Eerste Deeltoets Security

22 mei 2015, 13.30 – 15.30, Beatrix 7e.

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.
Cijfer: Vraag 3 en 4 zijn 3pt, de anderen 2pt. Omdat vraag 7 erg moeilijk bleek, is een extra voet van 1pt gegeven. Toetsresultaat is punten plus 1 gedeeld door 1,5.
Maak opg 1 en 2 op pagina 1, op 3 en 4 op pag 2, en opg 5, 6 en 7 op pagina 3.
Let op: er is ook een achterkant!!

1. **Zeven meerkeuzevragen:** (I) Als je een bericht onleesbaar maakt voor een onbevoegde buitenstaander doe je aan: (a) encryptie; (b) decryptie; (c) compressie; (d) steganografie.

   (II) Hoeveel sleutels zijn er nodig in een symmetrisch cryptosysteem bij 90 deelnemers, om ieder persoon met elkaar te laten communiceren? (a) 4005; (b) 915; (c) 180; (d) 90.

   (III) Het idee van een *éénrichtingsfunctie* (one-way function) speelt een centrale rol binnen public-key cryptografie. Wat zijn éénrichtingsfuncties? (a) Functies die zelf gemakkelijk uit te rekenen zijn, maar het bepalen van de inverse is aanzienlijk moeilijker; (b) Functies die zelf gemakkelijk uit te rekenen zijn, maar het bepalen van de inverse is aanzienlijk makkelijker; (c) Functies die zelf moeilijk uit te rekenen zijn, maar het bepalen van de inverse is aanzienlijk moeilijker; (d) Functies die zelf moeilijk uit te rekenen zijn, maar het bepalen van de inverse is aanzienlijk makkelijker.

   (IV) In een public-key cryptosysteem ontvangt B een vercijferde boodschap van A. Waarmee ontcijfert (decrypteert) B de boodschap van A? (a) de publieke sleutel van A; (b) de publieke sleutel van B; (c) de privésleutel van A; (d) de privésleutel van B.

   (V) Hoeveel sleutels zijn er nodig in een asymmetrisch cryptosysteem bij 90 deelnemers, om ieder persoon met elkaar te laten communiceren? (a) 4005; (b) 915; (c) 180; (d) 90.

2. **AES contra Moore:** De ontwerpers van AES verwachten dat AES nog zeker 50 jaar in gebruik blijft. Denk je dat het zo lang duurt tot een brutekracht-aanval op AES mogelijk is? Betrek in je antwoord de Wet van Moore, waarbij je een jaarlijkse verdubbeling van rekenkracht mag veronderstellen.
3. **AES Modes:** Je wilt met AES een hele disk versleutelen en je wilt niet dat een herhaald blok op de disk ($X_i = X_j$) ook een herhaling van een ciphertext blok geeft. Maar als je blok voor blok apart versleutelt ($Y_i = E_k(X_i)$ gebeurt dat wel.

   (a) Beschrijf hoe je voorkomt dat herhalingen in de plaintext leiden tot herhalingen in de ciphertext.
   (b) Je wilt delen van de disk los kunnen bekijken, zonder ook naar ander blokken op de disk te moeten kijken. Ken je een AES mode die dit mogelijk maakt?

4. **Hash met Verlenger:** Op Willems Wonder Web moet je wachtwoord minstens zes letters zijn. Willem slaat de wachtwoorden niet plain op, als `[login, ww]` omdat hij beseft dat hackers het wachtwoordbestand kunnen stelen met SQL-injecties. En ook niet de combinatie `[login, SHA1(wachtw)]` omdat hij weet dat zesletterige wachtwoorden met Rainbow Tables te ont-hashen zijn.

   (a) Willems eerste idee is, de hash te *salten*. Hoe werkt dit, en waarom beschermt het Willems klanten onvoldoende?
   (b) Willem kiest een random, geheime verlengstring `vs` van lengte 6 en slaat gebruikersinfo op als `[login, SHA1(ww+vs)]`. Een aanvaller die dit bestand steelt, moet SHA1 terugrekenen voor strings van (minstens) 12 lang, wat teveel werk is. Simon de Schurk weet inderdaad een truuk om de wachtwoordlijst te stelen, en strings van 12 terughalen uit een hash kan hij inderdaad niet. Help Simon om de wachtwoorden van Willems Web te stelen.

5. **Rekenen in AES:** In AES wordt gerekend in het Finite Field $F = \mathbb{Z}_2[X]/X^8 + X^4 + X^3 + X + 1$. Laat $A = 01000101$ en $B = 00010010$.
   (a) Hoeveel elementen heeft F?
   (b) Hoe wordt een som (de $+$) in F berekend en wat is de uitkomst van $A + B$?
   (c) Hoe wordt een product (de $*$) in F berekend en wat is de uitkomst van $A * B$?

6. **Fasen bij het hacken:** Bij Hacken worden vijf fasen onderscheiden, waaronder (alfabetisch) *Covering Tracks*, *Maintaining Access* en *Reconnaissance*.
   (a) Noem alle vijf de fasen in volgorde.
   (b) Wat doe je in Reconnaissance en hoe kun je dat bereiken?

7. **Bedreigingen:** STRIDE is een acroniem voor zes soorten dreiging, zoals S=Spoofing, T=Tampering, etc. De zes beschermingen ertegen zijn (alfabetisch) Authentication, Authorization, Availability, Confidentiality, Integrity, Nonrepudiation.
   (a) Waarvoor staan de R, I, D en E?
   (b) Geef de een-op-een koppelingen van dreigingen aan beschermingen.