Eerste Toets Security

10 oktober 2018, 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. Vraag 1 is 1pt, Vraag 2 en 6 zijn 2pt, vraag 3, 4 en 5 zijn 3pt. Maak vraag 1 en 2 op de voorkant, vraag 3 en 4 op pagina 2 en vraag 5 en 6 op pagina 3.

1. **Secure Lifecycle:** Welke maatregel gebruik je voor Software Security in (A) Initiation phase, (B) Planning phase, (C) Building phase, (D) Delivery phase, (E) Maintenance phase?
   Kies uit: (i) Attack Surface Analysis; (ii) Code Reviews; (iii) Code Signing; (iv) Incident Response; (v) Look at Quality Regulations; (vi) Training/Education.

2. **Big Caesar:** Piet bouwt voor Alice en Bob een applicatie waarin berichten van 128bits worden uitgewisseld. Er zijn dus 2^{128} verschillende berichten mogelijk en omdat 2^{128} veel meer is dan 26, besluit Piet om een variant van Caesar encryptie te gebruiken. Alice en Bob delen een 128-bits getal k, en in plaats van bericht x sturen ze $y = E_k(x) = (x + k)\%(2^{128})$.
   (a) Vijand Victor onderschept een bericht y, een rijtje van 128 bits; kan hij de plaintext x (van 128 bits) vinden met een Brute Force Attack? Zeg ook hoe of waarom!
   (b) Victor probeert, een door hem bedacht bericht x aan Bob te geven en hoopt dat Bob x aan Alice zal sturen. Welk voordeel heeft Victor van het onderscheppen van y, als hij de boodschap x immers toch al kent?

3. **AES Rekenen: Matrix:** (a) Uit welke vier operaties bestaat een ronde van AES?
   (b) Hoe wordt in het AES getalsysteem een waarde vermenigvuldigd met 00000011?
   (c) Wat is 0xAB + 0xAB en wat is 0x02 × 0xAB?

4. **$\mathbb{Z}_m^*$ is gesloten:** De verzameling $\mathbb{Z}_m^*$ is gesloten onder vermenigvuldiging, dwz., dat het product van twee getallen uit de verzameling ook weer in de verzameling zit.
   (a) Wat is $\mathbb{Z}_m^*$ (geef de definitie)?
   (b) Bewijs dat $\mathbb{Z}_m^*$ gesloten is onder vermenigvuldiging.
   (c) Is $\mathbb{Z}_m^*$ ook gesloten onder optelling? Leg uit!

5. **Inversen:** (a) Is $84 \in \mathbb{Z}_{1001}^*$? Zeg waarom niet of geef de inverse!
   (b) Is $85 \in \mathbb{Z}_{2018}^*$? Zeg waarom niet of geef de inverse!
   (c) Met hoeveel vermenigvuldigingen berekent het kwadrateringsalgoritme (Indisch machtsverheffen) de macht a^{103}?

6. **Malware Detection:** There are two main techniques for detecting malware. State and briefly describe each of them. *Answer in English!*