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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2011/2012
Übungsblatt 8

Abgabetermin: 11.01.2012 bis 14:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben benötigen Sie eine Rechnerkennung für unsere Praktikumsinfrastruktur. Um diese zu erhalten, melden Sie sich bitte über die Vorlesungswebseite zum Übungsbetrieb an.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (per **E-Mail** an die Adresse **uebung-itsec_AT_lrz.de** oder schriftlich vor der Übung). Während des Semesters werden vier Übungsblätter korrigiert. Bei vier richtigen Lösungen 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 17: (H) Sicherheitsmechanismen

Zum Erreichen der Sicherheitsziele Vertraulichkeit, Integrität und Authentizität werden unterschiedliche Mechanismen verwendet.

a. Die Autoren des Conficker-Virus waren gezwungen das auf mit dem Virus infizierten Systemen installierte Binary auszutauschen.

   (i) Im ersten Schritt wurde das neue 1345 Bits lange Binary mit dem Algorithmus MD5 gehasht. Skizzieren Sie welche Schritte an dieser Stelle zu durchlaufen waren. Der MD5-Hash wird mit M bezeichnet.

   (ii) Das Windows-Binary wurde mit der Stromchiffre RC4 und Schlüssel M verschlüsselt. Das Ergebnis lautete *enc.bin*. Um zusätzlich die Authentiztät zu gewährleisten, wurde ein asymmetrisches Verschlüsselungsverfahren mit privatem Schlüssel e^{priv} und öffentlichem Schlüssel e^{pub} angewendet. Wie lautet die Berechnungsvorschrift für eine digitale Signatur, wenn der eingebettete Modulus N lautet?

   (iii) Nach Übertragung über das Internet musste die Korrektheit verifiziert werden. Mit welcher Berechnungsvorschrift erhalten Sie den Hash-Wert M?

   (iv) Zum Entschlüsseln von enc.bin wurde erneut RC4 verwendet. Wie können Sie sicherstellen, dass bei der Übertragung keine Fehler auftraten?

Eingabe x (hex)	Ausgabe MD5(x) (hex)
0x1BAF81D154AD3D5600010203040506070809 0A0B0C0D0E0F	0xA339A0A2E397F5D59FFECED63B32B4FC
0x1B7381D122AD3D5600010203040506070809 0A0B0C0D0E0F	0x398A7DE773C25BE09AF3425D02EB216C
0x1B7381C822AD3D5601020304050607080 90A0B0C0D0E0F00	0xB9BFB2425097EE76B17C7AB7299F38D1
0x73DF81D154AD3D5600010203040506070809 0A0B0C0D0E0F	0xB239A0A2E397F5D59FFECED63B32755D
0x737381D122AD3D5600010203040506070809 0A0B0C0D0E0F	0x88D37DE773C25BE09AF3425D02EB218C
0x737399C822AD3D5601020304050607080 90A0B0C0D0E0F00	0xA23FB2425097EE76B17C7AB7299F3444
0xAC3881C822AD3D5601020304050607080 90A0B0C0D0E0F00	0xA95BBB4FF0A7511D07DC5CA6ACA6BE2E
0xAC7381C822ADF8560001020304050607080 90A0B0C0D0E0F	0x0898721134D8E73D7F0209244CFC733F
0xAC7393B143ADF8560001020304050607080 90A0B0C0D0E0F	0x58460D74328B15CC0E1B1FCF811E1621
0xC619EBA248C7923C0898721134D8E73D7F0209244CFC733F	0xA4167961D793AE17467720AB1C636951
0xC619EBF623542A340898721134D8E73D7F0209244CFC733F	0xDCB9C8C90936A7F26DC40C5403334AC8
0xC63AD4F623542A340898721134D8E73D7F0209244CFC733F	0x36165CCD748C4F0DA3CD51D83A5EA2BE
0xBB19EBA248C7923CB9BFB2425097EE76B17C7AB7299F38D1	0xB2167961D748AE17467720AB1C636425
0xBB59EBF623542A3458460D74328B15CC0E1B1FCF811E1621	0x14DFC8C90936A7F26DC40C54033388C3
0xBB3AD4F623542A340898721134D8E73D7F0209244CFC733F	0x54AB5CCD748C4F0DA3CD51D83A5ECC8B
0xFE19EBA248C7923CA339A0A2E397F5D59FFECED63B32B4FC	0x125388B1D748AE17467720AB1C9476D3
0xFE59EBF623542A3458460D74328B15CC0E1B1FCF811E1621	0xFF33236AF936A7F26DC40C540940ABE1
0xFE5D3AF623542A34B239A0A2E397F5D59FFECED63B32755D	0xCC325CCD748C4F0DA3CD51D83A19DA1F

b. Zukünftig wollten die Viren-Autoren ein HMAC-basiertes Verfahren verwenden. Berechnen Sie den HMAC für die folgenden Parameter:
   - Parameter P, der gesichert werden soll: 000102030405060708090A0B0C0D0E0F
   - Schlüssel k: 9A45B7FE149BCE60
   - Als Hashfunktion wird MD5 verwendet. Benutzen Sie obige MD5-Tabelle:

c. Welchen Vorteil bietet ein HMAC-basiertes Verfahren gegenüber einem asymmetrischen Verschlüsselungsverfahren?

Aufgabe 18: (H) Kerberos

Ein weitverbreitetes Protokoll zur Benutzerauthentisierung ist Kerberos. Beschreiben Sie den Ablauf sowie den konkreten Aufbau der ausgetauschten Nachrichten anhand des folgenden Beispiel-Szenarios:

a. Sie kommen um 08:00 Uhr in die Arbeit und loggen sich mit Ihrem Nutzernamen *zdf26395* und zugehörigem Passwort *3z!fG7qiT* ein. An welche an Kerberos-beteiligte Komponente werden diese Informationen übermittelt? Wie sieht die zugehörige Nachricht aus?

b. Die Antwort, die Sie auf Ihre erste Nachricht in Teilaufgabe a) erhalten ist verschlüsselt. Welcher Schlüssel wurde hierzu verwendet? Welche Informationen werden in der Antwort-Nachricht im allgemeinen übertragen?

c. Sie arbeiten gerade an einem Text-Dokument, welches Sie nun ausdrucken wollen. Die Steuerung des Druckers erfolgt über einen dedizierten Print-Server. An welche Kerberos-Komponente müssen Sie Ihre Druck-Anfrage übermitteln und welche Informationen enthält diese? Welchen Inhalt hat die entsprechende Antwortnachricht?

d. Welche Schritte sind abschließend zu durchlaufen, damit Ihr Dokument ausgedruckt wird?

Aufgabe 19: (Z) Hacking WebApps (optional)

Herr M. ist Administrator eines Webmail-Anbieters. Sie wollen sich Zugang zu einem Konto dieses Webmail-Anbieters verschaffen. Hierzu müssen Sie an eine Liste mit Nutzer-Passwörtern gelangen, die sich im Verzeichnis /etc/httpd/conf/htaccess befindet. Sie wissen, dass Herr M. den Benutzernamen admin verwendet, am 24.12. Geburtstag hat und eine Frau mit dem Namen Marlene.
Aufgabe: Beschaffen Sie sich Zugriff auf die Datei mit den Passwörtern. Die URL des Webmail-Anbieters lautet http://www.webmail-live.de.