



Falko Dressler      Tobias Limmer      Thomas Schneider

## Netzwerksicherheit WS 2007/08

### 8. Übungsblatt

8.1.2008

#### Aufgabenstellung:

In dieser Aufgabe sollen Sie einen Client (*mixclient*) und einen Knoten (*mixnode*) für ein Mix Net nach Chaum programmieren. In der nächsten Übungsstunde werden die implementierten Mixes der Übungsgruppen dann gemeinsam im CIP Pool getestet.

- Die Kommunikation erfolgt über TCP/IP, Port 4444.
- Der *mixclient* nimmt eine wie in der Übung besprochene S/MIME codierte Nachricht entgegen und sendet sie an den im "To: "-Feld angegebenen ersten *mixnode* (s. Beispiel).
- Der *mixnode* entschlüsselt die empfangene Nachricht mit dem *groupkey.pem* ihrer Übungsgruppe und dem zugehörigen *groupcert.pem*. Falls die entschlüsselte Nachricht mit einem "To: " beginnt, wird sie an den dort angegebenen nächsten *mixnode* weitergeleitet. Andernfalls wird die digitale Signatur des Absenders geprüft (mit NetSecCACert (*rootcert.pem*) als Root Zertifikat) und der Absender und die empfangene Nachricht ausgegeben (s. Beispiel).

#### Beispiel:

Codieren einer Nachricht *m.txt*, die von *A* an *B* via *M1* und *M2* geschickt werden soll. Zum Testen, verwenden Sie ihr eigenes *groupcert.pem* für alle Zertifikate (*\*cert.pem*). In der nächsten Übungsstunde können dann die Zertifikate der anderen Übungsgruppen entsprechend eingesetzt werden.

```
openssl smime -sign -in m.txt \  
  -inkey Akey.pem -signer Acert.pem | \  
openssl smime -encrypt -aes128 \  
  -to B_hostname Bcert.pem | \  
openssl smime -encrypt -aes128 \  
  -to M2_hostname M2cert.pem | \  
openssl smime -encrypt -aes128 \  
  -to M1_hostname M1cert.pem \  
> mix_message.txt
```

Absender der Nachricht:  
A> ./mixclient < mix\_message.txt  
Delivering message to 'M1\_hostname'

Mix M1:  
M1> ./mixnode  
Enter PEM pass phrase:  
Listening for incoming connections.  
---  
Starting to process message from IP\_A...  
Decrypting message...  
Delivering message to 'HOSTNAME\_M2'  
Message processed.

...

Empfänger der Nachricht:  
B> ./mixnode  
Enter PEM pass phrase:  
Listening for incoming connections.  
---  
Starting to process message from IP\_M3...  
Decrypting message...  
Verifying signature...  
Message from /C=DE/ST=Bavaria/L=Erlangen/O=FAU  
/OU=CS 7 / NetSec/CN=NetSec CA/emailAddress=...  
---  
Message Text...  
---  
Message processed.

#### Technische Hinweise:

- Die Aufgaben sind in C/C++ mit OpenSSL oder Java (no support !) zu erstellen.
- Der Code muss auf dem Betriebssystem Debian/Linux im CIP-Pool der Informatik mit der dort installierten Version des GNU C/C++- oder Java-Compilers kompilieren und lauffähig sein.
- Es ist ein Makefile oder ein ausführbares Skript zu bereitzustellen, welches temporäre Daten löschen (Target „clean“) und eine Binärdatei (Target „all“) erstellen kann.
- Es ist eine Dokumentation (*README.TXT*) im ASCII-Format zu erstellen, welche einen typischen Programmstart dokumentiert und über Besonderheiten des Programms berichtet.

Fragen und Abgabe der Lösungen bis Montag, den 14.1.2008 als Archiv im Format .tar.(gz|bz2) oder .zip per Mail an tobias.limmer@informatik.uni-erlangen.de und thomas.schneider@informatik.stud.uni-erlangen.de.