

Information zur Verschlüsselung bei den Swissvoice-DECT- Telefonen der Serien Avena (Analog) und Eurit (ISDN)

Bezug nehmend auf Berichterstattungen der Medien in den vergangenen Tagen

Das Problem, dass sich jederzeit ein neues Mobilteil bei der Basis anmelden kann, liegt bei den Produkten von Swissvoice nicht vor. Die Feststation / Basisstation akzeptiert Neuanmeldungen von Mobilteilen nur innerhalb von 60 Sekunden, nachdem sie durch langes Drücken der Paging - Taste in den Anmeldezustand versetzt wurde.

Da die Daten, welche zur Authentifizierung und zur Verschlüsselung verwendet werden, zusammengesetzt sind aus einem Teil, welcher aus der Seriennummer des Mobilteils (IPEI) besteht und aus einem Teil, der anlässlich der Registrierung zufällig erzeugt wird, genügt es nicht, eine IPEI zu stehlen oder zu duplizieren, um ein bestimmtes bereits registriertes Mobilteil vortäuschen zu können.

Die laufenden Gespräche werden mit einem publizierten Algorithmus mittels eines 64 Bit - Schlüssels chiffriert (DCK Derived CIPHER Key). Da der Algorithmus bekannt ist, kann unter Umständen ein gezieltes Verfahren verwendet werden, um die Chiffrierung zu knacken. Uns ist aber kein derartiges Verfahren bekannt. Ist dies nicht der Fall, so muss ein "brute force" Angriff gemacht werden. Geht man aus praktischen Gründen (man muss nach jedem Entschlüsselungsversuch kontrollieren, ob die Klartextdaten einem verständlichen Audio-Signal entsprechen) davon aus, dass ein Versuch 1 Millisekunde dauert (was sehr optimistisch ist), so beträgt die Zeit zum Ausprobieren aller möglichen 2^{64} Schlüssel ca. 585 Jahre.

Aus unserer Sicht hat deshalb nur ein sehr versierter Kryptologe überhaupt eine Chance, die Chiffrierung zu knacken. Es sind sehr gute theoretische Kenntnisse und eine nicht handelsübliche Infrastruktur notwendig, um zum Ziel zu kommen.

Für den Normalverbraucher kann der heutige Zustand (mit DECT-CIPHER-Verschlüsselung) unserer Meinung nach als absolut genügend betrachtet werden. Für Anwender mit besonderen Sicherheitsanforderungen gelten die gleichen Vorbehalte wie für den Einsatz von Mobiltelefonen.

Weitere Umstände, welche die Sicherheit der Swissvoice DECT-Telefone erhöhen:

- Die Swissvoice Basisstationen bestätigen die Anmeldung des zugehörigen Mobilteiles.
- Bei Swissvoice ist das Pairing zeitlich auf 60 Sekunden limitiert.
- Die Paarung kann nur über eine mechanische Betätigung der Paging-Taste auf der Swissvoice - Feststation ausgelöst werden.
- Bei Swissvoice ist die Verschlüsselung in jedem Fall immer eingeschaltet.
- Bei Swissvoice kann die Verschlüsselung nicht ausgeschaltet werden
- Eine Authentifizierung gemäss „ETSI EN 300 175-7, §4 .2.1 Authentifizierung des Mobilteils“ erfolgt bei der ersten Verbindungsaufnahme, nach einer Neuanmeldung oder nach einem „Reset“ der Feststation. (Anmerkung: Nur die Authentifizierung des Mobilteiles ist erforderlich um zu verhindern, dass ein Fremdes nicht angemeldetes Mobilteil über die Feststation telefonieren kann)
- Alle Swissvoice Telefone verschlüsseln Ihre Datenübertragung gemäß ETSI EN 300 175-7, § 4.2.4.
- Im „fulleco“-Modus schaltet das DECT-Funkfeld von Basis und Mobilteil völlig ab, wenn nicht telefoniert wird. Somit ist keine Möglichkeit gegeben für einen „Angriff“ über das Funkfeld.
- Im ECO-Modus schaltet das DECT-Funkfeld von Basis und Mobilteil völlig ab, wenn nicht telefoniert wird und das Mobilteil sich in der Basisstation befindet. Somit ist keine Möglichkeit gegeben für einen „Angriff“ über das Funkfeld