Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 176 (2010)

Heft: 12

Artikel: Vertrauensvolle Informationssicherung durch ganzheitliche Lösungsbeurteilung

Autor: Koch, Christoph

DOI: https://doi.org/10.5169/seals-131261

Vertrauensvolle Informationssicherung durch ganzheitliche Lösungsbeurteilung

Informationssicherheit beschäftigt verschiedenste Organisationen und ist nicht mehr nur im Militär- oder Behördenumfeld ein wichtiges Thema. Das Vertrauen in sichere kryptographische Chiffrierverfahren ist vor allem durch die Verbreitung des Advanced Encryption Standard (AES)-Algorithmus breit gestreut. Dies reicht jedoch für eine ganzheitliche Beurteilung von Sicherheitssystemen nicht aus. Nur die Möglichkeit der Einsicht in die Umsetzung dieser Chiffrierverfahren in produktive Systeme kann das Vertrauen etablieren.

Christoph Koch

Die Notwendigkeit, vertrauliche Informationen auszutauschen, ohne dass dabei ein Unberechtigter mitlauschen kann, ist ein Bedürfnis, welches schon seit Urzeiten existiert, in der heutigen Gesellschaft nichts an Aktualität verloren hat, und auch in absehbarer Zukunft kaum an Bedeutung verlieren wird. Die Lösungen, die dieses Bedürfnis befriedigen, haben sich jedoch im Laufe der Zeit tiefgreifend verändert – besonders wegen der rasanten Entwicklung der Computer-Hardware, aber auch wegen der enormen Fortschritte der Kryptografie.

Lange Zeit war die Datenverschlüsselung dem Militär und dem diplomatischen Corps vorbehalten. Dies hatte einerseits damit zu tun, dass Industrie und Privatpersonen gar nicht die technischen oder finanziellen Mittel besassen, über grosse Distanzen in Echtzeit miteinander zu kommunizieren. Andererseits beruhten aber auch die Mechanismen der Datenverschlüsselung darauf, dass die Endgeräte, welche die Verschlüsselung vorgenommen hatten, strikte unter Verschluss gehalten werden mussten. Der Diebstahl eines Geräts hätte einem Angreifer die Möglichkeit geboten, durch Analyse der Mechanik wichtige Komponenten der Verschlüsselung zu erkennen und die Verschlüsselung im Wesentlichen zu knacken.

Fortschritte in der Mechanik führten in den Dreissigerjahren des letzten Jahrhunderts dazu, dass das Reverse-Engineering eines Geräts allein nicht mehr ausreichte, um die verschlüsselte Kommunikation zu knacken. Die darin implementierten Chiffrierverfahren waren allerdings noch nicht genügend stark, um unsachgemässer Anwendung wirklich stand zu halten. So wurde bekanntlich die Enigma nicht zuletzt dadurch geknackt, dass ihre Benutzer die Schlüssel nicht häufig genug wechselten, die gleiche Meldung im Klartext sowie im Chiffrat verschickten oder die Meldung immer mit den gleichen Klartext-Sequenzen beginnen liessen.

Seit der Begründung der Informationstheorie im Jahr 1948 durch C.E. Shannon hat die Kryptografie die Defizite bezüglich Chiffrierverfahren mehr als wettgemacht. Algorithmen, die nach dem Stand der Technik entworfen und verifiziert worden sind, gelten heutzutage als sicher, selbst wenn der Analyst jedes Detail des Verfahrens kennt und alle nur denkbare Rechenleistung auf der Erde zur Verfügung hätte, um es zu knacken. Diebstahl und Reverse-Engineering lohnen sich somit nicht mehr, denn das Geheimnis ist nicht mehr im Verschlüsselungsverfahren, sondern einzig und allein in den kryptografischen Schlüsseln verborgen.

Warum werden dann Algorithmen überhaupt noch geheim gehalten? Und warum kommen dann trotz starker Algorithmen immer wieder Sicherheitslücken in Programmen und Geräten zum Vorschein? Im Folgenden wollen wir auf die wirklichen Schwachstellen eingehen.

Das PIN-geschützte und temperresistente Security Modul schützt die kryptografischen Schlüsse. Bild: Omnisec AG

Hardware ist nicht gleich Hardware

Um an Geheimnisse zu kommen, verspricht die direkte Attacke auf den Klartext den grössten Erfolg. Warum sich mit aussichtsloser Kryptoanalyse abmühen,

wenn man anderweitig einfacher zur Information kommen kann? Beliebtestes Mittel dazu ist der Einbau von Wanzen. Wanzen bestehen heute aber nicht nur aus Mikrofon und Sender im altbekannten Telefonhörer, sondern haben den Weg längst schon auf offene Computerplattformen in Form von Spyware und anderer bösartiger Software (z. B. Keylogger) gefunden.

Kryptografie auf dem Papier und im Produkt

Seit bald 40 Jahren hat die Wissenschaft immer bessere Informationsverschlüsselungs- und Authentisierungs-Methoden gefunden. Algorithmen werden in öffentlichen Verfahren evaluiert und die Entwurfskriterien dokumentiert. Es existiert z. B. zurzeit keine effiziente Attacke, um das Chiffrierverfahren AES (symmetrisches Kryptosystem, welches im Jahr 2000 vom National Institute of Standards and Technology (NIST) zum Standard erklärt wurde) zu knacken. Auf der anderen Seite darf starke Kryptologie auch heute in viele Länder nicht exportiert werden. Gewisse Hersteller behelfen sich damit, dass im Produkt gar nicht das darin ist, was sie auf dem entsprechenden Datenblatt anpreisen. Oder die Anwender nehmen konsterniert zur Kenntnis, dass in einem auf einem sicheren Algorithmus basierenden Produkt der verwendete Schlüssel künstlich reduziert wird.

Das Schlüsselmanagement – die vernachlässigte Komponente

Schlüssel können auch auf eine andere Art und Weise künstlich kurz gehalten werden, sodass bei einer Attacke nicht der gesamte Schlüsselraum abgesucht werden muss: durch unsachgemässe Anwendung eines Software-Zufallszahlengenerators. Oder durch schwache Verschlüsselung von Sessionsschlüsseln, die zusammen mit der verschlüsselten Nachricht übermittelt werden. Oder dadurch, dass über lange Zeit immer der gleiche Schlüssel angewendet wird.

Die Krux mit der Anwendung

Mit der Kryptografie wird uns eine Werkzeugkiste zur Verfügung gestellt, mit welcher sich mannigfaltige Sicherheitsdienste umsetzen lassen – von der Verwaltung der Zugriffsrechte über die Datenverschlüsselung bis hin zur Authentifizierung von Daten und deren Sender und Empfänger. Diese Sicherheitsdienste müssen aber nahtlos ineinander greifen, damit sie nicht ausgehebelt werden können. Die schlimmste Situation trifft ein, wenn ein ahnungsloser Anwender im Glauben an ein sicheres System dieses durch eine Fehlmanipulation zu einem unsicheren macht. Eine Fehlmanipulation – provoziert beispielsweise durch komplizierte Konfigurationsarbeiten, die zu einer unsicheren Datenübertragung führt, wird kaum bemerkt und nie rapportiert.

Ist keine Verschlüsselungsanwendung sicher?

In offenen Netzwerken ist «der Algorithmus» also in der Tat ein Nebenschauplatz in der Beurteilung der Informations- und insbesondere der Kommunikationssicherheit. Das Produkt muss bedeutend höheren Anforderungen genügen, nämlich der nahtlosen Integration und sicheren Umsetzung der Sicherheitsmechanismen.

Angesichts der geschilderten Probleme, die bei der sicheren Umsetzung der Kryptografie auftreten, müsste die Ratlosigkeit bei einer Organisation gross sein, die den Auftrag hat, ein sicheres Kommunikationssystem aufzubauen. Selbst Produkte, die durch Drittstellen auf hoher Sicherheitsstufe zertifiziert sind, zeigen Fehler in der Umsetzung; das Vertrauen ist dahin. Mit grossen Risiken verbunden sind beispielsweise Entschlüsse, etwa die Flucht nach vorne durch den Versuch einer Eigenentwicklung zu wagen, oder wenig vertrauenswürdige Produkte einzusetzen. Dabei hat deren Anwendung einer strikten Geheimhaltung zu unterliegen, um die Chancen einer erfolgreichen Lauschattacke durch Angreifer zu minimieren.

Vertrauen durch Methodik, Erfahrung, Kontrolle

Der Ansatz vieler Anbieter von Sicherheitslösungen, Kommunikationssicherheit durch Sicherheitsmechanismen nachträglich zu implementieren, schlägt ganz offensichtlich fehl. Die Sicherheitsmechanismen müssen bereits bei den allerersten Schritten in der Produktentwicklung berücksichtigt werden. Die Methode hierfür besteht in der Definition und der Anwendung einer ausgereiften Sicherheitsarchitektur.

Während der Produktentwicklung muss die Sicherheitsarchitektur strikte eingehalten werden, wobei der Erfahrung bei der Umsetzung grosse Bedeutung beizumessen ist. Ob diese Umsetzung auch fehlerfrei funktioniert hat, muss auf jeden Fall verifizierbar bleiben. Denn sichere Kryptografie existiert, und genauso existieren auch sichere Umsetzungen. Überzeugen Sie sich selbst! ■

Hptm
Christoph Koch
Dipl. El. Ing. ETH
Projektleiter
5512 Wohlenschwil

RUAG strukturiert sich neu

In Anlehnung an ihre Strategie einer Fokussierung auf die Kerngeschäfte hat der Verwaltungsrat der RUAG Holding AG entschieden, die Divisionen RUAG Electronics und RUAG Land Systems per 1. Januar 2011 zur Division RUAG Defence zusammenzuführen. Seit dem Abgang des CEO RUAG Electronics im Juni 2010 wurde diese Einheit ad interim durch Dr. Lukas Braunschweiler, CEO der RUAG Holding AG, geleitet.

Mit der neuen zusammengeführten Division RUAG Defence soll in Zukunft eine verbesserte Kundenansprache in der Schweiz – für den Schlüsselkunden Schweizer Armee – sowie im ausgewählten Ausland erreicht werden. Kunden, Partner und Mitarbeitende können von einem breiten Portfolio und Dienstleistungen aus einer Hand profitieren. Kern des Portfolios sind die Kampf-, Führungs- und Kommunikationssysteme sowie Schutzmodule für Landstreitkräfte samt den dazugehörenden Ausbildungs- und Simulationssystemen auf Basis der Bedürfnisse der Schweizer Armee.

Die Leitung der Division RUAG Defence übernimmt auf den 1. Januar 2011 Urs Breitmeier, seit 2006 CEO von RUAG Land Systems und Mitglied der Konzernleitung. *Ma*