Examenvragen

Information Security: Fundamentals

Nero Vanbiervliet

12 december 2017

0-Inleiding

1. Gegeven een caesarcijfer dat als alfabet de cijfers 0-9 gebruikt. Welke getallen kunnen hiermee niet gecodeerd worden?
   A. getallen groter dan 9999
   B. binaire getallen
   C. negatieve getallen
   D. oneven getallen

2. Gegeven een caesarcijfer dat gebruik maakt van een alfabet met 26 elementen (bv. a-z). De boodschap 'security' (8 tekens) wordt gecodeerd met dit caesarcijfer met rotatie 3. Wat kan je zeggen over de cijfertekst van ditzelfde woord, maar met rotatie 29?
   A. niets, de cijfertekst is onvoorspelbaar
   B. de cijfertekst zal anders zijn
   C. de cijfertekst zal hetzelfde zijn
   D. de cijfertekst zal 29 tekens lang zijn

3. Gegeven een caesarcijfer met bronalfabet a-z (26 tekens) en rotatie 12. Wat is de sleutel?
   A. 12
   B. 26
   C. caesarcijfer
   D. de sleutel is in het voorbeeld nog niet gekozen

4. Is frequentieanalyse toepasbaar op het caesarcijfer en op enigma?
   A. Ja, op beide
   B. Nee, op geen van beide

C. Enkel op het caesarcijfer

D. Enkel op enigma

5. Stel dat een wachtwoord de letters abcdefgh, de cijfers 123 en de tekens !? mag bevatten. Het wachtwoord moet uit exact 6 karakters bestaan. Hoeveel mogelijke wachtwoorden zijn er? (Extra vraag (apart op te lossen als doordenker): hoeveel mogelijkheden zijn er als het wachtwoord ook minder dan 6 tekens mag bevatten)

   A. $26^8 \times 10^3 \times 2^2$

   B. 13^6

   C. 6^{38}

   D. Oneindig veel

6. Stel dat een wachtwoord uit zes cijfers bestaat (0-9). Een computer kan 1000 mogelijkheden per seconde testen als brute force aanval. Hoeveel tijd (in seconden) heeft de computer nodig om alle mogelijkheden te testen?

   A. $6^{10}/1000$

   B. $1000/6^{10}$

   C. $10^6/1000$

   D. $1000/10^6$

1-Algemene principes

CIA

1. De batterij van Bob zijn telefoon is leeg dus hij kan zijn mails niet meer lezen. Welke eigenschap(pen) geldt niet?

   A. Availability

   B. Confidentiality

   C. Integrity

   D. Availability en Integrity

2. Door een bug in facebook kunnen alle mensen met dezelfde naam elkaars berichten lezen.

   A. Availability

   B. Confidentiality

   C. Availability en integrity

   D. Confidentiality en Integrity

3. Bob kan zijn examenresultaten niet raadplegen op toledo omdat iemand geprobeerd heeft 10 keer in te loggen op zijn account. Zijn account is vergrendeld en er staat dat hij de IT dienst van thomasmore moet contacteren om terug toegang tot zijn account te krijgen.
   A. Availability
   B. Confidentiality
   C. Integrity
   D. Availability en Integrity
4. Alice gebruikt een adblocker. Hierdoor worden de advertenties op alle webpagina's die ze bezoekt niet weergegeven.
   A. Availability
   B. Confidentiality
   C. Integrity
   D. Availability en Integrity

Access Control

1. Bob typt zijn wachtwoord in op zijn computer van het werk. Welke stap in het proces van toegangscontrole (access control) is dit?
   A. Identificatie
   B. Authenticatie
   C. Authorisatie
2. Een symmetric token bestaande uit 7 getallen [0-9] verandert om de 60 seconden. Een aanvaller kan 3 tokens raden per seconde. Wat is de kans dat een aanvaller binnen de 30 seconden binnen geraakt bij de bank?
   A. $10^7/30 \times 3$
   B. $10^7 \times 30 \times 3$
   C. $3/30/10^7$
   D. $3 \times 30/10^7$
3. **Leg uit: (10 lijntjes)** wat is het het verschil tussen een vals positef en een vals negatief in het geval van authenticatie door biometrie? Wat is de invloed van hoe streng je bent bij authenticatie op deze beide fouten en op het gebruiksgemak van de gebruiker?

Phising

1. **Leg uit (3 lijntjes)** wat phishing is en hoe je hiertegen kunt beveiligen met behulp van mutual authentication.

Secret sharing

1. Stel dat je een geheim wil delen met 5 personen. Je wil dat minimaal 3 personen nodig zijn om het gedeeld geheim te reconstrueren. Je geeft elke persoon:
   A. vijf rechten in een vlak, waarvan elke persoon er drie mag kiezen
   B. drie rechten in een vlak
   C. een vlak in een 3D ruimte
   D. vijf vlakken in een 3D ruimte

2. Stel dat je een geheim wil delen met 3 personen. Je wil dat minimaal 1 persoon nodig is om het gedeeld geheim te reconstrueren. Je geeft elke persoon:
   A. een rechte in een vlak
   B. een vlak in een 3D ruimte
   C. een punt in een vlak
   D. een punt in een 3D ruimte

3. Stel dat je een geheim wil delen met 2 personen (Bob en Alice). Je wil dat je allebei nodig bent om het gedeeld geheim te reconstrueren. Je krijgt dus allebei een rechte in een vlak. De rechten zijn van de vorm y = Ax + B, waarbij de coefficiënten A en B elk een een getal zijn van 12 cijfers [0-9]. De gedeelde code wordt bepaald als de 4 cijfers na de komma van de x-coordinaat van het snijpunt van de rechten. Bob wil nu het gedeeld geheim kraken zonder dat Alice het weet. Hij kent dus enkel zijn eigen rechte, niet die van Alice. Hoeveel mogelijkheden moet Bob proberen om het gedeeld geheim zeker te vinden?
   A. 10^{24}
   B. 12^9
   C. 10^4
   D. 10^{28}

4. Stel dat je een geheim wil delen met 2 personen (Bob en Alice). Je wil dat je allebei nodig bent om het gedeeld geheim te reconstrueren. Je krijgt dus allebei een rechte in een vlak. De rechten zijn van de vorm y = Ax + B, waarbij de coefficiënten A en B elk een een getal zijn van 2 cijfers [0-9]. De gedeelde code wordt bepaald als de 8 cijfers na de komma van de x-coordinaat van het snijpunt van de rechten. Bob wil nu het gedeeld geheim kraken zonder dat Alice het weet. Hij kent dus enkel zijn eigen rechte, niet die van Alice. Hoeveel mogelijkheden moet Bob proberen om het gedeeld geheim zeker te vinden?
   A. 10^2
   B. 10^4
   C. 10^8
   D. oneindig veel

Encryptie

1. Het caesarcijfer is een voorbeeld van symmetrische encryptie:
   A. Ja
   B. Nee
   C. Hangt af van welke sleutel gebruikt wordt
   D. Hangt af van welk bronalfabet gebruikt wordt

2. Welke uitspraak over asymmetrische encryptie klopt **niet**:
   A. Je private sleutel moet je geheim houden
   B. Je publieke sleutel mag je doorgeven aan de persoon waarmee je veilig wil communiceren
   C. Je publieke sleutel mag je doorgeven aan een aanvaller die kan meeluisteren met de communicatie
   D. Je private sleutel mag je doorgeven aan de persoon waarmee je veilig wil communiceren

3. Om een boodschap te versleutelen met asymmetrische encryptie, gebruik je je private key.
   A. Juist
   B. Fout, je hebt ook de private key van de andere persoon nodig
   C. Fout, je hebt de private key van de andere persoon nodig
   D. Fout, je hebt ook de public key van de andere persoon nodig

4. Duid aan wat klopt. Om een boodschap te versleutelen met asymmetrische encryptie, gebruik je:
   A. Je eigen private key
   B. Je eigen public key
   C. De private key van de persoon voor wie je de boodschap wil versleutelen
   D. De public key van de persoon voor wie je de boodschap wil versleutelen

5. Een boodschap is asymmetrisch vercijferd. Wie kan deze boodschap nu ontcijferen?
   A. Alle houders van de private key
   B. Alle houders van de public key
   C. De persoon die de boodschap vercijferd heeft
   D. Iedereen, behalve de persoon die het vercijferd heeft

6. Alice wil graag een bericht vercijferen met asymmetrische encryptie om het veilig te versturen naar Bob en Carol. Hoeveel paar keys (private en public) zijn er nodig

A. 1

B. 2

C. 3

D. 4

7. Wat is de juiste uitspraak over een digitale handtekening en een digitale vingerafdruk?

   A. Een digitale handtekening maakt gebruik van een hashfunctie, een vingerafdruk niet

   B. Om een vingerafdruk te verifiëren, heb je een sleutel nodig

   C. Voor het plaatsen van een digitale vingerafdruk is een sleutel nodig, voor het maken van een handtekening niet

   D. Voor het plaatsen van een handtekening is een sleutel nodig, voor het maken van een vingerafdruk niet

Hashfunctie

1. Welke uitspraak over hashfuncties is fout?

   A. Hashwaardes hebben een vaste lengte

   B. Je hebt een private sleutel nodig om een hashwaarde te berekenen

   C. In de praktijk kan uit een hashwaarde niet terug het originele bestand gerecupereerd worden

   D. Hashfuncties kunnen gebruikt worden om een digitale vingerafdruk te maken

2. **Leg uit (3 lijntjes)** hoe maak je een vingerafdruk van een bestand met een hashfunctie? Hoe kan een andere persoon een vingerafdruk controleren? Welke eigenschap van de informatie wordt door de vingerafdruk beschermd? Confidentiality, Integrity of Availability?

2-Wetgeving

1. **Leg uit (3 lijntjes):** de GDPR is een verordening (regulation). Wat betekent dit? Wat is het verschil met een richtlijn (directive)?

2. In welk geval is de GDPR **niet** van toepassing?

   A. De controller en de processor bevinden zich in de EU. Het individu bevindt zich ook in de EU.

   B. De controller en de processor bevinden zich niet in de EU. Het individu bevindt zich wel in de EU.

   C. De controller en de processor bevinden zich in de EU. Het individu bevindt zich niet in de EU.

D. De controller en de processor bevinden zich niet in de EU. Het individu bevindt zich ook niet in de EU.

3. Het is het jaar 2020. Een organisatie wil persoonsgegevens verwerken. Welke van volgende opties is geen wettelijke basis voor het verwerken van persoonsgegevens volgens de GDPR?
   A. de verwerking is nodig om te voldoen aan een overeenkomst (contract)
   B. toestemming van de gebruiker
   C. de persoonsgegevens waren al aanwezig in de organisatie vanaf voor mei 2018 (dus voor de GDPR geldig was)
   D. de verwerking is nodig voor het algemeen belang

4. **Leg uit (3 lijntjes):** wanneer er een gebruiker surft naar thomasmore.be komt er bovenaan de pagina een bericht 'door deze website te gebruiken, geeft u toestemming voor het verwerken van uw persoonsgegevens'. Is dit een geldige wettelijke basis? Waarom wel/niet?

3-Web security

1. In het veiligheidsmodel voor web security hebben we verondersteld dat we de client (web browser) niet kunnen vertrouwen. Waarom? Illustreer aan de hand van een voorbeeld (10 lijntjes).

4-Netwerk

1. **Leg uit:** wat is het nut van een cache (tijdelijk geheugen) bij een DNS resolver? Wat is de TTL (time-to-live)?

2. **Leg uit:** wat is cache poisoning? Maak een tekening/schema om je antwoord duidelijker te maken.

3. **Leg uit:** waarom wordt cache poisoning moeilijker om uit te voeren wanneer de resolver een Query ID (QID) en een poortnummer gebruikt?

4. Eve wil een cache poisoning aanval uitvoeren op een resolver. De resolver maakt gebruik van een Query ID (QID) en een poort waaraan het antwoord op zijn DNS request moet voldoen. Stel dat het QID uit 6 cijfers bestaat [0-9] en enkel poortnummers vanaf 100 tot 200 zijn mogelijk. Eve kan 100 valse DNS antwoorden aan de resolver geven per seconde. Als je weet dat de echte DNS server antwoordt na 4 seconden, wat is dan de kans dat Eve slaagt in de cache poisoning aanval?
   A. $10^8/4/100$
   B. $(10^6 + 10^2)/4/100$
   C. $4 \times 100/10^8$
   D. $4 \times 100/(10^6 + 10^2)$

5. **Leg uit:** hoe kunnen additional resource records bij DNS gebruikt worden voor Dan Kaminksky's aanval?

6. Waarom is een packet filter firewall vaak niet voldoende om een applicatie te verbieden om verbinding te maken met bv. een server?

   A. Een applicatie kan de poort die hij gebruikt om verbinding te maken steeds aanpassen, tot hij een poort vindt die niet geblokkeerd wordt door de packetfilter.

   B. Een packet filter houdt geen packetjes tegen, hij rapporteert enkel als er een verdacht pakketje is.

   C. Een packet filter firewall blokkeert enkel verkeer van buiten naar binnen, niet omgekeerd

   D. Een packet filter houdt enkel HTTP verkeer tegen, geen andere protocols zoals peer-to-peer

7. **Leg uit:** hoe werkt een TLS handshake? Leg de verschillende stappen uit.

8. **Leg uit:** wat is een man-in-the-middle (MITM)? Kun je hiervan slachtoffer zijn als je HTTP gebruikt? Kun je hiervan slachtoffer zijn als je https (HTTP + SSL/TLS) gebruikt?

9. **Leg uit: Wat zijn de drie hoofelementen van een certificaat?**

10. **Leg uit (3 lijntjes):** wat is certificate revocation?

11. **Leg uit (10 lijntjes):** wat is de PKI en waarvoor dient dit?

12. Tegen welk gevaar beschermt end-to-end encryption je **niet**? Veronderstel dat je zeker bent dat de public key van de tegenpartij klopt en niet die van een aanvaller is.

    A. wanneer in de server ingebroken wordt, kan gevoelige data door de hacker gelezen worden

    B. iemand onderschept je boodschap op het netwerk

    C. iemand hacket je telefoon en leest je berichten

    D. een hacker voert een man-in-the-middle aanval uit

13. **Leg uit (3 lijntjes):** wat is het voordeel van een (D)DoS aanval wanneer deze gebruikt wordt bij een DNS cache poisoning aanval?

14. **Leg uit (10 lijntjes):** hoe werkt de inlogprocedure om je aan te melden bij een website wanneer de server de wachtwoorden gehashet heeft met salt.

15. **Leg uit (10 lijntjes)** hoe een woordenlijst aanval werkt

16. **Leg uit (10 lijntjes) hoe SQL injectie werkt**

6-Client

1. Eve stuurt Bob een facebookbericht met daarin een stukje javascript <script>...</script>. Wanneer Bob het bericht leest, is de XSS aaval gelukt. Is dit een voorbeeld van stored of reflected XSS?
   A. Stored
   B. Reflected
   C. Het kan allebei zijn
   D. Geen van beide, dit is een voorbeeld van CSRF
2. **Leg uit (10 lijntjes)** aan de hand van een voorbeeld wat stored XSS is.
3. **Leg uit (10 lijntjes)** aan de hand van een voorbeeld wat reflected XSS is.
4. Cookie stealing is een toepassing van
   A. XSS
   B. CSRF
   C. DNS cache poisoning
   D. DoS aanval
5. **Leg uit (3 lijntjes)** waarom XSS en SQL injection op een gelijkaardige manier kunnen beveiligd worden door de server.
6. **Leg uit (3 lijntjes)** hoe je kunt beschermen tegen CSRF door maatregelen op de server.
7. Een same-origin code policy zegt dat een script enkel mag connecteren met het domein waar het vandaan komt (de origin). Welke van volgende elementen is geen criterium voor de origin?
   A. hostname bv. thomasmore.be
   B. pagina bv. /index.php
   C. poortnummer bv. 80
   D. protocol bv. HTTP

7-Bitcoin

1. Welk element is onmisbaar in een bitcoin wallet?
   A. de naam van de eigenaar
   B. het ip adres van een miner
   C. de private sleutel
   D. een kopie van de blockchain

2. **Leg uit (3 lijntjes):** is bitcoin een client-server systeem of een peer-to-peer syteem? Wat is een voordeel hiervan?

3. (10 lijntjes) Bespreek twee voordelen en één nadeel van bitcoin ten opzichte van traditionele betaalsystemen.

4. Het ledger (grootboek) in bitcoin is een overzicht van hoeveel bitcoins elke private key toebehoren. Hoe kun je dit ledger raadplegen op het bitcoin netwerk?
   A. dit kun je opstellen door alle transacties uit de blockchain te overlopen tot op heden. Dan weet je hoeveel bitcoins bij elke wallet horen.
   B. om dit te kennen zou je aan elke eigenaar van een wallet moeten vragen hoeveel bitcoins hij bezit
   C. er is niet één ledger, verschillende miners hebben een eigen versie van het ledger, die elke lichtjes verschillen van elkaar
   D. de miner berekent dit ledger wanneer je dit vraagt in ruil voor een betaling in bitcoins

5. Bob stuurt Eve 0.01 BTC. Hoe kan een miner controleren dat Bob wel degelijk deze transactie wil uitvoeren en dat Eve niet deze transactie gemaakt heeft in Bob zijn naam?
   A. de miner blijft hashwaardes van een block berekenen tot hij een hashwaarde met voldoende nullen heeft. Dan weet hij dat de transactie geldig is.
   B. dit is een zwakheid van het bitcoin netwerk. Er is geen manier om zeker te zijn dat een transactie geldig is
   C. 2-factor authentication wordt gebruikt: Bob moet via een sms-code bevestigen dat hij de transactie wil doen
   D. de miner kan met de publieke sleutel van Bob controleren of de handtekening op de transactie klopt

6. **Leg uit (10 lijntjes):** Wat is de difficulty in het bitcoin netwerk. Waarom moet deze steeds veranderen?

7. **Leg uit (3 lijntjes):** Hoe worden miners beloond voor het werk dat ze leveren voor het bitcoin netwerk?

8. Wat is het nut van mining pools?
   A. miners werken samen om het risico van minen te spreiden
   B. miners werken samen om meer hashwaardes te kunnen berekenen samen, zodat ze meer blocks vinden en dus allemaal meer verdienen
   C. miners werken samen om de difficulty laag te houden
   D. miners werken samen om de fees (fooi) van transacties te verhogen, zodat ze meer verdienen

9. **Leg uit (3 lijnen):** Wat zijn zogenaamde altcoins en waarom is het nuttig om deze te ontwikkelen als bitcoin al bestaat?

8-Informatiebeveiliging in organisaties

1. Leg uit (3 lijntjes) waarom het belangrijk is in een organisatie om de werknemers bewust te maken van waarom een maatregel nodig is voor de veiligheid van de organisatie.

2. (3 lijntjes) Geef twee manieren hoe je kan kijken naar een vertrouwd systeem in een organisatie.

3. De laptop van bedrijfsleider Bart bevat de private keys van de bitcoin wallet van het bedrijf. Wanneer de harde schijf van Bart zijn pc crashet, kunnen deze bitcoins dus verloren gaan. Bart heeft immers geen backup van deze private keys. Met welke term kun je de private keys in dit voorbeeld beschrijven?

   A. asset

   B. threat

   C. vulnerability

   D. risk

4. (10 lijntjes) Wat zijn de drie manieren om een risico te beheren in een organisatie. Illustreer je uitleg aan de hand van één groot voorbeeld waar je alles aan koppelt.

5. Het intelligente beveligingssysteem van bedrijf X heeft gedetecteerd dat iemand zonder toestemming zich in de server room bevindt. Iemand van de bewakingsdienst wordt naar de server room gestuurd om die persoon daar weg te halen. Is het doel van deze maatregel:

   A. preventie

   B. detectie

   C. repressie

   D. correctie

Overzichtsvragen

1. (3 lijntjes) Geef een voorbeeld van een situatie uit de cursus waar we op iemand/iets vetrouwen om de veiligheid van de informatie te garanderen. Geef ook een voorbeeld van een situatie waarin we iemand bewust niet vertrouwen.

2. (10 lijntjes) Geef drie voorbeelden uit de cursus waarbij er een tradeoff gebeurt tussen security en gebruiksgemak.