TENTAMEN: Netwerken

27 mei, 2014, 14:00 – 17:00

De duur van het tentamen is 3 uur. Het aantal opgaven is 5 met een totaal van 17 onderdelen. Achter elk onderdeel staat tussen vierkante haken het te behalen aantal punten (totaal aantal te behalen punten is 100). Het tentamen is **gesloten boek**, dus het is niet toegestaan om het college dictaat of eigen gemaakte aantekeningen te gebruiken. Beargumenteer al uw antwoorden.

Opgave 1

1. Gegeven de volgende bit string 0110001111011100. Stel we zouden deze bit string versturen met behulp van een ADSL modem (16 QAM), teken dan een mogelijke resulterend analoog signaal. Leg uit hoe dit signaal tot stand is gekomen. [5]
2. Stel we zouden bovenstaand analoog signaal versturen en er treedt attenuation distortion op teken dan, en leg uit!!, hoe bovenstaand signaal na verzending er uit zou kunnen zien. Dezelfde vraag maar nu met delay distortion. [5]
3. Leg uit waarom bovenstaand signaal eigenlijk niet zozeer vervormd wordt door attenuation en delay distortion als een willekeurig ander analoog signaal en dat dit ondermeer de reden is waarom bv. XS4ALL (en bv. ook Ziggo) in staat is om HDTV te faciliteren. [5]
4. Wat is de andere reden waarom XS4ALL en Ziggo bijna foutloos HDTV kunnen faciliteren. [5]

Opgave 2

1. Laat zien hoe CRC werkt. Gebruik hierbij als te verzenden frame 1011100011 en gebruik als generator polynoom:
$$G[X] = X^4 + X^3 + 1.$$ [5]

2. CRC-32: $X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$ wordt gebruikt in het ppp protocol. Welke error detectie eigenschappen heeft CRC-32 en leg uit waarom. [10]

Opgave 3

1. Leg uit hoe het Diffie-Hellman key exchange mechanisme werkt. [5]
2. Leg uit wat voor een rol het Diffie-Hellman mechanisme heeft via het SSL protocol in het https protocol. [5]
3. Drie dagen geleden stond er op telegraaf.nl:

za 24 mei 2014, 21:00 | 117 reacties

Betaalvereniging: gebruik geen Explorer

HOOFDDORP - Betaalvereniging Nederland waarschuwt bankklanten om geen Internet Explorer meer te gebruiken bij het internetbankieren. Dat zei adjunct-directeur Gijs Boudewijn zaterdag in Kassa. Eerder op de dag bleek uit onderzoek van NU.nl en beveiligingsbedrijf SecureLabs dat transacties van consumenten in verschillende browsers te zien en te manipuleren zijn door de versleuteling van internetverbindingen uit te schakelen.

Foto: ANP

De banken hebben al maatregelen genomen om het beveiligingslek te dichten, zo liet het Nationaal Cyber Security Centrum al weten. Maar de nieuwe techniek die fraude met de transacties moet voorkomen, het zogeheten HTTP Strict Transport Security (HSTS), wordt volgens NU.nl nog niet door elke bank en browser ondersteund. Zo zou Microsoft de ondersteuning pas in de volgende versie van Internet Explorer voor elkaar hebben. Google Chrome, Safari en Mozilla Firefox ondersteunen het nieuwe protocol wel.

Voor zover bekend is er nog nooit geld gestolen dankzij een uitgeschakelde versleuteling, maar Betaalvereniging Nederland vreest dat dat nog steeds kan gebeuren. „De eerlijkheid gebiedt me te zeggen, dat je als je het zeker wilt weten, je een andere browser moet gebruiken tot Internet Explorer is aangepast", aldus Boudewijn.

Om banktransacties te manipuleren is een wifi-hotspot nodig waarop speciale software kan worden geïnstalleerd. Terwijl de verbinding naar de bank gewoon versleuteld is, kan de hotspot de beveiligde verbinding naar de gebruiker dan uitschakelen. Omdat er wel een 'slotje' in de url-balk zichtbaar is, valt dat haast niet op.

Leg uit hoe de manipulatie zoals omschreven in de laatste paragraaf gerealiseerd kan worden. Of is dit niet echt mogelijk? [10]

Opgave 4

1. Schets de stappen die genomen worden nadat een http packet gegenereerd is op een laptop om vervolgens dit packet via een WIFI verbinding naar bv een ADSL modem te versturen. [5]
2. Zelfde vraag als onder 1, maar dan nu in het geval de laptop verbonden is via Ethernet met een netwerk switch. [5]
3. Ethernet is gewoonlijk geïmplementeerd zonder flow control. Leg uit waarom hiervoor gekozen is. [5]
4. Leg uit hoe flow control via Ethernet wel geïmplementeerd kan worden indien dit gewenst is, en wat de relatie is met het HDLC protocol. [10]

Opgave 5

1. Leg het verschil uit tussen Carrier Sensed Multiple Acces (CSMA) met Collision Detection (CD) of Collision Avoidance (CA). [5]
2. Wat zijn de functionaliteiten van de data link layer. [5]
3. Leg uit hoe de verschillende combinaties van datagram met virtual circuit routing werken. [5]
4. Hoe werkt smoothening bij Internet routing. [5]