

Sicherheitsevaluation des Siemens Scalance S 612/613 Security Moduls

escrypt GmbH – Embedded Security

<http://www.escrypt.com>

Version: 1.2

Date: 19. August 2005

Inhaltsverzeichnis

1	Einführung.....	4
2	Sicherheitsdienste.....	6
2.1	Annahmen.....	6
2.2	System.....	6
2.2.1	Firewall.....	7
2.2.2	VPN.....	8
2.2.3	Wechselmedium (C-Plug).....	9
2.2.4	Firmwareupdate.....	9
2.3	Konfigurationsmanagement.....	9
2.3.1	Urtaufe und erste Inbetriebnahme.....	10
2.3.2	Benutzermanagement:.....	11
2.3.3	Lernen.....	11
2.4	Schlüsselmanagement.....	11
3	Sicherheitsanalyse.....	12
3.1	Netzwerk- und Protokollanalyse.....	13
3.1.1	VPN.....	13
3.1.2	Firewall.....	14
3.1.3	Firmware Update.....	15
3.1.4	Betriebssystem.....	15
3.1.5	Webserver.....	15
3.1.6	Zeitsynchronisation und Protokollierung.....	16
3.2	Konfiguration.....	16
3.2.1	Konfigurationsdateien.....	17
3.2.2	Bridge.....	17
4	Zusammenfassung.....	19
5	Bezugsdokumente.....	20

Executive Summary

Das Scalance S 612 bzw. S 613 ist ein Gerät zur Absicherung der Kommunikation zwischen Automatisierungsnetzen. Diese Aufgabe leistet es mit der Funktionalität einer Firewall und der Möglichkeit, über ein Virtual Private Network (VPN) sicher zu kommunizieren. Das System ist mit dem Betriebssystem VxWorks ausgestattet und nutzt Firewall und VPN aus OpenBSD, für den Webserver und den Paketfilter der Ebene 2 wurden Siemens eigene Entwicklungen genutzt.

Ein Automatisierungsnetz hat als oberste Priorität die Verlässlichkeit und Robustheit zum Ziel. Insbesondere muss sichergestellt sein, dass das Netz auch bei Störungen funktionsfähig bleibt. Der Aspekt der Datensicherheit folgt darauf. Es ergeben sich daher konkurrierende Ziele, die bei der Umsetzung des Sicherheitskonzeptes in die Standardkonfiguration eingeflossen sind. Nichtsdestotrotz erlaubt das Sicherheitsmodul eine rundum sichere Konfiguration durch manuelles Verschärfen der Regeln. Das Gerät kann aufgrund seiner Bridge Funktionalität auf einfache Weise in bestehende Netzwerke eingefügt werden.

Das Security-Modul erfüllt seine Aufgabe und sichert ein Automatisierungsnetz ab. Hervorzuheben ist dabei die Einfachheit der Konfiguration, wobei trotz dieser Einfachheit die Sicherheit nicht leidet. Das Gerät ist extrem robust aufgebaut und erfüllt die besonderen Anforderungen der Automatisierungsbranche hervorragend. Insgesamt hebt sich das Gerät deutlich von anderen Sicherheitsmodulen (auch außerhalb der Industrialisierungstechnik) ab.

1 Einführung

Das Siemens Scalance S 613 ist ein Security-Modul, welches die Kommunikation zwischen Automatisierungsnetzen sichert. Es gewährleistet die Authentisierung, Datenintegrität und -vertraulichkeit und schützt vor Datenspionage und Datenmanipulation.

In der Automatisierungstechnik findet eine zunehmende Vernetzung der einzelnen Komponenten statt. Diese durchgängige Vernetzung untereinander und auch mit der Office-IT-Welt bietet die Möglichkeit, bekannte Technologien aus dem Office-Bereich im Zusammenhang mit dem Automatisierungsnetz zu nutzen, aber es besteht gleichzeitig auch eine größere Gefahr für Angriffe aus dem externen Netz. Die Absicherung der Automatisierungsnetze ist notwendig, um vor unerlaubtem Zugriff und Störungen aus dem externen Netz zu schützen. Abbildung 1 verdeutlicht diesen Umstand.

Im Gegensatz zur Office-Welt, in der standardisierte Verfahren wie SSL, TLS und IPsec angewendet werden, gibt es noch keine einheitlichen Standards, die die Sicherheit solcher Automatisierungsnetze gewährleisten sollen. Das Security-Modul schützt einzelne Komponenten oder auch ganze Netzsegmente in einem Automatisierungsnetz vor Datenspionage und Manipulation mit Hilfe einer Firewall und durch den Einsatz eines Virtual Private Networks (VPN).

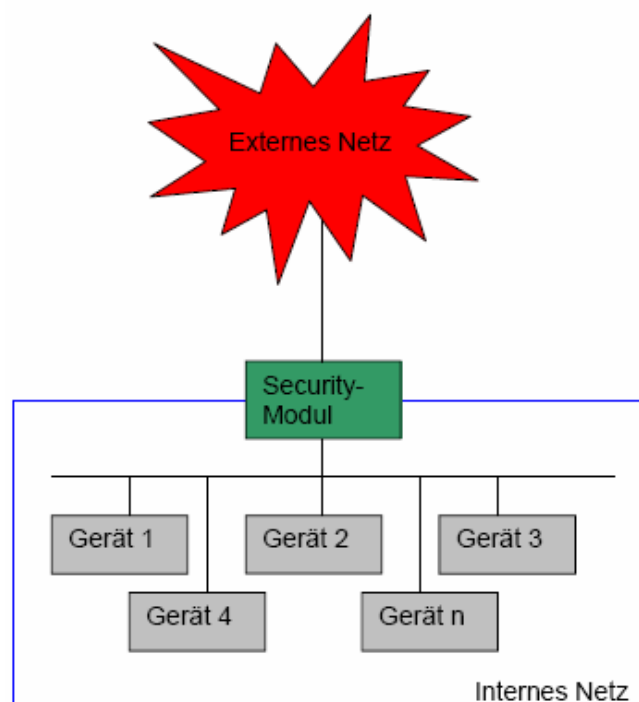


Abbildung 1: Externes Netz <-> Internes Netz

Automatisierungsnetze haben je nach Anwendungsgebiet unterschiedliche Sicherheitsbedürfnisse, so dass nur grundsätzliche Default-Regeln voreingestellt sind. Gleichzeitig sollen die Security-Module leicht zu projektieren sein und auch von Nicht-IT-Experten beherrschbar sein. Das Security-Modul lässt sich den jeweiligen Forderungen entsprechend projektieren, so dass immer ein starker Schutz gegeben ist. Darüber hinaus können Experten weitere Einstellungen im erweiterten Modus durchführen. Das Modul ist in ein bestehendes Automatisierungsnetz einbaubar, ohne dass die Netztopologie geändert werden muss oder Netzteilnehmer neu konfiguriert werden müssen.

Die Konfiguration wird auf einem PC durchgeführt, mit dem es möglich ist, mehrere Security-Module über das Netz gleichzeitig zu konfigurieren. Um den Austausch von defekten Geräten einfach zu halten, können die Konfigurationsdaten auf einem Wechselmedium gespeichert werden (C-Plug genannt). Muss ein defektes Modul ausgetauscht werden, so wird ein Wechselmedium mit gültigen Konfigurationsdaten eingesteckt und das neue Modul kann sofort seine Arbeit aufnehmen. Somit kann ein neues Gerät von jedermann mit einer sicheren Konfiguration in Betrieb genommen werden.

Das Modul arbeitet mit dem Betriebssystem VxWorks der Firma WindRiver. Aus OpenBSD, dem oft als „sichersten“ zitierten Betriebssystem, wurden einige Komponenten herausgelöst. Als HTTPs-Server zur Konfiguration wird MiniWeb verwendet, eine Eigenentwicklung von Siemens, dies wird genutzt um eine sichere HTTPs Verbindung zur Verfügung zu stellen. MiniWeb ist angelehnt an OpenSSL, es nutzt RC4, 3DES und es werden Schlüssellängen bis zu 2048 Bit zur Verfügung gestellt.

Security-Module können in Gruppen zusammengefasst werden, so dass alle Module einer Gruppe in der Lage sind, durch IPsec-Tunnel sicher miteinander zu kommunizieren. Die internen Netzknoten eines Moduls und auch andere Module mit ihren internen Netzknoten können automatisch ohne Projektierung gefunden werden. Das Scalance S 612 kann ein Netz mit bis zu 32 internen Knoten schützen. Das Scalance S 613 schützt bis zu 64 interne Knoten und hat einen erweiterten Temperaturbereich von -20° bis +70°. Mit der PC-Software SOFTNET Security Client sind gesicherte IP-basierte Zugriffe vom PC auf Automatisierungsgeräte in Subnetzen möglich, die durch ein Security-Modul geschützt sind. Mit Hilfe des SOFTNET Security Clients wird ein PC automatisch so konfiguriert, dass er eine gesicherte IPsec Tunnelkommunikation zu einem Security-Modul aufbauen kann. Versorgt wird das Gerät mit einer redundanten Spannungsversorgung von 24 Volt Gleichspannung.

2 Sicherheitsdienste

Das Security-Modul besitzt zwei Ethernet-Schnittstellen, an einer wird das interne zu sichernde Netz angeschlossen, an die andere Schnittstelle wird das externe Netz angeschlossen. Die Schnittstellen sind klar durch eine farbliche Markierung erkennbar, so dass ein Fehler im Anschluss nahezu ausgeschlossen ist. Als Prozessor wird ein Intel IXP425 eingesetzt, dieser unterstützt AES, SHA-1, MD5, DES und 3DES in der Hardware. RSA wird zur Signierung benutzt und ist in Software implementiert.

2.1 Annahmen

Für das Sicherheitsmodul wurden Annahmen für den Betrieb gemacht, um dem besonderen Umfeld der Automatisierung zu genügen. Das interne Netz wird als vertrauenswürdig angenommen. Ebenso wird angenommen, dass die autorisierten Benutzer vertrauenswürdig sind und entsprechend geschult sind, um das Modul richtig zu bedienen. Die Bedienung ist jedoch so einfach wie möglich gestaltet.

Es wird angenommen, dass das Gerät von einem Angreifer physikalisch nicht erreichbar ist. Das Modul kann keinen Schutz mehr bieten, wenn ein Angreifer physikalischen Zugriff auf das Gerät hat und so zum Beispiel das Gerät gegen ein manipuliertes Gerät austauschen kann, das Wechselmedium austauschen kann oder interne Knoten hinzufügen und entfernen kann.

Einen Content-Filter stellt das Security-Modul nicht zur Verfügung. Für den Schutz gegen bösartige Dateiinhalte wie Viren und trojanische Pferde, etc. muss ein Virens scanner bzw. Content-Filter zusätzlich im Netzwerk eingefügt werden.

Für das Automatisierungsnetz gilt, dass die Verlässlichkeit und Robustheit an erster Stelle noch vor der Sicherheit steht. Das bedeutet, dass in Bezug auf die Sicherheit Einschränkungen bei einigen Default-Einstellungen hingenommen wurden.

2.2 System

Das Sicherheitsmodul basiert auf einer Firewall und VPN. Die Firewall wird insbesondere durch einen Paketfilter zur Verfügung gestellt, wohingegen das VPN mit Hilfe von IPsec implementiert wird. SSL wird zur sicheren Konfiguration der Scalance Geräte genutzt, sonst jedoch nicht eingesetzt. Das Gerät verfügt über eine Bridge. Das bedeutet, dass beim Einsatz des Security-Moduls in einem

vorhandenen Netzwerk keine neue Konfiguration der beteiligten Systeme in Bezug auf ihre IP-Adressen, Subnetzmasken und Router erfolgen muss.

2.2.1 Firewall

Um das interne Netz zu schützen, werden nur vorher festgelegte Kommunikationsbeziehungen zwischen Geräten aus dem externen Netz und dem internen Netz erlaubt. Diese Aufgabe wird durch einen Paketfilter auf dem Security-Modul umgesetzt. Der Paketfilter überwacht und regelt die Kommunikation zwischen dem internen und dem externen Netz, siehe auch Abbildung 2.

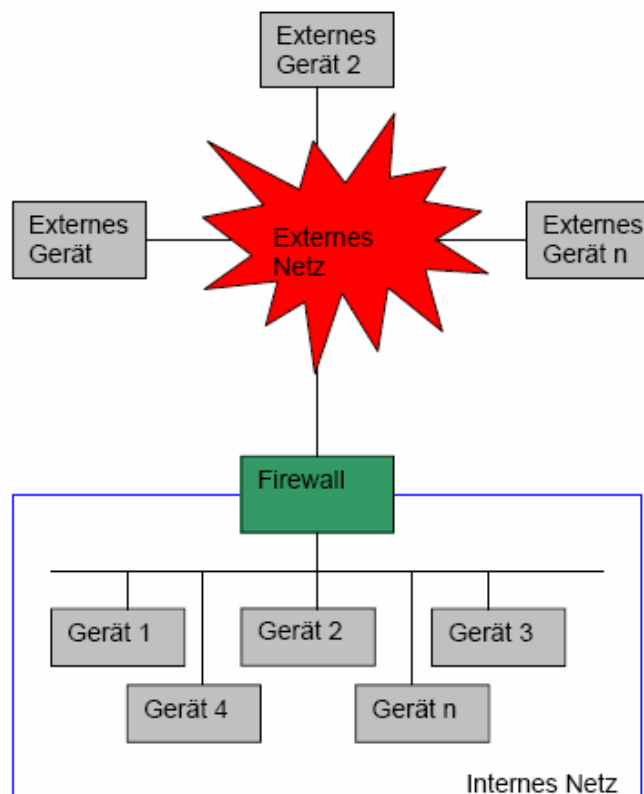


Abbildung 2: Firewall-Funktion des Security-Moduls

Die Firewall bietet einen Paketfilter für IP-Pakete mit Stateful Packet Inspection, diese Funktionalität wurde aus dem Betriebssystem OpenBSD herausgelöst. Ein weiterer Paketfilter für Non-IP-Pakete (Ethernet-Pakete oder Layer-2-Pakete) wurde von Siemens für das Security-Modul entwickelt. Zusätzlich gibt es eine Bandbreitenbegrenzung, um Denial of Service (DoS) Attacken und Cache Flooding zu vermeiden.

2.2.2 VPN

Weiterhin hat das Modul die Aufgabe, zwei oder mehrere interne Netze miteinander zu verbinden. Dies geschieht physikalisch über das externe Netz, das heißt die Nachrichten, die zwei geschützte Geräte austauschen wollen, werden über das ungeschützte Netz gesendet. Um die Vertraulichkeit der Daten zu sichern, kann das Security-Modul einen VPN-Tunnel aufbauen. Dieser Tunnel wird auf der Basis von IPSec realisiert. Werden mehrere bilaterale Tunnel zusammengefasst, ergibt sich ein Virtual Private Network (VPN) wie in Abbildung 3 dargestellt.

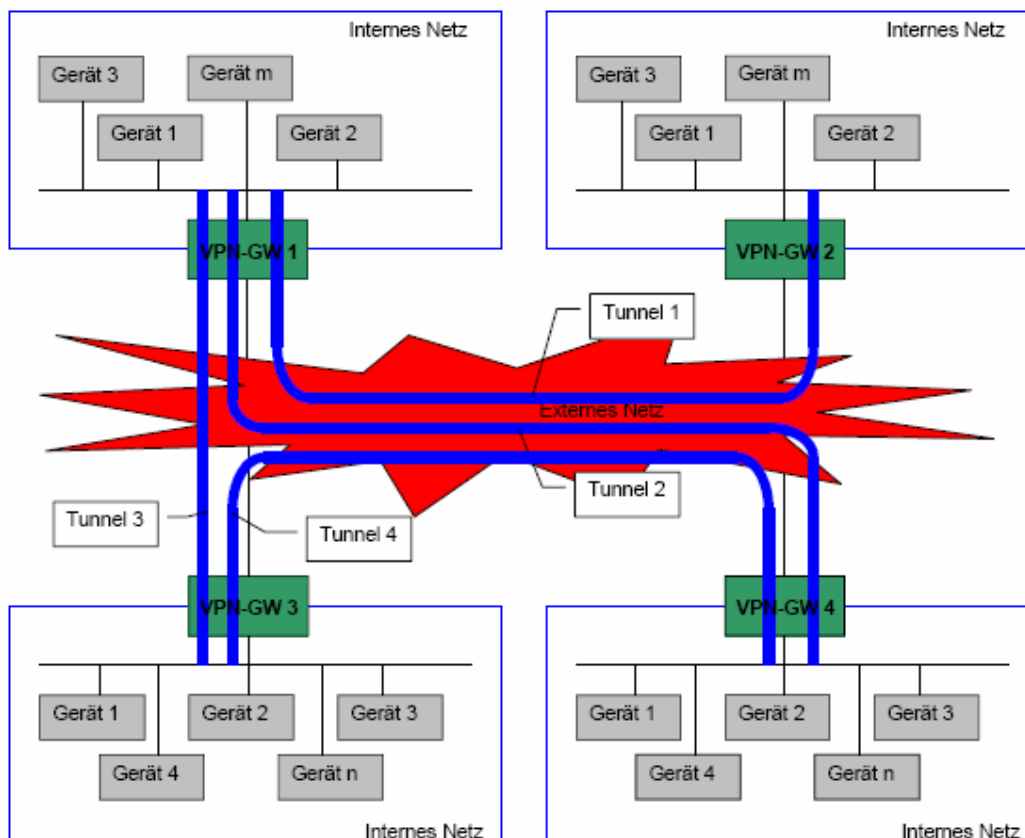


Abbildung 3: VPN-Funktion des Security-Moduls

Für die Kommunikation über ein VPN werden Security-Module zu Gruppen zusammengefasst. Jedes VPN hat ein so genanntes Netzzertifikat mit zugehörigem privatem Schlüssel, welches das VPN eindeutig identifiziert. Jedes Security-Modul, welches zu dem VPN gehört, hat ebenfalls ein Zertifikat, welches mit dem privaten Schlüssel des Netzzertifikats signiert ist. Das Netzzertifikat wird von einer Certification Authority (CA) erstellt oder es wird selbst erstellt.

Die VPNs sind auf der Basis von IPSec realisiert und benutzen die IPSec Schlüsselverwaltung IKE. Die Implementierung wurde aus OpenBSD übernommen.

2.2.3 Wechselmedium (C-Plug)

Die Konfigurationsdaten werden auf einem Wechselmedium, dem so genannten C-Plug, gespeichert. Damit bietet sich eine einfache Möglichkeit, ein defektes Security-Modul auszutauschen, indem man einfach ein C-Plug mit gültigen Konfigurationsdaten in das neue Security-Modul einsetzt. Die Daten auf dem C-Plug werden mit AES verschlüsselt im internen Flash abgelegt. Physikalisch befindet sich auf der Rückseite des Security-Moduls ein Steckplatz für den C-Plug. Dieser Steckplatz ist hinter einer Platte angebracht, diese Platte kann man nur mit Werkzeug öffnen. Dadurch soll ein Austauschen des Wechselmediums für Angreifer erschwert werden.

2.2.4 Firmwareupdate

Es besteht die Möglichkeit, die Firmware zu aktualisieren. Siemens liefert dazu neue Firmware, diese ist verschlüsselt und signiert. Vor dem Laden muss sich der Benutzer gegenüber dem Security-Modul authentifizieren. Vom Konfigurations-PC wird dann die neue Firmware per HTTPs an das Security-Modul übertragen, auf dem Modul wird dann die Signatur überprüft und anschließend wird die neue Firmware entschlüsselt und gespeichert. Ein Security-Modul akzeptiert nur neue Firmware mit korrekter Signatur. Dadurch wird sichergestellt, dass keine manipulierte Flashsoftware in ein Gerät geladen werden kann sondern nur originale authentische Software. Der private Schlüssel liegt bei Siemens, so dass nur Siemens eine neue Firmware ausgeben kann. Der entsprechende öffentliche Schlüssel zur Verifizierung ist im EEPROM eines jeden Scalance Sicherheitsmoduls gespeichert. Beim Aufspielen neuer Firmware wird die Signatur überprüft, beim Booten wird eine Prüfsumme verifiziert. Die Vertraulichkeit der Firmware ist kein Sicherheitsziel sondern lediglich ein Zusatz als größere Hürde falls jemand die Firmware auslesen will.

2.3 Konfigurationsmanagement

Bevor das Security-Modul seine Arbeit aufnehmen kann und ein Automatisierungsnetz schützen kann muss es konfiguriert werden. Dafür steht ein Tool bereit, mit dessen Hilfe die Parameter für die Firewall, das VPN und das Protokollieren eingestellt werden. Ein Modul benötigt mindestens IP-Parameter zum Betrieb, diese werden in den Standardeinstellungen automatisch ermittelt. Es ist möglich, mehrere Module gleichzeitig zu konfigurieren. Diese Konfigurationssoftware läuft auf einem externen PC, über HTTPs werden die Daten an die Module übertragen.

Der Datentransfer zwischen dem internen Netzwerk und dem externen Netzwerk müssen explizit durch Konfiguration zugelassen werden. Die Standardeinstellungen erlauben keinerlei Kommunikation zwischen den Netzen. Die Konfigurationsdaten enthalten entweder nur Paketfilterregeln oder nur die Parameter für die VPN-Funktionalität oder eine Kombination von Paketfilterregeln und VPN. Beim letzteren werden die Paketfilterregeln jeweils am Tunneleingang und Tunnelausgang angewendet.

Die Konfigurationsdaten werden remanent im internen Flash gespeichert. Die Daten werden unverschlüsselt gespeichert, nur während der Übertragung per SSL vom Projektierungs-PC zum Security-Modul sind die Daten verschlüsselt. Wird ein C-Plug gesteckt, werden die Konfigurationsdaten auf den C-Plug verschlüsselt gespeichert. Auf dem Modul werden die Daten gelöscht wenn sie auf dem Wechselmedium gespeichert sind.

Den Nutzern mit eingeschränkten Rechten sind nur wenige Möglichkeiten zur Konfigurierung des Security-Moduls gegeben. Nicht-IT-Experten können das Security Modul konfigurieren, ohne unwissend unsichere Parameter einzustellen. Den Nutzern in der Rolle des Administrators ist die Möglichkeit gegeben, die Parameter von Hand einzustellen.

2.3.1 Urtaufe und erste Inbetriebnahme

Bei der Erstinbetriebnahme erfolgt zunächst die Urtaufe, d.h. den Scalance S Modulen wird eine IP-Adresse zugewiesen. Nach der IP-Konfiguration sind die Module auch über Netz projektierbar. Der erste Benutzer, der das Modul in Betrieb nimmt, wird aufgefordert Benutzernamen und Passwort nach Wahl einzugeben, so dass er damit in der Position eines Administrators ist.

Wird das Security-Modul gestartet oder ein Reset durchgeführt wird enthält es weder im internen Speicher noch auf dem Wechselmedium Konfigurationsdaten, so lässt es keinerlei Kommunikation zu. Dies bedeutet, dass sich das Gerät im Auslieferungszustand und auch nach einer Rücksetzung in einem Zustand befindet, der auf keine Art für einen Angriff aus dem externen Netz genutzt werden kann.

Um das Gerät bei Verlust der Passwörter wieder in Betrieb zu nehmen befindet sich auf der Rückseite des Moduls eine Reset-Taste. Damit wird das Gerät in den Auslieferungszustand zurückgesetzt. Diese Taste befindet sich hinter einer Scheibe die nur mit Werkzeug zu entfernen ist. So ist sichergestellt dass die Reset-Taste nicht versehentlich gedrückt wird und potentiellen Angreifern mit physikalischem Zugriff wird ein Manipulieren erschwert.

2.3.2 Benutzermanagement:

Es gibt zwei Benutzergruppen mit jeweils unterschiedlichen Rechten, einmal den Administrator mit sämtlichen Rechten und dann den normalen User mit eingeschränkten Rechten. Der Administrator ist in der Lage, eine Person einer bestimmten Benutzergruppe zuzuteilen. Die Authentifikation des Nutzers geschieht mittels Digest Authentifikation mit Benutzername und Passwort. Bei dieser Art von Authentifikation wird das Passwort niemals unverschlüsselt übertragen.

2.3.3 Lernen

Um die Konfiguration der Module durch den Nutzer einfach zu halten, wurde die Möglichkeit des automatischen Lernens integriert. Ein Modul kann die Existenz (und damit die Adressen) anderer Module lernen und nimmt sie in seine eigene Liste von erreichbaren Modulen auf. Ebenso kann ein Modul lernen, welche Endgeräte sich im internen Netz eines anderen Moduls befinden. Ein VPN-Tunnel kann nur aufgebaut werden, wenn der Endpunkt (d.h. das Endgerät hinter einem anderen Modul) bekannt ist und damit auch das andere Modul, welches das Netz schützt, in dem sich der Empfänger befindet. Das Lernen geschieht automatisch oder mit manueller Konfiguration.

Dazu ruft das Security-Modul das Security Configuration Protocol (SCP) auf. Dieses Protokoll beinhaltet die Funktionen

- Finden anderer Security-Module
- Zyklischer Austausch der Adressen in den internen Netzen
- Signalisieren, dass ein Datenpaket abgewiesen wurde, weil es nicht über einen IPsec-Tunnel empfangen wurde.

Das Lernen wird immer dann angestoßen, wenn ein Knoten mit einem anderen Knoten kommunizieren will und bei Geräten, die sich im gleichen Subnetz befinden wird auch aktiv mittels ICMP-messages gescannt. Die Informationen über gelernte Teilnehmer wird verschlüsselt zwischen den Modulen übertragen.

2.4 Schlüsselmanagement

Auf dem Security-Modul werden eine Reihe von Zertifikaten, bzw. Schlüsseln verwendet. Die verwendeten Schlüssel werden im nachfolgenden anhand des Anwendungsgebiets beschrieben:

- *Firmware*: Um eine neue Firmware beim Aktualisieren auf Authentizität überprüfen zu können wird diese mit RSA signiert. Der private Schlüssel,

der zum Signieren benutzt wird, liegt bei Siemens, wohingegen der öffentliche Schlüssel zur Verifikation fest im Flash aller Scalance Geräte hinterlegt ist. Zusätzlich ist neue Firmware symmetrisch mit 3DES verschlüsselt, der entsprechende Schlüssel dazu liegt ebenfalls fest im Flash. Dazu wird derselbe Schlüssel für alle Geräte genutzt. Ist der geheime symmetrische Schlüssel zum Entschlüsseln der Firmware kompromittiert, so muss das Gerät an Siemens geschickt werden, dort wird das Security-Modul mit einem neuen Schlüssel versorgt.

- *SSL/Konfiguration:* Für die Kommunikation über SSL ist zur gegenseitigen Authentifizierung ein Server-Zertifikat mit passendem privatem Schlüssel für jedes Security-Modul vorhanden. Wird dieser Schlüssel kompromittiert, so kann ein Administrator neue Zertifikate und Schlüssel erzeugen.
- *VPN:* Hier werden Netzzertifikate mit öffentlichen Schlüsseln benötigt, die ein VPN eindeutig kennzeichnen. Der zugehörige private Schlüssel wird auf dem Konfigurations-PC verwahrt. Für jedes Security-Modul, das zu dem VPN gehört, wird ein Zertifikat ausgestellt, das mit dem geheimen Schlüssel des Netzzertifikats signiert wird. Ein Security-Modul hat somit für jedes VPN, zu dem es gehört, ein Zertifikat mit privatem Schlüssel. Mit diesem Zertifikat authentifiziert es sich bei anderen Security-Modulen, mit denen es einen Tunnel aufbauen will. Wird hier ein Schlüssel kompromittiert, so muss über die Projektierungsdaten ein neues Zertifikat mit Schlüssel erzeugt werden.
- *Konfiguration:* Zur Verschlüsselung der Konfigurationsdaten auf der Memory-Card steht ein globaler symmetrischer Schlüssel zur Verfügung. Die Firmware wird hier mit AES verschlüsselt auf der Karte abgelegt. Wird dieser kompromittiert, so muss eine neue Firmware geladen werden.

3 Sicherheitsanalyse

Das Security-Modul ist für den Einsatz in Automatisierungsnetzen entworfen worden. Für Automatisierungsnetze ist die Verfügbarkeit und Robustheit die erste Priorität, das heißt, dass das Netz vor Ausfällen geschützt sein muss damit die Produktion weitergehen kann. Das geschieht zum Beispiel in der chemischen Industrie auch aus Sicherheitsgründen.

Natürlich gibt es gleichzeitig hohe Anforderungen an die Datensicherheit, das beinhaltet die Vertraulichkeit und Integrität der Daten und Schutz vor Angriffen aus dem externen Netzwerk. Vom technischen Standpunkt erfüllt das Security-Modul diese hohen Anforderungen an die Datensicherheit. In diesem Kapitel werden die technischen Merkmale des Security-Moduls detailliert analysiert.

3.1 Netzwerk- und Protokollanalyse

3.1.1 VPN

Das VPN wird mit der IPsec-Protokollfamilie realisiert. Diese Protokollfamilie hat sich in den letzten Jahren als Industriestandard für VPNs etabliert. So ist eine Interoperabilität mit weiteren Systemen gewährleistet. Im Rahmen dieser Analyse wurde die Interoperabilität mit der IPsec-Implementierung des Linux Kernels 2.6.x unter Einsatz von Openswan und Racoon bestätigt. Für die VPN-Funktion des Scalance Sicherheitsmoduls wurde der IKE-Daemon Isakmpd des OpenBSD Projektes verwendet. Für das IKE-Protokoll unterstützt das Konfigurationswerkzeug die folgenden Algorithmen, wobei die Standardwerte fett dargestellt sind:

Phase 1	
Authentifizierung Modi	RSA-Signatur, PSK
DH-Gruppen	Main, Aggressive
Verschlüsselung	1 (768 Bit Schlüssel), 2 (1024-Bit Schlüssel) , 5 (1536 Bit Schlüssel)
Lebensdauer	DES, 3DES
Authentifizierung	999.999.999 Sekunden
	SHA1, MD5
Phase 2	
Lebensdauer	Time (7200s) , Limit
Verschlüsselung	DES, 3DES , AES
Authentifizierung	SHA1, MD5
PFS	ja, nein

Die Implementierung des IKE-Protokolls weist keine bekannten Fehler auf. Sämtliche in der Vergangenheit bekannt gewordenen Sicherheitslücken in dem OpenBSD-Isakmpd konnten nicht nachgestellt werden. Zusätzlich verfügt das System über eine so genannte VPN-Bridge. Diese ermöglicht es, Nicht-IP-Pakete durch den IPsec-Tunnel zu transportieren. Damit können Broadcast- und Multicast-Pakete als auch ISO-Protokolle transportiert werden. Die Schlüssellänge von 1024 Bit für die DH Gruppe 2 bietet ausreichenden Schutz für die nächsten drei bis fünf Jahre.

Der Aufbau des VPNs erfolgt bei Verwendung der Standardoptionen bei Bedarf. Hierzu tauschen die beteiligten Security-Module Systeme zunächst Informationen aus, welche betroffenen Systeme sie schützen. Ist gleichzeitig normale IP-Kommunikation mit der Außenwelt erlaubt, was jedoch nicht der Standardeinstellung entspricht, schickt das Security-Modul auf der Seite des Kommunikationsclients das erste Paket in Klartext über das Netzwerk. Das Security-Modul auf der Empfängerseite erkennt, dass die Kommunikation über den Tunnel erfolgen sollte, und der Tunnel wird aufgebaut.

Als kritisch ist die Möglichkeit des Einsatzes der DES Verschlüsselung zu betrachten. In Zusammenhang mit der voreingestellten, sehr langen Lebensdauer der Phase 1 von 31 Jahren ist es dann möglich, DES mit einem Brute-Force-Angriff zu brechen (schon 1999 wurde DES in einem Wettbewerb in weniger als einem Tag gebrochen). Da das Konfigurationswerkzeug standardmäßig keine Perfect-Forward-Secrecy (PFS) fordert, kann anschließend auch das gesamte Schlüsselmaterial für das ESP-Protokoll ermittelt werden. Diese Konfiguration ist unter sicherheitstechnischen Aspekten nicht zu empfehlen. Die lange Lebensdauer wurde gewählt um die Verlässlichkeit des Automatisierungsnetzes nicht zu gefährden. PFS ist standardmäßig ebenfalls aus Gründen der Robustheit und Performance ausgestellt. DES aber auch MD5 als Verschlüsselungsfunktion, bzw. Hashalgorithmus, die beide nicht mehr empfohlen werden, wurden aufgrund der RFC Konformität angeboten. Seit einer Aktualisierung der RFC 2409 auf RFC 4109 im Mai 2005 ist die Unterstützung von DES und MD5 jedoch nicht mehr notwendig.

3.1.2 Firewall

Das Security-Modul verfügt über zwei Paketfilter. Der Paketfilter e2f wurde speziell für das Security-Modul entwickelt und ist in der Lage, Ethernet-Pakete zu filtern. Der Paketfilter pf wurde von OpenBSD übernommen und filtert IP-Pakete. Hierbei wird die Stateful-Inspection-Technologie genutzt. Die Stateful-Inspection-Technologie erkennt IP-Verbindungen und erlaubt die Filterung dieser Verbindungen anstelle einzelner Pakete. Zusätzlich wird die Möglichkeit genutzt, die unterschiedlichen Pakete mit Class-Based-Queuing (CBQ) zu priorisieren. Hierdurch wird sichergestellt, dass für die Administrationsprotokolle immer ausreichend Bandbreite zur Verfügung steht und ein Denial-of-Service so nicht möglich ist. Um die Erkennung der Systeme hinter dem Security-Modul zu erschweren, führt der Paketfilter ein so genanntes Scrubbing der Pakete durch.

Der pf-Paketfilter von OpenBSD weist keine bekannten Schwächen auf. Ein Test der von dem Konfigurationswerkzeug umgesetzten Regeln lässt keine Schlüsse auf Design- oder Implementierungsfehler zu. Auch ein Test des Layer-2 Filters e2f offenbarte keine Sicherheitslücken.

3.1.3 Firmware Update

Eine neue Firmware wird verschlüsselt bereitgestellt und ist zusätzlich von Siemens digital signiert. Daher war es nicht möglich, eine manipulierte Firmware in das Gerät zu laden. Da für die Verschlüsselung ein globaler Schlüssel genutzt wird, der in allen Geräten gleich ist, ist es mit etwas Aufwand möglich, diesen aus einem Gerät herauszulesen. Ein Angreifer erhält durch die Kenntnis der Firmware jedoch keinen nennenswerten Vorteil, so dass die Verschlüsselung kein relevantes Sicherheitsziel darstellt.

Falls der geheime Schlüssel, der von Siemens zum Signieren der Firmware genutzt wird, kompromittiert wird, könnte eine beliebige Firmware in das Gerät geladen werden. Die einzige Möglichkeit im Fall einer solchen Kompromittierung ist der Rückruf aller eingesetzten Module. Die Möglichkeit zum Zurückziehen von Zertifikaten, z.B. mit Hilfe einer so genannten Certificate Revocation List (CRL) wäre hier wünschenswert. Weiterhin bietet das Gerät zwar eine Versionskontrolle an, verhindert jedoch nicht das Laden einer veralteten Firmware, die z.B. bekannte Sicherheitsmängel enthält. Eine entsprechende Sperre würde dem Grundsatz der Robustheit widersprechen.

3.1.4 Betriebssystem

Das Security-Modul bietet als einzigen Zugang ein mit SSL geschütztes Webinterface an. Hierüber erfolgt die Steuerung, der Upload der Konfigurationsdateien und der Download der Protokolle. Ein Kommandozeilenzugriff ist nicht vorgesehen. Schwachstellen in dem verwendeten VxWorks Betriebssystem konnten somit nicht festgestellt werden.

3.1.5 Webserver

Auf dem Security-Modul befindet sich ein SSL-Webserver, eine Eigenentwicklung von Siemens mit dem Namen MiniWeb-Server. Ein Zugriff auf den Webserver ist nur per SSL möglich. Der MiniWeb-Server basiert auf OpenSSL und nutzt standardisierte kryptographische Verfahren. Nach Anmeldung mit dem in dem Konfigurationswerkzeug angelegten Benutzer wird man mit der Meldung Siemens AG, Security Module begrüßt. Weitere Optionen sind nicht vorhanden. Eine Analyse des Konfigurationswerkzeuges ließ keinen Schluss auf die verwendeten

URLs zu. Die Zertifikate für den Webserver werden von dem Konfigurationswerkzeug automatisch erstellt. Dabei erhalten die Zertifikate 1024 Bit lange Schlüssel und eine Lebensdauer von ca. 32 Jahren. Als Hashverfahren wird MD5 genutzt. SSL Zertifikate können aber auch individuell durch eine externe Zertifikatsautorität erstellt und mit dem Konfigurationswerkzeug geladen werden.

Der MiniWeb-Server hinterließ einen soliden Eindruck. Die SSL-Implementierung scheint keinen Fehler aufzuweisen. Lediglich die hohe Lebensdauer des Zertifikates und die Verwendung des MD5 Hashwerts für die Erzeugung der Signaturen in den Zertifikaten könnte in Zukunft eine Sicherheitslücke darstellen. Die Schlüssellänge von 1024 Bit ist ausreichend für die nächsten drei bis fünf Jahre.

3.1.6 Zeitsynchronisation und Protokollierung

Das Security-Modul erlaubt eine Zeitsynchronisation mit dem (Simple-)Network-Time-Protocol (NTP). Das NTP-Protokoll ist ein UDP-Protokoll. Der Client fragt einen NTP-Server nach der Uhrzeit, worauf der Server mit seiner aktuellen Zeit antwortet. Da das UDP-Protokoll verwendet wird, bietet das NTP-Protokoll keinen Schutz vor IP-Spoofing oder Datenmanipulation.

Das NTP-Protokoll garantiert weder Authentizität noch Integrität der übertragenen Zeit. Eine Fälschung der Informationen erlaubt einen Denial-of-Service-Angriff (DoS) auf die VPN-Funktion. Das NTP-Protokoll sollte daher vorsichtig genutzt werden.

Die Protokollierung weist einige Lücken auf. So werden abgelaufene Zertifikate und ARP-Spoofing-Attacken nicht aufgezeichnet. Selbst wenn aufgrund von abgelaufenen Zertifikaten keine IPsec-Tunnel aufgebaut werden können wird dies nicht protokolliert. Eine Veränderung der Uhrzeit wird nur bei einer manuellen Einstellung protokolliert, nicht jedoch bei einer Änderung über NTP. In der Standardeinstellung werden zahlreiche Vorgänge nicht protokolliert. Selbst wenn alle Protokollierungseinstellungen aktiviert sind, werden einige der beschriebenen Vorgänge nicht protokolliert.

3.2 Konfiguration

Die Konfiguration erfolgt mit einem Security Configuration Tool. Dieses Werkzeug speichert seine Dateien verschlüsselt auf der Festplatte ab. Die Übertragung der Informationen zum Security-Modul erfolgt SSL-verschlüsselt. Bei der ersten Übertragung ist eine direkte Verbindung zum Security-Modul erforderlich, da die

Adressierung des Security-Modul über ihre MAC-Adresse erfolgt. Sobald die erste Übertragung der Daten stattgefunden hat, ist die weitere Konfiguration und Kommunikation über IP möglich. Hierzu werden von dem Konfigurationswerkzeug Zertifikate und Schlüssel übertragen, die anschließend für die Sicherung der Kommunikation genutzt werden.

Es war nicht möglich, die Verschlüsselung der Konfigurationsdateien zu brechen. Ein Angriff als Man-in-the-Middle auf die verschlüsselte SSL-Übertragung ist genauso wenig möglich. Da kein weiterer Zugang zum Security-Modul möglich ist, kann die Übertragung der Konfiguration als sicher eingestuft werden.

3.2.1 Konfigurationsdateien

Das Konfigurationswerkzeug überträgt die Konfiguration für das Security-Modul per SSL-Verbindung. Dadurch sind ein Abhören der Verbindung und eine Ermittlung der Dateien nicht möglich. Die Analyse der Konfigurationsdateien erlaubt nur eine Aussage über den Default-Zustand der Firewall. Die in der Datei definierten Regeln lassen jedoch keinen Fehler erkennen. Die Dateien sind sehr gut dokumentiert und weisen keine logischen Fehler auf.

3.2.2 Bridge

Um die Konfiguration und Implementierung des Security-Moduls zu vereinfachen, verfügt das Security-Modul über eine Bridge-Funktionalität. Standardmäßig befindet sich die Bridge normalerweise in einem Lernmodus, in dem sie selbst die Standorte der weiteren beteiligten Netzwerkkomponenten lernt. Dies erfolgt ähnlich einem Switch mit Hilfe des ARP-Protokolls. Es besteht auch die Möglichkeit, den Lernmodus zu deaktivieren und die MAC-Adressen der beteiligten Systeme manuell mit dem Konfigurationswerkzeug einzugeben. Dies ist jedoch nur möglich, nachdem der Anwender den erweiterten Modus aktiviert hat.

Es war möglich, mit ARP-Spoofing außerhalb der geschützten Netze einen geschützten Rechner zu imitieren und so die Security-Module zu veranlassen, die Daten ungeschützt zu versenden. Dies war jedoch nur möglich, wenn die Firewall-Funktionalität ungehinderten IP-Verkehr mit dem ungeschützten Netzwerk zuließ (nicht Default).

Obwohl die Bridge-Funktionalität mit ihrem Lernmodus die Administration der VPN und Firewallfunktionalität stark vereinfacht, befindet sich hier auch ihre größte Schwäche. Ein Angreifer in dem lokalen Netz kann mit Hilfe von ARP-Spoofing ein von dem Security-Modul geschütztes System imitieren und so in Klartext die einseitige Kommunikation führen oder sogar als Man-in-the-Middle arbeiten. Dies

ist jedoch ein prinzipielles Problem und kann nicht als spezielle Schwachstelle des Sicherheitsmoduls angesehen werden, insbesondere da die Standardeinstellung diesen Angriff verhindert.

4 Zusammenfassung

Das Security Modul ist für den Einsatz in einem Automatisierungsnetz vorgesehen. Dieses soll es vor Datenspionage und Manipulation sowie externen Angriffen schützen. Dabei hat die Zuverlässigkeit des Netzes die höchste Priorität, die Datensicherheit folgt sofort darauf. Zudem soll das Gerät einfach zu konfigurieren sein. Diese Grundannahmen spiegeln sich in den Standardeinstellungen wider.

Das Security-Modul leistet unter diesen Annahmen ausgezeichnete Dienste. Das Sicherheitsmodul bietet in der Standardkonfiguration einen ausreichenden Schutz für die meisten Anwendungen, obwohl hier auch einige Schwachstellen aufgrund der Zuverlässigkeit hingenommen werden müssen. Das Modul ist extrem einfach einzusetzen und zu konfigurieren, so dass auch Nicht-Datensicherheitsexperten das Gerät nutzen können. Es ist möglich, das Gerät für nahezu alle Anforderungen sicher einzustellen.

Zusammengefasst lässt sich sagen, dass das Scalance Security Modul die hohen Sicherheitsanforderungen erreicht. Die Konfiguration ist extrem einfach, so dass mit wenigen Handgriffen ein sicheres Netzwerk konfiguriert werden kann. Fehleinstellungen sind hier kaum möglich. Die Automatisierungsbranche erfordert extrem robuste Komponenten, so dass hier Zugeständnisse gemacht werden mussten. Auf der anderen Seite ist es jedoch leicht möglich, mit Hilfe des Sicherheitsmoduls ein nach dem heutigen Wissensstand rundum sicheres Netzwerk zu installieren. Ein sehr robustes Gehäuse rundet das Bild ab.

5 Bezugsdokumente

Pflichtenheft, Version 1.0 vom 7.10.2003

Sicherheitsvorgaben, Version 0.2 vom 31.10.2003

Betriebsanleitung, Ausgabe 1/2005

Entwurfsunterlage vom 19.1.2004