Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 147 (1981)

Heft: 2

Artikel: Erhöhung der betrieblichen Sicherheit von Chiffriersystemen

Autor: Hartmann, Peter

DOI: https://doi.org/10.5169/seals-53639

und **auf der einen das Imperium Russland 1939 und auf der andern das Imperium Russland 1980 rot anzufärben.** Diese beiden Karten solle er, als unzweifelhaft wahren Geographieunterricht, nebeneinander über dem Kasernentor annageln, im Theoriesaal und in den Schlafsälen aufhängen, verkleinert auf den Mostgläsern der Kantine einätzen und als Kleber auf die Effektentasche abgeben. Und den Aufdruck nicht vergessen: «Die ‚Befreiung' der freien Völker.» Ich befürchte, sein Kreditgesuch wird abgelehnt werden, das Aufheulen unserer totalitären Kamarilla wäre auch gar zu schrill. ■

Erhöhung der betrieblichen Sicherheit von Chiffriersystemen

Dipl. Ing. Peter Hartmann

Eine Sicherheitsanalyse von Chiffriersystemen zeigt, dass heute die Schwachstellen vor allem im betrieblichen Bereich liegen. Zu diesen gehört der Verlust des Schlüssels durch Verrat oder Erpressung. Es wird ein Verfahren beschrieben, welches diese Schwachstellen weitgehend ausschaltet. ewe

1 Rückblick

Das Bedürfnis, Nachrichten zu verschlüsseln, ist schon sehr alt. So trägt ein bekanntes, heute allerdings nicht mehr verwendetes Chiffrierverfahren den Namen Caesar, und auch dem amerikanischen Präsidenten Thomas Jefferson wird die Erfindung einer Chiffriereinrichtung zugeschrieben.

Mit dem Aufkommen der drahtlosen Funkübertragung, bei der grundsätzlich jedermann mithören kann, **stieg das Bedürfnis nach Chiffrierung** gewaltig an. Im Zweiten Weltkrieg wurden von allen Parteien mechanische und elektromechanische Chiffriergeräte eingesetzt, welche auf verschiedenen Funktionsprinzipien beruhten.

Parallel zum immer weiter verbreiteten Einsatz von Chiffriergeräten **stieg auch der Aufwand, um die chiffrierten Nachrichten der Gegenpartei zu entschlüsseln.** Es ist bekannt, dass die amerikanischen Behörden den von den Japanern benützten diplomatischen Code bereits 1940 geknackt hatten und so den Text der japanischen Kriegserklärung bereits vor der Überbringung durch den japanischen Botschafter kannten. In den letzten Jahren ist auch bekannt geworden, dass die Engländer das von der deutschen Wehrmacht verwendete Enigma-Gerät entschlüsseln konnten und dank der Tatsache, dass dieses Chiffriergerät auch auf den höchsten Stufen eingesetzt war, über die Entscheide der deutschen Heeresführung weitgehend auf dem laufenden waren. Eine spezielle Organisation mit dem Codenamen «Ultra» wurde aufgezogen, um die auf diesem Weg gewonnenen Informationen den alliierten Staatschefs und Heereskommandanten zu übermitteln. Dabei ging es aber auch um die Geheimhaltung der Quelle dieser Informationen, denn bei einem Bekanntwerden wäre diese wohl sofort versiegt.

2 Der heutige Stand der Technik

Die Computertechnik und das Aufkommen der modernen Halbleiterelektronik **eröffneten der Chiffriertechnik neue Horizonte.** So wie die elektromechanischen Rechner innert weniger als einem Jahrzehnt durch elektronische Rechner abgelöst worden sind, werden auch elektromechanische Chiffriergeräte bald der Vergangenheit angehören. Zur Zeit werden für die **Schweizer Armee** Kanalchiffriergeräte KCG-70 und Fernschreib- und Datenchiffriergeräte TC-535 beschafft. Bei beiden Geräten handelt es sich um vollelektronische Geräte.

Die heutigen modernen Mittel erlauben eine stark gesteigerte **Komplexität der Chiffriergeneratoren** bei gleichzeitiger Reduktion des Gerätevolumens und des Stromverbrauches. Die zunehmende Verbreitung digitaler Daten- und Sprachübertragung erleichtert die Integration von Chiffriergeräten in diese Netze.

Natürlich darf nicht übersehen werden, dass heute die moderne Computertechnik auch dem Gegner weitaus **leistungsfähigere Hilfsmittel zur Entschlüsselung** in die Hand gibt.

Sonderdrucke der ASMZ

«Menschenführung im Militär»
Dieser Sonderdruck der ASMZ erscheint der grossen Nachfrage wegen bereits in 4. Auflage! Die Leitsätze der «Menschenführung im Militär» eignen sich besonders in OS und UOS. Bezug von 1 bis 20 Ex. je Fr. 1.20, über 20 Ex. je Fr. 1.–, bei Huber & Co. AG, Presseverlag, 8500 Frauenfeld.

Bericht über Stand und Ausbau der materiellen Verteidigungsbereitschaft der Armee
Dieser Bericht des Generalstabschefs, als Sonderheft der ASMZ Juli/August 1980 der ASMZ beigelegt, wurde ebenfalls neu gedruckt, da er von verschiedenen Seiten vor allem als Dokumentation im Truppen-Informations-Dienst gewünscht wird. Bezug bei Huber & Co. AG, Presseverlag, 8500 Frauenfeld. Einzelexemplare bis 9 Stück je Fr. 1.50, 10 bis 99 Stück je Fr. 1.20, ab 100 Stück je Fr. 1.–.

Wir zitieren: Grundregeln für den militärischen Führer

Im Army-Officer-Guide, einem Handbuch für Offiziersanwärter der amerikanischen Kadetten in Westpoint, heisst es ganz simpel:
- Führe durch Beispiel.
- Kenne deine Männer und sorge für sie.
- Entwickle einen hohen Grad an Verantwortungsbewusstsein und Zutrauen in dich selbst und in deine Männer.
- Kenne deine Aufgaben.
- Informiere deine Männer.

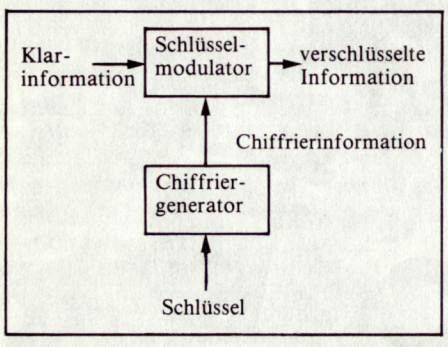
(Aus «Das Unteroffizierskorps der Bundeswehr» in «Information für die Truppe» Nr. 10/80, Bonn.)

3 Sicherheitsanalyse

Absolut sichere Chiffrierverfahren sind theoretisch möglich. Die meisten dieser Verfahren beruhen auf dem **Prinzip,** dass jede einzelne Amplitude der in eine diskrete Aplitudenfolge aufgelösten Klarinformation durch eine neue ersetzt wird, die einen beliebigen, zufällig gewählten Wert im ganzen Amplitudenbereich annimmt. Die auf der Sendeseite und Empfangsseite synchron zugefügte Chiffrierinformation ist eine unerschöpfliche Signalfolge, die eine reine Zufallsverteilung aufweist. Das so erzeugte und übertragene Chiffrat stellt **reines Rauschen** dar, enthält für sich allein keinerlei Information und kann somit unmöglich dechiffriert werden, wenn die Chiffrierinformation nicht zugänglich ist, beziehungsweise für Demodulationsversuche nicht zur Verfügung steht.

Wegen der benötigten grossen Menge an Chiffrierinformation im Fall der echt zufälligen Signalfolge bedingen diese Verfahren einen grossen Aufwand für deren Verteilung und Speicherung an den Endstellen einer Verbindung. **Daher werden in praktisch allen Anwendungsfällen auf der Sende- und Empfangsseite synchron zu startende und laufende Chiffriergeneratoren eingesetzt.** Diese erzeugen in Abhängigkeit von einem eingestellten Schlüssel die Chiffrierinformation, die sich aufgrund der inneren Gesetzmässigkeiten des Generators aufbaut und daher nicht mehr echt zufällig ist, sondern eine sogenannte Pseudo-Zufallsfolge darstellt. Der am Chiffriergenerator eingestellte Schlüssel umfasst je nach Anwendung zwischen 10 und 100 Ziffern. Die zu verteilende Informationsmenge ist dadurch erheblich reduziert, allerdings unter Inkaufnahme einer nicht mehr absoluten Sicherheit.

Das Blockschema eines derartigen Chiffriergerätes ist in Figur 1 gezeigt. Die Chiffrierinformation steuert den Schlüsselmodulator, welcher die Klarinformation in die verschlüsselte Information umwandelt.



Figur 1:
Blockschema eines Chiffriergerätes

Ansatzpunkt des Gegners	mögliche Schwachstellen	
	technisch	betrieblich
Klarinformation	Abstrahlung/Übersprechen	Verrat/Erpressung
Chiffrierinformation	Abstrahlung/Übersprechen	–
Geheimschlüssel	Probieren aller Möglichkeiten	Erbeutetes Gerät Verrat/Erpressung
Erzeugung der Chiffrierinformation	Modell des Chiffriergenerators	–

Das Ziel des Gegners ist die Kenntnis der geheimen Klarinformation, beispielsweise also das Abhören eines Telefon- oder Funkkanals. Um dem Gegner das Erreichen dieses Zieles unmöglich zu machen beziehungsweise möglichst zu erschweren, müssen **alle Schwachstellen** eines Chiffriersystems ausgeschaltet werden.

Bei der **Analyse der Schwachstellen** muss man davon ausgehen, dass **der Gegner die Funktion des Chiffriergerätes im Detail kennt** oder sogar im Besitz eines Gerätes ist und lediglich den eingestellten Schlüssel nicht kennt. In der obenstehenden Tabelle sind die möglichen Schwachstellen zusammengestellt; wie die Tabelle zeigt, liegen die Schwachstellen sowohl im technischen als auch im betrieblichen Bereich.

3.1 Schwachstellen im technischen Bereich

Der Gegner kann versuchen, direkt die Klarinformation zu gewinnen, indem er **ungewollte Abstrahlungen oder Übersprechen** dieser Information auswertet. So kann zum Beispiel bei nicht speziell geschützten Fernschreibern der übermittelte Text mit hinreichend empfindlichen Instrumenten direkt über die Netzleitung abgehört werden. Derartige Methoden sind in Botschaften erfolgreich praktiziert worden. Man kann sich dagegen schützen, indem man durch geeignete Schutzmassnahmen Abstrahlungen und Übersprechen der Klarinformation verhindert, beziehungsweise auf ein nicht mehr auswertbares Mass reduziert.

In gleicher Weise kann man sich **gegen Abstrahlung und Übersprechen der Chiffrierinformation schützen.** Kennt der Gegner die Chiffrierinformation, kann er damit in den meisten Fällen aus der verschlüsselten Information die Klarinformation zurückgewinnen.

Da man voraussetzen muss, dass der Gegner die Funktion des Chiffriergerätes kennt, kann er die geheime Nachricht durch **Probieren aller Schlüssel** immer entschlüsseln. Die Schlüsselvielfalt kann jedoch immer gross genug gewählt werden, damit der Aufwand für das Durchprobieren aller Schlüssel prohibitiv wird. Nimmt man beispielsweise an, der Gegner könne pro Sekunde 10^{15} Schlüssel probieren (10^6 parallele Computer, jeder probiert 10^9 Schlüssel pro Sekunde), so benötigt er bei 10^{50} Schlüsseln zum Probieren aller Schlüssel 10^{35} Sekunden oder 3×10^{27} Jahre. Der Gegner ist daher gezwungen, nach anderen Möglichkeiten Ausschau zu halten.

Durch **mathematische Analyse der Chiffrieralgorithmen** beziehungsweise -generatoren kann der Gegner versuchen, ein vereinfachtes (zum Beispiel lineares) Modell zu entwickeln. Er kann auch versuchen, **Schwachstellen im Algorithmus zu finden,** um diese bei der Entschlüsselung auszunützen. Der Chiffrieralgorithmus muss somit einerseits komplex sein, um eine mathematische Analyse zu erschweren, andererseits soll er aber hinreichend durchschaubar sein, um die Schwierigkeit einer mathematischen Analyse abschätzen zu können und eine eindeutige Aussage darüber zu ermöglichen, ob keine Schwachstellen vorhanden sind.

Bei mechanischen und elektromechanischen Geräten wurden mittels analytischer Methoden in der Vergangenheit beachtliche Erfolge erzielt. **Bei elektronisch erzeugten Chiffriersignalen** kann man jedoch die Komplexität derart steigern, dass der analytische und rechnerische Aufwand für den Gegner prohibitiv wird. Die Möglichkeit, dass er eine vorher unbekannte Schwachstelle entdeckt und ausnützt, kann jedoch nie ganz ausgeschlossen werden.

Zusammenfassend kann gesagt werden, dass die Schwachstellen im technischen Bereich durch die Wahl geeigneter Chiffrieralgorithmen, hinreichende Schlüsselvielfalt und sorgfältigen elektrischen Aufbau praktisch vollständig ausgeschaltet werden können.

3.2 Schwachstellen im betrieblichen Bereich

Der Gegner kann versuchen, **durch Verrat oder Erpressung in den Besitz**

der Klarinformation, das heisst der geheimen Nachricht, zu kommen. Die geheime Nachricht ist mindestens dem Sender und dem Empfänger bekannt, meistens aber auch einem weiteren Kreis von Personen. Je kleiner dieser Personenkreis, desto geringer die Gefahr, dass die Nachricht durch Verrat oder Erpressung in die Hände des Gegners gerät.

Im Verlauf von kriegerischen Handlungen besteht immer eine gewisse Möglichkeit, dass ein **Gerät mit eingestelltem Schlüssel** in die Hände des Gegners fällt. Tritt dieser Fall ein, muss der im Netz verwendete Schlüssel kurzfristig gewechselt werden können.

Analog zur geheimen Nachricht kann auch **der geheime Schlüssel durch Verrat oder Erpressung** in die Hände des Gegners gelangen. Die betrieblichen Schutzmassnahmen sind dabei gleich, das heisst die Kenntnis des Schlüssels soll auf einen möglichst kleinen Personenkreis beschränkt sein. Wäre der Schlüssel überhaupt niemandem bekannt, könnte er auch nicht verraten oder erpresst werden.

4 Schutz vor Verrat und Erpressung durch Autogenschlüssel

Die Sicherheitsanalyse von Chiffriersystemen zeigt, dass mit den heutigen mathematischen und technischen Mitteln die **Schwachstellen im technischen Bereich praktisch vollständig ausgeschaltet werden können.** Dadurch gewinnen die Schwachstellen im betrieblichen Bereich an Bedeutung; zu diesen gehört der Verlust des Schlüssels durch Verrat und Erpressung.

In den Entwicklungslaboratorien der Firma BBC Brown, Boveri wurde in der Form des Autogenschlüssels eine Lösung für dieses Problem gefunden. Diese Lösung ist in den Chiffriergeräten der neuesten Generation bereits verwirklicht.

Mit den heutigen technischen Mitteln ist die Möglichkeit gegeben, an den Endstellen einer Verbindung durch die Chiffriergeräte selbst identische neue Schlüssel (sogenannte Autogenschlüssel) erzeugen zu lassen. Voraussetzung dazu ist, dass die Geräte mit einem bereits eingegebenen Schlüssel synchronisiert sind. Der **Autogenschlüssel** ist eine komplizierte Funktion des früher eingegebenen Schlüssels und zusätzlich vom Zeitpunkt der Erzeugung abhängig.

Der Schutz vor Verrat und Erpressung wird dadurch erreicht, dass nach Inbetriebnahme einer Verbindung mit einem neu ins Gerät eingegebenen Schlüssel raschmöglichst ein Autogenschlüssel erzeugt und in den Chiffriergenerator eingegeben wird. Der neu erzeugte Autogenschlüssel wird durch das Gerät nicht angezeigt und kann auch nicht durch Manipulationen zugänglich gemacht werden.

Der Autogenschlüssel wird innerhalb einer Punkt-Punkt-Verbindung erzeugt, ohne dass dabei die Verbindung gestört wird. In einem Netz ergibt sich daraus – aus einem für alle Verbindungen identischen ersten Schlüssel für jede Strecke – ein individueller Schlüssel. Somit kann auch die Verteilung einer grossen Anzahl verschiedener Schlüssel vermieden werden. ■

Bücher und Autoren:

Die deutsche Luftwaffe im Afrika-Feldzug 1941/1943

Von Werner Held und Ernst Obermaier. 237 Seiten, über 500 Fotos und Abbildungen, Motorbuch-Verlag, Stuttgart 1979, DM 39,–.

Aus der Sicht der deutschen Führung zuerst als «Nebenkriegsschauplatz» betrachtet, hat der Krieg in Nordafrika trotz Klima- und Versorgungsproblemen rasch Dimensionen angenommen, die eine immer umfangreichere deutsche Beteiligung erzwangen. Dem tapferen Einsatz der deutschen Flieger in diesem im Grunde hoffnungslosen Kampf gegen einen zunehmend überlegener werdenden alliierten Gegner ist der vorliegende Band aus der Reihe «Bildreport Weltkrieg II» gewidmet. Die grosse Zahl unveröffentlichter Fotos, meist aus Privatarchiven, und ein leichtfasslicher, prägnanter Text machen dieses Buch für alle interessant, die sich in irgendeiner Form mit diesem Abschnitt der Weltgeschichte befassen. FS

Die Seeschlacht von Coronel und Falkland

Von Geoffrey Bennett. Heyne Taschenbuch Verlag, München 1980.

Spannend und lehrreich zugleich sind die mit zahlreichen durch den deutschen Übersetzer fachkundig ergänzten Schilderungen über die für die Royal Navy wenig ruhmreiche Schlacht von Coronel. Dort – vor der chilenischen Küste – hatten die britischen Schiffe («Good Hope», «Glasgow», usw.) gegen ein deutsches Geschwader («Scharnhorst», «Gneisenau», usw.) unter dem berühmten Admiral Graf Spee eine empfindliche Niederlage erlitten. Erstmals seit über 100 Jahren hatte ein deutsches Geschwader einen Sieg über die Royal Navy errungen. Im gleichen Jahre – im Dezember 1914 – revanchierte sich die britische Marine in der Schlacht von Falkland. Das kräftemässig unterlegene, deutsche Geschwader verlor bei diesem Gefecht auch den Chef des ursprünglich in ostasiatischen Gewässern operierenden Kreuzergeschwaders. Die Wiedergabe vieler Zitate aus Originaldokumenten verleiht dem Taschenbuch eine gewisse Lebendigkeit. Es lässt sich entsprechend leicht lesen. J. K.

Die Besatzer und die Deutschen: Amerikanische Zone 1945–1948

Von Klaus-Jörg Ruhl. 200 Seiten, 169 Abbildungen. Droste-Verlag, Düsseldorf 1980. DM 46,–.

Die deutsche Geschichte von 1945 bis 1948 – der Zeit, in der das Land zwischen Briten, Franzosen, Amerikanern und Russen in vier Besatzungszonen aufgeteilt war – dürfte denjenigen, die diese Jahre nicht selber miterlebt haben, eher unbekannt sein. Der vorliegende Text/Bild-Band über das Leben im amerikanisch besetzten Teil ist ein Beitrag, um diese Lücke zu schliessen. Zudem darf er wohl als Ergänzung der im gleichen Verlag erschienenen Text/Bild-Bände über die französische und die britische Zone verstanden werden.

In sechs Kapiteln schildert der Autor den Einmarsch der Amerikaner und ihre Versuche, die Deutschen zu entnazifizieren und zur Demokratie umzuerziehen. Er beschreibt aber auch die Existenzbedingungen in diesem in Trümmern liegenden Deutschland der ersten Nachkriegsjahre, die Not und Verzweiflung der Menschen, die sich wohl anfänglich über ihre Befreiung freuten, jedoch kurze Zeit später unter Hunger, Kälte und Wohnungsnot litten. Zahlreiche Abbildungen, Quellentexte von alliierter und deutscher Seite sowie Augenzeugen- und Erlebnisberichte ergänzen den Text. D. Heuberger

Militärgerichtsbarkeit in der DDR

Von Regina Rühmland. J.-Schweitzer-Verlag, BRD 1980.

Über die Militärgerichtsbarkeit in einem kommunistischen Staat gibt es auffallend wenig seriöse Literatur. Im Osten werden die mit diesem Fragenkomplex zusammenfallenden Probleme unter Ausschluss der Öffentlichkeit behandelt. Nicht einmal vollgestreckte Todesurteile an Soldaten, die in den Volksarmeen auch in Friedenszeiten keine Seltenheit sind, werden publik gemacht! So ist es nur zu begrüssen, wenn Frau Rühmland in ihrer knapp gehaltenen, aber das Wesentliche aufzeigenden Abhandlung die Militärgerichtsbarkeit in der DDR zusammenfasst. Sie schreibt dabei sowohl über die Militärgerichte als auch über die Rechtspflege in den DDR-Streitkräften und schildert die Zusammenstellung der Militärgerichte sowie ihre Zuständigkeit. Auch die Institution der Militärstaatsanwaltschaft gehört zum Inhalt der Abhandlung, deren Fortsetzung, wenn möglich, umfangreicher nur wünschenswert wäre! PG