ISSN 1861-0641

IT-Sicherheit & Datenschutz

Ausgabe 11/05
18.11. – 16.12. 2005

Zeitschrift für rechts- und prüfungssicheres Datenmanagement

Praxis – Anwendungen – Lösungen

Sicherheits- und Datenschutz-Management

Grundlagen – Technik und Methoden

EXTRA

Vorschriften – Gesetze – Urteile

Online-Service
www.it-sd.com

VOGEL

Der Informationsdienst für IT-Manager,
IT-Sicherheits- und Datenschutzverantwortliche.

Detlev Spierling

Public-Key-Infrastrukturen – ein Schlüssel zur IT-Sicherheit (Teil II): Symmetrische und asymmetrische Verschlüsselung

Als Grundvoraussetzung für das Funktionieren einer Public-Key-Infrastruktur (PKI) hatten wir im ersten Teil dieses Beitrags (vgl. Heft 9/2005, S. 126ff.) den Einsatz asymmetrischer Verschlüsselung genannt. In dieser Ausgabe wird die Technik näher erläutert und von anderen Verfahren abgegrenzt.

Alle Verschlüsselungsverfahren lassen sich in symmetrische und asymmetrische Verfahren einteilen

Alle Verschlüsselungs- oder Chiffrierverfahren lassen sich grundsätzlich in zwei Klassen einteilen: symmetrische und asymmetrische Verfahren. Der Austausch von Nachrichten zwischen zwei Kommunikationspartnern – ***Sender (S) und Empfänger (E)*** – folgt dabei immer dem gleichen Schema:

1. Beide Seiten vereinbaren ein *Chiffrierverfahren*.
2. Sie vereinbaren einen *Schlüssel* bzw. ein *Schlüsselpaar* (d. h. eine geheime Zahl oder Bitfolge).
3. S verschlüsselt eine Nachricht und sendet diese an E.
4. E entschlüsselt den von S gesendeten Geheimtext.

Symmetrische Verschlüsselungsverfahren

Symmetrische Verfahren setzen denselben Schlüssel zum Chiffrieren und Dechiffrieren ein; sie sind schnell und einfach zu handhaben

Diese Kategorie wird so genannt, weil S und E denselben Schlüssel sowohl für das Chiffrieren als auch das Dechiffrieren ihrer Nachrichten nutzen. Sie werden deshalb gelegentlich auch als Ein-Schlüssel-Verfahren bezeichnet. Bekannte symmetrische Verschlüsselungsverfahren sind z. B. DES, Triple DES, IDEA oder RC5. Symmetrische Verschlüsselungsverfahren haben folgende *Vorteile*:

- Sie sind schnell, d. h. sie haben einen hohen Datendurchsatz und sind deswegen für lange Texte bzw. häufiges Chiffrieren gut geeignet.
- Die Sicherheit wird im Wesentlichen durch die Schlüssellänge bestimmt, d. h. es gibt keine Angriffe, die mehr Erfolg versprechen als das Durchprobieren aller denkbaren Schlüssel (sog. Brute-Force-Attacken).
- Sie bieten hohe Sicherheit bei relativ kurzem Schlüssel.
- Die Schlüsselerzeugung ist einfach, da als Schlüssel gewöhnlich eine Zufallszahl gewählt und als beliebige Bitfolge einer festen Länge dargestellt werden kann.

Sicherheitsrisiken bestehen hinsichtlich Geheimhaltung und Übermittlung; zudem ist die Verwaltung einer Vielzahl von Schlüsseln problematisch

Daneben bestehen leider auch einige *Nachteile*, die allerdings weniger mit der Qualität der Verschlüsselung „an sich“ als vielmehr mit der Übermittlung zu tun haben:

- S und E müssen den Schlüssel stets absolut geheim halten. Desgleichen müssen die Übertragungswege für den Schlüsselaustausch hundertprozentig sicher sein, da jeder kundige Angreifer zunächst versucht, sich so viele Informationen wie möglich vorab zu beschaffen, ehe er mit dem Dechiffrieren einer Nachricht beginnt.
- Wollen beide mit mehreren Partnern Informationen austauschen, so benötigen sie für jeden einen eigenen Schlüssel – andernfalls wäre bei einem erfolgreichen Angriff sofort ihre komplette Kommunikation dechiffriert. Das bedeutet hohen „Verwaltungsaufwand“.
- Da sich bei Verwendung symmetrischer Schlüssel nicht ohne weiteres feststellen lässt, welcher Kommunikationspartner eine Nachricht verschlüsselt hat, fehlt ihnen die für einen gesicherten Datenaustausch unerlässliche Möglichkeit, ein Dokument eindeutig einem User zuzuordnen (Verbindlichkeit). Sie lässt sich nur durch eine zwischengeschaltete dritte Partei herstellen – ein weiterer Risikofaktor.

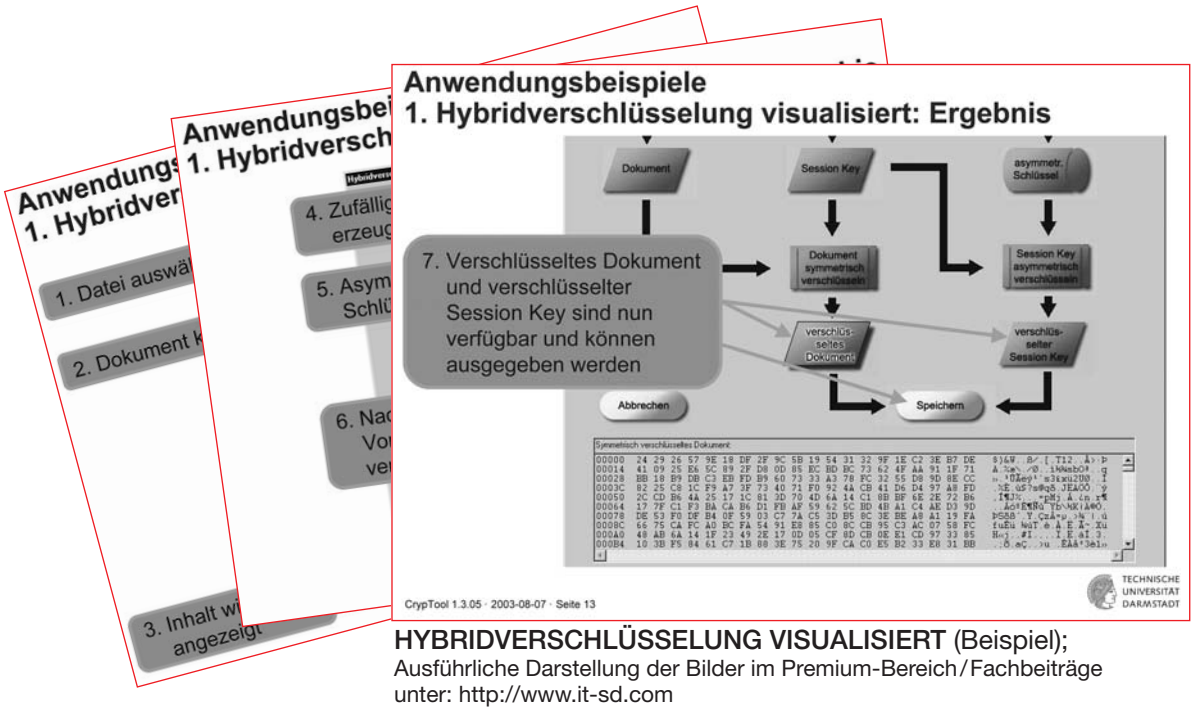
Asymmetrische Verschlüsselungsverfahren

Bei asymmetrischen Verfahren verfügt jeder Anwender über ein Paar verschiedener Schlüssel: den sog. „öffentlichen“ Schlüssel (*public key*), der zum Chiffrieren, und den „privaten“ Schlüssel (*private key*), der zum Dechiffrieren dient (daher auch Public-Key-Verfahren). Damit ein Sender S mit ihm kommunizieren kann, hinterlegt der Empfänger E seinen *public key* auf einem frei zugänglichen Server im Netz. Anders als beim vorgenannten Verfahren *muss* also ein Element öffentlich bekannt sein, damit die Prozedur funktioniert. Dabei darf sich der *private key* in keinem Fall aus dem *public key* ableiten lassen und auch sonst nicht bekannt werden, andernfalls ist die Verschlüsselung wertlos. Asymmetrische Verfahren haben also eine „Einbahn-Eigenschaft“: Eine Nachricht kann nicht wiederhergestellt werden, wenn der private Schlüssel vergessen oder gelöscht wurde. Bekannte asymmetrische Verschlüsselungsverfahren sind RSA und die Klasse der ElGamal-Verfahren.

Übermittlung und Geheimhaltung werden somit stark vereinfacht; außerdem bieten asymmetrische Verfahren einen Zusatznutzen, da sie sich für digitale Signaturen nutzen lassen

Die wichtigsten *Vorteile* von Public-Key-Verfahren sind:

- Jeder Kommunikationspartner muss nur seinen eigenen privaten Schlüssel geheim halten.
- Sie bieten elegante Lösungen für die Schlüsselverteilung in Netzen, da die öffentlichen Schlüssel frei zugänglich sind; die Sicherheit wird dabei nicht beeinträchtigt.
- Sie lassen sich einfach für digitale Signaturen benutzen, wodurch die Quelle eines Dokuments jederzeit feststellbar ist.



HYBRIDVERSCHLÜSSELUNG VISUALISIERT (Beispiel);
Ausführliche Darstellung der Bilder im Premium-Bereich / Fachbeiträge unter: http://www.it-sd.com

- Sie sichern darüber hinaus die Verbindlichkeit, etwa durch Erzeugung eines Zeitstempels für ein Dokument. Jede Manipulation daran zerstört auch die digitale Signatur.

Wie oben gibt es auch hier gewichtige *Nachteile*:

- Public-Key-Verfahren sind langsam, d. h. sie haben im Allgemeinen einen geringen Datendurchsatz.
- Um das gleiche Maß an Sicherheit zu erzielen wie bei symmetrischen Verfahren, müssen wesentlich längere und komplexere Schlüssel erzeugt werden; der Prozess ist damit länger und aufwändiger.
- Ferner beruht die Sicherheit auf einer von der Fachwelt anerkannten Schwierigkeit eines mathematischen Problems, z. B. der Zerlegung einer großen Zahl in ihre Primfaktoren. Diese Probleme werden jedoch Schritt für Schritt mit Hilfe immer leistungsfähigerer Rechner gelöst, so dass die Sicherheit letztlich immer nur relativ ist.

Asymmetrische Verschlüsselung ist deutlich komplexer und kostet daher mehr Zeit als ein symmetrisches Verfahren

Da der Anwender die Sicherheitsvorteile asymmetrischer Verfahren mit erhöhtem Rechenaufwand bezahlt, werden in der Praxis oft **hybride Verfahren** eingesetzt, die die Vorteile beider Methoden kombinieren: Dabei werden die Daten nach dem klassischen symmetrischen Muster verschlüsselt, während die Schlüsselverteilung asymmetrisch erfolgt, indem ein sog. *session key* (Sitzungsschlüssel) erzeugt wird.

In der Praxis werden daher meist Mischformen eingesetzt

Zum Autor:
Detlev Spierling ist freier IT-Fachjournalist und Inhaber des *Redaktions- & PR-Büros Spierling*. Er schreibt für die Tages- und Fachpresse und berät IT- und Telekommunikationsunternehmen bei ihrer Presse- und Öffentlichkeitsarbeit.
E-Mail-Kontakt: ds@spierling.de