Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
Prof. Dr. Helmut Reiser, PD Dr. Wolfgang Hommel

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2014/2015
Übungsblatt 7

Abgabetermin: 09.12.2014 bis 12:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben ist es notwendig sich über den Vorlesungsinhalt hinaus, durch Internet- und Literaturrecherche mit dem Thema zu beschäftigen.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (über Uniworx als Einzelabgabe). Während des Semesters werden vier Übungsblätter ausgewählt, korrigiert und bewertet. Bei vier als korrekt bewerteten Lösungen (mind. 75% der erreichbaren Punkte) erfolgt ein Bonus von zwei Drittel Notenstufen auf die Klausurnote, bei nur drei oder zwei richtigen Lösungen erhalten Sie einen Notenbonus von einer Drittel Notenstufe.

Aufgabe 16: **(H)** Rechtliche Randbedingungen der IT-Sicherheit (6 Punkte)

In der Vorlesung haben sie sich auch kurz mit einigen rechtlichen Rahmenbedinungen auseinander gesetzt. Folgende Szenarien seien gegeben.

a. Sie arbeiten in einem Consulting-Unternehmen, das Kunden auch in IT-Sicherheitsthemen berät. Um Ihren Kunden die Brisanz dieses Themas zu verdeutlichen, sind Sie im *Besitz* eines sogenannten Sniffer-Werkzeugs, um damit Datenpakete aus einem WLAN-Netz zu empfangen, d.h. auch Daten, die eigentlich für andere Empfänger bestimmt sind. Mithilfe dieser Datenpakete und einem weiteren, speziellen Tool kann der Zugangscode des WLAN entschlüsselt werden. Liegt hier eine Straftat Hinblick auf die Paragraphen §202b StGB und §202c StGB vor? Begründen Sie ihre Entscheidung knapp.

b. Das in Teilaufgabe a) beschriebene Werkzeug ist auf einer ausländischen Internetseite als Open Source Programm frei zugänglich und kann von dort herunteregeladen werden. Sie geben dem Sicherheitsbeauftragten eines Kunden den Link zu dieser Internetseite. Handelt es sich bei diesem Tatbestand um eine Straftat nach §202c StGB? Begründen Sie ihre Entscheidung kurz.

c. Eine Ex-Angestellte einer Schulbehörde konnte auch nach ihrem Ausscheiden auf deren Datenbank zugreifen. In zwei Fällen änderte sie Benotungen ihrer eigenen Kinder. Zu ihren ursprünglichen Aufgaben hatte gezählt, Passwörter für die Behördenleiterin und weitere Mitarbeiter zu verwalten. Dank ihrer Kenntnisse konnte sie von 2010 an – und auch weit über ihr Ausscheiden hinaus – auf Schülerbewertungen, Personalakten und E-Mail-Verkehr des Schulbezirks zugreifen.

   In zwei Fällen hat sie laut Tatvorwurf Eintragungen geändert: Aus einem Ungenügend („failing grade“) der Tochter wurde eine Entschuldigung aus gesundheitlichen Gründen, eine

Bewertung für ihren Sohn schraubt sie von 98 auf noch imposantere 99 Prozent. Als Motiv führte die 45-Jährige „Neugier und Langeweile“ an.

Nachdem ihr Arbeitsverhältnis im April 2011 endete, dauerte es noch bis Ende Februar 2012, bis die Behörde eine Untersuchung der Vorfälle einleitete. Diese ergab unter anderem, dass die Ex-Mitarbeiterin sich aus dem Netz einer anderen Behörde sowie von Rechnern des Shopping-TV-Senders QVC in die Schuldatenbank eingeloggt hatte.

(i) Welche rechtlichen Regelungen (vgl. die in der Vorlesung behandelten) sind in dem geschilderten Fall relevant?

(ii) Begründung Sie, ob es sich bei dem vorliegenden Fall um ein Offizialdelikt handelt.

(iii) Welche Besonderheiten erschweren im Allgemeinen eine zeitnahe Aufklärung einer IT-basierten Kriminalität.

Aufgabe 17: (H) Einfache Chiffriermethoden & Steganographie & One Time Pads (7 Punkte)

Eines der zentralen Themen in der Informationssicherheit ist die Kryptographie. Neben den bekannten symmetrischen und asymmetrischen Verfahren gibt es zahlreiche, auch sehr einfache und dennoch effektive Methoden, die Vertraulichkeit von Informationen sicher zu stellen.

a. Ein sehr altes kryptographisches Verfahren ist *Skytale*, welches auch als Spaltentransformation bezeichnet wird. Der Geheimtext nach Anwendung der Transposition lautet FNABAI-HUESNAFNSDUGKEESAL. Entschlüsseln Sie diesen und verwenden Sie hierbei eine Skytale mit einem Umfang U=5.

b. Neben additiven Chiffren (Caesar-Chiffre) existieren auch multiplikative Chiffren. Hierbei wird einem Buchstaben erst eine Zahl zugeordnet und anschließend mit einem Schlüsselwert k multipliziert. Das Ergebnis gibt die entsprechende Position im Alphabet (A-Z) an. Verwenden Sie den Wert $k = 2$. Der Buchstabe O soll dabei auf den Buchstaben D abgebildet werden. Geben Sie die Berechnungsvorschrift an und berechnen Sie die passenden Werte für alle Buchstaben. Was fälllt Ihnen bei dieser Substitution auf? Wie sollten Sie den Parameter k wählen, damit dieser Effekt nicht auftritt?

c. Auf der Vorlesungswebseite finden Sie im Abschnitt *Übung* zwei Bild-Dateien. In diese wurden mit den Steganographie-Werkzeug *Outguess* (Linux/Mac OS) bzw. *Steghide* (Linux/Windows) eine geheime Information eingebettet. Downloaden Sie das für ihr Betriebssystem geeignete Werkzeug und versuchen Sie den versteckten Nachrichtentext aus dem Bild zu extrahieren. Verwenden Sie als Schlüssel den Nachnamen ihres aktuellen Vorlesungsdozenten, das aktuelle Jahr und den Nachnamen des bisherigen Vorlesungsdozenten, also *Nachname1*2014*Nachname2*. Der Schlüssel enthält keine Leerzeichen. Achten Sie darauf, dass ihre Lösung nachvollziehbar ist (z.B. Angabe der verwendeten Befehlszeile, Screenshots, . . .).

d. One-Time-Pad gilt derzeit als eine der sichersten Verschlüsselungsmethoden. Geben Sie das Chiffrat für die Eingabe HALLOWELT an. Verwenden Sie als Pad die Information, die Sie aus dem Bild im Rahmen der vorherigen Teilaufgabe extrahiert haben. Sollten Sie die Information nicht extrahieren können, wenden Sie sich bitte per E-Mail an die Übungsleiter.