SECFORS

Security an der Fachhochschule Rhein-Sieg

Skalierbarkeit beim Betrieb von Key Recovery Centern

Maßnahmen zur Realisierung unterschiedlicher Sicherheitsniveaus

Thomas Hungenberg

03. Mai 1998

Dieser Text schlägt eine Skalierung von Sicherheitsstufen vor, mit deren Hilfe unterschiedliche Sicherheitsniveaus beim Betrieb von Schlüssel-Archiven (Key Recovery Centern) erreicht werden können. Mit steigender Sicherheitsstufe steigt der Widerstandswert des Schlüssel-Archivs.
Mit dieser Skala läßt sich ein Schlüssel-Archiv an unterschiedliche Sicherheitsanforderungen anpassen. Die jeweils aktuell angemessene Sicherheitsstufe muß im Falle der Realisierung anhand einer vollständigen Risikoanalyse festgelegt werden.
Tabelle 1 zeigt eine Auflistung der sieben hier verwendeten (Grund-)Sicherheitsstufen und die dabei jeweils erforderlichen Maßnahmen, die nachfolgend genauer erläutert werden. Bei der Darstellung der einzelnen Stufen werden jeweils immer nur die zusätzlichen Maßnahmen (bzw. die Veränderungen) zur vorhergehenden Stufe genannt.
Weiterhin läßt sich das Sicherheitsniveau der Stufen 4 bis 6 durch weitere Maßnahmen "aufwerten". Diese zusätzlichen Maßnahmen sind in Tabelle 2 dargestellt und werden anschließend erläutert.

Stufe	Maßnahme	
0	Klassische Informationssicherheitsmaßnahmen (PW, Firewalls, ...). **Unverschlüsselte** Übertragung und Speicherung der Daten	
1	**Verschlüsselte** Übertragung und Speicherung der Daten in allen Netzen. **Einheitlicher** Schlüssel für alle Endanwender. Wechsel des Schlüssels nie oder nur sporadisch. Speicherung des Schlüssels beim Endanwender	
2	**Unterschiedliche** Schlüssel für die Endanwender	
3	Endanwender setzt **Sitzungsschlüssel** (session keys) ein. Speicherung der Schlüssel beim Endanwender.	
4	Speicherung der Schlüssel in einem **zentralen Schlüssel-Archiv**	
5	Mehrere **dezentrale Schlüssel-Archive**. Speicherung des **kompletten** Schlüssels in **einem** der Schlüssel-Archive	Schlüssel-Archiv enthält nur **Pointer** auf dezentral gespeicherte Schlüssel
6	**Aufteilung** des Schlüssels (**split keys**) in mehrere Teile und verteilte Speicherung	

Tabelle 1

In der **Stufe 0** werden alle Daten in allen Netzen **unverschlüsselt** übertragen und gespeichert. Es werden lediglich "klassische Informationssicherheitsmaßnahmen" angewendet (wie z.B. der Zugangsschutz durch Passwörter, das Absichern der internen Netze gegen das Eindringen von außen durch Firewalls, Sensibilisierung der End-Anwender für die Risiken der Informationsverarbeitung, etc.).
Die Daten auf dem Netz können einfach abgehört und verändert werden. Die Gesamtsicherheit hängt also vom Sicherheitsniveau der benutzen Netze ab.

In **Stufe 1** werden alle Daten in allen Netzen **verschlüsselt** übertragen und gespeichert. Zur Verschlüsselung wird ein **einheitlicher Schlüssel für alle End-Anwender** benutzt, der nie oder nur sporadisch gewechselt wird. Der End-Anwender speichert den Schlüssel bei sich nach eigenen (Sicherheits-)Vorstellungen. Der Schlüssel wird von einem Schlüssel-Generator generiert, gespeichert und verteilt. Er kann jederzeit erneut vom Generator bezogen oder dem Backup des Schlüssels entnommen werden.
Wird (einer) dieser Schlüssel kompromittiert, so lassen sich **alle** Daten von **allen** End-Anwendern, die mit diesem Schlüssel verschlüsselt wurden (evtl. auch zukünftige, falls nicht auffällt, daß der Schlüssel kompromittiert wurde und der Schlüssel nicht gewechselt wird), entschlüsseln. Ebenso kann jeder End-Anwender die Daten von allen anderen End-Anwendern entschlüsseln.

Bei **Stufe 2** wird von jedem End-Anwender ein **unterschiedlicher** Schlüssel benutzt, der aber ebenfalls nie oder nur sporadisch gewechselt wird.
Wird (einer) der Schlüssel eines End-Anwenders kompromittiert, so lassen sich alle Daten, die mit diesem Schlüssel verschlüsselt wurden (bzw. zukünftig verschlüsselt werden), entschlüsseln.

In der **Stufe 3** kommen **Sitzungsschlüssel** (session keys) zum Einsatz. D.h., jeder End-Anwender wechselt bei **jeder** Übertragung oder Speicherung den verwendeten Schlüssel. Die Schlüssel werden beim End-Anwender gespeichert.
Wird nun **einer** dieser Schlüssel kompromittiert, so läßt sich damit nur max. ein Dokument entschlüsseln. Wird jedoch der **Rechner** des End-Anwenders kompromittiert, so finden sich dort zu allen verschlüsselten Dokumenten die dafür verwendeten Schlüssel. Es lassen sich dann also **alle** dort gespeicherten Dokumente des End-Anwenders entschlüsseln.

In **Stufe 4** wird ein **zentrales Schlüssel-Archiv** (Key Recovery Center) für die Verwaltung **aller** Sitzungsschlüssel von **allen** End-Anwendern eingesetzt. Die Schlüssel werden **nicht** mehr beim End-Anwender gespeichert. Wird einer der Schlüssel erneut benötigt, so können ihn **Berechtigte** vom Schlüssel-Archiv beziehen.
Wird das zentrale Schlüssel-Archiv kompromittiert, so fallen dem Angreifer **alle** Schlüssel in die Hände und er kann **alle** Dokumente von **allen** End-Anwendern entschlüsseln, wenn er auf die verschlüsselten Dokumente zugreifen kann.

Mit **Stufe 5** teilt sich weitere Erhöhung des Sicherheitsniveaus in zwei Strategien auf:
Zum einen wird ein höheres Niveau als in Stufe 4 dadurch erreicht, daß im Schlüssel-Archiv nicht die eigentlichen Schlüssel, sondern nur **Pointer** auf die Schlüssel, die dezentral (beim End-Anwender) gespeichert sind, gespeichert werden. Die Sicherheit ist höher, da die Schlüssel dezentral gespeichert sind und jeder End-Anwender weitere **informationswert-abhängige** Sicherheitsmaßnahmen auf seinem Rechner ergreifen kann, die ein Angreifer zusätzlich überwinden muß, nachdem er in das Schlüssel-Archiv eingedrungen ist.
Zum anderen kann ein höheres Sicherheitsniveau als in Stufe 4 erreicht werden, indem mehrere **dezentrale Schlüssel-Archive** eingesetzt werden. Jeder Schlüssel wird **komplett** in **einem** der Schlüssel-Archive gespeichert. Ein Angreifer muß also wissen, in welchem der Schlüssel-Archive der gesuchte Schlüssel gespeichert ist oder er muß in mehrere der Schlüssel-Archive eindringen, bis er den gesuchten Schlüssel gefunden hat.

In **Stufe 6** schließlich wird das Sicherheitsniveau dadurch noch weiter erhöht, daß jeder Schlüssel in mehrere Teile (max. entsprechend der Anzahl der eingesetzten Schlüssel-Archive) geteilt wird (**split keys**) und diese Teile zur Speicherung auf mehrere (alle) Schlüssel-Archive verteilt werden.
Der Angreifer muß also herausfinden, welche Schlüssel-Archive Teile des von ihm gesuchten Schlüssels enthalten und in diese (oder alle) eindringen. Weiterhin muß es ihm gelingen, die Schlüsselteile in der richtigen Weise wieder zusammenzusetzen.

Wie in der Einleitung schon angesprochen, lassen sich die Stufen 4 bis 6 durch die zusätzliche Anwendung der ersten bzw. beider der in Tabelle 2 aufgelisteten Maßnahmen weiter "aufwerten".

Aufwertung	Maßnahme
+1	**Verschlüsselung** der in den Schlüssel-Archiven abgelegten Daten
+2	Speicherung der privaten Schlüssel der Schlüssel-Archive in einem **Master Schlüssel-Archiv**

Tabelle 2

Eine **Aufwertung** der Sicherheitsniveaus 4 bis 6 um **eine Stufe** kann dadurch erreicht werden, daß die Daten (Schlüssel bzw. -Teile oder -Pointer) in dem/den Schlüssel-Archiv(en) mit dem **öfftenlichen Schlüssel** (public key) des jeweiligen Schlüssel-Archivs **verschlüsselt gespeichert** werden.
Nur wenn der **private Schlüssel** (private key) des Schlüssel-Archivs kompromittiert wird, können alle im Schlüssel-Archiv gespeicherten Daten entschlüsselt gelesen werden.

Eine Aufwertung um eine **weitere Stufe** wird dadurch erreicht, daß die privaten Schlüssel der einzelnen Schlüssel-Archive (bzw. des Schlüssel-Archivs), die zum Entschlüsseln der in den Schlüssel-Archiven gespeicherten Daten (Schlüssel bzw. -Teile oder -Pointer) benötigt werden, nicht im Schlüssel-Archiv selbst, sondern in einem weiteren - extra abgesicherten - **Master Schlüssel-Archiv** (Master Key Recovery Center) abgelegt werden.
Ein Angreifer muß nun zusätzlich in dieses Master Schlüssel-Archiv eindringen und sich die (den) privaten Schlüssel besorgen, um die in den Schlüssel-Archiven gespeicherten Daten entschlüsseln zu können.

Eine weitere (theoretische) Sicherheitsmaßnahme ist das Prinzip der "**Unvollständigen Hinterlegung**" (partial escrowing).
Dabei werden die Schlüssel nur unvollständig hinterlegt. Der fehlende Teil wird bei der Wiederherstellung eines Schlüssels durch eine "brute force attack" bestimmt.
Allerdings ist der Aufwand zur Wiederherstellung eines Schlüssels für den Berechtigten und einen Angreifer gleich hoch, so daß die Erhöhung des Sicherheitsniveaus durch diese Hinterlegungsart einem unangemessen hohen Aufwand gegenübersteht.

Quellen:

- Key Recovery Center, Vertrauenswürdige Schlüssel-Archive mit skalierbarer Sicherheit, Projektbericht 1/98 von Prof. Dr. Hartmut Pohl und Dipl.-Ing. (FH) Dietrich Cerny
- Inhalte der Vorlesungen und Diskussionen in den Übungsstunden zu dem von Prof. Dr. Hartmut Pohl geleiteten Projekt SECFORS im SS 1998 an der Fachhochschule Rhein-Sieg

---

Thomas Hungenberg