verlassen der verschlüsselten Umgebung bemerkt.

Angelangt in der BlackBerry-Umgebung kommt es darauf an, welches Standard-Profil in dem Handy eingestellt ist. Hierbei gibt es ebenfalls verschiedene Möglichkeiten. Eine Möglichkeit ist, standardmäßig zu verschlüsseln. Ist diese Option ausgewählt und unser Ziel startet den Anruf aus der dann angebotenen BlackBerry Umgebung, wird der Anruf abgebrochen, da es nicht möglich ist, verschlüsselt zu kommunizieren.

Dieses Profil gilt allerdings systemweit, ist es aktiv, sind keine Anrufe auf normale Telefone mehr möglich. Entsprechend wahrscheinlich ist es, dass solch ein Profil im Sinne der Sicherheit per Default aktiv ist. Eine weitere Möglichkeit wäre, dass „normale“ Profil zu verwenden. Wird dieses Profil eingesetzt und das Merkelphone befindet sich in der Basistation des Angreifers, erlaubt das Mobiltelefon den „unverschlüsselten“ Anruf. Resultat ist hier, dass der Angreifer mit hört.

Zusammengefasst bedeutet dies: Wenn ein Angreifer unter dem Einsatz einer eigenen Basisstation ein Merkelphone belauschen möchte, steht und fällt die Integrität der Information mit der Aufmerksamkeit des Benutzers - und zwar trotz der expliziten Intention ein vertrauliches Gespräch zu führen. Dem Benutzer muss proaktiv auffallen, dass er die SecuSmart App verlässt und dass bei dem dann gestarteten Gespräch die optische Aufbereitung der Anzeige der des BlackBerrys entspricht und nicht der SecuSmart Applikation.

Wie gut oder schlecht die Sicherheit basierend auf dem Erkennen nicht vorhandener Merkmale in der IT funktioniert, konnte die Branche ausreichend bei Techniken wie HTTPs oder ähnlichen erfahren. Maßnahmen wie sehr klare Hinweise beim Verlassen des sicheren Bereiches fehlen auf dem Cryptophone. Weiter wäre es denkbar, darauf hinzuweisen, dass mit der Partei bereits verschlüsselt kommuniziert wurde und den Benutzer infolge dazu zu verpflichten, dass unverschlüsselte Gespräch explizit freizugeben.

Natürlich handelte es sich bei dem von uns verwendeten Telefon nicht um das original Gerät von Frau Merkel, dennoch gilt auch bei diesem Hochsicherheits-Telefon:

Die Kette ist nur so stark wie Ihr schwächstes Glied. In dem Falle, wie so oft, der jeweilige Benutzer.

Antago GmbH | Heinrichstrasse 10 | D 64283 Darmstadt Sitz der Gesellschaft: Darmstadt | Registergericht: Darmstadt
Tel.: +49 . 6151 . 428568 . 0 | Fax: +49 . 6151 . 428568 . 1 Steuer-Nr.: 07 228 03 20 3 | Ust-IDNr.: DE 27 237 9849
E-Mail: sicherheit@antago.info | Web: http://www.antago.info Konto-Nr.: 0133 106 971 | BLZ: 508 526 51 | Sparkasse Dieburg
HRB: 89141| Geschäftsführerin: Silke Thielmann IBAN: DE07 5085 2651 0133 1069 71 | BIC: HELADEF1DIE