Examen Informatiebeveiliging/Information Security 2018-2019

Bachelor Informatica juni 2019

Naar de herinnering van de studenten

1

Question 1 (mondeling):
Advantages and disadvantages of TLS compared with IPsec for VPN's etc (with focus on interoperability, installation en maintainability, security, problems with NAT and (non-ipsec) firewalls)

Question 2 (mondeling):
Choose security mechanism for communication between two local networks in a company (see previous exams)

Question 3 (schriftelijk) :
Questions about tree hashing (Merkle trees):
1) compare complexity with normal hash function
2) if not a given depth of tree, no weak collision resistance.. Give M' with same hash as M and think of change to algorithm to fix this problem
3) If MD5 is used as hashing function in hash tree, is there strong collision resistance?

Question 4 (schriftelijk):
Compare computation time of GMF using SHA-2-256 and SHAKE256 (if known that SHA-2-256 uses 12 processor cycles and SHAKE256 uses 13 processor cycles)

2

1) de certificate chain van www.ugent.be is gegeven + alle eigenschappen (key length, algorithm,...). Verklaar de keuzes voor deze eigenschappen en zeg of je dit veilig genoeg vindt of wat je zou aanpassen.

2) badge systeem voor access control van een gebouw, de badge heeft geen power en heeft gelimiteerde rekencapaciteit. Schrijf een systeem uit + protocol.

3) PKCS BT=01 vs BT=02: waarom andere soort padding? + Wat voorkomt BT=01 dat BT=00 niet voorkomt. Wat voorkomt BT=02 en op welke manier?

4) Vergelijk de rekentijd voor signature verificatie bij DSA (p=3072, q=265) t.o.v. RSA (n=3072)

3

Vraag 1 (mondeling)
Bespreek de initialisatie communicatie van IKE. Hoe bereikt men authenticatie? Wat zorgt ervoor dat replay-attacks niet kunnen voorkomen? Welke cryptografische algoritmen zou je gebruiken?

Vraag 2 (mondeling)
Momenteel wordt gebruik gemaakt van RSA-2048 en soms nog RSA-1024. Hoe kan je ervoor zorgen dat de data integriteit behouden wordt over een tijdspanne van 30-100 jaar? Langere keys? Trusted third party?

Vraag 3 (schriftelijk)
Waarvoor wordt de seed gebruikt in RSA-OAPSE en welke attacks kunnen hierdoor niet meer voorkomen in vergelijking met raw RSA? Wat is een goede lengte voor deze seed + leg uit?

Vraag 4 (schriftelijk)
Momenteel wordt er gebruik gemaakt van GDFS met RSA-2048. Stel dat SDFS beter is in het factoriseren, wat zou de sterkte zijn van RSA-2048?
Bereken ook welke key lengte nodig is voor SDFS om dezelfde veiligheidsgraad te bekomen als voor GDFS met RSA-2048.

4

1) Gegeven: beschrijving over pepper. Wat zijn de voordelen/nadelen van de combinatie salt+pepper. Bespreek dit voor login, rainbow tables, dictionary attack
2) Ontwerp een systeem voor single sign-on
3) Is weak collision resistance een nodige voorwaarde als je al een one-way function hebt?
4) 512 bit input, versleuteld via RSA scheme rsa-oaep met SHAKE256 als MGF. Wat is de overhead tov versleuteling met pkcs1.5. Verder was er nog duurtijd gegeven van rsa encryptie en van sha-256.