Labreport #6

Patrick Eickhoff, Alexander Timmermann

Aufgabe 1. Absicherung des TCP-Chats mit SSL

Um unseren ursprünglichen TCP-Chat mit SSL zu sichern, bedienen wir uns des *javax.net.ssl* Packetes. Dieses beinhaltet `SSLSockets` und `SSLServerSockets`, die wir benutzen um, eine sichere Verbindung aufzubauen. Die Sockets werden mittels `SSLSocketFactory` erstellt. Alle SSLSockets greifen können auf einen *keyStore* und einen *trustStore* zugreifen. Diese Java-spezifischen Datenbanken beinhalten Zertifikate und private Schlüssel für den Aufbau der SSL-Verbindung. Der *keyStore* beinhaltet einen privaten Schlüssel und die Zertifikate, die beim SSL-Handshake mitgeschickt werden. Im *trustStore* sind, dann die Zertifikate gespeichert, denen vertraut wird (trusted Certificate). Den *keyStore* des Clienten, haben wir mit *keytool* wie folgt initiiert:

```
$ keytool -keystore clienttest.keystore -keyalg RSA -genkey -alias client
```

Dieser Befehl erzeugt ein neues Schlüsselpaar mittels RSA, sowie ein Zertifikat mit dem Alias "client". Beim Erzeugen des Zertifikats fragt uns *keytool* nach den üblichen Parametern, wie z.B. Name, Länderkürzel, Organisation, etc. Für unsere Anwendung ist nur wichtig, dass der Client einen Namen in sein Zertifikat einträgt. Für den Server erstellen wir respektive einen *keyStore*:

```
$ keytool -keystore servertest.keystore -keyalg RSA -genkey -alias server
```

Beim SSL-Handshake werden die Zertifikate aus den Keystores dem Verbindungspartner präsentiert. Also präsentiert z.B. der Client sein selbstsigniertes Zertifikat aus *clienttest.keystore* dem Server. Der Server präsentiert wiederum sein Zertifikat dem Client. Die präsentierten Zertifikate werden dann gegen die Zertifikate im *trustStore* abgeglichen. Also müsssen wir die Zertifikate jeweils in die *trustStores* des Verbindungspartners importieren:

```
$ keytool -importkeystore -srckeystore servertest.keystore -destkeystore clienttest.truststore
$ keytool -importkeystore -srckeystore clienttest.keystore -destkeystore servertest.truststore
```

Jetzt akzeptieren Server und Client die präsentierten Zertifikate und eine sichere SSL-Verbindung wird aufgebaut.

Nun wollten wir unsere Nutzername-Password-Authentifikation durch die Zertifikatsauthentifikation der SSL-Verbindung ersetzen. Wie zuvor erwähnt, muss jedes Clienten-Zertifikat mindestens einen Namen enthalten. So können wir ein vertrautes Zertifikat genau einem Nutzer zuordnen. Der Anzeige-Name im Chat ist dann dem Namen im Zertifikat identisch.

Bei der vorherigen Implementation unseres Chats konnte man sich einfach mittels *netcat* verbinden. Deshalb war kein Java-Client von Nöten. Da *netcat* aber kein SSL-Protokol unterstützt, benötigt man zur Kommunikation nun einen Java-Chat-Clienten. Für die Implementation siehe Anhang A.

Aufgabe 2. CAs und Webserver-Zertifikate

2. Um ein selbstsigniertes Zertifikat zu erzeugen, sind im wesentlichen drei OpenSSL-Befehle notwendig:

```
$ openssl genrsa -out server.key 2048
$ openssl req -new -key server.key -out server.csr
$ openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

Mit dem ersten Befehl erzeugen wir einen neuen, 2048-bit langen privaten Schlüssel. Wir erstellen dann mit dem zweiten Befehl die sog. *certificate signing request*, in der die Informationen enthalten sind, die das Zertifikat später umfassen soll. Diese werden interaktiv abgefragt. Als Common Name verwenden wir `vmsrv11.svslab`.

Im dritten Befehl verwenden wir schließlich den erstellten Private Key, um aus der CSR ein Zertifikat zu generieren, das 365 Tage gültig ist.

Um dieses Zertifikat für den Apache-Server einzusetzen, ersetzen wir in der Konfigurationsdatei die Pfade hinter `SSLCertificateFile` und `SSLCertificateKeyFile` mit den Pfaden zum Zertifikat und dem private key.

Dass selbst-signierte Zertifikate als unsicher angesehen werden liegt auf der Hand. Jeder kann sich ein Zertifikat erstellen, was bspw. für google.com gültig ist. Würde diesen Zertifikaten vertraut, ließe sich eine Man-in-the-Middle-Attacke zu google.com sehr leicht implementieren, da der User keinen Unterschied bemerkt, und ihm durch das Zertifikat weitere Sicherheit suggeriert wird.

Die Aufgabe einer CA ist es, diese Angaben zu validieren und im Zweifelsfall die Ausstellung eines Zertifikats zu verweigern. CAs sind deshalb Firmen oder Organisationen, denen vertraut wird, diese Macht nicht zu missbrauchen.

3. Um mit Hilfe von *mod_rewrite* eine Weiterleitung zu HTTPS zu realisieren, fügen wir folgende Optionen in die Apache-Config ein:[1]

```
1 RewriteEngine On
2 RewriteCond %{HTTPS} !=on
3 RewriteRule ^/?(.*) https://%{SERVER_NAME}/$1 [R,L]
```

Mit dem ersten Befehl wird die Bearbeitung der Rewrite-Regeln eingeschaltet. Danach wird geprüft, ob nicht bereits HTTPS verwendet wird, da damit die Weiterleitung hinfällig wird. Schließlich wird die Rewrite-Regel definiert, die dann weiterleitet. Die Optionen am Ende sind die Flags. `L` gibt an, dass die Regel die letzte ist, die ausgeführt wird. `R` spezifiziert, dass ein HTTP Redirect passieren soll.

Die Regel selbst ist ein regulärer Ausdruck, bei dem alles nach einem optionalen "/" matched und in die HTTPS-URL eingesetzt wird.

4. Über die verschlüsselte Verbindung können wir die Zugangsdaten selbstverständlich nicht mitlesen. Verwenden wir *sslstrip* als Proxy, so wird die Umleitung auf die verschlüsselte Verbindung verhindert und wir können die Zugangsdaten recht komfortabel im Log-File nachlesen.

[1] Quelle: `https://wiki.apache.org/httpd/RewriteHTTPToHTTPS`

Die Sicherheit der Weiterleitung ist damit maximal als "gut gemeinte" Maßnahme für Endanwender gedacht, taugt aber nicht, ernsthafte Angriffe abzuwehren. Hierzu sind weitere Maßnahmen nötig, wie beispielsweise HSTS.

HTTP Strict Transport Security (HSTS) ist ein in RFC 6797[2] beschriebener Standard, der einen solchen Angriff verhindern kann. Wird HSTS aktiviert, so können Seiten unter einer Domain, die HSTS setzt, nicht über eine unverschlüsselte Verbindung abgerufen weden. HSTS wird über einen Header aktiviert, der bei der Antwort mitgesendet wird und etwa so aussieht:

```
1 Strict-Transport-Security: max-age=15768000
```

Damit wird HSTS im Browser strikt forciert und lässt sich auch für den Endnutzer nicht wieder abschalten. Mit dem `max-age`-Parameter wird eine Art "Haltbarkeitsdatum" in Sekunden angegeben. 15768000 Sekunden entsprechen etwa einem halben Jahr, danach wird der Browser eine unverschlüsselte Verbindung prinzipiell wieder erlauben, wenn nicht erneut ein HSTS-Header mitgesendet wird.

Aufgabe 3. Unsichere selbstentwickelte Verschlüsselungsalgorithmen

1. Das Problem mit der BaziCrypt-Verschlüsselung ist, das die Paddingbytes (`0x00`) durch die XOR-Operation den Schlüssel direkt in den Ciphertext abbilden. Durch einfache Analyse der sich wiederholenden Bytes am Ende des Ciphertextes und ein paar Versuchen lässt sich sehr leicht der Schlüssel rekonstruieren. Mithilfe unseres Skripts B haben wir folgende Nachrichten entschlüsselt:

n01.txt.enc Hallo Peter. Endlich koennen wir geheim kommunizieren! Bis bald, Max

n02.txt.enc Hi Max! Super, Sicherheitsbewusstsein ist ja extrem wichtig! Schoene Gruesse, Peter.

n03.txt.enc Hi Peter, hast du einen Geheimtipp fuer ein gutes Buch fuer mich? Gruss, Max

2/3. Das PKCS7-Padding-Verfahren füllt die zu verschlüsselnde Nachricht nicht mehr mti Nullbytes, sondern mit Bytes die äquivalent zur Länge des Paddings sind.

Beispiel: Padding der Länge 6: `0x06 0x06 0x06 0x06 0x06 0x06`

Durch diese Methode lässt sich der Schlüssel nicht mehr einfach aus dem Ciphertext ablesen. PKCS7 unterstützt jedoch nur Blöcke bis zu 256-Byte und 256 mögliche Paddingbytes lassen sich in kurzer Zeit per Bruteforce durchprobieren [3]. Unser Skript (B) probiert einfach nur alle Paddingbytes von 0 bis 100 durch (100 da die Dateien nur 100 Byte groß sind) und versucht die Nachricht zu entschlüsseln. Dann suchen wir einfach die Entschlüsselung aus, die korrekt ist. Mithilfe dieses Skripts haben wir folgende Nachrichten entschlüsselt:

n04.txt.enc Hi Max, natuerlich: Kryptologie von A. Beutelspacher ist super. Gruss Peter

n05.txt.enc Hi Peter, worum geht es in dem Buch? Ciao, Max.

n06.txt.enc Hi Max, das ist ein super Buch, das viele Krypto-Themen abdeckt. Gruss Peter

[2] `https://tools.ietf.org/html/rfc6797`
[3] Quelle: `https://en.wikipedia.org/wiki/Padding_(cryptography)`

Aufgabe 4. EasyAES

Ein Meet-In-The-Middle-Angriff nutzt die Tatsache aus, dass wir sowohl Ciphertext als auch Plaintext besitzen[4]. Wir betreiben einen *Time-Space-Tradeoff* indem wir zuerst alle möglichen Schlüssel K1 erzeugen, dann den Plaintext mit jedem dieser Schlüssel verschlüsseln und diese Schlüssel-Cipher-Paare in einer Art Lookup-Table aufbewahren. Dann erzeugen wir Schlüssel K2 mit denen wir versuchen den Ciphertext zu dechiffrieren. Wenn wir jetzt den dechifrierten Ciphertext in unserer Lookup-Table finden, haben wir ein Schlüsselpaar K1,K2 gefunden, mit dem der Plaintext verschlüsselt wurde. Dadurch, dass wir die Lookup-Table besitzen, benötigen wir weniger Berechnungszeit im Austausch für einen höheren Speicherverbrauch. Mit Hilfe unseres Skripts (siehe Appendix C) haben wir folgende Schlüssel ermittelt:

Key 1: `00:00:00:f5:00:00:00:00:00:00:63:00:00:00:00:00`

Key 2: `00:00:00:00:77:00:00:00:b0:00:00:00:00:00:00:00`

Aufgabe 5. Bonus: Timing-Attacke

Disclaimer: Aufgrund der erhöhten Schwierigkeit im Vergleich zu den anderen Aufgaben, haben wir eng mit Gruppe 12 zusammengearbeitet. Diese Aufgabe ist daher deckungsgleich.

Unsere Timing-Attack ist im Anhang zu finden. Wir würden gerne an dieser Stelle einige Erkenntnisse auflisten. Zunächst haben wir die Object-File disassemblet. Dies ist sehr einfach mit `$ objdump -d password_compare.o`, oder etwas komplizierter, aber im Ergebnis übersichtlicher mit *radare2*.

Der Assembly können wir entnehmen, dass die Funktion keinen Boolean returnt, sondern einen Int. Obwohl auf dem Aufgabenblatt nicht eindeutig dargestellt war, welchen Returnwert die Funktion hat, wurde durch die gezeigte Java-Funktion Boolean impliziert. Bei einem korrekten Passwort wird 0 zurückgegeben, andernfalls -1. Dies ist ein wichtiges Detail, denn in C gelten alle Integer *ungleich* 0 als wahr, und nur 0 als falsch. Hat man also nur den Wiedergabe-Wert der Funktion z.B. in einer `if`-Klausel stehen, wird man sich wundern. Demnach ist die Aussage über *POSIX*-Erfüllung ebenfalls diskutabel.

Weiterhin ist der Assembly zu entnehmen, dass die Länge des Passworts gar nicht überprüft wird. Dafür gibt es gar nicht genügend Loops. Dies macht uns den Angriff recht einfach; wir nehmen einfach einen langen String, und justieren an einer Stelle die Zeichen so lange, bis wir eine eindeutige Spike in der Zeit sehen, und akzeptieren diesen Buchstaben dann als richtig. Sobald die Funktion 0 widergibt, sind wir durch.

Das Passwort lautet: `Licht-B()6eN`. Das Password lautet ebenfalls: `Licht-B()6eN1234lalalala`; tatsächlich wird jeder String, der mit `Licht-B()6eN` *beginnt*, und beliebig weitergeht, von der Funktion akzeptiert.

Unser Code ist in Appendix D zu finden. Zu beachten ist auch dass dem Compiler `-O0` übergeben wird, damit er nicht optimiert und somit die Zeiten verfälscht.

[4]Quelle: `http://www.crypto-it.net/eng/attacks/meet_in_the_middle.html`

Anhang A TCP-Chat

Listing 1: ChatServer.java

```
1  //SourceCode partially from:
2  // http://www.dreamincode.net/forums/topic/259777-a-simple-chat-program-with-
3  //    clientserver-gui-optional/
4  // http://www.oracle.com/technetwork/java/socket-140484.html
5  // http://www.java2s.com/Tutorial/Java/0490__Security/SSLServerSession.htm
6  package tcp_chat;
7
8  import java.io.IOException;
9  import java.util.LinkedList;
10 import java.util.List;
11
12 import javax.net.ssl.SSLServerSocketFactory;
13 import javax.net.ssl.SSLSocket;
14 import javax.net.ssl.SSLServerSocket;
15
16 import passwd_save_java.Useradmin;
17
18 public class ChatServer {
19
20         public static void main(String[] args) {
21                 System.setProperty("javax.net.ssl.trustStore", "/home/patrick/workspace2/project_netsec/src/tcp_chat/se
22                 System.setProperty("javax.net.ssl.keyStore", "/home/patrick/workspace2/project_netsec/src/tcp_chat/serv
23                 System.setProperty("javax.trustStorePassword", "123456");
24                 System.setProperty("javax.net.ssl.keyStorePassword", "123456");
25
26                 ChatServer chatserver = new ChatServer();
27                 chatserver.listenSocket();
28         }
29
30         private SSLServerSocketFactory sslf;
31         private SSLServerSocket server;
32         private List<ClientThread> connections;
33         private List<String> loggedInUsers;
34         private Useradmin useradmin;
35
36         public ChatServer() {
37                 this.sslf = (SSLServerSocketFactory) SSLServerSocketFactory.getDefault();
38                 this.connections = new LinkedList<ClientThread>();
39                 this.useradmin = new Useradmin();
40                 this.loggedInUsers = new LinkedList<String>();
41         }
42
43         public void listenSocket() {
44                 try {
45                         server = (SSLServerSocket) sslf.createServerSocket(4444);
```

```
46                      server.setNeedClientAuth(true);
47                      //server.setEnableSessionCreation(true);
48              } catch (IOException e) {
49                      System.out.println("Could␣not␣listen␣on␣port␣4444");
50                      System.exit(−1);
51              }
52              while (true) {
53                      try {
54                              ClientThread t = new ClientThread((SSLSocket)server.accept(),this);
55                              System.out.println("new␣Connection");
56                              t.start();
57                              connections.add(t);
58                      } catch (IOException e) {
59                              System.out.println("Accept␣failed:␣4444");
60                      }
61              }
62      }
63
64      protected void finalize() {
65              try {
66                      server.close();
67              } catch (IOException e) {
68                      System.out.println("Could␣not␣close␣socket");
69                      System.exit(−1);
70              }
71      }
72
73      public void notify(String message, int ID, String User) {
74              for (ClientThread t : connections) {
75                      if (t.ID != ID) {
76                              t.print(User + ":" + message);
77                      }
78              }
79      }
80
81      public void disconnect(int ID) {
82              for (ClientThread t : connections) {
83                      if (t.ID == ID) {
84                              loggedInUsers.remove(t.getUser());
85                              connections.remove(t);
86                              System.out.println("disconnected");
87                      }
88              }
89      }
90
91      public boolean authenticate(String username, char[] password) {
92              if (loggedInUsers.contains(username)) {
93                      return false;
```

```
94                  }
95                  if (useradmin.checkUser(username, password)) {
96                          loggedInUsers.add(username);
97                          return true;
98                  }
99                  return false;
100         }
101 }
```

Listing 2: ChatClient.java

```
1  /*
2          SourceCode partially from:
3          https://stackoverflow.com/questions/7872846/how-to-read-from-standard-input-
4                                  non-blocking
5  */
6  package tcp_chat;
7
8  import java.io.BufferedReader;
9  import java.io.InputStreamReader;
10 import java.io.PrintWriter;
11 import java.util.concurrent.BlockingQueue;
12 import java.util.concurrent.LinkedBlockingQueue;
13 import java.util.concurrent.TimeUnit;
14
15 import javax.net.SocketFactory;
16 import javax.net.ssl.SSLSocketFactory;
17 import javax.net.ssl.SSLSocket;
18
19 public class ChatClient {
20
21         private static final BlockingQueue<String> socketlines = new LinkedBlockingQueue<String>();
22         private static final BlockingQueue<String> systemlines = new LinkedBlockingQueue<String>();
23
24   public static void main(String[] args) throws Exception {
25           BufferedReader in = new BufferedReader(new InputStreamReader(System.in));
26           System.setProperty("javax.net.ssl.trustStore", "/home/patrick/workspace2/project_netsec/src/tcp_chat/clienttest.
27           System.setProperty("javax.net.ssl.keyStore", "/home/patrick/workspace2/project_netsec/src/tcp_chat/clienttest.k
28           System.setProperty("javax.trustStorePassword", "123456");
29           System.setProperty("javax.net.ssl.keyStorePassword", "123456");
30
31     SocketFactory sf = SSLSocketFactory.getDefault();
32     SSLSocket s = (SSLSocket) sf.createSocket("localhost", 4444);
33
34     BufferedReader sin = new BufferedReader(new InputStreamReader(s.getInputStream()));
35     PrintWriter sout = new PrintWriter(s.getOutputStream(),true);
36
37     Thread socketReaderThread = null;
38     socketReaderThread = new Thread(new Runnable() {
```

```
39          @Override
40                  public void run() {
41                          try {
42                                  while (!Thread.interrupted()) {
43                                          String line = sin.readLine();
44                                          socketlines.add(line);
45                                  }
46                          } catch (Exception e) {
47                                  // TODO: handle exception
48                          }
49                  }
50      });
51      socketReaderThread.setDaemon(true);
52      socketReaderThread.start();
53
54      Thread systemReaderThread = null;
55      systemReaderThread = new Thread(new Runnable() {
56          @Override
57                  public void run() {
58                          try {
59                                  while (!Thread.interrupted()) {
60                                          String line = in.readLine();
61                                          systemlines.add(line);
62                                  }
63                          } catch (Exception e) {
64                                  // TODO: handle exception
65                          }
66                  }
67      });
68      systemReaderThread.setDaemon(true);
69      systemReaderThread.start();
70
71      String line;
72      while (!s.isClosed()) {
73          if ((line = socketlines.poll(10L, TimeUnit.MILLISECONDS))!= null){
74                  System.out.println(line);
75          }
76          if ((line = systemlines.poll(10L, TimeUnit.MILLISECONDS))!= null){
77                  sout.println(line);
78                  if (line.equals("quit")) {
79                          s.close();
80                  }
81          }
82      }
83      socketReaderThread.interrupt();
84      systemReaderThread.interrupt();
85    }
86  }
```

Listing 3: ClientThread.java

```
1  //SourceCode partially from:
2  //http://www.dreamincode.net/forums/topic/259777-a-
3  //   simple-chat-program-with-clientserver-gui-optional/
4  //       http://www.oracle.com/technetwork/java/socket-140484.html
5
6  package tcp_chat;
7
8  import java.io.BufferedReader;
9  import java.io.IOException;
10 import java.io.InputStreamReader;
11 import java.io.PrintWriter;
12 import java.security.cert.Certificate;
13 import java.security.cert.X509Certificate;
14 import java.util.regex.Matcher;
15 import java.util.regex.Pattern;
16
17 import javax.net.ssl.SSLHandshakeException;
18 import javax.net.ssl.SSLSocket;
19
20 class ClientThread extends Thread implements Runnable {
21         private SSLSocket client;
22         private ChatServer observer;
23         public final int ID;
24         private String User;
25
26         ClientThread(SSLSocket client, ChatServer observer) {
27                 this.client = client;
28                 ID = this.hashCode();
29                 this.observer = observer;
30                 User = "";
31         }
32
33         public void run() {
34                 String line;
35                 BufferedReader in = null;
36                 try {
37                         PrintWriter out = new PrintWriter(client.getOutputStream(), true);
38                         in = new BufferedReader(new InputStreamReader(
39                                         client.getInputStream()));
40                         Certificate[] certs = client.getSession().getPeerCertificates();
41                         for (Certificate cert : certs) {
42                                 X509Certificate xcert = (X509Certificate)cert;
43                                 String cert_name = xcert.getSubjectDN().getName();
44                                 System.out.println(cert_name);
45
46                                 Pattern name = Pattern.compile("CN=((?:[\\pL\\p{Nd}_]{1,20}\\s*)*),.*");
47
```

```
48                              Matcher mname = name.matcher(cert_name);
49                              if (mname.matches()) {
50                                      User=mname.group(1);
51                              }
52                      }
53              }
54              catch (SSLHandshakeException e) {
55                              System.err.println("SSLHandshake failed");
56                              this.interrupt();
57              }
58               catch (IOException e) {
59                      System.err.println("in or out failed");
60                      this.interrupt();
61              }
62
63              while (!this.interrupted()) {
64                      try {
65                              line = in.readLine();
66                              if (line.equals("quit")) {
67                                      observer.disconnect(ID);
68                                      client.close();
69                                      client = null;
70                                      return;
71                              }
72                              observer.notify(line, ID, User);
73                      } catch (IOException e) {
74                              System.err.println("Read failed");
75                              this.interrupt();
76                      }
77              }
78      }
79
80      public synchronized void print(String message) {
81              try {
82                      PrintWriter out = null;
83                      out = new PrintWriter(client.getOutputStream(), true);
84                      out.println(message);
85              } catch (IOException e) {
86                      System.err.println("out failed");
87              }
88      }
89
90      public String getUser() {
91              return User;
92      }
93 }
```

Anhang B Decrypt

Listing 4: bazi_decrypt.py

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
# First Argument: File-Destination
# Second Argument: Tolerance Level

import sys


def translateMessage(key, msg):
    translated = [] # stores the encrypted/decrypted message string

    keyIndex = 0
    for c in msg: # loop through each character in message
        num = ord(c)
        num = num ^ ord(key[keyIndex]) # add if encrypting
        translated.append(chr(num))
        keyIndex += 1 # move to the next letter in the key
        if keyIndex == len(key):
            keyIndex = 0
    return ''.join(translated)

key = []
message = []
tolerance = int(sys.argv[2])

f = open(sys.argv[1], "rb")
byte = f.read(1)
while byte != "":
    message.append(byte)
    byte = f.read(1)
print(message)
print(len(message))

i = 1
while not key[-tolerance:] == message[len(message)-len(key)-tolerance:len(message)-len(key)]:
    key.insert(0,message[-i])
    i+=1
    print(key)

f.close()
decrypted = translateMessage(key, message)
print(decrypted)
```

Listing 5: advazi_decrypt.py

```python
#!/usr/bin/env python
# -*- coding: utf-8 -*-
# First Argument: File-Destination
# Second Argument: Tolerance-Level

import sys

def translateMessage(key, msg):
    translated = []

    keyIndex = 0
    for c in msg:
        num = ord(c)
        num = num ^ ord(key[keyIndex])
        translated.append(chr(num))
        keyIndex += 1
        if keyIndex == len(key):
            keyIndex = 0
    return ''.join(translated)

message = []
tolerance = int(sys.argv[2]) #The Amount of Chars that have to loop in the message to accept as key

f = open(sys.argv[1], "rb")
byte = f.read(1)
while byte != "":
    message.append(byte)
    byte = f.read(1)
print(message)
print(len(message))

for padding_length in range(100):
    i = 1
    key = []
    while not key[-tolerance:] == message[len(message)-len(key)-tolerance:len(message)-len(key)]:
        key.insert(0,message[-i])
        i+=1
    key = map(lambda x: chr(padding_length ^ ord(x)), key)
    f.close()
    decrypted = translateMessage(key, message)
    words = decrypted.split(" ")
    print(decrypted)
```

Anhang C EasyAES

Listing 6: easyAES_mitm.py

```
from Crypto.Cipher import AES

lookup_table = dict()
plaintext = "Verschluesselung"
ciphertext = "\xbe\x39\x3d\x39\xca\x4e\x18\xf4\x1f\xa9\xd8\x8a\x9d\x47\xa5\x74"
f = None
key1 = ""
key2 = ""

for byte1_position in range(1,16):
    for byte2_position in range(byte1_position):
        for byte1 in range(256):
            for byte2 in range(256):
                key = [chr(0)] * 16
                key.pop(-byte1_position-1)
                key.insert(-byte1_position,chr(byte1))
                key.pop(-byte2_position-1)
                key.insert(-byte2_position,chr(byte2))
                key = ''.join(key)
                aes = AES.new(key)
                lookup_table[aes.encrypt(plaintext)] = key

f = open("lookup_table", "w")
for key, value in lookup_table.iteritems():
    f.write(key + ":" + value + "\n")
f.close()

for byte1_position in range(1,16):
    for byte2_position in range(byte1_position):
        for byte1 in range(256):
            for byte2 in range(256):
                key = [chr(0)] * 16
                key.pop(-byte1_position-1)
                key.insert(-byte1_position,chr(byte1))
                key.pop(-byte2_position-1)
                key.insert(-byte2_position,chr(byte2))
                key = ''.join(key)
                aes = AES.new(key)

                if aes.decrypt(ciphertext) in lookup_table:
                    key1 = lookup_table[aes.decrypt(ciphertext)]
                    key2 = key
                    break

print("Key1: " + ":".join("{:02x}".format(ord(c)) for c in key1) + " Key2: "
        + ":".join("{:02x}".format(ord(c)) for c in key2))
```

Anhang D Timing-Attack

Listing 7: timing.h

```
1  #pragma once
2
3  #include <stdbool.h>
4  #include <time.h>
5  #include <stdint.h>
6
7  extern int password_compare(const char * password);
8  size_t time_max(clock_t * arr, size_t len);
```

Listing 8: timing.c

```
1  #include <stdio.h>
2  #include <assert.h>
3  #include <stdlib.h>
4  #include <string.h>
5  #include <stdbool.h>
6  #include "timing.h"
7
8  #define LENGTH 20
9
10 const char * symbols = "abcdefghijklmnopqrstuvwxyz"
11                         "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
12                         "0123456789"
13                         "!@#$%^&*()-_=+[]{}|/?.,<>;:'\"\\`~␣";
14
15 int main(void) {
16     const size_t len = strlen(symbols);
17     clock_t * times = (clock_t *) calloc(len, sizeof(clock_t));
18
19     clock_t start, stop;
20     char secret[LENGTH] = {'a'};
21
22     int res = 0;
23
24     for (uint32_t i = 0; i < LENGTH; i++) {
25         printf("i:␣%u\n", i);
26         for (uint64_t j = 0; j < len; j++) {
27             secret[i] = symbols[j];
28
29             start = clock();
30             for (uint64_t k = 0; k < 10000000; k++) {
31                 res = password_compare(secret);
32             }
33             stop = clock();
34             times[j] = stop - start;
```

```
35              if (res != -1) {
36                  printf("compare␣fct␣returned␣!=␣-1;␣pw␣might␣be:␣%s\n", secret);
37              }
38          }
39
40          secret[i] = symbols[time_max(times, len)];
41          printf("pw␣so␣far:␣%s\n", secret);
42      }
43
44      printf("timing␣attack␣says:␣%s\n", secret);
45      printf("password_compare␣says:␣%d\n", password_compare(secret));
46
47      free(times);
48
49      return EXIT_SUCCESS;
50  }
51
52  /* return the index holding the highest element */
53  size_t time_max(clock_t * arr, size_t len) {
54      clock_t max = 0;
55      size_t res = 0;
56
57      for (size_t i = 0; i < len; i++) {
58          if (arr[i] > max) {
59              max = arr[i];
60              res = i;
61          }
62      }
63      return res;
64  }
```