Eerste Toets Security

11 oktober 2017, 8.30 – 10.30, Educ-α.

Motiveer je antwoorden *kort*! 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: Maak vragen 1 en 2 op pagina 1, vraag 3 op pagina 2, en vragen 4 en 5 op pagina 3. Vraag 5 is 2pt, de andere vragen elk 3pt. Te halen 14pt, T1 is totaal plus 1,5, gedeeld door 1,4 (max 10).

1. **De Russen komen:** Alisya en Bobski sturen elkaar berichten in *extended ASCII*, waarin elk karakter acht bits inneemt, maar behalve 80 Westerse lettertekens, ook de 30 Cyrillische hoofdletters en 30 extra kleine letters voorkomen.
   (a) Wat is de entropie van hun berichten?
   (b) Alisya en Bobski versleutelen hun berichten met 3AES, waarbij driemaal AES wordt toegepast met sleutels van hoogste AES-lengte. Wat is de kritieke lengte?
   (c) Olga onderschept een bericht bestaande uit 100 3AES-blokken. Hoe staan haar mogelijkheden om dit met een Brute Force Attack leesbaar te maken?

2. **Trekking en Dekking:** Een website geeft nieuwe gebruikers *random* (uniform en onafhankelijk) rijtjes van zes kleine letters (zoals `hdiand` en `sxkinw`) als initieel wachtwoord, en slaat de hash ervan zonder salt op. Je gaat een Rainbow Table maken om gebruikers aan te vallen die hun wachtwoord niet hebben veranderd.
   (a) Hoeveel van deze wachtwoorden bestaan er?
   (b) Schat hoeveel *verschillende* wachtwoorden zijn uitgegeven na 50 miljoen aanmeldingen. Schat hoe groot je tabel moet zijn om 100 miljoen unieke wachtwoorden te bevatten.
   (c) Geef een schatting van de rekentijd (aantal hash berekeningen) van een query nadat je de tabel hebt gestolen.

3. **AES Operationeel:** (a) Uit welke vier deelstappen bestaat een ronde van AES versleuteling? Zeg van elk in 1 zin wat ze doen.
   (b) Welke keylengtes zijn toegestaan en hoeveel rondes worden gedaan?
   (c) Hoe werkt de ontsleuteling?

4. **Een LFSR:** Een zes bits LFSR A heeft twee taps, namelijk op posities 5 en 3, en begint met inhoud 110011.
   (a) Wat zijn de volgende vier toestanden van A?
   (b) Stel dat vanaf de beginstand 110011, de invoer 1010 wordt gegeven. Wat zijn dan de volgende vier toestanden?
   (c) Wat is de maximale lengte van een cykel voor een zes bits LSFR?

5. **Diversen:** (a) Wat staat op 1 in de OWASP top 10?
   (b) Hoe achterhaalt Facebook wie NU.nl bezoekt, ook zonder Facebook account?
   (c) Welke (vier) acties onderneemt de Universiteit als er een Phishing aanval is?