Eerste deeltoets Security

31 mei 2013, 8.30 – 10.30, Educ-α.

Motiveer je antwoorden *kort*! Zet je mobiel uit. Stel geen vragen over deze toets; als je een vraag niet duidelijk vindt, schrijf dan op hoe je de vraag interpreteert en beantwoord de vraag zoals je hem begrijpt.

1. **Aanvallen:** Wat is het verschil tussen een *KPA* en een *CPA* en wat betekenen deze letters? (Ca. 5-6 regels.)

2. **Symmetrische en asymmetrische cryptografie:** Wat is het verschil tussen *symmetrische* en *asymmetrische* cryptografie? Noem van beide vormen (twee) voorbeelden.

3. **Entropie:** (a) Wanneer heeft een taal *entropie* α?
   (b) Hoe gebruik je kennis van een taal L in een crypto-aanval?
   (c) Wat is de relatie tussen sleutellengte, entropie en kritieke lengte?

4. **Scrypt:** Een hashfunctie heet *memory-hard* als het geheugengebruik van (bijna) dezelfde grootteorde is als het tijdgebruik.

   Waarom zou je een memory-hard hashfunctie willen gebruiken om wachtwoorden op te slaan? Waarom telt dit voordeel dubbel ingeval je tegenstander over parallelle hardware beschikt?

5. **3DES en AES:** Hoewel 3DES niet direct onveilig was, zijn DES en 3DES vervangen door AES.
   (a) Wat zijn de sleutellengtes van DES, 3DES en AES?
   (b) Hoewel 3DES een langere sleutel heeft dan AES, bestaat er een KPA tegen 3DES met een lagere complexiteit. Beschrijf (kort) deze aanval.
   (c) Wat is de rekentijd van die aanval, en is dit in de praktijk een probleem voor 3DES?

6. **AES Rondes:** Uit welke vier stappen bestaat een ronde van AES? Hoeveel ronden worden er gebruikt?

7. **Stroomversleuteling:** GSM telefonie gebruikt het A5 algoritme, een vorm van stroomversleuteling.

   (a) Waarin komen stroomversleuteling en het One Time Pad overeen, en waarin verschillen ze?
   (b) Noem enkele (bv vier) voor- en nadelen van stroomversleuteling ten opzichte van blokversleuteling.
   (c) Waarom is stroomversleuteling zo geschikt voor telefonie?

8. **Wifi Acces:** Kabelaar Gizzo geeft elk van zijn 800.000 klanten een Wifi modem met ingesteld wachtwoord k; de meesten negeren het advies, dit wachtwoord te wijzigen. Als een station zich wil aanmelden, stuurt het modem een random x op, en vraagt de waarde $AES_k(x)$ terug. Het ingestelde wachtwoord bestaat uit 12 hexadecimale tekens (1234567890ABCDEF).

   (a) Hoeveel van deze keys zijn er?
   (b) Een woordvoerder van Gizzo zegt dat de modems veilig zijn omdat het vele jaren duurt om zo'n key te kraken. Hoe lang duurt het brute-forcen van de key als je 10 miljoen keys per seconde kunt proberen?
   (c) Binnen enkele dagen verschijnen er hack-apps gebaseerd op tabel-aanvallen. Geef een schatting van (1) het geheugengebruik van die app; (2) de rekentijd; (3) het aantal klanten dat je ermee kunt aanvallen.

9. **EMV Corner model en encryptie:** Het EMV betaalmodel gebruikt een Four Corner indeling. Welke zijn deze vier hoeken? Welke symmetrische encryptie gebruikt EMV?