Tweede Toets Security

4 november 2019, 8.30 – 10.30, Educ-Γ.

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. Vragen 7, 2 en 3 zijn 3pt, vraag 1 is 1pt, vragen 4 en 5 zijn 2pt, vraag 6 is 4pt. Maak vragen 1 en 2 op de vookant, vragen 3 en 4 op pagina 2, vragen 5 en 6 op pagina 3, en vraag 7 op de achterkant.

1. **Secure Coding:** (a) Orden deze beschrijvingen van proces-volwassenheid volgens het *Capability Maturity Model* van beginnend naar hoog: Capable, Defined, Efficient, Initial, Repeatable.
   (b) Wat is het principe van *Least Privilege* en welke moeilijkheden worden hiermee voorkomen?

2. **Chinese reststelling:** Je rekent in $\mathbb{Z}_{2921}$ en je weet gelukkig dat 2921 = 127x23.
   (a) Geef de waarden W_{127} en W_{23}.
   (b) Tot welke macht moet je verheffen om een wortel te trekken modulo 127? Hoeveel vermenigvuldigingen kost dit?
   (c) Je moet in $\mathbb{Z}_{2921}$ een gegeven getal x verheffen tot de macht 1215. Welke berekening doe je in de subgroepen en hoeveel vermenigvuldigingen kosten die?

3. **RSA Sleutelgeneratie:** (a) Welke stappen heeft de sleutelgeneratie van RSA?
   (b) Geef van elke stap de complexiteit, als functie van de gewenste sleutellengte k.
   (c) Hoe lang moet een RSA key zijn en waarom (twee redenen)?

4. **Signatures:** Bob ondertekent zijn berichten door eerst een SHA256 van een bericht te nemen en die vervolgens te ondertekenen met een Elgamal Signature. Hij gebruikt een generator g in de groep $\mathbb{Z}_p^*$, een private key a en een public key b.
   a) Noem twee redenen om eerst te hashen voordat je een Elgamal signature zet.
   b) Leg uit hoe iemand kan controleren of een handtekening van (c, d) van een bericht M wel echt de handtekening van Bob is.

5. **Cryptocurrency:** a) Geef een voordeel en een nadeel van een **block reward** ten opzichte van een **transaction fee**.
   b) Hoe kan in de bitcoin een **transaction fee** ingevoerd worden, zodanig dat er in 1 bitcoin block nog steeds 3499 transacties passen?

6. **Mirai botnet:** a) Het Mirai netwerk is een netwerk waarin we vier verschillende soorten nodes (entiteiten in het netwerk) onderscheiden. Welke vier verschillende soorten zijn dit en wat is hun respectievelijke rol?
   b) Noem drie vaak voorkomende zwakheden in IoT-devices waar het Mirai-netwerk gebruik van maakt. Geef niet alleen een naam maar ook uitleg.
   c) Alice haar buurman Bob heeft een eigen website gemaakt. Bob heeft zonder toestemming van Alice de schutting geschilderd in een kleur die Alice niet mooi vindt. Om wraak te nemen wil Alice een Denial of Service aanval op Bob zijn website uitvoeren en ze betaalt het Mirai botnetwerk voor een DDos aanval. Alice weet dat Bob een kleine website heeft met doorgaans weinig traffic. Kan Alice beter een SYN-FLOOD of een ACK-flood kopen? Leg uit.

7. **Offline Kahoot 2:** 1) Bob moet controleren of de transactie van Alice wel echt in bitcoin-blok 5 thuis hoort. Hoe veel hashes moet Bob maximaal doen voordat hij dit zeker weet?
a) 10 b) 11 c) 12 d) 13.

2) Een verjaardagsaanval is niet mogelijk wanneer een functie:
a) Perfect verhullend is. b) One way is. c) Zwak botsingsvrij is. d) Sterk botsingsvrij is.

3) Waarom vindt IBM dat Google nog geen **quantum supremacy** heeft bereikt?
a) IBM vindt dat de vergelijkingscomputer van Google een te trage processor heeft. b) IBM vindt het probleem dat Google heeft gekozen om op te lossen een makkelijk probleem voor een normale computer. c) IBM vindt het probleem dat Google heeft gekozen om op te lossen een onzinnig probleem. d) IBM zegt dat de vergelijkingscomputer van Google geen disk memory gebruikt.

4) Waardoor kon de Wana Crypt0r software zo goed devices infecteren?
a) Vanwege een fout in het SMB protocol van windows. b) Omdat veel IoT devices met een standaard wachtwoord werden geleverd. c) Vanwege een incorrecte implementatie van de double pulsar bij veel windows devices. d) Door misbruik te maken van de macro's in Microsoft Office software.

5) Welk van de volgende termen zit *niet* in de OWASP top 10?
a) Sensitive Data Exposure. b) Unvalidated Redirects. c) Cross-site scripting. d) SQL injections.

6) Een klein, gesloten cryptocurrencynetwerk kan in totaal 1789100 hashes per seconde berekenen. Wat is de *beste* keuze voor de target t van de hashpuzzel?
a) $t = 2^{224}$ b) $t = 2^{225}$ c) $t = 2^{226}$ d) $t = 2^{227}$.

7) Bob stuurt Alice berichten via een RSA-connectie in een groep $\mathbb{Z}_m^*$ waarbij de modulus k bits heeft. Hoe veel tijdsstappen kost het Alice om het bericht van Bob te ontsleutelen? Geef het *meest passende* antwoord.
a) k^2 stappen. b) $\frac{1}{4}k^3$ stappen. c) $\frac{1}{8}k^3$ stappen. d) k^3 stappen.

8) Alice ondertekent een aandelenaankoopopdracht M met een handtekening S. Bob koopt de aandelen voor Alice, maar als de volgende dag de koers gedaald is, ontkent Alice de opdracht te hebben gegeven. Welke eigenschap van een handtekening stelt Bob in staat om Alice toch aansprakelijk te houden?
a) Authenticiteit. b) Integriteit. c) Onloochenbaarheid. d) Confidentialiteit.

9) Stel dat Eve toegang krijgt tot alle rekenkracht van Google en dat zij besluit die rekenkracht los te laten op het bitcoin netwerk. Wat voor schade kan Eve aanrichten?
a) Een 51% attack. b) Eve kan het geld van anderen uitgeven. c) Een Denial of Service Attack. d) Inflatie.

10) Bob probeert wortel te trekken in $\mathbb{Z}_{pq}^*$ zonder dat hij kennis heeft van p en q. Welk statement is waar?
a) Dit is onmogelijk. b) Dit is mogelijk als pq een blum-integer is. c) Dit kost minimaal exponentiele tijd. d) Dit is practisch onmogelijk.