

Professur Netzwerktechnologien und multimediale Teledienste – LV Netzwerke Basistechnologien (SS 2006)

Aufgabenblatt 5, Thema: Sicherheit

Abgabe bis Freitag, 07.07. 2006, 24 Uhr! (Es zählt der Eingangszeitpunkt)

Hinweise:

- *Senden Sie Ihre Lösung als doc- oder (vorzugsweise) pdf-Datei an die Adresse qos@cs.uni-potsdam.de mit dem Betreff „NWBasis5 Nachname, Vorname“.*
- *Benennen Sie die Datei bitte wie folgt: „Nachname, Vorname (NWBasis5 SS2006)“.*
- *Eine Antwort pro Aufgabe sollte kurz und prägnant sein und darf 300 Worte nicht überschreiten!*
- *Geben Sie für die verwendeten Zitate stets die Quellen an, wenn Sie Informationen außerhalb der Vortragsfolien für Ihre Lösungen übernehmen. Ungekennzeichnete Zitate werden nicht gewertet!*
- *Haken Sie nach, wenn Sie innerhalb von 24h keine Bestätigung Ihrer Einsendung erhalten!*
- *Die Lösungen der Aufgaben sind einzeln zu bearbeiten, keine Gruppenlösungen!*
- *Bei identischen (Teil-)Lösungen wird nur die erste Einsendung bewertet!*
- *Geben Sie bei Rechenaufgaben die Formel, den Lösungsweg und die Einheiten mit an!*
- *Die Gesamtpunktzahl beträgt 30 Punkte.*
- *##) Multiple Choice („Alles oder nichts“): Jede Teilantwort ist ein elementarer Bestandteil der Lösung. Eine falsche oder ausgelassene Teilantwort ergibt für die Aufgabe 0 Punkte.*
- ***) Multiple Choice („Minus- und Pluspunkte“): Falsche oder fehlende Teilantworten führen zu Minuspunkten innerhalb der Aufgabe. Es gibt mindestens 0 Punkte für die Aufgabe.*
- ***In eigenen Worten:*** Zitate werden für die Benotung der Aufgabe nicht gewertet.

Nachname:

Vorname:

Matrikelnummer:

E-Mail:

1) Ordnen Sie die folgenden Sicherheitsverfahren den einzelnen Schichten des OSI-Modells zu (Mehrfachnennungen möglich). **(2 Punkte)**

verschlüsselte Ende zu Ende Verbindungen, Benutzerauthentifizierung, verschlüsselte Punkt zu Punkt Verbindungen, Versiegelte Übertragungsleitungen, verschlüsselte Prozess zu Prozess Verbindungen, Firewalls,

2) RSA

a) Wie funktioniert das RSA-Verschlüsselungsverfahren? **(4 Punkte)**

b) Worin unterscheidet sich dieses asymmetrische Verfahren gegenüber einem symmetrischen Verfahren (etwa AES)? **(1 Punkt)**

c) Welchen Vorteil bietet dieses asymmetrische Verfahren gegenüber einem symmetrischen Verfahren? **(1 Punkt)**

d) Sie kennen den öffentlichen RSA-Schlüssel (public key) einer Person X.

Dieser besteht aus den Zahlen $n=53387$ und $e=59$.

Brechen Sie den Schlüssel, d.h. ermitteln Sie den privaten Schlüssel von X. **(3 Punkte)**

e) Worin lag die Schwäche bei dem öffentlichen Schlüssel? Wie hätte man den Angriff verhindern/erschweren können? **(1 Punkt)**

3)

a) Wie funktioniert das PGP Verfahren? **(1 Punkt)**

b) Nennen Sie zwei Gründe weshalb PGP Nachrichten komprimiert. **(2 Punkte)**

4) ** Bewerten Sie die folgenden Aussagen zu Schutzzielen des Internet Protocol Version 4 (IPv4)! **(1,5 Punkte)**

	Aussage	wahr	Falsch
a)	IPv4 garantiert das Schutzziel der Authentizität.		
b)	IPv4 garantiert das Schutzziel der Vertraulichkeit.		
c)	IPv4 garantiert das Schutzziel der Integrität.		

5) ** Bewerten Sie die folgenden Aussagen zu IPsec! **(1,5 Punkte)**

	Aussage	wahr	Falsch
a)	IPsec definiert Sicherheitsdienste auf der Sicherungsschicht (Schicht 2).		
b)	IPsec garantiert das Schutzziel der Authentizität.		
c)	Die Implementierung der IPsec-Spezifikation ist für IPv6 nicht verpflichtend.		

6) ** Bewerten Sie die folgenden Aussagen zum Secure Socket Layer (SSL)! **(2 Punkte)**

	Aussage	Wahr	Falsch
a)	SSL definiert Sicherheitsdienste auf der Sicherungsschicht (Schicht 2).		
b)	SSL garantiert das Schutzziel der Integrität.		
c)	SSL garantiert das Schutzziel der Vertraulichkeit.		
d)	SSL garantiert das Schutzziel der Verbindlichkeit.		

7) Das SSL – Datentransportprotokoll enthält zwei Einmalinformationen wie auch einen Premaster-Schlüssel. Welchen Wert, wenn überhaupt, hat die Verwendung der Einmalinformationen? **(2 Punkte)**

8) Aufgabe (Firewall)

a) Wieso führt man für interne Netzwerke zusätzlich eine DMZ ein, wenn doch eine Firewall nach außen das Netzwerk schützen könnte? **(1 Punkt)**

b) Beschreiben Sie die Funktionsweise der Angriffe "Tiny Fragment Attack" und "Overlapping Fragment Attack". (RFC 1858) **(1 Punkt)**

c) Wieso schützt die Abwehrmaßnahme "Direct Method" nur vor "Tiny Fragment Attack"? **(2 Punkte)**

- d) Die zweite Abwehrmaßnahme "Indirect Method" schützt vor beiden Angriffen.
Gibt es bei dieser Maßnahme dennoch eine Möglichkeit, TCP-Header-Angaben im Nachhinein zu verändern? **(1 Punkt)**
- 9) Schicken Sie eine Email mit dem Absender qos@medienengineering.de und dem Betreff mit dem Betreff „Nachname hat NWBasis Aufgabe 9 gelöst,“ an qos@cs.uni-potsdam.de und nennen Sie Ihren Namen und Matrikelnummer, sowie das verwendete Programm/ Vorgehen im Body. **(3 Punkte)**