

Fundamental concepts

Introductie 13

Leerkern 14

- 1 Fundamental Concepts 14
 - 1.1 Confidentiality, Integrity, and Availability 14
 - 1.2 Assurance, Authenticity, and Anonymity 15
 - 1.3 Threats and Attacks 17
 - 1.4 Security Principles 17

Terugkoppeling 18

- 1 Uitwerking van de opgaven 18

Leereenheid 1

Fundamental concepts

INTRODUCTIE

IT security is een breed vakgebied. Daarin spelen niet alleen technische aspecten uit de informatica een rol, maar ook aspecten uit de gedragswetenschappen (zoals criminologische en psychologische aspecten), de maatschappijwetenschappen (zoals juridische en sociologische aspecten) en de managementwetenschappen (zoals bedrijfskundige en economische aspecten). De focus van deze cursus is echter geheel op informatica en techniek gericht.

In deze inleidende leereenheid komen diverse basisconcepten aan de orde. Allereerst brengen we de verschillende doelen in kaart die we met IT security proberen te bereiken. Vervolgens kijken we naar bedreigingen en aanvallen die een gevaar vormen voor het behalen van deze doelen. Tot slot kijken we naar een aantal belangrijke security-principes.

LEERDOELEN

Na het bestuderen van deze leereenheid wordt verwacht dat u

- de betekenis van de termen confidentiality, integrity en availability kunt uitleggen
- enkele maatregelen kunt noemen waarmee confidentiality, integrity en availability kunnen worden gerealiseerd
- de betekenis van de termen assurance, authenticity en anonymity kunt uitleggen
- bedreigingen en aanvallen als een vorm van eavesdropping, alteration, denial-of-service, masquerading, repudiation of correlation/traceback kunt typeren
- de principes van economy of mechanism, fail-safe defaults, complete mediation, open design (security by obscurity), separation of privilege, least privilege, least common mechanism, psychological acceptability, work factor, compromise recording, adequate protection en timeliness kunt uitleggen.

Studeeraanwijzing

In deze leereenheid gebruiken we sectie 1 'Fundamental Concepts' (pagina 2 tot en met 18) uit hoofdstuk 1 'Introduction' van het tekstboek. Deze leereenheid geeft veelal een impressie van diverse onderwerpen die later uitvoeriger aan bod komen. Voor een deel kunt u volstaan met het doorlezen ervan. Een aantal onderwerpen is verplichte stof, zoals aangegeven in de hierboven genoemde leerdoelen. Deze leereenheid bevat geen zelftoets.

De studielast van deze leereenheid bedraagt circa 4 uur.

LEERKERN

1 Fundamental Concepts

De introductie van sectie 1 ‘Fundamental Concepts’ op pagina 2 van het tekstboek is niet meer dan een eerste inleiding. Het volstaat om deze introductie oppervlakkig door te lezen. Begrippen zoals cryptographic primitives, vulnerabilities en attacks worden later in de cursus nader uitgelegd.

1.1 CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY

In deze sectie worden drie elementaire begrippen uitgelegd: confidentiality, integrity en availability. Als afkorting hiervoor wordt vaak het acroniem CIA gebruikt. Dit acroniem heeft in deze context niets te maken met de Amerikaanse inlichtingendienst CIA (Central Intelligence Agency), al is het wel treffend dat beide betekenissen van CIA gerelateerd zijn aan security. In het Nederlands worden deze begrippen respectievelijk aangeduid met vertrouwelijkheid (of confidentialiteit), integriteit en beschikbaarheid, met als gangbaar acroniem BIV (voor beschikbaarheid, integriteit en vertrouwelijkheid).

*Confidentiality**Cryptografie**Cryptologie**Klare tekst
Cijfertekst**Vercijferen
Ontcijferen
Cijfer**Sleutels*

In de tweede alinea op pagina 4 worden de termen ‘cryptography’ en ‘cipher’ gebruikt. De term *cryptografie* is afkomstig uit het Grieks en betekent letterlijk geheimschrift. Cryptografie is een onderdeel van de *cryptologie*, de wetenschap die zich bezighoudt met het beveiligen van informatie door middel van coderen en decoderen. Het doel van cryptografie is om een leesbaar of betekenisvol bericht (ook wel aangeduid als het bericht in *klare tekst*) om te zetten naar een bericht in geheimschrift (ook wel aangeduid als het bericht in *cijfertekst*). Het coderen van een bericht van klare tekst naar cijfertekst wordt aangeduid als *vercijferen* of *versleutelen*. Het decoderen van een bericht van cijfertekst naar klare tekst wordt aangeduid als *ontcijferen* of *ontsleutelen*. Een cipher, een *cijfer*, is een methode van vercijferen en ontcijferen. Daarbij spelen niet alleen algoritmes een rol die beschrijven hoe de vercijfering en ontcijfering worden uitgevoerd, maar ook zogenaamde *sleutels* die de werking van deze algoritmes sturen. Cryptografie neemt een centrale plaats in bij het beveiligen van gegevens en is de laatste jaren steeds prominenter geworden. In de leereenheden 3 tot en met 5 komt cryptografie uitvoerig aan bod.

Op pagina 4 en 5 worden concepten opgesomd waarmee confidentialiteit verkregen kan worden: encryption, access control, authentication, authorization en physical security. Ook deze concepten komen later in de cursus uitvoeriger aan bod (met uitzondering van physical security: dat is weliswaar het onderwerp van hoofdstuk 2 ‘Physical Security’ in het tekstboek, maar dat hoofdstuk behoort niet tot de leerstof van de cursus).

Availability

Het doel van IT security is om confidentialiteit, integriteit en beschikbaarheid te waarborgen. In de praktijk is het echter onmogelijk om deze drie doelen gelijktijdig te bereiken. Er is daarom altijd sprake van een compromis, waarbij voor een of meerdere doelen water bij de wijn moet worden gedaan. Het voorbeeld van informatie die is opgeslagen in een bewaakte kluis op een onherbergzame locatie, illustreert dat. De confidentialiteit en integriteit zijn daar in hoge mate gegarandeerd, maar de beschikbaarheid van de gegevens is zeer beperkt. Als de beschikbaarheid van de gegevens wordt verbeterd, zal dat echter een verslechtering van de confidentialiteit en/of integriteit tot gevolg hebben. Dit is in feite de hoofdoorzaak waarom 100% security onhaalbaar is. Het beste dat we kunnen doen is proberen om 100% security te benaderen door de drempels (security-maatregelen) voor kwaadwillenden zo hoog mogelijk maken. Hoge drempels maken het voor kwaadwillenden lastiger, maar niet onmogelijk om die drempels te nemen. Daarnaast geldt meestal dat hoe hoger de drempels, hoe hoger de kosten daarvoor. Bij het nemen van security-maatregelen moet er altijd op worden gelet dat de kosten voor beveiliging in verhouding staan tot de waarde van datgene wat moet worden beveiligd.

OPGAVE 1.1

Wat is in de volgende voorbeelden in het geding: confidentiality, integrity of availability?

- Uw buurman schrijft tijdens een tentamen de uitwerking van een opgave van u over en levert die in als eigen werk.
- U maakt met een overschrijvingsformulier € 100,- over naar een goed doel. Als de bank het formulier ontvangt, is het bedrag veranderd in € 1000,-.
- Op uw werk heeft een onbekende ervoor gezorgd dat uw pc is gecrasht.

1.2 ASSURANCE, AUTHENTICITY, AND ANONYMITY

Assurance

Weblink

Het begrip assurance, dat zekerheid betekent in de context van IT security, geeft aan in hoeverre er vertrouwen kan worden gesteld in een systeem. Een wat formelere omschrijving van assurance wordt gegeven door Brian Snow in het artikel 'We need assurance!' (in IEEE Proceedings 21st Annual Computer Security Applications Conference (ACSAC), 2005). Volgens Snow bestaat assurance uit activiteiten die aantonen dat we erop kunnen vertrouwen dat

- de security policy (de eisen aan de beveiliging) van een systeem intern consistent is en voldoet aan de eisen van de organisatie die het systeem gaat gebruiken
- er voldoende beveiligingsfuncties aanwezig zijn om de security policy te ondersteunen

- het systeem precies die functies uitvoert die het moet uitvoeren, en niet meer
 - alle functies correct geïmplementeerd zijn
 - de assurance van kracht is gedurende de vervaardiging, oplevering en de gehele levensduur van het systeem.
- Dit is te bereiken door gebruik te maken van gestructureerde ontwerp-processen, goede documentatie en testen. Hoe meer zekerheid we willen, hoe omvangrijker ontwikkelproces, documentatie en testen worden.

Evaluatie en certificatie

Er zijn veel methoden en technieken om assurance te verkrijgen, zoals het uitvoeren van security reviews, testen en formele verificatie. De meeste gebruikers van computersystemen zijn echter geen security-experts en hebben ook niet de kennis, tijd en middelen om een onderbouwde uitspraak over assurance te kunnen doen. Het kan daarom handig zijn om een onafhankelijke derde partij in de arm te nemen die wel een gefundeerde uitspraak over de assurance van een systeem kan doen. Om dit te reguleren zijn er zogenaamde *evaluatie- en certificatiestandaarden* ontwikkeld, die voorschrijven op welke wijze en aan de hand van welke criteria een objectief en reproduceerbaar oordeel over de assurance van een bepaald systeem kan worden opgesteld. De meest gangbare internationale standaard is tegenwoordig ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation (afgekort tot Common Criteria of CC). Een systeem evalueren en certificeren is een niet-vanzelfsprekende aangelegenheid, die tijd en geld kost. Certificeringen worden uitgevoerd door onafhankelijke organisaties, in Nederland bijvoorbeeld door Brightsight en TNO. Veel overheden en bedrijven stellen tegenwoordig een certificering verplicht voor met name besturingssystemen, databases en security-systemen.

Authenticity

Identificatie

Authenticatie is de stap die gewoonlijk volgt op identificatie. *Identificatie* is de handeling waarbij een entiteit (bijvoorbeeld een persoon of een systeem) aangeeft wat zijn identiteit is. Authenticatie is de handeling waarbij wordt nagegaan of die identiteit correct is. Populair gezegd: bij identificatie geeft u aan wie u bent; bij authenticatie wordt geverifieerd of u inderdaad diegene bent die u zegt te zijn. Een paspoort is een identiteitsbewijs, een authenticatiemiddel waarmee uw identiteit kan worden vastgesteld. Bij inloggen wordt vaak de combinatie van een gebruikersnaam en een wachtwoord gebruikt. De gebruikersnaam zorgt dan voor de identificatie (aangeven wie u bent) en het wachtwoord voor de authenticatie (controleren dat u het echt bent). Authenticatie kan plaatsvinden op basis van iets dat u weet (bijvoorbeeld een wachtwoord of pincode), iets dat u bent (bijvoorbeeld een vingerafdruk of irisscan), iets dat u bezit (bijvoorbeeld een smartcard of sleutel), iets dat u doet (bijvoorbeeld de snelheid waarmee u typt op een toetsenbord en de tijdsintervallen tussen toetsaanslagen), of waar u zich bevindt (bijvoorbeeld aan de hand van GPS-coördinaten of een IP-adres). Om de zekerheid in correcte authenticatie te vergroten, wordt in toenemende mate *multi-factor-authenticatie* toegepast, waarbij authenticatie op meerdere manieren plaatsvindt. Voorbeelden zijn een smartcard die pas geactiveerd wordt als u de juiste pincode intikt, of toegang tot een gebouw die pas wordt verleend nadat eerst uw toegangspasje en vervolgens uw irisscan zijn gecontroleerd.

Multi-factor-authenticatie

OPGAVE 1.2

Het is niet alleen mogelijk dat dingen die u bezit worden gestolen, maar ook biometrische gegevens die aanduiden wie u bent. Een voorbeeld is het kopiëren van vingerafdrukken. Leg uit waarom gestolen biometrische gegevens vervelender zijn dan bijvoorbeeld een gestolen wachtwoord of bankpas.

Na identificatie en authenticatie is de volgende stap autorisatie, waarbij toegang tot resources wordt verleend.

1.3 THREATS AND ATTACKS

OPGAVE 1.3

Bij een man-in-the-middle attack nestelt een kwaadwillende zich in het pad tussen zender en ontvanger. Zo'n man-in-the-middle kan verschillende aanvallen uitvoeren. In het tekstboek wordt alteration als voorbeeld genoemd. Hoe zou een man-in-the-middle ook de andere aanvallen die in sectie 1.3 worden genoemd, kunnen uitvoeren?

1.4 SECURITY PRINCIPLES

Principles van adequate protection en timeliness

Naast de tien security-principles die door Saltzer en Schroeder worden genoemd, zijn er ook andere belangrijke security-principles. Zo merkten we in sectie 1.1 op dat er bij het nemen van security-maatregelen op moet worden gelet dat de kosten voor beveiliging in verhouding staan tot de waarde van datgene wat moet worden beveiligd. Dit staat bekend als *principle of adequate protection*. Een ander principe dat hiermee verband houdt, is *principle of timeliness*. Dat principe stelt dat een security-maatregel zolang van kracht moet zijn als het te beveiligen object waarde heeft. Een voorbeeld is het strategisch plan van een bedrijf om een concurrent over te nemen. Om bijvoorbeeld speculatie op de beurs tegen te gaan, mag die informatie niet uitlekken en moet ze daarom adequaat worden beschermd, totdat de overname is afgerond en bekend wordt gemaakt.

OPGAVE 1.4

Welk van de security-principles van Saltzer en Schroeder is (enigszins) gerelateerd aan het principe van adequate protection?

TERUGKOPPELING

1 **Uitwerking van de opgaven**

- 1.1 a Als er gespiekt wordt, is de vertrouwelijkheid (confidentiality) in het geding. Het gemaakte werk, de tentamenopgave, is in deze context vertrouwelijk.
b Het overschrijvingsformulier is veranderd en de integriteit is dus in het geding. Als u het niet op prijs stelt dat anderen weet hebben van uw overboeking, is ook de confidentiality in het geding.
c Uw pc is voor u niet meer beschikbaar, dus is de availability in het geding.
- 1.2 Een bankpas of wachtwoord zijn te vervangen, maar biometrische gegevens niet. Als geconstateerd is dat een bankpas of wachtwoord in verkeerde handen zijn gevallen, kunnen deze ongeldig worden verklaard, zodat de dief deze niet meer kan gebruiken. Aan het slachtoffer kan een nieuwe bankpas of wachtwoord worden verstrekt. Als een biometrische eigenschap zoals een vingerafdruk in verkeerde handen is gevallen, kan die niet zomaar worden vervangen. Een vingerafdruk of iris kan nog wel operatief worden gewijzigd of vervangen (al is dat erg ingrijpend voor de betrokkene), maar een DNA-profiel van een persoon is onvervangbaar.
- 1.3 Een man-in-the-middle ontvangt de berichten die de zender verstuurt, kan die berichten vervolgens manipuleren, en tot slot deze gemanipuleerde berichten naar de ontvanger doorsturen. Als de berichten in klare tekst worden verstuurd, dus niet gecijferd, kan de man-in-the-middle de inhoud van de berichten te weten komen. De aanval is dan tevens een vorm van eavesdropping waarbij de confidentialiteit in het geding is. Zoals al gesteld in het tekstboek, kan de man-in-the-middle de berichten aanpassen, wat een vorm van alteration is waarbij de integriteit in het geding is. De man-in-the-middle zou ervoor kunnen kiezen om de berichten niet naar de ontvanger door te sturen, wat een vorm van denial-of-service impliceert waarbij de beschikbaarheid in het geding is. De man-in-the-middle kan in een bericht niet alleen de inhoud aanpassen, maar ook de naam van de afzender in het bericht wijzigen. Als bijvoorbeeld Alice een bericht naar Bob verstuurt, kan de man-in-the-middle het doen voorkomen alsof het bericht door iemand anders naar Bob is verstuurd. Dit is een vorm van masquerading (spoofing) waarbij de authenticiteit in het geding is. Daarnaast kan de man-in-the-middle het bericht ook naar een andere ontvanger sturen dan door de afzender bedoeld was. Een voorbeeld is een bericht waarin een bestelling bij een webwinkel wordt gedaan. In plaats van de bestelling te plaatsen bij de webwinkel die de afzender voor ogen had, kan de man-in-the-middle in naam van de afzender de bestelling naar een andere webwinkel sturen. Dit is een vorm van repudiation waarbij de assurance in het geding is. Tot slot kan een man-in-the-middle ook een bedreiging voor anonimiteit betekenen. De afzender kan bijvoorbeeld zowel anonieme als ondertekende e-mails versturen. Doordat de man-in-the-middle ziet dat al deze e-mails van dezelfde afzendende partij afkomstig zijn, kan hij afleiden van wie de anonieme mails afkomstig zijn. Hier hebben we te maken met een vorm van correlation en traceback.



- 1.4 Het work factor principe van Saltzer en Schroeder is enigszins gerelateerd aan het principe van adequate protection. Daarbij is het uitgangspunt voor de kosten van security-maatregelen echter niet de waarde van het te beveiligen object, maar de moeite die het een kwaadwillende kost om de security-maatregel te omzeilen.