Examen Beveiliging

11 januari 2019

Deel I
Gesloten boek

1 Terminologie

Leg volgende termen kort uit:

- Digraph Crypto.
- Degenerate signed data.
- Dual-homed firewall.
- Cross-Site Request Forgery.

2 Juist/Fout

Zijn volgende uitspraken waar of niet waar? Leg uit waarom.

- Ephemeral DH is veiliger dan traditionele DH.
- Een metamorphic virus is detecteerbaar met emulatietechnieken.
- TLS is niet beveiligd tegen trafiekanalyse.
- ??? vergeten

3 SSH

1. Van welke deelprotocollen maakt SSH gebruik? Wat is de functionaliteit van elk deelprotocol.
2. Geef aan of volgende beveiligingsdoelen gerealiseerd worden in SSH of niet. Leg uit.
    - Traffic-flow confidentialiteit.
    - Authenticatie.
    - Non-repudiation.

3. Geef drie verschillen tussen SSH en VPN.
4. Waarom maakt SSH gebruik van zowel RSA als Diffie Helman.
5. Stel dat je een connectie wil maken vanuit België naar China, maar de overheid blokeert actief al het SSH verkeer en filtert bovendien ook alle pakketten. Hoe kan je een SSH connectie openen (zonder hierbij een extra server te moeten inschakelen).

4 Malware

1. Geef vijf technieken die malware toepassen om niet gedetecteerd te worden.
2. Geef drie manieren om een buffer overflow te voorkomen.
3.

5 Bitcoin

1. Leg uit hoe een nieuwe transactie geregistreerd wordt.
2. Waarom maakt het bitcoin protocol gebruik van EC en niet van RSA?
3. Geef aan of volgende beveiligingsdoelen gerealiseerd worden in het bitcoin protocol of niet. Leg uit.
   - Authenticatie.
   - Beschikbaarheid.
   - Confidentialiteit.
4. Naast proof-of-work bestaat er een alternatieve manier (proof-of-stake) om consensus te verkrijgen over een transactie. Geef drie implementaties van deze alternatieve manier.

Deel II
Open boek

6 Blokcijfers

Als encryptieschema gebruiken we tabel 1. In plaats van de XOR operator maken we gebruik van optelling modulo 26, bijvoorbeeld: C XOR D = F en E XOR Y = C.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
k	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
E_k	P	K	X	C	Y	W	R	S	E	J	U	D	G	O	Z	A	T	N	M	V	F	H	L	I	B

Tabel 1: Encryptieschema.

1. Encrypteer `TRIPOS` met behulp van volgende blockcijfermodi:

- Electronic Codebook.
- Cipher Block Chaining (IV $c_0 = \mathrm{K}$).
- Output Feedback (IV $c_0 = \mathrm{K}$).

2. Decrypteer `BSMILVO` met behulp van Cipher Block Chaining (IV $c_0 = \mathrm{K}$). Welke operatie moeten we gebruiken in plaats van XOR?

7 Beveiliging van een online webshop

Een bepaalde webshop laat toe aan gebruikers om goederen aan hun digitale winkelkar toe te voegen. De server houdt per gebruiker een bestand bij, met daarin de goederen die in de winkelkar zitten. Indien een gebruiker op de knop *`voeg toe`* drukt, dan zal de server dit bestand aanvullen met de prijs, hoeveelheid en naam van het geselecteerde goed.

1. Is deze implementatie kwetsbaar voor een Denial of Service aanval? Leg uit.

De implementatie wordt nu aangepast. De gebruiker houdt nu client-side een lijst bij van zijn winkelkar. Telkens wanneer een gebruiker op de knop *`voeg toe`* drukt, zal de server een hidden form doorsturen met informatie over het object, die de client dan via javascript toevoegd aan zijn client-side winkelkar. Eens de client zijn bestelling wil afronden wordt de lijst doorgestuurd naar de server, die als antwoord het totaalbedrag terugstuurd en een bevestiging vraagt aan de gebruiker.

2. Is deze implementatie nog steeds kwetsbaar voor de Denial of Service aanval uit vorige implementatie? Leg uit.
3. Zijn er nog andere aanvallen mogelijk? Je mag veronderstellen dat er HTTPS gebruikt wordt en dat XSS, CSRF, SQL injection, ... onmogelijk zijn.

8 IPsec