Moderne Verfahren der Kryptographie
Grundlegene Protokolle

8. November 2001

Inhaltsverzeichnis

1 Allgemeines **3**

2 Paßwortverfahren **3**

3 Wechselcodeverfahren **3**

4 Challenge-and-Response **4**

5 Shamirs No-Key-Protokoll **4**

6 Diffie-Hellman-Schlüsselvereinbarung **5**

7 Das ElGamal-Verschlüsselungsverfahren **5**

8 Das ElGamal-Signaturverfahren **6**

1 Allgemeines

Protokolle sind Regeln, nach denen die sichere Kommunikation zwischen mehreren Teilnehmern abläuft. Protokolle werden fr komlpexere Interaktionen, als dem einfachen Senden verschlüsselter bzw. signierter Nachrichten benötigt. Protokolle müssen zwei Bedingungen erfllen:

- **Durchführbarkeit:**Das Protokoll liefert immer bzw. mit beliebig hoher Wahrscheinlichkeit das gewünschte Ergebnis.
- **Korrektheit:**Ein erfolgreicher Betrugsversuch ist mit beliebig hoher Wahrscheinlichkeit auszuschließen.

2 Paßwortverfahren

Ein Teilnehmer authentisiert sich gegenüber einer Zentrale mittels seiner Identität und einem individuellen Geheinmnis, welches nur ihm und der Zentrale bekannt ist. Dieses Verfahren ist durchführbar, da jeder Teilnehmer sein Paßwort kennt. Es Ist korrekt, solange nur die Zentrale und der Teilnehmer das individuelle Geiheimnis kennen, denn dann kann ein Betrüger das Paßwort nur raten. Die Wahrscheinlichkeit, daß er dies richtig rät, ist bei einem gut gewählten Paßwort verschwindend gering. Hier liegt aber auch schon eine von mehreren Schwächen dieses Verfahren, welche nur durch zusätzliche Maßnahmen zu beheben sind. Paßwörter sollten möglichst eine unsinnige Kombination von Zeichen sein, da sonst ein Betrüger durch ausprobieren eines Wörterbuchs das Paßwort finden könnte. Weiterhin kann sich ein Betrüger Zugriff auf Paßwörter einer Zentrale verschaffen, indem er sich Zugang zu der Datei, in der die Paßwörter gespeichert sind, verschafft. Dem Kann Abhilfe geschaffen werden, indem die Paßwörter verschlüsselt abgespeichert werden. Versucht nun ein Teilnehmer sich zu authentisieren, so wird sein angebliches Geheimnis mit der gleichen Funktion verschlüsselt und dieses verschlüsselte Paßwort mit dem verschlüsselten in der Datei der Zentrale verglichen. Ein weiteres Problem ist die offene Übertragung des Paßwortes, wird dies einmal abgehört kann es vom Dritten immer verwendet werden, Daher sollte die Lebensdauer eines Paßwortes sehr kurz gewählt werden.

3 Wechselcodeverfahren

Eine Schwäche des Paßwortverfahren liegt darin, daß nicht das Geheimnis statisch ist, sondern auch die gesendete Nachricht zur Authentikation(die Identität) immer gleich sind. Mithilfe des Wechselcodeverfahren kann dem Abhilfe geschaffen werden. Bei diesem Verfahren berechnet der A aus seinem statischen Geheimnis und einem anderen veränderlichem Wert einen Authentikationscode und sendet diesen mit seiner Identität an B. Realisiert werden kann dies folgendermaßen: beide Parteien kennen eine Verschlßselungsfunktion f, einen geheimen Schlüssel k und einen Anfagnszählerstand z_0. Will sich nun A gegenüber B authentisieren, berechnet A $c_i = f(k, z+i)$ und sendet c_i an B. B überprüft nun, ob $f(k, z+i) = c_i$ ist. Dieses Verfahren ist durchführebar, da A und B den gleichen

Schlüssel und den gleichen Zählerstand kennen. Dieses Verfahren ist korrekt, da ohne Kenntnis des geheimen Schlüssels k die Wahrscheinlichkeit den Wert c_i zu bilden nahezu Null ist. Ein Angriff auf dieses Verfahren beruht darin, sich A gegenüber als B auszugeben, und so den nächsten Wert c_i zu erhalten. Mit diesem Wert kann dann der Dritte B gegenüber die Rolle von A spielen. Dem kann dadurch begegnet werden, indem man eine solche Authentikationsnachricht sehr kurzlebig werden läßt.

4 Challenge-and-Response

Der eben beschrieben Angriff auf das Wechselcodeverfahren beruht darauf, daß man die Authentikationsnachrichten vorproduziert. Bei Challange-and-Response-Verfahren ist dies nicht möglich. Bei diesem Verfahren stellt B A eine unvorhersagbare Frage, auf die nur A eine Antwort wissen kann. A athentisiert sich dann mit der richtigen Antwort. Bei diesem Verfahren handelt es sich um ein biderektionales, da Nachrichten nicht mehr nur von A zu B, sondern auch in umgekehrter Richtung fließen. In der technischen Anwendung wird wie folgt vorgegangen: beide Teilnehmer kennen eine Einwegfunktion f_k, welche von einem Schlüssel k abhängig ist(z.b. $f_k(x) = f(k||x)$, will heißen k konkateniert mit x). B sendet eine Zufallszahl $RAND$ an A. A bildet $RES = f_k(RAND)$ und sendet RES an B. B überprüft nun, ob $f_k(RAND) = RES$. Dieses Verfahren ist trivialerweiser durchfhrbar, da beide Teilnehmer f_k und k kennen. Dieses Protokoll ist korrekt, da k geheim ist.

5 Shamirs No-Key-Protokoll

Wie der Name schon sagt, beruht dieses Verfahren darauf, daß beide Teilnehmer keinen gemeinsamen Schlüssel k benutzen. Bildlich kann man sich das so vorstellen, daß A eine geheime Nachricht s in eine Kiste legt und mit einem Schloß die Kiste verschließt, dann sendet er die Kiste an B. Dieser Hngt ebenfalls ein Schloß vor die Kiste und sendet diese an A zurück. A nimmt dann sein Schloß ab und sendet die Kiste wieder an B zurück. Dann kann B sein Schloß wieder abnehmen und die geheime Nachricht s der Kiste entnehmen. Mathematisch realisiert werden kann dieses Prinzip mit einer diskreten Exponentialfunktion. Dazu einigen sich beide Parteien auf eine große Primzahl p. A und B wählen dann jeweils ein a und a' bzw. b und b' für die gilt $aa' \equiv 1(modp-1)$, das gleiche für B. Es gilt $aa'bb' \equiv 1(modp-1)$. a entspricht dem Schließen des Schlosses der Kiste und a' dem Aufschließen des Schlosses durch A. Analog dazu gilt das gleiche für b und b' für B. Es gilt dann:

$$s = s^{aa'} modp \text{ und } s = s^{bb'} modp$$

A bildet nun $x = s^a modp$ und sendet x an B. B bildet $y = x^a modp$ und sendet y an A zurück. A berechnet jetzt $z = y^{a'} modp$ und sendet z an B. B berechnet $z^{b'} modp$. Dieses Verfahren ist durchführbar, da:

$$\begin{aligned} z^{b'} mod p &= (y^{a'})^{b'} mod p = y^{a'b'} mod p = (x^b)^{a'b'} mod p = x^{ba'b'} mod p \\ &= (s^a)^{ba'b'} mod p = s^{aba'b'} mod p = s^{aa'bb'} mod p = (s^{aa'})^{bb'} mod p = s \end{aligned}$$

Das Verfahren ist so sicher wie das Problem des diskreten Logarithmus, doch diesen zu berechnen ist mit heutigen Verfahren viel zu aufwendig. Nachteile sind, daß eine Authentisierung bzw. Identifiezierung zusätzliche Maßnahmen benötigte. Außerdem gehen 3 korrospondierende kryptografische Nachrichten über die Leitung, gut für einen Angreifer.

6 Diffie-Hellman-Schlüsselvereinbarung

Das Problem der klassischen Kryptographie besteht darin, daß beide Parteien einen gemeinsamen geheimen Schlüssel k benötigen um gesichert miteinander kommunizieren zu können. Der Schlüssel muß also kryptographisch ungesichert ausgetauscht werden. Es müsste also eine Möglichkeit geben sich offen zu unterhalten, am Ende dann ein gemeinsames Geheimnis zu kennen, auf das aufmerksam lauschende Dritte nicht kommen. Eine Lösung dafür fanden Diffie und Hellman in den 70er Jahren. Diesem Protokoll liegt folgende diskrete Exponentialfunktion zugrunde:

$$\alpha = g^a mod p$$

Beide Teilnehmer einigen sich auf ein g und eine Primzahl p. Dann wählt A ein persönliches a und berechnet $\alpha = g^a mod p$, analog dazu berechnet B $\beta = g^b mod p$. Dann senden sich A und B α bzw. β zu. Nun berechnet A $\beta^a mod p$ und B $\alpha^b mod p$. Dieses Verfahren ist durchführbar, da A und B den gleichen Schlüssel besitzen, da gilt:

$$\beta^a mod p = (g^b)^a mod p = g^{ba} mod p = g^{ab} mod p = (g^a)^b mod p = \alpha^b mod p$$

Die Diffie-Hellman-Schlüsselvereinbarung ist korrekt, da der gemeinsame Wert, der errechnet wurde geheim ist. Ein Dritter erhlt zwar aus dem Gespräch β und könnte versuchen $\beta^a mod p$ zu berechnen, müsste dafür aber a kennen, dies kann nur mittels diskretem Logarithmus von α zur Basis g geschehen, welches mit heutigen Verfahren nahezu unmöglich ist.

7 Das ElGamal-Verschlüsselungsverfahren

Das ElGamal-Verschlüsselungsverfahren ist eine Variante der Diffie-Hellman-Vereinbarung. Man benötigt wieder eine Zahl g und eine Primzahl p, welche öffentlich sind. Jeder Teilnehmer T wählt sich einen persönlichen Schlüssel t und veröffentlicht $\tau = g^t mod p$ als seinen öffentlichen Schlüssel. Jetzt kann ein Teilnehmer A eine verschlüsselte Nachricht wie folgt an T schicken: A wählt eine zufällige Zahl a und berechnet $\alpha = g^a mod p$ und $k = \tau^a mod p$. Dann verschlüsselt er einen Nachricht m in $c = f(k, m)$ und sendet α und c an T. T berechnet dann $k = \alpha^t mod p = (g^a)^t mod p = (g^t)^a mod p = \tau^a mod p$ und mit k $m = f^{-1}(k, c)$.

Dieses Verfahren ist durchführbar, wie schon gezeigt. Das Verfahren ist korrekt, da k nur mit hilfe von a bzw. t berechnet werden kann, dem wieder das Problem des diskreten Logarithmus von τ zur Basis g zugrunde liegt.

8 Das ElGamal-Signaturverfahren

Zur Erzeugung und Verifikation einer digitalen Unterschrift wird wie beim ElGamal-Verschlüsselungsverfahren ein privater Schlüssel t und ein öffentlicher Schlüssel $\tau = g^t mod p$ benutzt. Um eine Nachricht m zu signieren bildet ein Teilnehmer T eine zu p-1 teilerfremde zufällige Zahl und berechnet $k = g^r mod p$. Dann sucht T eine Lösung der Kongruenz $tk + rs \equiv m(mod p - 1)$, indem er z.b. mit Hilfe des erweiterten euklidischen Algorithmus das multiplikative Inverse r^{-1} zu r modulo $p-1$ berechnet und dann $s = ((m - tk)r^{-1} mod p - 1$ bildet. Die digitale Unterschrift von m ist das Paar k und s. Der Empfänger kann diese Signatur von m verifizieren, indem er überprüft ob $g^m mod p = \tau^k k^s mod p$. Dieses Verfahren ist durchführbar, da nach dem Satz von Fermat gilt $g^m \equiv g^{tk+rs} \equiv \tau^k k^s (mod p)$. Das ElGamal-Signaturverfahren ist korrekt, da bis heute kein effizienter Angriff auf dieses Verfahren gefunden wurde.