UNIVERSIDADE DE BRASÍLIA

INSTITUTO DE LETRAS

DEPARTAMENTO DE LÍNGUAS ESTRANGEIRAS E TRADUÇÃO - LET

CURSO DE LETRAS – TRADUÇÃO

Talita Freire Arantes

TRADUÇÃO DE ARTIGOS CIENTÍFICOS NO CONTEXTO DA SEGURANÇA DA INFORMAÇÃO

Brasília, 2011

UNIVERSIDADE DE BRASÍLIA

INSTITUTO DE LETRAS

DEPARTAMENTO DE LÍNGUAS ESTRANGEIRAS E TRADUÇÃO - LET

CURSO DE LETRAS – TRADUÇÃO

Talita Freire Arantes 08/41226

Projeto Final de Tradução de um
livro do francês para o português, exigido como
requisito à aprovação na disciplina de Projeto
Final de Tradução do Curso de Letras – Tradução
da Universidade de Brasília – UnB.

Orientadora: Dr. Alice Maria de Araújo Ferreira

Brasília, 04 de julho de 2011.

AGRADECIMENTOS

A Deus por ser minha fonte de força e sustentação; a minha família e a meu noivo por me apoiarem em todos os meus projetos e sonhos; e aos meus professores que durante essa longa jornada de curso compartilharam comigo seus conhecimentos.
Talita

“Informação é poder.”

RESUMO

A Segurança da informação é um tema de capital importância para a sociedade atual haja vista que as informações tornaram-se ativos de grande valor para os indivíduos e para as organizações em geral. Neste sentido, a publicação de artigos científicos da área tem crescido exponencialmente. Por isso, o objetivo deste trabalho foi realizar a tradução de três artigos científicos desta área de conhecimento. Outrossim, por se tratar de um gênero cuja linguagem é especializada, foram utilizados os preceitos da terminologia para a elaboração de um glossário; cujo principal critério para a escolha dos termos foi a análise do tradutor especialista.

Palavras-chave : Segurança da informação, artigos científicos, terminologia, tradutor especialista.

SUMÁRIO

1. INTRODUÇÃO

A presente monografia teve como enfoque a tradução de artigos científicos da área de segurança da informação. Por se tratar de um gênero textual cuja linguagem é especializada, foi elaborado um glossário. Levantou-se, também, a discussão sobre a tradução feita por um especialista da área do texto de partida.

A escolha por textos do domínio da Segurança da Informação deveu-se a sua relevância para a sociedade. É ponto pacífico que as informações tornaram-se um dos ativos[1] mais valiosos para as pessoas em seu trabalho e em sua vida privada. Por isso, assegura-las é fundamental para que se preserve a sua confidencialidade, integridade, disponibilidade e autenticidade (DIAS, 2001). Neste sentido, práticas e procedimentos de segurança diversos têm sido adotados na rotina dos usuários e demais pessoas que manuseiam as informações; além da adoção dos mais variados tidos de recursos tecnológicos, que constituem uma parte fundamental para que a segurança logre sucesso. Dentre esses recursos, destacam-se os *firewalls, IPS, IDS, anti-spywares e anti-vírus.*

A Segurança da Informação tem ganhado, também, destaque no âmbito acadêmico. O resultado são as inúmeras publicações de artigos da área em periódicos científicos. No entanto, ainda são poucos os artigos em português; o que evidência a importância em se traduzir artigos da área para esta língua.

Ainda com relação à tradução de artigos científicos, o número de publicações de textos brasileiros deste gênero em periódicos nacionais e internacionais tem crescido exponencialmente nos últimos anos. Consequentemente, a demanda por traduções deste gênero textual também tem aumentado, alertando para a importância em se investigar a prática e a teoria que envolve o seu processo

[1] Ativo é algo tangível ou não , que possui valor para os indivíduos ou organizações. Por exemplo: pessoas são ativos importantes para a organização.

tradutório. Por isso, neste trabalho foram considerados os aspectos referentes à linguagem de especialidade, tais como a terminologia da área e a estrutura textual.

Foram, portanto, traduzidos neste trabalho três artigos que abordam os mecanismos de segurança da informação utilizados em sistemas de informação. O primeiro artigo, *La détection d'intrusions : les outils doivent coopérer* possui seis páginas e faz uma reflexão sobre os métodos de detecção de intrusos em redes de computadores. O outro artigo intitulado *MotOrBAC : un outil d'administration et de simulation de politiques de securite,* analisa a utilização de uma ferramenta de controle de acesso a sistemas e possui onze páginas. E o último, por sua vez, cujo título é *CryptoPage-1 : vers la fin du piratage informatique?* tem como enfoque o mecanismo de criptografia , visando a redução da pirataria na informática. Embora os artigos sejam de autores diferentes, observou-se uma uniformidade dos termos utilizados, principalmente, de termos em inglês.

O principal objetivo desse trabalho foi realizar uma análise terminológica dos artigos supracitados, haja vista seu cunho técnico/científico. Neste sentido, serão abordadas as duas dimensões da terminologia, sendo a primeira relacionada ao campo teórico (caracterização dos termos técnicos) e a segunda a dimensão aplicada (construção de um glossário técnico). Para tanto, os seguintes objetivos específicos serão contemplados:

1) Fazer uma tradução comentada dos três artigos para a língua portuguesa;
2) Analisar os termos utilizados;
3) Construir mapas conceituais com os termos; e,
4) Construir um glossário da área de segurança da informação com base nos mapas conceituais elaborados.

1.1JUSTIFICATIVA

O presente trabalho justifica-se por quatro principais fatores, a saber: 1) relevância da segurança da informação para a sociedade; 2) importância dos artigos acadêmicos para a fomentação da pesquisa científica no Brasil; 3) relevância da análise terminológica para a tradução; e 4) a figura do tradutor especialista da área.

Com relação à segurança da informação, pretendeu-se com este trabalho enriquecer a literatura em língua portuguesa da área; Além de facilitar o acesso de pesquisadores brasileiros às pesquisas sobre mecanismos de segurança realizadas em países francófonos.

Pretendeu-se, também, contribuir com a literatura da área de tradução; lançando luz à importância em se traduzir artigos científicos para a língua portuguesa e o papel da terminologia nessa tarefa. Com relação à figura do tradutor especialista da área, este trabalho buscou evidenciar a importância da figura do especialista da área, como fonte de consulta ou mesmo como tradutor.

2. METODOLOGIA

2.1 Pesquisa terminológica

O trabalho obedeceu, primeiramente, a três etapas: 1) leitura aprofundada dos artigos de modo a evitar dúvidas e/ou ambigüidades na leitura do texto original, 2) identificação dos termos em francês por meio de pesquisa terminológica em textos paralelos na língua de chegada com o intuito de identificar os termos e expressões equivalentes mais utilizados nesse tipo de texto,e 3) elaboração de mapas conceituais e fichas terminológicas para redação da microestrutura do glossário.

2.2 Tradução propriamente dita

A tradução foi realizada apenas por uma tradutora, que é especialista na área de segurança da informação; o que nos levou a levantar a questão do tradutor especialista no processo tradutório e como critério para seleção dos termos do glossários.

A tradução foi comentada pela tradutora por meio de rodapés. Nestes comentários, foram ressaltadas as dificuldades do processo tradutório e questões terminológicas ; bem como, culturais.

Por fim, foi elaborado um glossário de Segurança da Informação com base em mapas conceituais e fichas terminológicas elaborados pela tradutora.

3. REFLEXÕES TEÓRICAS

3.1 Terminologia

Os artigos científicos são constituídos, em grande parte, de termos específicos do domínio de especialidade; por isso é de fundamental importância que o tradutor análise tais termos sob a ótica do universo discursivo da área que pretende trabalhar . Afinal, este campo tem por objetivo o estudo dos traços semânticos e morfossintáticos dos termos técnico-científicos; bem como de fraseologias e definições terminológicas, visando a uma possível univocidade nas linguagens especializadas. Neste sentido, serão apresentados os principais conceitos e modelos teóricos da terminologia que servirão de base para a análise dos termos extraidos dos artigos traduzidos.

3.1.1 Conceitos

A terminologia representa os conhecimentos das áreas especialidades; exercendo funcionalidades de cunho linguístico, conceitual; e, comunicativa nas comunicações profissionais. Logo , é um reflexo formal da organização conceitual de uma especialidade posto que os termos transmitem conteúdos próprios de cada área. Para Kreiger e Finatto (2004), a terminologia exerce duas funções essenciais: a de representação e a de transmissão do conhecimento. As autoras ressaltam que estas funções estão associadas à natureza constitutiva dos termos que, por sua vez, são considerados como signos linguísticos de valor monossêmico e monorreferenciais; pois, em geral, veiculam apenas o significado específico de cada área. Outrossim, estabelecem uma única referência com o mundo exterior, sempre na ótica da área em que a unidade lexical está inserida.

Ainda segundo as autoras, a terminologia tornou-se mais relevante nos dias de hoje, com o acelerado desenvolvimento científico e necessidade constante de disseminação do conhecimento.

> A funcionalidade operada pelo léxico especializado na transmissão de conhecimentos, na transferência de aparatos tecnológicos, bem como nas relações contratuais faz com que a Terminologia assuma relevância na e para a sociedade atual, cujos paradigmas de desenvolvimento estão intimamente

> relacionados ao processo de economia globalizada e ao acelerado desenvolvimento científico e tecnológico. (KREIGER & FINATTO, 2004 pg. 18)

Consoante Kreiger e Finatto (2004), o campo de estudo da terminologia possui duas faces , a saber: teórica e aplicada. A primeira se refere à análise dos termos, englobando desde sua constituição até o seu comportamento em determinados léxicos. Tal análise oferece subsídios para a fundamentação de princípios e diretrizes de tratamento dos termos nas aplicações terminológicas. A segunda face, por sua vez, estabelece princípios e métodos de elaboração de ferramentas e produtos, tais como sistemas de reconhecimento automático de terminologias, glossários, dicionários técnico-científicos e bancos de dados terminológicos. O processo de elaboração de glossários será retomado no capítulo 5 deste trabalho

As autoras apresentam, também, as características principais da terminologia classificando-as (Tabela 1).

VERTENTES	PRÁTICA E TEÓRICA
ORIGEM	CONTEMPORANEIDADE
OBJETO	LÉXICO TEMÁTICA/TERMOS
PRODUTO	LÉXICOS, GLOSSÁRIOS, DICIONÁRIOS TERMINOLÓGICOS MONO,BI E MULTILINGUES, BANCOS DE DADOS TERMINOLÓGICOS
NATUREZA	COGNITIVA-NORMALIZADORA
OBJETIVOS E FUNÇÕES	-REPERTORIAR O LÉXICO GERAL -OFERECER INFORMAÇÕES ETIMOLÓGICAS, GRAMATICAIS, SOCIOLINGUISTICAS -OFERECER INFORMAÇÕES SEMANTICAS GERAIS E ESPECIALIZADAS DE TODAS AS UNIDADES LEXICAIS DE UM IDIOMA (POLISSEMIA)

	-OFERECER PADRÕES DE USOS LINGUISTICOS -LEGITIMAR O LÉXICO DE UMA LINGUA
USUÁRIO	ESPECÍFICO
FONTES	TEXTOS DE ESPECIALIDADE
ENTRADAS	
CRITÉRIOS DE SELEÇÃO	PERTINENCIA DO TERMO À ÁREA DE CONHECIMENTO/FREQUENCIA EM MENOR ESCALA
TIPOLOGIA	VERBAL:TERMOS SIMPLES, COMPOSTOS, SIGLES E ACRÔNIMOS NÃO-VERBAL: SIMBOLOS E FÓRMULAS
TRATAMENTO	MANUTENÇÃO DA FORMA PLENA E DECORRENTE DOS TERMOS

Tabela 1 : Características da Terminologia . Adaptada de Kreiger e Finatto (2004).

A Tradução e a Terminologia são áreas inter-relacionadas, haja vista que os termos técnico-científicos constituem elementos chaves para os textos especializados. Para Kreiger e Finatto(2004), o reconhecimento da funcionalidade, simultaneamente, cognitiva e comunicativa operada pelas terminologias explica a preocupação dos tradutores de textos especializados com esse componente léxico. Para o tradutor é fundamental ter um domínio da terminologia dos textos que traduz, para que se realize a adequada seleção dos termos equivalentes aos do texto da língua de partida. Para tanto, é necessário conhecer e poder acessar repertórios terminológicos utilizados na comunicação profissional tanto na língua de partida quanto na língua de chegada.

As autoras ressaltam, ainda, que a utilização adequada da terminologia contribui para o alcance da precisão semântico-conceitual, requisito essencial para toda a tradução de textos especializados. Além disso, o respeito pelo uso profissional de

termos e das fraseologias é , também, um respeito pelo estilo do texto original, o que favorece a aceitabilidade do texto de chegada, independente da língua em que será traduzido. No entanto, embora o domínio de uma terminologia seja condição necessária , não é suficiente para efetuar uma boa tradução, considerando que o processo tradutório é algo complexo que envolve muitos outros componentes.

Kreiger e Finatto (2004) advogam que apesar da relação de parceria entre Terminologia e Tradução, estes são dois campos distintos quer de atuação, quer de investigação. Entre as distinções das áreas, destaca-se a finalidade de seus produtos. Enquanto a Tradução constitui uma finalidade em si mesma pela produção de um texto em outra língua; a Terminologia aplicada realiza um trabalho de suporte na medida em que elabora instrumentos pragmáticos que se constituem em meios para facilitar o trabalho de tradutores, intérpretes, dentre outros. No entanto, tais áreas também possuem características em comum, como , por exemplo, a interdisciplinaridade.

3.2.2 Objetos da terminologia

A terminologia é composta por três elementos, a saber: o termo, a fraseologia e a definição. Ambos representam de formas diferentes o conhecimento especializado.

O termo constitui a unidade terminológica, ou seja, uma palavra à qual se atribui um conceito como seu significado. Neste sentido, o termo traz consigo o conceito de alguma ciência ou técnica de cuja característica principal é invariância conceitual; podendo ser igualmente denominado de unidade de conhecimento. Consoante Rondeau (1984) apud Kreiger e Finatto (2004), no termo para uma noção dada, há uma única denominação; e esta possui uma relação de univocidade entre denominação e noção. É importante ressaltar que o termo se difere da palavra, haja vista que esta última é unidade inseparável composta de forma e conteúdo (Kreiger e Finatto (2004)). A grande dificuldade está em se diferenciar termo e palavra. Kreiger e Finatto(2004) afirmam que a descrição detalhada das configurações terminológicas não pode se restringir à identificação dos componentes

moforssintáticos dos termos. É igualmente importante entender a forma como os termos se instituem nas diferentes comunicações especializadas e levar em conta os aspectos semânticos, textuais e pragmáticos que contribuem para o processo de gênese das terminologias. Emmel (1998) apud Polcholopek (2010), apresenta algumas características atribuídas ao termo, tais como:

- ➔ Etiqueta para uma determinada área;
- ➔ Unidade verbal especifica que designa um conceito já definido no sistema da área técnica;
- ➔ Não estático e nem isolado;
- ➔ De caráter relacional, operacional (permite entendimento geral da expressão);
- ➔ tem função textual e léxica bem abrangentes;
- ➔ unidade lexical definida na área de especialidade;
- ➔ qualidade que a palavra técnica adquire no âmbito teórico.

Para Kreiger e Finatto(2004), a fraseologia é um elemento constitutivo das comunicações profissionais. As autoras acrescentam que:

> A ideia de fraseologia está associada a uma estrutura linguística estereotipada que leva a uma interpretação semântica independente dos sentidos estritos dos constituintes da estrutura. É nessa perspectiva que se enquadram as expressões idiomáticas, frases feitas e provérbios utilizados nas diferentes línguas.(KREIGER e FINATO, 2004, p.84)

A descrição das estruturas que compõe a fraseologia é de grande valia para a produção de instrumentos de referência como glossários, dicionários e banco de dados. No âmbito da tradução, este tema destaca o problema da transposição semântica de uma língua para outra, já que o sentido das estruturas fraseológicas não se depreende da soma de seus componentes.

A definição veicula, também, conceitos de uma área de conhecimento por meio de enunciados-textos que fornecem significados aos termos ou expressões especializadas. Neste sentido, a definição deve ser aplicada apenas a um conjunto específico de entes e deve ser objetiva e clara.

3.1.3 Terminologia aplicada : elaboração de glossários

A elaboração do glossário de segurança da informação realizado neste trabalho,teve como base os conceitos de terminologia. Por isso, detalhamos neste capítulo tal processo de elaboração.

O primeiro passo para a elaboração de um glossário é o reconhecimento terminológico. Para tanto, é preciso levar em conta que os termos possuem sintagmas e pragmáticas com outras unidades, que de alguma forma, tais relações precisam ser mantidas ao se transpor o termo do texto de partida em um outro ambiente. É fundamental, também, saber se os termos são representativos da área de conhecimento em questão e se dizem “algo” para o público alvo.

O reconhecimento terminológico deve ser feito a partir de um *corpora* representativo constituído por textos técnicos ou científicos. As expressões de valor terminológico podem ser de natureza verbal, não verbais ou mista. Em geral, os glossários são compostos de expressões nominais. No entanto, a terminologia de uma área especializada é composta, igualmente, por adjetivos, verbos, sintagmas terminológicos e fraseologias, que devem ser levados em conta.

Kreiger e Finatto (2004) destacam alguns pontos que devem ser considerados no processo de elaboração do glossário, a saber: 1) o produto deve atender às necessidades de um público-alvo, e de preferência deve preencher uma lacuna de informação; 2) todos os dados registrados ou utilizados para a futura geração do produto devem ser plenamente confiáveis; 3) a utilização e ordem dos dados registrados devem ser convencionais e sistemáticos; e, 4) a ordenação dos dados de informação sobre o termo deve ser adaptada aos objetivos do trabalho e ao uso que será feito das informações.

Uma importante ferramenta de auxílio para a elaboração do glossário é a árvore de domínio, que constitui um diagrama hierárquico composto por termos-chave de uma especialidade. Tal diagrama é útil, pois mostra as inter-relações conceituais de uma especialidade; além de situar aonde se encontra um trabalho específico de termos para o glossário.(Kreiger e Finatto,2004). Outra importante ferramenta é a ficha terminológica que representa um núcleo de informações sobre um termo ou expressão de estudo. Esta ficha pode ser composta dos seguintes campos: termo; fonte do termo; definição; fonte de definição; contexto; fonte do

contexto; observações. Ambas as ferramentas foram elaborados neste trabalho e serão apresentadas mais adiante.

3.3 Linguagem de especialidade e o texto especializado

Uma das principais características do artigo científico é a linguagem de especialidade. Destarte, nesta etapa serão apresentados, brevemente, alguns conceitos da área.

Para Cabré (1999) apud Polchlopek (2010), a linguagem de especialidade não pode ser reduzida ao conteúdo científico que vincula; mas principalmente a maneira como este conteúdo será tratado no processo de comunicação.

Já para Aubert (2001) apud Polchlopek (2010), a linguagem de especialidade constitui um conjunto de marcas sintáticas, lexicais, estilísticas e discursivas. Ou mesmo, de um conjunto de termos característicos de uma área específica e estudo desses termos.

O texto especializado é, pois, a linguagem de especialidade na situação real de comunicação (Maciel , 2001, Hoffmann, 2004 apud Polchlopek, 2010), ou seja, constitui ao mesmo tempo o instrumento e resultado da atividade comunicativa de uma área especializada. Neste sentido, o texto especializado não se define apenas pelo critério tema (área científica ou técnica), mas também pela sua macroestrutura, relação de coerência entre seus elementos e utilização de unidades sintáticas, lexicais, morfológicas, dentre outros.

3.4 Tradução de textos técnicos

Embora de capital importância para a Era da Informação e do Conhecimento; a tradução de textos técnico-científicos ainda é marginalizada devido a algumas concepções, tais como: menor valor estilístico se comparada à tradução literária; não apresenta variações lexicais devido à especificidade de cunho terminológico; e, tem como ponto central de discussão a questão da equivalência textual.

De fato, os textos técnicos não permitem muitas variações estilísticas, o que, no entanto, não reduz o seu valor; haja vista que servem como disseminadores de dados e conhecimentos tecnológicos e científicos. Outrossim, os textos técnicos também estão expostos a fatores culturais, lexicais, sintáticos ou mesmo da própria área técnica em que se está traduzindo(POLCHLOPEK, 2010). Portanto, o domínio da terminologia , por si só, não é garantia de que a tradução seja bem sucedida.

Para Azenha Jr (1999), é preciso que sejam realizadas reflexões mais sistemáticas sobre a natureza e características da tradução técnica, abandonando a pré-concepção de que os textos técnicos são qualitativamente “inferiores” aos textos de base cultural mais evidente, já que

> Em se tratando de traduções técnicas, não é pequeno o anedotário sobre os “desastres” provocados por erros: os casos relatados vão desde acontecimentos mais corriqueiros como eletrodomésticos queimados e motores fundidos, até óbitos decorrentes da ingestão em dosagem indevida de medicamentos. (AZENHA JR, 1999,p.137)

Para Azenha Jr (1999), as principais características estilísticas do texto técnico são : a objetividade, o factual, uso de asserções, frases curtas e orações simples, a ausência de ambiguidade, pouco uso de adjetivação valorativa, o emprego de voz passiva e auxiliares modais, os parágrafos curtos e itemizados, dados estatísticos, as nominalizações, conclusões parciais , e a terminologia técnica. O autor acrescenta que , ao contrário do que se pensa, os textos técnicos possuem formas híbridas, estão sujeitos a um número elevadíssimo de variáveis e a terminologia é longe de ser algo estático, é dinâmico, sendo, portanto, difícil de controlar a subjetividade no tratamento da linguagem.

Ainda segundo o autor, o tradutor técnico dispõe hoje de ferramentas eletrônicas para otimizar sua tarefa e reduzir a margem de erros de tradução; bem como, suas consequências. Neste sentido, a consulta a bancos terminológicos deve ser uma atividade paralela ao processo tradutório, seja o tradutor especialista ou não numa determinada área. Para ele, o processo de tradução desse tipo de texto envolve os seguintes passos: a leitura crítica, a revisão terminológica através do acesso a banco de dados, a consulta a especialistas de seu país e do exterior, a

marca do seu estilo na constituição das estruturas sintáticas, o diálogo texto-imagem, e a formatação final.

Polchlopek (2010) ressalta que a maior responsabilidade do tradutor de textos técnicos científicos é

> a definição de estratégias, escolhas e gerenciamento de variáveis que vão desde a sua competência linguística e cultural até a avaliação da função que o texto traduzido pretende alcançar na cultura alvo.(POLCHLOPEK, 2010, p. 13)

A autora defende a ideia de que a tradução deve ser feita por profissionais tradutores, ainda que não sejam especialistas nas suas áreas de trabalho; cabendo ao técnico (médico, economista) revisar a terminologia e questões de ordem estilístico-discursivas. A autora também advoga que a terminologia é fator crucial para que a tradução logre sucesso haja vista que um erro de interpretação de algum termo pode resultar em um texto pobre, ou mesmo hilário.

Em suma, tanto a tradução de textos técnicos quanto de textos literários apresentam diversos desafios e barreiras. Afinal, fazer com que a tradução pareça tão natural e tão técnica quanto o texto de partida não é tarefa fácil.

3.4.1 Utilização de corpus na tradução técnica

Consoante Baker (1993) apud Paiva (2006), a análise de corpus constitui uma rica fonte de material descritivo-comparativo que pode ajudar a perceber diferenças entre a linguagem dos textos traduzidos e a dos textos originalmente escritos na língua de partida. Esta análise justifica-se pelo fato de que a tradução baseada em corpus parte do pressuposto de que a linguagem deve ser estudada por meio de exemplos de uso real da língua. A autora ressalta, ainda, que as pesquisas de tradução baseadas em corpus apontam para a noção de equivalência funcional entre o texto original e o texto alvo; o que mostra que o significado não é independente , mas se dá dentro de um contexto linguístico situacional e específico.

Paiva (2006) destaca algumas das vantagens da utilização de corpora, a saber: 1) integração de abordagens linguísticas e de estudos culturais à tradução;

b) a obtenção de resultados teóricos e práticos; c) o potencial de se investigar as particularidades de fenômenos específicos da linguagem; d) a flexibilidade e adaptabilidade dos corpora.

Neste trabalho foi utilizado como corpus para os três artigos científicos traduzidos, bem como alguns textos paralelos da área. É importante ressaltar que todos são digitalizados e consistem em um conjunto de dados linguísticos, sistematizados segundo determinados critérios, suficientemente extensos em amplitude e profundidade ; e que podem propiciar vários resultados úteis para a descrição e análise do texto.(Sanchez, 1995, Beber Sardinha, 2000, apud Paiva (2006)).

Para Paiva (2006), os seguintes pontos devem ser seguidos na construção de um corpus, a saber: 1) a origem dos dados; b) o propósito do corpus; c) a composição ; d) a formatação; e) representatividade; e f) extensão (BERBER SARDINHA, 2004 apud PAIVA (2006)).

3.5 Tradução por especialista

Discute-se na literatura do domínio da tradução; se o tradutor deve ou não ser especialista da área dos textos que traduz. Por isso, buscamos trazer esta discussão para o trabalho, haja vista que a tradutora é especialista da área de segurança da informação.

Para Finatto e Kerscher (2000), o domínio da linguagem especializada é fundamental para a identificação de suas terminologias. Neste sentido, as autoras acreditam que a cooperação entre linguistas e especialistas da área é peça fundamental para a definição da terminologia da área; e, também, no processo tradutório; produzindo um texto o mais fiel possível ao domínio e à linguagem de especialidade. Além disso, esta cooperação qualifica o trabalho e agrega valor econômico em um mercado tão concorrido e imediatista como é o da tradução especializada no Brasil.

Finatto e Kerscher (2000) traduziram um dicionário de química do espanhol para o português, por meio da cooperação entre tradutor, terminológo e especialista. Durante o processo, os especialistas indicavam impropriedades conceituais e denominativas na grande maioria dos conjuntos de verbetes do dicionário; além de

indicar os termos ultrapassados e não utilizados no Brasil. As principais inadequações encontradas pelos especialistas foram: 1) variação de não aceitação de terminologia normatizada; 2) variação de diferença de orientação entre escolas de nomenclatura; 3) variação de estilo condicionada por escolas de pensamento; 4) diferenças culturais; e 5) impropriedades conceituais. No entanto, o tradutor não poderia aderir a todas as recomendações; já que para as autoras este não tem condições de interferir significativamente na seleção lexical do texto original , por exemplo; podendo, no entanto, indicar as impropriedades nas notas de rodapé.

Em suma, as autoras acreditam que no processo de cooperação o especialista contribui com a revisão terminológica do texto de chegada e com a adequação do registro desse conhecimento. Já o terminológo, aborda a teoria e metodologia que são fundamentais para a prática tradutória. O tradutor , por sua vez, reconhece a terminologia que mais se adequa ao texto de chegada , visando a harmonia entre padrões de linguagem e conhecimento dos especialistas falantes da língua de chegada.

Para Araújo Ferreira (2000), o contato com os especialistas é primordial para qualquer trabalho terminológico e, também, para a tradução. A autora advoga que o contato com os especialistas deve ser preparado e orientado segundo os objetivos de cada trabalho terminológico. Entrevistas, palestras e cursos na área de conhecimento podem auxiliar o tradutor no contato com diferentes especialistas.

3.6 Tradução de artigos científicos

O número de publicações de artigos científicos tem aumentado significativamente, notadamente no Brasil. Em 2008, o país subiu duas posições no *ranking* mundial de número de artigos publicados, ocupando a 13ª posição; ultrapassando países como a Holanda e a Rússia de acordo com pesquisa feita pela Thomson Reuters. Outrossim, a área de Engenharia e Ciência da Computação (domínio dos textos que foram traduzidos), é a que mais apresenta número de artigos brasileiros completos em anais de eventos internacionais, conforme dados do MCT.

Os artigos científicos são compostos, em geral, de Introdução, Métodos, Resultados , Discussão e Conclusão, não apresentando grandes variações de formato entre áreas. Para Possamai (2004), o momento da redação de artigos

científicos é de capital importância e merece ser analisado. Isso, porque, entre o trabalho de campo ou no laboratório e o artigo final há uma grande distância, mostrando que nem sempre este representa a própria pesquisa.

Além disso, a elaboração do artigo é influenciado por fatores contextuais tais como regras impostas pelo periódico, colegas e a própria comunidade científica; o que reflete nos padrões textuais e nas expressões utilizadas. Neste contexto, caberá ao tradutor a tarefa de fazer o artigo operar, mantendo sua estrutura de gênero no texto de chegada, da mesma forma que opera no texto de partida. (ALBIR, 2001 apud POSSAMAI, 2004)

Possamai (2004) ressalta que os artigos científicos possuem marcadores textuais, ou seja, expressões ou unidades que são frequentes em certa área, ou ainda, expressão de mais de uma palavra que realiza uma função pragmática ou de estruturação do texto. São exemplos desses marcadores: é importante ressaltar que, como mostra a figura X, a partir da análise, dentre outros. Em sua pesquisa, a autora agrupa marcadores provenientes de artigos da área da Ciência da computação, tendo em vista sua função. Tais funções podem ser de três tipos, a saber: unidades relacionadas ao propósito do artigo científico (expressões que versam sobre o problema de pesquisa, objetivos, como é abordado, quando acontece, e etc; unidades metatextuais referentes à estruturação e organização discursiva do texto , como gráficos, figuras e tabelas; e, unidades modalizadoras que são relacionadas ao caráter persuasivo do artigo científico e evidenciam a presença do sujeito no texto (é importante ressaltar que...). A Tabela 2 apresenta de forma resumida alguns dos marcadores encontrados nos artigos em português agrupados por suas funções. Tais marcadores foram percebidos durante o processo tradutório dos três artigos científicos. No entanto, devido ao curto espaço de tempo para realização do trabalho, não foi possível aprofundar no estudo do tema.

Objetivo	**Forma**	**Método**	**Ancoragem**	**Quantificação**	**Tempo**
Com o objetivo de	Da mesma forma que	Através do uso	A partir de um/uma	A grande maioria	A partir do momento em que
Com a finalidade	De forma que	Através da utilização	A partir dos resultados	Na maioria dos casos	Até o presente

de			A partir da definição		momento
O objetivo central deste estudo	De modo que	Através de um processo	A partir das informações	A maior parte	primeiramente
O principal objetivo deste estudo	De maneira que	Através da realização	Como ponto de partida para	Em grande parte	Durante a realização Durante a fase de
A fim de	De tal forma que	Com o uso de	De base para	Na maioria das vezes	A medida que
A fim de que	É uma forma de	Com a utilização	Como base para	Um grande número de	Ao longo do tempo
		Para a realização		Uma grande variedade de	Ao longo do processo
		Com o auxílio		Até que ponto	Ao longo de

Tabela 2. Marcadores textuais de artigos em português. Adaptado de Possamai (2004).

4. Texto traduzido

Esta tradução possui comentários em notas de rodapé sobre as dificuldades encontradas pela tradutora, notadamente da área terminológica. Tais comentários substituíram o relatório de tradução. É importante ressaltar que as notas de rodapé dos textos de partidas encontram-se marcados com asteriscos (*), já que são a minoria.

Texto 1

Detecção de intrusos[2]:
As ferramentas devem cooperar

Resumo

A detecção de intrusos tem como objetivo detectar violações a politica de segurança em vigor no sistema de informação. Ela se baseia na análise no momento[3] da intrusão[4] ou em tempo diferente desta. Para tanto, duas abordagens são utilizadas: a abordagem baseada em conhecimento[5] (misuse detection) e a abordagem comportamental [6](anomaly detection). Cada uma dessas apresenta pontos fortes, mas também pontos fracos. O objetivo da presente pesquisa é mostrar a

[2] Existem duas possibilidades de tradução para a expressão Détection d´intrusion: a tradução literal detecção de intrusão ou detecção de intrusos. No entanto, ao fazer uma pesquisa em textos da área e no google a segunda opção apresentou maior número de frequência ; por isso a escolha.

[3] A tradução do termo à la volée mostrou-se problemática já que significa " ao vôo"; "no ar"; "na passagem"; e nenhuma dessas opções se enquadram no contexto. No entanto, foi encontrado em um texto de informática a expressão sendo usada como just-in-time, o nos levou a traduzir o termo por no momento.

[4] O termo **intrusão** foi acrescentado para ressaltar que a detecção se baseia na análise no momento de ocorrência da própria intrusão. Já no francês o termo à la volée não pede completo por isso não houve a necessidade da repetição da palavra intrusão: *La détection d'intrusions a pour objectif de détecter toute violation de la politique de sécurité en vigueur sur un système informatique.Elle est basée sur l'analyse à la volée*.

[5]Na frase Existem três opções para a tradução do termo approche par scénario: abordagem por cenário; abordagem baseada em conhecimento e abordagem baseada em assinaturas. Ambos possuem a mesma significação: um método de detecção que se baseia em comportamentos conhecidos pelo sistema, ou seja, assinaturas (vide glossário). No entanto, o termo abordagem baseada em conhecimento é mais usual nesta área de conhecimento; o que justifica a escolha.

[6] O termo approche comportementale pode ser traduzido por: abordagem comportamental (tradução literal) ou abordagem baseada em anomalias. Como ambas as opções são frequentementes adotadas nos textos desta área de conhecimento, optou-se pela tradução literal, a fim de ser mais fidedigno ao texto de partida.

necessidade da cooperação entre as ferramentas de detecção de intrusos para agrupar as forças e eliminar as falhas. Neste artigo [7]são oferecidas poucas referências bibliográficas a fim de direcionar o leitor para as obras de síntese, as quais fornecem várias referências. (1,2)

1. Introdução

A segurança dos sistemas de informação[8] visa proteger o acesso e a manipulação de dados e recursos de um sistema por meio de mecanismos de autenticação, autorização, controle de acesso, etc. No entanto, com a abertura e interconexão de sistemas de informação, explorar as falhas dos sistemas e contornar [9] seus mecanismos de segurança é sempre possível. Logo, não é suficiente agir apenas preventivamente, ou seja, definir uma politica de segurança (em termos de confidencialidade, integridade e disponibilidade de dados e recursos do sistema à proteger); e , implementar mecanismos que operacionalizem[10] esta politica. É preciso, também, ser capaz de detectar toda tentativa de violação da politica de segurança, ou seja, toda intrusão. Para tanto, pode-se utilizar uma ferramenta automática de detecção de intrusos (*IDS, Intrusion Detection System)*[11], o que implica em uma constante observação das ações organizacionais no sistema a fim de assegurar sua legitimidade. Esta observação é realizada pelo viés do mecanismo de auditoria de segurança que coleta informações sobre as ações realizadas no sistema. As informações coletadas são reagrupadas em arquivos nomeados de trilhas de auditoria.

---

[7] Nos artigos desta área de conhecimento, não é usual utilizar o pronome nós; que no francês é utilizado para empregar impessoalidade, se referindo a um grupo determinado de pessoas. Desta forma, optou-se por empregar a voz passiva a fim de omitir o pronome *nous.* A frase *Nous donnons peu de références bibliographiques dans cet article* foi então traduzida por *Neste artigo [7]são oferecidas poucas referências bibliográficas*

[8] A tradução do termo systèmes informatiques para a sua tradução literal sistemas informáticos não está errada, no entanto, esta é mais usual no português de Portugal. Já no português do Brasil é mais usual o termo sistemas de informação. Por isso , optou-se por este último.

[9] Na frase Néanmoins, avec l'ouverture et l'interconnexion des systèmes informatiques, des attaques exploitant les failles de ces systèmes et contournant leurs mécanismes de sécurité sont toujours possibles; o tempo verbal(participe du présent) do termo contournant e do termo exploitant foi alterado para infinitivo, haja vista que este tempo não é tão usual neste contexto do texto de chegada.

[10] No trecho mettre en oeuvre des mécanismes implantant cette politique; optou-se por traduzir o termo implantant por operacionalizam ao invés de implantam , já que o termo mettre em oeuvre foi traduzido por implementar.

[11] Os termos em que foram escritos em inglês no texto de partida tal como (*IDS, Intrusion Detection System*), não foram traduzidos já que mostram como o termo é utilizado em inglês, que é a língua mais usual desta área de conhecimento.

O restante deste artigo está organizado como se segue. As duas abordagens da detecção de intrusos estão apresentadas no parágrafo dois[12]. O paragrafo três é dedicado a uma breve apresentação das ferramentas de detecção de intrusos. Por fim, o parágrafo quatro discute a cooperação inter- IDS.

2. As duas abordagens de detecção de intrusos

A detecção de intrusos foi introduzida em 1980 por J.P. [13]Anderson que foi o primeiro a mostrar a importância da auditoria de segurança [3] com o objetivo de detectar as eventuais violações da politica de segurança de um sistema. Anderson definiu a violação da politica de segurança como uma tentativa deliberada de:

- ➔ Acessar de maneira não autorizada a informação. O acesso não autorizado pode ser efetuado por uma pessoa externa ao sistema (que não possui nenhum direito de acesso) ou mesmo por uma pessoa interna (que possui direitos de acesso limitados: neste caso, há uma violação de direitos de acesso). Nestes dois casos, fala-se em violação do contrato de confidencialidade de dados.
- ➔ Modificar a informação de forma não autorizada. Trata-se, neste caso, de atingir a integridade dos dados.
- ➔ Deteriorar toda ou parte dos dados e recursos de um sistema a fim de torná-lo não utilizável ou não confiável. É o caso da violação do contrato de disponibilidade dos dados e dos recursos de um sistema.

2.1 Abordagem comportamental e abordagem baseada em conhecimento

[12] Na tradução do trecho Le reste de cet article est organisé comme suit. Les deux approches de la détection d'intrusions sont présentées dans le paragraphe 2, o número foi escrito por extenso, por ser mais usual nesta área de conhecimento.

[13] Ao se traduzir o trecho La détection d'intrusions a été introduite en 1980 par J.P Anderson surgiu dúvidas quanto à normatização do texto, já que segundo a norma ABNT, que é a mais adotada em trabalhos acadêmicos e artigos científicos, ao citar um autor deve-se colocar apenas o último sobrenome. No entanto, optou-se por manter a normatização do texto de partida já que alguns periódicos do Brasil aceitam a citação desta forma.

Anderson propôs descrever estatisticamente o comportamento usual de um usuário a fim de detectar toda ação inabitual deste, para evitar repe((horários de conexão anormal, volume importante de ações ao sistema, etc.). É a primeira abordagem possível na detecção de intrusões, chamada " abordagem comportamental"; que permite detectar todo o desvio em relação à um comportamento normal previamente definido, geralmente por aprendizagem; e , armazenado em uma base de comportamentos. Hoje, não é mais o comportamento de um usuário que se busca modelar, mas de uma aplicação ou de um serviço particular.

Outra abordagem, cuja origem é desconhecida [14] , consiste em modelar não mais comportamentos normais, mas sim comportamentos não autorizados. Trata-se da "abordagem baseada em conhecimento" na qual se analisa os dados auditados em busca de cenários de ataques pré-definidos em uma base de assinaturas de ataque.

Cada uma dessas abordagens podem conduzir a falsos positivos (detecção de ataques na falta de um ataque real) ou falsos negativos (falta de detecção na presença de ataques):

- ➔ Uma ferramenta baseada na abordagem comportamental gera um alarme que detecta um comportamento não permitido. Ora, o desvio de comportamento observado pode ser devido a uma evolução natural do ambiente e do sistema: é um falso positivo. Ademais, o atacante (usuário interno malicioso) pode modificar lentamente seu comportamento a fim de ter um comportamento intrusivo que, sendo progressivamente captado , não será detectado: é um falso negativo.
- ➔ O risco de falsos positivos é menor com a abordagem baseada em conhecimento, pois a atividade litigiosa é descrita na base de ataque. No entanto, a qualidade da assinatura é importante: se ela não é precisa, pode também conduzir a vários falsos positivos. Por fim, evidentemente, se a

[14] A tradução do trecho *a la paternité mal définie* mostrou-se problemática, já que a sua tradução literal causaria estranhamento no texto de chegada. Como o termo partenité refere-se a paternidade o que nos remete a origem de algo, optou-se então pela seguinte tradução : cuja origem é desconhecida.

assinatura do ataque não estiver na base de assinaturas[15] (como no caso de novos ataques), o ataque em questão não será detectado(é um problema similar ao que se conhece com as bases de assinaturas de vírus).

2.2 Implementação das duas abordagens

O comportamento habitual, usualmente conhecido como perfil, pode ser construído de diferentes maneiras. Dentre os métodos propostos para construir os perfis, os mais relevantes são os seguintes[16]:

- ➔ Métodos estatísticos: o perfil é calculado a partir de variáveis consideradas como aleatórias e selecionadas[17] a intervalos regulares. Em um ambiente de informática clássico (rede de máquinas UNIX e NT), estas variáveis podem ser o tempo do processador utilizado, a duração, o horário de conexões, e etc. Um modelo estatístico é utilizado para construir a distribuição de cada variável e para medir, através de uma magnitude sintética, a taxa de desvio entre um comportamento atual e um comportamento passado.
- ➔ Imunologia: esta analogia com a imunologia da biologia consiste em construir um modelo de comportamento normal dos serviços (e não de usuários) por meio de cortes sequenciais de chamadas ao sistema que são considerados como representativos de uma execução normal de serviços considerados. A fase de aprendizagem consiste em observar um serviço durante um certo período de tempo para construir uma base de sequencias de chamadas normais. Na fase de detecção, toda sequencia externa a este conjunto é considerada como uma exploração potencial de uma falha de segurança do serviço.

---

[15] A inserção do termo de *assinatura após base* no trecho si la signature de l'attaque n'est pas dans la base (comme c'est le cas pour les nouvelles attaques), afim de enfatizar que a base se trata de uma base de assinaturas; evitando assim ambiguidade no texto.

[16] As redes neurais e sistemas especializados foram utilizados também, mas hoje em dia não o são mais.*

[17] Embora a tradução do termo échantillonnées do trecho le profil est calculé à partir de variables considérées comme aléatoires et échantillonnées à intervalles réguliers; é amostrada que provêm de amostras, optou-se por selecionados por ser mais usual nos artigos desta área de conhecimento.

- ➔ Gráficos: certas abordagens comportamentais utilizam modelos à base de gráficos para evidenciar propriedades e relações entre estes. Esta abordagem permite tratar mais facilmente os eventos raros.
- ➔ A abordagem Bayesiana: as redes Bayesianas permitem modelar situações nas quais a causalidade exerce uma função, mas o conhecimento do conjunto das relações entre os fenômenos é incompleto, de tal forma que é necessário descrevê-los de maneira probabilística. Os indicadores obtidos progressivamente sobre o estado do sistema modelado influem na confiança que condiz com uma preposição dada.

Vários mecanismos foram , igualmente, propostos a fim de localizar as assinaturas de ataques nas trilhas de auditoria (sistemas inteligentes, algoritmos genéticos, etc.). Hoje, no entanto, quase todas as ferramentas adotam algoritmos de análise de assinaturas, mas que se resumem essencialmente em operações de filtragem e de contagem. As técnicas de filtragem permitem, por exemplo, analisar os pacotes da rede um após na busca de motivos expressos em meio a expressões regulares. Os algoritmos de contagem permitem, por sua vez, detectar intrusões utilizando técnicas repetitivas, tais como um ataque com um dicionário de senhas usuais. Estes algoritmos simples permitem exprimir um grande número de assinaturas de ataques e há implementações muito eficazes para buscar expressões regulares. Entretanto, estes tipos de operação geram um grande número de falsos positivos durante a detecção haja vista que não permitem correlacionar as informações contidas em vários eventos, por exemplo, vários endereços[18] IP ou várias chamadas ao sistema efetuadas por um mesmo processo. Ainda há muita pesquisa a ser feita antes de disponibilizar um algoritmo de análise de assinaturas verdadeiramente eficaz em um ambiente operacional.

	Host based	Network based	Abordagem comportamental	Abordagem por cenário
BlackICE		pk IP		A.S.

[18] Outro termo problemático para traduzir foi *trame Ip* do trecho *par exemple plusieurs trames IP ou plusieurs appels systèmes effectués par un même processus.* Buscamos por uma tradução do termo completo em português, mas não encontramos nada. Optamos então pela busco do significado apenas de *trame* separadamente (trama,estrutura) que , no entanto, não se aplica ao contexto. Por fim, optamos pelo termo que mais se enquadra no contexto que é endereço IP.

Centrax	Audit NT	pk IP		A.S.
CyberCop	Audit	pk IP		A.S.
Monitor	Unix/NT	pk IP		A.S.
Dragon		pk IP		A.S.
Intruder		pk IP		A.S.
Alert	Audit Unix	pk IP		A.S.
NetProwler		pk IP		A.S.
NetRanger		pk IP		A.S.
NFR		pk IP		A.S.
Real Secure	Audit NT	pk IP		A.S.
Etrust(ex		pk IP		A.S.
Session				A.S.
Wall)				A.S.
				A.S.
AAFID	Audit Unix			
ASAX	Audit Unix			S.E
BRO		pk IP		A.S.
DIAMS		pk IP		A.S.
EMERALD		pk IP	Stat.	A.S.
GASSATA	Audit Unix			A.S.
GrIDS		pk IP		A.S.
Shadow		pk IP	S.E.	
SNORT		pk IP		A.S.
				A.S.

Tabela 1: Algumas ferramentas de detecção de intrusão (A.S. = Análise de Assinatura; S.E.= Sistema Especialista).

3. Ferramentas de detecção de intrusão

Desde a metade dos anos 80, vários trabalhos têm sido inspirados no modelo de Anderson e vários IDS que o implementaram foram comercializados. De 1984 a 1986, Denning *et al.* trabalharam na concepção de um sistema de detecção de intrusão baseado em métodos estatísticos e sistemas especialistas. Esta ferramenta, conhecida como IDES (*Intrusion Detection Expert System)* é a primeira ferramenta hibrida que reagrupa o método comportamental e baseado em conhecimento. O protótipo do IDES foi, posteriormente , desenvolvido e melhorado para chegar em 1993, ao NIDES. O NIDES e outras ferramentas desenvolvidas durante os mesmos anos mostraram a possibilidade de distinguir um comportamento normal de um comportamento anormal na máquina UNIX, utilizando as informações nos comandos passados nesta máquina. Entretanto, se o comportamento do usuário é muito variado[19], sua modelagem torna-se difícil e o método comportamental encontra sua limitação. A partir da metade dos anos 90, o método baseado em conhecimento tornou-se o principal implantado em ferramentas. Hoje, a maior parte dos IDS comerciais adotam este principio.

Os primeiros IDS eram destinados aos servidores de cálculo baseados na arquitetura UNIX com usuários essencialmente locais. As informações de auditoria coletadas provinham, sobretudo, da própria máquina a partir de diversas fontes (histórico de comandos de sistemas realizados por usuários; uso de recursos compartilhados pelos usuários; trilhas de auditoria do sistema; etc). Os IDS que utilizam estas fontes de dados são chamados de *Host Based Intrusion Detection Systems* ou *HIDS..* Com a abertura e a interconexão de sistemas de informação via internet, novos ataques de rede apareceram (Negação de Serviço, IP Spoofing,...). As fontes de auditoria locais passaram a não ser mais suficientes para detectar estes ataques. Os dispositivos físicos e lógicos foram, então, desenvolvidos a fim de capturar o tráfico da rede em tempo real, permitindo sua análise na busca de ataques de rede. Os IDS que utilizam

[19] No trecho Cependant, si le comportement de l'utilisateur est trop riche, sa modélisation devient difficile et l'approche comportementale trouve sa limite; o termo *trop riche* mostrou-se problemático no momento da tradução, já que sua tradução literal(muito/demasiadamente rico, presunçoso,abundante...) não fazia sentido no contexto. Por isso, optou-se por uma expressão mais próxima de abundante que foi o *termo muito variado.*

estas fontes de dados são chamados de *Network Based Intrusion Detection Systems* ou *NIDS,* que hoje[20] constitui a maior parte dos IDS comerciais[21].

A tabela 1 apresenta os métodos de detecção e as fontes de dados utilizadas por algumas ferramentas do comércio e do mundo livre. [22]

Pode-se dizer que hoje se dispõe de bons IDS que respondem perfeitamente às necessidades de segurança das empresas? Infelizmente, parece que não. De fato, os IDS comerciais são sem dúvidas mais simples quanto as técnicas de análise de trilhas que implementam (filtragem, contagem). Em termos de desempenho, suas bases de assinatura são frequentemente limitadas a cenários mono ambientes, o que gera vários falsos positivos. Com relação ao IDS do domínio público, é possível encontrar geralmente ferramentas melhores em termos de qualidade de detecção, mas que apresentam ainda vários problemas (instalação e configuração frequentemente difíceis, falta de bases de ataques sequenciais e diários). Ademais, as taxas de falsos positivos encontrados com os IDS públicos são ainda muito importantes.

4 **A cooperação inter-IDS**

Foi visto que as duas abordagens de detecção possuem forças e fraquezas intrínsecas com as quais se deve contar. O mesmo serve para mecanismos escolhidos para implementar estas abordagens no IDS. Consequentemente, é indispensável a cooperação entre diversas ferramentas afins; de um lado, para aproveitar as potencialidades de cada uma a fim de limitar as taxas de falsos negativos; por outro lado, para correlacionar alarmes emitidos a fim de limitar as taxas de falsos positivos.

O objetivo é de disponibilizar um sistema de detecção de intrusos global, que utilize como entrada tanto dados de rede quanto dados do sistema, analisando estes

[20] Optou-se por traduzir *maintenant* por *hoje* por ser um termo mais utilizado dentro deste contexto. Nota do tradutor.

[21] No trecho *Les IDS utilisant ces sources de données sont appelés Network Based Intrusion Detection Systems ou NIDS. La plupart des IDS commerciaux sont maintenant des NIDS,* optou-se por fazer uma junção das duas frases evitando a repetição do IDS e do NIDS (já que isso não prejudicaria a compreensão do texto.

[22] Monde libre do trecho *le tableau 1 montre les méthodes de détection et les sources de données utilisées par quelques outils du commerce et du monde libre.* é uma expressão do discurso de Fulton de Winston Churchill proferido em 1946, que descreve a divisão da Europa em dois blocos separados por uma cortina de ferro. Já que não foi encontrada uma expressão equivalente para o termo, optou-se pela tradução literal.

dados segundo uma abordagem comportamental e segundo uma abordagem baseada em conhecimento, ambas implementadas de várias formas diferentes por mecanismos diferentes.

Para chegar a este nível de cooperação inter-IDS, serão úteis e verdadeiramente indispensáveis:

1- Uma linguagem de descrição comum dos eventos a analisar;
2- Uma linguagem de descrição comum dos ataques de busca;
3- Uma linguagem de descrição comum dos comportamentos normais;
4- Uma linguagem de descrição comum de alarmes a enviar ou a receber;
5- Técnicas de correlação destes alarmes.

Estes diferentes sujeitos começaram a ser estudados por diversos projetos de pesquisa. Com relação à descrição de alarmes (e eventualmente a descrição de eventos a serem analisados), os trabalhos mais bem sucedidos e que tem todas as chances de se impor nos próximos meses são os do grupo IDWG e do IETF. Um formato, IDMEF (*Intrusion Detection Message Exchange Format)* , foi definido e as ferramentas já começaram a utilizá-lo. No que tange a descrição dos ataques, pode-se citar, a título de exemplo, os trabalhos geridos na França no projeto MIRADOR[23] que propôs duas linguagens de descrição de ataques (ADeLe e Lambda). Por fim, o último ponto, a correlação de alertas, aparece como particularmente importante. De fato:

➔ É muito raro que um alarme gere apenas um alarme. A correlação permite agrupar os alarmes relativos a um mesmo ataque, estudar os diferentes ataques em curso, avaliar globalmente a situação e preparar uma resposta apropriada.

➔ Como já foi mencionado, os IDS geram vários falsos positivos. A correlação permitirá, utilizando várias fontes de dados, verificar a pertinência de alarmes e aprimorar o diagnóstico pelo crescimento de vários alarmes ou pela pesquisa de informações complementares.

➔ O custo da coleta e da análise de informações por uma ferramenta de detecção de intrusos é altamente mais elevada do que a precisão da fonte de

[23] Iniciado pela DGA, este projeto é gerenciado pela Alcatel e entrou no mundo acadêmico através da Supélec, da ENST Bretagne e da ONERA. *

informações . A correlação permitirá adaptar a quantidade de informações coletadas às ameaças potenciais das quais os alarmes indicam a presença.

A nível de informação, os trabalhos sobre as técnicas de correlação de alarmes estão em andamento (mas ainda não foram publicados) no MIRADOR.

5 **Conclusão**

Dispor de ferramentas de detecção de intrusão eficazes parece ser uma aposta essencial para a segurança dos sistemas de informação. A eficácia buscada apenas será atingida pelo através da cooperação entre várias ferramentas de detecção de conceituação diferentes[24]. Há uma aposta de pesquisa maior a ser levantada pela comunidade.

Texto 2

MotOrBAC: uma ferramenta de gerenciamento[25] e simulação de politicas de segurança

Resumo

Face a grande complexidade dos sistemas de informação e das dificuldades em se adotar uma política de segurança coerente, os administradores necessitam de ferramentas de gestão simples e eficazes. Neste artigo, será apresentado o protótipo MotOrBac que permite centralizar em um modelo único, a estrutura[26] e o gerencimamento da politica de segurança do sistema de informação. O MotOrBAC analisa e simula uma política de segurança especifica, conforme o modelo OrBac (Organization Based Access Control). Este protótipo implementa , também, um conjunto de funções introduzidas no modelo AdOrBAC (

[24] Certos algoritmos de detecção deverão também ser melhorados.*

[25] No trecho *un outil d´administration et de simulation de politiques de sécurité,* optou-se por traduzir a palavra administration por gerenciamento ao invés da tradução literal *administração* apesar de ambos possuírem o mesmo significado, por ser um termo mais utilizado nesta área de conhecimento.

[26] No trecho *Dans cet article, nous présentons le prototype MotOrBAC qui permet de centraliser dans un modèle unique, l'expression et l'administration de la politique de sécurité du système d'information,* o termo expression mostrou-se problemático já que a sua tradução literal não faz sentido neste contexto. Como este termo também pode significar articulação; aparência; aspecto; optou-se por um equivalente desses termos que é o termo estrutura.

Administration Organization Based Access Control) que permitem o gerenciamento do OrBAC.

Neste artigo, serão apresentadas as vantagens que o modelo OrBAC apresenta para desenvolver um protótipo. Em seguida, serão estudadas as diversas funcionalidades do MoTOrBAC: 1) especificação de uma política de segurança; 2) simulação; 3) análise da coerência e 4) administração da política.

Palavras-chave: modelo de segurança, modelagem lógica, gerenciamento de uma política de segurança, OrBAC.

1 Introdução

Os sistemas de informação (SI) tornam-se cada vez mais complexos. Estes sistemas combinam frequentemente as infraestruturas de redes fixas e móveis (sem fio), que ficam em vários sistemas operacionais[27] (Windows, Linux, Unix. MacOs, etc) e fornecem várias aplicações (mensagens, navegadores, servidores de base dados, serviços web, etc).

Neste contexto, definir e posteriormente gerar uma politica de segurança é uma tarefa complexa para os administradores. Na maioria dos casos, esta tarefa é , na verdade, realizada de forma artesanal: os administradores devem configurar manualmente os diferentes componentes de segurança da arquitetura do SI do qual são responsáveis.

Ferramentas de gerenciamento, tais como Firewall Builder ou Solsoft Net-Partioner, existem. Estes softwares[28] são indiscutivelmente úteis, mas se limitam ao gerenciamento de componentes de segurança de redes. As ferramentas para administrar os componentes de segurança do sistema (por exemplo, um sistema operacional tal como o SE-Linux) ou aplicativo (por exemplo, um sistema de gestão de base de dados tal como a Oracle), são muito mais limitados e necessitam de conhecimento especializado, o que é muito importante.

O objetivo deste artigo é apresentar um protótipo, MotOrBAC, que foi desenvolvido para gerenciar uma politica de segurança. O MotOrBAC fornece as

[27] No trecho *reposant sur divers systèmes d'exploitation (Windows, Linux, Unix, MacOS, etc)* Optou-se por traduzir systemes d'exploitation por sistemas operacionais devido principalmente aos termos entre parênteses serem todos sistemas operacionais; e, também, por ser um termo mais usual nesta área de conhecimento.

[28] No trecho *Ces logiciels sont incontestablement utiles mais se limitent à l'administration des composants de sécurité réseau.* Embora em Francês exista uma tradução para o termo Software (logiciel), no português do Brasil é mais usual adotar o termo em inglês , por isso a escolha.

seguintes funções: 1) estrutura de uma politica de segurança baseada no modelo OrBAC; 2) simulação da politica; 3) análise da coerência da política e 4) especificação da politica de gerenciamento.

O objetivo da MotOrBAC é centralizar em um modelo de segurança único a expressão de todas as exigências de segurança de redes, sistemas ou aplicativos. Por isso, o MotOrBAC é baseado no modelo OrBAC. O OrBAC é um modelo que permite representar uma politica de segurança no nível organizacional, ou seja, independente da implantação que será feita em seguida por esta politica. Destarte, é possível também divulgar o conjunto de exigências de segurança do SI e posteriormente distribuir estas nos diferentes componentes de segurança, vistos como pertencentes[29] à sub-organização da organização que constitui o SI. Esta distribuição contém igualmente as responsabilidades da administração que podem ser entregues aos sujeitos atribuídos a funções distintas.

Uma vez que a politica de segurança representa o nível organizacional, o administrador de segurança pode utilizar o MotOrBAC para introduzir as entidades concretas (sujeitos, ações e objetos) aos quais a politica se aplica. Desta forma, a função de simulação permite testar a politica de segurança organizacional nestas entidades concretas.

O objetivo de centralizar a estrutura da politica de segurança é dispor de uma visão global da politica da qual se pode analisar a coerência. Como o modelo OrBAC oferece a possibilidade de divulgar uma politica de segurança mista, incluindo privilégios positivos (permissões) e negativos (proibições), os conflitos podem aparecer. O objetivo da função da análise da coerência é detectar estes conflitos e , posteriormente, oferecer uma possibilidade de definir as estratégias para solucionar estes conflitos.

Por fim, a função da administração contribui para especificar quem possui a responsabilidade de divulgar; e, posteriormente, atualizar a politica de segurança do sistema de informação. Atualmente, a maior parte dos modelos de segurança é de responsabilidade de um administrador de segurança único que tem plenos poderes para definir a politica de segurança (redes, sistema ou aplicativos). Esta

[29] O termo *autant* do *trecho vus comme autant de sous-organisations de l'organisation que constitue le SI,* que significa tanto quanto, foi traduzido por pertencente à devido ao contexto.Já que sua tradução literal provocaria estranhamento no texto.

hipótese de um administrador único não se enquadra mais nas infraestruturas de SI , cada vez mais distribuídas. A função de gerenciamento implantada no MotOrBAC baseia-se no modelo AdOrBAC, que permite definir uma politica de administração utilizando os mesmos conceitos que o OrBAC (o que faz do OrBAC um modelo auto-administrável[30]). Utilizando-se o AdOrBAC, é possível distribuir a administração da política sob várias funções tendo cada qual direitos de administração restritos. No MotOrBAC, a estrutura da politica de gerenciamento é utilizada como politica de controle de acesso aplicado aos administradores que acessam o MotOrBAC.

A estrutura[31] do restante do artigo é a seguinte: na primeira seção, é motivada a implementação do protótipo de simulação e análise da política de segurança baseada no modelo OrBAC; a seção dois justifica as diferentes funcionalidades oferecidas pela MotOrBAC, relembra os conceitos introduzidos no modelo OrBAC e apresenta os principais gêneros do protótipo que foram desenvolvidos; a seção três explica como definir uma politica de segurança utilizando o MotOrBAC. A seção quatro descreve a função de simulação da política de segurança no nível concreto; e, a seção cinco apresenta a função da gestão de conflitos. Na seção seis, mostramos como o MotOrBAC implanta o modelo de gerenciamento AdOrBAC. Este artigo conclui-se na seção sete, na qual são apresentadas as perspectivas da evolução do MotOrBAC.

2 **Necessidade de uma ferramenta de gerenciamento**

2.1 Motivação

Atualmente, as sociedades privadas e os órgãos públicos enfrentam inúmeros problemas para adotar a política de segurança de sua SI. Para ilustrar alguns desses problemas, será apresentada[32] uma organização e suas necessidades

[30] Ao se traduzir o *trecho ce qui fait de OrBAC un modèle auto-administré* , deparamos com três possibilidades de tradução para o termo auto-administré : auto administrável, auto-administrável e autoadministrável. Neste sentido, a escolha do termo a ser utilizado no texto foi feita por meio do número de ocorrências do google.

[31] Nos artigos científicos desta área de conhecimento, utiliza-se o termo *estrutura* para se referir à organização dos tópicos/capítulos do artigo, o que justifica a tradução do termo *plan* do trecho *le plan du reste de l'article est le suivant,* para estrutura.

[32] A expressão intéressons-nous do trecho *Pour illustrer certains de ces problèmes, intéressons-nous à une organisation et à ses besoins de définition et de gestion de la sécurité de son SI*, foi traduzida

de definição da gestão de segurança de sua SI. Uma sociedade *WorldCompany* possui várias filiais (*FranceCompany, EnglandCompany...).*Ela subcontrata outras empresas (*TaiwanSousTrait)* para realizar uma parte de suas atividades; e possui vários administradores (François, Ali e Juda[33]). Todas as filiais da *WorldCompanu* tratam do mesmo produto. Sua hierarquia, sua política e seus mercados, que aqui são definidos, são similares. A *WorldCompany* deseja definir uma politica de segurança idêntica e coerente em todas as suas filiais. Entretanto, a *WorldCompany* enfrenta dificuldades. De fato, a *FranceCompany* e *a EnglandCompany* são filiais situadas em dois países diferentes, que não possuem a mesma legislação. Os administradores da *WorldCompany* devem adaptar as politicas destas filiais a fim de que elas sejam compatíveis com as legislações dos países nas quais se situam. Diante desta adaptação, a *WorldCompany* se deu conta de que um de seus administradores, *Juda,* definiu regras na política de segurança que deixam as informações muito vulneráveis. Não sabendo se Judá é um administrador mal intencionado, incompetente ou se lhe faltam elementos necessários para se ter uma visibilidade global acerca do conjunto que compõe a SI, a *WorldCompany* deseja reduzir os direitos deste administrador. Por outro lado, a *WorldCompany* deve autorizar um certo número de acessos a seus subcontratantes, e os modificar segundo os papéis que devem exercer na sociedade. Ademais, os administradores da *WorldCompany* devem gerir as aposentadorias, os estagiários, etc. Eles devem poder modificar facilmente a politica de segurança em caso de mudança radical desta, como a passagem das 39 horas para 35 horas, na França[34].

Está claro que, entre os problemas encontrados pela *WorldCompany* e que podem ocorrer a qualquer organização que implemente uma politica de segurança, alguns são ligados a restruturação, outros a verificação da coerência

---

pelo termo *será apresentada,* já que o objetivo deste termo no contexto é apresentar uma organização.

[33] No trecho *Elle possède plusieurs administrateurs (Francois, Ali et Juda),* surgiu uma questão cultural , ou seja, deveria se traduzir ou não os nomes dos administradores da organização, já que estes nomes não são típicos no Brasil. No entanto, como trata-se de um artigo científico cujos leitores muitas vezes se interessam em saber a procedência do mesmo, optou-se por manter os traços culturais do texto de partida.

[34] Devido há uma medida da política econômica francesa do governo de Jospin, desde 2000 a jornada de trabalho semanal, que antes era de 39 horas, passou a ser de 35 horas.

da politica, ou ainda a centralização e especificação dos direitos da administração. É difícil para os administradores terem uma visão global da política de segurança para elaborá-la corretamente. Esta é uma das razões pela qual a utilização de um software de gerenciamento de suporte[35] permite visualizar e obter rapidamente informações de que se tem necessidade. No entanto, para que este software seja eficaz, este deve se apoiar em um modelo que ofereça as propriedades necessárias para responder aos problemas de especificação e gestão da politica de segurança, tal como estes que ocorrem na sociedade *World Company.* Este modelo deve permitir gerar simplesmente várias entidades, possuindo diversos modos de gerenciamento (centralizados ou não, um super administrador ou vários administradores tendo os mesmos direitos limitados, contextuais,...) e permitindo verificar a coerência com a politica. O estado da arte do domínio possibilitou a conclusão de que o modelo OrBac é um dos modelos que atende melhor as especificações requeridas por este software.

2.2 OrBAC

O objetivo do OrBAC [ABB+03, CM04b] é modelar uma política de segurança centrada na organização que a define ou que é responsável por esta. Consequentemente, uma empresa é uma organização, mas um componente de segurança, tal como um firewall corresponde igualmente a uma organização. A especificação de uma política OrBAC se dá no nível organizacional (abstrato) independentemente de sua implantação. A politica implantada (concreta) é derivada da politica organizacional. Esta abordagem torna toda a politica representada no modelo OrBAC, reproduzível e evolutiva. De fato, esta não necessita de nenhum reajustamento no nível concreto, que poderá introduzir incoerências dificilmente recuperáveis; tudo é feito no nível organizacional. O nível concreto é constituído de sujeitos, ações e objetos. O nível organizacional contem as funções, as atividades e as visões. A função (respectivamente da atividade, a visão) é um conjunto de sujeitos (respectivamente de ações, objetos) nos quais são aplicadas as mesmas regras de segurança.

[35] Outro termo problemático foi utilisation aisée do trecho *C'est l'une des raisons pour laquelle l'utilisation d'un logiciel d'administration d'utilisation aisée leur permettraient de visualiser et d'obtenir rapidement les informations dont ils ont besoin*. A principio,optou-se pela tradução literal, que no entanto não fazia sentido no contexto. Ao jogar o termo no google, no entanto, este sempre estava localizado em sites de produtos como a Nokia com informações referentes a suporte, o que nos levou a optar por este termo para a tradução.

O modelo OrBAC apoia-se em um formalismo baseado na lógica da primeira ordem com negação. Entretanto, como a lógica da primeira ordem é em geral indecidível , o modelo foi limitado para que seja compatível com um programa Datalog estratificado [Ull89]. Um programa Datalog não deve utilizar termos funcionais e deve incluir apenas regras definidas e seguras. Uma regra é definida se cada variável que aparece na conclusão da regra aparece, também, na premissa. Uma regra é segura se permite apenas derivar um conjunto finito de expressões. Em todas as regras, as variáveis são universalmente quantificadas. As literais negativas são autorizadas na premissa, mas as regras devem poder ser estratificadas. A estratificação de um programa Datalog consiste em ordenar as regras:[36] se uma regra contem uma negativo literal, então as regras que definem este literal são, a principio, avaliadas. Um programa Datalog estratificado é calculável em tempo polinomial.

Posteriormente, todas as regras que definem a política de segurança devem, pois, corresponder a um programa Datalog estratificado. Para representar estas regras, deve-se utilizar uma notação a Prolog[37]. Os termos começam por uma letra maiúscula correspondente às variáveis, enquanto que os termos que começam com letra minúscula, por exemplo, jean, correspondem às constantes. Um fato, tal como parent(jean, marie)., indica que jean é um parente de marie. Uma regra tal que

Grand_parent (X,Z):- parent (X,Y), parent (X,Z)[38].

indica que x é um avo de z se existe um sujeito y tal que x é um parente de y e y é um parente de z.

Utilizando-se este formalismo, cada organização pode, posteriormente, definir as regras de segurança para especificar que certas regras tem a permissão, proibição ou obrigação de realizar certas atividades em certos cenários. Estas regras de segurança não são estatísticas, mas sua ativação depende, ao contrário de condições contextuais. Neste sentido, o conceito de contexto é

[36] O sinal de ponto e vírgula foi substituído por dois pontos para adequar-se às regras gramaticais do português.

[37] É ,entretanto, importante ressaltar que os administradores introduzem as regras via uma interface e que não se introduz, em geral, regras lógicas quando se utiliza o MotOrBAC.*

[38] Nos trechos com linhas de código , tais como grand parent(X,Z) :- parent(X,Y),parent(Y,Z), optou-se por manter em inglês, já que está é a língua universal dos programas de compilação de códigos de programação, e caso este não esteja programado para ler códigos em português, a tradução poderia gerar um erro na hora de rodá-los.

explicitamente introduzido no OrBAC e intervém na definição de regras de segurança. Desta forma, utilizando-se tal formalismo baseado na lógica da primeira ordem, as regras de segurança são representadas utilizando-se três predicativos de aridade 5: permissão, proibição e obrigação. Por exemplo:

● permission (org, role, activity, view, context) significa que, na organização org, os sujeitos atribuídos à role possuem a permissão de realizar uma activity na visão view no contexto context.

Os predicativos prohibition e obligation são definidos de forma similar. Por exemplo, a permissão seguinte:

● permission (hospital, nurse, consult, medical_record, urgency)

Especifica que, na organização hospital, os enfermeiros possuem a permissão de consultar os dossiês médicos em um contexto de urgência.

Todos os conceitos da organização, de regra, de atividade, de visão e contexto, podem ser estruturados hierarquicamente. As permissões, proibições e obrigações são ,então ,herdadas quando se elevam na hierarquia (ver [CCBM04] para mais detalhes). Como uma politica de segurança pode incluir regras de segurança conflituosas (por exemplo, conflito entre uma permissão e uma proibição), é necessário definir estratégias de resolução de conflitos. A forma como este problema é resolvido no OrBAC é apresentada na seção 4.

Uma vez definida a política de segurança organizacional, é possível testar como esta política se aplica a entidades concretas que são os sujeitos, ações e objetos. Para tanto, serão introduzidos três predicativos de aridade 3 para atribuir a um sujeito um papel ([39]uma ação à uma atividade) (um objetivo à uma visão):

●empower (org, subject, role): especifica que na organização org, o sujeito subject é atribuído a um papel role.

● consider (org, action, activity): especifica que na organização org, a ação action implanta uma atividade activity.

● use (org, object, view): especifica que na organização org, o objeto object é utilizado na visão view.

[39] No trecho *(resp. une action à une activité) (resp. un objet à une vue),* optou-se por retirar a abreviação resp. que em inglês significa *response;* já que esta não foi encontrado em artigos desta área de conhecimento . Ademais, a sua retirada não prejudica a compreensão do texto.

Por exemplo, o fato empower (hospital, jean, physician) especifica que a jean atribui-se um papel physician na organização hospital.

Os contextos são definidos por regras lógicas que caracterizam naquelas condições que o contexto é ativo. No modelo OrBAC, este é modelado por regras lógicas tendo o predicativo hold como conclusão. Hold é um predicativo de aridade 5 definido da seguinte forma:

●hold (org, subject, action, object,context): especifica que na organização org, o sujeito subject realiza a ação action no objeto object no contexto context.

Utilizando-se este modelo, é possível, posteriormente, derivar as autorizações concretas que se aplicam aos sujeitos, ações e visões. O principio geral de derivação de autorizações concretas a partir das autorizações organizacionais é apresentado na seção 5 e é utilizado por simular a politica de segurança em nível concreto.

2.3. MotOrBAC

Para que os administradores possam definir facilmente uma politica de segurança baseada no modelo OrBAC, foi desenvolvido o protótipo MotOrBAC. A arquitetura do MotOrBAC é apresentada na figura 1. Este protótipo é composto de quatro módulos: (1) analisar a coerência da política, (2) a salvaguarda de dados (em XML ou Prolog), (3) o módulo de comunicação e (4) a interface gráfica (figura 2).

O protótipo MotOrBAC assegura cinco funcionalidades:

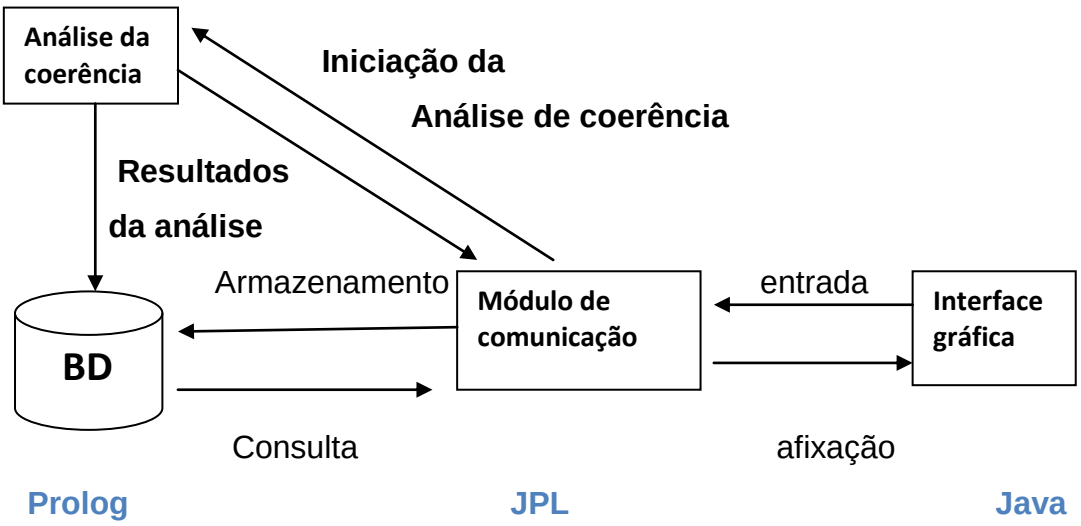


Fig.1: Arquitetura do MotOrBAC

● Entrada de uma politica de segurança: o administrador pode introduzir com MotOrBAC as diferentes entidades específicas no SI com o qual gera a segurança (organizações e sub-organizações, papéis, atividades, visões e contextos) e as regras de segurança associadas (ver seção 3).

●Simulação da política: o MotOrBAC permite simular a política entrando com os sujeitos, ações e objetos da organização e derivando automaticamente a política no nível concreto à partir da política organizacional introduzida por administradores. Os sujeitos, ações, e objetos são caracterizados por atributos (ver seção 4).

●Verificação da coerência da política de segurança : o MotOrBAC permite detectar os conflitos no nível concreto ou abstrato da política de segurança especificada pelo administrador (ver seção 5.1).

●Resolução de conflitos: uma vez os conflitos detectados, o MotOrBAC integra as estratégias de resolução de conflitos que se aplicam a política de segurança introduzidas pelo administrador para restabelecer a coerência (ver a seção 5.2).

●Gestão de direitos de gerenciamento: o MotOrBAC permite especificar os direitos que fornecem a um sujeito, atribuído a um papel administrativo, a possibilidade de gerar tudo ou parte de uma política de segurança OrBAC (ver seção 6).

3 Especificação de uma política de segurança

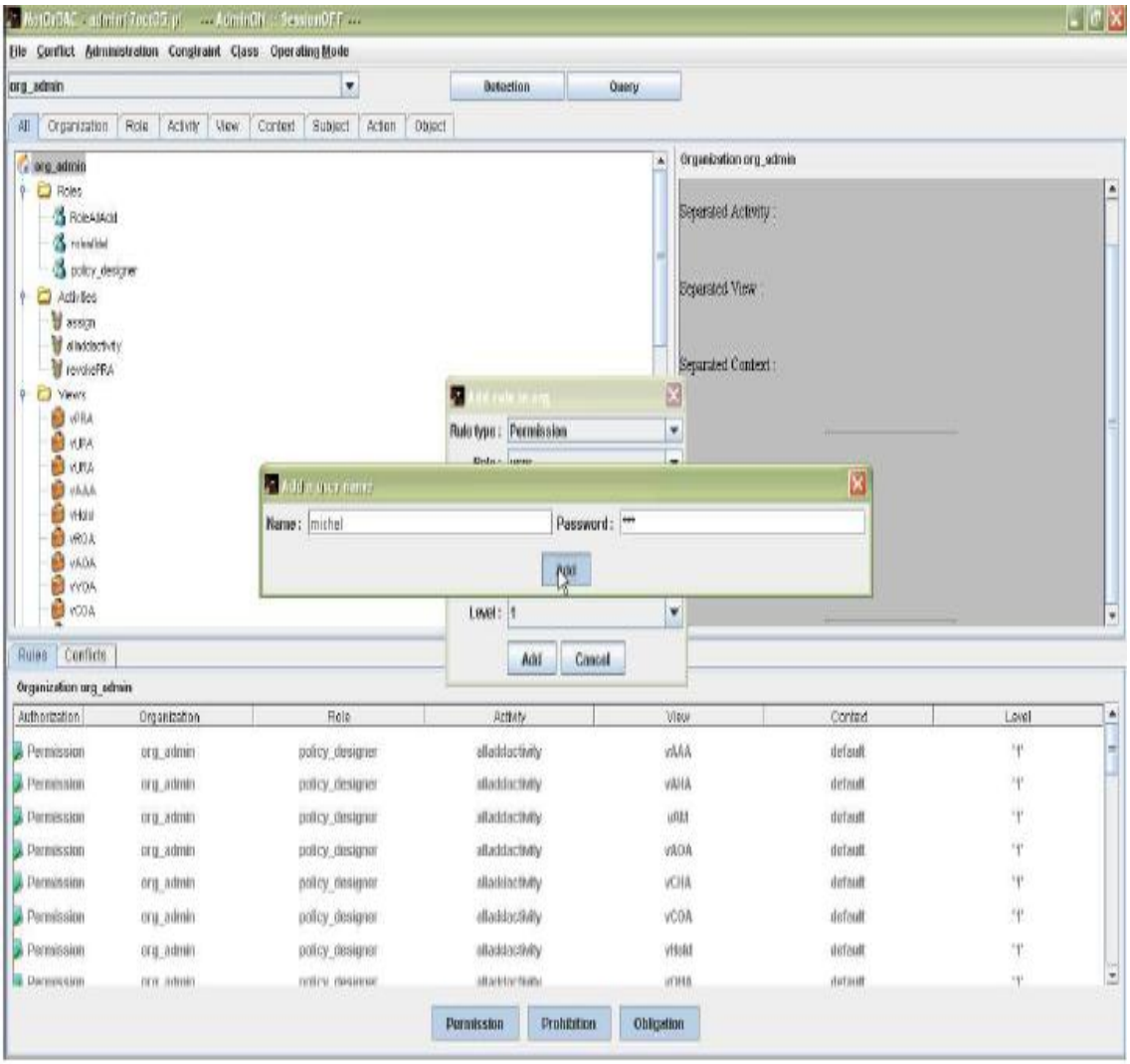
3.1 As entidades organizacionais do OrBAC no MotOrBAC

Quando um administrador designado deseja definir uma politica de segurança de uma organização, o MotOrBAC vai , a principio, demandar aos administradores introduzir o nome desta organização. Este administrador pode , posteriormente, definir várias sub-organizações. Esta conduz a inserção na politica de segurança de fatos da seguinte forma:

- sub_organization (org1,org2): org1 é uma sub-organização de org2.

Logo, o administrador tem a escolha de visualizar unicamente a política de segurança ligada a uma sub-organização ou a uma organização e a todas as suas sub-organizações graças a um menu deslizante [40].

O administrador pode, em seguida, definir para cada organização, os diferentes papéis, atividades e visões, bem como, os contextos. Desta forma, para criar um papel via MotOrBAC, o *Role* previsto para este efeito permite resignar o nome do papel bem como as relações de herança existentes entre este papel e outros papéis já definidos. Por exemplo, supõe-se que o administrador cria, na organização *hospital,* o papel *head_nurse*



[40] No trecho *l'administrateur a alors le choix de visualiser uniquement la politique de sécurité liée à une sousorganisation ou à une organisation et à toutes ses sous-organisations grâce à un menu déroulant,* a expressão *menu déroulant* foi traduzida para *menu deslizante ,* um termo equivalente ao termo em francês e que representa os menus que ao se passar o mouse apresentam seu conteúdo.

Fig.2: Interface MotOrBAC

e especifica que este papel é hierarquicamente superior ao papel *nurse.* Este conduz a inserção na politica de segurança as seguintes expressões:

- use (hospital, head_nurse, role): a organização *hospital* utiliza *head_nurse* na visão *role.*[41]
- senior_role(hospital, head_nurse, nurse): na organização *hospital,* o papel *head_nurse* é hierarquicamente superior a função *nurse.*

Após a criação de entidades organizacionais, é possível, também, definir *restrições* que devem respeitar estas entidades. Toda atualização da política de segurança que viola uma dessas restrições é rejeitada. No OrBAC, uma restrição é modelada por uma regra que deriva de um predicativo error de aridade 0. Certas restrições como a separação de papel tem um formato genérico predefinido no OrBAC. Esta restrição utiliza o predicativo *separated_role* da aridade 4 e corresponde à regra seguinte:

error: -

separated_role (Org1, Role1, Org2, Role2),

empower(Org1, Subject, Role1),

empower(Org2, Subject, Role2).

Esta regra especifica que se uma regra de separação de papeis existe entre *role1* e *role2* nas organizações *org1* e *org2,* então nenhum sujeito *Subject* pode ser simultaneamente afetado no papel *Role1* na organização *Org1* e no papel *Role2* na organização *Org2.*

O MotOrBAC permite especificar simplesmente este tipo de restrição de separação entre papeis. Estas restrições de separação similares podem ser especificadas pelas visões, atividades e contextos. A definição de outros tipos de restrição é possível no MotOrBAC conhecendo-se uma expressão Prolog que define a regra correspondente a restrição.

Por fim, o MotOrBAC oferece naturalmente ao administrador um menu permitindo criar regras de segurança. Uma regra de segurança é definida na organização especificada (selecionada em um menu deslizante), para um tipo

[41] O modelo OrBAC inclui quatro visões pré-definidas *role, activity, view e contexto* que permitem respectivamente gerar as funções, atividades, visões e contextos de cada organização.*

de privilégio (permissão, proibição, obrigação). Esta regra se aplica a um papel, uma atividade, uma visão e um contexto de organização comum e possui um nível de prioridade. Este nível de prioridade associado a cada regra de segurança é utilizado para gerar os eventuais conflitos entre regras (ver seção 5 abaixo). Por exemplo, pode-se definir a regra de segurança seguinte:

Permission (hospital, nurse, consult, medical_record, urgency,1).

Esta regra especifica que, em uma organização *hospital,* a permissão concede aos enfermeiros o poder de consultar os dossiês médicos em um contexto de urgência, em um nível de prioridade igual a 1.

A interface (fig.2) permite igualmente visualizar todas as entidades organizacionais (papel, atividade, visão , contexto...) bem como as informações que lhes concernem (privilégios, entidades concretas atribuídas,...).

3.2 Herança

Para gerar mais facilmente sub-organizações, automatizando a derivação de privilégios, o OrBAC permite definir hierarquias de papéis, atividades, visões e contextos [CCBM04]. As entidades nos níveis altos da hierarquia herdam privilégios de entidades hierarquicamente inferiores. O MotOrBAC permite introduzir facilmente relações de herança, demandando sistematicamente face a criação de uma entidade abstrata se o administrador deseja fazer uma sub-entidade de uma outra entidade. Em caso afirmativo, o administrador pode fazer uma chamada ao menu deslizante que o propõe as entidades as quais pode associar uma relação de hierarquia com a entidade que deseja criar.

Há quatro mecanismos de herança no OrBAC:

A herança de privilégios ligada à hierarquia de entidades abstratas: em uma mesma organização, se uma regra de segurança se aplica a uma entidade abstrata (papel, atividade ou visão), então suas sub-entidades (respectivamente sub-função, sub-atividade ou sub-visão) herdam estas regras de segurança. Por exemplo, a herança das permissões na hierarquia de papeis corresponde à regra seguinte:

```
permission (Org, Senior role, Activity, View, Context, Priority) :-
permission(Org, Junior role, Activity, View, Context, Priority),
    senior role (Org, Senior_role, Junior_role).
```

A herança das restrições de separação : as restrições de separação são herdadas através das hierarquias de entidades abstratas bem como da herança de privilégios.

A herança de privilégios ligados à hierarquia da organização: as organizações herdam privilégios através da herança das organizações se os papéis, atividades, visões e contextos contidos nas regras de segurança são definidos nessas organizações. Supõe-se que uma regra de segurança *r* é associada a uma organização *org* e que seja definida uma sub-organização *sorg* de *org. Sorg* herda *r* se a função, a atividade, a visão e o contexto implicado na *r* são definidos na *Sorg:*

permission (Sorg, Role, Activity, View, Context, Priority) :-
    sub organization (Sorg, Org),
    use(Sorg, Role, role),
    use(Sorg, Activity, activity),
    use(Sorg, View, view),
    use(Sorg, Context, context),
permission (Org, Role, Activity, View, Context, Priority).

A herança da definição dos contextos: se um contexto é definido em uma organização e esta organização possui uma sub-organização, a sub-organização herda da definição do contexto, salvo menção explicita em contrário.

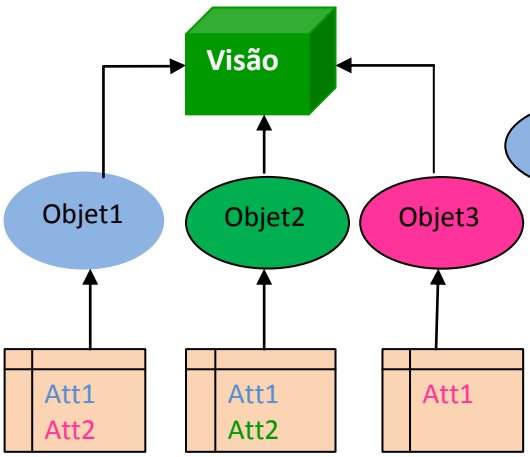


Fig. 3: Visões e atributos

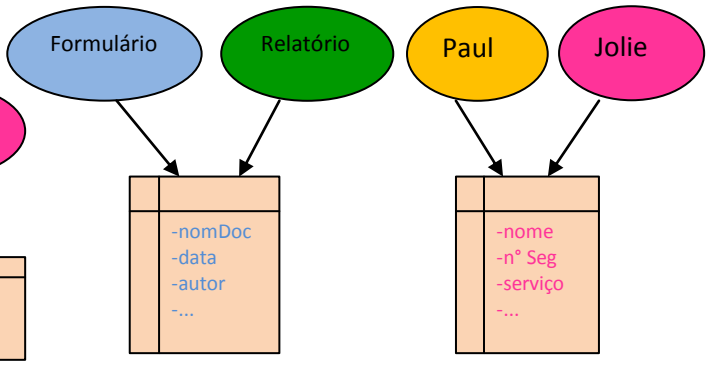


Fig. 4: Classes e Atributos

4 Simulação

4.1 Criação de entidades concretas

Para poder simular uma politica de segurança no nível concreto, convém introduzir, no MotOrBAC, as entidades concretas do modelo OrBAC. Para tanto, adotou-se uma abordagem orientada a objeto.

No formalismo lógico do modelo OrBAC, os atributos são representados por predicativos binários. Por exemplo, a expressão[42] *age(S1,20),* mostra que *s1* possui um atributo *age* que tem como valor o número 20.Os objetos pertencem às classes, o que é representado utilizando-se o predicativo binário *class.* Por exemplo, a expressão *class(s1,student),* indica que *s1* pertence a classe *student.*

Os sujeitos e as ações correspondem, de fato, a duas sub-classes particulares de objetos. Os sujeitos são entidades ativas que podem realizar ações em outros objetos. As ações são programas concretos que se pode ver como métodos, mas são opcionais no modelo OrBAC. As organizações do modelo são também objetos. Elas possuem, pois, atributos e pertencem a classes, por exemplo, a classe dos hospitais.

Utilizando-se a interface do MotOrBAC, um usuário pode criar novos objetos, especificar a classe a que pertence estes objetos e informar seus diferentes atributos. O usuário pode, em seguida, atribuir uma entidade concreta a uma entidade organizacional. Para isso, deve-se selecionar uma organização e atribuir um objeto a uma visão, respectivamente, um sujeito a uma função; ou uma ação a uma atividade. Se a politica de segurança da organização considerada autoriza esta atribuição, então uma nova instancia do predicativo *use* , *empower* ou *consider* será inserida nesta.

É importante ressaltar que[43] o conceito de visão do modelo OrBAC é diferente do conceito de classe. Um classe é um conceito taxonômico utilizado para reestruturar a descrição dos objetos enquanto que uma visão é um conceito organizacional que serve para estruturar uma especificação da política de segurança. Pode-se, igualmente, ressaltar que os objetos atribuídos a uma visão podem ter atributos diferentes (figura 3), enquanto que estes que pertencem a

[42] No trecho *par exemple, le fait age(s1,20). exprime que s1 a un attribut age qui a pour valeur 20.;* o termo fait mostrou-se problemático, já que a tradução literal (fato) não se enquadra neste contexto. Por isso, optou-se pelo equivalente *expressão* haja vista que o autor do texto de partida se refere às expressões lógicas do programa, tais como class(s1,student) e *age(s1,20).*

[43] No trecho *Il faut insister sur le fait que le concept de vue du mod`ele OrBAC est distinct de celui de class,* o termo *Il faut insister sur* pode ser traduzido por Deve-se acentuar que, deve-se sublinhar que, deve-se dar ênfase à. No entanto, nenhum dos termos são usuais na área de conhecimento em questão, por isso optou-se pelo termo equivalente É importante ressaltar que.

uma classe possuem os mesmos atributos, apenas seus valores diferem (figura 4).

No entanto, uma classe pode ser utilizada como uma visão organizacional se esta especifica a a política de segurança. Um objeto pode pertencer a uma classe sem ser utilizado por uma organização na visão correspondente. Por exemplo, se *dossier_medical* é , ao mesmo tempo, uma classe e uma visão, então certos objetos desta classe podem ser utilizados em uma organização *purpan*[44]*_hospital* mas não em uma organização *rangueil*[45]*_hospital.* Além disso, várias organizações podem, em certos casos, compartilhar objetos na mesma visão ou em visões diferentes. De forma similar, um mesmo sujeito pode ser atribuído, em várias organizações, a papéis diferentes.

A interface do MotOrBAC permite gerar estas diferentes situações.

4.2 *Derivação de privilégios concretos*

Uma vez que as entidades concretas são definidas no MotOrBAC, pode-se aplicar a política de segurança organizacional nas entidades concretas para derivar se tal sujeito possui a permissão de realizar tal ação em tal objeto.

Para tanto, foi introduzido o predicativo *is_permitted* de aridade 4 e aplicou-se o principio geral da derivação das permissões concretas:

```
Is_permitted( Subject, Action, Object, Priority) : -
    permission(Org,Role,Activity,View,Context,Priority),
    empower(Org,Subject,Role),
    consider(Org,Action,Activity), use(Org,Object,View),
    hold(Org,Subject,Action,Object,Context).
```

Esta regra especifica que em uma certa organização se (1) uma permissão existe para um papel, uma atividade e uma visão em um certo contexto, (2) um sujeito é habilitado para este papel, (3) uma ação implementa esta atividade, (4) um objeto é utilizado nesta visão e (5) este contexto é ativo para este sujeito, esta ação e esta visão, então este possui uma permissão concreta para realizar esta ação neste objeto. Esta permissão concreta possui o mesmo nível de prioridade que a permissão organizacional que a permitiu derivar.

[44] Purpan é um bairro em Toulouse.
[45] Rangueil é um bairro residencial de Toulouse.

Regras similares permitem derivar as interdições e obrigações no nível concreto. Um administrador pode requerer que o MotOrBAC aplique estas regras para conhecer um conjunto de privilégios deriváveis no nível concreto. Utilizando-se a interface, o administrador pode igualmente formular um requerimento lógico para conhecer um conjunto de privilégios que se aplicam às entidades (sujeitos, ações e objetos) que satisfazem o este requerimento

O nível de prioridade associado a um privilégio derivado permite solucionar eventuais conflitos entre permissão e proibição por um lado e obrigação e proibição por outro lado. Este permite testar a presença de conflitos no nível concreto tendo em vista o conjunto de entidades concretas consideradas e verificar se estes conflitos podem ser resolvidos aplicando-se os níveis de prioridade.

No entanto, é possível que a criação de novas entidades concretas gerem novos conflitos que não possam ser resolvidos. Esta é a razão pela qual propõe-se, na seção 5, uma abordagem para resolver os conflitos no nível organizacional. O objetivo desta abordagem é poder garantir que não exista conflito no nível organizacional, consequentemente este não poderá existir no nível concreto.

5 Análise

5.1 Os conflitos no OrBAC

A função de simulação descrita na seção anterior permite destacar os conflitos no nível concreto. Nesta seção, é apresentada outra função ofertada pelo MotOrBAC para analisar os conflitos no nível organizacional. Para detectar estes conflitos, será introduzido, a princípio, o predicativo de aridade 0 *conflit.* A presença de conflitos é detectada em seguida, aplicando-se a seguinte regra:

```
conflit :-
permission(Org1,Role1,Activity1,View1,Context1,Priority1),
prohibition(Org2,Role2,Activity2,View2,Context2,Priority2),
not (separated role(Org1,Role1,Org2,Role2)),
not (separated activity(Org1,Activity1,Org2,Activity2)),
not (separated view(Org1,View1,Org2,View2)),
not (separated context(Org1,Context1,Org2,Context2)),
not (Priority1 < Priotity2),
```

not (Priority2 < Priotity1).

Esta regra indica que se (1) uma permissão e uma proibição organizacionais existem nas organizações Org1 e Org2, (2) não há imposições de separação entre os papéis, atividades, visões e contextos e (3) as prioridades associadas respectivamente à permissão e à proibição não são comparáveis, de forma que um conflito é derivado.

De fato, se esta situação ocorre, é possível atribuir, simultaneamente, a um sujeito dois papéis *Role1* e *Role2*(o mesmo pode acontecer ao atribuir[46] para uma ação as atividades *activity1* e *activity2* e um objeto às visões *view1* e *view2)* ; e derivar uma permissão e uma interdição conflitual no nível concreto aplicando-se o principio geral da derivação de privilégios apresentados na seção 4.2. Pode-se notar que este conflito no nível concreto é somente *potentiel* na medida em que o sujeito, a ação e o objeto possam gerar o conflito que talvez não exista no nível concreto.

Uma regra similar à regra abaixo, permite detectar os conflitos entre as interdições e as obrigações.

Quando não é possível derivar o predicativo *conflit* , diz-se que a política de segurança é *coerente.* O interessante desta abordagem de detecção de conflitos no nível organizacional é o seguinte: uma vez que a política organizacional é coerente, o usuário pode atribuir entidades concretas a entidades abstratas sem risco de introduzir conflito no nível concreto. De fato, pode-se demonstrar que se não existe conflito no nível organizacional, então não existirá no nível concreto [CCB05].

Utilizando-se a função de detecção do MotOrBAC, o usuário pode, graças à uma opção, requisitar a visualização tanto dos conflitos organizacionais quanto dos concretos.

5.2 *Resolução de conflitos no MotOrBAC*

[46] No trecho il est possible d'affecter un sujet simultan´ement aux rˆoles Role1 et Role2 (idem pour une action aux activit´es Activity1 et de Activity2 et un objet aux vues View1 et de View2) optou-se por acrescentar o termo atribuir no parênteses tornar o texto de chegada mais claro para os leitores.

Supõe-se que um ou vários conflitos apareçam no nível da política de segurança organizacional. O usuário deve, primeiramente, identificar estes conflitos. Uma vez que o problema foi identificado, o usuário possui[47] várias soluções:

Modificar uma das regras conflituais – O usuário pode considerar que o conflito detectado é devido a um erro na especificação da política. Neste caso, pode-se atualizar a política modificando uma das regras conflituais.

Acrescentar uma ou várias restrições de separação: o usuário pode acrescentar restrições[48] de separação. Por exemplo, introduzindo-se uma restrição de separação entre os papéis *nurse* e *physician,* tem-se a segurança de que os privilégios destes dois papéis não podem mais entrar em conflito.

Modificar o nível de prioridade de uma das regras conflituais: Mudar o nível de prioridade de uma regra é uma forma simples de resolver o conflito. Entretanto, deve-se assegurar que esta modificação não tenha como consequência tornar uma das regras redundantes ou inaplicáveis. O problema das regras redundantes não foi desenvolvido neste artigo. Trata-se de um problema complexo e reporta-se à [CCBGA05] aonde é definido um algoritmo para detectar este tipo de anomalia em uma política de segurança de rede.

Ignorar o conflito: O usuário pode simplesmente ignorar o conflito. No entanto, todo o conflito não resolvido no nível organizacional pode gerar conflitos no nível concreto.

6 AdOrBAC

6.1 *Administração por visão*

[49]Um modelo de controle de acesso é geralmente constituído de duas partes distintas: um modelo para representar uma política de autorização e um modelo de administração desta política. O modelo de administração permite especificar quem possui privilégios para atualizar a política de autorização e sob quais condições. Por exemplo, o modelo ARBAC [SBM97, SM99] foi definido para administrar o modelo de controle de acesso RBAC [SCFY96, FSG+01].

---

[47] Uma opção de tradução para o termo *a* (verbo avoir) do trecho *l'utilisateur a plusieurs solutions* é o termo *possuir* que foi adotado na tradução para manter o caráter formal do texto.

[48] Outra opção seria limitação , mas optou-se por restrição por ser um termo mais utilizado nesta área de conhecimento.

[49] Optou-se por manter o não espaçamento nos primeiros parágrafos de cada sessão a fim de manter o estilo do texto de partida.

O modelo OrBAC possui, igualmente, seu modelo de administração: o modelo AdOrBAC [CM04a]. Este[50] permite especificar uma política de administração no mesmo formalismo lógico e utilizando-se os mesmos conceitos que aqueles introduzidos para definir o modelo OrBAC. Desta forma, o[51] AdOrBAC faz do modelo OrBAC um modelo *auto-gerenciável*[52]**.** O princípio da base do modelo AdOrBAC é considerar que todas as operações da administração da política de segurança devem ser realizadas gerando, ou seja, criando, modificando ou suprimindo, objetos particulares chamados objetos da administração. A estrutura da política de gerenciamento consiste em especificar quem possui privilégios para gerar estes objetos do gerenciamento.

Para estar em conformidade com o modelo OrBAC, os objetos da administração são reagrupados em diferentes visões (figura 5). Como no OrBAC, os objetos atribuídos a estas visões são especificados utilizando o predicativo *use.* O AdOrBAC permite administrar as seguintes atividades : (1) gestão de permissões (pra); (2) gestão de atribuições de papéis aos sujeitos e das atividades às ações (*ura, aaa*); (3) gestão de hierarquias de entidades organizacionais (*rha,aha,vha,oha,cha*); (4) gestão de definições de contextos (*hold).*A gestão de privilégios será estudada via visão *pra* na seção seguinte[53]. As outras funções da administração são apresentadas em [CM04a].

Gestão de privilégios

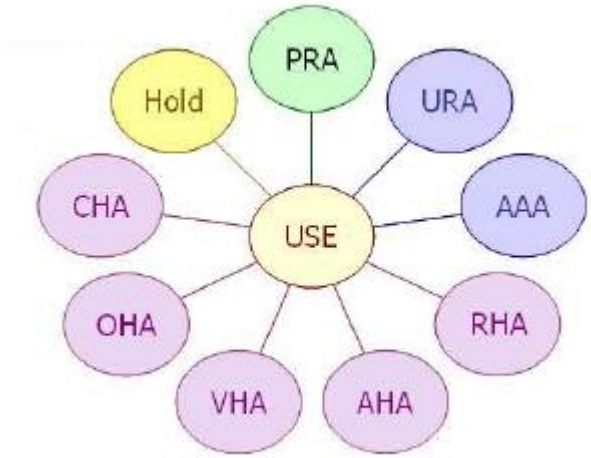
[50] O termo AdOrBAC do trecho *AdOrBAC permet de sp´ecifier une politique d'administration dans le mˆeme formalisme logique et em utilisant les mˆemes concepts que ceux introduits pour d´efinir le mod`ele OrBAC* foi substituído pelo termo *este*, afim de evitar repetição.

[51] Em francês , não é usual utilizar o artigo antes de nomes próprios, mas em português isso é usual, por isso realizou-se a inserção do termo *o* em frente ao AdOrBAC no trecho *AdOrBAC permet de sp´ecifier une politique d'administration dans le mˆeme formalisme logique et em utilisant les mˆemes concepts que ceux introduits pour d´efinir le mod`ele OrBAC.*

[52] A expressão auto-gerenciável desta área de conhecimento é mais usual que a tradução literal auto-administravel do *trecho AdOrBAC fait donc du modèle OrBAC un mod`ele auto-administré*, por isso a escolha.

[53] A inversão foi feita a fim de manter a impessoalidade do texto.

Gestão de contextos



Gestão de abstrações

Gestão de hierarquias

Fig.5: Visões de gerenciamento

6.2 Gestão de privilégios

A visão *pra (*Permission Role Assignement) permite gerenciar as atribuições de privilégios aos papéis. Esta visão é , também, uma classe munida de atributos permitindo descrever os diferentes parâmetros de um privilégio. Desta forma, define-se os atributos seguintes para a classe *pra:* (1) *type (*tipo de privilégio *{permission,prohibition,obligationg}), (2) authority (* a organização na qual se aplica o privilégio*), (3) grantee (*o papel que possui o privilégio), *(3) grantee (* a atividade que poderá ser realizada quando o privilégio é utilizado). (5) *target* (a visão que contém o privilégio), (6) *contexto* (o contexto de utilização do privilégio) e (7) *level (*o nível de prioridade associado ao privilégio e que é utilizado para resolver os conflitos).

A inserção de um novo objeto na visão *pra* é interpretado como a criação de um novo privilégio. Para isso, foi definida uma regra a fim de derivar automaticamente uma permissão a partir de objetos atribuídos à visão *pra* e tendo *permission* como valor para o atributo *type:*

permission(Auth,Role,Activity,View,Context,Priority) :-
use(Org,ObjAdmin,pra),

type(ObjAdmin,permission),
authority(ObjAdmin,Auth),
grantee(ObjAdmin,Role),
privilege(ObjAdmin,Activity), target(ObjAdmin,View),
context(ObjAdmin,Context), level(ObjAdmin,Priority),
sub organization(Org,Auth).

Pode-se notar nesta regra que um objeto de gerenciamento que pertence à visão *pra* é interpretado como uma permissão que se a organização *Auth* aparece no atributo *authority* é uma sub-organização da organização *Org* que utiliza este objeto gerenciável. Esta restrição é chamada de *princípio de confinamento hierárquico* e dispõe que uma organização pode controlar apenas a política de segurança de uma de suas sub-organizações.

Duas outras regras similares à regra apresentada acima, permitem derivar proibições e obrigações quando um objeto que pertence a visão *pra* possui um valor de atributo *type* igual à *prohibition* ou *obligation.*

6.3 AdOrBAC no MotOrBAC

O MotOrBAC abrange uma função de gerenciamento ao implantar o modelo AdOrBAC. Uma vez autenticado pelo MotOrBAC, um usuário tendo privilégios de gerenciamento, ou seja, tendo a permissão para criar objetos que pertencem às visões de gerenciamento do modelo AdOrBAC, pode, desta forma , criar uma política de segurança correspondente ao modelo OrBAC. No [CM04a], foi mostrado que a presente abordagem permite modelar uma política de gerenciamento distribuída entre vários administradores tendo cada um privilégios de gerenciamento restritos. Pode-se , assim, partir da hipótese que o super administrador único acumula todos os direitos de gerenciamento. Pode-se, igualmente, especificar políticas de gerenciamento flexíveis, por exemplo, uma política que fornece privilégios de gerenciamento sob certas condições (por um dia ou quando o administrador titular estiver ausente).

Uma vez que a política de gerenciamento da organização é definida, esta politica é aplicada para controlar as ações efetuadas pelos usuários do MotOrBAC. Desta forma, cada vez que um usuário do MotOrBAC tentar executar uma ação (por

exemplo, inserir um objeto na visão *pra* para criar uma nova permissão), a política de gerenciamento é aplicado para verificar se o usuário possui efetivamente a permissão de criar este objeto. Se este não é o caso, a tentativa de criação será rejeitada.

7 Conclusão

Este artigo mostrou que é possível fornecer aos administradores de segurança os meios de especificar de forma fácil sua política de segurança e de ter o controle: (1) um modelo de segurança estruturado em torno de entidades organizacionais as quais o administrador é rapidamente familiarizado (organização, papel, atividade, visão, contexto), (2) uma separação clara entre o nível organizacional e o nível concreto (sujeito, ação, objeto), (3) um modelo de privilégios abundantes incluindo permissão, interdição e obrigação, (4) uma ferramenta de simulação , de visualização e de análise da política , (3) uma automatização da detecção e da resolução de conflitos eventuais e (5) uma administração descentralizada da política de segurança. O administrador pode introduzir sua política de segurança com o MotOrBAC diretamente a partir da expressão desta política no modelo OrBAC. O administrador pode especificar de forma natural as entidades manipuladas neste modelo, caso essas sejam intuitivas[54]. Os enriquecimentos trazidos no modelo OrBAC de base são ,igualmente, considerados no protótipo MotOrBAC. Desta forma, o administrador pode afinar sua política de segurança e otimizar sua gestão por meio da introdução de diferentes hierarquias de entidades OrBAC ,assim como restrições que regem as diferentes atribuições de entidades organizacionais. As entidades concretas são descritas utilizando-se uma abordagem orientada a objetos que possa atribuir às entidades organizacionais adequadas. Todas as entidades (organizacional ou concreta) e todas as relações (atribuição, hierarquia, privilégio, restrição) associadas a essas entidades introduzidas utilizando-se a interface gráfica do MotOrBAC, se traduzem por inserções no banco de expressões; e, o banco de regras descreve a política de segurança. Enfim, o gerenciamento da política de

[54] Na tradução do trecho Les entités manipulés dans ce modèle étant assez intuitives, il devrait pouvoir les spécifier de facon naturelle, teve de se inverter a frase para respeitar o sentido do texto de partida , ficando da seguinte forma *O administrador pode especificar de forma natural as entidades manipuladas neste modelo, caso essas sejam intuitivas*

segurança, conhecido por ser um grande quebra-cabeça é, também, uma das funcionalidades ofertadas pelo protótipo. No meio de uma utilização combinada dos conceitos de visão OrBAC e do objeto, a atribuição de um privilégio de gerenciamento consiste na atribuição de um *privilegio de um objeto a visão de gerenciamento adequada.* Uma vez que o modelo implantado no protótipo é auto-gerenciável, a gestão desses direitos de gerenciamento é , então, feita da mesma forma como na gestão de toda politica de segurança OrBAC. No MotOrBAC, o gerenciamento não é necessariamente confiado a um só sujeito. Os privilégios dos diferentes sujeitos atribuídos a um papel de administrador são ativados depois da identificação/autenticação no nível da interface gráfica.

A definição de uma política de segurança dedicada, tal como uma política de segurança de redes que se traduz pela derivação de regras genéricas de configuração de um firewall, foi , também, considerada. Baseado nos trabalhos que foram conduzidos no [CCBSM04], uma primeira versão experimental foi implantada no MotOrBAC.

A consideração sobre delegação não foi descrita neste artigo em razão da falta de lugar disponível. Ela é particularmente gerenciada no protótipo como um privilégio de gerenciamento e consiste em atribuir um objeto à uma visão particular de delegação, abordagem que foi adotada pela gestão do privilégio de gerenciamento. O objeto em questão (o ticket) contem características da delegação, em particular: (1) a autoridade que delega, (2) o beneficiário desta delegação, (3) o privilégio acordado pelo viés desta delegação e (4) seu contexto de aplicação.

MotOrBAC gerencia , também, diferentes funcionalidades permitindo definir uma política de segurança coerente. Vários enriquecimentos do protótipo são previstos, em particular, implantar uma larga variedade de contextos [CM03] e completar os trabalhos efetuados no contexto de uma política voltada para redes no processo de implantação da política em outros componentes que compõe a segurança.

Texto 3

CryptoPage-1: Em direção[55] ao fim da pirataria na informática?

Resumo

A fim de ajudar a resolver os problemas da pirataria na informática e as necessidades de confidencialidade nas aplicações e comunicações modernas, este artigo apresenta uma técnica material permitindo aliar um ciframento forte a um processador. Este mecanismo associado aos caches e a gestão de memória permite cifrar instruções do programa bem como os dados na memória para assegurar uma boa resistência aos ataques no barramento do processador. Esta permite conceder , por exemplo, programas capazes de rodar apenas em uma única máquina no mundo, assegurando, desta forma, a confidencialidade da aplicação e das comunicações.

1 Introdução

Com o desenvolvimento das mídias de alta capacidade e baratas[56]; tais como os CD-ROM e DVD-ROM, a difusão de softwares e de conteúdos artísticos como os filmes ou músicas, entrou-se em uma era de difusão em massa: o custo baixo da reprodução do conteúdo numérico, que consiste em recopiar uma sequencia de 0 e 1, esquiva das leis econômicas clássicas de produção na medida em que o custo é concentrado na confecção do original e não mais na produção de cópias vendidas.

O aparecimento de redes mundiais em grande escala de tipo Internet traz outro tipo de distribuição de softwares ou de conteúdos artísticos, no qual cada um pode comprar uma cópia e a baixar diretamente em seu computador.

Infelizmente, o desenvolvimento de versões graváveis destas mídias e ,mais geralmente, do baixo preço dos discos rígidos de mega bits; permitem, também, o desenvolvimento de utilizações muito além do uso de um objetivo de cópia privada de salvaguarda... Este uso ilegal é também auxiliado pela possibilidade que a internet oferece de disseminar mundialmente todo tipo de informação numérica.

---

[55] Na tradução do título *CryptoPage-1 : vers la fin du piratage informatique? ,* haviam várias opções para a tradução do termo vers que se encaixavam no contexto, dentre elas: próxima ao fim, perto do fim e em direção ao fim. A opção por em direção ao fim, por soar melhor neste contexto.

[56] No trecho *Avec le développement de médias de forte capacité et peu chers*, optou-se por adotar um termo equivalente ao *peu chers* já que nesta área de conhecimento a tradução literal(pouco caro) não é usual. Portanto, adotou-se o termo *barata.*

Outra problemática é a segurança informática e a necessidade de se ter sistemas resistentes aos ataques informáticos[57] , mas também aos ataques físicos de um sistema sensível, tal como a manipulação de barramentos dos sistemas de um computador, ligações de comunicação, etc. Menos conhecido pelo público em geral, estes sistemas nos quais as intrusões são evitadas , são utilizadas todos os dias: nos bancos, nos caixas eletrônicos, no comércio eletrônico, ou ainda nos sistemas confidenciais de defesa, e de maneira mais geral, nas telecomunicações.

Este artigo pode ser obtido no http://www.cri.ensmp.fr/~keryell/articles_et_programmes.html#ENSTBr_INFO_2001-001 e uma versão mais completa no http://www.cri.ensmp.fr/~keryell/articles_et_programmes.html#ENSTBr_INFO_2000-001.

2 Princípios do sistema

O primeiro problema pode ser resolvido especializando cada computador a ponto que um programa esteja rodando apenas em uma máquina [58] no mundo. A técnica utilizável é o uso da criptografia de chave pública e chave secreta [8] no coração[59] do microprocessador. É a técnica utilizada nos cartões inteligentes. No entanto, no caso de um computador genérico, o principio é mais difícil de implementar, pois há elementos periféricos que são espionáveis (ao contrário de um cartão inteligente que é um computador completo): os barramentos são espionáveis e seus estados são modificáveis, bem como as entradas e saídas , dentre outros. Apesar de complicados, tais ataques são possíveis e uma vez que o software é exposto, seu conteúdo pode ser replicado por hackers[60].

---

[57] No trecho *Une autre problématique est celle de la sécurité informatique et la nécessité d'avoir des systèmes résistants aux attaques informatiques bien sûr mais aussi aux attaques physiques d'un système sensible ,* optou-se pela retirada do termo *bien sûr* a fim de manter o caráter formal do texto.

[58] No trecho *le premier problème peut être résolu en spécialisant chaque ordinateur au point qu'un programme ne peut plus tourner que sur un seul ordinateur unique au monde.*, optou-se pelo uso do sinônimo do termo ordinateur que é *máquina ,*para evitar repetição do mesmo na frase.

[59] No trecho *La technique utilisable est l'usage de la cryptographie à clé publique et clé secrète [8] au sein même du microprocesseur*, utilizou-se o termo no coração do como tradução do termo au sein du *,* por ser mais usual nesta área de conhecimento.

[60] Como no Brasil adota-se o termo em inglês hacker , optou-se por utiliz-lo como tradução ao termo pirate do trecho *Bien que compliquées, de telles attaques sont possibles et une fois le logiciel mis à nu son contenu peut être répliqué par des pirates..*

Na sequencia deste artigo serão apresentadas as técnicas que buscam evitar este tipo de ataque cifrando e assinando eletronicamente todos os fluxos de informação que entram e saem do microprocessador, a fim de resolver o segundo problema.

2.1 Criptografia

A abordagem é esquematizada como um todo na figura 1. O princípio é cifrar o acesso à memória no barramento *D* inserindo os operadores de ciframento C_d ($c_{2,}$ *a,d)* que depende dos endereços utilizados a fim de complicar o trabalho de um atacante. Para evitar os ataques no qual se faz a decriptografia pelo programa do seu próprio código e a sair em uma entrada - saída, utiliza-se duas chaves diferentes para as instruções e os dados.

Classicamente, por razões de desempenho, utiliza-se um algoritmo simétrico para a criptografia e as chaves são obtidas por decriptografia com a chave privada de um decodificador cifrado do software.

Para produzir um software para esta máquina, deve-se , pois, criptografar dados e código com duas chaves aleatórias e acompanhar o software com o decodificador contendo as duas chaves aleatórias, cifradas com a chave pública do processador.

Com esta abordagem , é quase certo que o código somente pode ser executado no processador alvo. Entretanto, é possível injetar instruções ou dados aleatórios no barramento para extrair informação no desenvolvimento do programa [7].

2.2 Assinatura digital

Para evitar este tipo de ataque, pode-se ou cifrar blocos de dados mais importantes de uma vez, tipo de linha de cache [7], ou acrescentar uma assinatura digital [8]. Nestes dois casos, o objetivo é realizar uma busca exaustiva[61] em um espaço muito mais vasto, o que é concretamente impossível.

[61] No trecho *Dans les deux cas le but est de devoir faire une recherche brute dans un espace beaucoup plus vaste et être concrètement impossible,* existem duas opções de tradução para o termo recherche brute: força bruta

Se a opção é por cifrar os blocos de dados ou instruções, toda injeção hacker de outros valores no barramento externo serão de forma bijetora[62] traduzidos por valores internos que alterarão a execução do programa.

Logo, é um método com assinatura eletrônica que preferimos. A ideia é associar todo valor *v* a um valor aberto para uma função criptográfica *h* tendo como propriedade que H^{-1} é muito difícil (praticamente impossível) de se calcular com as medidas atuais. No lugar de armazenar a memória $CD\ (c_s,a,d)$, armazena-se o valor criptografado da concatenação *de* v e de seu hash, ou seja, o dado assinado e cifrado $ds = C_d(c_s, a, (d, H(d)))$.

Diante da decriptografia de uma informação cifrada[63] *ds,* extrai-se (d', h'). Se o principio abaixo foi utilizado para o ciframento, deve-se encontrar a expressão $H(d'')=h''$, o que é suficiente para o cálculo de verificação. Se a propriedade não é verificada, é que se tenta decifrar os dados que não foram cifrados desta maneira. Se o tamanho do resultado de *h* é b_s bits, um hacker tem potencialmente uma oportunidade sobre 2^{bs} de injetar um valor que passará a verificação. Se, por exemplo, bs = 128, este possui uma oportunidade em 3,4, 10^{38} ,o que parece razoável para evitar ataques igualmente intensos no estado atual da tecnologia.

O problema com o sistema de assinatura é que se as informações são criptografadas por blocos de *b* bits e se a assinatura possui um tamanho de *b,* uma quantidade de *n* bits não criptografados internamente necessitará de ter ao menos $\lceil \frac{n}{b} \rceil (b + b_s)$ bits de memória externa na forma criptografada. Concretamente, se no nível de uma linha de cache de 32 octetos (seja 256 bits) é criptografado e se tem um resultado de hash de 128 bits, a ocupação da memória do programa aumenta 50% , o que é razoável.

O colorário é que vai precisar encontrar uma forma de armazenar esses b_s bits suplementares na memória. Pode-se escolher estocar os blocos cifrados de maneira continua ou ainda estocar os dados por blocos de *b* bits aos endereços

---

e busca exaustiva. Como ambos possuem o mesmo significado, e são usualmente encontrados na literatura desta área de conhecimento, optou-se pelo termo que mais se aproxima do original.

[62] Como não existe uma tradução para o termo *bijectivement* do trecho *Si on se contente de chiffrer des blocs de données ou d'instructions, toute injection pirate d'autres valeurs sur le bus externe seront bijectivement traduites par des valeurs internes qui perturberont l'exécution du programme.,* a solução encontrada foi traduzir por adaptar o termo para preservar o sentido do texto original.

[63] Outra opção seria *codificado*

virtuais internos e acrescentar os b_s bits suplementares em uma outra zona virtual à um endereço A_S+*a,* por exemplo.

Em um primeiro caso, um octeto criptografado no endereço virtual interno *a* se reencontrará em memória em um bloco de endereço virtual $[\lfloor \frac{a}{b} \rfloor \frac{b+b_s}{b}, \lfloor \frac{a}{b} + 1 \rfloor \frac{b+b_s}{b} - 1]$.É a tradução física a_{pl} deste endereço virtual linearizado a_1 que sairá na memória durante o acesso criptografado no lugar do endereço físico *ap clássico. Esta conversão pode estar integrada a* MMU do sistema.

No segundo caso, o octeto se encontrará em duas zonas $[\lfloor \frac{a}{b} \rfloor b, \lfloor \frac{a}{b} \rfloor b + b - 1]$ et $[A_S + \lfloor \frac{a}{b} \rfloor b_s, A_S + \lfloor \frac{a}{b} \rfloor b_s + b_s - 1]$. .Nos dois casos , é importante se atentar aos conflitos de endereço quando um programa manipulará, em um momento, os valores criptografados e os valores em claro na memória.

2.3 **Proteção e implantação**[64]

A fim de melhor resistir a um ataque tentando modificar de maneira interna o microprocessador, pode-se acrescentar procedimentos de testes rastreando-se todo a cifrador pelo decifrador [1] e verificar o resultado encontrado é o mesmo. Qualquer incoerência provocará a iniciação de um sistema de destruição pura e simples do processador.

Pode-se , também, expandir o sistema fazendo votar vários sistemas de criframento/deciframento. Desta forma, se o processador é submetido a ataques do tipo *glitch,* a variações de frequência do relógio impedido ou a tensão da alimentação, raios ionizantes, variações de temperatura, etc. Será muito provável que haverá comportamentos diferentes entre o cifrador/decifrador redundantes. Na medida em que o sistema visa os processadores modernos de mais de 10^7 ou 10^8 transistores, o custo da redundância é negligenciado.

Pelas mesmas razões, a chave privada do processador deve existir em vários exemplares em diferentes espaços do processador, a fim de dificultar as tentativas de modificação.

---

[64] Outra opção para o sub título *Sécurisation et mise en oeuvre* seria a sua forma no gerúndio *protegendo e implantando.*

Como o sistema deve poder começar um processo em modo criptografado, acrescenta-se uma instrução RTIEC permitindo iniciar um processo a partir de um decriptor de material criptografado com a chave pública do processador. Igualmente, quando um processador criptografado é interrompido , escreve-se o contexto material de execução em uma zona especial na forma cifrada com a chave simétrica dos dados a fim de que se possa, eventualmente , ser examinado ou modificado pelo próprio programa com as instruções de acesso à memória.

Em suma, o processo criptografado deve ser capaz de escrever e ler dados em claro. Desta forma, acrescenta-se ao processador as instruções STNC e LDNC, permitindo o acesso à memória sem passar pelos sistemas de criptografia.

O modo de intrusão JTAG e, mais geralmente, todo o modo de teste não devem poder ser utilizados em modo criptografado. Como se deve ajustar e em seguida testar o processador, também, em modo de criptografia, é preciso um sistema capaz de suprimir esta possibilidade, uma vez que o processador é testado logo após a sua fabricação; e que esta supressão não seja controlada por um simples bit que um cortador a laiser intrusivo poderá , por exemplo, o restabelecer.

3 Outros trabalhos da área e trabalhos futuros

As pesquisas sobre este tema na área são voltadas aos sistemas de pequeno porte [2, 3, 4, 5,6]; sobretudo aqueles direcionados a um processador genérico e um sistema operacional padrão, devem trabalhar com diferentes níveis de segurança. Não se conhece um estudo na área de sistemas operacionais para processadores, incluindo uma execução criptografada.

Existem outras abordagens tais como a alocação de procedimentos, por exemplo, mas esta necessita de requerer a um servidor distante regurlamente e esta técnica não resiste a plotagem do programa.

Na continuação deste artigo, deve-se focar em definir de forma mais detalhada a arquitetura do processador em via de uma realização, desenvolver um modelo de nível de segurança e completar o sistema com uma verificação global de coerência para evitar os ataques pela recuperação de blocos já cifrados.

5. Percurso metodológico

Neste capítulo, será descrita a definição e delimitação do glossário, bem como as etapas que envolveram a sua constituição.

Optou-se por trabalhar neste glossário com um *campo do saber* , ou seja, um discurso científico que se apresenta em constante transformação. Este campo é a Tecnologia da Informação, mais precisamente a Segurança da Informação.

Atualmente, a área de segurança da informação tornou-se complexa, uma vez que a informatização tem avançado de forma contínua e dinâmica. Como a sociedade atual depende de informações armazenadas em sistemas computacionais para tomar decisões de negócios ou de bem-estar social, a segurança dessas informações deve ser absoluta. (DIAS, 2001).

A rede de computadores é o fator que mais contribuiu para o aumento da preocupação em se proteger as informações de todo o tipo de dano ou roubo. E juntamente com este crescimento, aumentou também o acesso às informações e, consequentemente, as chances de se atacar os sistemas de informação.

Ferramentas que antes eram apenas utilizadas pelo governo e agências de inteligência, hoje se encontram disponíveis a qualquer pessoa.

Dias(2001) defende que a certo tempo atrás segurança da informação resumia-se em guardar documentos dentro de um cofre, e este, geralmente se localizava numa espécie de sala própria para este fim, da qual apenas uma ou poucas pessoas tinham acesso.

No entanto, para a autora nunca foi tão fácil atacar sistemas informatizados como nos dias de hoje, tendo em vista que os sistemas de informação institucionais estão conectados a redes externas. Neste sentido, a segurança da informação torna-se essencial para a sobrevivência das organização, pois as informações fazem parte do patrimônio de uma empresa e são críticas tanto para a concretização de negócios quanto para a tomada de decisões .

Este glossário será voltado para os especialistas e acadêmicos da área , buscando de forma atualizada, apresentar conceitos essenciais para a compreensão deste campo do saber.

Para a análise terminológica dos textos realizou-se os seguintes passos :

1) Elaboração de um mapa conceitual e das categorias temáticas, conforme dispõe Demai (2006);
2) Elaboração de fichas terminológicas, conforme Fromm (2005);
3) Elaboração do glossário.

5.1 Delimitação

O glossário da área de segurança da informação elaborado neste trabalho tem como principais características as seguintes:

GRANDE ÁREA DE	Generalidades. Ciência e

CONHECIMENTO	Conhecimento. Organização. Informação. Documentação. Biblioteconomia. Instituições. Publicações
ÁREA DE CONHECIMENTO	Ciência e tecnologia dos computadores
SUBÁREA	Segurança da Informação
ORGANIZAÇÃO	Sistemática
TRATAMENTO	bilingue
IDIOMAS	Francês - Português
AMPLITUDE	30 termos
DESTINATÁRIO	Estudantes; acadêmicos e profissionais da área de tecnologia da informação
FUNÇÃO	Difusão e descrição dos termos de Segurança da Informação

Tabela 3 . Características Gerais do Glossário. Fonte: adaptado de Demai (2006)

5.2 Mapa Conceitual

Consoante Demai (2006), o mapa conceitual visa estabelecer e hierarquizar os termos de uma área em suas classes semânticas; sendo , portanto, o primeiro passo a identificação e segmentação dos termos que comporão o glossário final.

Portanto, a segurança da informação foi enquadrada na categoria 3.1 0 Generalidades. Ciência e Conhecimento. Organização. Informação. Documentação. Biblioteconomia. Instituições. Publicações; na subcategoria 0 004 Segurança da Informação da Classificação Decimal Universal. No entanto, as subcategorias da subcategoria Segurança , foram baseadas nas seções da norma ISO/IEC 27002 , um padrão de fato mundialmente reconhecido na área.

Durante o processo de tradução foram extraídos termos e delimitados seus contextos. Além disso, utilizou-se textos paralelos relacionados aos textos de partida como forma de apoio. Neste processo, verificou-se também a autenticidade dos termos equivalentes aos da língua de partida.

Os seguintes critérios foram adotados para a extração dos termos consoante Aubert (2001) apud Demai (2006):

a) Identificação de recursos gráficos e do leiaute – neste quesito analisa-se o destaque gráfico que é dado ao termo, como, por exemplo, negrito; itálico e cores.

b) Critério estatístico: frequencia e regularidade – verifica-se o número de ocorrência do termo no corpus. Este método apresentou algumas limitações ao presente trabalho. Primeiramente, conforme a Lei estatística dos grandes números, uma estimativa probabilística baseada apenas em poucas observações pode apresentar grande divergência, mas com um número crescente de observações a estimativa tende a ser mais fidedigna. Como o corpus utilizado na presente pesquisa é composto apenas por três textos, as frequências da maioria dos termos eram baixas, tornando este critério não fidedigno.

   Segundo, ao listar os termos mais frequentes nos textos dos corpus, notou-se que noções importantes tais como sécurité des informations; integrité; confidentialité; dentre outras, não apareciam na lista dos mais frequentes. Destarte, optou-se pelo critério epistêmico, que segundo Ferreira (2000) relaciona-se a teoria da área em questão. Neste sentido, a teoria é considerada como um “conjunto sistêmico de idéias”; e , para reconhecer as categorias analíticas da teoria a fim de relacionar os conceitos-chaves ligados à área, foram elaborados mapas conceituais que serão apresentados mais adiante.

c) Critério do especialista- Este critério foi considerado o mais adequado para a seleção dos termos do glossário deste trabalho; devido às limitações do critério estatístico supracitadas, na maior parte das vezes optou-se pelos termos que possuíam maior relevância para a segurança da informação.

O mapa conceitual (Figura 2) é composto por dez categorias principais da área de segurança de acordo com a norma ISO/IEC 27002. Cada categoria é representada por sub-mapas conceituais que, por sua vez, possuem sub-categorias. Os termos de entrada do glossário estão alocados em seus respectivos sub-mapas e sub-categorias.

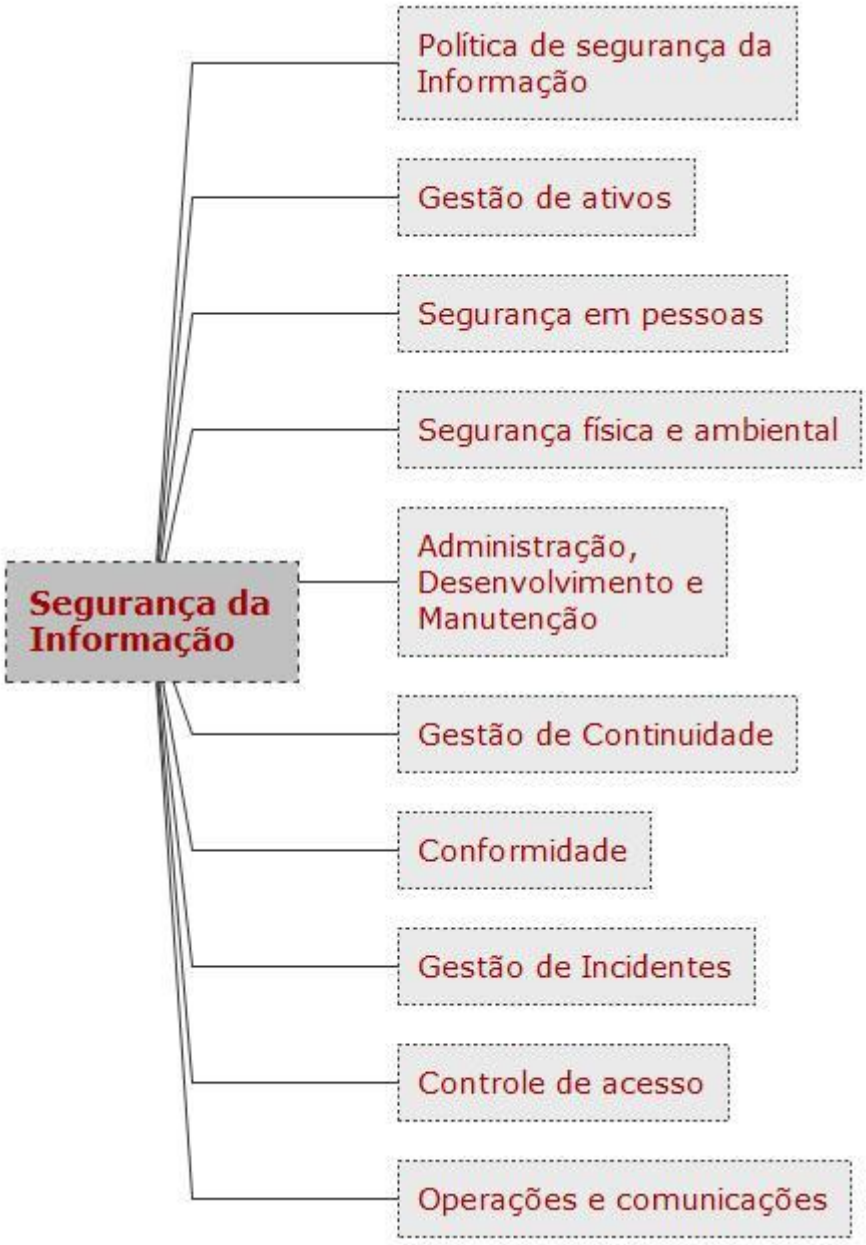


Figura 2: Mapa Conceitual Segurança da Informação. Fonte: Elaborado pela autora.

Figura 3. Sub Mapa Conceitual 1. Fonte: Elaborado pela autora.

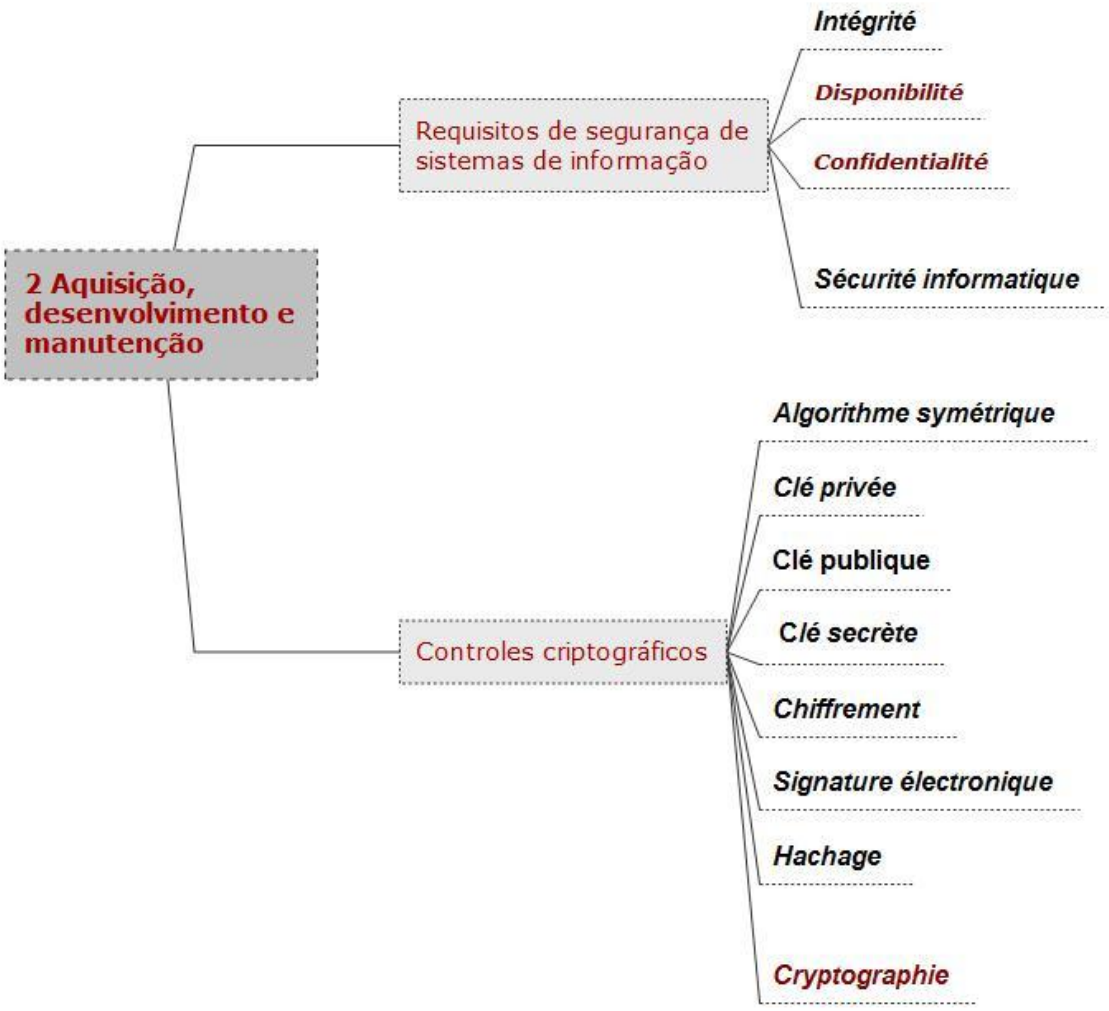


Figura 7. Sub Mapa Conceitual 2. Fonte: Elaborado pela autora.

Figura 9. Sub Mapa Conceitual 3. Fonte: Elaborado pela autora.

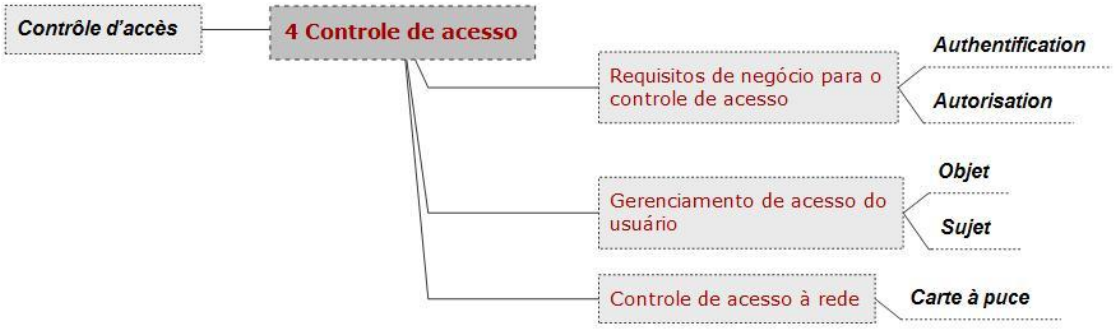


Figura 11. Sub Mapa Conceitual 4. Fonte: Elaborado pela autora.

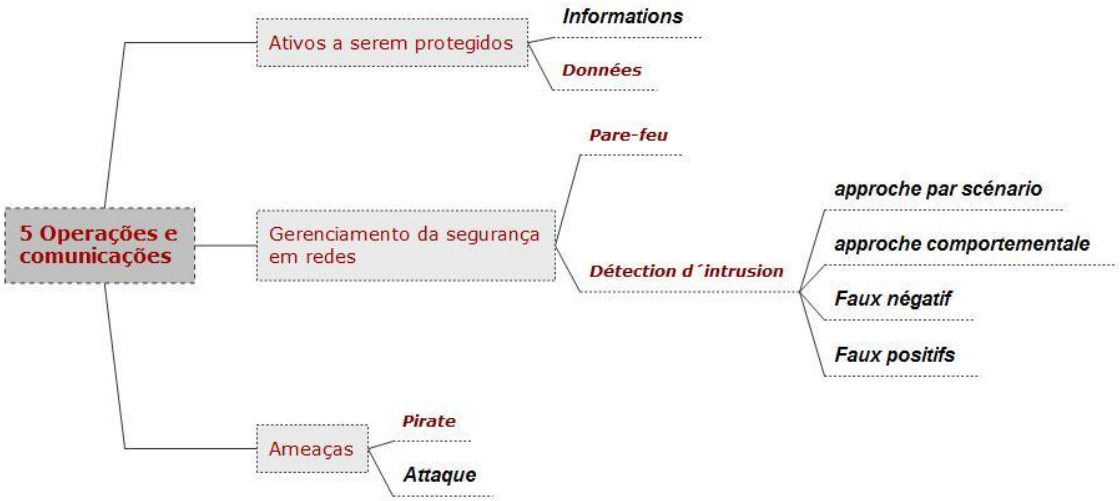


Figura 12. Sub Mapa Conceitual 5. Fonte: Elaborado pela autora.

Em seguida, os termos foram alocados em fichas terminológicas. Para Demai (2006), estes instrumentos servem para coleta, sistematização e análise de termos quantitativamente e qualitativamente. A ficha utilizada contém os seguintes campos: entrada, que é o termo propriamente dito; forma equivalente; categoria gramatical representado por siglas (adjetivo – adj.; substantivo feminino – s.f.; substantivo masculino – s.m., verbo – v.); número (singular ou plural); sigla/acrônimo que constituem as abreviações nos contextos selecionados, área (baseado nos mapas e submapas); contexto que é retirado da fonte em que o termo ocorre e seu conceitos relacionados ao contexto; termo

dicionarizado que indica se há coincidência entre a definição do dicionário e a definição final estabelecida; e, conceito final . A ficha (Anexo I) foi adaptada de Froom (2005).

5.4 COMPOSIÇÃO DO GLOSSÁRIO

O glossário a seguir baseia-se, em termos de microestruturas, em três paradigmas, conforme dispõe Barbosa (1999) :

d) Paradigma informacional (PI) - categorias gramatical, gêneros, números e domínio da área;

e) Paradigma definicional (PD)- na língua de chegada e;

f) Paradigma pragmático (PP) – constituídos por segmentos de frases extraídos dos textos de partida.

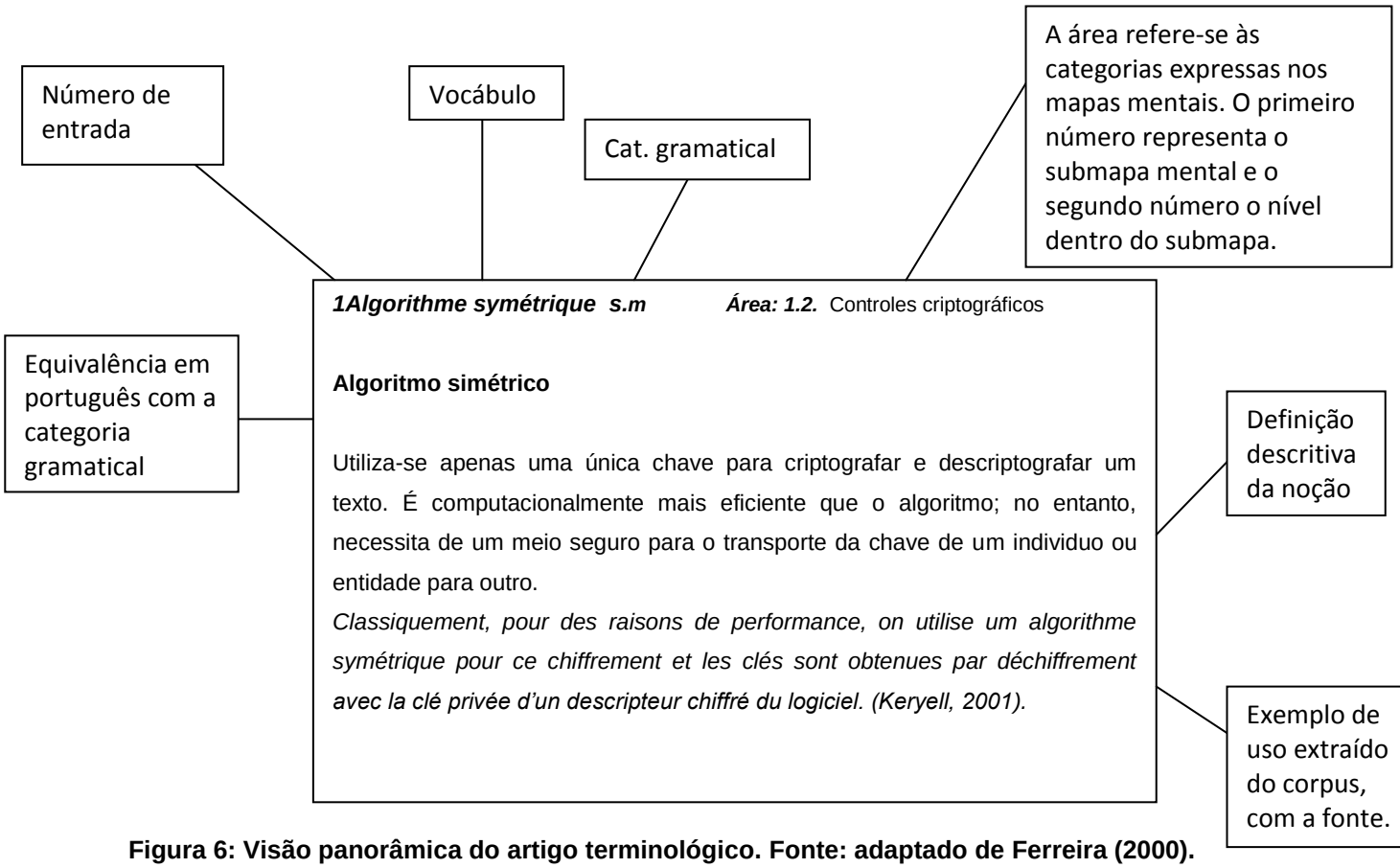


Figura 6: Visão panorâmica do artigo terminológico. Fonte: adaptado de Ferreira (2000).

6. GLOSSÁRIO

SEGURANÇA DA INFORMAÇÃO

1 Algorithme symétrique s.m. ***Área: 2.2.*** **Controles criptográficos**

Algoritmo simétrico s.m.

Algoritmo criptográfico que utiliza apenas uma única chave para criptografar e descriptografar um texto. É computacionalmente mais eficiente que o algoritmo assimétrico; no entanto, necessita de um meio seguro para o transporte da chave de um individuo ou entidade para outro.

Classiquement, pour des raisons de performance, on utilise um algorithme symétrique pour ce chiffrement et les clés sont obtenues par déchiffrement avec la clé privée d'un descripteur chiffré du logiciel. (Keryell, 2001).

2 Attaque ***s.m*** ***Área: 5.2 Ameaças***

Ataque *s.m*

Tentativa de acesso ou uso não autorizado a um programa ou computador. Exploração por uma ameaça da vulnerabilidade de um ativo informacional.

*Il est très rare qu'une attaque génère une seule alarme. (*Marrakchi et al , 2006)

3 Authentification s.f. ***Área: 4.2 Requisitos de negócio para o controle de acesso***

Autenticação s.f.

Processo que visa comprovar a identidade de um indivíduo, normalmente, no momento em que ele requisita um acesso em um programa ou computador.

*La sécurité des systèmes informatiques vise à protéger l'accès et la manipulation des données et des ressources d'un système par des mécanismes d'authentification, d'autorisation, de controle d'accès, etc. (*Marrakchi et al , 2006)

4 Autorisation s.f. ***Área: 4.2 Requisitos de negócio para o controle de acesso***

Autorização

Mecanismo responsável por fornecer permissão aos usuários autorizados para que estes utilizem os recursos protegidos de um sistema.
En utilisant ce modèle, il est ensuite possible de d´eriver les autorisations concr`etes qui s'appliquent aux sujets, actions et vues.(Cuppens *et al, 2005).*
C.f. Controle de acesso

5 Approche par scénario s.f. ***Área: 5.3 Gerenciamento de segurança em redes***

Abordagem baseada em conhecimento s.f.

Método de detecção que analisa a atividade do sistema em busca de padrões de ataque ou instrução conhecidos por meio de uma base de dados de ataques conhecidos e assinaturas.
*Il s'agit de l'« approche par scénario » dans laquelle on analyse les données d'audit à la recherche de scénarios d'attaques prédéfinis dans une base de signatures d'attaque. (*Marrakchi et al , 2006)

6 Approche comportementale s.f. ***Área: 5.3 Gerenciamento de segurança em redes***

Abordagem comportamental s.f.

Abordagem que visa identificar desvios de comportamento do usuário ou sistemas independente do sistema operacional ou plataforma utilizada.
C'est la première approche possible en détection d'intrusions, appelée « approche comportementale » ; elle permet de détecter toute déviation par rapport à un comportement normal préalablement défini, généralement par apprentissage, et stocké dans une base de comportements. *(*Marrakchi et al , 2006)

7 Confidentialité s.f. ***Área: 2.2 Requisitos de segurança De sistemas de informação***

Confidencialidade s.f.

Serviço que garante que a informação não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem autorização.
Cela permet de concevoir par exemple des programmes capables de ne tourner que sur une seule machine au monde, assurant ainsi la confidentialité de l'application et des communications.(Keryell, 2001).

8 Contrôle d'accès s.m. ***Área: 4.1 Controle de acesso***

Controle de acesso s.m.

Para a segurança da informação, controle de acesso é um conjunto de procedimentos e práticas que visam assegurar o ambiente físico e lógico que contém informações sensíveis para certos indivíduos e/ou organizações. Os principais métodos utilizados são a tríade autenticação, autorização e auditoria. *La sécurité des systèmes informatiques vise à protéger l'accès et la manipulation des données et des ressources d'un système par des mécanismes d'authentification, d'autorisation, de controle d'accès, etc. (*Marrakchi et al , 2006)

9 Clé privée s.f ***Área: 2.2.*** **Controles criptográficos**

Chave privada s.f

Chave de uma par de chaves do sistema assimétrico de criptografia que , dependendo do objetivo do processo criptográfico, pode cifrar ou decifrar uma mensagem.
Classiquement, pour des raisons de performance, on utilise un algorithme symétrique pour ce chiffrement et les clés sont obtenues par déchiffrement avec la clé privée d'un descripteur chiffré du logiciel. *.(Keryell, 2001).*

10 Clé publique s.f. ***Área: 2.2.*** **Controles criptográficos**

Chave pública s.f.

Chave de um par de chaves do sistema assimétrico de criptografia que , dependendo do objetivo, pode cifrar ou decifrar uma mensagem. Este termo é , também, utilizado como alternativa para o termo sistema assimétrico.
La technique utilisable est l'usage de la cryptographie à clé publique et clé secrète [8] au sein même du microprocesseur. *.(Keryell, 2001).*

11 Clé secrète s.f. ***Área: 2.2.*** **Controles criptográficos**

Chave secreta s.f.

A criptografia de chave secreta, também conhecida como chave única, pertence ao sistema simétrico de criptografia e utiliza a mesma chave tanto para codificar quanto para decodificar mensagens. Apesar deste método ser bastante eficiente em relação ao tempo de processamento, ou seja, o tempo gasto para codificar e decodificar mensagens, tem como principal desvantagem a necessidade de utilização de um meio seguro para que a chave possa ser compartilhada entre pessoas ou entidades que desejem trocar informações criptografadas.
La technique utilisable est l'usage de la cryptographie à clé publique et clé secrète [8] au sein même du microprocesseur. .(Keryell, 2001).

12 Chiffrement s.m ***Área: 2.2.*** **Controles criptográficos**
Encriptação s.m.

É o processo que visa cifrar um texto em claro tornando-o ilegível , salvo para as pessoas que possuem a chave para desencriptá-lo.
Cet article présente une technique matérielle permettant de rajouter du chiffrement fort à un processeur. .(Keryell, 2005).

12 Cryptographie s.f. ***Área: 2.2.*** **Controles criptográficos**
Criptografia s.f.

Conjunto de técnicas e procedimentos que visam transformar um texto claro em um texto legível apenas para o destinatário possuidor da chave criptográfica.
La technique utilisable est l'usage de la cryptographie à clé publique et clé secrète [8] au sein même du microprocesseur. (Keryell, 2005).

13 Carte à puce s.f. ***Área: 4.2.*** **Controle de acesso à rede**
Cartão inteligente s.f.

Na segurança da informação, o cartão inteligente assemelha-se a um cartão de crédito com chip, que é utilizado no processo de autenticação de usuários. Este pode ser com ou sem contato. No primeiro caso, o chip é encostado fisicamente na máquina leitora. No segundo caso, por sua vez, a leitura do cartão é feita por uma antena, por isso não é necessário contato direto.

La technique utilisable est l'usage de la cryptographie à clé publique et clé secrète [8] au sein même du microprocesseur. C'est la technique utilisée dans les cartes à puces.(Keryell, 2005).

14 Disponibilité s.f. ***Área: 2.2 Requisitos de segurança De sistemas de informação***

Disponibilidade s.f.

Requer que um sistema computacional e seus ativos de informação estejam disponíveis às pessoas autorizadas quando necessário.

C'est le cas de violation de la contrainte de disponibilité des données et des ressources d'un système. *(*Marrakchi et al , 2006)

15 Détection d'intrusions s.m. ***Área: 5.2 Gerenciamento de segurança em redes***

Detecção de intrusos s.m.

Mecanismo que indica que alguma tentativa de intrusão ocorreu no sistema, violando a política de segurança deste.

*Denning et al. Ont travaillé à la conception d'un système de détection d'intrusions basé sur des méthodes statistiques et des systèmes experts. (*Marrakchi et al , 2006)

16 Données s.f. ***Área: 5.2.*** **Ativos a serem protegidos**

Dados s.m.

Representação dos fatos, conceitos ou instruções de uma maneira normalizada que se adapte à comunicação, interpretação e processamento pelo ser humano ou por meio de máquinas automatizadas.
Ce mécanisme associé aux caches et à la gestion mémoire permet de chiffrer les instructions du programme ainsi que les données en mémoire pour assurer une bonne résistance aux ataques sur le bus du microprocesseur. .(Keryell, 2001).

17 Faux négatif s.m ***Área: 5.3 Gerenciamento de segurança em redes***

Falso negativo s.m.

Ocorre quando uma intrusão real acontece, mas a ferramenta permite que ela passe como se fosse uma ação legítima.
*Chacune de ces approches peut conduire à des faux positifs (détection d'attaque(s) en absence d'attaque) ou à des faux négatifs (absence de détection en présence d'attaque(s)). (***Marrakchi et al , 2006)**

18 Faux positifs s.m. ***Área: 5.3 Gerenciamento de segurança em redes***

Falso positivo s.m.

Ocorre quando a ferramenta aponta uma ação como uma possível intrusão, quando na verdade trata-se de uma ação legítima.
*Chacune de ces approches peut conduire à des faux positifs (détection d'attaque(s) en absence d'attaque) ou à des faux négatifs (absence de détection en présence d'attaque(s)). (*Marrakchi et al , 2006)

19 Hachage s.f ***Área: 2.2.*** **Controles criptográficos**

Hash s.m.

Método de autenticação e integridade de informações, que utiliza um bloco de tamanho arbitrário e o transforma em uma string de bits fixos. Desta forma, se o bloco de entrada dos dados for alterado, a função hash produzida também o será.
Concrètement si on crypte au niveau d'une ligne de cache de 32 octets (soit 256 bits) et qu'on a un résultat de hachage de 128 bits, l'occupation mémoire du programme. augmente de 50 %, ce qui est raisonnable. *(Keryell, 2005).*

20 Intégrité s.f. ***Área: 2.2 Requisitos de segurança De sistemas de informação***

Integridade s.f.

Garantia de que os dados recebidos estão exatamente como foram enviados por uma entidade autorizada.
*Il n'est donc pas suffisant d'agir préventivement, c'est à dire de définir une politique de sécurité (en termes de confidentialité, d'intégrité et de disponibilité des données et ressources du système à protéger) et de mettre en oeuvre des mécanismes implantant cette politique. (*Marrakchi et al , 2006)

21 Informations s.f. ***Área: 5.2.*** **Ativos a serem protegidos**

Informações s.f.

Resultado do processamento, manipulação e organização de dados, de forma que represente uma modificação no conhecimento do sistema (pessoa, animal ou máquina) que a recebe. No contexto da segurança da informação, a informação sensível deve ser assegurada contra possíveis ataques.

Lors de cette adaptation,WorldCompany se rend compte que l'un de ses administrateurs, Juda, définit des règles dans la politique de s´ecurit´e qui laissent des informations trop vulnérables.(Cuppens *et al, 2005).*

22 Objet s.m. ***Área: 4.2 Gerenciamento de Acesso do usuário***

Objeto s.m.

No contexto do controle de acesso, objeto se refere a entidades protegidas que serão acessadas por sujeitos autorizados.

Une fois définie la politique de sécurité organisationnelle, il est possible de tester comment cette politique s'applique aux entités concrètes que sont les sujets, actions et objets. .

(Cuppens *et al, 2005).*

23 Politiques de sécurité s.f. ***Área: 1.2.*** **Documentação da política De segurança da informação**

Política de segurança s.f.

Normas, procedimentos e diretrizes formalmente expressas pela direção; que visam assegurar a confidencialidade, a integridade e a disponibilidade das informações bem como os recursos do sistema de informação.

Il n'est donc pas suffisant d'agir préventivement, c'est à dire de définir une politique de sécurité (en termes de confidentialité, d'intégrité et de disponibilité des données et ressources du système à protéger) et de mettre en oeuvre des mécanismes implantant cette politique.

*(*Marrakchi,2005)

24 Pirate s.m. ***Área: 5.2.*** **Ameaças**

Hacker s.m.

Programadores maliciosos e ciberpiratas que agem com o intuito de violar ilegal ou imoralmente sistemas de informação. Em geral, é confundido com o termo hacker que se refere a programadores e desenvolvedores que buscam aprimorar o software e o hardware.

Bien que compliquées, de telles attaques sont possibles et une fois le logiciel mis à nu son contenu peut être répliqué par des pirates. .(Keryell, 2005).

25 Pare-feu s.m. ***Área: 5.3 Gerenciamento de segurança em redes***

Firewall s.m.

Mecanismo de redes de computadores que visa aplicar uma política de segurança, em um determinado perímetro da rede, por meio da filtragem dos pacotes de dados que entram e saem.

Par conséquent, une entreprise est une organisation mais un composant de sécurité tel qu'un pare-feu correspond également à une organisation.

.**(** Cuppens *et al, 2005).*

26 Signature électronique s.f. ***Área: 1.2.*** **Controles criptográficos**

Assinatura digital s.f.

Método que visa assegurar a autenticidade e integridade da informação digital;é , também, tratada de forma análoga à assinatura física em papel.Faz uso do sistema assimétrico cuja entidade ou individuo utiliza sua chave privada para assinar.

Afin d'éviter ce type d'attaque, on peut soit chiffrer des blocs de données plus importants d'un coup, de type ligne de cache [7], soit rajouter une signature électronique [8]. (Keryell, 2005).

27 Sécurité informatique s.f ***Área: 2.2 Requisitos de segurança De sistemas de informação***

Segurança da informação s.f.

Conjunto de práticas e procedimentos que visam prover confidencialidade, integridade, autenticidade , disponibilidade, não repúdio, dentre outros serviços, aos ativos de informação que possuem valor para a organização ou para os indivíduos.
Une autre problématique est celle de la sécurité informatique et la nécessité d'avoir des systèmes résistants aux attaques informatiques bien sûr mais aussi aux attaques physiques d'un système sensible, telle que la manipulation des bus systèmes d'un ordinateur, des liens de communication, etc. *(Keryell, 2005).*

28 Sujet s.m. ***Área: 4.2 Gerenciamento de Acesso do usuário***

Sujeito s.m.

No âmbito do controle de acesso, sujeito é aquele que requer acesso a um determinado objeto (informação, arquivo, sistema computacional, dentre outros).
Cette distribution porte également sur les responsabilités d'administration que l'on peut confier à des sujets affectés à des rôles différents. .(Cuppens *et al, 2005).*

29 Traces d´audit* s.f.** ***Área: 3.2 Auditoria

Trilhas de auditoria s.f.

Conjunto de informações registradas que permite analisar as ações ou eventos que foram realizados no sistema. Consiste em um importante material para a auditoria do sistema.
*Les informations collectées sont regroupées dans des fichiers appelés traces d'audit. (*Marrakchi,2005).

7. Conclusão

Neste trabalho, foi possível alcançar todos os objetivos traçados. O primeiro objetivo alcançado foi a tradução dos três artigos da área de segurança da informação. As principais dificuldades do processo tradutório foram de cunho terminológico. Neste sentido, os conceitos da área da terminologia foram de grande valia na medida em que forneceram o direcionamento necessário para a tomada de decisão. Outra dificuldade encontrada foi a diferença entre as normas de formatação dos artigos do texto de partida e chegada; já que, em geral, adota-se as normas da ABNT nos periódicos brasileiros. Como, no entanto, isso não é regra geral (alguns periódicos adotam outras normas como a APA , por exemplo), optou-se por manter a formatação dos textos de partida.

Outro objetivo atingido foi a elaboração dos mapas conceituais e dos fichamentos terminológicos. Na elaboração desses instrumentos, a figura do tradutor especialista foi de capital importância haja vista que seus conhecimentos serviram como critério final para a extração dos termos dos textos traduzidos. Além de servir , também, como base para a categorização dos termos nos mapas conceituais e definição conceitual destes durante a elaboração dos fichamentos. Outrossim, ambos os instrumentos foram essenciais para a construção do glossário.

Por fim, o objetivo final, que era a construção do glossário de segurança da informação, foi alcançado com êxito. É importante ressaltar, porém, que devido ao tamanho reduzido do corpus (apenas três textos) ,o glossário limitou-se a um N de 29 termos. Por isso, recomenda-se para trabalhos futuros que seja utilizado um corpus maior, para que se possa ter um glossário mais rico.

Com relação ao tradutor especialista, concluiu-se que agrega-se valor ao produto final quando o tradutor domina a área de conhecimento em questão. As escolhas dos termos e expressões a serem utilizadas são otimizadas e mais fidedignas. Na elaboração do glossário, como já dito antes, o conhecimento do tradutor especialista pode ser utilizado como critério para a extração dos termos. No entanto, não basta apenas dominar a área de conhecimento do texto de partida, é preciso também dominar as técnicas de tradução, conhecendo os conceitos, as teorias e discussões do domínio. Já que muitas vezes o especialista de uma área,

tal como a segurança da informação, não tem consciência da importância de fatores culturais que envolvem o processo tradutório, conceitos como tradução livre e literal. Esta falta de conhecimento resulta, muitas vezes, em um texto sem sentido para o público alvo e ao *pé da letra.*

8. Referencial bibliográfico

ARAUJO FERREIRA, A.M. Para um vocabulário fundamental da obra de Milton Santos: 2000. Tese (Doutorado em Linguistica) Universidade de São Paulo, USP, Brasil.

.

AZENHA JR, João.Tradução técnica, condicionantes culturais e os limites da responsabilidade do tradutor. In: IV Congresso Brasileiro de Linguistica Aplicada, Unicamp, 1999.

DEMAI, F.M. Um dicionário terminológico da área de Ortopedia técnica: descrição e análise: 2006. Dissertação (Mestrado em Linguistica) – Universidade de São Paulo, USP, Brasil.

DIAS, Cláudia. Segurança e Auditoria da Tecnologia da Informação. Rio de Janeiro: Axcel Books do Brasil, 2001.

FINATTO, M.J.B,KERSCHER,S. Qualificação da pesquisa terminológica: cooperação para a identificação de terminologias químicas. In: IV Simposio RITERM, Lisboa , 2000. Disponível em : http://www.riterm.net/actes/7simposio/finatto.htm. Acesso em 24 mai. 2011.

FROMM, G. Ficha terminológica Informatizada: etapas e descrição de um banco de dados terminológico bilíngue. São Paulo: FFLCH/USP, 2005.

KREIGER, M.G, FINATTO, M.J.B. Introdução à terminologia: teoria e prática. Ed.Contexto, São Paulo, 2004.

PAIVA, P.T.P. Estudo de traços de simplificação e explicitação em artigos científicos de anestesiologia. Cadernos de Tradução, ISSN 2175-7968, Florianópolis,2006.

POLCHLOPEK, S.; AIO, M. Tradução técnica: armadilhas e desafios. **Tradução & Comunicação**, Brasil, v. 0, n. 19, p. 101-114, 2010. Disponível em: <http://sare.unianhanguera.edu.br/index.php/rtcom/article/view/1638/768>. Acesso em: 24 mai. 2011.

POSSAMAI, V. Marcadores textuais do artigo científico em comparação português e inglês – um estudo sob a perspectiva da tradução. Dissertação de mestrado. UFRS, 2004.

9. ANEXO I

FICHA TERMINOLÓGICA

Entrada: Politique de Sécurité	**Forma equivalente:** Politica de segurança	**Cat.Gram.** s.f.	**Número** S	**Sigla/Acrônimo:**	**Domínio:** Política de segurança da informação
Contexto: La détection d'intrusions a pour objectif de détecter toute violation de la politique de sécurité en vigueur sur un système informatique Fonte: Marrakchi et al (2008)			**Conceito:** Normas e procedimentos que visam assegurar a confidencialidade, a integridade e a disponibilidade das informações.		
Contexto2: Os controles considerados práticas para a segurança da informação incluem: a) documento da política de segurança da informação;b)atribuição de responsabilidades para a segurança da informação;c)atribuição de responsabilidades para a segurança da informação. Fonte: Norma ISO/IEC 27002			**Conceito2:** Intenções e diretrizes globais formalmente expressas pela direção Fonte: Norma ISO/IEC 27002		
Conceito final: Normas, procedimentos e diretrizes formalmente expressas pela direção; que visam assegurar a confidencialidade, a integridade e a disponibilidade das informações bem como os recursos do sistema de informação.			**Dicionarizada: Sim() Não(X)** **Conceito do dicionário:**		

Entrada: Détection	**Forma equivalente:**	**Cat.Gram.** s.f.	**Número** Pl.	**Sigla/Acrônimo:**	**Área:** Gerencia

d'intrusions	Detecção de intrusão			IDS	mento de segurança da rede
Contexto: La détection d'intrusions a pour objectif de détecter toute violation de la politique de sécurité en vigueur sur un système informatique. **Fonte:** Marrakchi et al (2008)			**Conceito:** Mecanismo que visa detectar violações à politica de segurança do sistema.		
Contexto2: Um sistema de detecção de intrusos geralmente detecta manipulações de sistemas de computadores indesejadas, normalmente através da internet. Essas manipulações normalmente vêm de ataques de hackers Fonte: http://www.gta.ufrj.br/grad/07_2/rodrigo_leobons/deteccao.html			**Conceito2:** Sistema que detecta comportamentos indesejados que , por sua vez, podem comprometer a segurança e confiabilidade do sistema.		
Conceito final: Mecanismo de defesa que detecta comportamentos indesejados e/ou violações à política de segurança do sistema.			**Dicionarizada: Sim() Não(X)** **Conceito do dicionário:**		

Entrada:	**Forma equivalente:**	**Cat.Gram.**	**Número**	**Sigla/Acrônimo:**	**Área:**
Confidentialité	Confidencialidade	s.f.	S.		Serviços de segurança
Contexto: Cela permet de concevoir par exemple des programmes capables de ne tourner *que* sur une seule machine au monde, assurant ainsi la confidentialité de l'application et des communications. Fonte: Keryell(2001)			**Conceito:** Garantia de que as informações contidas em uma aplicação e/ou que estão vinculadas à um processo de comunicação estão resguardadas contra a sua revelação não autorizada.		

Contexto2: Dans les deux cas on parle de violation de la contrainte de confidentialité des données. Fonte: Marrakchi et al (2008)	**Conceito2:** Garantia de que as informações só estarão disponíveis para as pessoas, processos ou aplicações autorizadas.
Conceito final Garantia de que as informações estão resguardadas contra a sua revelação não autorizada.	**Dicionariazada: Sim(x) Não()** **Conceito do dicionário:** Qualidade do que é confidencial

Entrada:	**Forma equivalente:**	**Cat.Gram.**	**Número**	**Sigla/Acrônimo:**	**Área:**
Contexto:			**Conceito:**		
Contexto2:			**Conceito2:**		
Contexto3:			**Conceito3:**		
Conceito final:			**Dicionariazada: Sim() Não()** **Conceito do dicionário:**		

10. INDICE REMISSIVO

A

C

Controle de acesso - *Contrôle d'accès*

Criptografia – *Cryptographie*

D

Disponibilidade – *Disponibilité*

Detecção de intrusos – *Détection d´intrusion*

Dados - *Données*

E

Encriptação – *Ciffrамment*

F

Falso negativo - *Faux négatif*

Falso Positivo – *Faux positif*

Firewall- *Pare-feu*

H

Hash – *Hachage*

Hacker – *Pirate*

I

Integridade – *Intégrité*

Informations – *Informations*

O

Objeto – *Objet*

P

Politica de Segurança - *Politiques de sécurité*

S

Segurança da Informação - *Sécurité informatique*

Sujeito - *sujet*

T

Trilhas de auditoria - *Traces d´audit*