

Plan van Aanpak
7^{de} semester project: Intrusion Detection Systems

J.E. Barhorst W. Coene J.C.J. van Dam
M.P. Rijkeboer

9 oktober 2003

Inhoudsopgave

1	Achtergronden	3
1.1	Uitgangssituatie	3
1.2	Aanleiding	3
1.3	Relevantie	3
1.4	Relaties	4
1.5	Definities	4
2	Doelstelling en probleemstelling	5
2.1	Doelstelling	5
2.2	Probleemstelling	5
3	Projectopdracht	6
3.1	Budget	6
3.2	Planning	6
4	Projectgrenzen en randvoorwaarden	7
4.1	Projectgrenzen	7
4.2	Randvoorwaarden	7
4.2.1	Projectruimte	7
4.2.2	Internet	8
4.2.3	Beschikbaarheid	8
5	Op te leveren producten	9
5.1	Plan van Aanpak	9
5.2	Demonstratieopstelling	9
5.3	Toepassingsvoorstel	9
5.4	Projectverslag	9
6	Uit te voeren activiteiten	11
6.1	Inrichting projectruimte	11
6.2	Opstellen Plan van Aanpak	11
6.3	Inwerken in gebruikte software	12
6.4	Bouwen demonstratieopstelling	12

6.5	Opstellen Toepassingsvoorstel	12
6.6	Opstellen Projectverslag	12
7	Risicoanalyse	13
8	Methoden, technieken en standaarden	14
8.1	Extreme Programming	14
8.2	L ^A T _E X	14
8.3	Versiebeheer	14
8.4	OpenBSD	15
8.5	Backupstrategie	15
9	Kwaliteitsbewaking	16
10	Projectorganisatie	17
10.1	Aanwezigheid	17
10.2	Communicatie	18
10.2.1	Intern	18
10.2.2	Intern naar extern	18
10.2.3	Extern naar intern	18
11	Projectarchief	19
A	Versies	20

Hoofdstuk 1

Achtergronden

1.1 Uitgangssituatie

Veel bedrijven en instellingen hebben tegenwoordig een open internet verbinding om hun medewerkers en/of servers toegang op en vanaf het internet te geven. Echter, wanneer een dergelijke verbinding niet goed beveiligd is kan dat erg gevaarlijk zijn, aangezien er mogelijk ingebroken kan worden op de systemen van de organisatie en er vitale gegevens op straat kunnen komen te liggen. Een goede oplossing hiervoor is het gebruik van een firewall welke veel ongewenst verkeer buiten het netwerk kan houden. Hiermee zijn al een hoop pogingen tot inbraak op het netwerk af te slaan, maar lang niet alles. Voor dit soort zaken zou een Intrusion Detection Systeem in gebruik genomen kunnen worden. Helaas zijn er nog maar weinig organisaties die gebruik maken van een dergelijk systeem.

1.2 Aanleiding

De aanleiding voor dit project is tweeledig. Ten eerste onze gemeenschappelijke interesse voor netwerken en aan beveiliging gerelateerde zaken. Ten tweede onze onvrede over de slechte beveiliging van een groot aantal netwerken.

1.3 Relevantie

Voor eenieder die een netwerk beheerd waarover hij voor een gedeelte of voor het geheel geen controle bezit, maar wel een afdoende beveiliging wil bieden voor het deel waar hij wel controle over heeft. Een voorbeeld hiervan zijn onderzoeksnetwerken.

1.4 Relaties

Er zijn voor zover bekend geen relaties met andere projecten.

1.5 Definities

Beveiliging Het afschermen of monitoren van een geheel met als doel het buitenhouden van ongeautoriseerde personen of organisaties. Beveiliging valt uiteen in twee vormen, zijnde proactieve en reactieve beveiliging.

Proactieve beveiliging Het voorkomen van ongeautoriseerde toegang, zoals bijvoorbeeld de gecontroleerde uitgifte van een sleutel tot een ruimte, of het dichtzetten van bepaalde netwerkpoorten.

Reactieve beveiliging Het detecteren en signaleren van ongeautoriseerde toegang, bijvoorbeeld met behulp van een gesloten camerasysteem of het af luisteren en analyseren van netwerkverkeer.

Systeembeveiliging Het fysiek of elektronisch beveiligen van een enkel computersysteem, waarbij weinig tot geen rekening wordt gehouden met de eventuele netwerkverbindingen van dat computersysteem.

Netwerkbeveiliging Het fysiek of elektronisch beveiligen van een netwerk, waarbij weinig tot geen rekening wordt gehouden met de individuele computersystemen.

Meerlaags beveiligingssysteem Een systeem waarbij beveiliging van zowel individuele hosts als netwerken aan bod komen.

Intrusion Detection System Een reactief beveiligingssysteem voor losse systemen of een netwerk als geheel.

Hoofdstuk 2

Doelstelling en probleemstelling

2.1 Doelstelling

Het opbouwen van kennis en het onderzoeken van mogelijkheden op het gebied van Intrusion Detection Systems. Daarnaast het opzetten van een omgeving om eventueel demonstraties te kunnen geven op het gebied van Intrusion Detection Systems.

2.2 Probleemstelling

Hoe en in hoeverre kan een Intrusion Detection System positief bijdragen aan de beveiliging van een netwerk omgeving?

Hoofdstuk 3

Projectopdracht

Onderzoek en test de mogelijkheden van Intrusion Detection Systems op individuele systemen en binnen een netwerk infrastructuur.

Verder dient onderzocht te worden hoe de bevindingen van het voorgaande in een meerlaags beveiligingssysteem kunnen worden ingepast.

Maak aan de hand van de eerder uitgezochte oplossingen een toepassingsvoorstel voor een klein tot middelgroot onderzoeksnetwerk (50 tot 200 gebruikers).

3.1 Budget

De totale kosten van het project mogen het door de school vastgestelde projectbudget niet overschrijden, tenzij er uitdrukkelijk toestemming is gegeven door de projectbegeleiding.

3.2 Planning

Alle in de projectopdracht gedefinieerde producten dienen te worden opgeleverd vóór het einde van de vastgestelde projectperiode, zijnde januari 2004.

Ook mag de aan het project besteedde tijd niet het maximale aantal vastgestelde studiebelastingsuren overschrijden, te weten $13 \cdot 40 = 520$ uur per projectteamlid, dus totaal 2080 uur.

Hoofdstuk 4

Projectgrenzen en randvoorwaarden

4.1 Projectgrenzen

Om niet te verzanden in allerlei verschillende mogelijke uitwerkingen van de projectopdracht zullen wij hierbij de grenzen van het project definiëren.

Wat valt binnen de projectgrenzen:

- Het onderzoeken en uitwerken van algemene oplossingen voor het detecteren van inbraak pogingen en/of misbruik van hosts en netwerken;
- het opzetten van een netwerk waarin bovengenoemde oplossingen kunnen worden getest.

Wat valt er buiten:

- Het aanpassen of beveiligen van individuele softwarepakketten;
- het geven van adviezen over de beveiliging van het schoolnetwerk;
- het opstellen van inleidingen en installatiehandleidingen voor besturings-systemen.

4.2 Randvoorwaarden

4.2.1 Projectruimte

Om de onderlinge mondelinge communicatie van de projectleden te bevorderen heeft het projectteam de beschikking over een eigen projectruimte nodig, daarnaast zijn er interne afspraken nodig over aanwezigheid en gedrag van eenieder.

4.2.2 Internet

Gezien de onmisbaarheid van deze wereldwijde informatiebron tegenwoordig hebben de projectleden toegang tot het Internet nodig. Verder dient deze verbinding geschikt te zijn om in een UNIX omgeving gebruikt te kunnen worden.

4.2.3 Beschikbaarheid

De projectleden dienen in staat gesteld te worden aan het project te werken voor het totaal vastgestelde aantal uren en dienen niet anderszins van het project af gehouden te worden door nevenactiviteiten.

Hoofdstuk 5

Op te leveren producten

5.1 Plan van Aanpak

Er dient een Plan van Aanpak voor het project geschreven te worden, aan de hand van de richtlijnen van de Hogeschool van Utrecht. Dit Plan van Aanpak dient gepresenteerd te worden.

5.2 Demonstratieopstelling

Er dient een demonstratieopstelling gebouwd te worden, waarmee verschillende aspecten van Intrusion Detection Systems kunnen worden gedemonstreerd.

In deze demonstratieopstelling zal beveiliging door middel van een Intrusion Detection System voor zowel individuele systemen als netwerken gedemonstreerd worden.

5.3 Toepassingsvoorstel

Aan de hand van bevinding van het project dient een toepassingsvoorstel voor de implementatie van een Intrusion Detection System voor een klein tot middelgroot onderzoeksnetwerk gemaakt te worden.

5.4 Projectverslag

Aan de hand van de bevindingen van het project dient een Projectverslag geschreven te worden. Dit Projectverslag zal onder andere de volgende onderdelen bevatten:

- Een verslag van de uitgevoerde tests;
- een verslag van de opzet van het meerlaags beveiligingssysteem;
- een verslag van de opzet van de demonstratieopstelling;
- een overzicht van de opgedane kennis over Intrusion Detection Systems.

Dit verslag dient gepresenteerd te worden.

Hoofdstuk 6

Uit te voeren activiteiten

In dit hoofdstuk zal uiteengezet worden welke activiteiten er uitgevoerd moeten worden tijdens het project. Totaal is er volgens de projectopdracht 2080 uur voor beschikbaar. Indien niet anders vermeld heeft het gehele team verantwoording voor het uitvoeren van de activiteiten.

6.1 Inrichting projectruimte

Resultaten:

- Een werkbare inrichting van de projectruimte conform de wensen van de projectleden en de ARBO¹-wetgeving;
- een computerinfrastructuur waarbinnen het project goed uitgevoerd kan worden;
- onbeperkte toegang tot het Internet aangezien deze wereldwijde informatiebron onmisbaar is voor de correcte uitvoering van het project.

Benodigde tijd: \pm 300 uur.

6.2 Opstellen Plan van Aanpak

Resultaten:

- Plan van Aanpak waarin algemene zaken worden omschreven, zoals de op te leveren producten, randvoorwaarden, succesfactoren, kostenschatting en een globale planning;

¹Arbeids Omstandigheden Wet, ook van toepassing op studenten.

- presentatie van het Plan van Aanpak, waar in de begeleiding er van moet worden overtuigt dat het project voortgezet kan worden.

Benodigde tijd: ± 200 uur.

6.3 Inwerken in gebruikte software

Resultaten:

- Kennis van het opzetten en configureren van de gebruikte software.

Benodigde tijd: ± 200 uur.

6.4 Bouwen demonstratieopstelling

Resultaten:

- Een demonstratieopstelling volgens sectie 5.2;
- een verslag van de bouw van deze opstelling.

Benodigde tijd: ± 540 uur.

6.5 Opstellen Toepassingsvoorstel

Resultaten:

- Een toepassingsvoorstel volgens sectie 5.3.

Benodigde tijd: ± 420 uur.

6.6 Opstellen Projectverslag

Resultaten:

- Projectverslag conform de standaard die wordt gehanteerd bij de Hogeschool van Utrecht, afdeling ICIM van de faculteit Natuur en Techniek.

Benodigde tijd: ± 420 uur.

Hoofdstuk 7

Risicoanalyse

Gestreefd wordt naar een succesvolle voltooiing van het project. Helaas zijn er een aantal factoren die mogelijk roet in het eten kunnen gooien als er niet aan wordt voldaan.

Het is van belang dat alle projectleden voor de gehele periode beschikbaar zijn en zich voor de volle 100% inzetten. Dit is een kritische factor die een aantal risico's met zich meebrengt.

Zo is het mogelijk dat er iemand ziek wordt. Mocht dit een van de projectleden betreffen, dan betekent dit dat het project vertraging oploopt. Betreft het iemand van de begeleidende teams dan is er een grote kans dat het project ook enige vertraging zal oplopen. De kans op het ziek worden van een projectlid is relatief klein.

Een ander risico is het wegvallen van motivatie. Ook dit zal het project in zekere mate vertragen. Helaas is alleen niet te zeggen wanneer dit zou kunnen gebeuren en wat er tegen te doen valt.

Een derde risico is het wegvallen van de eenheid binnen de projectgroep. Wanneer dit gebeurt, kan dit leiden tot grote vertragingen en uiteindelijk tot het mislukken van het project.

Een andere factor is het blijven functioneren van de apparatuur. Risico's hierbij zijn het defect raken ervan of het uitvallen van de stroom wat beide tot gegevensverlies kan leiden. De kans dat dit optreedt is erg klein, maar als het gebeurt ligt het project direct stil. Bij een stroomstoring is het duidelijk dat er gewacht moet worden tot de stroom teruggekeerd is. Voor defecte hardware zal gewacht moeten worden tot er nieuwe geleverd is. Dit risico is echter zo klein dat hiervoor, naast het maken van de dagelijks backup, geen maatregelen voor hoeven te worden genomen.

Hoofdstuk 8

Methoden, technieken en standaarden

8.1 Extreme Programming

Voor ontwikkeling zal gebruik worden gemaakt van Extreme Programming¹ methodes. Dit ter voorkoming van het maken van fouten en het zo vroeg mogelijk opsporen van toch gemaakte fouten.

8.2 L^AT_EX

Voor het opstellen van documenten wordt gebruik gemaakt van L^AT_EX², een typesetting systeem wat ons in staat stelt complexe documenten op een vrij eenvoudige manier op te stellen en wat esthetisch verantwoorde resultaten produceert. Dit document is in een uitbreiding van L^AT_EX, L^AT_EX 2_ε genaamd, opgesteld.

8.3 Versiebeheer

Om het aan een gezamenlijke set documenten en code werken te bevorderen is besloten tot de invoer van een versiebeheerssysteem, genaamd CVS (Concurrent Versioning System³).

Alle producten, inclusief dit document, bevinden zich in de CVS Repository.

¹Zie www.extremeprogramming.org voor meer informatie.

²Zie www.L^AT_EX-project.org voor meer informatie.

³Zie www.cvshome.org voor meer informatie.

8.4 OpenBSD

OpenBSD⁴, een van UNIX afgeleidt systeem, stelt het projectteam in staat om zo nu en dan vrij ingewikkelde netwerkoplossingen goed te testen, aangezien het OpenBSD project vrij bewust van beveiliging is en een hoop aan beveiliging gerelateerde software standaard als “port” wordt meegeleverd.

8.5 Backupstrategie

Om eventuele desastreuze gevolgen van menselijk- of hardwarefalen te onder-
vangen wordt er gebruik gemaakt van een backup strategie waarbij van de CVS
Repository en andere belangrijke onderdelen wekelijks een offsite backup gemaakt
wordt.

⁴Zie www.openbsd.org voor meer informatie.

Hoofdstuk 9

Kwaliteitsbewaking

Om tijdens het project de kwaliteit van het uiteindelijke product te kunnen waarborgen, zal er regelmatig overleg zijn tussen alle projectleden. Er zal dan gekeken worden naar de vorderingen en hetgeen er nog moet gebeuren.

Eventuele fouten en problemen zullen besproken worden om er een passende oplossing voor te vinden. Het uiteindelijke doel van het project is een kwalitatief goed product op te leveren.

Naast de bovengenoemde kwaliteitswaarborgen zal er ook regelmatig overleg zijn met de begeleiding, zodat zij een onafhankelijk beeld van de kwaliteit kunnen geven.

Hoofdstuk 10

Projectorganisatie

De bedrijfsopdrachtgever van dit project is Dhr. A. van Doesburg en de schoolbegeleider is Dhr. L.J.M. van Moergestel, beiden als docent verbonden aan de Hogeschool van Utrecht, Faculteit Natuur & Techniek.

De projectleider, Martijn P. Rijkeboer, is eerste onder gelijken. De overige projectleden zijn:

- Jelmer E. Barhorst;
- Wouter Coene;
- Jesse C.J. van Dam.

Alle projectleden delen de verantwoordelijkheid voor het correct bereiken van de doelstellingen van dit project.

10.1 Aanwezigheid

De opdrachtgever, Dhr. A. van Doesburg, is op donderdag en vrijdag op school aanwezig en op woensdag telefonisch bereikbaar.

De schoolbegeleider, Dhr. L.J.M. van Moergestel, is de gehele week door beschikbaar en anders per e-mail bereikbaar.

De projectleden zijn woensdag t/m vrijdag op de volgende tijden aanwezig in de projectruimte (D221):

Jelmer	9:00 - 9:30 t/m 16:00
Wouter	9:30 - 10:00 t/m 17:00
Jesse	9:00 - 9:30 t/m 16:00
Martijn	9:00 - 9:30 t/m 16:00

10.2 Communicatie

10.2.1 Intern

De communicatie tussen de projectleden vindt voornamelijk mondeling plaats. Aantekeningen of mededelingen van diverse projectleden worden op een interne Wiki¹ site geplaatst. Voor urgente zaken die eventueel buiten de projecturen om geregeld moeten worden, zijn e-mail adressen en telefoonnummers uitgewisseld.

10.2.2 Intern naar extern

Met de diverse externe contactpersonen wordt voornamelijk mondeling gecommuniceerd. Indien een betreft persoon niet aanwezig is kan hem een e-mail gestuurd worden.

10.2.3 Extern naar intern

De begeleiders vanuit school en het bedrijf (wat in ons geval dezelfde instantie is), kunnen ons op de dagen dat wij aanwezig zijn vinden in de toegewezen projectruimte. Tevens hebben zij het e-mail adres en telefoonnummer van elk projectlid.

¹Zie www.usemod.com voor meer informatie.

Hoofdstuk 11

Projectarchief

Alle versies van producten, verslagen en configuratiebestanden zullen in het systeem dossier worden opgeslagen. Dit systeem dossier wordt gevormd door een speciaal daarvoor bestemd versiebeheersysteem. Van dit systeem zullen regelmatig backups worden gemaakt om verlies van belangrijke gegevens te voorkomen.

Alle beslissingen en andere administrativa welke betrekking hebben op het project zelf zullen worden opgeslagen in het project dossier, wat gevormd wordt door een Wiki-systeem. Zie voor meer informatie sectie 10.2.1.

Bijlage A

Versies

Hieronder volgt een lijst van de CVS versies van alle \LaTeX bronbestanden.

Bestand	Versie	Laatste wijziging	
pva.tex	1.22	2003-10-08	14:14
achtergronden.tex	1.7	2003-12-03	14:17
doelstelling.tex	1.3	2003-10-08	12:30
projectopdracht.tex	1.11	2003-10-07	11:55
activiteiten.tex	1.12	2003-10-07	11:56
randvoorwaarden.tex	1.13	2003-10-08	14:03
resultaten.tex	1.12	2003-10-07	11:55
risicos.tex	1.5	2003-10-07	11:15
methoden.tex	1.8	2003-10-07	11:15
kwaliteitsbewaking.tex	1.6	2003-10-07	11:15
projectorganisatie.tex	1.10	2003-12-03	10:27
projectarchief.tex	1.7	2003-10-07	11:15