“Need-To-Know” scheiding op geheime, beveiligde netwerken bij de NATO

Eindverslag

Student	**:**	Asim Malik, 97005749
Afstudeerperiode	**:**	2004-1.1
School	**:**	Haagse Hogeschool
Sector	**:**	Informatica & Informatiekunde
Afstudeerrichting	**:**	BOIV
Examinator	**:**	Dhr. W.B. Elschot
Examinator	**:**	Dhr. T.W.M. van Gerwen
Bedrijfsmentor	**:**	Dhr. R. Malewicz
Document	**:**	Eindverslag
Datum	**:**	11-06-2004

© NC3A

Referaat

Malik, A.Z, het schrijven van een adviesrapport "Need-To-Know" scheiding op geheime, beveiligde netwerken, eindverslag van een afstudeerproject bij NC3A, te Den Haag.

Dit verslag beschrijft de werkzaamheden die door de auteur zijn uitgevoerd in het kader van zijn afstudeerproject. Het afstudeerproject omvat het schrijven van een adviesrapport over "Need-To-Know" scheiding op geheime, beveiligde netwerken. Het afstudeerproject is uitgevoerd in het kader van de eindfase van de afstudeerrichting BOIV van de opleiding Informatica & Informatiekunde (I&I), aan de Haagse Hogeschool, afdeling Informatica.

Descriptoren:

- Afdeling Informatica;
- Informatica & Informatiekunde;
- BOIV;
- NC3A;
- NTK;
- CVI.

Voorwoord

Voor u ligt het eindverslag dat ik geschreven heb naar aanleiding van mijn afstudeerproject bij NC3A te Den Haag. In het kader van de opleiding Informatica & Informatiekunde aan de Haagse Hogeschool.

Hoewel het afstuderen voornamelijk een individuele aangelegenheid is, wil ik op deze plaats een woord van dank uitspreken aan al diegenen die mij op de één of andere manier behulpzaam zijn geweest tijdens mijn afstudeerperiode.

In het bijzonder wil ik de heren R. Malewicz & C. Shawcross van NC3A bedanken voor het aanbieden van de afstudeeropdracht en voor de goede begeleiding. Ik wil ook de heer P. Groen, EDP-auditor bij PricewaterhouseCoopers (PWC), bedanken voor zijn hulp, kennis en ervaring bij het schrijven van mijn adviesrapport.

Tenslotte wil ik de heren W.B. Elschot en T.W.M. van Gerwen bedanken voor hun hulp en begeleiding vanuit de Haagse Hogeschool.

A.Z. Malik
Den Haag, 11 juni 2004

Inhoudsopgave

1. Inleiding

Dit eindverslag beschrijft het afstudeerproject 2004-1.1, dat de afstudeerperiode van 9 februari 2004 tot en met 11 juni 2004 omvat. Het afstudeerproject was het schrijven van een adviesrapport over "Need-To-Know" (NTK) scheiding op geheime, beveiligde netwerken bij NATO.

In dit eindverslag worden de werkzaamheden weergegeven, alsmede de gemaakte overwegingen en keuzes, ondervonden problemen en de oplossingen daarvoor en tenslotte de leermomenten en, achteraf gezien, opvallende zaken gedurende het afstudeerproject.

De rode draad door mijn eindverslag is als volgt: De hoofdstukken 2 en 3 bevatten mijn oriëntatie op de afstudeeropdracht en mijn leren kennen van de organisatie NC3A. Hierna beschrijf ik in hoofdstukken 6 tot en met 10 de activiteiten die ik heb uitgevoerd om tot een advies over NTK toegangsbeveiliging te komen. De gemotiveerde keuze van de methoden die een ordening in mijn activiteiten hebben bewerkstelligd, is in hoofdstuk 4 te vinden. Mijn eindverslag eindigt met een evaluatie van de procesgang en de opgeleverde producten.

Hoofdstuk 2 geeft een weergave van de voor het afstudeerproject relevante gegevens over de organisatie. Hierdoor leer ik de organisatie NC3A kennen.

Hoofdstuk 3 beschrijft de oriëntatie op mijn omgeving en de afstudeeropdracht. Zowel de probleemstelling als de doelstelling wordt uitgelegd, maar ook de sleutelterm NTK. Binnen dit hoofdstuk wordt ook de aanleiding tot de afstudeeropdracht duidelijk gemaakt.

Na de oriëntatie wordt in hoofdstuk 4 beschreven hoe ik tot de gefaseerde aanpak van literatuuronderzoek en tot het acht stappenplan van Oud[1] ben gekomen. Ook beschrijft dit hoofdstuk mijn keuze voor de projectmanagementmethode "Projectmatig werken". De methoden worden, na een korte beschrijving, met voor- en nadelen beschreven en mijn motivatie met betrekking tot mijn keuzes wordt toegelicht.

Dan volgt in hoofdstuk 5 de projectplanning van mijn afstudeerproject. Hierin wordt beschreven hoe ik tot het plan van aanpak ben gekomen en tot de definitieve opdrachtsomschrijving. Beide zijn integraal opgenomen in de bijlagen, dit evenals de Engelse opdrachtsomschrijving.

Hoofdstuk 6 beschrijft de procesgang van de gekozen gefaseerde aanpak literatuuronderzoek.

Hoofdstuk 7 start dan met een beschrijving van de eerste stap. Dit is het acht stappenplan van Oud, namelijk: stap 1 Informatiebeveiligingsbeleid. Het huidige

[1] Oud, Ernst J.: *Praktijkgids Code van Informatiebeveiliging*; Academic Service Schoonhoven; 1e druk; 2002; p. 40.

informatiebeveiligingsbeleid wordt beschreven en voor zover relevant voor mijn onderzoek getest met behulp van de criteria van een informatiebeveiligingsbeleid volgens de Code van Informatiebeveiliging (CVI).

Hoofdstuk 8 beschrijft de procesgang van stap 2 Inventarisatie van huidige situatie en in hoofdstuk 9 volgt de beschrijving van stap 3 Eisen.

Hoofdstuk 10 geeft de laatste beschrijving weer van stap 4 Ontwerp. Dit is de laatste stap binnen het voornoemde stappenplan van Oud. Deze stap Ontwerp bestaat uit drie deelstappen. Maar alleen de stappen maatregelen en procedures zijn beschreven.

In hoofdstuk 11 geef ik tot slot een Evaluatie van mijn afstudeerproject. Zowel de procesgang als de producten worden geëvalueerd.

2. Beschrijving van de organisatie NC3A

2.1 Inleiding

In dit hoofdstuk twee wordt een korte beschrijving gegeven van de organisatie, NATO Consultation Command and Control Agency (NC3A). NATO is mijn opdrachtgever maar ik ben werkzaam geweest binnen NC3A. Totaal werken er bij de NC3A 450 mensen; hiervan zijn er 320 in Den Haag gevestigd en 130 in het hoofdkwartier in Brussel. Informatie over de organisatie wordt verkregen uit een interne NC3A brochure.

2.2 Korte beschrijving van de organisatie

De rol van NC3A is de volgende[2]:

NC3A geeft wetenschappelijk advies aan NATO militairen en politieke autoriteiten.

De missie van NC3A is[3]:

- Het personeel van NC3A houdt zich bezig met het ontwerpen en implementeren van kosteneffectieve systemen om politieke en militaire functies te ondersteunen;
- De missie van de organisatie is gebruik te maken van een centrale planning om systemen te integreren, te ontwerpen en te onderhouden, technische ondersteuning en configuratie van bestaande systemen en installaties te bieden.

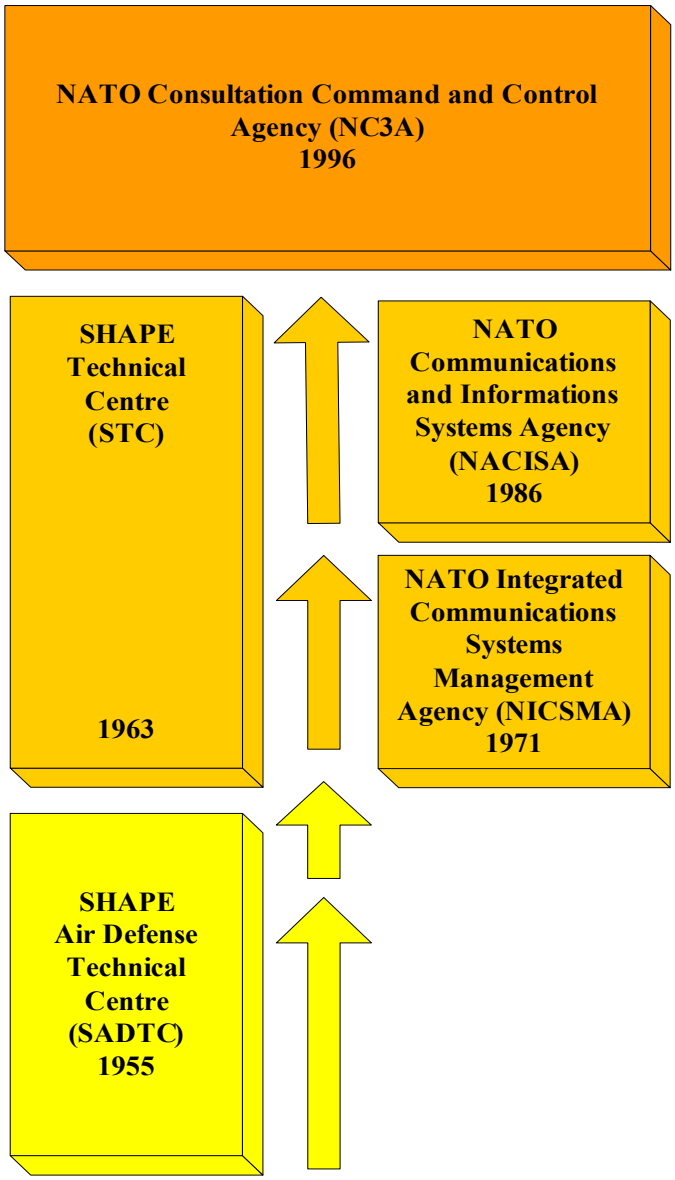
Om de rol en de missie van de NC3A te realiseren hanteert de NC3A drie richtlijnen namelijk[4]:

- Het aannemen van hoog opgeleid personeel in een omgeving waar verschillende mogelijkheden beschikbaar zijn zoals de mogelijkheid om met recente technologie te werken;
- Veelvuldig gebruik maken van gebruikers georiënteerde laboratoria. Dit gebeurt om zoveel mogelijk prototypes te ontwikkelen en te testen;
- Het aanschaffen van nieuwe systemen, die snel en simpel geïmplementeerd kunnen worden.

[2] *NC3A Brochure*; p .1.
[3] *NC3A Brochure*; p .1.
[4] *NC3A Brochure*; p .1.

2.3 Geschiedenis van de NC3A

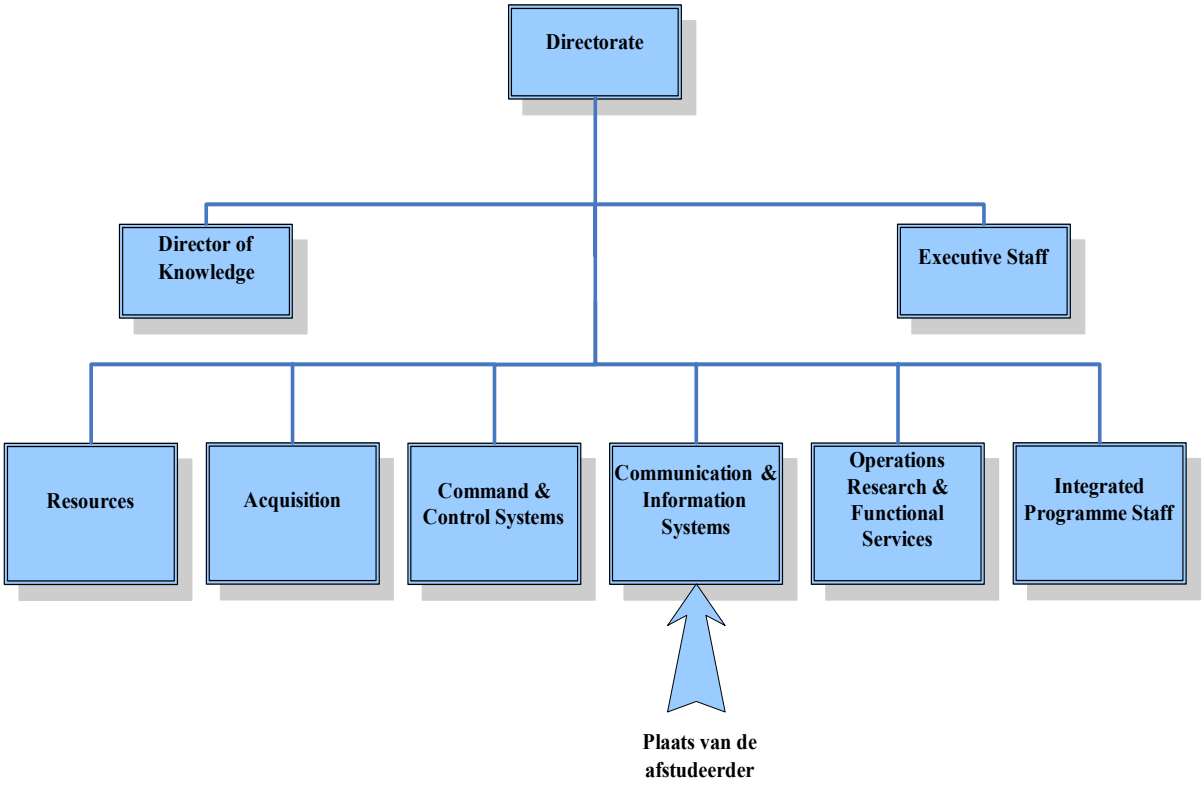
De NC3A is opgericht op 1 juli 1996 door de samenvoeging van het toenmalige SHAPE Technical Centre (STC) en de toenmalige NATO Communications en Information Systems Agency (NACISA) (zie figuur 1).



Figuur 1: Evolutie van de NC3A

2.4 Organogram van de organisatie

Om beter inzicht te krijgen in de organisatiestructuur van NC3A heb ik een organogram gemaakt[5]. De Engelse naamgeving heb ik behouden, omdat ik er de voorkeur aan heb gegeven om de werkelijke gebruikte termen te tonen. De Engelse naamgevingen, vooral de afdelingen en de functie van die afdelingen, heb ik onder het organogram uitgelegd.



Figuur 2: Organogram van de organisatie

De volgende afdelingen zijn binnen de NC3A aanwezig[6]:

- Integrated Programme Staff (IPS); Bestaat uit acht Integrated Programme Teams (IPT). Zij zijn belast met de taak om een goed samenwerkingsverband en coördinatie te bewerkstelligen binnen en buiten de organisatie;
- Operation Research and Functional Services (ORFS); ORFS houdt zich bezig met het bestuderen van toekomstige militairen concepten en benodigdheden door het ontwikkelen van prototypes voor huidige operaties;
- Communication and Information Systems (CIS); CIS levert wetenschappelijke en technische ondersteuning op het gebied van communicatie, zowel vast als mobiel.

[5] *NC3A brochure*; p. 5-6.
[6] *NC3A brochure*; p. 8-19.

CIS levert ook communicatie systemen, beveiligingssystemen en elektronische oorlogsvoering systemen. Dit is de afdeling waar ik werkzaam ben;

- Command and Control Systems (CCS); CCS levert essentiële wetenschappelijke en technische ondersteuning aan het strategisch commando en andere NATO klanten op het gebied van commando en controle technologie en sensors en surveilleren;
- Acquisition (ACQ); De ACQ brengt mensen van verschillende vakgebieden naar de NC3A. Het zijn vooral mensen met een technische achtergrond, maar ook mensen met een logistieke achtergrond;
- Resources; Resources levert ondersteuning aan andere gebieden binnen de organisatie namelijk het financiële management de ondersteuning van personeel, het systeembeheer en de servicedesk, de beveiliging en de interne diensten.

NC3A kwalificeert zich door hoog opgeleid personeel aan te nemen en die in te delen in gespecificeerde classificatieniveaus. Daarnaast vindt het werk op hoog niveau plaats. Dit gold ook voor het opstellen van het adviesrapport.

3. Oriëntatie bij NC3A

3.1 Inleiding

Na de korte beschrijving van de organisatie in het vorige hoofdstuk schets ik in dit hoofdstuk een beeld van mijn oriëntatie op de werkomgeving en de afstudeeropdracht. Voordat aan het afstudeerproject werd begonnen, moest het nodige vooronderzoek gedaan worden. Het soort organisatiecultuur binnen de NC3A wordt beschreven en de functionarissen waarmee ik zowel informeel als formeel overleg heb gevoerd, komen ook aan bod.

3.2 Oriëntatie bij NC3A

Bij aanvang van mijn afstudeerperiode oriënteerde ik me op de werkomgeving. Ik kreeg een computer die op het geheime, beveiligde netwerk aangesloten was, zonder Internet toegang. Wegens veiligheidsredenen kon ik alleen toegang krijgen tot het Internet via een aparte computer die op een apart netwerk aangesloten was. De Internet beveiligingsmaatregel vormde een hindernis voor mij. Ik kon hierdoor mijn werk niet goed uitvoeren. Aangezien er geen informatie over NTK aanwezig was op papier, was het voor mij noodzakelijk om toegang te krijgen tot het Internet om informatie te zoeken. Als oplossing kreeg ik toestemming van de bedrijfsmentor om mijn laptop als Internet computer te gebruiken. Na een grondige controle en het installeren van een virusscanner, door de servicedesk, op schadelijke programma's, virussen en Windows XP versie was dit toegestaan. Beide netwerken worden gescheiden gehouden door twee verschillende accounts als beveiligingsmaatregel.

De NC3A heeft een hiërarchische lijnstaf structuur (zie figuur 2 op p. 11). De organisatie structuur is van boven naar beneden. De afdeling CIS waar ik me bevond, is het best te omschrijven als zeer zelfstandig. De NC3A voldoet aan de typologie van Harrison en Handy, want er wordt vooral gekeken naar taken, personen, regels en macht. Daarnaast is de NC3A een rollencultuur[7], omdat de basis wordt gevormd door regels, afspraken, procedures en de hiërarchie binnen de NC3A. Verder is de rol en status van een persoon belangrijker dan prestaties. NC3A is dus met name een bureaucratische organisatie. De rapportages, systemen en spreektaal binnen de NC3A zijn in het Engels. Beveiliging speelt een grote rol. Zonder een bepaald classificatieniveau mag niemand het gebouw in.

Het zelfstandig werken was niet altijd ideaal; ik kreeg niet regelmatig genoeg feedback op mijn werk. Hierdoor wist ik niet of ik op het goede spoor zat. Dit werd na enige weken opgelost. In een gesprek tussen mijn bedrijfsmentor, zijn manager en mij werd afgesproken dat er wekelijks door mij aan genoemde personen een statusrapport, in het

[7] Alblas, Gert/ Wijsman, Ella: *Gedrag in Organisaties*; Wolters Noordhoff Groningen; 2e druk; 1998; p. 319-320.

Engels, en het adviesrapport zou worden verstuurd. Dit had voor mij het gewenste gevolg dat ik in principe wekelijks een terugkoppeling ten aanzien van mijn werk kon krijgen. Mijn bedrijfsmentor en diens manager konden tegelijkertijd zo de voortgang van mijn werkzaamheden controleren. Dit had binnen korte tijd een positief effect op mijn functioneren. Het kwam ook voor dat de bedrijfsmentor voor bepaalde periodes niet aanwezig was. Bij dringende vragen kon ik terecht bij de heer D. Stanley, onderzoeker en collega van mijn bedrijfsmentor. Dit is tijdens mijn afstudeerperiode niet nodig geweest.

3.3 Oriëntatie afstudeeropdracht

Tijdens mijn eerste dag bij NC3A had ik een informeel overleg met de bedrijfsmentor over de afstudeeropdracht. Ik had de afstudeeropdracht, in het Engels, bij mijn eerste bezoek al doorgenomen en had tijdens het informeel overleg de kans om vragen te stellen. Hierdoor ben ik tot de definitieve opdrachtsomschrijving gekomen. Mijn afstudeeropdracht was het geven van een advies over "Need-To-Know" scheiding op geheime, beveiligde netwerken.

3.4 Probleemstelling en Doelstelling

De aanleiding tot de afstudeeropdracht interesseerde mij. Er was mij verteld door mijn bedrijfsmentor dat er een informatiebeveiligingsbeleid op papier aanwezig is binnen de NATO. Dit informatiebeveiligingsbeleid geeft aan hoe de informatie binnen de NATO afgeschermd wordt. Dit wordt gedaan door middel van classificatieniveaus toe te wijzen namelijk:

- Unrestricted (onbevoegd); Iedereen binnen de organisatie heeft toegang bijvoorbeeld tot de kantine;
- Restricted (bevoegd); Dit geldt alleen voor personeel dat bevoegd is om bepaalde taken uit te voeren of tot een bepaald gebied binnen de organisatie;
- Secret (geheim); Dit geldt alleen voor personeel wiens werk geheim is;
- Top Secret (zeer geheim); Dit geldt alleen voor personeel wiens werk zeer geheim is.

Alle netwerken binnen de NAVO maken gebruik van deze classificaties. Mijn afstudeeropdracht geldt met name alleen voor de geheime en zeer geheime, beveiligde netwerken. Er zijn totaal drie soorten netwerken aanwezig namelijk:

1. Een netwerk met algemene informatie, dat toegankelijk is voor alle gebruikers binnen de NATO;
2. Een geheim beveiligd netwerk, waarop geheime informatie is opgeslagen. Gebruikers die tot het geheime beveiligde netwerk toegang hebben, hebben een hoog classificatieniveau;
3. Een zeer geheim beveiligd netwerk aanwezig dat alleen toegankelijk is voor gebruikers met een zeer hoog classificatieniveau.

Deze laatste twee groepen gebruikers zijn verder niet afgeschermd binnen het geheime beveiligde netwerk en zeer geheime beveiligde netwerk. Dit kan voor problemen gaan zorgen. De gebruikers kunnen elkaars bestanden lezen terwijl dit niet voor alle gebruikers, binnen het geheime beveiligde netwerk, toegankelijk hoort te zijn. Informatie kan zo in verkeerde handen vallen. Het komt weleens voor dat een gebruiker met een hoog classificatieniveau, informatie te zien krijgt waarvoor hij niet bevoegd is. Dit is mij verteld door de bedrijfsmentor. Informatie over het geheime beveiligde netwerk is niet voor buitenstaanders toegankelijk. Er is in het verleden een zakelijke analyse uitgevoerd, door NATO Security Comittee (NSC) en goedgekeurd door de North Atlantic Council (NAC), voor de geheime, beveiligde netwerken van NATO. De zakelijke analyse concentreerde zich op risico's en bedreigingen voor het geheime, beveiligde netwerk. In de zakelijke analyse zijn ook maatregelen beschreven om de risico's en bedreigingen uit te sluiten. Uit de zakelijke analyse is het informatiebeveiligingsbeleid voortgekomen. Ik ben uitgegaan van dit informatiebeveiligingsbeleid om mijn adviesrapport te schrijven. Het voldeed aan de CVI richtlijnen. Dit wordt uitgebreider beschreven in hoofdstuk zeven.

Ondanks dit informatiebeveiligingsbeleid, ondanks de verschillende classificaties en netwerken blijkt er toch voor bepaalde groepen gebruikers te vaak toegang te zijn tot irrelevante informatie. Irrelevant qua kennis, niet ter zake doende, veiligheid etc. Dat leidt tot de volgende probleemstelling, geformuleerd als vraag: "*Welke mogelijkheden zijn er om voor een goede NTK beveiliging binnen de NATO te zorgen"*[8]

Daarmee is de doelstelling van mijn afstudeeropdracht geworden: "*Het opstellen van een advies over de mogelijkheden die er zijn om voor een goede NTK beveiliging binnen de NATO te zorgen"*.
De opdrachtgever is NATO zelf, maar de opdracht wordt uitgevoerd bij NATO Consultation, Command and Control Agency (NC3A), afdeling Communications Informations Systems (CIS).

Om tot het advies te komen, dient er een algemeen rapport geschreven te worden over toegangscontroles (access controls) in de context van NTK. Hierbij is van belang om uit te zoeken aan welke specifieke beveiligingscriteria moet worden voldaan om NTK beveiliging "goed" te realiseren. Het rapport moet in de huisstijl van de NC3A geschreven worden. Het rapport moet een soortgelijke structuur hebben als het rapport "Windows 2000 Certificate Services"[9].

Een belangrijk vraag was, wat de sleutelterm uit de opdracht NTK precies inhoudt? NTK is een sleutelterm die binnen de NC3A organisatie in de context van beveiliging van informatie wordt gebruikt. NTK is gebaseerd op het concept, dat gebruikers alleen toegang hebben tot informatie die ze nodig hebben om hun werk of verplichtingen uit te voeren. Een gebruiker meer rechten geven, is vragen om problemen en dan bestaat er de mogelijkheid tot misbruik van die rechten, die aan de gebruikers zijn verleend. Informatie

[8] Bijlage A: *Definitieve opdrachtsomschrijving*;
[9] Bijlage A: *Definitieve Opdrachtsomschrijving*;

die een gebruiker nodig heeft om zijn/haar taak uit te kunnen voeren, refereert naar het NTK principe. NTK refereert naar kennis, wat hij/zij met die informatie kan doen en refereert naar het geven van zo min mogelijk rechten. De definitie van NTK heb ik ontleend aan een Engels boek[10] en vertaald in het Nederlands. Deze definitie heb ik aan mijn bedrijfsmentor voorgelegd en hij ging ermee akkoord.

[10] Harris, Shon: *CISSP Certification Exam Guide Second Edition*; Mc Graw Hill Osborne; 1e druk; 2003; p. 125.

4. Gekozen methoden

4.1 Inleiding

Na het beschrijven van de organisatie en de oriëntatie beschrijf ik nu mijn gemotiveerde keuze van de methoden die een ordening in mijn activiteiten hebben bewerkstelligd. De NC3A organisatie zelf maakt geen gebruik van een standaard projectmanagementmethode of een ontwikkelmethode. Ik heb ervoor gekozen om naast de gefaseerde aanpak van het literatuuronderzoek een andere gefaseerde aanpak te kiezen gebaseerd op de CVI. Mijn reden hiervoor wordt in § 4.3 uitgelegd. Naast beide gefaseerde aanpakken wil ik ook een gedeelte van een projectmanagementmethode hanteren. Het gebruik van beide gefaseerde aanpakken en een projectmanagementmethode zorgt voor een gefaseerde en gestructureerde aanpak van mijn afstudeerproject. Hierdoor kon ik het afstudeerproject in goede banen leiden. Er zijn verschillende soorten projectmanagementmethodes en gefaseerde aanpakken aanwezig. In dit hoofdstuk zal ik beschrijven hoe ik tot mijn gekozen gefaseerde aanpakken en projectmanagementmethode ben gekomen. De methoden die besproken worden, staan hieronder beschreven.

De twee gefaseerde aanpakken zijn:

- Literatuuronderzoek[11];
- Het acht stappenplan van Oud[12];

De twee projectmanagementmethodes zijn:

- Projects In Controlled Environments 2 (Prince2)[13];
- Projectmatig werken[14].

Ik zal eerst een korte beschrijving geven van elk van de bovenstaande punten en waarvoor ze gebruikt worden. Hierna beschrijf ik de voordelen en nadelen van deze methoden voor mijn afstudeerproject. Als laatst beschrijf ik de motivatie voor mijn keuzes uit deze methoden.

4.2 Literatuuronderzoek

Literatuuronderzoek bestudeert gericht de literatuur, maar gaat verder dan onderzoek naar boeken en tijdschriften. Digitaal opgeslagen gegevens kunnen ook geraadpleegd worden.

[11] Klein, R: *Moduleboek OR-03*; Haagse Hogeschool; 1e druk; 1997; p. 6.
[12] Oud, Ernst J.: *Praktijkgids Code van Informatiebeveiliging*; Academic Service Schoonhoven; 1e druk; 2002; p. 40.
[13] Jansen, Peter: *Projectmanagement volgens Prince2*; Pearson Education Benelux; 1e druk; 2003; p. 10.
[14] Wijnen, Gert., Renes, Willem., Storm, Peter.: *Projectmatig werken*; Het Spectrum; 18e druk; 2002; p. 11.

Gegevens zoals databanken, Internet, video, foto, geluid. Al deze zaken geven een goed inzicht in de stand van zaken van de wetenschap op een van te voren omschreven onderwerp.

Voordelen:

- Door de gefaseerde aanpak van literatuuronderzoek te gebruiken, heb ik in een korte tijd veel informatie kunnen vinden;
- De zes stappen van het literatuuronderzoek brengen structuur aan in mijn afstudeerproject.

Nadelen:

- Door gebruik te maken van de gefaseerde aanpak van een literatuuronderzoek, om informatie over mijn onderwerpen te vinden, kwam het voor dat de stroom van informatie mij teveel werd. Hierdoor verloor ik het overzicht;
- Het kwam regelmatig voor dat ik iteratief te werk moest gaan. Dit houdt in dat ik na een bepaalde stap terug ging na een voorgaande stap. Hierdoor had ik het gevoel dat ik de structuur verloor in mijn afstudeerproject.

Daar de voordelen in mijn ogen groter waren dan de nadelen heb ik voor de gefaseerde aanpak van een literatuuronderzoek gekozen.

4.3 Code van informatiebeveiliging

Er is gebruik gemaakt van het boek "Praktijkgids Code van Informatiebeveiliging" (CVI). Het boek beschrijft de acht stappen van Oud. CVI beschrijft vooral welke maatregelen getroffen kunnen worden om risico's te minimaliseren binnen de organisatie. Deel twee van de CVI bevat de beschrijving van een managementmodel om de juiste maatregelen te selecteren en te beheersen. De CVI beschrijft echter niet in technisch detail hoe op operationeel niveau de maatregelen vormgegeven kunnen worden. CVI is namelijk platformonafhankelijk en kan daardoor niet ingaan op de technische details van de grote diversiteit binnen ICT-infrastructuren. Ik heb gebruik gemaakt van de acht stappen van Oud die ontwikkeld zijn met betrekking tot het CVI (zie figuur 3 op p. 19)[15].

De acht stappen, die ontwikkeld zijn met betrekking tot het CVI, realiseren het tweede deel van CVI. De acht stappen van Oud gaven mij de kans, naast de gefaseerde aanpak van het literatuuronderzoek, meer structuur in mijn afstudeerproject te brengen.

Voordelen:

- De acht stappen van Oud sloten, qua informatiebeveiliging zeer goed aan bij mijn afstudeeropdracht.

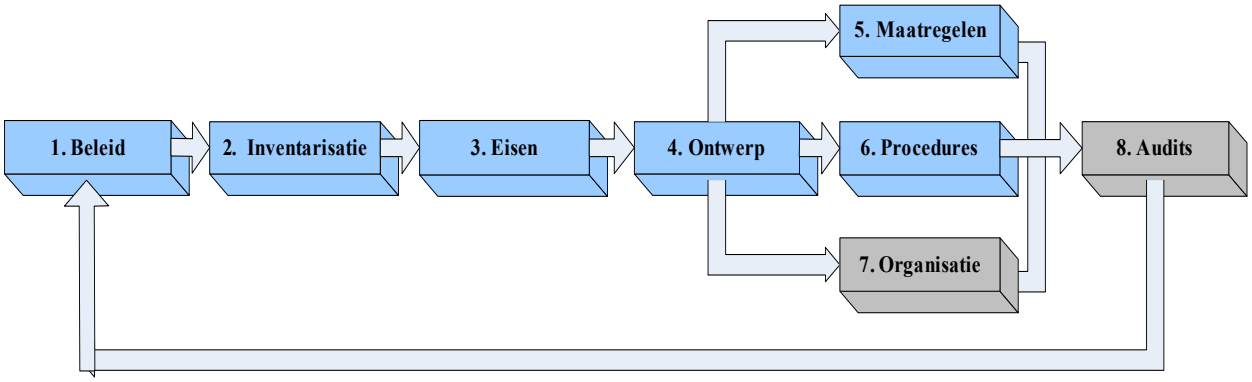
[15] Oud, Ernst J.: *Praktijkgids Code van Informatiebeveiliging*; Academic Service Schoonhoven; 1e druk; 2002; p. 40.

- Het bracht fasering en structuur aan in mijn afstudeerproject.

Nadelen:

- Vanwege de technische inhoud van het boek vond ik het vrij lastig om de acht stappen van Oud te begrijpen.

Ik heb ervoor gekozen om de acht stappen van Oud te gebruiken. Zowel de acht stappen van Oud als mijn onderwerp zijn beide gerelateerd aan informatiebeveiliging. Hiervan heb ik alleen zes van de acht stappen van Oud gebruikt: beleid, inventarisatie, eisen, ontwerp, maatregelen en procedures. Ik heb de stap organisatie niet uitgevoerd, omdat op organisatieniveau geen verandering plaatsvindt. Het uitvoeren van een audit is momenteel niet noodzakelijk. Er wordt alleen een adviesrapport geschreven. In een later stadium kan alsnog een audit uitgevoerd worden. De acht stappen van Oud brachten tevens structuur aan in mijn afstudeerproject. Daarnaast heb ik ervoor gekozen om op mijn eigen manier de stap risicoanalyse uit te voeren. Ik heb gekeken naar de bedreigingen zowel binnen als buiten de NATO. Hierna heb ik een analyse uitgevoerd. Mijn analyse was gebaseerd op informeel overleg met mijn bedrijfsmentor en op het doornemen van het informatiebeveiligingsbeleid. Hierdoor kon ik bepalen in hoeverre de bedreigingen een risico vormen.



Figuur 3: Het 8 stappenplan[16]

4.4 Projectmanagementmethode Prince2

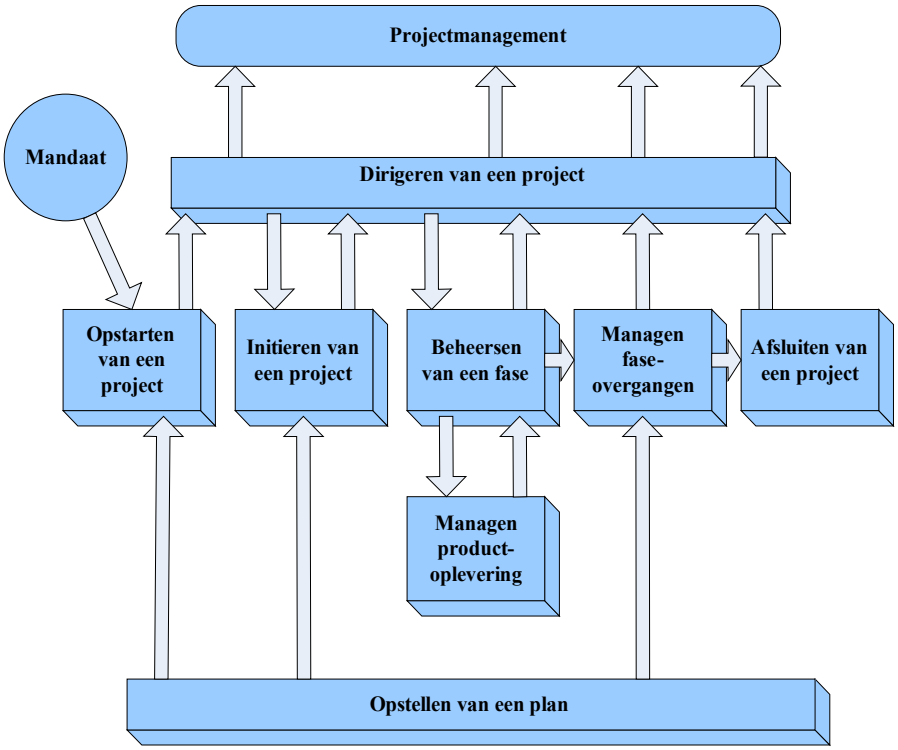
De projectmanagementmethode Prince2 is een gestructureerde projectmanagementmethode die gebaseerd is op bestaande projectmanagementmethodes. Prince2 heeft de volgende kenmerken:

- Procesmatig aanpak; Hierdoor komt het doel van een proces centraal te staan;

[16] Oud, Ernst J.: *Praktijkgids Code van Informatiebeveiliging*; Academic Service Schoonhoven; 1e druk; 2002; p. 41.

- Public-domaingedachte; Het gebruik van de projectmanagementmethode is vrij, hiervoor is geen licentie nodig;
- Gebruik van best practices; De methode wordt voortdurend aangepast aan de praktijk.

Prince2 benadert projectmanagement procesmatig. Een proces kan worden omschreven als een serie logisch samenhangende activiteiten die leiden tot een van tevoren bepaald doel. De projectmanagementmethode Prince2 is geschikt voor alle projecten en kan naar behoefte worden aangepast in schaalgrootte van de toepassing van de processen, technieken en componenten. De processen worden gedefinieerd aan de hand van de te behalen doelstelling[17]. Prince2 wordt gebruikt om projecten te beheersen.



Figuur 4: Prince2 procesmodel

Voordelen:

- Een gecontroleerde start, uitvoering en afsluiting;
- Reguliere voortgangscontroles en terugkoppeling;
- De betrokkenheid van belanghebbenden.

[17] Jansen, Peter: *Projectmanagement volgens Prince2*; Pearson Education Benelux; 1e druk; 2003; p. 16.

Nadelen:

- Prince2 is voor mij een onbekende projectmanagementmethode. Het doornemen van het boek "Projectmanagement volgens Prince2" kan enige tijd in beslag nemen.

Ik heb bewust niet gekozen voor Prince2 dit is een projectmanagementmethode waarover ik nog veel moet leren. Een andere projectmanagementmethode waarmee ik wel bekend ben is, "Projectmatig werken".

4.5 Projectmanagementmethode Projectmatig werken

Het boek "Projectmatig werken" bedrijft een projectmanagementmethode. De methode kent een aantal fasen die doorlopen moeten worden namelijk:

- Initiatiefase/ Oriëntatiefase;
- Definitiefase/ Analysefase;
- Ontwerpfase;
- Voorbereidingsfase;
- Realisatiefase/ Uitvoeringsfase;
- Nazorgfase.

Door het afstudeerproject op te delen in fasen, kon ik een planning maken voor elke fase (zie tabel 2 op p. 26.). Hierin wordt door mij omschreven welke activiteiten er in de betreffende fase moeten worden uitgevoerd. Bovendien kan ik aan het einde van elke fase een weloverwogen beslissing nemen om al of niet verder te gaan met de volgende fase.

Voordelen:

- De projectmanagementmethode bood aan het eind van elke fase een beslismoment, wel of niet door te gaan naar de volgende fase;
- Het bracht structuur aan in mijn afstudeerproject;

Nadelen:

- De projectmanagementmethode is te uitgebreid.

Het nadeel van de projectmanagementmethode, dat deze te uitgebreid is, heb ik als volgt proberen te ondervangen: Ik heb niet alle fasen c.q. activiteiten eruit toegepast. Ik heb ervoor gekozen om alleen de oriëntatiefase, analysefase en de uitvoeringsfase te gebruiken. Ik heb de oriëntatiefase gebruikt om informele gesprekken te voeren met de bedrijfsmentor om zo meer inzicht te krijgen in de afstudeeropdracht en om zo een definitieve afstudeeropdracht te formuleren. Met behulp van de analysefase heb ik de situatie, binnen de complexe organisatie van NC3A, grondig geanalyseerd door het informatiebeveiligingsbeleid document te lezen en door informeel overleg te voeren met

de bedrijfsmentor om zo de eisen van het adviesrapport vast te stellen. In de uitvoeringsfase heb ik de afstudeeropdracht uitgevoerd. Binnen deze fasen heb ik de activiteiten opgenomen van de gefaseerde aanpakken, literatuuronderzoek en CVI. De overgebleven fasen, ontwerpfase en voorbereidingsfase vond ik overlappen met mijn activiteiten en heb ik op informele wijze toegepast. De nazorgfase vond ik niet nodig aangezien het mij alleen ging om het schrijven van een adviesrapport.

5. Projectplanning

5.1 Inleiding

Hoofdstuk vijf beschrijft zowel de totstandkoming van het plan van aanpak als de totstandkoming van de definitieve opdrachtsomschrijving. De definitieve opdrachtsomschrijving is opgesteld in samenwerking met mijn bedrijfsmentor de heer dr. R. Malewicz, en met de examinatoren van de Haagse Hogeschool, de heer W.B. Elschot en de heer T.W.M. van Gerwen. Zowel de opdrachtsomschrijving als het plan van aanpak zijn bijgevoegd als bijlagen in het eindverslag. Voor de integrale tekst verwijs ik de lezer naar *Bijlage A: Definitieve opdrachtsomschrijving, Bijlage B: Engelse opdrachtsomschrijving en in Bijlage C: Plan van aanpak.*

Ik heb ervoor gekozen om de beschrijving van de afstudeeropdracht en het plan van aanpak op te nemen in één hoofdstuk, omdat beide sterke overeenkomsten vertoonden. Ik zal alleen de zaken noemen die nog niet beschreven zijn in dit eindverslag. Zaken die relevant zijn omtrent de afstudeeropdracht zijn al beschreven in hoofdstuk 3, § 3.4.

Het maken van het plan van aanpak leverde geen problemen op. Het plan van aanpak is niet specifiek gebaseerd op een projectmanagementmethode. Ik heb de standaard indeling van een plan van aanpak gebruikt van de in "System Development Methodology" (SDM) beschreven wijze[18].

Er was al een opdrachtsomschrijving aanwezig in het Engels bij NC3A. Deze was opgesteld door mijn bedrijfsmentor. Bepaalde onderdelen van de Engelse opdrachtsomschrijving heb ik vertaald naar het Nederlands en anders geformuleerd om aan de eisen van de Haagse Hogeschool te voldoen. Hierbij verwijs ik de lezer naar de Nederlandse opdrachtsomschrijving (bijlage A) en die van de Engelse opdrachtsomschrijving (bijlage B).

5.2 Doel plan van aanpak

Het doel van het plan van aanpak was het plannen van mijn activiteiten en diende tevens als blauwdruk voor het schrijven van mijn adviesrapport.

5.3 Organisatie

Binnen dit gedeelte van het plan van aanpak heb ik de namen van alle betrokkenen bij het project beschreven en de taken die elke persoon heeft. Ook zijn hier de verantwoordelijkheden beschreven en de contractuele voorwaarden. Totaal zijn er twee

[18] *SDM Reader*; Haagse Hogeschool Den Haag; 1e druk; 1997; p. 12.

functionarissen bij mijn afstudeerproject betrokken: de heer R. Malewicz, bedrijfsmentor, en de heer C. Shawcross, afdelingshoofd. De verantwoording die ik moet afleggen, is aan het begin van mijn afstudeerperiode besproken met de bedrijfsmentor. Er was afgesproken om wekelijks contact te houden met de bedrijfsmentor. In de praktijk was dit niet altijd het geval. Dit kwam mede doordat de bedrijfsmentor het druk had met zijn werk. Hierdoor kon ik geen wekelijks informeel overleg voeren met de bedrijfsmentor. Als tijdelijke oplossing gebruikte ik email om vragen te stellen. Maar sommige vragen konden alleen beantwoord worden door middel van een dialoog.

Naam	Functie	Locatie	Telefoon
Dhr. Chuck Shawcross	Afdelingshoofd	NC3A	070-3743047
Dhr Dr. Robert Malewicz	Bedrijfsmentor	NC3A	070-3743477
Dhr. Asim Malik	Afstudeerder/ Consultant	NC3A	070-3743436

Tabel 1: Rol van functionarissen

5.4 Project

Om de randvoorwaarden van mijn adviesrapport te bepalen, voerde ik een informeel overleg met de bedrijfsmentor. De randvoorwaarden zijn:

- Het adviesrapport wordt geschreven volgens de wensen en eisen van de opdrachtgever;
- De benodigde software en hardware (zie bijlage C hoofdstuk 5, § 5.2) zal beschikbaar moeten worden gesteld;
- De bedrijfsmentor is tijdens kantooruren bereikbaar voor vragen of ondervonden problemen.

Door de randvoorwaarden vast te leggen, wist ik aan welke wensen en eisen ik me moest houden om het adviesrapport te schrijven.

Er was geen documentatie over "Need-To-Know" scheiding aanwezig bij NC3A, bij aanvang van mijn afstudeerperiode. Dit heb ik nagevraagd aan de bedrijfsmentor. Hierdoor was ik genoodzaakt om zelf informatie te zoeken uit boeken en tijdschriften en door het medium Internet. Dit zoeken staat beschreven in hoofdstuk zes.

5.5 Risico's

Bij elk afstudeerproject zijn er risico's. Ik heb de risico's in kaart gebracht en ben tot drie risico's gekomen[19].

- *Het onvoldoende vinden van informatie over betreffende onderwerp.* De afstudeerder kan onvoldoende informatie vinden over het betreffende onderwerp.

[19] Bijlage C: *Plan van aanpak*;

Hierdoor kunnen bepaalde activiteiten meer tijd in beslag nemen. Dit risico kan beperkt worden door tijdig de bedrijfsmentor te informeren. Tijdens mijn afstudeerperiode vond ik onvoldoende informatie over NTK. Als aanvullende maatregel nam ik een interview af met de heer Peter Groen, EDP-auditor bij PWC.

- *Het product kan niet tijdig worden opgeleverd.* De afstudeerder heeft geen ervaring met het plannen van een dergelijk project; activiteiten kunnen te optimistisch zijn ingepland, waardoor tijdnood kan ontstaan. Dit risico kan beperkt worden door de bedrijfsmentor de voortgang te laten bewaken en indien nodig, tijdig bij te sturen. De afstudeerder kan zelf ook aangeven wanneer bijsturing gewenst is. Als aanvullende maatregel heb ik gebruik gemaakt van een projectmanagementmethode "Projectmatig werken" om structuur aan te brengen in mijn afstudeerproject. Daarnaast heb ik gebruik gemaakt van de stappen van een gefaseerde aanpak literatuuronderzoek, maar ook van het acht stappenplan van Oud.

- *De afwezigheid van de bedrijfsmentor kan het project ernstig vertragen.* De bedrijfsmentor kan onvoldoende tijd hebben of niet aanwezig zijn voor de afstudeerder. Hierdoor kan het project ernstige vertraging oplopen. Dit risico kan beperkt worden door een vervangende begeleider toe te wijzen. Aan het begin van mijn afstudeerperiode had ik onvoldoende terugkoppeling gekregen van mijn bedrijfsmentor. In deze korte tijd zag ik de noodzaak tot meer maatregelen. Tijdens een overleg tussen mijn bedrijfsmentor, zijn manager en mij werd afgesproken om wekelijkse rapportages op te sturen en terugkoppeling te ontvangen over het adviesrapport.

5.6 Uitvoering

Een belangrijk onderdeel voor mijn afstudeerproject was welke gefaseerde aanpak of projectmanagementmethode ik zou gebruiken. Dit is een te groot onderdeel om in één paragraaf te bespreken. Daarom heb ik dit onderdeel opgenomen in hoofdstuk vier.

5.7 Planning

Door een planning op te stellen en die met de werkelijkheid daarvan te vergelijken, ben ik in staat om de voortgang van mijn afstudeerproject te bewaken. Mijn planning was gebaseerd op de gefaseerde aanpak van een literatuuronderzoek, maar al snel werd mij duidelijk dat de gefaseerde aanpak van het literatuuronderzoek niet voldoende was om structuur aan te brengen binnen mijn afstudeerproject. Ik heb ervoor gekozen om naast de gefaseerde aanpak een andere gefaseerde aanpak te kiezen en een gedeelte van een projectmanagementmethode (zie hoofdstuk 4) te gebruiken. Aan de hand van beide gefaseerde aanpakken en de projectmanagementmethode is een uiteindelijke planning

opgesteld. Er is uitgegaan van een periode van negentien weken, omdat de afstudeerperiode negentien weken in beslag nam.
Ik heb de planning opgenomen in tabelvorm. Het geeft de uit te voeren activiteiten uitgezet tegen de tijd weer:

Week nr. / Activiteit	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Oriëntatiefase																			
Projectplanning																			
Analysefase:																			
Uitzoeken beveiligingscriteria																			
Literatuurstudie, CVI																			
Uitvoeringsfase:																			
Ordenen onderzoeksgegevens																			
Opstellen adviesrapport																			
Afstudeerverslag																			

Tabel 2: Uiteindelijke planning

In de oriëntatiefase oriënteer ik mij op de werkomgeving en op de afstudeeropdracht. Na de oriëntatiefase plan ik mijn afstudeerproject in. De volgende stap is de analysefase. De analysefase bestaat uit de volgende activiteiten: Het uitzoeken van de beveiligingscriteria bij NATO, dit staat beschreven in het informatiebeveiligingsbeleid, de activiteiten uitvoeren van de stappen van een gefaseerde aanpak literatuuronderzoek en het uitvoeren van het acht stappenplan van Oud. In de uitvoeringsfase worden de gegevens geordend. Na het ordenen van de gegevens wordt het uiteindelijke adviesrapport opgesteld.

6. Literatuuronderzoek

6.1 Inleiding

Dit hoofdstuk beschrijft de procesgang van de activiteiten van de gefaseerde aanpak van een literatuuronderzoek. Het literatuuronderzoek is één van de gefaseerde aanpakken die ik heb gekozen om voor mijn afstudeerproject te gebruiken. Door middel van het literatuuronderzoek kom ik meer te weten over de sleutelterm NTK en over methoden, technieken en producten waarin NTK geïmplementeerd kan worden. De keuze hiervoor staat beschreven in hoofdstuk vier.

Ik ben begonnen met een gefaseerde aanpak van literatuuronderzoek omdat ik van mening was, aan het begin van mijn afstudeerperiode, dat het voldoende fasering kon brengen in mijn afstudeerproject. Ik heb gebruik gemaakt van de volgende stappen[20]:

1. Bepalen van doelstelling en begrenzingen;
2. Opstellen van een zoekplan;
3. Verzamelen van bibliografische gegevens;
4. Bijeenzoeken van de literatuur;
5. Bestuderen van de literatuur;
6. Zoeken en bestuderen van heel recente literatuur.

Mijn werkwijze bij literatuuronderzoek was iteratief. Het kwam regelmatig voor dat ik bij stap vijf erachter kwam dat ik niet genoeg literatuur had verzameld voor mijn onderzoek. Hierdoor ging ik terug naar stap drie om meer gegevens te verzamelen.

6.2 Bepalen van doelstelling en begrenzingen

Mijn eerste activiteit was het bepalen van de doelstelling. Ik gaf hiermee aan wat ik wilde bereiken met mijn onderzoek. Mijn doelstelling was: *"Het zoeken naar informatie over de sleutelterm NTK en de daarbij behorende methoden, technieken en producten waarin NTK geïmplementeerd kan worden*". Naast het bepalen van de doelstelling moest ook een korte omschrijving gegeven worden over het onderwerp NTK, zodat het onderwerp, voor mijzelf en de lezer van het adviesrapport, duidelijk is. Een gedeelte hiervan was al beschreven in de opdrachtsomschrijving. Maar dat was heel beperkt. Ik heb het onderwerp uitgebreider beschreven (zie adviesrapport hoofdstuk 3).

Tijdens het afbakenen van het onderzoek stelde ik mijzelf de volgende vragen. Wat wil ik weten en wat niet, welke informatie is er nog meer over de sleutelterm NTK en welke methoden, technieken en producten zijn er waarin NTK geïmplementeerd kan worden? Is mijn onderwerp niet te ruim, zodat ik dadelijk niet word overspoeld met informatie; of is

[20] Klein, R: *Moduleboek OR-03*; Haagse Hogeschool; 1e druk; 1997; p. 6.

het te beperkt, zodat ik niet voldoende informatie vind. Om dit probleem op te lossen, heb ik besloten een rijtje op te stellen met trefwoorden waarop ik ging zoeken. De trefwoorden heb ik in het Engels geformuleerd, omdat in het Engels meer informatie hierover te vinden is.

De trefwoorden die ik heb opgesteld zijn:

- Need-To-Know;
- NTK;
- Access Controls;
- AC;
- Multilevel Security;
- MLS;
- Separation of duties;
- Separation of privileges;
- Separation of rights.

Ik maakte hiervoor gebruik van het Internet. Bij het opstellen van de rij met trefwoorden ging ik voor mezelf, door middel van het moduleboek OR-03, een aantal vragen na:

- Wat moest er met de resultaten gebeuren? De resultaten worden apart opgeslagen in een directory en gesorteerd, hierna neem ik ze door en haal alleen de relevante informatie eruit;
- Waarvoor zouden ze worden gebruikt? De relevante informatie wordt gebruikt voor het opstellen van een adviesrapport;
- Voor wie zijn ze bestemd? De resultaten zijn voor mij bestemd maar het adviesrapport is voor de NATO bestemd;
- Hoe kun je het onderwerp het beste omschrijven of definiëren? Zie hoofdstuk 3, § 3.4;
- Welke zoekvragen hanteer ik precies? What is NTK? How can NTK be implemented in an access control? What kind of MLS products are there?
- En welke zoektermen? Ik hanteer de Engelse zoektermen die ik heb opgesteld in de trefwoordenlijst.

Niet alleen de doelstelling werd bepaald, maar ook de begrenzingen van mijn onderzoek. Dit was al voor een klein gedeelte beschreven in de opdrachtsomschrijving. Nu ging ik de begrenzingen wat nader beschrijven. Ik had besloten om het zoeken naar informatie te begrenzen tot boeken, Internet en interviews. Boeken blijven altijd een bron van betrouwbare informatie, Internet en interviews leveren actuele informatie op en kunnen vragen beantwoorden op basis van kennis en ervaring. Ik heb me gehouden aan recente literatuur, hoogstens een paar jaar oud omdat informatica zich snel ontwikkelt. Daarnaast heb ik alleen gebruik gemaakt van de talen Engels en Nederlands. Hiervoor heb ik een aantal redenen, namelijk: binnen NC3A heerst de Engelse spreektaal, veel informatie is beschikbaar in het Engels en het merendeel van mijn boeken is in de Nederlandse taal geschreven.

6.3 Het opstellen van een zoekplan

Na het bepalen van de doelstelling en de begrenzingen van het literatuuronderzoek ben ik gekomen bij de volgende stap. Bij stap twee moest er volgens de aanpak een planning opgesteld worden. Deze was al opgesteld in het plan van aanpak (zie tabel 2 op p. 26.). De planning geeft een tijdschema aan waarin bepaalde activiteiten en mijlpaalproducten op tijd opgeleverd dienen te worden. Naast het maken van een planning werd ook het zoekproces beschreven. Ik heb hiervoor gebruik gemaakt van de volgende twee methodes: heuristische methode en de sneeuwbalmethode. Door gebruik te maken van deze twee methodes was ik in staat snel informatie te vinden. De heuristische methode is een methode waarbij er onderscheid gemaakt kan worden tussen informele methoden en formele methoden. Door middel van de informele gesprekken en emails communiceerde ik met de bedrijfsmentor om vragen te stellen en terugkoppeling te krijgen op mijn werk. Door gebruik te maken van informele overleggen was de bedrijfsmentor minder terughoudend met het geven van informatie.

Ik heb naast het informele overleg ook een formeel overleg gehad in de vorm van een interview. Het interview werd gehouden met de heer Peter Groen, een EDP-auditor bij PricewaterhouseCoopers (PWC). Als EDP-auditor was hij bekend met de sleutelterm NTK en alles daaromheen. De interview techniek die ik gebruikte, was gebaseerd op open vragen. NTK was een onderwerp waar ik nog weinig van afwist. Door open vragen te stellen, kreeg ik hierover meer informatie (zie bijlage D). Een vraag, die ik stelde was: "Hoe kan ik mijn conclusie beter beargumenteren?". Als antwoord hierop werd mij de werking uitgelegd van een tabel waarin selectiecriteria worden gehanteerd (zie tabel 6 op p. 42.). Het interview nam ongeveer anderhalf uur in beslag. Het interview was zeer informatief. De sleutelterm NTK was mij geheel duidelijk dankzij het "Need-To-Know" artikel[21] dat ik had gekregen van de heer Peter Groen. Daarnaast kreeg ik advies over het schrijven van mijn adviesrapport, zoals over de indeling van het rapport en over het beargumenteren van mijn conclusies. Hij stelde voor om meer over de huidige situatie binnen de NATO met betrekking tot de netwerken te schrijven. Hierdoor kon ik mijn argumentatie beter in relatie brengen met de organisatie. Ik kon de conclusie het best beschrijven aan de hand van verschillende situaties. De antwoorden die verkregen waren tijdens het interview waren voor mij duidelijk en helder. Ik vond het daarom niet noodzakelijk om terugkoppeling te geven. Ik heb mijn vervolgactiviteiten deels moeten aanpassen om veranderingen in mijn adviesrapport aan te brengen. Een vervolgactiviteit was het zoeken naar producten waarin NTK geïmplementeerd kon worden. Daarnaast ontving ik het boek "PricewaterhouseCoopers information security a strategic guide for business" en het vakblad "Informatiebeveiliging", waarin producten, methoden en technieken met betrekking tot informatiebeveiliging beschreven worden.

Naast de heuristische methode heb ik een methode gebruikt die gebruik maakt van citaatverbindingen. Deze methode gaat uit van een startartikel en aan de hand daarvan zoekt men naar welke andere werken dit verwijst (citeert) of welke andere werken hiernaar verwijzen. De sneeuwbalmethode is zo'n onderzoeksmethode.

[21] *http://www.dss.mil/training/csg/security/S1class/Need.htm*

Door middel van het Internet ging ik op zoek naar een artikel over NTK. Hierdoor hoopte ik meer informatie te vinden, ook met betrekking tot methodes, waarin NTK geïmplementeerd kon worden, zoals toegangscontroles[22] (access controls). Ik gebruikte het artikel "Need-To-Know", dat ik had gekregen van de heer Peter Groen, met de daarbij behorende referenties waar het artikel naar verwees[23]. Door de referenties na te gaan, vond ik weer artikelen die op hun beurt weer als bron fungeerden naar andere artikelen. Voordeel van deze methode was dat ik in een korte tijd heel veel informatie kreeg. Maar naast dit voordeel waren er ook nadelen aan verbonden. Ik was erg afhankelijk van de referenties, die stonden vermeld in het startartikel. Ik kwam ook geregeld verouderde literatuur tegen. Ik nam de verouderde literatuur door, op zoek naar relevante trefwoorden zoals MLS[24]. Bepaalde trefwoorden worden in de hedendaagse literatuur nog steeds gebruikt. Hierdoor heb ik mijn kans op relevante informatie over het onderwerp NTK, vergroot.

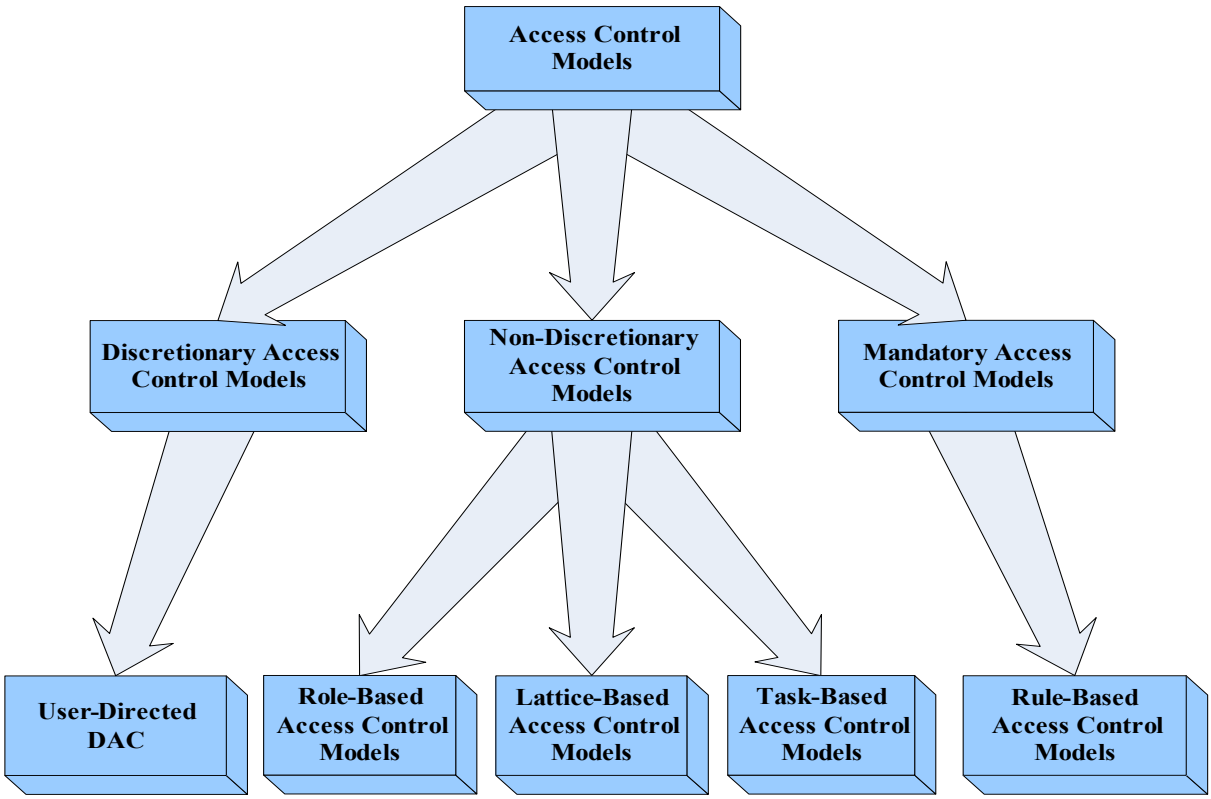
6.4 Verzamelen van bibliografische gegevens en het bijeenzoeken van de literatuur

Na het opstellen van een zoekplan was de volgende stap het verzamelen van bibliografische gegevens en het bijeenzoeken van literatuur. Ik heb deze twee stappen samengenomen, omdat ik hier voornamelijk iteratief te werk ging. Dit ging niet zonder problemen. Aan het begin van mijn afstudeerperiode had ik weinig informatie kunnen vinden met betrekking tot mijn onderwerp. Als eerste keek ik naar mijn eigen studieboeken, die ik tijdens mijn opleiding had gebruikt. Ik vond hierin geen bruikbare informatie. Ik had meer geluk bij het raadplegen van boeken over informatiebeveiliging zoals "All in One CISSP Certification Secound Edition Exam Guide", zowel in het Engels als in het Nederlands. Hierin stond het onderwerp helder en duidelijk beschreven. Het merendeel van de gebruikte boeken heb ik geleend van een Engelse collega en een gedeelte heb ik gevonden in de bibliotheek van de NC3A, zoals "Information Security, Dictionary of Concepts, Standards and Terms". Andere literatuur heb ik via het Internet kunnen vinden zoals "Access Control Layers". Ik zocht op trefwoorden die ik bij stap één had opgesteld, zoals "AC". Naast het raadplegen van boeken heb ik ook een EDP-auditor geïnterviewd (zie § 6.3).

6.5 Bestuderen van de literatuur

Het bestuderen van de literatuur leverde mij geen problemen op. Informatie die in boeken stond beschreven, was helder en duidelijk. Een gedeelte van de informatie die ik op het Internet had gevonden was zeer informatief. Hierdoor begreep ik de sleutelterm NTK en de daarbij behorende methoden, technieken en producten beter. Daarnaast vond ik een illustratie die mij een duidelijk beeld gaf van de methoden waarin NTK geïmplementeerd kan worden (zie figuur 5 op p. 31.):

[22] Toegangscontroles: De Engelse benaming ervoor is access control, het brengt scheiding van autorisatie en rechten aan in netwerken voor gebruikers. Meestal gebaseerd op een NTK beleid.
[23] *http://www.dss.mil/training/csg/security/S1class/Need.htm*
[24] Multilevel Security (MLS): Verschillende niveaus van beveiliging



Figuur 5: Toegangscontroles[25]

Figuur vijf geeft een hiërarchische structuur weer van alle toegangscontroles die ik heb onderzocht. Het figuur geeft op een hiërarchische manier weer hoe de toegangscontroles zijn onderverdeeld. De toegangcontroles zijn:

- Access Control Models: Toegangscontroles;
- Discretionary Access Control Models (DAC): Een gebruiker die een bestand aanmaakt is tevens de eigenaar en kan dezelfde rechten toevertrouwen aan andere gebruikers;
  - User-Directed DAC: Gebruikers met het recht om de toegangsrechten te veranderen van een bestand;
  - Identify-based access control: Dit is gebaseerd op de identiteit van de gebruiker en op het bestand;
  - Hybrid access control: Een combinatie van gecentraliseerde en gedecentraliseerde toegangscontrole.
- Non-Discretionary Access Control Models bestaat uit de volgende toegangscontroles:
  - Role-Based Access Control Models: Groepen gebruikers worden ingedeeld in rollen gebaseerd op hun functie of taak binnen de organisatie;
  - Lattice-Based Access Control Models: Verschillende niveaus van beveiliging op basis van de gebruikers classificatieniveau;

[25] Malik, Asim: *Need-To-Know separation on Classified Systems*; NC3A Den Haag; 1e druk; p. 6.

- Task-Based Access Control Models: Toegangscontrole waarbij een gebruiker autorisatie per taak krijgt.

❖ Mandatory Access Control Models: Toegang tot gegevens wordt verleend op basis van de gevoeligheid van de gegevens en op formele autorisatie van gebruikers die toegang willen tot gevoelige gegevens;

- Rule-Based Access Control Models: Rechten die aan specifieke voorwaarden moeten voldoen en aangeven wat wel of niet mogelijk is met een bestand dat opgevraagd wordt.

6.6 Zoeken en bestuderen recente literatuur

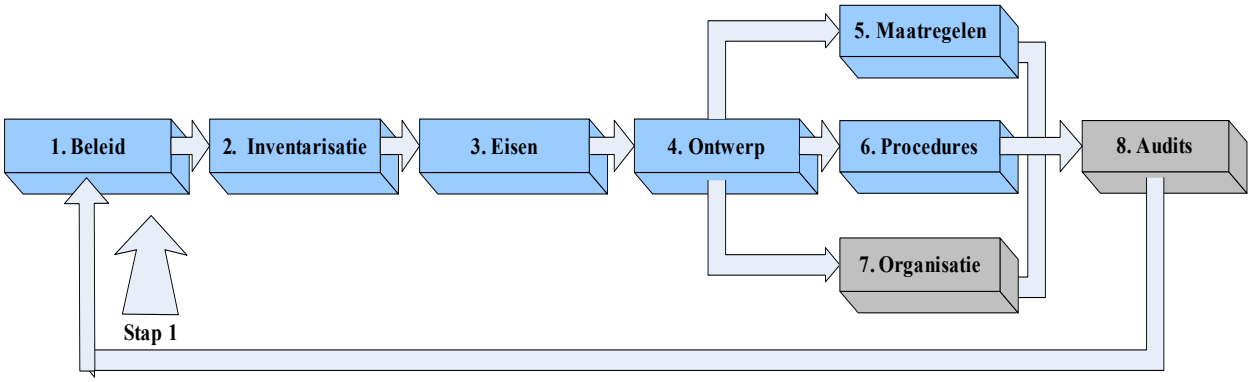
Het zoeken en bestuderen van recente literatuur leverde geen problemen op. Een actueel vakblad dat ik heb gekregen van de heer Peter Groen was het blad "Informatiebeveiliging". Elke maand komt een editie van dit blad uit, het beschrijft recente ontwikkelingen binnen de context van informatiebeveiliging. Daarnaast had ik een Engels boek gevonden, in de bibliotheek van NC3A, dat vorig jaar was uitgebracht. Het heet "CISSP Certification Exam Guide Second Edition" en legt in duidelijke en heldere taal alle informatiebeveiliging termen uit, in het bijzonder de sleutelterm NTK.

6.7 Conclusie

Door middel van het literatuuronderzoek heb ik informatie gevonden over methoden, technieken en producten, waarin NTK geïmplementeerd kan worden. Er was veel informatie beschikbaar over de methode toegangscontrole. Hierdoor werd dit onderwerp mij duidelijk. Op grond van het literatuuronderzoek heb ik NTK kunnen definiëren als: "NTK is het aanbrengen van een scheiding binnen een netwerk gebaseerd op het concept dat gebruikers alleen toegang hebben tot informatie die ze nodig hebben om hun werk of verplichtingen uit te voeren". Tevens heb ik uit de literatuur kunnen concluderen welke methoden en technieken bruikbaar waren voor de implementatie van NTK. Zo zijn access controls, cryptografie en op Web gebaseerde mechanieken zeer geschikt.
Er was weinig informatie aanwezig over de inhoud van de producten waarin NTK geïmplementeerd kan worden, dit vormde voor mij een probleem. Als oplossing heb ik, telefonisch en per email, contact opgenomen met de des betreffende bedrijven die de producten aanboden, zoals IBM. Hierdoor heb ik toch meer informatie over het product "IBM zSeries Mainframe operating system 1.5 en 1.6" kunnen verkrijgen (zie adviesrapport hoofdstuk 5, § 5.1).

Na het verwerken van de informatie in het adviesrapport, heb ik dit laten zien aan de bedrijfsmentor. De bedrijfsmentor keurde het goed. Na het literatuuronderzoek had ik informatie nodig over de huidige situatie binnen NC3A met betrekking tot de netwerken zoals het huidige informatiebeveiligingsbeleid. Voordat er maatregelen gekozen worden, moet de huidige situatie duidelijk zijn. Het doornemen van het huidige informatiebeveiligingsbeleid is de eerste stap binnen de acht stappen van Oud.

7. Stap 1 Informatiebeveiligingsbeleid



Figuur 6: Stap 1 Informatiebeveiligingsbeleid

7.1 Inleiding

Het informatiebeveiligingsbeleid is de eerste stap binnen de gefaseerde aanpak van het acht stappenplan van Oud. Binnen dit hoofdstuk wordt beschreven of het informatiebeveiligingsbeleid van de NATO zich aan de CVI richtlijn houdt. De CVI richtlijn beschrijft de minimale inhoud waaraan het informatiebeveiligingsbeleid[26] moet voldoen.

7.2 Informatiebeveiligingsbeleid

Er is een informatiebeveiligingsbeleid aanwezig binnen de NATO. Dit informatiebeveiligingsbeleid voldeed mijns inziens aan de minimale richtlijnen van de CVI[27]:

- Een definitie van informatiebeveiliging, de doelstellingen, de reikwijdte en het belang van informatiebeveiliging; Geheime, beveiligde informatie moet beschermd worden tegen verlies van betrouwbaarheid, integriteit en beschikbaarheid. Geheime, beveiligde informatie van de NATO en informatie die verkregen is van organisaties buiten de NATO moeten beschermd worden;
- Een verklaring van de intenties van het management ter ondersteuning van de doelstellingen en principes van informatiebeveiliging. Het North Atlantic Council (NAC) oftewel het Noord Atlantisch Raad, bestaat uit een raad wiens leden afkomstig zijn van de NATO landen. Het NAC gaat over het beleid binnen de

[26] Oud, Ernst J.: *Praktijkgids Code van Informatiebeveiliging*; Academic Service Schoonhoven; 1e druk; 2002; p. 54.
[27] Robertson, George: *Security within the North Atlantic Treaty organization*; NATO Brussel; 2002; p. 4.

NATO en over cruciale beslissingen betreffende NATO. Het NAC heeft negen basis principes opgesteld met betrekking tot informatiebeveiliging[28]:

- Een minimum set van beveiligingsstandaarden voor het uitwisselen van geheime, beveiligde informatie;
- Geheime, beveiligde informatie mag alleen bekeken en uitgegeven worden op basis van NTK;
- Het uitvoeren van een risicoanalyse is verplicht binnen NATO organisaties, in NATO landen is dit optioneel;
- Geheime beveiligde informatie wordt beschermd door middel van een set van beveiligingsmaatregelen, dit geldt ook voor het personeel. Fysieke beveiliging, beveiliging met betrekking tot geheime, beveiligde informatie en geheime beveiligde informatie die op media wordt opgeslagen;
- Verdachte inbreuk op beveiliging zal onmiddellijk worden gerapporteerd door de security manager. Hierna wordt het rapport geëvalueerd door autoriteiten en wordt de schade bekeken. Daarna worden stappen ondernomen;
- Geheime, beveiligde informatie, van de NATO, mag alleen vrijgegeven worden door de oorspronkelijke auteur aan de NATO en aan NATO landen. De vrijgegeven geheime, beveiligde informatie wordt beschermd aan de hand van NATO Information Management Policy (NIMP);
- De oorspronkelijke auteur van een geheim beveiligd document heeft zeggenschap over zijn werk;
- Het vrijgeven van geheime, beveiligde informatie gebeurt volgens de richtlijnen van de NATO;
- Geheime, beveiligde informatie mag alleen vrijgegeven worden aan niet NATO landen als een beveiligingsverklaring is ondertekend.

❖ Een toelichting op de beleidsmaatregelen, principes, normen en op de nalevingeisen ten aanzien van de beveiliging. Deze zijn voor de organisatie van bijzonder belang; Zie vorig punt;
❖ Een omschrijving van de algemene en specifieke verantwoordelijkheden voor het management van informatiebeveiliging, waaronder het rapporteren van beveiligingsincidenten; Zie vorig punt;
❖ Verwijzingen naar documentatie die het beleid kan ondersteunen. Er zijn een aantal verwijzingen naar andere documenten, die gespecificeerde informatie bevatten met betrekking tot het informatiebeveiligingsbeleid. Dit zijn de volgende documenten: Directive on Personnel Security, Directive on Physical Security, Directive on Security of information and Directive on Industrial Security.

Dit informatiebeveiligingsbeleid vormde mijn uitgangspunt voor het schrijven van mijn adviesrapport. Ik heb het informatiebeveiligingsbeleid gekregen van mijn bedrijfsmentor. Het huidige informatiebeveiligingsbeleid is wegens veiligheidsredenen niet als bijlage opgenomen in dit eindverslag. Ik heb alleen bepaalde onderdelen opgenomen (zie § 7.2) die algemene informatie bevatten en door het informatiebeveiligingsbeleid door te nemen begreep ik de aanleiding om een adviesrapport te schrijven over NTK scheiding op geheime, beveiligde netwerken (zie hoofdstuk 3, § 3.4). In het

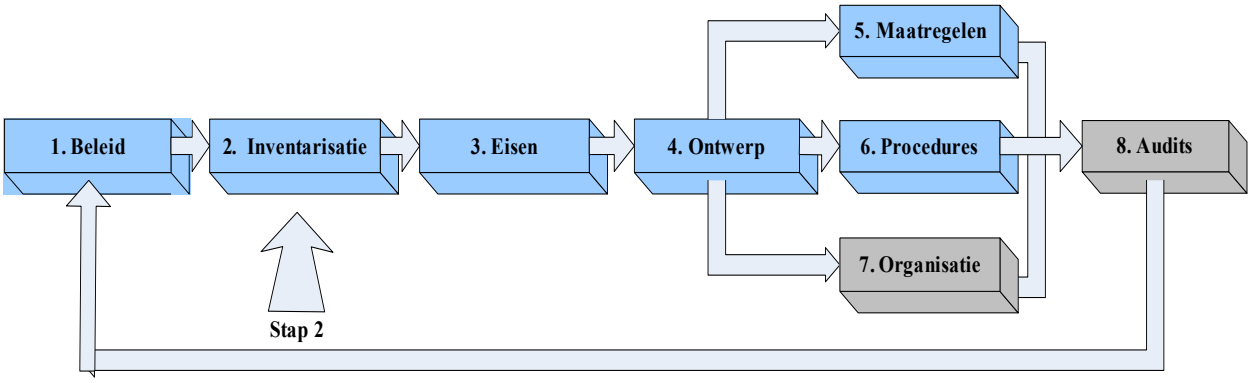
[28] Robertson, George: *Security within the North Atlantic Treaty organization*; NATO Brussel; 2002; p. 6.

informatiebeveiligingsbeleid stond namelijk dat er geen scheiding aanwezig was binnen de geheime, beveiligde netwerken. Gebruikers werden alleen ingedeeld per netwerk. In werkelijkheid zijn er drie netwerken en vier verschillende classificatieniveaus (zie hoofdstuk 3, § 3.4).

7.3 Conclusie

Het informatiebeveiligingsbeleid van de NATO voldeed aan de CVI richtlijnen Daarnaast verschafte het informatiebeveiligingsbeleid mij informatie over de beveiligingsmaatregelen. Dit heeft mij geholpen bij stap vier, ontwerp. Binnen deze stap stel ik nieuwe maatregelen op. In het volgende hoofdstuk wordt de huidige situatie met betrekking tot de geheime, beveiligde netwerken geïnventariseerd.

8. Stap 2 Inventarisatie van huidige situatie



Figuur 7: Stap 2 Inventarisatie

8.1 Inleiding

Na stap één van het acht stappenplan van Oud, dus na het beschrijven van het huidige informatiebeveiligingsbeleid van de NATO, komt het analyseren van de huidige situatie met betrekking tot de geheime, beveiligde netwerken aan bod. Een gedeelte hiervan was al beschreven in hoofdstuk 3, § 3.4. Ik heb deze stap uitgevoerd omdat ik de huidige situatie beter wilde begrijpen. Het inventariseren van de huidige situatie is een aangepaste stap binnen het acht stappenplan van Oud. Normaal gesproken worden de bedrijfsprocessen geïnventariseerd. Maar het opstellen van het adviesrapport is voornamelijk gericht op de geheime, beveiligde netwerken waarin NTK geïmplementeerd kan worden met behulp van methoden, technieken en producten. Ik maak hierbij, naar mijn eigen inzicht, alleen gebruik van bepaalde onderdelen binnen stap twee. Dit zijn de onderdelen die het boek "Praktijkgids Code van Informatiebeveiliging" beschrijft. Een onderdeel waarvan ik bijvoorbeeld gebruik heb gemaakt, is een tabel waarin de classificatie van betrouwbaarheidseisen wordt weergegeven[29]. Hiermee geef ik aan welke betrouwbaarheidseisen belangrijk zijn met betrekking tot de geheime, beveiligde netwerken binnen de NATO.

8.2 Classificatie betrouwbaarheidseisen

In tabel drie wordt, met behulp van betrouwbaarheidseisen, de waardering voor de geheime, beveiligde netwerken weergegeven. De betrouwbaarheidseisen zijn als volgt gedefinieerd:

[29] Oud, Ernst J.: *Praktijkgids Code van Informatiebeveiliging*; Academic Service Schoonhoven; 1e druk; 2002; p. 62.

- ❖ Beschikbaarheid: De mate waarin de geheime, beveiligde netwerken beschikbaar moeten blijven;
- ❖ Exclusiviteit: De mate waarin de geheime, beveiligde netwerken exclusief moeten blijven;
- ❖ Integriteit: De mate waarin de geheime, beveiligde netwerken foutloos moeten blijven.

Ik heb de tabel opgesteld door informeel overleg met de bedrijfsmentor te voeren, door het observeren van de geheime, beveiligde netwerken en door het huidige document informatiebeveiliginsbeleid. Hieruit is gebleken dat er hoge eisen worden gesteld aan de geheime, beveiligde netwerken.

Betrouwbaarheidseisen	Waardering
	Essentieel
	De geheime, beveiligde netwerken zijn essentieel voor het bewaken van gevoelige informatie binnen de NATO.
Beschikbaarheid	**Onmisbaar**
	De geheime, beveiligde netwerken moeten altijd operationeel blijven.
Exclusiviteit	**Dwingend**
	De belangen van de NATO organisatie worden ernstig geschaad als ongeautoriseerde gebruikers toegang krijgen tot de geheime, beveiligde netwerken.
Integriteit	**Onontbeerlijk**
	De geheime, beveiligde netwerken moeten foutloos draaien.

Tabel 3: Betrouwbaarheidseisen

8.3 MAPGOOD-verdeling

Het volgende onderdeel waarvan ik gebruik heb gemaakt om de huidige situatie met betrekking tot de geheime, beveiligde netwerken beter te begrijpen, is de MAPGOOD-verdeling: Mensen, Apparatuur, Programmatuur, Gegevens, Organisatie, Omgeving, Diensten[30]. Dit vormt samen met de betrouwbaarheidseisen een tabel (zie tabel 5 op p. 38). De gewenste informatie stond beschreven in het informatiebeveiligingsbeleid. Het noemen van elke component bij naam is wegens veiligheidsredenen niet opgenomen in dit eindverslag. Ik heb in plaats daarvan abstracte gegevens opgenomen als voorbeelden (zie tabel 4 op p. 38). Door middel van de MAPGOOD-verdeling weet ik, bijvoorbeeld, welke gegevens op de geheime, beveiligde netwerken zijn opgenomen.

[30] Oud, Ernst J.: *Praktijkgids Code van Informatiebeveiliging*; Academic Service Schoonhoven; 1e druk; 2002; p. 63.

Component	Voorbeelden
Mensen	Eigenaar, Systeembeheerder, Gebruikers
Apparatuur	Cryptografische computers
Programmatuur	Database programma's
Gegevens (verzamelingen)	NATO gegevens
Organisatie	Bureaucratische organisatie
Omgeving	NATO gebouw
Diensten	Energie, water, telefoon, gas

Tabel 4: MAPGOOD-verdeling

8.4 Betrouwbaarheidseisen en MAPGOOD-verdeling

Na het in kaart brengen van de MAPGOOD-verdeling heb ik de betrouwbaarheidseisen aan de componenten binnen de MAPGOOD-verdeling gekoppeld (zie tabel 5). Hierdoor weet ik welke componenten met betrekking tot welke eisen beschermd dienen te worden.

Onderwerp: Geheime, beveiligde netwerken
Typering: Essentieel

Eis / Component	Beschikbaarheid	Integriteit	Exclusiviteit
Mensen	Hoog	Hoog	Hoog
Apparatuur	Hoog	Hoog	Hoog
Programmatuur	Hoog	Hoog	Hoog
Gegevens	Hoog	Hoog	Hoog
Organisatie	Hoog	Hoog	Hoog
Omgeving	Hoog	Hoog	Hoog
Diensten	Hoog	Hoog	Hoog

Tabel 5: Betrouwbaarheidseisen uitgezet tegen componenten

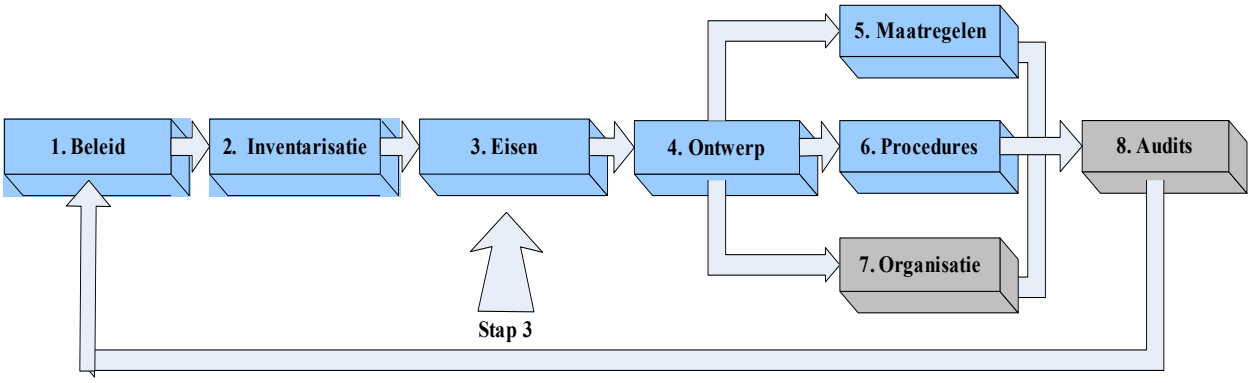
Door de betrouwbaarheideisen te verbinden met de componenten van de MAPGOOD-verdeling, zie ik welke niveaus de NATO organisatie met betrekking tot de geheime, beveiligde netwerken heeft[31]. Op basis van tabel vijf heb ik de maatregelen gekozen (zie hoofdstuk 10) met betrekking tot NTK-scheiding op geheime, beveiligde netwerken.

8.5 Conclusie

Door gebruik te maken van de beschreven onderdelen binnen stap twee, heb ik veel informatie kunnen vinden over geheime beveiligde netwerken. Door terug te kijken naar stap één en twee begrijp ik de huidige situatie beter.

[31] Oud, Ernst J.: *Praktijkgids Code van Informatiebeveiliging*; Academic Service Schoonhoven; 1e druk; 2002; p. 65.

9. Stap 3 Eisen



Figuur 8: Stap 3 Eisen

9.1 Inleiding

Naar aanleiding van de vorige twee stappen heb ik in stap drie de eisen ten aanzien van de inhoud van mijn afstudeeropdracht bepaald. Stap drie is de volgende stap van het acht stappenplan van Oud. Een gedeelte van de eisen was aan het begin van mijn afstudeerperiode al bekend (zie § 9.2). De eisen zijn opgesteld door mijn bedrijfsmentor. De inhoudelijke eisen van het adviesrapport werden gemaakt met behulp van een voorlopige inhoudsopgave (zie adviesrapport), welke ook door mijn bedrijfsmentor was opgesteld. Naast de eisen voor het adviesrapport zijn er ook eisen geformuleerd ten aanzien van de afstudeeropdracht.

9.2 Eisen

De eisen betreffende de inhoud van de afstudeeropdracht zijn:

- Het adviesrapport moet informatie bevatten over welke mogelijkheden er zijn voor een goede NTK scheiding op geheime, beveiligde netwerken binnen de NATO;
- Er moet beschreven worden hoe NTK scheiding kan plaatsvinden met behulp van de methode toegangscontroles;
- Andere mogelijkheden; zoals Public Key Infrastructure (PKI)[32], moeten beschreven worden (waarin NTK geïmplementeerd kan worden);
- Producten, waarin NTK geïmplementeerd kan worden, zoals TSOL[33], moeten ook beschreven worden;

[32] PKI: Public Key Infrastructure, dit is een versleutel (encryptie) methode om berichten en bestanden te versleutelen. Zodat alleen de ontvanger en de zender van het bericht of bestand het kunnen openen.
[33] Malik, Asim: *Need-To-Know separation on Classified Systems*; NC3A Den Haag; 1e druk; 2004; p. 17.

- Het adviesrapport moet in een formele schrijfstijl geschreven worden; Er mag, bijvoorbeeld, niet geschreven worden in de jij-vorm;
- Het adviesrapport moet in het Engels geschreven worden;
- Het adviesrapport moet enige diepgang bevatten;
- Het adviesrapport moet actualiteit bevatten; bijvoorbeeld recente producten, zoals op MLS gebaseerde IBM besturingssysteem[34];
- Het adviesrapport moet volledig zijn; alle hoofdstukken die opgesteld zijn door mijn bedrijfsmentor moeten beschreven worden;
- Het adviesrapport moet in de context van NTK beschreven worden.

Het was af en toe lastig om aan al deze eisen te voldoen. Zo kwam het, bij het zoeken naar geschikte producten, waarin NTK geïmplementeerd kan worden, regelmatig voor dat inhoudelijke informatie over een product niet aanwezig was; bij de internetsite van het bedrijf IBM was dit het geval. Ik had hiervoor twee oplossingen gevonden. Mijn eerste oplossing was het bedrijf een email te sturen of het bedrijf telefonisch te bereiken en zo de desbetreffende informatie op te vragen. De telefonische oplossing was succesvol. Mijn tweede oplossing was het gebruik maken van selectiecriteria. De selectiecriteria zijn opgesteld uit een aantal eisen, namelijk:

- Er wordt gebruik gemaakt van een scheidingstechniek, zoals MLS;
- Binnen de scheidingstechniek moet het mogelijk zijn om NTK te implementeren;
- Er wordt gebruik gemaakt van een wachtwoord.

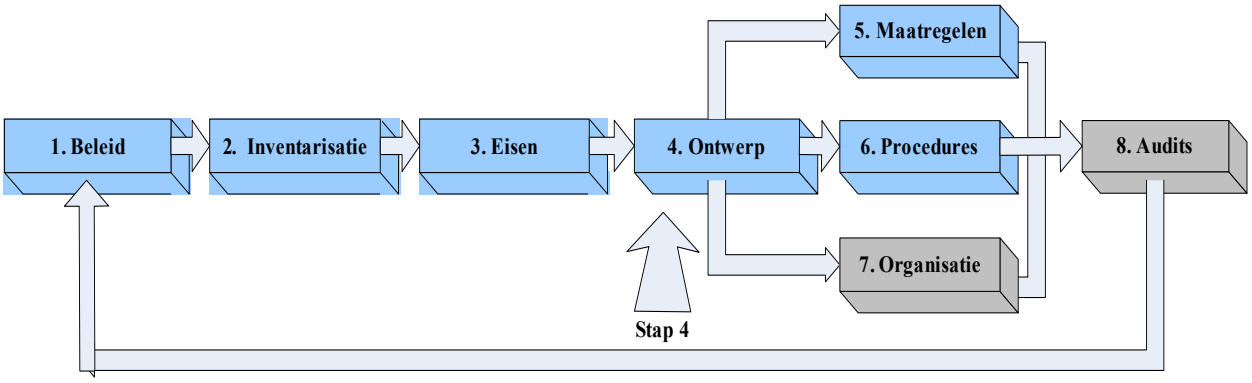
Dankzij de selectiecriteria, had ik voldoende informatie en kon ik een oordeel geven over de gevonden producten (zie hoofdstuk 5 van het adviesrapport).

9.3 Conclusie

Aan de hand van de eisen kan ik in stap vier van het acht stappenplan van Oud aan het ontwerp beginnen. Ik kan nu de maatregelen en procedures bepalen.

[34] Malik, Asim: *Need-To-Know separation on Classified Systems*; NC3A Den Haag; 1e druk; 2004; p. 16.

10. Stap 4 Ontwerp



Figuur 9: Stap 4 Ontwerp

10.1 Inleiding

Aan de hand van de eisen, die in het vorige hoofdstuk zijn beschreven, ben ik gekomen tot stap vier van het acht stappenplan van Oud. Stap vier, ontwerp, is onderverdeeld in drie stappen, namelijk: maatregelen, procedures en organisatie. Ik heb alleen de stappen maatregelen en procedures uitgewerkt.
De stap organisatie heb ik niet uitgevoerd omdat dezelfde taken en verantwoordelijkheden worden aangehouden zoals die staan omschreven in het huidige informatiebeveiligingsbeleid. Een voorbeeld hiervan is de security manager en de personeelsmanager binnen de NATO. De taak van de security manager is de beveiliging binnen het NC3A gebouw te waarborgen. Daarnaast is er ook een personeelsmanager binnen de NC3A aanwezig, die het aankomende personeel screent door hun achtergrond te controleren.

De NATO is een grote organisatie en hierdoor zijn de functies binnen de organisatie gescheiden van elkaar. Er bestaan verschillende security officers, die onder leiding staan van een security manager. Hierdoor kan controle op het beleid van de NC3A makkelijk uitgevoerd worden. Het uitvoeren van een audit (stap 8) valt echter buiten de reikwijdte van mijn opdracht.

10.2 Maatregelen

De gekozen maatregelen, met betrekking tot NTK scheiding op geheime beveiligde netwerken, staan beschreven in hoofdstuk acht "Conclusions/ Recommendations" van het adviesrapport. Binnen dit hoofdstuk adviseer ik welke maatregelen er genomen moeten worden voor NTK scheiding op geheime, beveiligde netwerken. Voor het kiezen van een geschikte maatregel heb ik gebruik gemaakt van een methode die door de heer Peter

Groen, EDP-auditor bij PWC, aangeraden was, namelijk selectiecriteria (zie tabel 6). Voor verdere uitleg van de termen in tabel zes verwijs ik naar § 6.5.

Products / Demands	DAC	MAC	Non-Discretionary AC		
	ACL	Rule-based AC	Role-based AC	Task-based AC	Lattice-based AC
NTK Separation	+	+++	++	++	++
Simple to use	++	++	+++	+	+
Administrator friendly	+	+++	+++	+	+
Security	++	+++	++	+++	+++

Tabel 6: Selectiecriteria

Hierdoor was ik in staat advies te geven over een bepaalde toegangscontrole. De eisen die in tabel zes gesteld zijn, zijn voor een deel gebaseerd op tabel vijf op pagina 38, "Betrouwbaarheidseisen uitgezet tegen componenten", maar ook op de eisen die geformuleerd staan in hoofdstuk negen. Hierdoor ben ik tot een viertal eisen gekomen namelijk:

- NTK scheiding; De toegangscontrole moet NTK scheiding ondersteunen;
- Gebruiksvriendelijkheid; De toegangscontrole moet gebruiksvriendelijk zijn voor de gebruiker. De gebruiker moet geen hinder ondervinden van de toegangscontrole om zijn werk goed uit te kunnen voeren;
- Systeembeheer vriendelijk; Het onderhoud en de gebruiksvriendelijkheid van de toegangscontrole moet hoog zijn;
- Beveiliging; Beveiliging moet hoog blijven, dit is van essentieel belang, met name voor een organisatie als de NATO.

De te nemen maatregelen zijn de volgende:

- NTK scheiding op geheime, beveiligde netwerken moet bepaald worden door middel van de procedures, regels en richtlijnen, die beschreven staan in het huidige informatiebeveiligingsbeleid;
- De gebruiker moet een ter zake doende reden opgeven om bepaalde informatie te verkrijgen en zijn classificatieniveau moet dit toelaten;
- Het wachtwoord van de gebruikers moet verschillende karakters bevatten en een aantal hoofdletters, waardoor het lastig wordt om het wachtwoord te kraken;
- De aanschaf van software en hardware moet gebaseerd worden op de toepassingsmogelijkheden en de kwaliteit van het product.

10.3 Procedures

De volgende procedures worden door middel van de maatregelen ingevoerd:

- Andere wachtwoord procedure, in plaats van "password" kan er bijvoorbeeld gebruik worden gemaakt van "P@55w0rD";
- Een procedure om te bepalen welke toegangscontroles, in verschillende situaties, worden gebruikt binnen de NATO;
- Een procedure om de rechten van de gebruikers te bepalen.

10.4 Conclusie

Ik ben tot de maatregelen in § 10.2 gekomen door middel van de voorgaande stappen en de door doelstelling als leidraad te gebruiken. Door het lezen van verschillende artikelen, "Access Control Layers", "Need-To-Know", heb ik informatie over NTK scheiding kunnen vinden. De huidige maatregelen heb ik al beschreven in § 7.2. Een deel van de nieuwe maatregelen is hierop gebaseerd.

11. Evaluatie

11.1 Procesevaluatie

In de procesevaluatie kijk ik terug naar mijn afstudeerperiode. Ik beschrijf hierbij de volgende onderdelen:

- Doel; Het bewijs moet geleverd dat ik de doelstelling heb behaald, zo niet, waarom niet;
- Verschillenanalyse; De geplande tijd en de werkelijke tijd van mijn afstudeerperiode worden met elkaar vergeleken. Daarbij beschrijf ik de belangrijkste verschillen;
- Methoden en technieken; Binnen dit gedeelte wordt beschreven wat ik na afloop van mijn onderzoek van de gekozen methoden en technieken vond;
- Risico's; Binnen dit gedeelte beschrijf ik of ik de risico's voor mijn afstudeerproject goed heb ingeschat en of mijn voorgestelde maatregelen hierbij hebben geholpen en of er aanvullende maatregelen nodig waren;

11.1.1 Doel

De doelstelling van de afstudeeropdracht luidde: Er moet een algemeen rapport geschreven worden over toegangscontroles (access controls) in de context van NTK. De opdrachtgever is NATO zelf, maar de opdracht wordt uitgevoerd bij NATO Consultation, Command and Control Agency (NC3A), afdeling Communications Informations Systems (CIS). Er moet geadviseerd worden over welke mogelijkheden er zijn om NTK goed te beveiligen.

Hierbij is van belang om uit te zoeken aan welke specifieke beveiligingscriteria moet worden voldaan om NTK beveiliging 'goed' te realiseren. Het rapport moet in de huisstijl van de NC3A geschreven worden. Het rapport moet een soortgelijke structuur hebben als het rapport "Windows 2000 Certificate Services"[35]. Daarnaast wordt er gekeken naar de volgende punten:

- Volledigheid van het adviesrapport; Alle mogelijke informatie over methoden, technieken en producten waarin NTK geïmplementeerd kan worden, is onderzocht en beschreven met betrekking tot de NATO.
- Actualiteit van het adviesrapport; Het adviesrapport is gebaseerd op actuele informatie, zoals het vakblad "Informatiebeveiliging". Daarnaast zijn recente producten, "IBM zSeries Mainframe operating system 1.5 en 1.6" (zie adviesrapport hoofdstuk 5, §5.1), op het gebied van technologische

[35] Bijlage A: *Definitieve opdrachtsomschrijving*;

ontwikkelingen binnen de informatiebeveiliging uitgebreid bestudeerd en beschreven;
- ❖ Diepgang van het adviesrapport; Elk onderwerp in het adviesrapport is met diepgang beschreven, zoals de toegangcontroles (zie hoofdstuk 4 van het adviesrapport);
- ❖ Relevantie met de organisatie; Het adviesrapport is geschreven voor de situatie binnen de NATO met betrekking tot geheime beveiligde netwerken.

De doelstelling voor mijn afstudeeropdracht heb ik weten te realiseren. In het adviesrapport[36] heb ik de toegangscontroles beschreven in de context van NTK. In de conclusie van mijn adviesrapport heb ik adviezen beschreven, waarbij ook andere methodes, zoals PKI , software en hardware, geadviseerd worden. Daarnaast heb ik gebruik gemaakt van de huisstijl van de organisatie en de structuur van het voorbeeld document "Windows 2000 Certificate Services". Bij het schrijven van het adviesrapport heb ik ook gebruik gemaakt van de oogst van mijn interview met de heer Peter Groen, EDP-auditor bij PWC.

11.1.2 Verschillenanalyse

De geplande tijd heb ik afgezet tegen de werkelijk bestede tijd per doorgelopen fase gedurende het afstudeerproject (zie tabel 7 op p. 46.). De tabel moet als volgt gelezen worden: de grijze balken geven de geplande tijd weer en de zwarte balken geven de werkelijk bestede tijd weer. Het verschil tussen de geplande tijd en de werkelijk bestede tijd is niet zo groot. Ik had bepaalde activiteiten binnen een fase ruimer ingepland. Hierdoor kon ik meer tijd besteden aan het opstellen van het adviesrapport en aan het schrijven van mijn afstudeerverslag.

[36] Malik, Asim: *Need-To-Know separation on Classified Systems*; NC3A Den Haag; 1e druk; 2004;

Activiteit \ Week nr.	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Oriëntatiefase																			
Projectplanning																			
Analysefase:																			
Uitzoeken beveiligingscriteria																			
Literatuurstudie, CVI																			
Uitvoeringsfase:																			
Ordenen onderzoeksgegevens																			
Opstellen adviesrapport																			
Afstudeerverslag																			

Legenda:

Geplande tijd :
Werkelijke tijd :

Tabel 7: Verschillenanalyse planning

11.1.3 Methoden en technieken

Zoals vermeld staat in hoofdstuk vier heb ik een aantal methoden gebruikt. Dit zijn de volgende methoden:

- De gefaseerde aanpak van het stappenplan van het literatuuronderzoek;
- De gefaseerde aanpak van het acht stappenplan van Oud;
- De projectmanagementmethode "Projectmatig werken".

Ik vond het stappenplan van de gefaseerde aanpak literatuuronderzoek erg nuttig, omdat het structuur bracht in mijn afstudeerproject. De gefaseerde aanpak van het acht stappenplan van Oud vond ik nuttig om mijn activiteiten te plannen en om structuur aan te brengen in mijn afstudeerproject. Dankzij de projectmanagementmethode "Projectmatig werken" kon ik mijn activiteiten in fasen onderverdelen.

11.1.4 Risico's

De risico's die ik beschreven heb in het plan van aanpak heb ik redelijk goed kunnen inschatten. De maatregelen waren echter niet altijd voldoende. Dit geldt voor de volgende twee risico's:

- *Het product kan niet tijdig worden opgeleverd.* De afstudeerder heeft geen ervaring met het plannen van een dergelijk project, activiteiten kunnen te optimistisch zijn ingepland, waardoor tijdnood kan ontstaan. Dit risico kan beperkt worden door de bedrijfsmentor de voortgang te laten bewaken en indien nodig, tijdig bij te sturen. De afstudeerder kan zelf ook aangeven wanneer bijsturing gewenst is. Als aanvullende maatregel heb ik gebruik gemaakt van een projectmanagementmethode "Projectmatig werken" om structuur aan te brengen in mijn afstudeerproject. Daarnaast heb ik gebruik gemaakt van de stappen van een gefaseerde aanpak literatuuronderzoek, maar ook van het acht stappenplan van Oud. De aanvullende maatregel bleek voldoende te zijn.

- *De afwezigheid van de begeleider kan het project ernstig vertragen.* De bedrijfsmentor kan onvoldoende tijd hebben of niet aanwezig zijn voor de afstudeerder. Hierdoor kan het project ernstige vertraging oplopen. Dit risico kan beperkt worden door een vervangende begeleider toe te wijzen[37]. Aan het begin van mijn afstudeerperiode had ik onvoldoende terugkoppeling gekregen van mijn bedrijfsmentor. In deze korte tijd zag ik de noodzaak tot meer maatregelen. Tijdens een overleg tussen mijn bedrijfsmentor, zijn manager en mij werd afgesproken om wekelijkse rapportages op te sturen en terugkoppeling te ontvangen over het adviesrapport. Een vervangende begeleider was in mijn situatie niet voldoende als maatregel maar de aanvullende maatregel wel.

11.2 Productevaluatie

Over het opgeleverde product, "*Need-To-Know separation on Classified Systems"*, ben ik tevreden. De bedrijfsmentor heeft zijn goedkeuring aan het adviesrapport gegeven. Hierdoor voldeed het adviesrapport aan de eisen die aan het begin van mijn afstudeerperiode zijn gesteld:

- Het adviesrapport is in een formele schrijfstijl geschreven;
- Het adviesrapport is in het Engels geschreven;
- Het adviesrapport beschrijft methoden, technieken en producten waarin NTK geïmplementeerd kan worden;
- Alle componenten van de inhoudsopgave, die door de bedrijfsmentor is opgesteld, zijn behandeld;
- Eisen ten aanzien van de volledigheid, diepgang en actualiteit zijn ook gehaald.

[37] Bijlage C: *Plan van aanpak*

Literatuurlijst

Boeken:

Alblas, Gert/ Wijsman, Ella: *Gedrag in Organisaties*; Wolters Noordhoff Groningen; 2e druk; 1998; ISBN 90-010-3213-3

Harris, Shon: *CISSP Certification Exam Guide Second Edition*; Mc Graw Hill Osborne; 1e druk; 2003; ISBN 00-722-2967-5

Jansen, Peter: *Projectmanagement volgens Prince2*; Pearson Education Benelux; 1e druk; 2003; ISBN 90-430-0697-1

Klein, R: *Moduleboek OR-03*; Haagse Hogeschool; 1e druk; 1997;

Longley, D., Shain, M., Caeli, W: *Information Security, Dictionary of Concepts, Standards and Terms*; Stockton Press; 1e druk; 1992; ISBN 05-624-4563-6

Malik, Asim: *Need-To-Know separation on Classified Systems*; NC3A Den Haag; 1e druk; 2004;

NC3A Brochure

Robertson, George: *Security within the North Atlantic Treaty organization*; NATO Brussel; 2002;

Oud, Ernst J.: *Praktijkgids Code van Informatiebeveiliging*; Academic Service Schoonhoven; 1e druk; 2002; ISBN 90-526-1427-X

Parker, B: *PricewaterhouseCoopers information security a strategic guide for business*; PricewaterhouseCoopers Global Technology Centre San Jose; 1e druk; 2003; ISBN 1-891865-11-0

SDM Reader; Haagse Hogeschool Den Haag; 1e druk; 1997;

Weeren-Braaksma, M. (redactrice); *Informatiebeveiliging*; Academic Service Schoonhoven; 1e druk; 2004; ISSN 1569-1063

Wijnen, Gert., Renes, Willem., Storm, Peter.: *Projectmatig werken*; Het Spectrum; 18e druk; 2002; ISBN 90-274-6905-9

Websites:

Access Controls	:	http://www.cs.ru.ac.za/courses/Honours/Security/lectures/Computer%20Security-accesscontrols.pdf
NC3A website	:	http://www.nc3a.nato.int
NTK artikel 1 website	:	http://www.cccure.org/Documents/HISM/021-023.html
NTK artikel 2 website	:	http://www.dss.mil/training/csg/security/S1class/Need.htm
Prince2 website	:	http://www.prince2.com

Zoekmachines:

http://www.google.com

http://www.yahoo.com

http://www.lycos.com

Figurenlijst

Tabellenlijst

Technische termen- en afkortingenlijst

ACQ	: Acquisition
Beschikbaarheid	: De mate waarin de geheime, beveiligde netwerken beschikbaar moeten blijven
CCS	: Command and Control Systems
CIS	: Communication Information Systems
CISSP	: Certified Information Systems Security Professionals
CVI	: Code van Informatiebeveiliging
EDP-auditor	: Electronic Data Processing auditor
Exclusiviteit	: De mate waarin de geheime, beveiligde netwerken exclusief moeten blijven
I&I	: Informatica en Informatiekunde
Integriteit	: De mate waarin de geheime, beveiligde netwerken foutloos moeten blijven
IPS	: Integrated Programme Staff
IPT	: Integrated Programme Teams
MAPGOOD	: Mensen, Apparatuur, Programmatuur, Gegevens, Organisatie, Omgevingen en Diensten
MLS	: Multilevel Security
NAC	: North Atlantic Council
NACISA	: NATO Communications Information Systems Agency
NC3A	: NATO Consultation Command and Control Agency
NIMP	: NATO Information Management Policy
NSC	: NATO Security Committee
NTK	: Need-To-Know
ORFS	: Operation Research Functional Services
PKI	: Public Key Infrastructure, dit is een versleutel (encryptie) methode om berichten en bestanden te versleutelen. Zodat alleen de ontvanger en de zender van het bericht of bestand het kunnen openen.
Prince2	: Projects In Controlled Environments 2
PWC	: PricewaterhouseCoopers
STC	: SHAPE Technical Centre
Toegangscontrole	: De Engelse benaming ervoor is access control, het brengt scheiding van autorisatie en rechten aan in netwerken voor gebruikers. Meestal gebaseerd op een NTK beleid.

Bijlage A: Definitieve opdrachtsomschrijving

Afstudeerblok: 2004-1.1
Studentnummer: 97005749
Afstudeerrichting: BOIV

Achternaam: Malik
Voorletters: A.Z.
Roepnaam: Asim
Adres: Dibbetsstraat 75c
Postcode: 2518 PP
Woonplaats: Den Haag
Telefoon: 070-3623550

Naam bedrijf: NC3A
Afdeling bedrijf: CIS
Bezoekadres bedrijf: Oude Waaldorperweg 61
Postcode bezoekadres: 2501 CD
Postbusnummer: 174
Postcode postbusnummer: 2501 CD 174
Plaats: Den Haag
Telefoon bedrijf: 3743000
Telefax bedrijf: 3743239

Achternaam bedrijfsmentor1: Malewicz
Voorletters bedrijfsmentor1: R
Titulatuur bedrijfsmentor1: Dr.
Doorkiesnummer bedrijfsmentor1: 3743477

Achternaam bedrijfsmentor2: Dhr. Shawcross
Voorletters bedrijfsmentor2: C
Titulatuur bedrijfsmentor2:
Doorkiesnummer bedrijfsmentor2: 3743047

Doorkiesnummer afstudeerder: 3743436

Titel afstudeeropdracht:

"Need- To- Know" scheiding op geheime, beveiligde netwerken bij NC3A

Omschrijving afstudeeropdracht:

Inleiding (organisatorische omgeving, kader, historie):

Korte schets van de organisatie:

De opdracht wordt uitgevoerd bij de NATO Consultation, Command and Control Agency (NC3A). Omdat mijn opdracht hier zal worden uitgevoerd, geef ik een korte beschrijving van de organisatie. De afdeling waar ik werkzaam zal zijn, is bij Communication and Information Systems (CIS).

NC3A is een onderdeel van de NATO die gespecialiseerd is in de technische kant van de NATO. NC3A zorgt bijvoorbeeld voor het aanleggen van communicatie netwerken ter ondersteuning van de troepen op vredesmissies.

De NC3A is opgedeeld in meerdere afdelingen, namelijk:

- Integrated Programm Staff;
- Operation Research;
- Communication and Information Systems;
- Command and Control Systems;
- Acquisition;
- Resources.

Beveiliging is een heel actueel onderwerp en steeds meer organisaties willen hun gegevens zo goed mogelijk beveiligen. Er is een beveiligingsplan aanwezig voor de NATO over geheime, beveiligde netwerken. In het beveiligingsplan wordt beschreven welke geheime, beveiligde netwerken er allemaal aanwezig zijn. Gebruikers worden ingedeeld per geheim, beveiligd netwerk om zo bepaalde informatie af te schermen voor andere gebruikers. In het beveiligingsplan wordt echter niet beschreven hoe binnen een geheim, beveiligd netwerk autorisatie wordt verleend aan gebruikers.

Een belangrijk onderdeel van beveiliging bij de NATO is op "Need-To-Know" (NTK) basis ingericht. "Need-To-Know" is een term die in de context van beveiliging van informatie wordt gebruikt. Het houdt in informatie die alleen toegankelijk is voor een bepaalde gebruiker met de juiste toegang.

Probleemstelling:

Welke mogelijkheden zijn er om voor een goede NTK beveiliging binnen de NATO te zorgen?.

Doelstelling van de opdracht:

Er moet een algemeen rapport geschreven worden over toegangscontroles (access controls) in de context van NTK. De opdrachtgever is NATO zelf, maar de opdracht wordt uitgevoerd bij NATO Consultation , Command and Control Agency (NC3A), afdeling Communications Informations Systems (CIS). Er moeten mogelijkheden geadviseerd worden om NTK goed te beveiligen.

Hierbij is van belang om uit te zoeken aan welke specifieke beveiligingscriteria moet worden voldaan om NTK beveiliging 'goed' te realiseren. Het rapport moet in de huisstijl van de NC3A geschreven worden. Het rapport moet een soortgelijke structuur hebben als het rapport "Windows 2000 Certificate Services".

Uitgangssituatie:

a. Benodigde software:

- MS Word.

b. Benodigde hardware:

- PC;
- Laptop;
- Printer.

c. Beschikbare rapporten:

Voorbeeld documentatie: "Windows 2000 Certificate Services"

d. Aanwezige ideeën:

Concrete werkzaamheden:

- Oriëntatiefase:
  - Oriënteren op de opdracht.
- Projectplanning:
  - Plan van aanpak maken
- Analysefase
  - Uitzoeken beveiligingscriteria;
  - Literatuurstudie;
  - Code voor informatiebeveiliging;
  - Projectmatig werken van Wijnen.
- Uitvoeringsfase:
  - Ordenen onderzoeksgegevens;
  - Opstellen adviesrapport.

a. Te gebruiken technieken:

- Interviewen;
- Observatie.

b. Te gebruiken methoden:

- Literatuurstudie;
- Het achtstappen plan van Oud bij de CVI (Code Voor Informatiebeveiliging), gedeeltelijk gebruiken;
- Projectmatig werken van Wijnen, gedeeltelijk gebruiken.

c. Te vermelden nadrukken:

Eventueel aanvullende opmerkingen:

Resultaten voor de opdrachtgever (op te leveren producten):

Adviesrapport "Need-To-Know" scheiding op geheime, beveiligde netwerken bij NC3A.

Bijlage B: Engelse opdrachtsomschrijving

Name: Need-To-Know separation on classified networks
Background: One of the pillars of NATO Security is Need-To-Know (NTK). NATO Communication and Information Systems (CIS), do not necessarily provide good NTK boundaries and their protection. Taking as one example the various local NATO Secret (NS) LAN's (or subjects and objects on the NS WAN), there are very little protection mechanisms as a minimum, NS, CIS have been implemented such that once subject is recognized as a authorized user, he/she has the capability of searching and finding data for which no NTK for this person exists.

Aim of Task: The task will assess the specific coverage areas that NTK need to address, placing NTK in proper place of CIS security infrastructure. Theoretical solutions to provide NTK will then be identified that address these areas. The task will also identify tools being offered by the COTS market support NTK.

Scope of Tasks: Since NATO does not have CIS's which provide, through their inherent security policies, the functionality and assurance to implement mandatory NTK restrictions, the task need to come up with solutions that provide NTK protection using the extent CIS infrastructures. Another big concern is the "user friendliness" of such solutions, since, if the mechanisms are too cumbersome or demanding, implementation of these solutions might either be refused or ways to circumvent them will be found by both administrators and users. Since more and more information is posted on NATO Intranet Web Sites, the task should look at ways to improve the NTK mechanisms for the web-based information. Simple Identification and Authentication (I&A) mechanisms can be found already on a number of pages, but these provide just weak protection. Information objects (or entire areas of a page, or a page by itself) should be accompanied by meta data, featuring, inter alias, the security classification level and straight forward, easy to implement and maintain Access Control Lists (ACL), the granularity of these could be for example:

- ALL (not NTK restrictions)
- HEADQUARTERS (x,y)
- DIVISION (all members of Division x,y..)
- SECTION (all members of Section x,y..)
- INDIVIDUALS

and any feasible permutation. These ACLS's need to be synchronized with Discretionary access control (DAC) mechanism of the operating system, DBMS, Applications SW. Secure XML could be a option to get this in a organized and secure fashion. Also, audit information about which subject accessed which object should be gathered.
Using PKI, in future, should be considered to support or replace the above proposed mechanisms.
Deliverables: Written report describing the possible NTK solutions and tools determined to be of significant use to NATO CIS.
Risks/Problems/Areas of Concern: The report will be a "snapshot in time" o the state-of art, solutions and tools in the market place.

Bijlage C: Plan van aanpak

1. Inleiding

In dit document wordt beschreven hoe het onderzoek naar het schrijven van een adviesrapport wordt uitgevoerd.

2. Opdracht

2.1 Titel

De titel van de opdracht luidt: "Need-To-Know" scheiding op geheime, beveiligde netwerken bij NC3A

2.2 Probleemstelling

Welke mogelijkheden zijn er om voor een goede NTK beveiliging binnen de NATO te zorgen?.

2.3 Doestelling van de opdracht

Er moet een algemeen rapport geschreven worden over toegangscontroles (access controls) in de context van NTK. De opdrachtgever is NATO zelf, maar de opdracht wordt uitgevoerd bij NATO Consultation , Command and Control Agency (NC3A), afdeling Communications Informations Systems (CIS). Er moeten mogelijkheden geadviseerd worden om NTK goed te beveiligen.

Hierbij is van belang om uit te zoeken aan welke specifieke beveiligingscriteria moet worden voldaan om NTK beveiliging 'goed' te realiseren. Het rapport moet in de huisstijl van de NC3A geschreven worden. Het rapport moet een soortgelijke structuur hebben als het rapport "Windows 2000 Certificate Services".

2.4 Afbakening

Om tijdens het project geen onduidelijkheden over het beschouwen gebied te krijgen, was het belangrijk om vanaf de start al een afbakening te maken. De afbakening is dat de opdracht alleen zal gaan om het schrijven van een adviesrapport over "Need-To-Know" scheiding op geclassificeerde netwerken.

3. Organisatie

3.2 Opdrachtgever

De oorspronkelijke opdrachtgever is de NATO maar wordt uitgevoerd bij het NC3A, vertegenwoordigd in de persoon van Dhr. Dr. Robert Malewicz.

Naam	Functie	Locatie	Telefoon
Dhr. Chuck Shawcross	Afdelingshoofd	NC3A	070-3743047
Dhr Dr. Robert Malewicz	Bedrijfsmentor	NC3A	070-3743477
Dhr. Asim Malik	Afstudeerder/ Consultant	NC3A	070-3743436

De verschillende contactpersonen hebben ieder hun eigen verantwoordelijkheid binnen het project. De verschillende functies in het project worden hieronder opgesomd met hun omschrijving:

- Afdelingshoofd:
  Heeft de afstudeerder de opdracht toegewezen via de bedrijfsmentor;
- Bedrijfsmentor:
  Heeft de supervisie over de inhoudelijke kant van het project en de procesgang;
- Afstudeerder/ Consultant:
  Uitvoerder van het project.

3.3 Verantwoordelijkheden

De afstudeerder zal verantwoording afleggen aan:

- Bedrijfsmentor:
  Minstens 1 keer per week wordt er met de bedrijfsmentor een overleg gehouden om eventuele vragen te stellen en de voortgang van het project te bespreken. In de bespreking met de bedrijfsmentor kunnen besluiten worden genomen of acties ontstaan. Verder kunnen gesprekken worden gehouden over de inhoud van de opdracht wanneer dit nodig blijkt.

3.4 Contractuele voorwaarden

Bij aanvang van het project dienen door de afstudeerder en opdrachtgever een contract ondertekend te worden. Dit contract kent de volgende voorwaarden:

- Alle informatie betrokken bij dit project wordt gezien als vertrouwelijk en mag daarom ook niet openbaar gemaakt worden. Alle documentatie die naar school wordt verzonden, heeft als enige doel beoordeling van de afstudeerder;
- De afstudeerperiode loopt van 9 februari 2004 tot 11 juni 2004;

4. Project

4.1 Randvoorwaarden

De volgende randvoorwaarden zijn voor dit project te onderkennen:

- Het adviesrapport wordt geschreven volgens de wensen en eisen van de opdrachtgever;
- De benodigde software en hardware, zie hoofdstuk 5 paragraaf § 5.2 Software en hardware, zal beschikbaar moeten worden gesteld;
- De bedrijfsmentor is tijdens kantooruren bereikbaar voor vragen of ondervonden problemen.

4.2 Uitgangssituatie

Er is geen documentatie aanwezig over "Need-To-Know" scheiding op geclassificeerde netwerken. Informatie moet worden opgezocht op het Internet en uit boeken.

4.3 Risico's

Het project heeft de volgende risico's:

- *Het onvoldoende vinden van informatie over betreffende onderwerp.* De afstudeerder kan onvoldoende informatie vinden over het betreffende onderwerp. Hierdoor kunnen bepaalde activiteiten meer tijd in beslag nemen. Dit risico kan beperkt worden door tijdig de bedrijfsmentor te informeren.

- *Het product kan niet tijdig worden opgeleverd.* De afstudeerder heeft geen ervaring met het plannen van een dergelijk project, activiteiten kunnen te optimistisch zijn ingepland, waardoor tijdnood kan ontstaan. Dit risico kan beperkt worden door de bedrijfsmentor de voortgang te laten bewaken en indien nodig, tijdig bij te sturen. De afstudeerder kan zelf ook aangeven wanneer bijsturing gewenst is.

- *De afwezigheid van de bedrijfsmentor kan het project ernstig vertragen.* De bedrijfsmentor kan onvoldoende tijd hebben of niet aanwezig zijn voor de afstudeerder. Hierdoor kan het project ernstige vertraging oplopen. Dit risico kan beperkt worden door een vervangende begeleider toe te wijzen.

5. Uitvoering

5.1 Methoden en technieken

Er zal gebruik worden gemaakt

- Literatuurstudie;
- Interviewen;
- Bestuderen van documentatie;
- Observatie.

5.2 Software en Hardware

De software die tijdens het project zal worden gebruikt is:

- MS word;
- Visio 2003;
- MS project 2003;
- Adobe acrobat.

De hardware die tijdens het project zal worden gebruikt is:

- PC;
- Laptop;
- Printer.

6. Planning

Op te leveren produkten:

- Adviesrapport "Need-To-Know" scheiding op geheime beveiligde netwerken bij NC3A.

Uit te voeren activiteiten

- Schrijven van plan van aanpak;
- Literatuurstudie;
- Schrijven adviesrapport "Need-To-Know" scheiding op geheime beveiligde netwerken bij NC3A;
- Schrijven afstudeerverslag.

Uiteindelijke planning

Week nr. / Activiteit	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Oriëntatiefase																			
Projectplanning																			
Analysefase:																			
Uitzoeken beveiligingscriteria																			
Literatuurstudie, CVI																			
Uitvoeringsfase:																			
Ordenen onderzoeksgegevens																			
Opstellen adviesrapport																			
Afstudeerverslag																			

Bijlage D: Interview vragen

Dit interview vond plaats met de heer Peter Groen, EDP auditor bij PricewaterhouseCoopers, op vrijdag 9 april om 16:30 in de middag het gesprek nam ongeveer anderhalf uur in beslag.

Vraag 1:

Wat is uw functie binnen het bedrijf?

Vraag 2:

Wat kunt u mij vertellen over NTK?

Vraag 3:

Wat voor methoden zijn er aanwezig waarin NTK geïmplementeerd kan worden?

Vraag 4:

Wat voor producten zijn er aanwezig die gebruik maken van het NTK principe?

Vraag 5:

Hoe kan ik mijn adviesrapport nog beter maken?

Vraag 6:

Hoe kan ik mijn conclusie beter beargumenteren?

NATO UNCLASSIFIED

NATO Consultation, Command and Control Agency
Agence de Consultation, de Commandement et de Conduite des Opérations de l'OTAN

Technical Note

NEED-TO-KNOW SEPARATION ON CLASSIFIED SYSTEMS

FINAL

Asim Malik

June, 2004
The Hague

NATO UNCLASSIFIED

FINAL

CONDITIONS OF RELEASE

With reference to NATO Documents C-M(55)15(Final) and AC/322-D/1, this document is released to a NATO Government at the direction of the NATO Consultation, Command and Control (C3) Agency subject to the following conditions:

1. The recipient NATO Government agrees to use its best endeavours to ensure that the information herein disclosed, whether or not it bears a security classification, is not dealt with in any manner (a) contrary to the intent of the provisions of the Charter of the NATO C3 Organization, or (b) prejudicial to the rights of the owner thereof to obtain patent, copyright or other likely statutory protection therefor.

2. If the technical information was originally released to the Agency by a NATO Government subject to restrictions clearly marked on this document the recipient NATO Government agrees to use its best endeavours to abide by the terms of the restrictions so imposed by the releasing Government.

Technical Note

NEED-TO-KNOW SEPARATION ON CLASSIFIED SYSTEMS

Asim Malik

Communications Systems Division

Abstract

Classification Abstract

This Note describes an investigation into NTK separation on classified systems for NATO and theoretical solutions to provide NTK will then be identified that address these areas.

The work described in this report was carried out under Project of the NC3A Programme of Work for and was concluded in June 2004

This document is a working paper that may not be cited as representing formally approved NC3A opinions, conclusions or recommendations.

Approved: _____

NATO Consultation, Command and Control Agency
The Hague
June 2004

This document consists
of 41 pages
(excluding covers)

This page is left blank intentionally

SUMMARY

As classified information in today's world keeps growing the need for information security also grows. Restricting users to classified machines and unclassified machines is not enough. Separation of duties and privileges has to be applied in order to safeguard the classified information. By doing so users are only given access to classified information that is work related.

This document addresses methods and ways how "Need-To-Know" (NTK) separation can be implemented and which products are available that support NTK separation. The primary focus of this assessment was what kind of methods and products are available in which NTK separation could be implemented.

On the whole the access controls provide a good way to separate duties and privileges on NTK criteria. Depending on the situation and organization there are several ways in which access controls can be used for NTK separation. Discretionary access control (DAC), the owner of a classified file can decide based on NTK criteria which user he can give access to. The problem is the user can copy the file and give it to someone else who does not have the right NTK privileges. Mandatory access control (MAC) provides much better conditions for NTK separation application, access to data is based on the sensitivity (represented by a label) of the data and on formal authorization (i.e. clearance) of users to access this sensitive information. In the Non-Discretionary access control group, three main types of access controls can be identified: role-based access control, lattice-based access control and task-based access control. Role-based access control can separate users based on their role within an organization, but users with the same role have the same privileges within that role. Lattice-based access control provides an upper bound and lower bound of access capabilities for every user and file relationship. This is a very complex access control to manage and maintain. Task-based access control is the authorizations of tasks rather than users and files. Task-based access control would be suitable to use in a distributed computing and information processing activities. The choice depends on which environment and organization the access control is going to be used in. In an organization where security plays a high role it is best to use an access control in which the user can be limited in his privileges and can get only access if he/she fulfils defined NTK criteria. Also several products have been reviewed in this document that use access control methods.

Another method that gives users an access, based on their NTK criteria, is PKI. There are two kinds of encryption methods discussed in this document: symmetric and asymmetric encryption. The asymmetric encryption is the most secure way for a user to access information on NTK criteria. It makes use of a set of two separate, public and secret, keys for encryption and decryption, while the symmetric encryption makes use of one secret key to encrypt and decrypt.

Web-based NTK mechanisms are also discussed in this document. There are several mechanisms available. All the mechanisms provide a similar way for a user to be granted access on NTK criteria.

At the end of this document conclusions/recommendations will be discussed.

This page is left blank intentionally

TABLE OF CONTENTS

This page is left blank intentionally

1. INTRODUCTION

In the beginning information was represented through different media. Media like stone tablets, papyrus and finally paper. People used physical means to secure their valuable information that was written on it. As long as information was written on those media, protecting that information was easy. People used vaults, secret places and/or banks to hide their valuable information.

Nowadays there is an enormous amount of information and most of it has a digital representation, it is being stored as a sequence of bits in mass storage media, sent through public communications and processed in computer network systems.

Since information itself, having digital representation, has no material form, it is a very specific asset and more difficult one to protect than traditional assets. For example stealing information is an act that can be easily hidden because stolen information does not change its location (opposite to traditional assets).

As a result the information securing process is much more complex. The computer network environment makes information much more susceptible to varied threats. There are several kinds of threats for a network environment.

An outside attacker who is not authorized to access (logon to) the system can use several attacks to get an unauthorized access into a computer system. One of these attack methods is a dictionary attack. This also refers to breaking a cipher, or obtaining a password by running through a list of likely keys, or a list of words. Brute force attack is another method of attacking a network environment, e.g. guessing passwords, wardialing telephone numbers. Also spoofing at login can be recognised as one of these attack techniques, where an attacker can use a fake login screen in which a user fills in his/her username and password and send it to the attacker without the user's knowledge. A countermeasure for such an attack is creating a trust path by using strong authentication and cryptographic techniques.

Given the variety of threats, the computer network environment has to be secured using a wide range of security techniques applying a concept of defense-in-depth. One of the techniques to secure classified information in a network environment is an access control defined and based on Need-To-Know (NTK) criteria.

Within every organization there usually is classified information. This information is not for everyone to access. Who has an access and who does not have one to a classified file can be decided also through NTK criteria.

2. BACKGROUND

This chapter describes the background of the task, the aim of the task, the scope of the task and the document organization.

2.1 BACKGROUND OF THE TASK

One of the pillars of NATO Security is NTK. NATO Communication and Information Systems (CIS), do not necessarily provide good NTK boundaries and their protection. Taking as one example the various local NATO Secret (NS) LANs (or subjects and objects on the NS WAN), there are very little protection mechanisms. As a minimum NS systems have been implemented such that once subject is recognized as an authorized user, he/she has the capability of searching and finding data even if no NTK for this person exists.

2.2 AIM

The task will assess the specific coverage areas that NTK needs to address, placing NTK in proper place of Communication & Information System (CIS) security infrastructure.

Theoretical solutions to provide NTK will then be identified that address these areas. The task will also identify tools being offered by the Commercial-Of-The-Shelf (COTS) market support NTK.

2.3 SCOPE

The scope of this investigation was constrained by looking into NTK separation within a classified network. What is the best way to control NTK and what means and solutions are available to implement NTK on a classified network.

2.4 DOCUMENT ORGANIZATION

In the first chapter an introduction is given. It describes how information security evolved and describes various security threats.

The second chapter gives background information on the task, aim, scope and document organization. It will also describe data separation for NATO networks.

In the third chapter the principal of NTK is explained. A definition and an example of NTK will be given. This example will also be explained through an illustration (figure 1).

The fourth chapter discusses access control models in the context of methods to give rights and permissions to users based on NTK criteria. The pros and cons, through examples and illustrations, of the access control models are also being discussed.

The fifth chapter covers NTK product solutions. These are products that are available on the market where NTK can be implemented. The performance of the products, in a NTK context, is explained through examples.

The sixth chapter discusses solutions based on PKI in a NTK context. Encryption methods, symmetric and asymmetric encryption, being used in PKI are reflected on NTK perspective through examples and illustrations.

The seventh chapter discusses Web-based solutions suitable for NTK mechanisms implementation.

Chapter eight concludes this report with conclusions\recommendations. An overview will be given of all the subjects that have been discussed in this document.

3. NEED-TO-KNOW

NTK is based on the concept that individuals should only be given an access to information that they absolutely require in order to perform their job duties. Giving any more rights to a user can cause problems and the possibility of abusing the permissions assigned to the user. What information the user needs to be equipped in performing his/her task refers to NTK principles. Hence, NTK refers to knowledge. The least privilege principle, related to the NTK, refers to what the user can do with the information [6].

The typical administrative rule in an organization is to give (according to least privilege principle) a user the least amount of privileges to the least amount of data necessary to keep him/her productive when carrying out tasks. Those principles are being applied by defined appropriate regulations in security policies, guidelines, and directives. This will be explained in the example below.

Management's role is to create and/or co-ordinate definition of a set of security policies, guidelines and directives that should then be applied in an organisation (figure 1). One of the aspects that needs to be reflected in the documents is NTK criteria definition. When NTK criteria is applied, it is the principle with the least privileges that defines the type of operations allowing users to execute data (read, write, modify, delete, etc). The NTK criteria should be defined in such a way that it is easy to apply when creating a new user's profile on a computer network, and is later easy to manage and control.

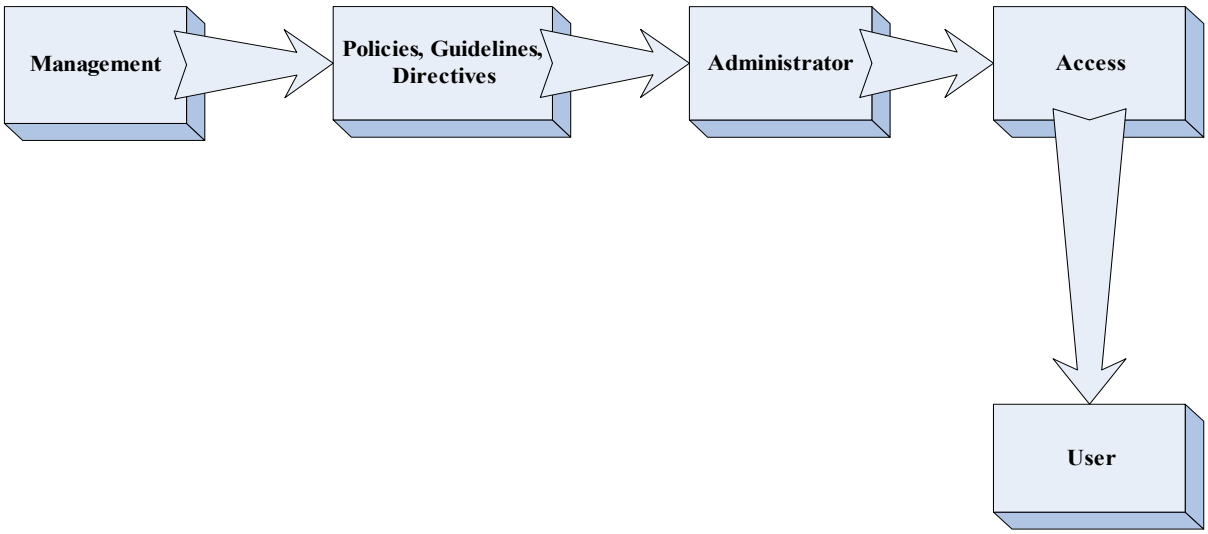


Figure 1: NTK Example

NTK criteria provides access control definitions that are to be applied in order to access information on a computer network. However, NTK criteria is only one solution for defining access controls. Depending on the organization and its particular demands there are several access control models that can be applied, in which NTK has to be implemented. These access control models will be discussed in the next chapter.

4. ACCESS CONTROL MODELS

This chapter discusses, through examples and illustrations, the access control models that are available in which NTK can be implemented. Also the pros and cons, of the access controls, are being discussed in this chapter.

4.1 SECURITY TRIAD

The need for information security occurred when multi-user computer systems were introduced. This need gained significance as computer systems evolved from isolated mainframes behind protected doors to interconnected and decentralized open configurations. As a result information exchange kept growing. There was public information, accessible to everyone, and protected information, where the access was limited exclusively to the legitimate users, often both existing in one computer system. New threats and challenges following from that situation led to emerging and rapid development of Information Security (INFOSEC) units.

Information security (INFOSEC) is based on three tenets (figure 2), there separate but interrelated objectives:

- Confidentiality (or secrecy), related to disclosure of information;
- Integrity, related to modification of information;
- Availability, related to denial of access to information.

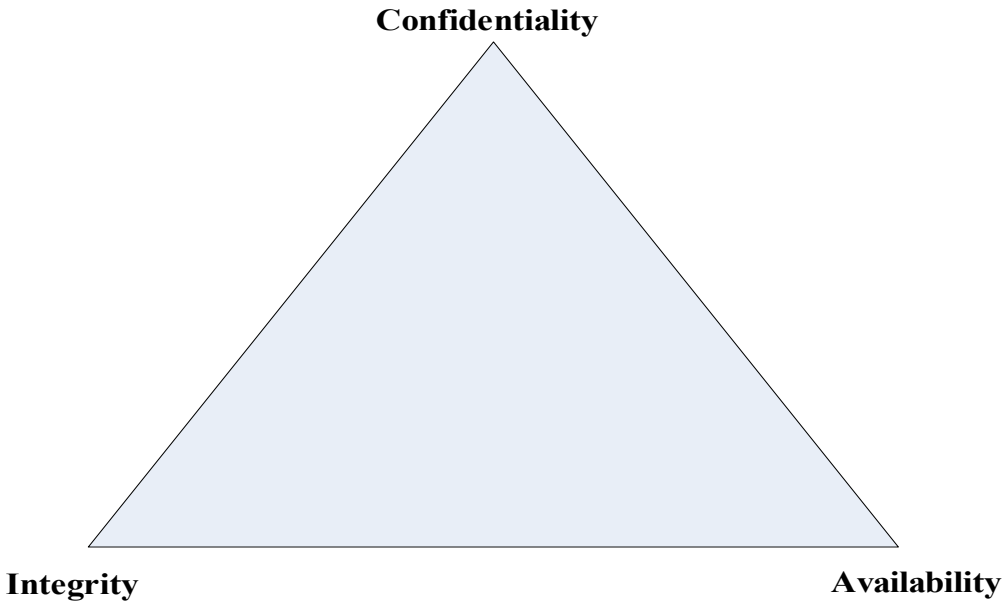


Figure 2: Security Triad

Information flow is clearly focused on confidentiality and also applies to integrity to some extent. The primary concern of access control models is confidentiality. Also access control models can deal with some aspects of integrity. E.g. access control models can determine "read/execute" type of access, in which it directly supports confidentiality, or "write/delete" type of access, in which it directly supports integrity.

4.2 ACCESS CONTROL MODELS

Access control is the collection of mechanisms that exercises a directing or restraining influence over behavior, usage and content of a system. Among others it allows management to specify what users can do, which resource they can access and what operations they can perform. This report is focused on the NTK aspect of the access control mechanisms. With discussing every access control model a question has to be asked whether it is possible to implement NTK with a certain access control model.

There are three types of access control models, i.e. Mandatory Access Controls (MAC), Discretionary Access Controls (DAC), and Non-Discretionary Access Controls (Non-DAC):

- Mandatory Access Control (MAC)
  - Rule-based Access Control.
- Discretionary Access Control (DAC)
  - User-Directed DAC, identity-based AC and/or a hybrid AC.
- Non Discretionary Access Control (Non-DAC)
  - Role-based Access Control;
  - Lattice-based Access Control;
  - Task-based Access Control.

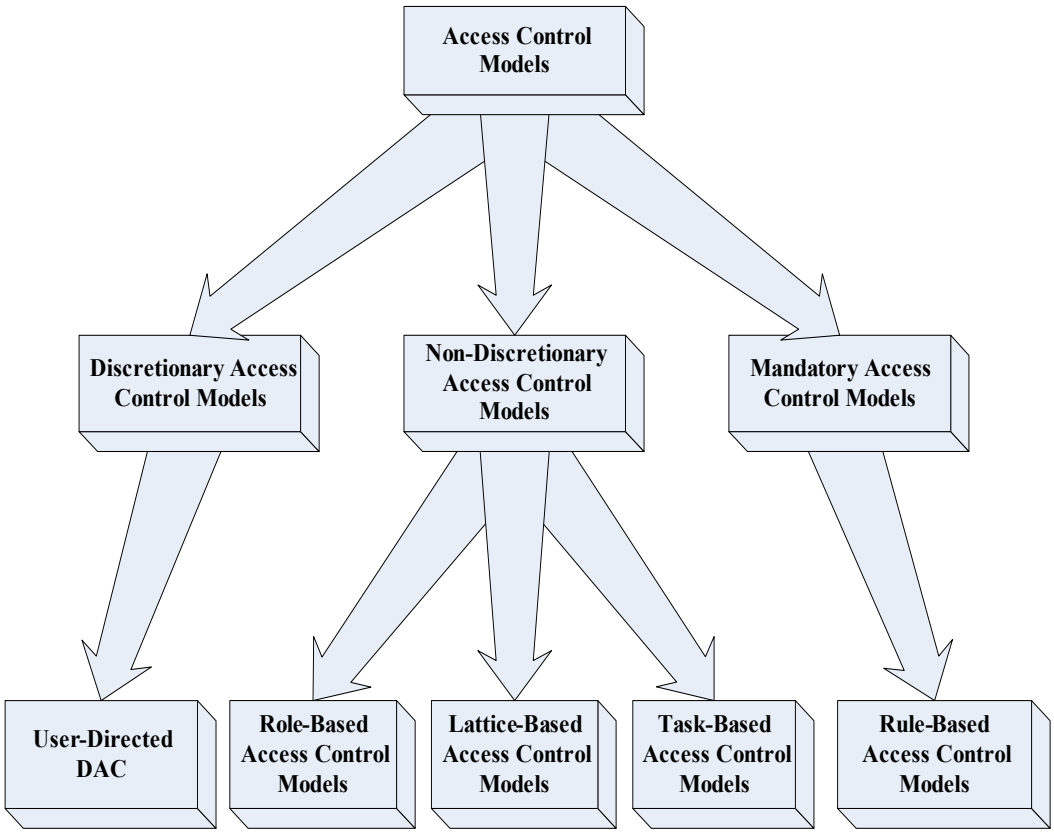


Figure 3: Access Control Models Diagram

4.2.1 Mandatory Access Control

In the Mandatory Access Control (MAC) model access to data is based on the sensitivity (represented by a label) of the data and on formal authorization (i.e. clearance) of users to access this sensitive information [5].

Users are given a security clearance (secret, top secret, confidential, and so on), and data is classified in the same way. The classification is stored in the security labels of the resources. The classification label specifies the level of trust a user must have to be able to access the data. It is based on the clearance of the user and the classification of the data. The rules for how users access data in a computer network are defined by management in security documentation, configured by the system administrators, enforced by the operating system, and supported by security technologies.

Security labels are attached to all objects. Thus, every file, directory, and device has its own security label with its classification information. A user may have a security clearance of secret, and the data that he requests may have a security label of top secret. In this case, the user will be denied because his clearance is not equivalent or superior to the classification of the file. An operating system has to be purchased that has been specifically designed to enforce MAC rules, e.g. SE Linux by NSA and Secure Computing.

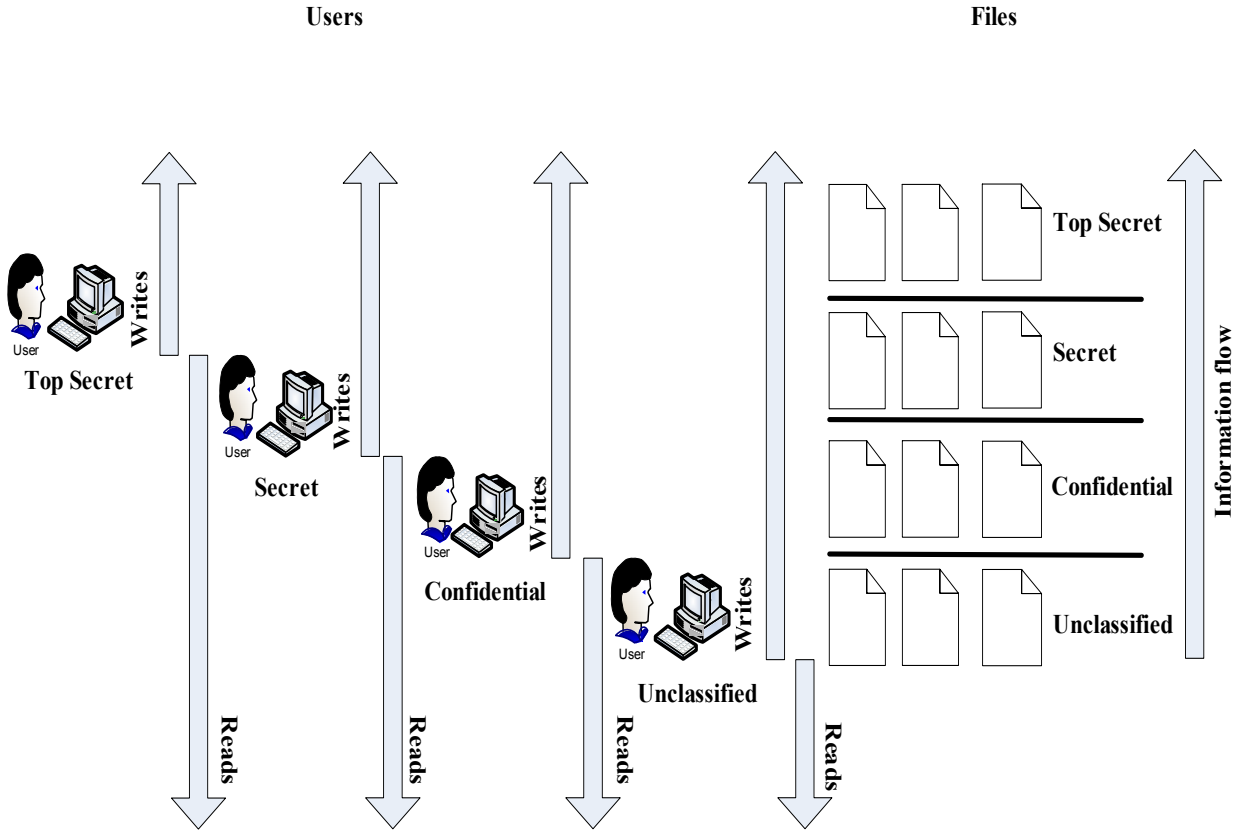


Figure 4: The MAC Model

- Users and files in a system have a certain classification;
- Read up: A user's integrity level must be dominated by the integrity level of the file being read;
- Write down: A user's integrity level must dominate the integrity level of the file being written.

Example 1

This example refers to figure 5. There is a classified file with classification top secret. The file belongs to the following categories: projects, budgets and tasks. User A has classification top secret but he/she does not have a need to know about any of the listed categories: projects, budgets and tasks. Hence, if NTK rules are applied, the user cannot get any access to this file. As one can see the categories portion of the label enforces NTK rules as an additional criteria for access control.

Example 2

This is the same example as the one above but with another user. User B has classification top secret and a need to know about the categories: projects, budgets and tasks. NTK rules are applied granting user B access to this file. User B then has access to any of the listed categories.

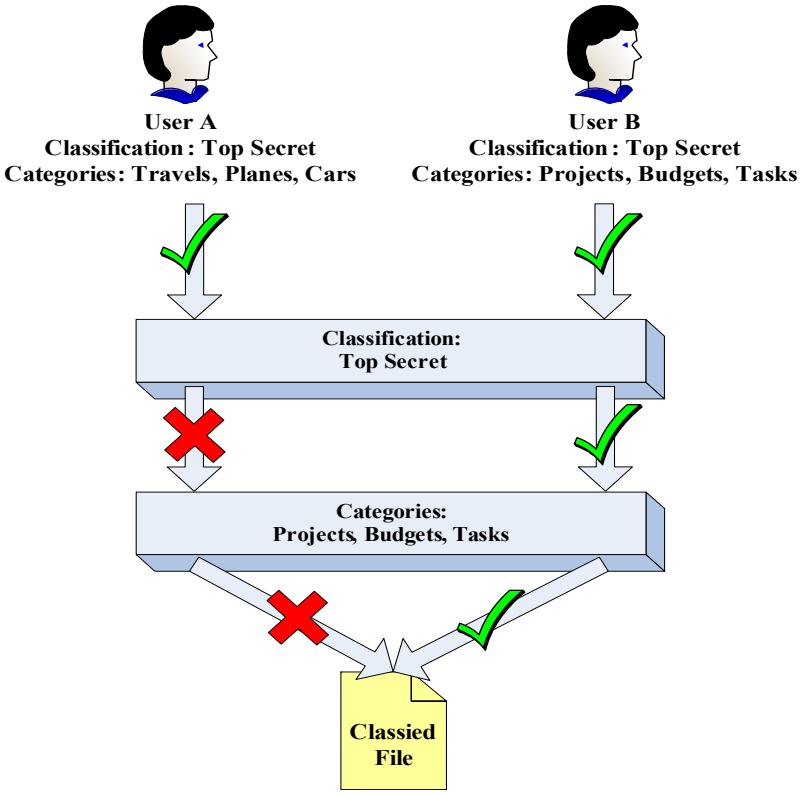


Figure 5: Sensitivity Label

The advantages of using MAC are:

- Users can be given a specific access within specific areas of a file, thus limiting the risk of breaching in a system. Hence, users with different NTK criteria cannot access the file if their NTK criteria does not allow it.

The disadvantages of using MAC are:

- Information flow can pass through covert channels in prohibited ways;
- There is no solution to the interference problem where high information is deduced by low information, assembled and combined intelligently.

4.2.1.1 Rule-based Access Control

This type of control further defines specific conditions; rules that indicate what can and cannot happen to an object that is being requested. It is a kind of MAC because the administrator sets the rules and the users cannot modify these controls [6]. A rule-based control means that everyone is restricted by it no matter what his identity is.

Rule-based access control systems allow users to access systems and information based on pre-determined and configured rules. Rules can be established that allow access to all end-users coming from a particular domain, host, network, or IP addresses. If their roles within the organization are changed their existing authentication credentials remain in effect and do not need to be re-configured.

Many routers and firewalls use rules to determine which types of packets are allowed to pass into a network and which ones are rejected.

Advantages of the rule-based access control are:

- From a security perspective one of the primary advantages of using a rule-based access control approach is that the "principle of least privilege" can be applied;
- Rule-based access control provides ease of understanding and management. A user's role can be tied to a well defined list of NTK access privileges that are required for a specific task;
- Scalability is another important issue. In an area where the number of users far exceeds the number of required roles, it is much easier to administer privileges of a small number of roles;
- Separation of duties based on NTK criteria can be enforced this makes roles mutually exclusive such as requiring that a person cannot have both a communication officer role and a transport officer role;
- Inheritance can reduce the number of explicitly stated access privileges by using a hierarchical role structure such that a superior role inherits all the privileges from a subordinate role. For example, a sergeant's privilege automatically (and implicitly) inherits the privileges of the private. The sergeant's NTK criterion is higher than the private's NTK criteria;
- Delegation of duties further simplifies privilege management. A role can be delegated to another user without having to explicitly change the delegate's access privileges. If role hierarchy is supported, a subordinate role can be delegated instead of the entire role. This principle is also used in role-based access control (paragraph 4.2.3.1).

Rule-based access control provides specific rules that indicate the actions a user is allowed. NTK separation can be implemented in rule-based access control.

4.2.2 Discretionary Access Control

Discretionary access control (DAC) is a means of restricting access to files in a computer system based on the identity of users and/or groups to which they belong. The controls are discretionary in the sense that a user with a certain access permission is capable of passing that permission on to any other user. A system that uses DAC enables an owner of the resource to specify which users can access specific resources. This access control model is called discretionary because the control of access is based on the discretion of the owner. The following example will explain how NTK can be used in a DAC environment [5].

Example

In this example there is a classified file that contains information about communication networks. The classified file may only be accessed on NTK criteria. The owner of the classified file can specify which user can access his classified file. There is user A and user B. User A is working on a project about communication networks and user B is working on a financial project. Given that data in the classified file is related to the work being performed by user A (NTK criteria are met), the owner of the file may grant user A access to the file. User B's NTK criteria indicates no need to know about the content of the file (NTK criteria are not met) therefore access is denied for user B by the owner of the classified file.

In the example above the owner controls which individual users and/or groups get access to certain classified files. Through the example it becomes clear how NTK can be implemented within a DAC environment and in practice it may lead to problems during implementation. One must find a way during implementation to keep an overview of the users who have access to classified files. This won't lead to any problems in a small organization, but in a big organization it may become a problem.

The biggest benefit of using NTK within a DAC environment is the case in which the administration of permissions can be maintained. For example, the network administrator can allow file owners to control who has access to their files. The most common implementation of DAC is through ACL's which is dictated and set by the owners and enforced by the operating system.

Example

In the DAC environment user A can share his D: drive with user B, so user B can copy all of user A's classified files. User A can also block access to his D: drive from his manager so his manager does not know that user A is sharing his classified files with user B.

The above given extreme example reflects an instance of ACL's enforcing the DAC model.

The advantages of using DAC are:

- Users can specify without an administrator who can get access to their files and who can not.

The disadvantages of using DAC are:

- It is difficult to get an overview which users have access to classified files;
- It is difficult for users to keep track to which they have given access to their files. This problem is particularly awkward when access to their files has been given to third parties;
- Does not provide real assurance on the flow of information in a system;
- Does not impose any restriction on the usage of information by a user once the user has received it;
- Files are at the whim or fancy of their owners to grant access to them for other users;
- Information can be copied from one file to another, so access to a copy is possible even if the owner of the original does not provide access to it.

Other types of DAC are a user-directed access control and an identify-based access control/or hybrid access control. When a user within certain limitations has the right to alter the access control to certain files, this is termed as user-directed. An identify-based AC and/or hybrid AC is a type of DAC based on an individual's identity. In some instances, a hybrid approach is used, which combines the features of user-based and identity-based DAC.

Figure 6 shows a hybrid model where the administrator can control which users can access specific files within the network environment and data owners can control which users can access the resources they are responsible for.

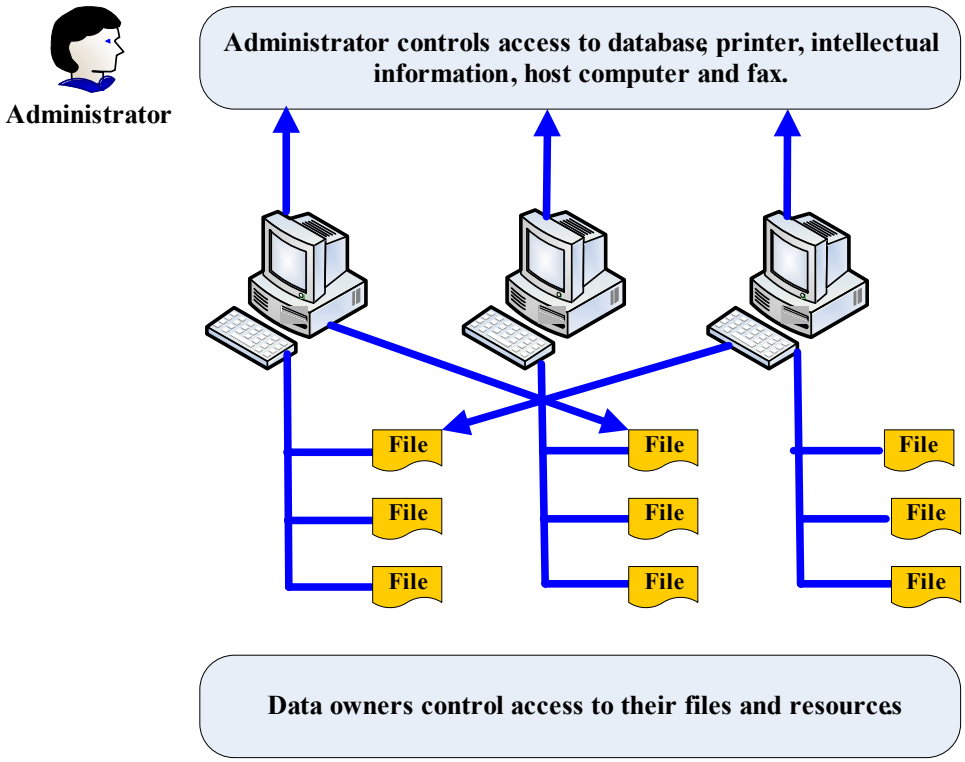


Figure 6: Hybrid Access Control Administration Example

The next section describes a DAC implementation that is commonly used which is called Access Control List (ACL).

4.2.2.1 Access Control List

An Access control list (ACL) stores the access rights to a file with the file itself. An ACL therefore corresponds to a column of the access control matrix (see table 1) and states who may access a given file. Adding privileges to ACL based on NTK criteria [6]. The following example will explain how NTK can be used in an ACL environment.

Example

This example refers to table 1. There are three users, user A, B and C and there are three files, file A, B and C. User A is working on a project about communication networks, user B is working on a project about Web technology and user C is working on a project about security. File A contains information about communications networks, file B about security and file C concerns Web technology. User A needs to know the information in file A, therefore user A is given read and write access. User A does not need to know the information that is in file B because it is not work related. The same goes for the other users. But user B is working on Web technology what may also concern communications networks. User B already has read and write access to file C and now he also has access to read file A. ACL corresponds to a column of the access control matrix (see table 2).

Table 1 Access Control Matrix

User	File A	File B	File C
A	read, write	n/a	n/a
B	Read	n/a	read, write
C	n/a	read, write	n/a

Table 2 Access Control List

User	File A
A	read, write
B	read
C	n/a

The advantages of using ACL are:

- The administrator or the super user has a good overview of all the permissions given to the users, this makes it controllable;
- Changes can be made quite easily;
- Implementation of NTK in ACL is fairly simple in a small well defined community and should not lead to any major problems.

The disadvantages of using ACL are:

- Implementation of NTK in ACL in distributed systems can be difficult without additional countermeasures.

4.2.3 Non-Discretionary Access Control

4.2.3.1 Role-Based Access Control

In the Role-based access control model, group membership assignment is based on organizational or functional roles. This type of access control model allows access to resources based on the role a user holds within the organization. The following examples will explain how NTK can be used in a role-based access control [6].

Example

This example refers to figure 8. A new employee joining the sales department as a sales clerk will require access to IT resources (such as read and update access to selective customer and inventory records). This access will be granted by connecting the sales manager organizational profile to the user's ID, thus enabling the user to perform his or her duties on a NTK basis, such as create customer orders, check status of customer orders and check inventory levels.

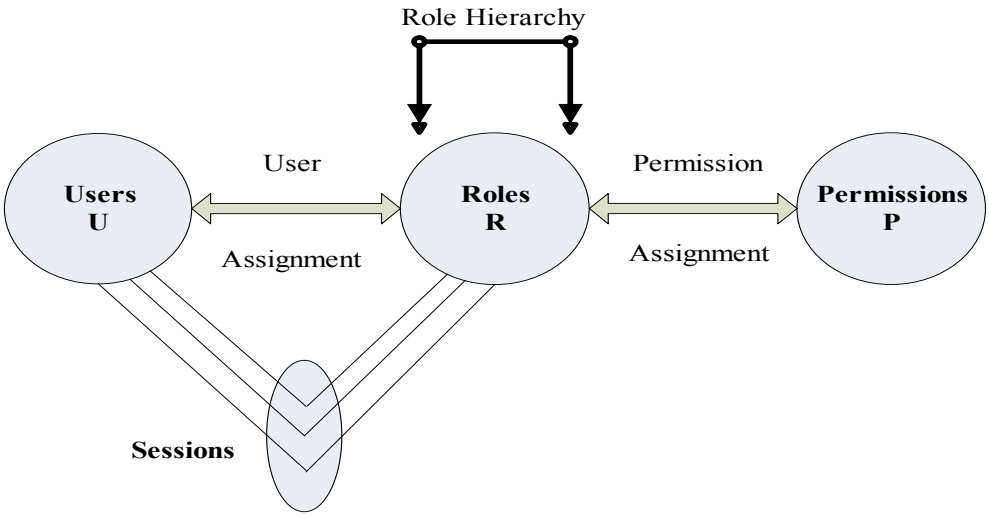


Figure 7: Role-Based Access Control Model

Figure 8 shows that users are member of roles and permissions are associated with those roles. There are many relations between user/role and role/permission. Users have the ability to change roles for each session.

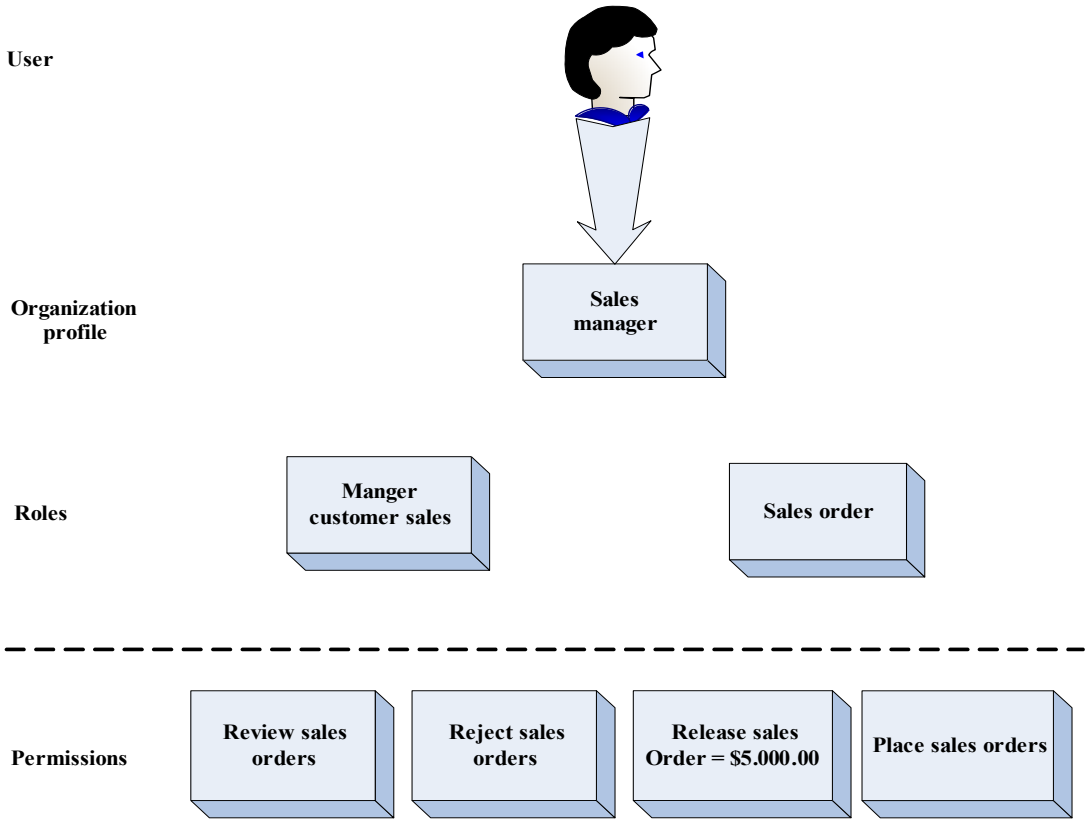


Figure 8: Role-Based Access Control Example

The advantages of using role-based access control:

- Delegation of duties further simplifies privilege management. A role can be delegated to another user without having to explicitly change the delegate's access privileges. If role hierarchy is supported, a subordinate role can be

delegated instead of the entire role. This principle is also used in role-based access control;

- Authorization management;
- Hierarchical roles;
- Least privilege;
- Separation of duties.

The disadvantage of using role-based access control:

- Implementation of RBAC can be difficult to implement on a wide scale if the organizational policy is poorly documented. Because the organizational policy or layout defines model.

Implementation of NTK within a role-based access control environment would be simple if roles are clearly defined in an organization due to the fact of the simplified administration of permissions.

4.2.3.2 Task-based Access Control

Task-based access control (TBA) is the authorizations of tasks rather than users and files. The tasks involve other subtasks. Authorization is transient and models the organizational structure [6].

TBA is particularly suited for distributed computing and information processing activities with multiple points of access, control, and decision making. TBA articulates security issues at the application and enterprise level. As such, it takes a "task-oriented" or "transaction-oriented" perspective rather than the traditional user-file view of access control. Access mediation now involves authorizations at various points during the completion of tasks in accordance with some application logic. In contrast, the user-file view typically divorces access mediation from the larger context in which a user performs an operation on a file.

Example

Figure 9 shows how a user has to be authorized for certain tasks. The user has authorization, based on the NTK criteria, to open the file, T1. The user wants to proceed to read the file based on his NTK criteria, his NTK criteria permits him to read the file, thus granting him access, T4. The user also wants to write to the file but his NTK criteria does not permit it. So the user is not authorized for that task.

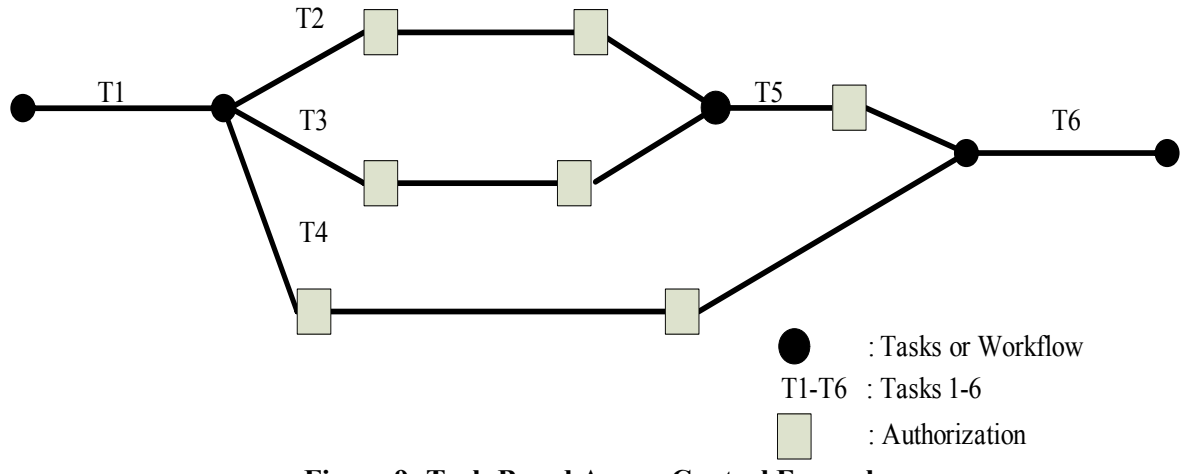


Figure 9: Task-Based Access Control Example

The advantages of using TBA are:

- TBA has broad applicability ranging from access control for fine-grained activities such as client-server interactions in a distributed system, to coarser units of distributed applications and workflows that cross departmental and organizational boundaries.
- TBA takes actively part in access control management in contrast to traditional passive user-file models that merely store primitive access control definition tuples.

The disadvantages of using TBA are:

- TBA is more suitable for distributed computing and information processing activities.

TBA can be efficient in a distributed computing and information processing network environment. The user can perform a task if he is authorized for that task, based on his NTK criteria.

4.2.3.3 Lattice-based Access Control

Lattice-based access control is a variation of nondiscretionary access control and provides an upper bound and lower bound of access capabilities for every user and file relationship. When using the lattice-based model, users have the least upper bound and the greatest lower bound of access to labeled files, based on their clearances, or assigned lattice position.

Example

A user who is mapped to a specific role wants to carry out an operation on an file, the system will look at the clearance and NTK of that role (role lookup box), look at the operation that is being requested (permissions lookup box), and compare this to the file's classification and access restrictions (classification lookup box), All of this information is combined to generate a class or a relationship between that user and that file, which dictates what the subject can or cannot do with it. The upper bound and lower bounds of access are illustrated in figure 10.

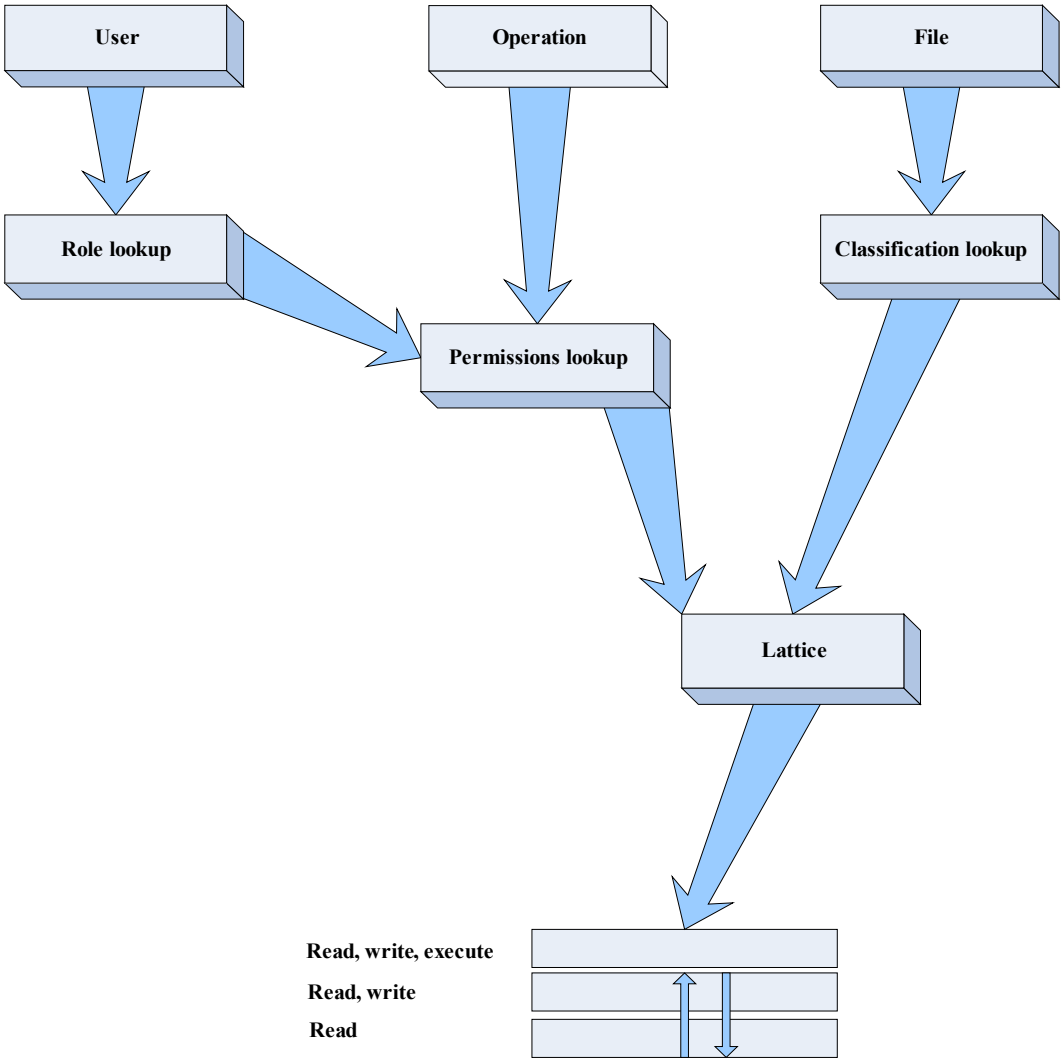


Figure 10: Lattice-Based Access Control Example

5. NEED-TO-KNOW PRODUCT SOLUTIONS

NTK product solutions that are available are described in this chapter, including what means of security they can provide for a NTK implementation and what other possible features they have of improving security.

It is not economically justified to maintain separate computer systems for processing information of different classification. Such a situation enforces solutions implementing multilevel security (MLS) systems. Apart from different classifications of information being processed, one of the issues that needs to be addressed is also NTK implementation in the MLS environment.

Several models to implement MLS exist [6]:

- Dedicated; All users have the clearance and formal NTK to all data processed within the system;
- System-High; All users have a security clearance or authorization to access the information but not necessarily a NTK for all the information processed on the system;
- Partitioned (compartmented); All users have the clearance to access all the information processed by the system, but might not have the NTK and formal access approval.

Multilevel security is a mode of operation that provides a capability for various levels and categories or compartments of data to be concurrently stored and processed in an automated system and permits selective access to such material concurrently by users who have different security clearances and NTK [5].

In a standard MLS model, all users and files have security labels. The access class (security label) of database transactions and operations can be determined as follows:

- When a user logs in, a process is started that runs with the clearance at which the user has logged in;
- When this process starts a transaction, the transaction inherits the access class of the process;
- When this transaction issues an operation, the operation inherits the access class of the transaction.

5.1 IBM ZSERIES MAINFRAME OPERATING SYSTEM Z/OS

The z/OS 1.4, introduced by IBM, first came out in 2002. It provided Web-based improvements, added PKI support (see chapter 6), network enhancements. z/OS 1.5 operating system is a successor of z/OS 1.4 for the eServer zSeries mainframe of IBM. The system provides multilevel security as its primary mechanism. Given the stringent security requirements of government agencies, this can improve the way government agencies share critical classified information also on NTK criteria.

NTK criteria can be applied within a multilevel security. This technology allows IT administrators to assign users access to information based on their NTK criteria. It is designed to prevent individuals from accessing unauthorized information and to prevent individuals from declassifying information. The operating system enables a single repository of data to be managed at the row level and accessed by individuals based on their NTK criteria.

Multilevel security is based on cryptographic separation. The zSeries Cryptographic Coprocessor Facility (CCF) and PCI Cryptographic Coprocessor (PCICC) both have tamper-proof designs and support high-speed triple DES (TDES) encryption, as well as symmetric and asymmetric encryption. The IBM PCICC has a FIPS 140-1 Level 4 certification. Both systems support SSL and digital certificates. Other features are: logical partitions, Resource Access Control Facility (RACF)

DB2 UDB for z/OS V8 provides the support for Multilevel Security. Each row of a DB2 database contains a DB2 security label. This label is checked against the security label of the requester. Only rows containing matching security labels can be accessed by the requester. The security of a row or column is maintained at a Database Administration or Security Administration level.

The Multilevel security on the operating system can take full advantage of the IBM's eServer zSeries functionality. Functionalities that provide a highly secure environment are:

- Robust cryptography;
- High availability;
- Scalability;
- Flexibility.

Other capabilities which refer to security on the operating system are:

- Intrusion detection;
- Management of digital certificates.

The difference between the z/OS 1.5 and its successor, z/OS 1.6, on a multilevel security, are the enhancements that will be included in the 1.6 version of the operating system.

These enhancements are:

- Labeled Security Protection Profile (LSPP) at Evaluation Assurance Level (EAL3+);
- Controlled Access Profile (CAPP) at EAL3+.

The advantages of using IBM zSeries mainframe operating system z/OS are:

- Provides a security-rich platform;
- Operating system integrity;
- Controlled access to resources;
- Supports SSL;
- Supports a type of labelling.

The disadvantages of using zSeries mainframe operating system z/OS are:

- No role-based access control support;
- No rule-based access control support.

The operating system z/OS 1.5 and z/OS 1.6 both provide good features in which NTK can be implemented. The operating system is especially suited for government agencies with classified information.

5.2 TRUSTED SOLARIS

The Trusted Solaris (TSOL) software package is an enhanced version of the Solaris operating environment, with special security features. Among its capabilities, TSOL ensures that all administrative actions are traceable to an authenticated individual; audits all transactions; requires all files to be labeled and all users to have defined clearance levels; and ensures that data is sent only to other users (or devices) certified to be at the same access level or at a higher one.

The software enables an organization to define and implement a security policy for a single workstation or a network of workstations. A security policy is the set of rules and practices that help protect information and other resources (such as computer hardware) in your system. Typically, rules deal with such items as who has access to which information or who is allowed to write files to tape; practices are recommended procedures for performing tasks.

TSOL controls do everything through permissions on NTK criteria. There are added file label permission (MAC) and kernel permissions that control the actions an executable can perform. TSOl is based on MAC by requiring all files to be labeled. But it also supports role-based access control and concepts of least privilege.

TSOL controls the operating system by splitting the administrative responsibilities. It uses role-based access controls to divide administrative task to a number of roles that only grant authority on NTK criteria.

TSOL supports information labeling and gives user clearance levels based on their NTK criteria. MAC is one of the models being supported. MAC allows information to be processed at multiple security levels allowing users to share files with other users of the same security level. The system provides functions to restrict the security levels of information sent to individual printers and restrict who can view print queue information through NTK criteria.

Summary of the features and benefits are:

- Configurable Security Functionality, the TSOL operating environment can easily be configured to meet a wide range of security policies, guidelines and directives without impacting functionality;
- Trusted Roles, there are no super user accounts with TSOL software; systems administrators are as accountable for their actions as users;
- Multilevel File System, The TSOL operating environment uses a multilevel file system that allows segregation of different classes of (internal and external) users, with strictly enforced control over what data they can see and what operations they can perform;
- Execution Profiles, with the TSOL operating environment, users and roles can be limited to a specific set of commands and actions that are needed for individuals to perform specific jobs. Execution profiles can be defined to assign authorizations to accounts and privileges to commands and actions. This enables users or roles to bypass security restrictions when needed to accomplish a defined set of tasks, without providing them access to everything.

Example

A user has the classification “top secret” and wishes to view a classified file with the classification “secret”. The user will be granted access to this classified file. The user’s classification level is higher than the classification level of the classified file. The user’s rights to a classified file can also be set. This can be done with the rule-based access control feature. In this situation the user’s classification level can give him/her access to all classified files. The NTK criteria of the user allows him to access all the classified files. In another situation it is possible for the user, with the same classification level, to be rejected by a classified file while writing to the classified file. This can be

done by restricting rights to the profile of the user. For example the user can only read the classified file.

The above given example shows how a user, with the classification “top secret”, can access the classified file. But the actions of the user can also be limited based on his NTK criteria.

The advantages of using TSOL are:

- Supports MAC;
- Supports rule-based access control;
- Supports both Sun SPARC and Inter x86 environments.

The disadvantages of using TSOL are:

- No cryptographic support;
- No SSL support;
- No RACF support.

TSOL uses MAC and rule-based access control to implement NTK. Both models can separate users on NTK criteria. TSOL supports both Sun SPARC and Intel x86 environments.

5.3 SGI TRUSTED IRIX SYSTEM

This operating system also uses multilevel security policy that can be used on different domains, it mainly uses labels and ACL can be attached to files, this is optional. The operating system compartmentalizes user’s interactions according to specific security labels. The user and process labels contain two main elements, sensitivity level and sensitivity category. Users can continue to execute policy abiding functions while unauthorized accesses are disallowed before data is compromised.

The operating system is fully configurable to networks security policy requirements. The security administrator is able to program the networks own security clearance definitions and limitations, permitted special operational capabilities, file access control lists, and choice of password protection scheme. It allows for auditing and monitoring of key and site-defined operational events, such as file access and modification, invocation of programs, login and logout, and unauthorized attempted accesses to files. The audit log could be used to discover malicious intent.

In addition to MLS labels, the operating system provides other discretionary file-access control mechanisms. Optionally, access control lists (ACLs) can be attached to files. ACLs specify what group(s) and what user(s) are allowed to read or write the corresponding file. This provides access control granularity to the user account or accounts.

The security policy Identification and Authentication (I&A) can be enforced. The identification and authentication mechanism controls user access to the system. The I&A facilities of the operating system allow the administrator to be certain that the people on the system are authorized users and that private password integrity is maintained to the highest possible levels.

Other features the operating system supports are:

- System audit trail: The audit subsystem allows the system administrator to keep a precise log of all system activity. The system audit trail provides the means for the system administrator to oversee each important event occurring on the system. The audit trail is useful for tracking changes in sensitive files and programs and for identifying inappropriate use of system;
- Capability based privilege mechanism: The mechanism determines the privilege based on the set of effective capabilities for a given process. Also, it is how capabilities are assigned to a process or an executable file, and how a process

manages its capabilities. This mechanism is utilized to grant very specific, controlled privileges to specific functions without granting access to key user accounts;

- Object reuse policy (object scrubbing): To preclude accidental disclosure of data, display memory and long-term data storage are subject to an object reuse policy and implementation. For example, all system memory is always automatically cleared before it is allocated to another program. Surrendered disk space is also cleared before it is reallocated.

SGI Trusted IRIX System offers mainly the feature labels to separate users from accessing certain files. Apart from the label feature it also provides the feature ACL. The next example will explain how NTK can be implemented.

Example

There is a classified file with the sensitivity level top secret and has the following sensitivity categories, geography, demography and astronomy. A user has to have the sensitivity level top secret and the sensitivity category, geography, demography and astronomy to gain access to the classified file. The user is cleared to access this file, the user fulfils the NTK criteria of the classified file.

The advantages of using SGI Trusted IRIX system are:

- Supports a type of labelling;
- Supports ACL.

The disadvantages of using SGI Trusted IRIX system are:

- No rule-based access control support;
- No role-based access control support;
- No cryptographic support;
- No SSL support;
- No RACF support.

A combination of ACL and MLS labels is used in this product. It is advised that such a system should only be used in a small organization or in a small network environment. Furthermore it is a system in which NTK can function. By using MLS labels and ACL users can be given access to classified files based on there NTK criteria.

5.4 IX

IX is an experimental multilevel secure variant of the UNIX operating system. IX supports document classification with mandatory access control. Furthermore it can also be used on different security domains for example, unclassified domains and restricted domains.

IX preserves data classification. Every file and every process has a label, which tells its classification. Users are allowed to see only information they are cleared for. Data transfers may only happen in a direction of increasing labels. Labels of processes or files may adjust automatically during computation to guarantee that outputs are classified at least as high as the inputs from which they derive.

Activities, such as declassification, that deviate from the usual labeling rules can be accomplished only with the exercise of privilege. A trusted user may be endowed with one or more privileges, which may be exercised only through trusted programs that have been certified for those

privileges. In normal usage each use of privilege is vetted by a privilege server, which confirms the client's authority and hands out exactly the privileges needed for the operation at hand.

IX safeguards outside communication. External media such as tape cartridges or communication ports can be opened and labeled only by trusted code. That code has the duty to authenticate the clearance of the destination. After trusted code has set the label, an external medium can be used like any other file. In particular network connections, once established, are as easy to use as in ordinary UNIX systems. In the following section an example will be given how NTK can function within IX.

Example

If a file has a classification level secret, then a user with the same classification level, secret, or higher, top secret, will get access to the classified file. The user fulfills the NTK criteria of the classified file

Advantages of using IX are:

- Supports MAC.

Disadvantages of using IX are:

- No cryptographic support;
- No SSL support;
- No RACF support.

IX only uses MAC to enforce security policies. While other products have a variety of methods they support. But depending on how an organization wants to protect his/her information the use of only one type of method, MAC, can be sufficient. However IX only makes use of classification levels and no categories.

6. PKI-BASED MECHANISMS FOR NTK

Ways of securing a computer infrastructure of an organization from external threats has come a long way. The problem with the online media issues of authentication, confidentiality, integrity, and non-repudiation of online communication remain unsolved. Public Key Infrastructure (PKI) has been designed to solve this dilemma.

PKI is based on cryptographic techniques. Therefore some light will be shed on encryption technologies and how NTK can be implemented.

6.1 ENCRYPTION TECHNOLOGIES

There are two basic types of cryptographic techniques: symmetric key encryption (also known as secret key or shared secret) and asymmetric key encryption (also known as public key). A key is a binary number, typically 40 to 256 bits in length for shared-key systems, or 2048 bits or more for public key systems. In symmetric key encryption, the same key is used for both encryption and decryption (figure 11). Asymmetric key encryption uses a public and private key pair. In the typical encryption mode the recipient's public key (known to everybody) is used to encrypt the data and the recipient's private key (known exclusively to the recipient) is used to decrypt the data (figure 12). A user would need to worry only about the security of his own private key, as knowledge of the public key does not affect (weaken) the encryption [6].

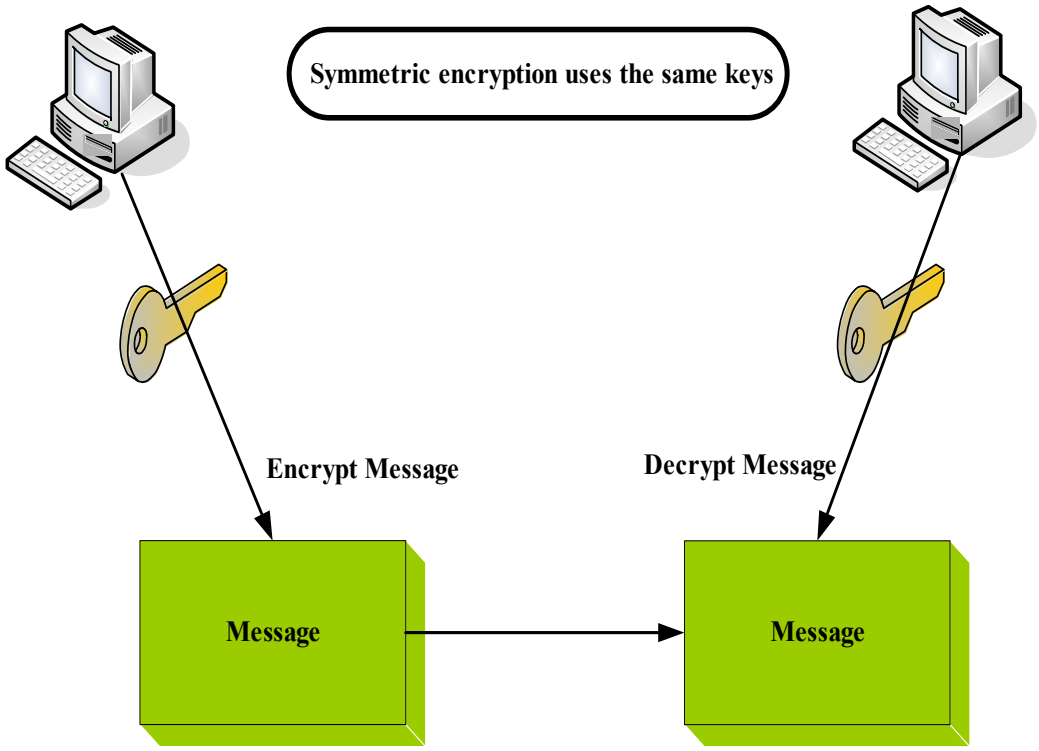


Figure 11: Symmetric Key Encryption

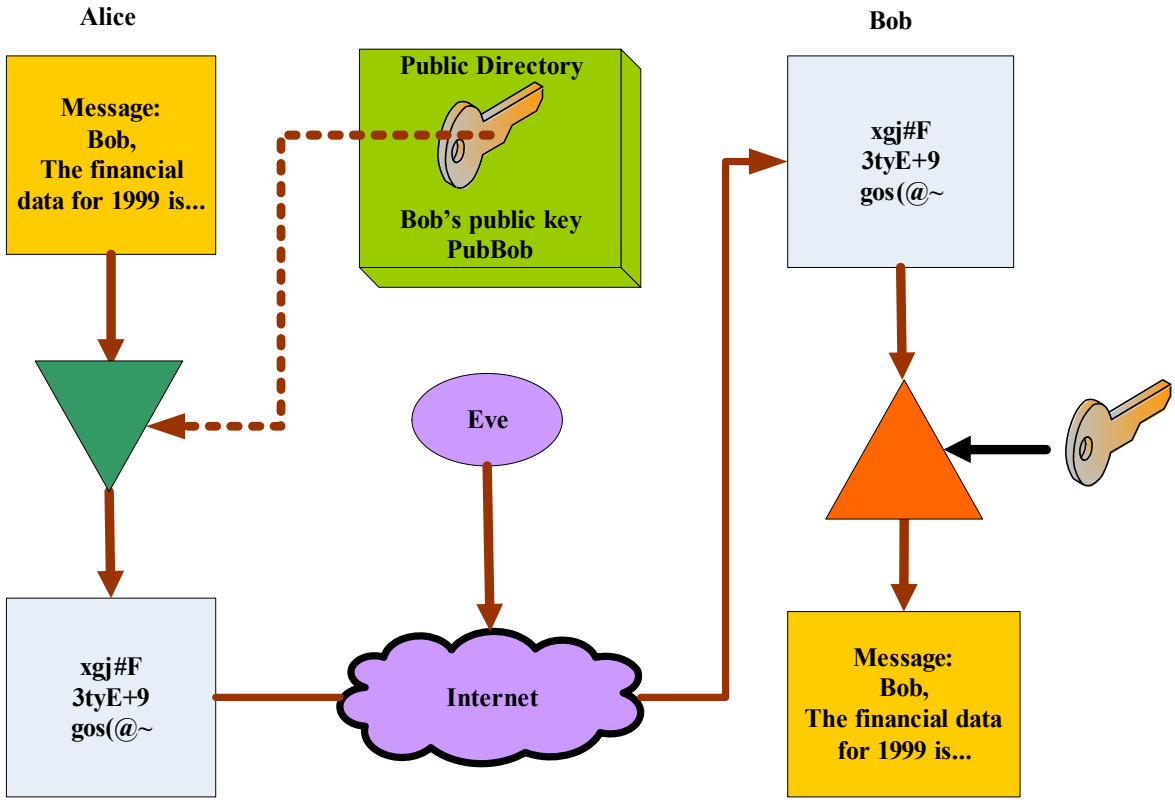


Figure 12: Assymmetric Key Encryption Used IN PKI

The major advantage of asymmetric key encryption is that apart from confidentiality it also provides non-repudiation and authentication services. A major disadvantage of asymmetric systems is that they have slower performance. Symmetric key cryptosystems are efficient, but key management is an issue.

6.2 PKI

PKI provides a structured, secure mechanism for the distribution of digital certificates and most importantly protection of the corresponding private keys. To perform the task PKI uses asymmetric key encryption. The encryption and decryption transformation are sufficiently different and the corresponding algorithms implement a model where the encryption key can be made public and it still would be computationally infeasible to derive a private decryption key from the public key. Access to the public (encryption) key does not allow decryption of a message.

Example

If Alice wants to send a secret message to Bob, that only Bob needs to know, she looks up Bob's public key (PubBob), uses it to encrypt the message and sends the encrypted message to Bob. Bob then uses his private key (PrivBob) to decrypt the message and read it. Eve, listening in, cannot decrypt the message, even though she also knows Bob's public key. Anyone can send an encrypted message to Bob, but only Bob can read it, because only Bob knows his private key. Alice can send a secret message to Bob with no prior arrangement between the two. Only public keys are transmitted; no private key is ever transmitted or shared (figure 12).

In the example above only Bob has the private key to decrypt his message that was send to him by Alice, using his public key. The NTK criterion was that only Bob is allowed to read the message and no one else.

In the example it is said that Alice looked up Bob's public key, but it does not describe how she got the public key. Exchanging it personally is rarely an option, sending it through the internet gives no assurance about the recipient and searching for it in a public-key database neither. The solution for this problem is offered through certification. A certification is being given through a certification authority (CA) and binds the name of a person or an entity to a public key, in a way it is a form of a document. For example, the owner(1) of the public key is Bob.

To control a certificate one must know the public key of the CA. If there was only one CA in whole world, this would not be a problem. But to give out millions of certificates one CA is a bottleneck. This dilemma can be solved because, PKI is a hierarchical order of different CA's, see figure 12. At the top of the hierarchy is the Root-CA. The Root-CA gives the certificates, with name en public key, to the direct underlying CA's, they in turn do the same for the underlying CA's. The CA's on the lowest level give the certificates out whose identities are bind to public keys.

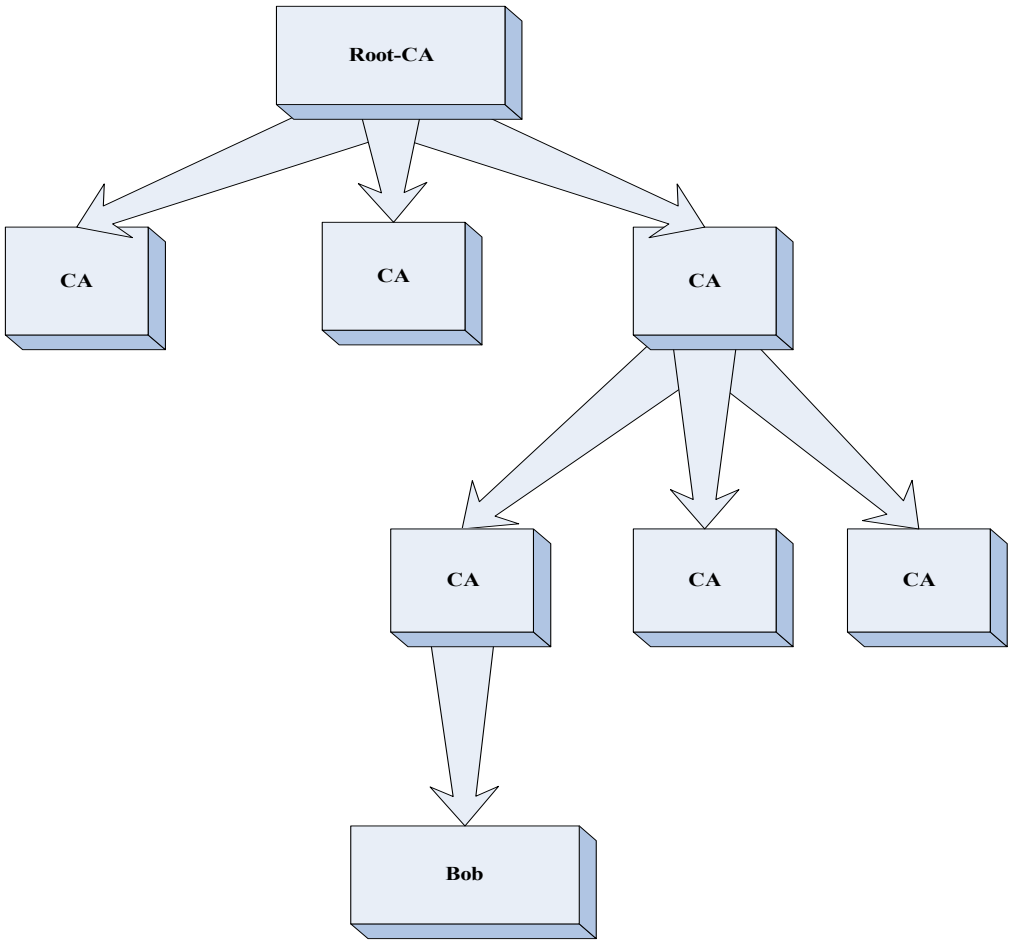


Figure 13: PKI-hierarchy

Theoretically PKI solves major problems within information security. But this does not always apply in practice, the biggest problem with PKI is implementation.

The certificates can be granted on the basis of NTK principles. Hence, PKI provides a mechanism for cryptographic separation that can be based on NTK.

7. NTK MECHANISMS FOR WEB-BASED INFORMATION

This chapter describes mechanisms that can be used for web-based information in which NTK principle can be implemented.

7.1 VIRTUAL PRIVATE NETWORK

A Virtual private network (VPN) allows two or more private networks to be connected over a publicly accessed network. In a sense, VPNs are similar to wide area networks (WAN) or a securely encrypted tunnel, but the key feature of VPNs is that they are able to use public networks like the Internet rather than rely on expensive, private leased lines. At they same time, VPNs have the same security and encryption features as a private network.

A VPN is an effective means of exchanging critical information for users working remotely for example, branch offices, at home, or on the road. It can securely deliver information between users, who may have a huge physical distance between them. Since organizations no longer have to invest in the actual infrastructure themselves, they can reduce their operational costs by outsourcing network services to service providers.

VPNs today are set up a variety of ways, and can be built over ATM, frame relay, and X.25 technologies. However, the most popular current method is to deploy IP-based VPNs, which offer more flexibility and ease of connectivity. Since most organizational intranets use IP or Web technologies, IP-VPNs can more transparently extend these capabilities over a wide network. An IP-VPN link can be set up anywhere in the world between two endpoints, and the IP network automatically handles the traffic routing.

Privacy and protection of data is of utmost importance when deploying services over the Internet, where it can be vulnerable to attacks or illegal entry. Secure IP-VPNs are networks that are secured by encryption and authentication, and layered on an existing IP network. In response to security issues, the Internet Engineering Task Force (IETF) has developed the IP Security (IPSec) protocol suite, a set of IP extensions that offer strong data authentication and privacy guarantees.

VPN products fall into three broad categories: hardware-based systems, firewall-based systems, and standalone application packages. Most hardware-based VPNs are encrypting routers, which are considered secure and simple to use, as they are the nearest thing to "plug-and-play" equipment available. However, they may not be as flexible as software-based systems, which are ideal in situations where both endpoints of a VPN are not controlled by the same organization, which is typical for business partnerships or when client support is required. Firewall-based VPNs are considered among the most secure, as they take advantage of the firewall's existing security mechanisms. However, if the firewall is already loaded, performance issues may pop up.

Example

Remote users can use VPNs to connect to their organizational network to access their e-mail, network resources and personal files. A remote user must have the necessary software loaded on his computer to use a VPN. The user first makes a PPP (Point to Point Protocol) connection to an ISP, and the ISP makes a full connection for the user to the destination network. PPP encapsulation datagram’s to be properly transmitted over an IP network. Once this connection has been made, the user’s software initiates a VPN connection with the destination network. Because data exchanged between the two entities will be encrypted, the two entities go through a handshaking phase to agree upon the type of encryption that will be used and the key that will be employed to encrypt their data. The ISP is involved with the creation of the PPP connection, which is a type of foundation for the VPN connection. Once the PPP connection is set up, the ISP is out of the picture and the VPN parameters are negotiated and decided upon by the user and the decided upon by the user and the

destination network. After this is complete, the user and network can then communicate securely through their newly created virtual connection. When a user is successfully logged in, access to data in the network is granted, because the user is logged in locally.

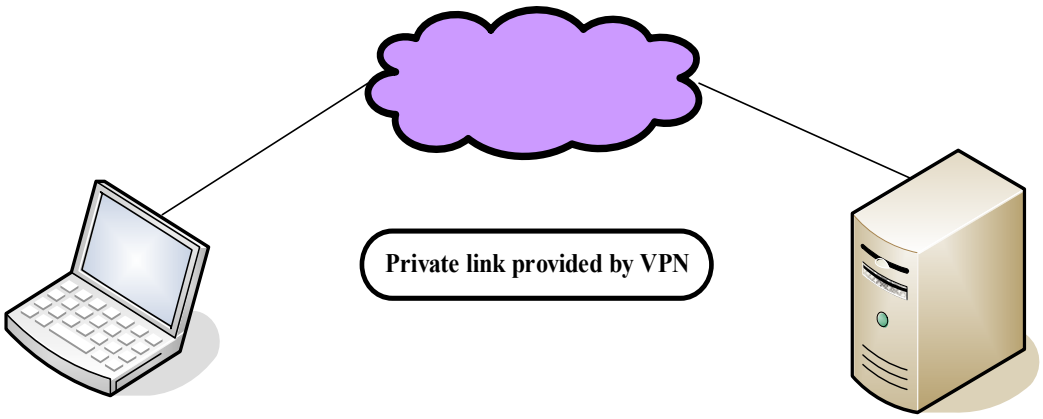


Figure 14: VPN example

Advantages of VPN are:

- VPN can takes place over dial up connections;
- VPN can take place between firewalls.

Disadvantages of VPN are:

- Degradation in performance can occur if packets have to be encrypted en decrypted through the network.

7.2 SECURE SOCKET LAYER/ TRANSPORT LAYER SECURITY

Secure Socket Layer (SSL) is a protocol developed by Netscape for transmitting private documents through the Internet and it is a two-layered protocol that contains the SSL Record Protocol and the SSL Handshake Protocol. It operates in the transport layer of the Open System Interconnect (OSI) model. SSL works by using a private key to encrypt data that's transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with “https:\\” instead of “http:\\” Also Web browsing with SSL uses port 443 instead of the standard port 80 for HTTP [6]. Transport Layer Security (TLS) is based on SSL [12].

The SSL protocol allows the client and server to authenticate each other as well as negotiate an encryption algorithm plus session keys a Message Authentication Code (MAC) algorithm. The browser first sends a client-hello message, the most important contents of which are the SSL version number and a list of supported algorithm suited in preferred order. The server selects the strongest algorithm that it can support and returns this in a server-hello message followed by its certificate, containing its public key. The client then optionally sends its certificate, if the server requires user authentication, followed by one-time session key encrypted under the server’s public key. The server can now decrypt the session key and the secure communication can now commence. Verification of the certificates provides the authentication. Random numbers and a MAC applied to all messages guarantee integrity and prevent replay attacks. The actual process depends to a great extent on the type of encryption, key exchange and key agreement algorithms used.

Example

When a client accesses a Web site, it is possible for that Web site to have secured and public portions based on NTK of the user. The secured portion would require the user to be authenticated in some fashion and have a NTK to access the secured portion. When the client goes from a public page on the Web site to a secured page, the Web server will start the necessary task to invoke SSL and protect this type of communication. The server sends a message back to the client indicating that a secure session needs to be established and the client sends its security parameters. The server compares those security parameters to its own until it finds a match, this is the handshaking phase. The server authenticates itself to the client by sending it a digital certificate and if the client decides to trust the server, the process continues. The client generates a session key and encrypts it with the server's public key. This encrypted key is sent to the Web server and they both use this symmetric key to encrypt the data they send back and forth. This is how the secure channel is established. SSL can enforce authentication.

Advantage of SSL/TLS:

- SSL/TLS can be used with, e.g. HTTP, LDAP, IMAP.

Disadvantage of SSL/TLS:

- The symmetric key uses the same key to encrypt and decrypt, this can lead to security issues in a NTK environment.

7.3 SECURE-HTTP

Another protocol for transmitting data securely over the World Wide Web is Secure HTTP (S-HTTP). Whereas SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely. S-HTTP is a protocol that operates on the application level of the OSI model, it is designed to transmit individual messages securely. SSL and S-HTTP, therefore, can be seen as complementary rather than competing technologies [6].

Example

The client and server both have a list of cryptographic preferences and keying material. When a client makes a request to a server and the server deems, based on NTK, that this type of communication should be protected, the server will query the client about the type of encryption methods it is configured to use. Once the client and server agree upon a specific encryption method, the client sends the server its public key. The server generates a session key, encrypts the session key with the client's public key and sends it back. From here on out, the client and server encrypt their messages with the newly calculated session key.

Advantages of S-HTTP are:

- Data integrity and sender authentication capabilities;
- Stateless protocol;
- Multiple encryption modes and types;
- Can use PKI technology.

Disadvantages of S-HTTP are:

- Using the symmetric key in a NTK environment is less secure.

7.4 SINGLE SIGN-ON

Web-based single sign-on (SSO) applications goal is to sign in once and to gain authenticated access to multiple, independent Web-based services. Web-based SSO is often associated with access control because many Web-based access control products provide SSO. “Oracle9iAS Single Sign On: SSO for Web applications” and “Sun One Identity Server” are such products. The “Oracle9iAS Single Sign On”, uses a native authentication mechanism, users can log in once to get access to multiple applications. While the “Sun One Identity Server”, forces the users to log into the Identity Server first to get access to other SSO configured servers. Users with a NTK will be given a login and a password for the Identity Server before continuing to other SSO configured servers.

SSO is often used to enable secure and seamless authentication to multiple applications and content inside portal environment. SSO solutions support integration with portal products, which provides a more secure environment to control access to multiple organizational systems and software applications. But because the level of integration differs from product to product, so does the level of security. Most portal vendors can integrate with Lightweight Directory Access Protocol (LDAP) directories as well as policy-management products.

An SSO system can also enable centralized policy management. This capability is important, especially when an SSO product supports both Web and non-Web-based SSO: The integration in the SSO implementation may help organizations avoid compromising the security of back-end applications or services accessible through the portal. A portal system equipped with this type of centralized policy management can offer its participants an acceptable level of security and the confidence that their data and applications are protected from unauthorized access and that this protection is implemented according to the organizations policies, guidelines, directives of the portal members.

Example

A user gets his/her credentials on NTK criteria based on the policies, guidelines, directives of the organization. The user enters its credential one time and is able to access all resources that are work related.

Advantages of using SSO are:

- Reduces the amount of time the user spends authenticating to resources;
- It gives the administrator the ability to streamline user accounts and have better control over access rights;
- It improves security by reducing the probability of disclosing users passwords;
- It reduces the administrator’s time spent on adding and removing user accounts and modifying access permissions. In the event that an administrator needs to disable or suspend a specific account, it can be done uniformly instead of having to alter configurations on each and every platform.

Disadvantages of using SSO are:

- For SSO to work, every platform, application and resources needs to accept the same type of credentials, in the same format and interpret their meanings the same;
- There is also a security issue to consider in a SSO environment. Once access is granted to an individual, with malicious intent, he/she is in. That person, attacker, has access to everything that the original user’s profile had.

8. CONCLUSIONS / RECOMMENDATIONS

This chapter will describe the conclusions and the recommendations. It will be partially based on selection criteria tables.

Table 4: Selection Criteria Methods

Products / Demands	DAC	MAC	Non-Discretionary AC		
	ACL	Rule-based AC	Role-based AC	Task-based AC	Lattice-based AC
NTK Separation	+	+++	++	++	++
Simple to use	++	++	+++	+	+
Administrator friendly	+	+++	+++	+	+
Security	++	+++	++	+++	+++

Explanation of symbols:

+++	= very good
++	= good
+	= fair
-	= bad
--	= very bad
*	= not available

Access control models provide a secure way in which NTK can be implemented. This report has discussed several basic types of access control models. DAC, is a model that is being applied in the Windows operating system; it belongs to one of the most popular access control models.

DAC can work very well in a small organization where overview on the users can be maintained. The owner of the classified files can track who has access to the classified files and who has not. In big organizations it is difficult to keep track of the users who have access to classified files. There are two types of access controls that are based on DAC, a user-directed access control and an identity-based access control/or hybrid access control. When a user within certain limitations has the right to alter the access control to certain files, this is termed as user-directed. An identity-based AC and/or hybrid AC is a type of DAC based on an individual's identity. In some instances, a hybrid approach is used, which combines the features of user-based and identity-based DAC.

In the group of non-discretionary access control models there are three approaches that should be mentioned, i.e. role-based access control, task-based access control and lattice-based access control.

Role-based access control separates users on the role level. This makes it easy to maintain the user's profile for system administrators, e.g. in situations when users are moved within an organization. That makes role-based access control an administrator friendly model. But there are certain security issues that have to be considered. A role for a certain department gives all the users the

same rights. An individual profile might have to be created if the role does not fully reflect the scope of the user's duties.

Task-based access control is a system of task authorization rather than users and files and can be useful in information processing activities.

Lattice-based access control provides an upper bound and lower bound of access capabilities for relationships among users and files. When using the lattice-based model, users have the least upper bound and the greatest lower bound of access to labeled files, based on their clearances, or assigned lattice position.

Although lattice-based access control can provide a good security it still is a complex access control to use and to maintain. Role-based access control can provide good NTK separation but an organization requires a structure that clearly and fully reflects the functional model of the organization. Task-based access control can also provide good NTK separation but it is mostly intended for activities like information processing. Lattice-based access control is one of the securest ways to protect information if complexity of the access control is not an issue.

In the MAC model the authorization of an access of a user to a file depends on labels, which indicate the user's clearance, and the classification or sensitivity of the file. Rule-based access control is an access control model based on MAC. It is determined by rules such as the correspondence of clearance labels to classification labels, rather than the identity of the users and files alone.

The choice which access control model to use and how to implement it should respect specific requirements of the organization where it is going to be applied. The solution should also cover application of NTK principle. As it follows from table 4, the decision about access control models is not neutral for providing the NTK separation.

One of the methods that provide a good NTK separation, in a specific access control model, is PKI. The infrastructure is designed to generate certificates that grant access to network resources (e.g. data). The certificates can be granted on the basis of NTK principles. Hence, PKI provides a mechanism for cryptographic separation that can be based on NTK.

In this report there are several Web-based mechanisms discussed as well. SSO is one of the most promising Web-based application. Once a user signs in he/she is granted access to classified files on NTK criteria. The user does not have to log in every time. But this is also a security threat, if an attacker logs in once he is in and has access to all the classified files.

The products reviewed in chapter 5 of the report all provide good security features. IBM uses MLS, and TSOL is based on MAC and provides a very robust least privilege role-based access control mechanism. The SGI IRIX system is based mainly on labeling and ACL. IX supports only MAC. Among all the solutions, from the supported security mechanisms point of view, TSOL and the IBM z/OS 1.5 (and the upcoming z/OS 1.6) seem to be the most effective operating systems where NTK principle can be successfully implemented.

ABBREVIATIONS

CAPP	Labeled Security Protection Profile
CCF	Cryptographic Coprocessor Facility
CIS	Communication Information Systems
COTS	Commercial-Of-The-Shelf
DAC	Discretionary Access Control
DES	Data Encryption Standard
EAL3+	Evaluation assurance level
FIPS	Federal Information Processing Standards Publications
IETF	Internet Engineering Task Force
INFOSEC	Information security
IPsec	IP security
ISP	Internet Service Provider
MAC	Mandatory Access Control
MLS	Multi level security
NS	NATO Secret
NSA	National Security Agency
NTK	Need-To-Know
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LSPP	Labeled Security Protection Profile
MVS	Multiple Virtual Storage
OSI	Open System Interconnect
PCICC	PCI Cryptographic Coprocessor
PPP	Point to Point Protocol
RACF	Resource Access Control Facility
S-HTTP	Secure HTTP
SECAN	NATO Military Committee Communications and Information Systems Security and Evaluation Agency
SSL	Secure Socket Layer
SSO	Single Sign-ON
Sysplex	An IBM term for communicating multiple virtual storage systems
TDES	Triple DES
TSOL	Trusted Solaris

ABBREVIATIONS *(continued)*

Tunnelling	This is a term used when data of a particular classification is passed across a bearer or network which is not accredited to the same level
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

REFERENCES

[1] [Weber 1999]:
Weber, R., “Information Systems Control and Audit”, 1999; Prentice Hall

[2] [Maiwald 2001]:

Maiwald, E., “Netwerk Beveiliging”, 2001; Academic Service

[3] [Lindgreen, Overbeek, Spruit]:

Lindgreen, E. R., Overbeek, P., Spruit, M., “Infortmatiebeveiliging onder controle”, 2000; Pearson education

[4] [Sandhu]

Sandhu, R.S., “Lattice-Based Access Control Models”, 2000; George Mason University

[5] [Longley, Shain, Caelli]

Longley, D., Shain, M., Caeli, W., “Information Security, Dictionary of Concepts, Standards and Terms”, 1992; Stockton Press

[6] [Harris]

Harris, S., “All in One CISSP Certification Secound Edition Exam Guide”, 2003; McGraw-Hilll

[7] [Krutz, Vines]

Krutz, R.L., Vines, R.D., “The CISSP Prep Guide, Gold Edition”, 2003; Wiley

[8] [Parker]

Parker, B., “PriceWaterhouseCoopers information security a strategic guide for business”, 2003; PWC

[9] http://www.docs.sun.com

[10] http://www.ibm.com

[11] ftp://ds.internec.net/internet-drafts/draft-ietf-tls-protocol-05.txt

[12] [Richardson]

Richardson, M., “Data Separation for NATO Networks”, 2003; NATO


SCIENTIA PRO VIGILIA