Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 168 (2002)

Heft: 6

Artikel: Die Kryptologie : der Schlüssel zum Informationsschutz

Autor: Curiger, Andreas / Minder, Markus

DOI: https://doi.org/10.5169/seals-67969

Die Kryptologie – der Schlüssel zum Informationsschutz

Sicherheit ist ein Thema, welches uns nicht erst seit den Ereignissen vom 11. September 2001 stark beschäftigt. Die Sicherheit ist gar als Staatszweck in der Bundesverfassung verbrieft, wo es wörtlich heisst: «Die Schweizerische Eidgenossenschaft schützt die Freiheit und die Rechte des Volkes und wahrt die Unabhängigkeit und die Sicherheit des Landes.» Während dem Schutz von Personen und Material meist die gebotene Aufmerksamkeit geschenkt wird, fehlt oft die letzte Konsequenz beim Schutz digitaler Information, obschon die dazu von der Kryptologie bereitgestellten Mechanismen vorhanden wären.

Andreas Curiger und Markus Minder

Die Sicherheit im Visier

Sicherheit kann als Zustand definiert werden, in welchem bestimmte Vermögenswerte (Menschen, Land, Information) vor möglichen Bedrohungen (Naturgewalten, böswillige Zerstörung, Abhorchen) geschützt sind. Dieser Zustand ist jedoch ständigem Wechsel unterworfen, weil sich die Rahmenbedingungen im steten Fluss befinden. Somit ist die Sicherheit eher eine Abfolge von Zuständen und damit ein ständiger Prozess.

Um Sicherheit zu erreichen, muss man die erwähnten Rahmenbedingungen kennen. Dies erfolgt durch Analyse möglicher Bedrohungen. Wenn man sich im Klaren ist, durch welche Faktoren die zu schützenden Vermögenswerte bedroht werden, ist mittels Risikoanalyse die Eintretenswahrscheinlichkeit der Bedrohung und deren existenzielle Auswirkung auf die Vermögenswerte abzuwägen. Erst nach eingehender Risikoanalyse kann mit dem Erstellen eines Sicherheitskonzepts begonnen werden. Das Sicherheitskonzept listet schliesslich konkrete Massnahmen in personeller, organisatorischer, technischer und baulicher Hinsicht auf, die ergriffen werden müssen, um die Sicherheit der zu schützenden Vermögenswerte zu gewährleisten.

Spätestens hier wird klar, dass die absolute Sicherheit nicht erreicht werden kann. Mit der Risikoanalyse befinden wir uns im Gebiet der Wahrscheinlichkeitsrechnung, und das Sicherheitskonzept muss sich auch nach finanziellen Limiten ausrichten. Es gilt somit, mit den vorhandenen Mitteln die wahrscheinlichsten Bedrohungen und solche mit den grössten existenziellen Auswirkungen abzuwenden. Eine wahrlich schwierige und immer wieder zu rechtfertigende Aufgabe, sich gegen etwas teuer zu versichern, wenn dieser Akt gar nie eintreten sollte – nicht nur im militärischen Bereich!

Sorgenkind Informationsschutz

Relativ gut beherrschen wir personelle (Ausbildung), organisatorische (Protokollierung, unumgehbares Rollenkonzept) und bauliche (Zugangskontrolle, Brandschutz) Massnahmen im Sicherheitskonzept, weil wir es hier mit physischen Objekten, d. h. mit Menschen und Sachen zu tun haben. Die technischen Massnahmen zum Schutz elektronischer Information (Verschlüsselung, Passwort, digitale Unterschrift) jedoch sind zwar verfügbar, aber werden nicht konsequent angewandt. Die Schwierigkeit mit den digitalen Objekten hat verschiedene Ursachen: Die Bedeutung der Informationstechnologie wächst, neue technische Anwendungen (E-Mail, WWW, E-Commerce) schiessen wie Pilze aus dem Boden. Sicherheitsmechanismen in Systemen und Netzwerken fehlen, da normalerweise Verbindung vor Sicherheit kommt. Zudem sind heutige informationstechnologische Systeme sehr komplex. Nicht zu vergessen ist auch die Tatsache, dass die Rechtsprechung der technischen Entwicklung stets hinterher läuft und die Entscheidungsträger oft wenig sensibilisiert sind. Beispiele liefern uns die Medien en masse. Sobald Software mehr als nur ein paar Seiten Code umfasst, enthält sie immer Fehler. Programme verhalten sich dann unter selten auftretenden Bedingungen nicht wie erwartet, was von entsprechend geübten Personen ausgenutzt wird – deshalb auch die immer wiederkehrenden «Security Patches», mit welchen mehr oder weniger verzweifelt versucht wird, entdeckte Sicherheitslöcher zu stopfen.

Wird Information von einem als sicher eingestuften Ort zu einem ebensolchen durch ein als nicht sicher klassiertes Gebiet übermittelt, tritt ein weiteres Problem auf. Eine Umfrage in Deutschland hat gezeigt, dass nur 4% der befragten Firmen die Daten, welche sie übers Internet verschicken, auch verschlüsseln. Dem Missbrauch sind damit Tür und Tor geöffnet. Verschicken denn tatsächlich 96% aller Firmen nur Daten, welche sie gerade so gut auch in der Tageszeitung veröffentlichen würden?

Information kann nur dann effizient geschützt werden, wenn entsprechende Sicherheitsdienste zur Verfügung stehen: Dienste, welche die Geheimhaltung (Vertraulichkeit), die Unversehrtheit der Daten (Integrität) während der Übertragung, den Nachweis der Echtheit des Senders oder des Empfängers gewährleisten (Authentisierung); Dienste, mit welchen gemachte Vereinbarungen im Nachhinein nicht mehr abgestritten werden können; Dienste, welche eine Beglaubigung der Übertragung durch eine Drittinstanz ermöglichen.

Um Informationssicherheit zu erreichen, müssen nicht alle denkbaren Sicherheitsdienste zusammen vorhanden sein. Es reicht, wenn Geheimhaltung, Authentisierung und Integrität garantiert sind. Diese Dienste können effizient durch Sicherheitsmechanismen in Hard- oder Software aufgebaut werden.

Die Kryptologie als Schlüsseltechnologie

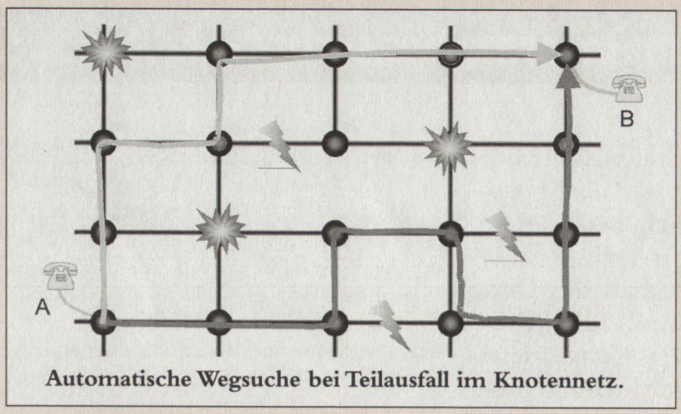
Bei diesem Aufbau kommt uns die Kryptologie zu Hilfe. Die Kryptologie befasst sich mit denjenigen mathematischen Verfahren, welche sich auf alle Aspekte der Informationssicherheit beziehen, eben zum Beispiel auf Vertraulichkeit, Unversehrtheit der Daten, Authentisierung von Einheiten (Geräten, Personen) und Authentisierung des Ursprungs der Daten. Die Kryptologie selbst besteht aus zwei Studienrichtungen:

Gelesen

in der NZZ vom 10. Mai 2002 unter dem Titel: ***«Die Armee XXI zur Kooperation befähigen»*** von bre.

«Gemäss der politischen Vorgabe ‹Sicherheit durch Kooperation› hat die Armee XXI internationale Kooperations- und Einsatzfähigkeit zu erreichen …

Berufsoffiziere sollten deshalb vor allem in entsprechende multinationale Brigadestäbe und in Bataillonsstäbe entsandt werden. Nach dem Motto ‹Train the trainers› kann das Berufskader dereinst für die geforderte Breitenwirkung in der Armee besorgt sein.» G.



Automatische Wegsuche bei Teilausfall im Knotennetz.


Digitale Teilnehmerstation KP


Digitale Teilnehmerstation Gefecht

Die Kryptografie befasst sich mit dem Entwurf und dem Gebrau0ch der kryptologischen Verfahren, Werkzeuge und Protokolle, also dem «Code Making», während die Kryptoanalyse versucht, Schwächen in Verfahren, Werkzeugen und Protokollen zu finden und sich somit dem «Code Breaking» widmet.

Die Geschichte der Kryptologie ist lang und faszinierend. Der ständige Kampf zwischen Kryptografen und Kryptoanalysten spielte sich bis in die zweite Hälfte des 20. Jahrhunderts fast ausschliesslich im militärischen Bereich ab. Seit der Begründung der Informationstheorie durch C. Shannon im Jahr 1948 und unterstützt durch die rasante Entwicklung der elektronischen Rechenanlagen hat sich seit den 70er-Jahren ein eigenes Wissenschaftsgebiet entwickelt. Aus den einfachen Buchstabensubstitutionen, mit denen Julius Caesar dazumal seine Texte verschlüsselt haben soll, sind komplexe Strom- und Blockchiffrierer geworden, welche eine effiziente Analyse des chiffrierten Texts selbst mit der gesamten Rechenleistung, die auf der Erde in fünfzig Jahren zur Verfügung stehen könnte, wenn sich diese alle 18 Monate verdoppeln sollte, verunmöglicht. Seit der Entdeckung der Public-Key-Verfahren im Jahr 1976 und der zwei Jahre später publizierten RSA-Methode gibt es auch Instrumente, wie geheime Schlüssel über einen unsicheren Kommunikationskanal vereinbart werden können, ohne dass ein Horcher dabei fähig wäre, ebenfalls den geheimen Schlüssel zu errechnen. Dies sind nur zwei von etlichen Beispielen, die belegen, wie es die Kryptografie ermöglicht, mathematisch gut erforschte und nicht knackbare Sicherheitsmechanismen zu konstruieren – wenn sie nur angewendet würden!

Schweizer Armee und Kryptologie

Die Schweizer Armee hat den Wert der Kryptografie als Werkzeugkiste für den Informationsschutz schon früh erkannt und ihre Kommunikationssicherheit kontinuierlich darauf aufgebaut. Das integrierte militärische Fernmeldesystem IMFS ist das automatische, flexible und feldtaugliche Telekommunikationsnetz der beweglich eingesetzten Grossen Verbände. IMFS optimiert den Einsatz bei beweglichen und semi-stationären Verbänden. Durch Integration des taktischen Funks lassen sich auch hochmobile Einheiten rasch und sicher erschliessen. Die Kommunikation mit anderen Netzen ist durch Netzübergänge im IMFS gewährleistet. Das öffentliche Wählnetz, das automatische Fernmeldenetz Stufe Landesregierung und Armeekommando und die Funknetze der Truppe können auf diese Art eingebunden werden.

Ab dem Jahr 2004 wird das Transparente Datennetz mobil der Grossen Verbände des Heeres und der Luftwaffe (TRANET mob) eingeführt. Dabei handelt es sich um eine Erweiterung des IMFS mit einer durchgängigen Datenkommunikation zugunsten von Führungsinformations- und Fachsystemen.

Fazit: Das IMFS ist das Hauptübertragungssystem für Sprache und Daten auf Stufe der beweglich eingesetzten Grossen Verbände. Dieses System macht sich die durch die Kryptografie ermöglichten Sicherheitsdienste bei der Übertragung von Sprache, Fax und Daten voll zunutze.

Problematisch wird die Situation jedoch dort, wo die Sicherheit nicht genügend analysiert worden ist. Hand aufs Herz: Wie steht es mit der Vertraulichkeit und Integrität der Daten auf Ihrem persönlichen Notebook, welches Sie zur Erleichterung der Abläufe mit in den WK nehmen? Wie gross ist das Risiko, dass ein Unbefugter an diese Daten gelangen kann? Verwenden Sie Sicherheitsmechanismen auf Ihrem Notebook, welche es Ihnen erlauben, auch dann ruhig zu schlafen, wenn es Ihnen entwendet worden ist?

Sicherheit bedeutet immer einen zusätzlichen Aufwand. Dies gilt auch für die Informationssicherheit. Die Werkzeuge für den Schutz der Information sind vorhanden. Es ist höchste Zeit, dass sich nicht nur Fachleute diese Werkzeuge zunutze machen! ■

Gelesen

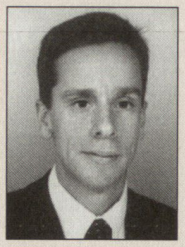
in Jane's Defence Weekly Article, 9th May 2001: ***«Russia has no reconnaissance satellites in orbit»*** by Philip S. Clark, JDW Special Correspondent, London.

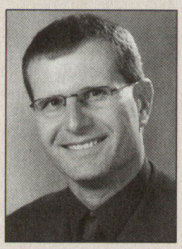
Russia no longer has any photo-reconnaissance satellites in orbit following the return to earth of two satellites in recent weeks.

First to return was Cosmos 2372, which was de-orbited on 19 April after 207 days in orbit. Then Cosmos 2370 was de-orbited after a year in orbit on 3 May or 4 May.

The Russian photo-reconnaissance satellite programme has been running at a low level in recent years after the 1970s and 1980s when more than 30 launches would take place each year: in 1999 there was only one launch and in 2000 three launches took place.

Four types of photo-reconnaissance satellite are currently operated by Russia, three belonging to the Yantar family and one to the Orlets family. The Yantar-1KFT, codename Kometa, satellites are launched once every year or two and undertake missions to update topographic and mapping data maintained by the Ministry of Defence. A. St.


Andreas Curiger, Dr. sc. techn. ETH, Leiter Kryptologie, Omnisec AG, 8108 Dällikon.


Markus Minder, Oberstlt i Gst, Instr Of BAUT/AUEM, 8733 Eschenbach.