

Sicherheit im Netzwerk

Im Zusammenhang mit Cyberkriminalität und Online-Terrorismus werden seit einiger Zeit neue Anforderungen für den Datenverkehr in IP-Netzwerken diskutiert und erstellt. Hier einige wichtige Gesichtspunkte zu dem Thema:

Anforderungen des BSI

Das BSI erstellt Profile für verschiedene Anwendungen im Netzwerkbereich, aber auch allgemeine Empfehlungen. Diese Anforderungen sind größtenteils schon sehr hoch. Zwar kann man deutlich bessere Sicherheitsmechanismen realisieren, die vom BSI genannten Standards werden allerdings in den meisten Anwendungen vorausgesetzt werden.

Zurzeit wird die Fassung 2.0 der technischen Richtlinie TR03109 erarbeitet, die bislang die Voraussetzungen für Smart Meter Gateways regelt. Es kann davon ausgegangen werden, dass die Richtlinie die Sicherheitsanforderungen aller embedded Systeme regeln wird. Es wird dafür angepasste Protection Profiles geben. Daraus wird sich ergeben, dass PC-typische Betriebssysteme die Bedingungen nicht erfüllen können.

TLS 1.2

In fast allen Unterlagen nennt das BSI TLS 1.2 (Transport Layer Security) als Grundlage für die Datensicherung. TLS ist einerseits Voraussetzung für viele Protokolle, stützt sich aber andererseits auch auf eine ganze Reihe von enthaltenen Sicherheitsstandards (AES, SHA, DSA usw.).

Für viele dieser Aufgaben steht bei TLS eine ganze Reihe alternativer Methoden zur Verfügung, die laut Standard ausgewählt werden können. Dies ist notwendig, um Kompatibilität zu älteren Anwendungen herzustellen.

Das BSI verbietet die Verwendung der älteren Standards und schränkt TLS auf bestimmte hochklassige Verfahren ein. Unter anderem deshalb lassen sich übliche PC-Lösungen nicht verwenden.

Die erwarteten neuen technischen Richtlinien werden das bisher übliche AES voraussichtlich durch CME mit Brainpool-Kurven, die nicht denen von NIST entsprechen, ersetzen. Die NIST-Kurven werden als eventuell manipulierbar eingestuft, auch werden dort Empfehlungen der NSA berücksichtigt. Auch diese Anforderung wird von PCs nicht erfüllt.

Protokolle

Auf TLS fußen Protokolle wie HTTPS, FTPS, SSH und SIPS. Anstatt FTPS kann auch SFTP eingesetzt werden, eine Alternative, die oftmals als noch sicherer eingestuft wird.

HTTPS sichert den Zugriff auf die, in den Geräten enthaltenen, Webserver zur Konfiguration der Systeme ab.

FTPS und SFTP dienen dem gesicherten Datenaustausch zwischen dem Zielsystem und einem Manager (gewöhnlich ein PC).

SSH sichert die Daten, die über eine steuernde Managementschnittstelle ausgetauscht werden, ab.

SIPS sichert das übliche VoIP-Protokoll SIP ab.

In allen Fällen gelten für die beteiligten PCs (die Gegenstellen) besondere Sicherheitsanforderungen, damit die bis dahin gesicherten Daten nicht nach der Entschlüsselung oder vor der Verschlüsselung verfälscht werden können.

Betriebssystem

Das eigentliche Betriebssystem der beteiligten Geräte ist natürlich ebenfalls Gegenstand der Sicherheitsbetrachtungen. Übliche Systeme wie Windows, Linux, MacOS, iOS und Android (um die wichtigsten zu nennen), laufen auf PCs oder ähnlicher Hardware. Diese Betriebssysteme stellen eine Unzahl von Funktionen, unter anderem auch die notwendigen Sicherheitsfunktionen, zur Verfügung.

Diese Vielseitigkeit ist der Grund für die Popularität solcher Systeme, die weit mehr können, als nur Daten zu sichern. Leider ist es auch sehr einfach, PCs mit Schadsoftware zu infizieren, die die gesicherten Daten leicht manipulieren können, weil sie dank der Sicherheitsfunktionen im System mit dem Codieren und Decodieren kein Problem haben. Man greift die Daten einfach in ihrer lesbaren Form ab.

Das BSI kennt diese Schwäche und macht es deshalb fast unmöglich, solche Systeme für Hochsicherheitsanwendungen einzusetzen. Unser Betriebssystem ellan:RTOS kann von Viren, Trojanern oder anderer Schadsoftware nicht angegriffen werden, weil es nichts anderes macht, als es in der jeweiligen Anwendung soll.

ellan:RTOS läuft auf extrem kleiner und preiswerter Hardware, die man speziell für die Audiokommunikation und Steuerungstechnik einsetzen kann.

Streams

TLS sichert Daten auf TCP-Verbindungen. Für Streams (Audio, Video und andere Echtzeitanwendungen) ist TLS nicht geeignet. SIPS sieht aber für die Streams SRTP vor, allerdings in einer nicht akzeptablen Form. Das BSI trifft zu diesem Thema keine Aussagen, aber SIPS sieht die Abschaltung der Verschlüsselung bei Übertragungsfehlern zwangsweise vor, was völlig unbrauchbar ist.

Wir können SRTP auch ohne Zwangsabschaltung nutzen, was dem Standard zwar widerspricht, aber eher dem nahekommt, was das BSI für sinnvoll hält.

Zertifizierung

Es ist möglich, Geräte beim BSI zertifizieren zu lassen. Unsere Lösungen sind grundsätzlich zertifizierungsfähig, weil sie alle Anforderungen des BSI erfüllen. Ein Zertifizierungsverfahren hat es aber bisher nicht gegeben, weil das sehr kostspielig ist und nur in Frage kommt, wenn man ein Gerät hat, das zugelassen werden soll.

Wir als Dienstleister können eine Zulassung aber unterstützen. Es gibt verschiedene Evaluierungsstufen bei solchen Prüfungen. Wir können auch die Stufe EAL4 (die höchste unter den militärischen) unterstützen. Für manche Anwendungen mögen auch EAL3 oder EAL2 genügen, was das Verfahren vereinfacht.

Die Elink Sicherheitsprotokolle

Nachdem wir von unseren Kunden mehrfach nach erweiterter Sicherheitstechnik gefragt wurden, haben wir beschlossen unser ellan:RTOS über die bereits bestehenden Sicherheitsmechanismen hinaus zu erweitern.

Bestehendes

Um den Zugriff auf Betriebsparameter zu beschränken, wurden bisher hauptsächlich passwortgeschützte Webseiten verwendet. Außerdem war es möglich mit einer verschlüsselten Terminalemulation zu arbeiten (SSH). Darüber hinaus gab es auch die Möglichkeit, Dateninhalte durch eine Hashfunktion abzusichern (Erkennung von Fälschungen oder Modifikationen).

Dabei ist hier nicht von üblichen PC-Techniken die Rede, sondern von Funktionen im ellan:RTOS, unserem virensicheren Echtzeitbetriebssystem. Es ist zu beachten, dass Daten im Allgemeinen nicht auf dem Transport ausgespäht werden, sondern vor oder nach der Entschlüsselung auf dem Sender oder dem Zielsystem. Das ist bei ellan:RTOS nicht möglich, höchste Datensicherheit ist also gewährleistet.

Die Verschlüsselungsverfahren sind heutzutage recht sicher. Angreifbar werden sie, wenn auch der gesamte Verbindungsaufbau mitgeschnitten wird. Deshalb sollten die Schlüssel auch nicht über die zu schützende Verbindung ausgetauscht werden.

Wenn es einen Zugriff hinter oder vor der gesicherten Übertragungsstrecke gibt, ist die Verbindung nicht sicher. Das ellan:RTOS ist von Fremdcode nicht angreifbar und deshalb auch virensicher. Das System soll und kann fremden Code nicht ausführen.

Hardware

Das ellan:RTOS ist für verschiedene Prozessorplattformen verfügbar. Die meisten davon sind auch in der Lage, die Verschlüsselungstechnologie zu realisieren. Das gilt sogar auch für etwas ältere Systeme, die schon länger im Dienst sind.

Neu entwickelte Systeme werden in Absprache mit dem Kunden immer mit diesen Fähigkeiten ausgestattet, es sei denn, dass es mit Absicht weggelassen werden soll, z.B. aus Kostengründen.

Eigenentwicklung

Die Softwareteile für die Verschlüsselungstechniken in unserem System, sind auch von uns selbst entwickelt worden. Es gibt keinen Rückgriff auf offenen oder bekannten Code. Die Algorithmen halten sich lediglich an die vorgeschriebenen Regeln, damit die Kompatibilität gewährleistet bleibt.

Sicherheitstechniken sind in der Praxis nicht immer interoperabel. Deshalb ist es besonders wichtig, dass wir die Verfahren in unserem System jederzeit anpassen und verfeinern können.

Transport Layer Security

TLS erweitert einige gängige Protokolle um Sicherheitsaspekte. So wird aus HTTP HTTPS, aus FTP FTPS und aus SIP SIPS. TLS ist recht verbreitet und schützt nur das vorhandene Protokoll, indem es in eine gesicherte Schicht verpackt wird.

TLS wurde aus dem älteren SSL entwickelt, das einige Schwächen beim Schlüsselaustausch zeigte. TLS ist auf einfachste Weise interoperabel mit fast beliebigen Gegenstellen. HTTPS wird z.B. von jedem Browser unterstützt. Wir bieten TLS nun für diese drei genannten Protokolle an.

SIP/SIPS

SIPS verschlüsselt nur die Signalisierung zwischen den Endgeräten und zwischen diesen und dem Server. Spätestens auf dem Server ist es mit der Sicherheit nicht mehr weit her.

Auch die meisten SIP-Endgeräte (sogar Telefone) fußen auf gängigen Betriebssystemen wie Linux oder Android, sind also angreifbar.

Damit auch das eigentliche Gespräch verschlüsselt wird, stützt sich SIPS auf SRTP. SRTP verwendet nur eine relativ schwache Verschlüsselung. Darüber hinaus schaltet SRTP bei Übertragungsfehlern die Verschlüsselung ab. Der Standard sieht vor, dass jedes SIPS- Endgerät diese Abschaltung unterstützen muss.

In einem LAN kommen Übertragungsfehler selten vor, aber über das Internet zum Beispiel, kommen Fehler häufig vor. Diese führen dazu, dass der Schlüssel verloren geht und die Verbindung letztlich unverschlüsselt bleibt. Das lässt sich auch leicht provozieren.

Unsere eigene Stream-Verschlüsselung verkraftet Paketverluste und erzeugt dabei lediglich kleine Knackser, wie man sie auch von unverschlüsselten Verbindungen her kennt. Die dafür notwendige Technik unterscheidet sich sehr deutlich von den üblichen Verfahren. Die Verschlüsselung selbst ist auch stärker als bei SIPS, zumal wir zwei verschiedene Verfahren ineinander verschränken.

Trotzdem können wir „einfaches“ SIPS/SRTP natürlich anbieten.

Secure Shell

SSH stellt einen verschlüsselten Verbindungstunnel zwischen zwei Endstellen her. Damit ist SSH nicht an ein bestimmtes Protokoll gebunden. Obwohl die Verschlüsselung prinzipiell die gleiche ist, wie bei TLS, kann man wegen des verbesserten Schlüsselaustauschs von einer höheren Sicherheit ausgehen.

SSH eignet sich vor allem durch die Verwendung von TELNET für eine Kommandozeilensteuerung. Auf sehr ähnliche Weise können auch nichtöffentliche Kommunikationsteile, wie sie auch in unserem neuronalen System Verwendung finden, durch SSH abgesichert werden.

SSH ermöglicht auch SFTP (nicht zu verwechseln mit FTPS), ein Hochsicherheitsfiletransferprotokoll, das sich für den Austausch von Konfigurationsfiles zwischen den einzelnen Geräten eines Systems eignet.

Für SFTP gibt es auch PC-Clients. Wir haben die neueste Version 6.0 in unser System implementiert.

Advanced Encryption Standard

Für die eigentliche Verschlüsselung wird zumeist AES verwendet. Dieses Verfahren ist sehr sicher und leistungsfähig. Deshalb wird es auch bei uns eingesetzt. Es ist nur wichtig, dass der Schlüssel selbst nicht bekannt wird. Hierfür gibt es verschiedene Lösungen.

Mit einem preshared key (PSK) kann man den Austausch des Schlüssels über die Leitung verhindern. Wenn die beteiligten Endstellen den PSK kennen, muss man ihn nicht übersenden oder aushandeln.

Mit einem PSK kann man aber nicht immer arbeiten. Wenn man eine gesicherte Verbindung mit einer Gegenstelle aufbauen will, die man vorher nicht kennt, muss man den Schlüssel verhandeln. Genau diese Aufgabe übernehmen TLS und SSH.

RSA/DSA/ECDSA

RSA liefert das Zertifikat, das aus den beiden Schlüsselpaaren für den öffentlichen und den privaten Schlüssel sorgt. Durch diese Schlüssel werden dann die Informationen signiert die dann endgültig als Schlüssel für den Datentransport verwendet werden.

Man kann Zertifikate selbst erzeugen, aber manche Anwendungen akzeptieren nur solche von bekannten Zertifikatsanbietern. Unsere Geräte akzeptieren alle Zertifikate und können auch selbst welche erzeugen. Beschränkungen können natürlich eingebaut werden.

DSA erfüllt die gleiche Aufgabe, ist aber deutlich verbessert. ECDSA wiederum verbessert das Verfahren ein weiteres Mal. Das BSI akzeptiert in den Protection Profiles nur ECDSA. Wir rechnen mit einer verstärkten Reglementierung des Datenverkehrs in nächster Zukunft. Das BSI ist hierbei die federführende Behörde und unsere Sicherheitsfunktionen, sowie unser Betriebssystem, entsprechen den Anforderungen des BSI.

VPN/IPsec

Virtual Private Networks gibt es in verschiedensten Ausführungen. Viele der dafür verwendeten Verfahren, werden auch von uns unterstützt. Das gilt auch für IPsec. Die verschiedenen Methoden setzen auch auf unterschiedlichen Kommunikationslayern auf, sind teilweise an bestimmte Applikationen gebunden oder auch fast voll transparent.

Wir unterstützen die meisten gängigen Protokolle. Welches letztlich verwendet wird, hängt von der Anwendung ab. Wir können eine komplette Routingfunktion implementieren, aber auch eine Endpoint-Verbindung.

VPNs können mit und ohne Verschlüsselung realisiert werden. SSL, PPTP und L2TP stehen zur Verfügung, aber auch eigene Protokolle.

Für unsere Geräte werden meistens End-to-End Realisierungen verwendet. Wir können aber auch VPN-Gateways für echten Site-to-Site-Betrieb implementieren. Dementsprechend ist auch die Betriebsart End-to-Site kein Problem.

Eigene Verfahren

Da wir alle notwendigen Sicherheitsroutinen für unser Betriebssystem selbst geschrieben haben, war es uns auch möglich, die Algorithmen zu verändern oder durch eigene zu ersetzen. Unsere eigenen Lösungen sind zwar vom Grundsatz her nicht besser als die bekannten, da sie aber unbekannt sind, werden für Angreifer die Chancen noch einmal deutlich verschlechtert.

Wenn man den Algorithmus nicht genau kennt, gibt es kaum einen Angriffspunkt, über den man das Verfahren knacken kann. Vor allem, weil das auch kaum schon möglich ist, wenn man das Verfahren kennt.

Unsere proprietären Verfahren bieten also eine noch einmal deutlich erhöhte Sicherheit, verzichten dafür aber bewusst auf Kompatibilität. Mit diesen Verfahren ist eine Kommunikation also nur zwischen unseren Geräten möglich.

Auf dieser Grundlage haben wir unser AntiSpyFon entwickelt, ein Kommunikationsgerät für die Übertragung von Sprache und Daten über Netzwerke, auch das Internet. Hier verwenden wir nur unsere eigenen Protokolle, wodurch wir absolute Sicherheit gewährleisten können.

Es ist genauso möglich, kundenspezifische Verschlüsselungsverfahren zu schaffen.

Sicherheitsstufen

Wir ordnen den Sicherheitsstufen, die wir anbieten, verschiedene Algorithmen zu. Die folgende Tabelle zeigt welche Verfahren in welchem Paket enthalten sind. Das ist dann schon eher etwas für Spezialisten, wir wollten es aber nicht vorenthalten.

sec1	Die Minimalkonfiguration für geringe Anforderungen
sec2	Kompletter Umfang für maximale Kompatibilität nach den gültigen RFCs
sec3	Angepasst auf BSI-Anforderungen mit entsprechenden Erweiterungen unter Weglassung der nicht erlaubten Verfahren
sec4	Zusätzlich mit den Hochsicherheitsverfahren nach ellan:sec4

	sec1	sec2	sec3	sec4
Verschlüsselung				
3DES		X		X
AES128	X	X	X	X
AES256		X	X	X
ellan:sec4				X
Hashing				
MD5	X	X		X
SHA-1	X	X		X
SHA-256		X	X	X
ellan:sec4				X
Schlüsselaustausch und Signierung				
DHE		X		X
ECDHE		X		X
RSA	X	X		X
ECDSA		X	X	X
ellan:sec4				X
Zertifikat				
ladbar		X	X	X
enthalten	X	X	X	X
ellan:sec4				X
Protokolle				
TLS 1.2	X	X	X	X
HTTPS	X	X	X	X
FTPS		X	X	X
SFTP		X	X	X
SIPS		X	X	X
SSH		X	X	X
SRTP		X	X	X
ellan:sec4				X