Universidade do Minho
Escola de Engenharia

Pedro Miguel Terroso de Andrade Tarrinho

A Confiança como factor de Segurança num Ambiente de Vida Assistido

Novembro de 2009

Universidade do Minho
Escola de Engenharia

Pedro Miguel Terroso de Andrade Tarrinho

A Confiança como factor de Segurança num Ambiente de Vida Assistido

Tese de Mestrado
Mestrado em Informática

Trabalho efectuado sob a orientação do
Professor Paulo Novais

Novembro de 2009

Agradecimentos

Agradeço ao Professor Paulo Novais toda a orientação pessoal e científica com todo o tempo que me deu, toda a confiança, incentivo e apoio sem o qual não teria conseguido chegar ao fim desta jornada.

Agradeço ao amigo Ricardo Costa pela colaboração e apoio pessoal e científico.

Aos colegas Ângelo Costa e Davide Carneiro pela camaradagem e ajuda que é necessária num grupo de trabalho.

Ao Professor Francisco Andrade da Escola de Direito pela preciosa colaboração.

À Denise Terroso pelas revisões consecutivas dos artigos e tese.

Aos meus Pais pelo apoio e compreensão.

A Multicert e todos os seus colaboradores pelo tempo disponibilizado e pelo encorajamento.

Resumo

A Segurança é um conceito algo abstracto e muito relativo, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si.

Normalmente, sempre que se analisa, do ponto de vista da segurança, um qualquer sistema, no âmbito deste trabalho sobre Ambientes de Vida Assistidos, tende-se a idealizar uma solução fechada, no entanto tal é tecnologicamente "impossível".

Pretendeu-se conduzir uma investigação que abrangesse as diferentes vertentes de segurança na área da saúde. Como caso de estudo foi utilizado o *VirtualECare*, uma rede colaborativa de entidades prestadores de serviços de saúde.

Na impossibilidade de se definir ou estabelecer segurança, optou-se por designar a Confiança como elemento fundamental. A Confiança foi subdividida em diferentes vertentes para facilitar a sua compreensão e respectivas recomendações/soluções. Este conjunto de boas práticas abrange uma miríade de áreas, que vão desde a arquitectura à infra-estrutura do sistema, passando pelas comunicações e normas de utilização.

Abstract.

Security is an abstract concept and is also very relative, including not only the security of data / information, but also the systems themselves.

Normally, when we analyze through the point of view of safety any system, in this work, on ambient assisted living, we tend to idealize a closed solution, but it is technologically impossible.

The intention was to conduct an investigation covering the different aspects of security concerning the health sphere. A case study was used, VirtualECare, a collaborative network of health services providers.

In the impossibility of defining or establishing security, we chose to designate Trust as a key element. Trust has been subdivided into different sections to facilitate their understanding and their recommendations / solutions. This set of good practices covers a wide range of areas, from architecture to the system infrastructure, through communications and use standards.

Ao meu avô que foi o meu norte...

À Deni que me aturou o stress e que não me deixou desistir.

Índice

Índice de Figuras

Índice de Exemplos

Acrónimos/ Glossário

AmI – Ambiente Inteligente

ApS – Application Server

AUML – Agent Unified Modeling Language

AVA – Ambiente de Vida Assistido

CC – Centro de atendimento de Chamadas

DOS – Denial of Service

DDOS – Distributed Denial of Service

FIPA – Foundation for Intelligent Physical Agents

GSM - Global System for Mobile communications

HSM – High Security Module

IA – Inteligência Artificial

ITIJ - Instituto de Tecnologias de Informação da Justiça

Jade – Framework de desenvolvimento java para agentes

JGa – Jade Gateway

OSGI - Open Services Gateway Initiative

PKI – Public Key Infrastructure – Infrastrutura de Chave Pública

R-OSGI – Remote Open Services Gateway Initiative

RFID – Radio Frequency Identification

SGC - Sistema de Gestão de Chaves

SMA - Sistema MultiAgente

SSGD – Sistema de Suporte ao Grupo de Decisão

UPnP – Universal Plug and Play

UML - Unified Modeling Language

1-wire – solução de comunicação baseada em apenas num fio

Agente – sistema informático autónomo, que toma decisões (termo usado em situações de alto nível)

Bundle – programa informático autónomo (termo usado em situações mais técnicas)

e-Health – sistema de saúde relacionado com as tecnologias de informação

Malware – software desenhado para se infiltrar em computadores com objectivos maliciosos

Spam – software desenhado para se infiltrar em computadores e enviar publicidade enganosa, ou até vírus.

TeleAssistência – sistema de assistência remota

TeleMedicina – sistema de medicina remota

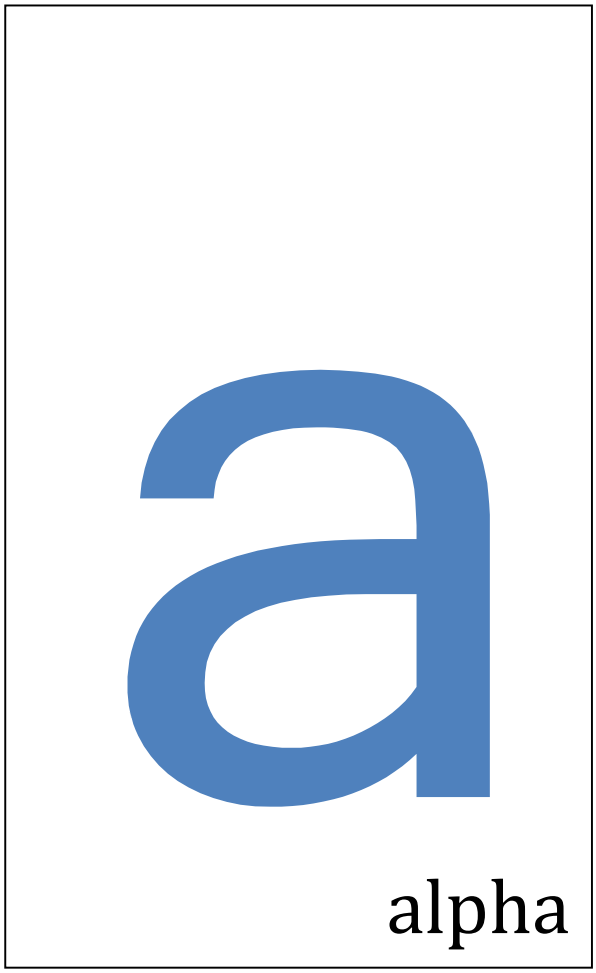
Spyware – software desenhado para se infiltrar em computadores e recolher informações

Vírus – software desenhado para se infiltrar em computadores e corromper sistemas

X10 – standard de comunicações para equipamentos electrónicos, normalmente usados em domótica

Zigbee - Tecnologia de comunicações sem fios que usa frequências rádio de curtas distâncias

1 Introdução



"Se-Cura", termo proveniente da antiga Grécia cujo significado "sem medo" é considerado como a primeira referência à problemática da segurança, realçando-se a necessidade de não se temer um qualquer atacante.

Quando nos foi apresentada a proposta para este trabalho, imaginamos que no final apresentaríamos uma solução para o problema. No entanto, com o decorrer da investigação, chegamos à conclusão de que mais do que uma solução prática, apresentamos um conjunto de boas práticas que devem ser seguidas, materializadas em termo de recomendações, pelos analistas que concebem estes sistemas.

1.1 Motivação

O envelhecimento da população, tem vindo a ser combatido com o aumento da idade da reforma e incentivos à natalidade, mas os resultados não tem sido encorajadores. Estamos a falar a nível global e com especial foco nos países desenvolvidos/industrializados. No gráfico que apresenta a relação entre pessoas com mais do que 65 anos e crianças com menos de 5 (Figura 1) [3], podemos ver uma redução drástica no número de crianças e um aumento relativamente proporcional do número de idosos. A pergunta que se coloca é: Quem cuidará destas pessoas idosas quando surgirem os problemas de saúde relacionado com a idade?

Embora se esteja a focar o problema dos idosos, não nos podemos esquecer que existe uma parte da população não idosa que também necessita de cuidados continuados (por exemplo: as pessoas com mobilidade reduzida ou com necessidades especiais).

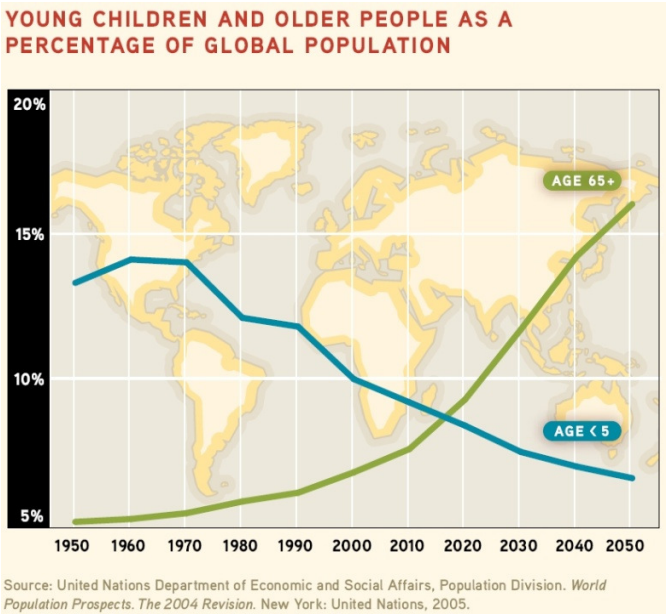


Figura 1 - Número de Crianças verso número de idosos

Outro problema que se coloca é: Como vamos impedir que os sistemas de saúde se deteriorem, que entrem em falência e que as entidades sociais do estado entrem em rotura? Podemos analisar no gráfico seguinte a relação entre o produto interno bruto de cada país e as pensões (Figura 2) [4]. Verificamos que existe uma percentagem ainda grande do valor a pagar aos pensionistas em relação ao valor do produto interno bruto, o que no caso de chegarmos ao rácio de 1 trabalhador para 7 idosos (caso da Itália), verificamos que entraríamos em rotura.

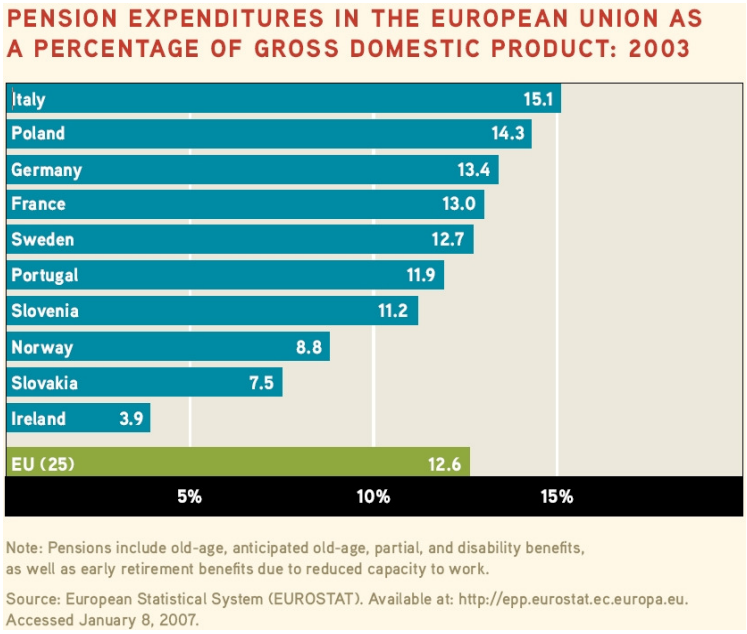


Figura 2 - Percentagem das pensões aos idosos na EU

Podíamos continuar a analisar mais gráficos da evolução humana, mas só íamos chegar à conclusão de que vamos precisar de uma solução rápida e fiável. Nós acreditamos que essa solução passa por reduzirmos o número de pessoas nos hospitais e instituições estatais que já por si se encontram perto dos limites. Como solução, achamos que a população deve usar a TeleAssistência e a TeleMedicina [5, 6].

Já existem soluções que dão provas de serem vantajosas para a população, mas será que são seguras? O que é que protege a nossa privacidade?

- Será que realmente precisamos de segurança, num sistema fechado, com agentes confiáveis, num local onde não existem intervenções externas?

Por mais óbvio que possa parecer, e como definido na própria pergunta, não precisamos de segurança. Se um sistema fechado é uma indicação de um sistema seguro, com as outras premissas que indicam que não existem entidades participantes com o objectivo ou intenção de violar essa informação, então não precisaríamos de mecanismos de segurança.

No mundo real, no entanto, não conseguimos encontrar sistemas fechados. Existem sistemas de alta segurança, mas ninguém pode garantir um sistema 100% seguro, é um objectivo inatingível.

1.2 Objectivos

A problemática do envelhecimento da população apresentada anteriormente, deveria obrigar todos os países a uma investigação contínua de soluções. Isto porque estamos a falar de um problema ao nível mundial e não um problema localizado. Acreditamos que a solução passa por uma apresentação de uma lista de recomendações, boas práticas, para obtermos resiliência no sistema. Lista essa que não vai implicar novas descobertas, utilizando tecnologias já existentes. No entanto, impõe-se uma questão pertinente:

- Como é que a tecnologia pode ajudar os sistemas de saúde, de forma segura e credível?

Para respondermos a esta pergunta, desenvolveu-se este trabalho. Criou-se uma arquitectura corporativa com uma variedade de agentes que permitem ao cidadão/sujeito ter a sua vida normal, mas vivendo em sua casa onde existem sensores e actuadores que podem antever problemas e resolvê-los mesmo antes que aconteçam, projecto *VirtualECare*. Um ponto fulcral neste projecto está baseado na segurança, na confiança que temos nesse sistema.

Assim, o objectivo principal desde projecto é melhorar o projecto *VirtualECare*, alterando-o de forma a haver confiança e segurança. Com este propósito em mente apresentamos uma lista de objectivos que iremos seguir para chegar a essa resiliência do sistema:

- Analise do projecto já existente, o *VirtualECare*, compreendendo a estrutura e a sua forma de funcionar;
- Identificar o que é preciso para obter confiança, explorando os vários níveis em que se decompõe:
    - Ao nível Individual, é necessário obter confiança no sistema. Para isso: reeducar os indivíduos de forma que sejam sensibilizados das implicações das engenharias sociais; permitir observação e experiência para a credibilização do sistema;

- Identificar e avaliar os riscos existentes de forma a podermos aceitar ou providenciar uma solução para esses mesmos problemas, através da identificação dos factores críticos que devem ser implementados (Autenticidade, Confidencialidade, Integridade, não Repudio e Disponibilidade) ao nível do Sistema;
- Comunidade será o terceiro e último nível a ser estudado que através da Lei nos vai permitir definir o que é ou não é seguro, de confiança.

- Analise e identificação de todos os pontos importantes no sistema actual de forma a avançarmos para uma apresentação de solução que o possam melhorar.
- Implementação de todos os pontos sugeridos de forma a obtermos o melhor e mais seguro sistemas de *e-Health*;
- Por fim, definir os critérios que estabelecem a confiança no sistema;

1.3 Metodologia da Investigação

A análise do processo de investigação foi definida em conjunto com os vários grupos associados a este projecto. O primeiro passo, foi investigar o panorama actual e avaliar quais seriam as tecnologias necessárias para um melhoramento ao nível da segurança, mantendo o bom funcionamento do sistema.

Começamos por examinar todos os módulos e como se interligavam, quais as tecnologias que utilizavam, a semântica e a sintaxe das comunicações existentes. Averiguamos quais as necessidades, a nível de cada módulo, no que diz respeito às tecnologias sem fios, como por exemplo: energia necessária, largura de banda, zona de segurança e distância do ponto de emissão. Todos estes pontos são relevantes quer a nível da segurança, quer a nível da usabilidade. Isto porque pretendemos um sistema seguro, mas que continue a ser utilizado.

Ao nível do core do sistema, ponto central onde são executados os vários agentes, foi feito um exame crítico do serviço onde detectamos que um agente podia tomar quail medida. Para

resolvermos este problema, investigamos várias soluções existentes e novas ideias, chegando às conclusões descritas mais à frente.

1.4 Organização da Tese

A Tese está organizada da seguinte forma: como verificamos, no primeiro capítulo fazemos uma introdução aos vários temas sendo seguido por um segundo capítulo em que apresentamos o panorama geral do sistema *e-Health*, explorando as várias soluções existentes.

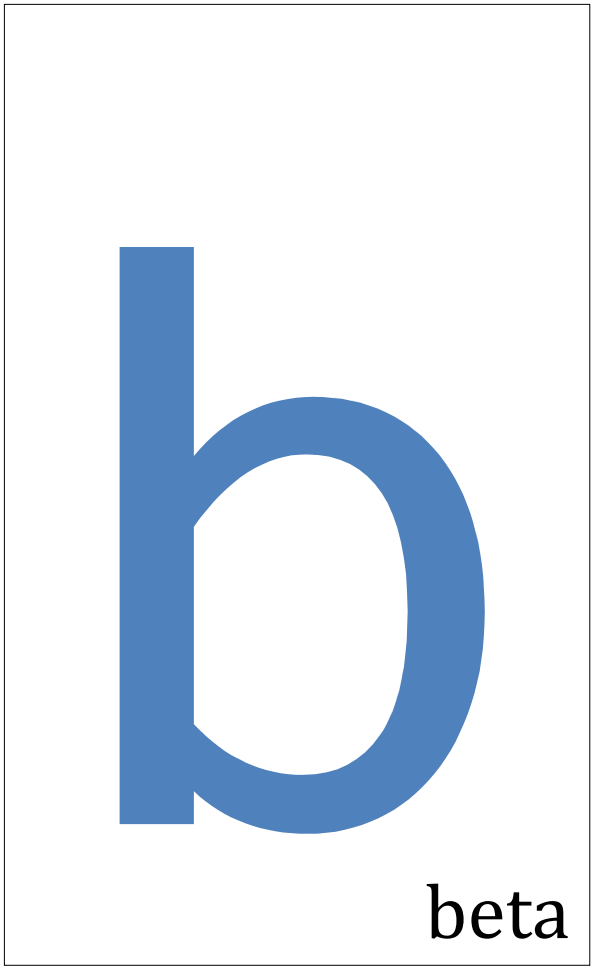
A Segurança dos Sistemas Informáticos é aprofundada no terceiro capítulo, onde endereçamos o significado de segurança e de um sistema seguro, os sistemas inseguros e as estatísticas associadas.

No quarto capítulo, explanamos a problemática da confiança dividindo-a em três esferas. Esferas essas que iremos apresentar e explicar as suas relações.

O quinto capítulo serviu para expormos o projecto *VirtualECare* e apresentarmos as soluções de segurança para os vários problemas encontrados.

Por fim, o capítulo sexto, sintetiza todos os pontos mais importantes da tese e apresenta trabalhos futuros.

2 Segurança em Sistemas Informáticos



2.1 Introdução

A segurança de sistemas informáticos é um tema vasto que não envolve apenas questões de natureza técnica (o factor humano é sempre um dos aspectos mais sensíveis em termos de segurança, em qualquer contexto). Um outro aspecto está relacionado com o objectivo dessa falta de segurança, que nem sempre é de origem criminal/maliciosa, mas sim relacionada com acidentes, desastres naturais e falhas técnicas. Isto significa que para obtermos resiliência nestes sistemas temos que obrigar que sejam aceiteis ciber-ataques, cortes de serviços, catástrofes naturais e falhas de sistemas.

2.2 Segurança

Como apresentamos anteriormente, Segurança é um termo ambíguo que varia dependendo da situação e do indivíduo. Pode ser caracterizado por 5 aspectos: a Integridade, a Confidencialidade, a Autenticidade, o não Repúdio e a Disponibilidade [7].

Integridade - a informação não pode ser destruída nem corrompida, para que o sistema execute as suas funções correctamente;

Confidencialidade - a informação apenas deve ser disponibilizada segundo critérios rigorosos;

Autenticação - validação da identidade de um utilizador, dispositivo ou processo (verifica se uma entidade é quem afirma ser), caso contrário impede acesso não autorizado;

Não repúdio - impedir que uma entidade negue a execução de uma determinada acção;

Disponibilidade - os serviços oferecidos pelo sistema devem estar disponíveis sempre que tal seja necessário.

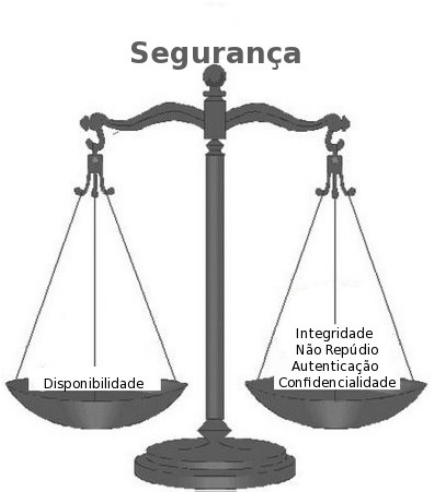


Figura 3 - Balança entre 5 características da Segurança

Como podemos ver na Figura 3 existe uma relação directa entre a Disponibilidade e as outras características, o que isto significa que não pode deixar de haver disponibilidade para se obter por exemplo, confidencialidade. No entanto, podemos reduzir a grandeza das outras quatro que mantemos a relação directa com a Disponibilidade. Isto não quer dizer que o façamos pois iria reflectir-se no nível de segurança.

Significa que o nível de Segurança pode variar e que devemos ter em conta :

- – **Riscos** associados a falhas de segurança. (subcapítulo 2.3);
- – **Custos** de implementação dos mecanismos de segurança;
- – **Benefícios** dos mecanismos de segurança, que implicam directamente um aumento de Confiança (capítulo 4).

Os mecanismos de segurança adoptados para atingir um determinado nível de segurança constituem a política de segurança.

"Uma política de segurança é um conjunto de regras formais que estabelecem os procedimentos a seguir pelos utilizadores dos recursos informáticos de uma organização." [8]

2.3 Riscos

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." [9]

Sun Tzu escreveu a Arte da Guerra [9] e desse livro podemos obter muitas lições importantes, como é o caso da definição de Risco. Como podemos ver na Figura 4, existe uma relação directa entre conhecermo-nos a nós (Vulnerabilidades), o nosso inimigo (Ameaças) e o Risco.

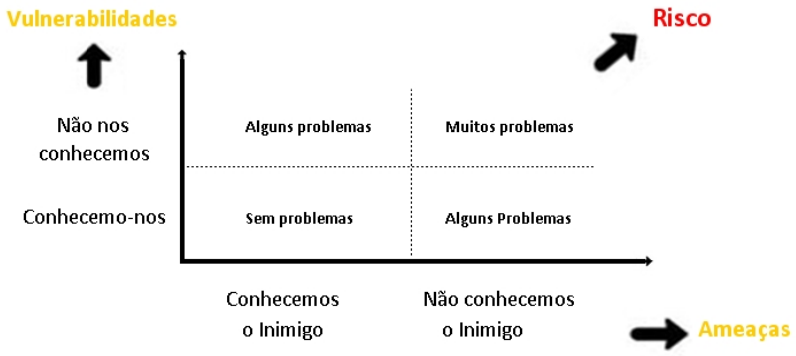


Figura 4 – Risco, Vulnerabilidades e Ameaças

Analisando a Figura 4 [9] apercebemo-nos que quantas mais Vulnerabilidades do sistema e mais Ameaças conhecermos, menor será o Risco. Esta relação já foi escrita e utilizada há mais de dois mil e quinhentos anos pelo militar Sun Tzu e é hoje usada em Segurança de Sistema Informáticos.

Vulnerabilidade

"Vulnerabilidade é uma fragilidade de um recurso ou grupo de recursos que pode ser explorada por uma ou mais Ameaças" [8]

Alguns exemplos de vulnerabilidades:

- Localização geográfica – se o local que está a ser monitorizado é remoto, vai implicar uma lenta reacção no caso de uma emergência;
- Excesso de credenciais – por exemplo, no caso de um acesso requerer uma password cujo tamanho mínimo é 20 caracteres, vai haver uma percentagem mínima de pessoas a decorá-la e uma percentagem alta a usar métodos inseguros para a guardar;
- Condições Climatéricas – no caso de uma intempérie, podemos obter danos no local que está a ser monitorizado que coloquem o sistema em mau funcionamento;
- Inexistência de sistema de autenticação – qualquer área que seja deve obrigar a uma restrição a pessoal autorizado. Tomamos essas medidas em nossa casa, no nosso carro, porque razão não o fazer nos nossos sistemas informáticos.

Ameaça

"Ameaça é uma potencial causa de um incidente, que pode provocar danos num sistema de informação ou numa organização" [8]

Alguns exemplos de Ameaças:

- Radiação electromagnética – pode simplesmente apagar todos os dados dos servidores, quer os centrais, quer os locais;
- Doença – no caso de doença de um técnico cujo trabalho é efectuar monitorização, o sistema deixa de ser vigiado;
- Picos de corrente – podem causar falha nos sistemas;
- Acesso não autorizado – significa que informações seguras deixam de o ser;
- Fogo – um resultado de uma vulnerabilidade que pode destruir todo o sistema.

Risco

"Risco é o resultado da combinação da probabilidade de ocorrência de um determinado evento e o impacto que este provoca numa determinada actividade" [8]

A relação entre os vários elementos de risco [10] pode ser examinada na Figura 5. Podemos ver que as ameaças e as vulnerabilidades aumentam o risco de segurança. Verificamos também que quando indicamos requisitos de segurança e esses são convertidos em medidas de segurança (controlos), reduzimos os problemas/riscos.

Figura 5 - Relação entre elementos de Risco

2.4 Sistemas inseguros – Exemplos

O primeiro exemplo que apresentamos data de 29 de Setembro de 2009 está relacionado com o nosso Presidente da República, Cavaco Silva. Neste exemplo, referimos o problema do acesso indevido ao computador pessoal do Presidente e aos computadores da presidência da república. Terá sido violada a

informação confidencial desses mesmos computadores, incluindo o correio electrónico do Presidente da República! Após uma análise extensiva deste caso, identificamos algumas soluções para o problema apresentado. A primeira será o uso de certificados digitais para assinar e cifrar os emails. Neste momento já existem dois milhões e trezentos mil portugueses com cartão de cidadão cujas funcionalidades incluem as referidas anteriormente. Apenas será necessária uma melhor informação aos utentes do cartão do cidadão e das suas funcionalidades no que diz respeito à segurança. Uma outra forma de manter segura a informação é o uso de discos cifrados em que apenas se consegue aceder à informação neles contida através de protocolos criptográficos. Avaliando esta situação de um ponto de vista mais geral, detectamos que houve falta de protecção de dados, falta de sensibilidade da criticidade dos mesmos, falta de encriptação e de autenticação. Se estes aspectos tivessem sido levados em consideração, esta situação teria sido evitada. Por fim, um ponto muito importante no desenrolar destes problemas, foi que não se seguiu um plano de contenção de crise. Normalmente passa por identificar, resolver, e apenas no fim apresentar o problema, sem dano à credibilidade da instituição [11].

Um segundo caso remonta a 12 de Junho de 2008, data em que foram encontrados num comboio em Inglaterra documentos secretos relacionados com investigações ao Iraque e Al-Qaeda. Nesta situação detectamos uma falta de protecção dos dados, falta de sensibilidade da criticidade dos mesmos nas pessoas que os transportavam e uma classificação indevida dessa mesma criticidade. Mais uma vez, indicamos que se estes aspectos tivessem sido levados em consideração, esta situação teria sido evitada [12].

Num último exemplo, vamos apresentar o caso dos ciber-ataques aos sistemas informáticos da Policia Judiciária, Brisa e Portugal Telecom, reportado em Janeiro de 2009 (JN). Estes ataques foram minimizados pelo Instituto de Tecnologias de Informação da Justiça (ITIJ) e foi garantido também que não estava em causa qualquer perda de informação. No entanto, através do Jornal de Noticias de dia 24 de Outubro de 2009, veio-se a saber que foram copiados [13]:

- documentos e informações altamente sensíveis do Ministério de Justiça;
- documentos da Direcção Geral de Registos e Notariado;
- programas internos, emails e documentos de funcionários do ITIJ;

Esta falha de segurança foi criada devido a engenharia social, falha na classificação da informação crítica, falha na protecção dos dados, falta de sensibilidade para essa mesma criticidade, falta de encriptação e falta de autenticidade dos sujeitos que podem tem acesso.

2.5 Elementos estatísticos – Segurança

Como vimos anteriormente a História pode-nos trazer mais-valias, desde ensinar novos métodos através de experiências passadas, como vamos ver de seguida, através de estatísticas onde podemos prever o que irá acontecer no futuro. A Figura 6 representa um gráfico das principais causas de falhas dos sistemas entre 1982 e 1996 nos Estados Unidos da América [14]. Este gráfico permite-nos antever que os principais problemas nos sistemas serão a falha de energia, problemas de hardware e fogo. Através deste gráfico e destas informações, podemo-nos precaver e estabelecer planos de prevenção.

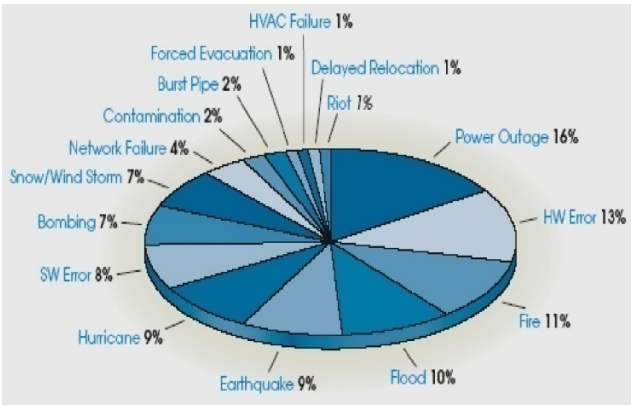


Figura 6 - Gráfico das principais causas de falha dos sistemas [14]

A empresa *Deloitte* apresentou o estudo de 2007, "Global Security Survey" [15] que entre outras estatísticas apresentou dados referentes às origens dos ataques externos (Figura 7) e internos (Figura 8). Após a interpretação dos dados, identificamos que os pontos de falha de intrusão externos são maioritariamente relacionados com engenharia social (vírus, spam e spyware) e má conduta de empregados.

External breach experience	One occurrence (%)	Repeated occurrences (%)
Viruses/Worms outbreaks	11	40
Email attacks (i.e. spam)	5	52
Spyware	6	26
Zombie networks	2	6
Denial of Service	7	8
Website defacement	2	2
Malicious remote access	4	4
Online extortion	1	1
Wireless network breach	1	1
Phishing/Pharming	5	35
Social engineering	5	17
Employee misconduct	8	31
Theft or leakage of intellectual property	5	8
External financial fraud involving information systems	5	13
Exposure of sensitive data through Web attacks	1	1
Physical threats	8	10
Accidental instances	4	14
Other form of external breach	3	2
Do not know	3	4

Figura 7 - Tabela de Falhas de Segurança de Origem Externa [15]

No caso de ataques internos, voltamos a encontrar a engenharia social (vírus) e a má conduta de empregados (perda de dados de clientes e fraude interna).

Internal breach experience

	One occurrence (%)	Repeated occurrences (%)
Viruses/Worms outbreaks	8	13
Wireless network breach	1	0
Loss of customer data/privacy issues	4	8
Internal financial fraud involving information systems	7	11
Theft or leakage of intellectual property (e.g. customer leakage)	3	7
Accidental instances	5	13
Other form of internal breach	2	10
Do not know	3	2

Figura 8 - Tabela de Falhas de Segurança de Origem Interna [15]

2.6 Conclusão

Existem sistemas inseguros em todo o lado, mas o que falta é determinar o que precisa realmente ser protegido e que soluções podem evitar essa insegurança. Podemos aprender bastante com os exemplos de falha de segurança (internos e externos). O primeiro passo para a criação de um sistema seguro é determinar os riscos associados a falhas de segurança e em seguida, implementar mecanismos de segurança, verificando quais os benefícios e se implicam directamente um aumento de Confiança.

A conclusão a que chegamos, em relação ao estado da segurança dos sistemas actuais, é que existe uma tentativa para um aumento dessa segurança. No entanto, continuamos a verificar a existência de problemas no que diz respeito ao âmbito mal escolhido ou à inexistência da identificação de riscos. Estas situações tendem a ser resolvidas com soluções que não são devidamente planeadas (soluções proactivas), o que pode levar a uma solução ineficaz, ou simplesmente a uma solução reactiva.

3 e-Health

3.1 Introdução

Nos dias de hoje, em pleno século XXI, começamos a analisar a saúde com outros olhos. Começamo-nos a preparar para as doenças, não esperamos que elas apareçam, tentamos erradicá-las antes, como por exemplo com as vacinas. No entanto, podemos ir mais além, utilizando o exemplo de um carro: quando vemos uma luz vermelha a acender com a indicação que estamos a ficar sem óleo, ou travões, (significa que um sensor detectou uma anomalia) sabemos que nos devemos deslocar a um mecânico, de forma a prevenirmos problemas futuros. No caso da saúde, podemos e devemos fazer o mesmo. Se tivemos sensores específicos que analisem por exemplo o sangue, o coração ou outros órgãos, podemos antecipar graves problemas de saúde.

E-Health ou *eHealth* significa "Electronic Health", ou seja, existe uma ligação directa entre a saúde e as tecnologias de informação. Vamos analisar neste capítulo o "State of the Art":

- na secção 2.2, vamos aduzir os vários sistemas de saúde com assistência remota;
- na secção 2.3, vamos apresentar algumas empresas que estão a trabalhar no âmbito da Telemedicina;
- na secção 2.4, vamos expor os requisitos necessários para termos um sistema de saúde com assistência remota;
- na secção 2.5, vamos analisar os sistemas existentes em termos de segurança, o que existe;
- por fim, vamos explicar o que são ambientes inteligentes e ambientes de vida assistidos.

3.2 Sistemas de assistência remota

O uso de um sistema de assistência remota pode simplesmente fazer uma chamada para um centro de suporte de um operador móvel, resolvendo assim a falta da opção de envio de mensagens no telemóvel. No entanto, no âmbito desta tese, vamos analisar apenas as soluções relacionadas com saúde. Existe neste momento em Portugal, devido à problemática da Gripe A, algo semelhante: a "Linha Saúde 24"

que rapidamente indica ao cidadão o que fazer quando se tem dúvidas acerca da saúde. No entanto, este sistema é uma solução activa, o que obriga a uma acção do cidadão, ou seja, na equação *dúvida saúde* vs *assistência*, a dúvida só é esclarecida quando efectuarmos a chamada e somos atendidos por um operador qualificado.

No caso de termos um problema de saúde que nos impede de comunicar ou falha na mobilidade, estamos a acrescentar mais uma variável ao problema *dúvida* vs *assistência*. Como solução, existem pelo menos duas empresas em Portugal (Portugal Telecom[16] e Primus Care[17]) e uma empresa em Inglaterra (QuickSafe) [18] que fornecem uma alternativa. O uso de uma pulseira ligada directamente a um telefone fixo (Figura 9), ou ligada a um telemóvel (Figura 10), que quando accionada efectua uma chamada para um centro de suporte que valida se existe a necessidade de intervenção ou não.

Nalguns casos este atendimento é feito por um operador, mesmo que o botão seja premido por acidente, existe um acompanhamento, uma avaliação humana da situação, podendo chegar a servir para alguma companhia.

Figura 9 - Pulseira e unidade central rede fixa (Primus Care)

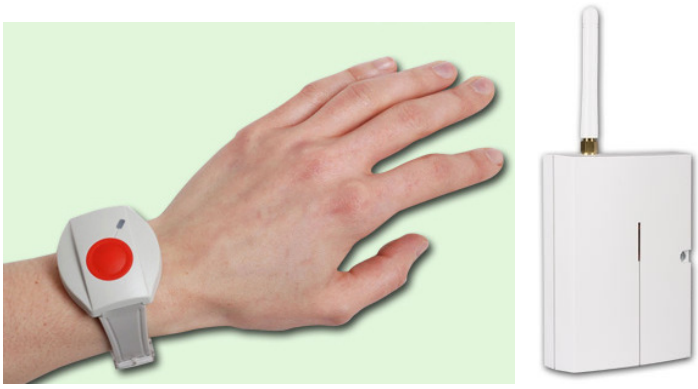


Figura 10 - Pulseira e unidade central GSM (Quicksafe)

Vital Jacket ® é um projecto iniciado na Universidade de Aveiro e que originou um produto na empresa *Biodevices*. O objectivo deste colete é monitorizar os sinais vitais do sujeito de forma a precaver futuros problemas, ou no caso falha de sinal, um aviso imediato aos médicos/enfermeiros para tomarem as devidas acções. (Figura 11 – *VitalJacket* ®) [20]

Figura 11 - VitalJacket ®

3.3 Telemedicina / Telesaúde

Quando a distância é uma barreira, procuram-se alternativas para quebrar esses limites. A falta de recursos humanos especializados em determinadas partes do mundo obrigou a uma solução, que para já, passa por uma assistência remota. A Telemedicina, não é mais do que a utilização das modernas tecnologias de informação e telecomunicações no fornecimento de informações e atenção médica a pacientes localizados à distância (Figura 12) [21].

Figura 12 - Optometrista remoto

Existe um mito urbano, segundo o qual, o uso do telemóvel para abrir um carro quando nos esquecemos das chaves em casa, pode ser efectuado, desde que alguém em casa use o segundo comando/chave do carro através do telefone. A ideia da Telemedicina assenta no mesmo princípio, ou seja, o ouso do telefone, a Internet, ou outros meios de comunicação para nos aproximarmos dos especialistas (psicologia, clínica geral, reabilitação, cardiologia, pediatria, obstetrícia, ginecologia, neurologia, terapia da fala, optometrista, oftalmologista, etc) para nos aproximarmos dos médicos que nos podem ajudar a resolver os problemas de saúde (Figura 12).

Em Portugal existe um projecto chamado *PEDITEL* [22] cujo objectivo é interligar o Hospital Pediátrico de Luanda ao Hospital Pediátrico de Coimbra (Figura 13).

Figura 13 - Platafoma Medigraf (sucursal da PT Inovação)

3.4 Requisitos para um sistema de Telemedicina

A assistência a pessoas necessitadas é normalmente feita por familiares ou centros de assistência. No entanto, estas duas soluções não têm vindo a responder ao problema devido às seguintes situações:

- ao aumento de pessoas com necessidades (que está directamente relacionado com o aumento do numero de pessoas idosas);
- a diminuição do tempo que os familiares dispõem para acompanhar pessoas com necessidades;
- a um insuficiente número de centros de assistência;
- aos avanços na Medicina, pois hoje em dia, já é possível viver, em casa, com doenças que antigamente exigiam internamento ou cuidado permanente, ou porque simplesmente as pessoas que tinham problemas graves não tinham soluções médicas, agora existentes.

Para combatermos estas situações, a assistência tem que ser melhorada usando tecnologia sem descorarmos o contacto humano. Recorrendo a tecnologias já existentes, podemos obter soluções que

permitem cuidados suficientes de forma remota aos necessitados, que lhes permite não saírem do seu meio ambiente, da sua casa. No entanto, temos que ter em atenção o contexto de cada sujeito, porque alterações dramáticas podem ter resultados drásticos, por exemplo [16-20]:

- os idosos, que tem necessidades especiais no que diz respeito à medicação, por vezes podem-se esquecer de a tomar, ou alterar a hora da mesma, ou podem simplesmente não ter a habilidade motora para o fazer. Por estas razões, sempre que possível devem-se manter na sua casa, mantendo as suas ligações sociais, impedindo desta forma problemas relacionados com ansiedade e solidão;
- os familiares são por vezes, além do sujeito, os mais interessados em serem mantidos a par do estado de saúde do sujeito e que por vezes podem ser um elo de ligação entre eles e o sistema, monitorizando e vigiando de forma a servirem de elemento de socorro em emergências;
- o ambiente ou o lar, visto que a palavra lar significa local onde o sujeito vive e não a sua casa, é necessário que o ambiente onde vive tenha os requisitos necessários para manter a segurança e o nível de saúde que pretendemos;
- os centros de assistência, além de servirem para monitorizar o bem estar do sujeito devem mantê-lo em ligação social e recordá-lo da sua agenda, mantendo-o ocupado;
- os centros de lazer são muito importante pois mantêm o sujeito ocupado negando a possibilidade de ansiedade ou solidão, com os tempos livres bastante preenchidos com eventos sociais, desporto, actividades culturais, etc;
- os centros de saúde, devem além de monitorizar a saúde do sujeito, fornecer recomendações sobre que medicamentos, exercício físico, etc tendo como base os seus dados médicos;
- os serviços, permite ao sujeito um meio especializado de comprar o que precisa de uma forma fácil e sem complicações;
- a segurança, a privacidade e a confiança são aspectos críticos nesta tese e que devem ser sempre tidos em conta no que trata comunicação e armazenamento de informações médicas.

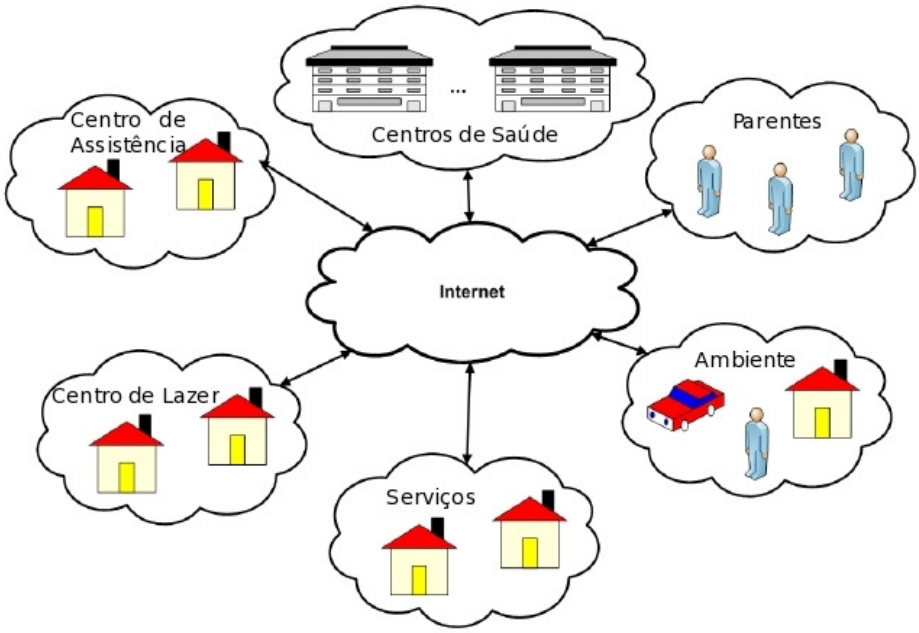


Figura 14 - Cenário genérico de um sistema de Telemedicina [22]

De forma a obtermos uma distribuição geográfica vasta, não só em áreas urbanas, mas também em áreas rurais, devemos usar a Internet com ponto central das comunicações por é um meio barato e abundante nos dias de hoje.

3.5 Segurança e Confiança

Um sistema de *e-Health*, um sistema de Telemedicina, só é aceite pelo público se houver confiança.

A confiança estará dividida em três esferas, a Individual, a do Sistema e a da Comunidade que serão melhor analisados no próximo capítulo. No entanto, vamos fazer uma pequena apresentação deste tópico [23].

A confiança a nível Individual está directamente ligada à segurança que o sistema nos transmite através de experiências passadas, ou por simples observações actuais. Ao nível do Sistema há a introdução dos requisitos tecnológicos para a obtenção da segurança. Por fim, ao nível da Comunidade, a sociedade com leis e regras permite-nos obter mais algumas garantias de segurança.

Um dos pontos mais importantes que vamos analisar é o sistema e as suas áreas, a garantia de confidencialidade, integridade dos dados, autenticação, não repúdio e infra-estruturas de confiança [7, 23] :

- confidencialidade – assegurar que a informação é apenas acedida por entidades autorizadas;
- integridade – certificar que não houve alteração de dados, ou seja, que não foram adicionadas ou removidas informações;
- autenticação – permite assegurar que as entidades são quem dizem ser;
- não repúdio – está ligado com a certeza, com a prova, de que quem efectuou uma determinada acção não a pode negar;
- infra-estruturas de confiança – são entidades cujos procedimentos para definir confiança são auditados e aceites como seguros pela comunidade;

Projectos existentes com falta de segurança

De forma a melhor compreendermos todos os requisitos necessários para que exista confiança, vamos analisar primeiro o que implica não ter segurança num sistema de saúde. Se analisarmos o serviço do *Primus Care*, constatamos que o equipamento que disponibilizam, apenas efectua a chamada se, se carregar num botão de pânico. Neste sistema verificamos que podem acontecer uma serie de situações:

- falha de comunicações entre os dispositivos, o que implicaria uma falha total no sistema, deixando o sujeito sem ajuda;

- alteração no equipamento para fazer uma chamada para outro número, que viria a impedir que ajuda chegasse;
- chamadas para a central indicando ser o número de origem do sujeito poderiam criar um ataque de DOS (que explicarei mais à frente);

Estes ataques podem acontecer e iriam minimizar a confiança no sistema. A situação mais normal seria a primeira, pois se o sujeito saísse da área coberta pelo sistema, ficaria sem apoio e que facilmente seria detectada por este.

Uma outra situação seria a solução do *Quicksafe* que usa o GSM para fazer chamadas de pânico. No entanto, nesta solução encontramos dois problemas, a necessidade de rede GSM para fazer as chamadas de emergência e a obrigatoriedade de transportar o equipamento transmissor GSM que em certas situações pode ser um obstáculo. Numa primeira análise, chegamos à conclusão que os sujeitos iriam aceitar a mais-valia da solução. No entanto, com o passar do tempo, iriam fazer pequenas correcções (não carregar a caixa, não recarregar as baterias do equipamento, não verificar se as pilhas estão carregadas) à solução, que poderiam ser fatais.

3.6 Ambientes Inteligentes e Ambientes de Vida Assistidos

3.6.1 Ambiente Inteligentes

Em 1956, na conferência de *Dartmouth*, John McCarthy avançou com o termo Inteligência Artificial (IA) e referiu que "Inteligência Artificial é a ciência e o engenho de criar máquinas inteligentes" [25]. Foi em 1968 com o primeiro filme "2001 Odisseia no Espaço" de Stanley Kubrick, que se generalizou o termo IA. A história passava-se numa nave cujo computador de bordo, o HAL 9000, já tinha Inteligência Artificial. Apesar de usar para o mal, usava todos os sensores e dispositivos da nave, com o objectivo de gerir um ambiente, um Ambiente Inteligente (AmI). A ideia foi ter controlo sobre tudo o que se passava na nave, naquele ambiente, de forma a melhor servir o um objectivo. Esse objectivo devia ser servir o Homem, ao contrário do que aconteceu.

Como podemos ver existe uma ligação directa entre o *IA* e o *AmI*, pois o AmI é uma especialidade de IA. Neste novo paradigma (AmI), os computadores vão tomar um papel mais activo, mais simples, mas relacionado com a nossa assistência. Vamos deixar de ter cartões perfurados, teclados ou ratos, vamos simplesmente aparecer numa sala, e os nossos gostos e particularidades vão ser reflectidos no ambiente. Por exemplo, estamos cansados e é tomada a decisão pelo AmI em colocar as luzes com menos intensidade, uma música mais calma, mas dentro dos nossos gostos sem qualquer necessidade de interacção nossa com o sistema.

Alguns exemplos, são as casas inteligentes como o *Mordomus* [26] ou a casa do Bill Gates (Figura 15) que usam a tecnologia conhecida como Domótica (Figura 16). Ou então hospitais ou lares como o que construído pela empresa *MEDeTIC* (Figura 17) [27].

Figura 15 - Modelo da casa de Bill Gates

Figura 16 - Arquitectura de uma casa inteligente

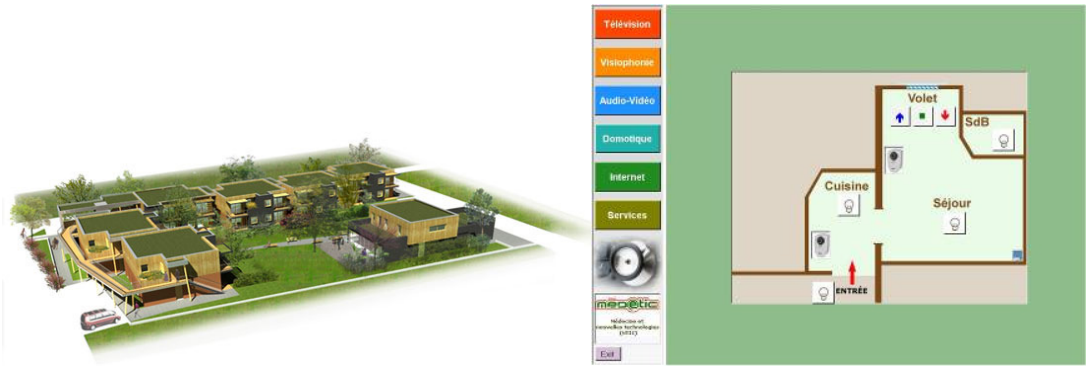


Figura 17 - Lar de Idosos da MEDeTIC com o uso de domótica

3.6.2 Ambiente de Vida Assistidos

Sendo um do principais objectivos do *AmI* a segurança e se adicionarmos o factor saúde obtemos os Ambiente de Vida Assistidos (AVA). Um AVA pode e deve ser usado por pessoas que tenham problemas de saúde, por idosos, por pessoas com deficiências, com o objectivo de lhes dar uma vida o mais normal possível com segurança. De forma que os parentes se sintam confiantes no sistema, se sintam seguros.

A segurança não é o único ponto positivo do AVA, mas o conforto, a calma e o ambiente familiar que rodeia o sujeito são outras vantagens deste subdomínio [22].

Os *AVA* não são só usados nos lares dos sujeitos, mas também podem ser usado em hospitais, centros de lazer e lares de terceira idade. Nestes estabelecimentos, os sistemas não são só apreciados pelos sujeitos, mas também pela equipa técnica o que origina a um melhor tratamento médico.

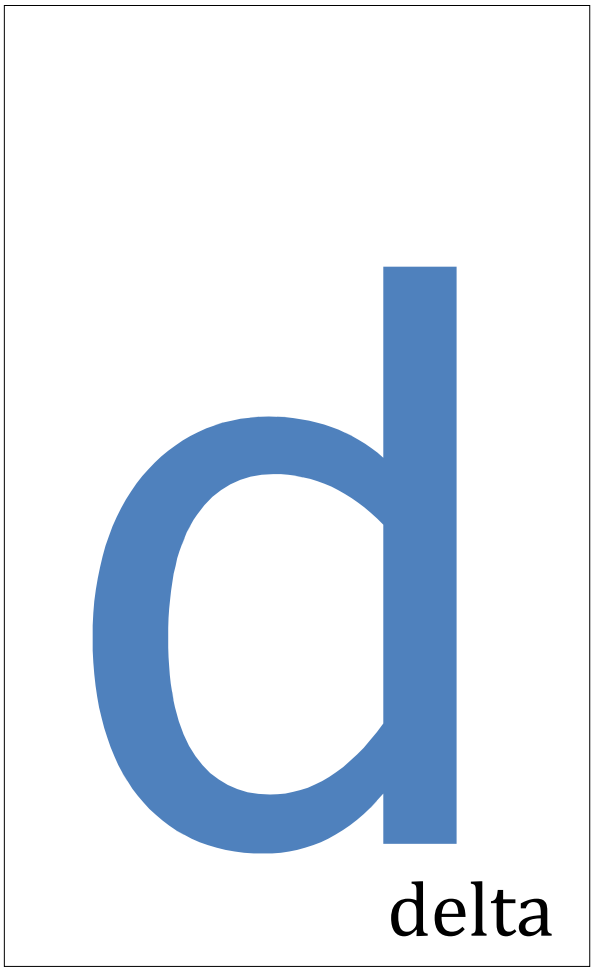
Um ponto fulcral neste tipo de projectos é a forma como é feita a comunicação. Já referimos que deve ser feita usando a Internet, mas será seguro? Podemos dar garantias aos utilizadores de que os seus dados são reais, que as acções são as correctas e que as decisões são tomadas dentro do maior sigilo possível? Estas questões serão debatidas e analisas no próximo capítulo.

3.7 Conclusão

Em suma, neste capítulo apresentamos a saúde electrónica, *e-Health*. Exploramos as variações como a *TeleAssistência* e *TeleMedicina*, apresentamos algumas soluções já disponíveis ao público em geral. Identificamos os pontos que obrigaram a estes novos avanços e os requisitos dos vários sistemas. Estudamos a ligação entre a Inteligência Artificial e os Ambientes de Vida Assistidos e por fim identificamos alguns casos de sucesso relacionado com as técnicas de domótica.

Estudamos também as diferentes vertentes do e-Health e tecnologias envolvidas de forma a determinar as suas vulnerabilidades.

4 Confiança



4.1 Introdução

Conhecer todos os participantes de um evento, ter a certeza das suas boas intenções e que elas não detêm uma agenda privada, é a base da Confiança. Podemos dizer que confiamos em alguém baseado nas nossas experiências pessoais que recaem na crença, observação, razão, estereótipos pré-definidos, experiências passadas, indicações de outros (que nós já confiamos baseado no mesma lista de experiências), mecanismos de confiança baseados em reputação ou em empresas de confiança. Baseado em *Ramchurn et al*, 2004, implementamos a ideia da confiança baseada em três esperas [2, 23]:

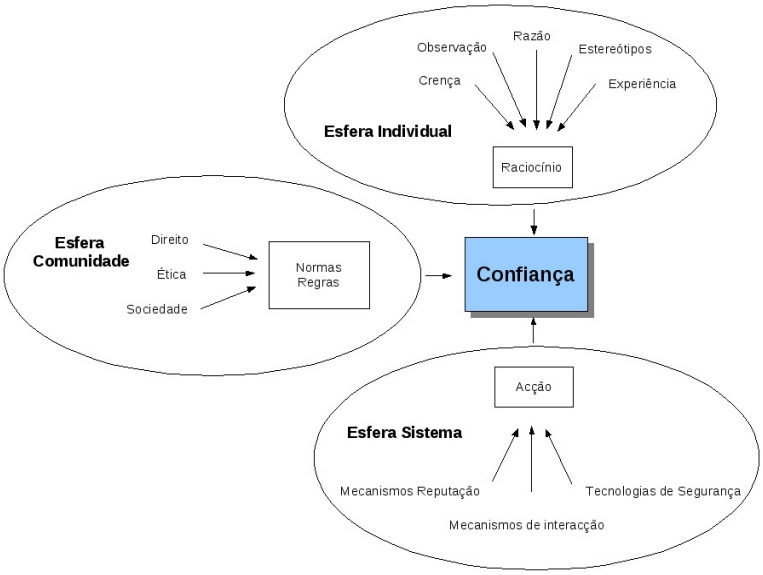


Figura 18 - Diagrama com as três esferas de Confiança

"Trust is a belief an agent has that the other party will do what it says it will (being honest and reliable) or reciprocate (being reciprocative for the common good of both), given an opportunity to defect to get higher payoffs." [23]

Como podemos ver na Figura 18, temos três níveis de Confiança:

O primeiro nível é o da Razão, ligado com funções cognitivas do pensamento humano. As características da condição humana: razão, observação, experiência, crença e a definição de estereótipos fazem parte da esfera única, individual e pessoal. Por isso, usado como o básico da definição de Confiança, cada um deles formaliza a sua aproximação ao problema.

Acção é a palavra-chave para o segundo nível. Nesta esfera, o Sistema é baseado em algoritmos de comunicação, na confiança desses algoritmos, na reputação dos mecanismos envolvidos e nas tecnologias de segurança.

Finalmente, o terceiro nível, o Standard e as regras criam um balanço entre as duas esferas anteriores. O país e as leis da sociedade definem, por exemplo, quais serão os requisitos técnicos necessários para manter a confiança, em termos dos protocolos e agentes de reputação.

4.2 Individual

Como apresentado anteriormente a esfera Individual está interligada com uma série de características do indivíduo ou do agente. Vamos agora enunciar cada um deles e apresentar exemplos [23]:

- **Observação** – quando falamos de observação estamos a falar de várias formas de obter dados de os receber para depois os processarmos e obtermos as devidas elações;
- **Razão** – usando a sua própria definição: é a faculdade de raciocinar, de apreender, de compreender, de ponderar, de julgar, a inteligência;
- **Experiência** – da mesma forma que existe um Lei americana, da jurisprudência, o indivíduo, deve aprender com a experiencia passada, e agir em concordância;
- **Crença** – apesar de hoje em dia se associar esta palavra a crença religiosa (no seu extremo ao fanatismo religioso), esta característica também está associada ao acreditar positivo, confiar em alguém;

- **Estereótipo –** é uma forma de avaliar, de julgar certas pessoas, assumindo uma determinada acção relacionada com a forma de vestir, da idade de alguém, a cor, etc. É uma forma de racismo, no entanto, não deixa de ser uma forma de análise do meio ambiente.

Depois de identificar todas as características, há que determinar uma forma de as contabilizar, de obter um grau de confiança. Temos que criar métricas para cada uma delas, para que os Agentes possam tomar decisões dependendo dos dados da esfera Individual.

4.3 Sistema

Ouvimos falar do Sistema, sem nunca nos preocuparmos com o mecanismo que utiliza para aumentar a nossa segurança. Num sistema de detecção de incêndios, além do alarme sonoro, podemos ter várias soluções com por exemplo: um alarme silencioso que alerta os bombeiros ou um sistema automático que acciona os chuveiros anti-fogo. Neste capítulo, vamos analisar os mecanismos do sistema que nos permitem confiar nele. Utilizando novamente o exemplo de um fogo: Será que os bombeiros são de confiança? Será que não haverá falta de água quando mais precisamos? Num caso de alarme quem é que devemos avisar primeiro, quem terá a melhor solução?

Protocolos de interacção

Algoritmos que permitem e/ou impedem que agentes mintam ou especulem sobre o seu funcionamento enquanto comunicam. Uma das medidas é a criação de uma sintaxe e de uma semântica para atribuição de valores entre os agentes.

Os protocolos de interacção entre agentes (ou protocolos de comunicação) são responsáveis por governar e gerir as trocas de mensagem dentro de uma conversa. Uma conversa é formada por um conjunto de mensagens trocadas entre os agentes com o propósito de se alcançar um determinado objectivo. A utilização de um protocolo de interacção aumenta o desempenho desta comunicação já que este permite

o estabelecimento de objectivos em comum e determinação das tarefas conjuntas, evitando-se assim conflitos desnecessários.

Os protocolos de interacção normalmente obedecem a um conjunto de regras pré-estabelecidas. Algumas destas regras são: cooperação (os agentes trabalham com um objectivo comum), coordenação (os agentes juntam-se de modo a explorar interacções benéficas e a evitar as prejudiciais) ou negociação (os agentes interagem à procura de chegar a um acordo que seja aceitável para todas as partes envolvidas).

Uma proposta recente, recomendada pela *FIPA* (Foundation for Intelligent Physical Agents) tem se tornado num standard para a representação destes protocolos de interacção [28]. Trata-se da Agente Unified Modeling Language (AUML) [29] uma adaptação da técnica de modelagem de orientação a objectos UML (Unified Modeling Language).

Mecanismos de reputação

Entre agentes, existem soluções que permitem determinar qual o melhor, o que nos fornece qual a melhor solução para um determinado problema. No entanto, ao usarmos mecanismos de reputação, temos que definir regra [31, 32]:

- Dificuldade na mudança de identidade;
- Novos agentes não podem ser penalizados por não terem uma reputação;
- A avaliação feita por agente com altas reputações deve ter maior peso;
- Os agentes devem poder manter um histórico de avaliações, mas devem ter maior consideração pelas mais recentes.

Tecnologias de Segurança

Este último ponto, apesar de ser analisado em mais profundidade no próximo capítulo, é o que irá manter a segurança do sistema. Permitindo que se obtenha sempre a identidade dos agentes, que haja sempre um controlo de acessos, uma integridade dos conteúdos comunicados, privacidade dos

mesmos e por fim um não repúdio dos dados, isto sempre sem descorar a disponibilidade do Sistema.

4.4 Comunidade

Para melhor percebermos o que pretendemos com a esfera da comunidade, vamos apresentar alguns exemplos de como a confiança é importante e é fornecida pela sociedade.

O primeiro caso está relacionado com uma comunicação entre duas pessoas usando telefones e/ou telemóveis que confiam no meio de comunicação que escolherem para comunicarem. No entanto, é bastante fácil ter acesso a essa comunicação, como podemos ver na Figura 19, através de vários equipamentos que podem aceder a essa conversa. No entanto, e como existem leis que impedem as escutas, tornando-as ilegais, estas duas pessoas confiam no meio de comunicação que escolheram [33, 34].

Figura 19 - Equipamentos para escutas de comunicações

Um segundo caso, é o uso de certificados digitais. Sempre foi possível o uso de certificados digitais, para assinar e-mails e outros documentos. No entanto, apenas depois de ser publicada o artigo 3º do DL 62/2003 no qual é dado valor legal a determinadas acções quando usados os mesmos certificados, o seu uso massificado. Essa lei indica que quando criada uma assinatura electrónica qualificada e certificada por uma entidade certificadora, o documento electrónico tem a força probatória de um

documento particular assinado, nos termos do artigo 376º do Código Civil. Estamos, por exemplo, a falar do uso de certificados digitais para envio de propostas para a plataforma electrónica de contratação pública do governo [35].

4.5 Confiança em Ambientes de e-Health

Quando o nosso principal objectivo é criar um sistema de saúde de confiança, precisamos de nos assegurar, por exemplo, que todas as comunicações são confiáveis e seguras. Devemo-nos assegurar que todos os eventos despoletados pelos agentes intervenientes são, sem margem de dúvidas, correctamente providenciado ao sistema, sem a possibilidade de falsos positivos ou falsos negativos. Falsos positivos são eventos que não foram bloqueados pelos mecanismos de segurança do sistema. O oposto é quando temos agentes de confiança, cujos eventos são bloqueados e a sua funcionalidade removida.

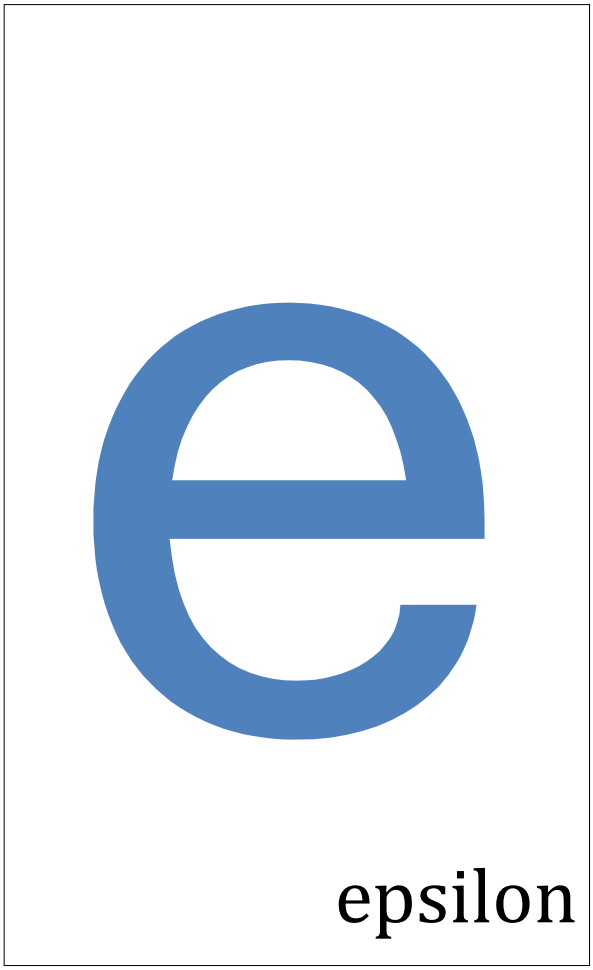
De forma a resolver os problemas de segurança associados a transacções electrónicas no mundo digital, recorremos à Criptografia. Esta ciência assegura a protecção da informação usando várias funções/algoritmos matemáticos para cifrar e decifrar mensagens, estabelecer comunicações, identificar agentes, etc. Estas acções permitem a prevenção do acesso e alteração da informação por terceiros. Em certas situações saber a origem de uma determinada mensagem é suficiente para confiarmos nela. No entanto, noutras situações, como administração de drogas, a falta ou o excesso na toma pode causar problemas sérios ao paciente.

Existem muitas circunstâncias que têm que ser tidas em conta. Como relacionamos a segurança e os sistemas de saúde? Devemos aprender uma miríade de informações ao nível legal, por exemplo, simplesmente se guardamos ou distribuímos informação de segurança de um determinado paciente.

4.6 Conclusão

Para obtermos um sistema de *e-Health* credível, precisamos de investigar e analisar todas as soluções de segurança existentes para todos os equipamentos usados. Abordou-se a Confiança subdividida em três níveis. Devemos aprender com a História e com as experiências que dela podemos retirar, usando para isso os exemplos de problemas antigos. As novas tecnologias e a Sociedade podem e devem dar uma grande ajuda, como veremos nos próximos capítulos.

5 Caso de Estudo - VirtualECare



5.1 Introdução

O objectivo do projecto *VirtualECare* é apresentar um sistema multi-agente inteligente, não apenas para comunicar com os clientes (quer os idosos ou os seus familiares), mas também para interligar com outros sistemas computacionais em diferentes instituições de saúde, centros de lazer, ginásios ou lojas. O projecto *VirtualECare* usa uma arquitectura distribuída, sendo que os vários componentes se encontram interligados por uma rede (exemplo: LAN, MAN, WAN), e cada um tem um determinado papel (Figura 20) [36-39]:

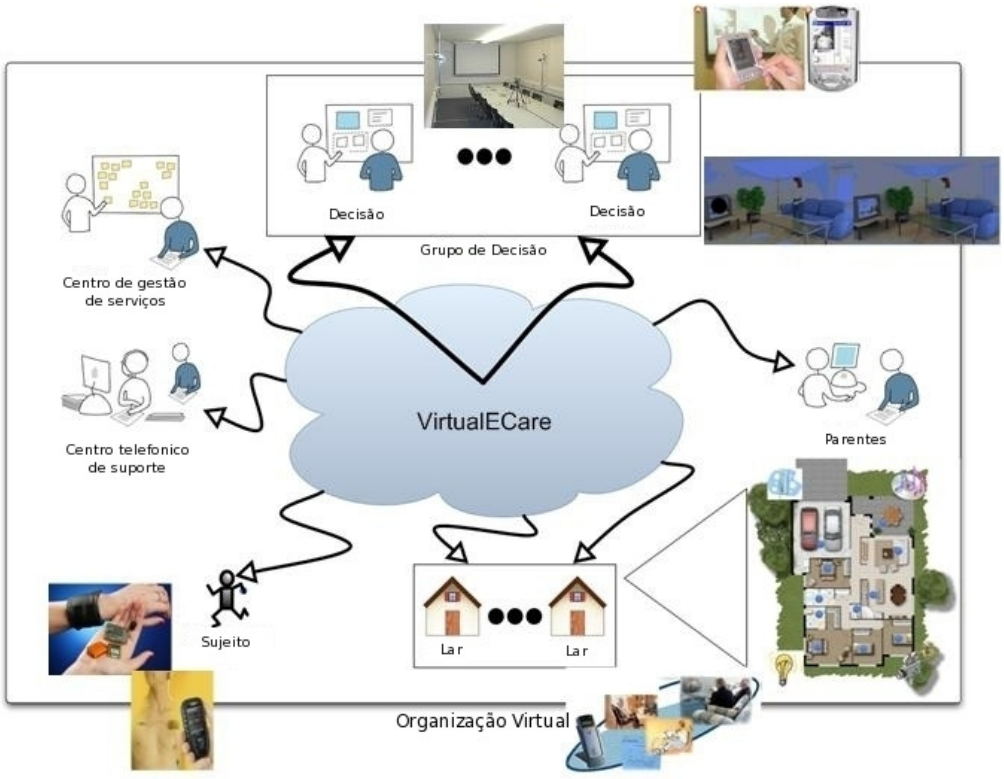


Figura 20 – VirtualECare

Sujeito – Idosos com necessidades de saúde especiais, cujos dados críticos são enviados ao ***Centro de Gestão de Serviços*** e ao ***Grupo de Decisão do Sistema***;

- ***Lar –*** o Lar do ***Sujeito***. Os dados aqui recolhidos são enviado para ***Grupo de Decisão do Sistema*** através do ***Centro Telefónico de Suporte*** ou através do ***Centro de Gestão de Serviços*** (que será responsável pelas decisões tomadas);
- ***Grupo de Decisão –*** É responsável por todas as decisões tomadas na plataforma do *VirtualECare*;
- ***Centro de Gestão de Serviços –*** Entidade com todo o poder computacional e os recursos humanos qualificados capazes de receber e analisar os dados mais heterogéneos e tomar as necessárias acções de acordo;
- ***Parentes/Familiares do Sujeito*** – Familiares que podem e devem ter um papel activo na tarefa da supervisão dos seus entes queridos, providenciando informações complementares preciosas.

Para o Grupo de Decisão do Sistema poder tomar as suas decisões, é necessário ter um perfil digital do Sujeito, de forma a poder perceber as necessidades especiais dele/dela. Nesse perfil podemos ter vários tipos de dados, desde os registos electrónicos de saúde às suas preferenciais e experiencias pessoais. (por exemplo: musicais, gastronómicos). Isto pode providenciar ferramentas e métodos para criar um ambiente que pode melhorar a qualidade de vida, segurança e qualidade dos cuidados de saúde. [38,40]

5.2 Infra-estrutura

Considerando o cenário acima mencionado, e tudo o que implica, desenhamos uma genérica, configurável, flexível e escalável infra-estrutura apresentada na Figura 21. É expectável que além dos mencionados, o número de serviços cresça progressivamente. Estes serviços devem, e vão ser desenvolvidos como "Web Services", permitindo o desenvolvimento de software em várias plataformas, usando mensagens comuns [37].

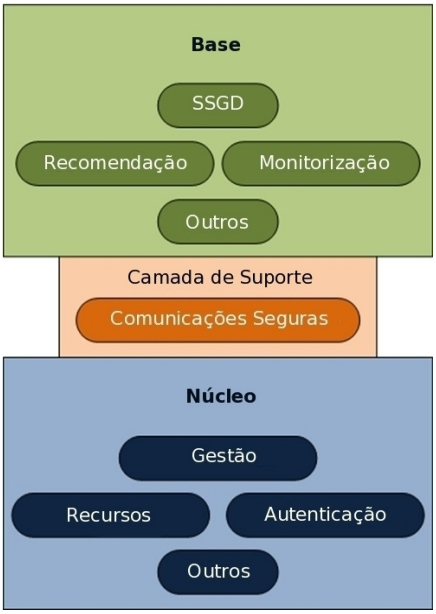


Figura 21 - VirtualECare Infra-estructura

Os componentes fundamentais da infra-estrutura [38] proposta são:

- ***Comunicação Seguras –*** para que todos os componentes interajam de forma segura é mandatório que haja uma camada de segurança para as comunicações;
- ***Gestão*** – responsável por configurar e monitorizar todos os componentes envolvidos;
- ***Recursos*** – responsável pelo registo de todos os componentes no sistema e pela gestão do catálogo de recursos;
- ***Autenticação*** – cada componente deve-se autenticar de forma a poder interagir com os outros;
- ***Recomendação*** – responsável pelas recomendações para resolução de problemas;
- ***Monitorização*** – responsável por interagir com todos os sensores e reportar os resultados ao GDSS;
- ***SSGD*** – responsável por tomar as decisões.

5.3 Arquitectura

Consideramos que a Arquitectura do *VirtualECare* é distribuída, composta por uma serie de elementos diferentes, eventualmente separada geograficamente (Figura 22). Também é considerada dinâmica pois existem elementos/agentes que podem entrar ou sair a qualquer altura, logicamente, geograficamente ou os serviços que fornecem podem variar. Os componentes principais da arquitectura são o Sujeito, a seu Lar, o módulo de Monitorização e o Grupo de Decisão. Cada módulo da arquitectura pode variar ao nível das funcionalidades ou da linguagem do software, daí o nome de arquitectura heterogenia. Estes são os assuntos principais que foram analisados e estão descritos de uma forma detalhada nesta secção: como distribuímos a nossa arquitectura, modular, dinâmica, extensível, flexível, escalável e compatível. Para obtermos isto, tivemos que adoptar tecnologias abertas, largamente usadas e alguns standards, como o OSGI (Open Services Gateway Initiative [40]), R-OSGI (Remote OSGI), FIPA (Foundation for Intelligent Physical Agents) [28,29] e Web Services.

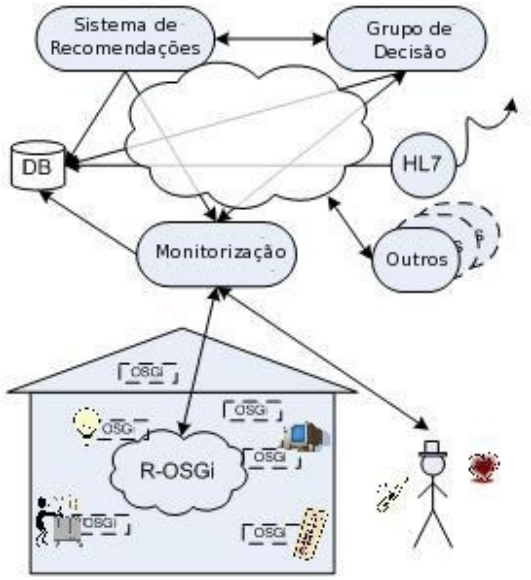


Figura 22 - VirtualECare Arquitectura

Como foi referido anteriormente, de forma a permitir a interoperabilidade entre várias plataformas, foi decidido a disponibilização dos vários componentes do sistema através de Web Services. Os Web Services podem ser vistos como uma forma de partilhar informações através de uma rede sendo independente da

plataforma usada, sendo o ideal para este tipo de sistemas. Cada um dos componentes que providencia informação declara Web Services que serão requeridos pelos outros componentes que por sua vez necessitam dessa mesma informação. Um componente pode, no entanto, ser servidor e cliente ao mesmo tempo. O Sistema de Recomendações, por exemplo, usa Web Services providenciados pela Casa (Lar) e pela Base de Dados (Database) e por outro lado providencia um Web Service que é usado pelo Grupo de Decisão. O protocolo de comunicação e exemplos de sequências das mensagens necessárias para todos os componentes trabalharem em conjunto serão analisados mais à frente.

Na Figura 22 podemos observar uma vista simplificada da nossa arquitectura. As setas representam Web Services que permitem a interacção entre vários componentes através da troca de informações. As setas podem ser vistas como "usando um serviço de" apontando do cliente para o servidor. A Casa (Lar) é um pouco mais de detalhada, mostrando o OSGi e os sub-componentes do R-OSGi responsáveis pela intercomunicação entre os vários elementos.

Vamos agora descrever as tecnologias usadas nos componentes, para isso vamos fazer uma observação mais pormenorizada da arquitectura. Neste nível, dois bem conhecidos standards foram usados: *OSGi* e *R-OSGi* são iniciativas com o intuito de estabelecer standards em programação Java, altamente específicas, partilhando as classes *Java*, que devem seguir o paradigma de uma plataforma de serviços. O uso destas tecnologias vai permitir aos programadores construir aplicações *Java* de uma forma modular. Os módulos resultantes são chamados de "bundles" que não só disponibilizam Web Services, como também estão preparados para os usar/aceder. Em *OSGi*, um "bundle" pode ser instalado, arrancado, parado ou desinstalado com o sistema em funcionamento sem necessidade de qualquer reinício do sistema, o que faz com que tecnologias baseadas em *OSGi* sejam muito modulares e dinâmicas.

R-OSGi é uma extensão do *OSGi*, que permite aceder a serviços providenciados por implementações remotas de *OSGi*, de uma forma totalmente transparente, como se tratasse de um serviço local. Mas para que servem estas tecnologias no nosso caso?

OSGi e *R-OSGi* são usadas no nosso projecto de forma a realizarmos dois objectivos em cada nível dos componentes: garantir a compatibilidade e a comunicação entre as diferentes partes que definem

cada componente e estabelecer uma organização lógica dentro de cada componente. Estas questões surgiram de uma miríade de partes de que cada componente pode ser feito.

Finalmente, vamos descrever como é que um Agente ou um Sistema Multi-Agente (SMA) [42] é interligado neste sistema. O SMA é responsável por regularmente verificar os valores dos sensores, actuando de acordo com o previsto, (exemplo: a temperatura baixou de repente, ligar o aquecimento) e registar todos os eventos e as decisões que forem sido tomadas. Vamos agora analisar como integramos o nosso SMA com o resto da arquitectura. O objectivo é tornar as funcionalidades de um agente acessíveis (exemplo: os seus métodos) como um serviço aos outros "bundles". Não é aconselhável converter todos os agentes num "bundle" OSGi, visto que iria aumentar o tempo de desenvolvimento e diminuir as vantagens das metodologias de resolução de problemas baseados no SMA. Dai a decisão de criar um "bundle" OSGi que pudesse servir de ligação entre os "bundles" normais e o Jade: o "bundle" que implementa o SMA. Este "bundle" pode tratar de um "Agent Container" (AC) e implementar os métodos declarados no interface do agente do AC como serviços próprios. Ainda mais, este "bundle" deve poder parar e arrancar agentes, que na prática, corresponde a arrancar e parar serviços providenciados por eles. Um "bundle", depois de ser invocado por outro "bundle", envia o respectivo pedido ao agente correspondente e entrega o respectivo resultado ao "bundle" que fez o pedido. Deve-se ter em conta que o agente, quando está a tentar responder a uma invocação, pode necessitar de serviços fornecidos por outros "bundles" disponíveis no momento. Isto é possível através do "bundle" SMA.

O interface de ligação entre o "bundle" SMA e o sistema Jade, existe um agente JadeGateway (JGa) que é usado. A tarefa deste agente é servir de ligação entre o código Jade e não-Jade. Este agente é criado quando o "bundle" SMA é arrancado, em conjunto com os outros agentes. O JGa tem o conhecimento de que serviços são providenciados por cada agente em execução. Por isso quando um pedido de um serviço chega ao "bundle" SMA, ele sabe a que agente deve reencaminhar o pedido. Igualmente, se um agente precisa de usar um serviço de outro "bundle", ele contacta o "bundle" SMA, que é responsável por contactar o "bundle" correcto, invocando o serviço e reencaminhando o resultado de volta ao agente. Desta forma, nós criamos um "bundle" que permite que as instâncias do Jade possam correr por detrás das implementações OSGi numa forma totalmente transparente.

A nossa arquitectura, num nível mais alto, é composta por componentes que partilham informações usando "Web Services". Cada um destes componentes pode ser analisado ao pormenor. Olhando de uma forma mais atenta, significa que as partes são compostas por: sensores, actuadores, SMA, software, etc. A comunicação dentro dos componentes é baseada em standards abertos OSGi e R-OSGi, permitindo extensibilidade, modularidade, dinâmica e uma organização lógica e hierárquica das partes que formam cada componente.

5.3.1 Visão Tecnológica

5.3.1.1 OSGi

OSGi é uma iniciativa com o intuito de estabelecer standard em programação Java, altamente específicas, partilhando as classes Java, que devem seguir o paradigma de uma plataforma de serviços. Naturalmente, a forma de executar tarefas em nome do utilizador, implica o uso de dispositivos e aplicações capazes de detectar a presença do utilizador (quer fisicamente ou não), que nos leva aos chamados sistemas sensíveis ao contexto. Este tipo de sistemas consegue aproveitar as novas soluções de computação que são capazes de disponibilizar a computação "em qualquer altura, em qualquer lugar", que por sua vez tem atraído muita atenção de investigadores nos últimos anos numa tentativa de demonstrar que é uma utilidade da tecnologia. No entanto, construir aplicações sensíveis ao contexto é relativamente complexo e necessita uma infra-estrutura adequada para suportar uma plataforma genérica e independente.

Quando tentamos adaptar a arquitectura proposta para ajustar as especificações *OSGi* deparamo-nos com alguns desafios, sendo um dos mais óbvios "como fazer com que alguns dos agentes, usados em alguns componentes da arquitectura serem compatíveis com *OSGi* (visto que alguns dos nossos componentes são baseados em agentes), e como usar o *OSGi* numa arquitectura distribuída (visto que o *OSGi* é uma arquitectura centralizada e orientada ao serviço). Além disso, os agentes podem ser muito diferentes entre eles, incluindo as assinaturas dos métodos a declarar, por isso devemos ter a certeza de que cada agente é compatível com o próximo e com os normais "bundles" *OSGi*. Estes assuntos e as suas soluções serão abordados nas secções seguintes, onde é descrito como fazer a arquitectura *OSGi* compatível.

5.3.1.2 Sistema Multi-Agente e OSGi

Adoptar o OSGi em cada componente da arquitectura, forçou-nos a encontrar uma forma para criarmos os nossos agentes compatíveis com os "bundles" OSGi. O objectivo é fazer com que as funcionalidades de um agente (exemplo: os seus métodos) sejam acessíveis como serviços aos outros "bundles". Não é aconselhável converter todos os agentes num "bundle" OSGi, visto que iria aumentar o tempo de desenvolvimento e diminuir as vantagens das metodologias de resolução de problemas baseados no SMA. Dai a solução de criar um "bundle" OSGi que pudesse servir de ligação entre os "bundles" normais e o Jade: o "bundle" que implementa o SMA. Este "bundle" pode tratar de um "Agent Container" (AC) e implementar os métodos declarados no interface do agente do AC como serviços próprios. Ainda mais, este "bundle" deve poder parar e arrancar agentes, que na prática, corresponde a arrancar e parar serviços providenciados por eles. Um "bundle", depois de ser invocado por outro "bundle", envia o respectivo pedido ao agente correspondente e entrega o respectivo resultado ao "bundle" que fez o pedido. Deve-se ter em conta que o agente, quando está a tentar responder a uma invocação, pode necessitar de serviços fornecidos por outros "bundles" disponíveis no momento. Isto é possível através do "bundle" SMA.

Vamos agora descrever mais detalhadamente o "bundle" SMA. Ele tem dois métodos para controlar o "bundle" que vai ser usado, quer pelo cliente, quer pelo administrador, de forma a arrancar ou parar o "bundle" respectivo. Uma vez que o "bundle" SMA regista os serviços dos agentes que cria, declara os métodos dos agentes na sua própria interface, de forma a torná-los visíveis para os outros "bundles" como um serviço normal. O interface de ligação entre o "bundle" SMA e o sistema Jade, existe um agente JadeGateway (JGa) que é usado. A tarefa deste agente é servir de ligação entre o código Jade e não-Jade. Este agente é criado quando o "bundle" SMA é arrancado, em conjunto com os outros agentes. O JGa tem o conhecimento de que serviços são providenciados por cada agente em execução. Por isso quando um pedido de um serviço chega ao "bundle" SMA, ele sabe a que agente deve reencaminhar o pedido.

Igualmente, se um agente precisa de usar um serviço de outro "bundle", ele contacta o "bundle" SMA, que é responsável por contactar o "bundle" correcto, invocando o serviço e reencaminhando o resultado

de volta ao agente. Quando o pedido chega, um objecto partilhado é criado no "bundle" SMA, ou seja, no "blackboard". Este objecto contém alguns campos como o nome do serviço a ser invocado e o conteúdo que é a resposta do agente final. O "bundle" SMA simplesmente preenche o nome do campo, que é o nome do serviço que foi invocado por outro "bundle". Então, no "blackboard", há uma interacção entre um ou mais agentes de forma a obter a resposta necessária para a invocação do serviço. A resposta é escrita no campo do objecto partilhado e devolvido ao "bundle" SMA. A parte final consiste no fim da invocação do serviço, sendo que para isso é preciso voltar ao "bundle" que fez a invocação do objecto partilhado. O "bundle" que fez o pedido não se irá aperceber de tudo o que se passou durante o tempo que esperou desde o momento que fez o pedido. Da mesma forma, se um agente precisar de usar um serviço de outro "bundle", ele contacta o "bundle" do SMA, que é responsável por contactar o "bundle" correcto, invocando o serviço e reencaminhando o resultado de volta ao agente.

A parte mais específica da interacção de agentes, dentro da plataforma, é fora da esfera do OSGi, e por isso deve ser analisada. A comunicação entre agentes, é de certeza um tópico muito importante pois tem implicações directas com a performance e o comportamento de todo o sistema. FIPA estabelece vários standards de relações entre agentes, sendo um o "Agent Communication Language" (FIPA-ACL) [29]. Este standard define como é que a construção da mensagem deve ser quer ao nível da sintaxe, quer ao nível da semântica. Especifica os parâmetros que a mensagem deve ter (exemplo: origem, conteúdo), e como os usar. A comunicação entre os agentes na nossa arquitectura satisfaz o standard definido pelo FIPA-ACL. Ao fazermos isto, resolvemos alguns inconvenientes e aumentamos a compatibilidade da arquitectura com agentes externos que seguem os mesmos standards. Neste ponto, podemos dizer que qualquer agente que siga o standard FIPA-ACL pode ser executado e controlado pelo "bundle" SMA e pode disponibilizar os seus métodos como serviços.

5.3.1.3 OSGi – Como é que funciona

Vamos descrever nesta secção o papel que o OSGi irá desempenhar a nossa arquitectura. O que temos é um grupo de nós (exemplo: o "Sujeito" , o "*Centro Telefónico de Suporte*") e usamos OSGi em cada um destes nós. Vamos tomar em exemplo a casa do Sujeito. Existe um grupo de componentes que fazem parte da casa e devem estar ligados ao sistema. No entanto, por um lado temos sensores "1-Wire", que

servem para informar o sistema da temperatura, humidade, luminosidade e outros factores, por outro lado, usamos a rede "X10" que permite que lâmpadas ou outros dispositivos eléctricos sejam controlados por um computador. O nosso objectivo é ligar um grupo de dispositivos heterogéneos de uma forma integrada e é neste campo, a este nível que o OSGi contribui.

Dentro da casa, os sensores estão ligados a um computador central através de uma porta de série e existe um "bundle" responsável por constantemente ler os valores dos sensores e os registar. Este bundle exporta como um serviço os valores dos sensores da casa, que podem ser usados pelo resto dos "bundles". Existe também um bundle para cada equipamento X10 e cada "bundle" desses, exporta como serviço, os comandos que podem ser emitidos ao equipamento que representa (como ligar, desligar, para cima, para baixo, etc).

Vamos assumir que o sistema de ar condicionado tem autonomia suficiente para controlar a temperatura baseado nas preferências do cliente. É uma tarefa muito complicada pedir a um equipamento X10 para interagir com um sensor "1-Wire" de forma a obter informação sem um equipamento intermediário. Com o OSGi, a autonomia é dada ao "bundle", que por sua vez facilmente emite o comando ao equipamento X10 baseado na informação obtida pelo "bundle" do sensor ligado pela porta de série. Com o OSGi, entidades que são diferentes podem facilmente ser integradas de forma a por em marcha um leque de sensores, actuadores, equipamentos da casa, pessoas e até agentes de software de forma a chegarem a um fim comum, que é o bem estar do Sujeito.

Outro problema com o qual nos deparamos quando adoptamos o OSGi foi a falta de compatibilidade entre "bundles". Este problema surgiu devido à diversidade de "bundles" que temos, agregado ao facto de que em OSGi, qualquer "bundle" escrito por quem quer que seja, tem que ser possível incorporar no sistema. Como um exemplo, imaginemos uma classe que exporta um método cuja assinatura é uma estrutura de dados declarada dentro do próprio método. Um "bundle" que faça uma invocação a esse serviço não irá perceber o resultado. Daí a necessidade de obrigar a compatibilidade entre os "bundles". Conseguiu-se definindo uma regra ontológica para ser usada por todos os "bundles". Esta regra ontológica foi definida uma classe java em que as outras classes se têm que relacionar ao nível de todos os objectos que podem ser usados pelos métodos e as assinaturas que tem que ser declaradas. Se cada "bundle" importar esta ontologia, a compatibilidade é assegurada e, se um "bundle" que implementa um

novo objecto é adicionado, apenas a ontologia precisa de ser corrigida/actualizada. No entanto, nada disto seria necessário se apenas fossem usadas as classes de java standards.

Tendo já analisado os assuntos principais, o OSGi pode ser usado nos componentes da nossa arquitectura simplificando a sua implementação. Mais ainda, que o OSGi providencia um "bundle" pronto a usar que já vem com os componentes UPnP para serem visto por outros "bundles" como serviços, estendendo assim as suas possibilidades. Olhando novamente para a casa do "*Sujeito*": cada "bundle" pode providenciar serviços locais com o controlo das luzes ou do sistema de ar condicionado. Se um utilizador, por exemplo tiver uma televisão UPnP, o seu controlo também será providenciado ao utilizador, no momento em que a liga. O facto de o OSGi suportar dispositivos UPnP, significa que não tem qualquer necessidade de configuração, para se incluir novos serviços, que é especialmente útil para pessoas de maior idade.

Tendo em atenção aos fornecedores de serviço, como o "*Centro Telefónico de Suporte*", a implementação OSGi permite uma melhor organização local. Cada profissional de saúde ou recursos computacionais podem por exemplo ser serviços locais utilizados por uma entidade responsável por gerar uma resposta para o utilizador que a pediu.

5.3.2 Comunicações

O desafio agora, será fazer com que todos os componentes funcionem em conjunto. Este desafio não advém só do facto de usarmos uma arquitectura distribuída, mas também dos componentes que podem ser programados em diferentes linguagens de programação e em plataformas diferentes. Existe, por isso, a necessidade de estabelecer um mecanismo de comunicação que seja possível de usar em todas as plataformas e entre todas as linguagens que os componentes possam usar. Além de apenas escolher os meios de comunicação, a linguagem usada deve ser especificada para que haja interoperabilidade entre os componentes.

Como definimos anteriormente, escolhemos a utilização de Web Services para implementar a comunicação entre os componentes visto que são independentes das plataformas e funcionam sobre redes de comunicação. A informação que é partilhada nos Web Services está no formal XML e a sintaxe que os nossos Web Services usam segue o standard FIPA-ACL em XML [28,29]. Este standard FIPA

permite a descrição do conteúdo principal da mensagem sem ter de aceder ao conteúdo usando conceitos como ontologia e linguagem. Desta forma, as mensagens podem ser encaminhadas e enviadas para os agentes finais sem que seja necessário verificar o seu conteúdo.

5.3.3 Análise de Segurança

Vírus, "worms", "phishing", má conduta moral de empregados e spyware são os principais problemas de acordo com o relatório de 2007 da Deloitte "2007 Global Security Survey" [15]. Má conduta pode ser prevenida ao nível/esfera da comunidade. As outras quatro podem ser combatidas usando mecanismos de alto nível, com por exemplo: anti-vírus, anti-spam, etc. Existem também ataques em níveis mais baixos, como por exemplo: Troca de identidade/Men in the Middle, Denial OF Service(DOS) e Distributed Denial of Service (DDOS), Colisões de Hash, etc. [43]

- Men in the Middle – é possível alterar o MAC Address de uma placa de rede. Desta forma podemos re-injectar a resposta ARP na rede de forma a desviar o tráfego para um determinado IP. Simplemente restringir o IP da rede não seria o suficiente para ter a certeza que estaríamos a comunicar com o destino desejado. Desta forma, as vítimas iriam acreditar que estariam a comunicar numa forma segura, sem que ninguém soubesse do que estaria a comunicar, quando na realidade seriamos o "homem no meio" (Figura 5). Uma forma de prevenir este ataque seria usando entidades de confiança. [44]

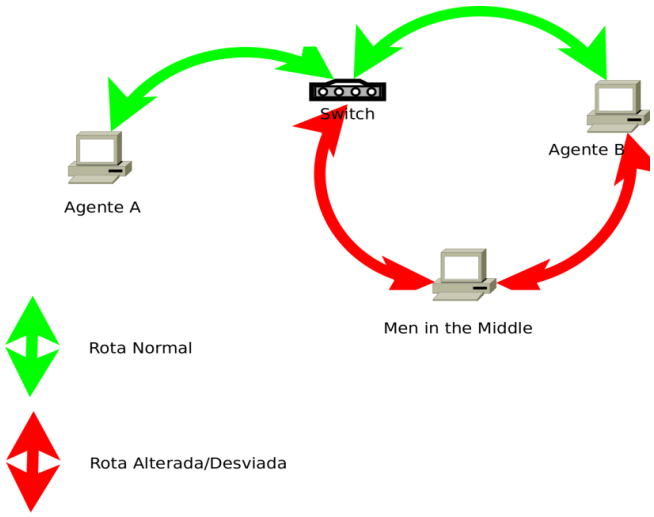


Figura 23 - Exemplo de uma ataque Men in the Middle com arp poisoning

- DOS e DDOS (Figura 6) são ataques com o intuito/objectivo de parar um determinado serviço (disponibilidade). Uma forma de se fazer isto é criar demasiadas ligações ao serviço, de forma que quando um cliente real tentasse se ligar ao servidor, não iria conseguir, visto que estaria inundado com ligações (o limite de conexões do serviço seria ultrapassado). Uma forma de nos defendermos seria restringir o número de acesso de um determinado IP. No entanto, em ataques de DDOS, onde a origem dos ataques são múltiplos IPs, vai-se tornar mais difícil de bloquear. Felizmente existem firewalls dinâmicas que têm mecanismos que permitem prevenir este ataques. [45]

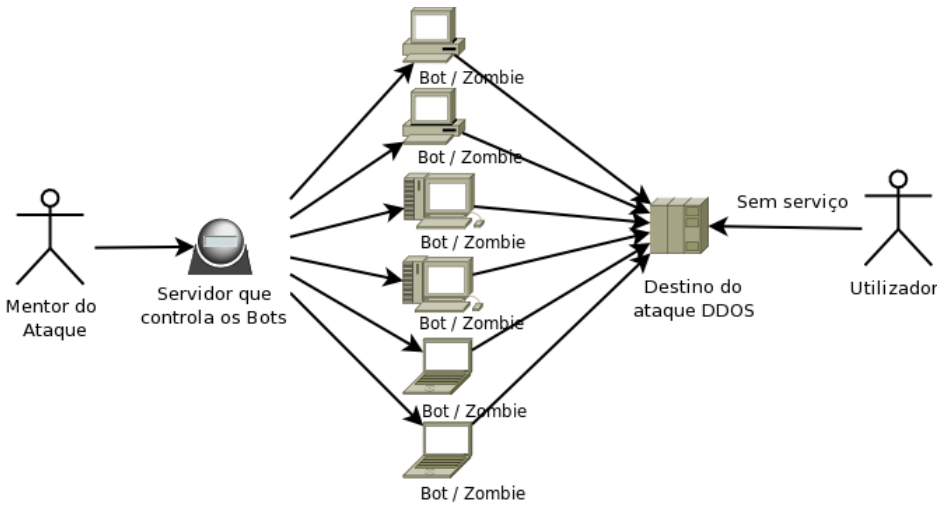


Figura 24 - Exemplo DDOS

- Colisões de Hash (Figura 7) – usar criptografia poderia ser a solução. No entanto, se usarmos o protocolo de geração de hash MD5, a solução não é segura. Conseguimos facilmente e em tempo útil criar duas cartas, uma de recomendação e uma segunda de autorização de acesso a instalações secretas, ambas com a mesma hash MD5. Isto implicaria que alguém que assinasse a primeira carta usando o algoritmo MD5, estaria automaticamente a assinar a segunda. [46]

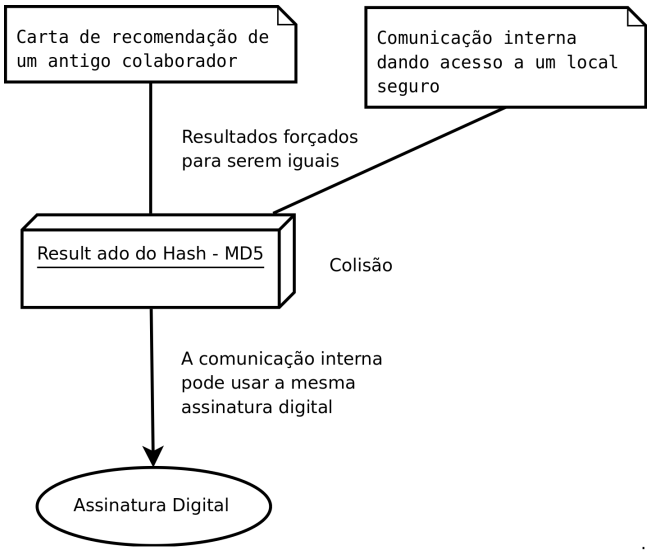


Figura 25 - Colisões de Hash

5.3.4 Segurança

De forma a melhor entender os problemas de segurança e apresentarmos a melhor solução para cada problema, os agentes foram divididos em duas categorias: agentes num ambiente controlado/ espaço fechado e os outros.

A comunicação entre agentes em ambientes fechados, foi inicialmente feita usando cabos que iria permitir a segurança da informação e a alimentação ao nível da energia. A evolução deste sistema obriga ao uso de comunicações sem fios para maior mobilidade.

Analisamos várias tecnologias em termos da segurança (tamanho da cifra), distância das comunicações, a energia que consome e a quantidade de informação que permite circular (Tabela 1). A segurança do hardware está relacionada com três pontos que tem que ser tidos em conta: o algoritmo, a versão e o tamanho da cifra. A distância máxima em que os agentes conseguem comunicar é muito importante para prevenir falhas de comunicação em momentos críticos. A energia que cada tecnologia consome está relacionada directamente com o seu uso. Por exemplo, não vamos obrigar o *Sujeito* a carregar baterias que tem um peso considerável. Finalmente, é importante saber qual a largura de banda disponível de forma a decidirmos que informação podemos trocar (vídeo, áudio, sinal, etc) e se uma análise continua é possível.

Tecnologia	Segurança Tamanho da Cifra	Distância	Consumo Energia	Largura de Banda
Bluetooth	Não Disp.	10 m	40 mA Tx, 0,2 mA standby	1 MBit
Bluetooth II	128 Bits	100 m	40 mA Tx, 0,2 mA standby	3 MBits
RFID	Não Disp.	40 cm	Desprezável	2 KBits
RFID II	Não Disp.	1,5 m	Não Disp.	2 KBits
ZigBee	32 Bits	10 m	30 mA Tx, 3 mA standby	250 KBits
ZigBee Comp	32 Bits	300 m	30 mA Tx, 3 mA standby	250 KBits
Wi-Fi	256 Bits	100 m	400 mA Tx, 20 mA standby	54 MBits
Wi-Fi Comp	256 Bits	300 Kms	6 Watts	54 MBits

Figura 26 - Tabela Comparativa de Tecnologias [47, 48, 49]

A categoria de comunicações dos Outros pode existir em dois tipos de redes. As redes abertas (exemplo: a Internet) onde toda a gente tem acesso a tudo e as redes privadas (exemplo: Frame Relay e ATM - Asynchronous Transfer Mode) onde a segurança é suportada pelas tecnologias. No entanto, em redes fechadas existe sempre a hipótese de haver uma falha de segurança, um intruso. Por isso é que decidimos tratá-los como iguais, como inseguros, como a Internet.

A Internet é uma rede global sem a possibilidade de se ter a certeza de quem é quem. Por isso, é que temos que usar protocolos/sistemas para assegurar a integridade, confidencialidade, autenticidade, o não repúdio e a disponibilidade.

Protocolos/Sistemas

Existem inúmeras formas de aumentar a segurança de um sistema. Vamos focar-nos em três níveis, ao nível da rede, do sistema e da aplicação.

Ao nível da rede temos as seguintes soluções de novas tecnologias para aumentar a resiliência:

- DNSSEC são extensões de segurança para o DNS, um sistema muito importante nas comunicações na internet. A Internet está directamente dependente do funcionamento normal do DNS que traduz os nomes associados a IPs (exemplo: 62.48.217.202) com nomes facilmente reconhecidos por humanos (www.multicert.com). Este novo sistema foi desenhado para proteger a Internet de certos ataques como *DNS cache poisoning*. São definidas extensões que providenciam: a) autenticação da origem dos dados de DNS, b) integridade dos dados e c) autenticação da negação de existência do domínio [50];

- IPv6, Internet Protocol version 6, é o novo protocolo de que vai substituir o IPv4. A segurança está embutida nesta nova versão. O protocolo de comunicação IPsec foi inicialmente desenvolvido para este protocolo (IPv6), o que mostra o aumento de segurança que vamos obter com esta solução [51];

- MPLS, Multiprotocol Label Switching é uma nova tecnologia utilizada por operadores de rede em servidores centrais com o intuído de substituir o Frame Relay e o ATM [52];

- A Virtual Private Networks (VPN) pode ser feita usando vários protocolos (SSL/TLS VPN, IPSec VPN, Open VPN, Cisco VPN, etc) que permitem criar uma rede segura para todos os Agentes [52, 53];

- Intrusion Detection System (IDS) como os Honeypots e os Tarpit são uma grande vantagem para o sistema, porque podem detectar e alertar anormalidades no funcionamento [54, 55];

- Por fim, uma outra solução para não termos acessos não autorizados é tornarmo-nos invisíveis. Usando Firewalls podemos criar várias restrições: primeiro rejeitamos/descartamos qualquer pedido vindo de um IP/Mac Address excepto os que conhecemos, seguidamente impomos que cada conexão tem uma sequência (pacotes fora da ordem serão rejeitados) e finalmente descartamos quaisquer sondas feitas à nossa rede, e novas ligações feitas o IP originador da sonda.

Mesmo usando estas bem conhecidas soluções devemos ir um pouco mais longe, implementando medidas de segurança no e para o código, de forma a prevenir acesso de agentes não autorizados.

OSGi Camada de Segurança da Estrutura

Ao nível do Sistema e da Aplicação, depois de termos apresentado o OSGI, vamos agora apresentar as frameworks que o implementa e que tiveram que ser estudadas, devido a algumas limitações individuais. A especificação OSGi definiu que a Camada de segurança é opcional, o que levou a essas limitações.

Esta camada de segurança usa a ciência da Criptografia, que nos garante melhorias ao nível da confiança do sistema.

Knopflerfish

Esta framework foi a primeira a ser estudada pois era a que estava a ser utilizada como base no sistema antigo. Deparamo-nos com o problema que é geral em quase todas as frameworks que analisamos, a falta do módulo de segurança. E até à data ainda não foi implementado este módulo [56].

Figura 27 - Logo Knopflerfish

Felix (Apache)

A fundação Apache, criou um projecto chamado Felix que implementa várias versões do OSGI. O problema em usar esta implementação reside no facto do módulo de segurança ser um "bundle" à parte. Isto implica que no arranque do sistema, o bundle pode não ter arrancado e nesta situação podem haver outros bundles que tenham arrancado antes dele. Também significa que pode ser desligado de forma a retirar as restrições do sistema.

No final de Março, foi disponibilizado um componente pela Comunidade JBoss de forma a interligar o "application server" da JBoss com a framework Felix. No entanto, também ainda é muito simplista e não contem o modulo de segurança [57].

Figura 28 - Logo Felix (Apache)

Figura 29 - Logo Jboss

Concierge

Esta framework está direccionada para equipamentos mais simples (móveis) e com pouco poder de computação, razão pela qual apostou em vários módulos móveis (telemóveis). No entanto, o problema, não se centra nesses módulos, mas sim com duas questões bem mais importantes: não ter o módulo de segurança, que apesar de opcional no OSGI é impreterível no nosso trabalho, e a falta de um upgrade de versão 3, para a versão 4 [58].

Figura 30 - Logo Concierge

Equinox (Eclipse)

A empresa Eclipse desenvolveu a framework Equinox. Visto ser uma empresa de grande dimensão e com boa implementação no mercado, conseguiu desenvolver todos os requisitos dos programadores. Como um dos principais receios estava relacionado com a segurança, o módulo opcional, indicação dada pela OSGI, foi desenvolvida e foram até feitas várias apresentações/formações em como o utilizar.

Por estas razões, este Framework foi o utilizado para prova de conceito. De seguida, descrevemos o procedimento de utilização [59].

Figura 31 - Logo Equinox

Primeiro, tivemos que constituir uma Autoridade de Certificação de forma a produzir certificados digitais e compelir que o Application Servers os usassem. Este uso tem o intuito de forçar o uso de "bundles" assinados nesta mesma hierarquia.

Usando o comando "openssl", criamos um ficheiro chamado ca-cert.pem que tem o certificado de topo da Autoridade de Certificação (Root CA) (Exemplo 1). [60]

```
[~]$ openssl req -nodes -config openssl.cnf -days 1825 -x509 -newkey rsa:4096
-out ca-cert.pem -outform PEM
```

Exemplo 1 - Criação do certificado da Autoridade de Certificação

De forma a gerarmos novos certificados folha, tivemos que criar o pedido de certificado (Exemplo 2), isto para que usado o certificado de topo pudesse assinar os de folha e usassem a mesma hierarquia.

```
[~]$ keytool -certreq -alias USER
```

Exemplo 2 - Criação do pedido de certificado

A emissão do certificado na hierarquia correcta, ou seja, debaixo do certificado da Root, definido no ficheiro openssl.cnf, deve ser feita da seguinte forma (Exemplo 3):

```
[~]$ openssl ca -config openssl.cnf -policy policy_anything -out user.cer -
infiles user.csr"
```

Exemplo 3 - Emissão do certificado

Depois de obtermos os certificados emitidos, vamos precisar de os usar. A forma que definimos como os certificados podem ser usados é através da "keystore" do Java (Exemplo 4).

```
[~]$ keytool -import -alias USER -file user.cer
```

Exemplo 4 - Actualização da Keystore do Java

A habilidade de assinar os "bundles" permite-nos identificar a quem é que pertencem e se existe autorização para serem usados no nosso sistema. Ou seja, se estiverem assinados pelo certificado gerado por nós associado a este determinado projecto, o sistema vai aceitá-los. (Exemplo 5).

```
[~]$ jarsigner C:\Bundle.jar USER
```

Exemplo 5 - Como assinar um "bundle"

Depois destes pré-requisitos todos, temos que configurar o sistema para apenas aceitar os "bundles" assinados na nossa hierarquia. A forma de o fazer será quando iniciarmos a nossa estrutura devemos fazê-lo com a opção que restringe o uso de "bundles" assinados e que especifica qual a "KeyStore" que confiamos (Exemplo 6).

```
[~]$ java -Dosgi.framework.keystore=file:.keystore -
Dosgi.signedcontent.support=true -
Dosgi.signedcontent.authorization.engine.policy=validity -jar
org.eclipse.osgi_XXX.jar -console -debug –consoleLog
```

Exemplo 6 - Como arrancar o "Application Server" Equinox com a verificação de "bundles" assinados activa

Usando este mecanismo conseguimos aumentar o nível de segurança, pois se implementarmos politicas documentais e procedimentais relativamente à Autoridade de Certificação, e tivermos garantia de segurança física das infrastruturas onde se encontram estes sistemas, podemos garantir que os certificados usados são qualitativos e que até têm valor legar. Neste caso, o uso de certificados é muito vantajoso pois garantimos que só serão assinados os "bundles" em que confiamos o que significa que só esses poderão ser usados no nosso sistema.

Sistema de Gestão de Chaves

A introdução de certificados no sistema, e a interligação com outros centros, vai obrigar à criação de um novo sistema para os gerir, SGC. O exemplo apresentado anteriormente serviu como prova de conceito. No entanto, estamos a falar da necessidade de um sistema que vai permitir gerir todo o processo de vida dos certificados.

- Pedido de certificado – autorização tem que ser dada, depois de analisada toda a documentação;
- Publicação do certificado – para que possa ser usado em comunicações cifradas;
- Controlo da vida do certificado – gerir a vida do certificado desde a emissão à expiração, ou mesmo revogação;
- Gestão dos certificados de topo – desde a sua comunicação aos agentes, à comunicação entre instituições.

Um último ponto na geração de certificados é que os mesmos podem ser gerados por software ou hardware (HSM) dependendo da quantidade necessária pois está directamente relacionado com o tempo que demora essa mesma geração.

Role Base Access Control

O modelo de controlo ser baseado em papeis, Role Base Access Control (RBAC) [61, 62] também é utilizado no nosso sistema, isto porque restringimos que tipo de acesso que cada agente tem. Dentro deste sistema, cada agente sabe o seu papel, o que é suposto fazer e que tipo de informação pode enviar e receber de outros. Existe um papel, uma política, que cada agente é forçado a conhecer. Por exemplo, se o agente que monitoriza a temperatura recebe informações do agente das luzes ele não irá aceitar porque foi definida uma autorização que indica que só deve receber informações do agente da temperatura, ou se o agente da temperatura indica que está vento num determinado quarto, o monitor de temperatura também não irá aceitar essa informação.

5.3.5 Autenticidade

Mesmo que já existam características de segurança já implementadas, a autenticação, deve também estar presente. Isto significa que quando um membro do grupo de decisão, um parente ou outra pessoa fora da área predefinida como segura, acede ao sistema, deve autenticar-se. Usando Web Services e certificados x509, permite-nos aumentar o nível de segurança. Ligação por "SSL-Client side" significa que ambos o servidor e o cliente são obrigados a apresentar um certificado válido. O certificado apresentado tem que ser emitido na hierarquia da nossa Autoridade de Certificação, isto ajuda no sistema de verificação que não aceita todos os certificados válidos, mas sim apenas os que respeitem a nossa hierarquia. No caso de certificados pessoais, devem ser guardados em "tokens" de alta segurança, como smartcards ou "tokens" USB, que usam mecanismos especiais para guardar a chave privada, e que não permite a sua distribuição.

5.3.6 Privacidade dos dados

Ao nível da Comunidade temos que ter em conta a Ética, a Sociedade e as Leis que a geram. A Ética é uma qualidade humana que ajuda a Sociedade a definir o que é certo ou errado. A Sociedade auto regula-se com um sistema de regras, que normalmente são obrigados a cumprir através de uma serie de instituições, que são a Lei.

A Lei, relacionada com a informação/dados médicos, foca duas áreas: a segurança da comunicação de informações médicas entre entidades em redes públicas e a protecção de dados pessoais.

As comunicações seguras estão definidas na Constituição Portuguesa Lei 41/04 e 31/08. A primeira foca o uso de segurança nas comunicações e a segunda identificação das informações sobre as próprias comunicações, como a origem, o destino, a data/hora, o tipo de equipamento usado e a localização quando falamos de equipamentos com alguma mobilidade. Também define que a empresa que disponibiliza o serviço deve garantir que as comunicações são seguras, mas também define que aceder (escutas) à comunicação é ilegal, que nos dá a oportunidade de não fazer nada. Esta situação sugere algo saído do bom senso, no entanto, para centros de suporte de assistência existem algumas regras na

Lei 134/2009 que indicam que as chamadas devem ser gravadas e guardadas por um período não inferior a 90 dias.

A Lei 67/98 da Constituição Portuguesa de 26 de Outubro, que define a protecção dos dados pessoais, indica que existem vários tipos de dados, o direito ao acesso do assunto dos dados, a segurança do tratamento dado aos dados, o sigilo profissional necessário para se trabalhar com os dados, as características das comunicações fora das fronteiras do país e a prevenção do acesso de pessoas não autorizadas à informação. Está definido no Artigo 15 da lei anterior que tudo deve ser feito para impedir o acesso não autorizado a informações médicas, usando para isso 8 tipos de controlos/barreiras.

Por isso tem que existir uma separação/divisão entre os dados que são guardados, entre os dados administrativos e os dados médicos. Isto porque a informação médica não deve ser acessível a um administrativo, secretária ou pessoal que gere os arquivos. Apenas elementos da equipa médica devem ter acesso a eles.

6 Conclusões e Trabalho Futuro

"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards – and even then I have my doubts." [63]

O cenário apresentado é irrealista, pretende-se claramente, um sistema a funcionar e interligado com o exterior, não podemos seguir a ideia apresentada pela citação de Eugene H. Spafford. Por esta razão, tivemos de usar muita técnica e genuidade na solução apresentada.

6.1 Conclusões - Síntese do trabalho feito

Neste trabalho, o mais difícil foi identificar qual seria a pergunta que pretendia que fosse feita. Precisamos de segurança num sistema de e-Health? Que riscos são corridos se não houver Confiança num sistema de e-Health? Em que pilares é que a Segurança assenta? De forma a obtermos o melhor sistema ao nível da Segurança num ambiente assistido, identificamos a Confiança, subdividida em três níveis de abstracção, como ponto-chave. Apesar da ideia de termos um sistema 100% seguro ser uma utopia, deve-se fazer com que seja o mais seguro que a tecnologia actual nos permite.

Ao nível Individual, através das experiências, razões e observação estabelecemos um nível de Confiança no sistema. É essa sensação de segurança que nos vai permitir acreditar e utilizá-lo.

O Sistema também é outro dos pilares da Confiança, que significa que num sistema como aquele que mostramos existem uma variedade de tecnologias que foram estudadas e outras que ainda serão para aumentar a segurança. Cada transacção/módulo/função deve ser analisada individualmente de forma que podemos definir a criticidade e que permissões devem ter.

A Comunidade é o ultimo pilar da Confiança, e a Lei deverá ser analisada exaustivamente de forma que a possamos usar no nosso âmbito e não sermos apanhados em actividades ilegais. (como comunicações entre dois países sem a autorização necessária)

Da mesma forma que apresentamos os trabalhos a efectuar, vamos agora apresentar o que foi realizado:

- Analisamos o *VirtualECare*, compreendendo a estrutura e a sua forma de funcionar;
- Em segundo lugar, identificamos todos os pontos necessários para obtermos Confiança:
  - Desde o nível Individual, em que validamos que é necessário reeducar os indivíduos de forma que sejam sensibilizados das implicações das engenharias sociais; permitir observação e experiência para a credibilização do sistema;
  - Ao nível do Sistema, identificamos e avaliamos os riscos e como os resolver usando para isso uma quantidade enorme de soluções tecnológicas.
  - Ao nível da sociedade, fizemos alguns estudos da Lei e identificamos as que precisamos seguir e usar para mantermos o nosso sistema seguro.
- Por fim, estas propostas estão a ser objecto de integração no sistema *VirtualECare*.

6.2 Trabalho Publicado

Foi objecto de submissão a uma Conferência o artigo "Ambient Assisted Living: a Security Aproach".

6.3 Trabalho Futuro

Um trabalho que não chegou a ser implementado foi o Sistema de Gestão de Chaves, pela simples razão de que desenvolvemos uma solução simplista que não obrigava uma gestão complexa dos certificados. Isto significa que o primeiro passo a seguir deste projecto será fazer essa implementação.

Em investigações futuras é imperativo que se defina como os agentes vão reagir/responder à falha de comunicações, ou seja, tolerância a falhas. Vamos também analisar a possibilidade de usar o tão mencionado "Cloud Computing" e por isso a investigação da tolerância a falhas será um passo mais perto do nosso objectivo.

Referências Bibliográficas

[1] Costa R., Novais P., Machado J., Alberto C., Neves J., "Inter-organization Cooperation for Care of the Elderly", in Integration and Innovation Orient to E-Society, Wang W., Li Y, Duan Z., Yan L., Li H., Yang X., (Eds), Springer-Verlag, Series: IFIP International Federation for Information Processing, ISBN: 978-0-387-75493-2, 2007 ((The 7th IFIP Conference on e-Business, e-Services, and e-Society (I3E 2007), Wuhan, China , 10-12 September 2007).

[2] S. D. Ramchurn, D. Huynh and N. R. Jennings, "Trust in multi-agent systems", The Knowledge Engineering Review 19 (1) 1-25, 2004.

[3] United Nations Department of Economic and Social Affairs, Population division, "World Population Prospects", The 2004 Revision, New York, United Nations, 2005.

[4] European Statistical System (Eurostat), "Pension Expenditures in the European Union as a Percentage os Gross Domestic Product 2003" , http://epp.eurostat.ec.europa.eu.

[5] P. Tang and T. Venables, "'Smart homes and telecare for independent living," J Telemed Telecare, vol. 6, pp. 814, February 2, 2000 2000.

[6] K. Doughty, K. Cameron, and P. Garner, "Three generations of telecare of the elderly," Telemedicine and Telecare, vol. 2, pp. 7180, 1996.

[7] Bruce Schneier, "Applied Cryptography", Second Edition, John Wiley & Sons, 1996, ISBN 0-471-11709-9.

[8] K. Houshiaryan, K. Kim, Y. Kwak, N. Phuong 2003 "Multi-Agent Based Healthcare Interface Manager: Related to Interface Engine(2.4) Project".

[9] Sun Tzu, "The Art of War", Cosimo Inc., ISBN1-59605-478-6.

[10] Paulo Borges, "Segurança da informação: da tecnologia aos processos", Curso ISEP, Dia 4.

[11] Cavaco Silva, Declaração do Presidente da República, Palácio de Belém, 29 de Setembro de 2009 - http://www.presidencia.pt/?idc=22&idi=31744

[12] Correio da Manhã, "Documentos secretos abandonados em comboio" , 18 de Junho de 2008

[13] Jornal de Notícias, "JN noticiou ataques há 9 meses", 24 de Outubro de 2009

[14] Disaster Recovery Jornal, http://www.drj.com.

[15] 2007 Global Security Server – Deloitte

http://www.deloitte.com/dtt/cda/doc/content/ca_en_Global_Security_Survey.final.en.pdf

[16] Telesegurança da Portugal Telecom,

http://casa.telecom.pt/ptresidencial2/tabs/sobre_ptcomunicacoes/noticias/arquivo/noticiasem2003/julho/ptcomunicacoesdisponibilizasolucoesdeteleseguran%C3%A7a.htm

[17] PrimusCare, http://www.primuscare.pt/

[18] QuickSafe, http://www.quicksafe.co.uk/

[19] Vital Jacket, BioDevices, http://www.vitaljacket.com/

[20] Scottish Centre of Telehealth, http://www.sct.scot.nhs.uk/

[21] PEDITEL, PT Inovação/Medigraf, 2007

http://www.telecom.pt/InternetResource/PTSite/PT/Canais/Media/DestaquesHP/destaques_2007/telemedicinangola.htm

[22] Costa R., Carneiro D., Novais P., Lima L., Machado J., Marques A., Neves J., "AmbientAssisted Living", in Advances in Soft Computing, Vol. 51, Springer-Verlag, ISBN 978 978-3-540-85866-9, pp. 86-94, 2008 (3rd Symposium of Ubiquitous Computing and Ambient Intelligence 2008 (UCAMI 2008), Salamanca, Spain, 22-24 October 2008)

[23] P. Novais, F. Andrade, J. Machado e J. Neves, "Agents, Trust and Contracts" in Departamento de Informática, Universidade do Minho, 2009.

[24] D. Carneiro and P. Novais, "Monitoring Ambient Assisted Living," in Departamento de Informática, vol. MsC Braga: Universidade do Minho, 2009.

[25] J. McCarthy, Dartmouth Artificial Intelligence Conference 1956, http://www.dartmouth.edu/

[26] Mordomus - Intelligent House Management, http://www.mordomus.com/

[27] MEDeTIC solutions of teleassistance, http://www.medetic.com/

[28] Foundation for Intelligent Physical Agents, http://www.fipa.org/

[29] K. Houshiaryan, Il Kon Kim Ph.D, Yun Sik Kwak M.D, Nguyen Woang Phuong Ph.D, "Multi-Agent Based Healthcare Interface Manager: Related to Interface Engine (2.4) Project", National University Department of Computer Science, Daegu South Korea

[30] Bernhard Bauer, Jörg P. Müller, James Odell: Agent UML: A Formalism for Specifying Multiagent Software Systems. International Journal of Software Engineering and Knowledge Engineering 11(3): 207-230 (2001)

[31] Josang, A., Ismail, R., Boyd, C. "A Survey of Trust and Reputation Systems for Online Service Provision", Distributed Systems Technology Centre and Information Security Research Centre, Queensland University of Technology Brisbane Qld 4001, Australia (2006)

[32] O'Donovan, J., Smyth, B. "Trust in Recommender Systems", Proceedings of the 10th International Conference on Intelligent User Interfaces - IUI'05, January 9–12, 2005, San Diego, California, USA

[33] Constituição Portuguesa, Lei 41/04 (2004)

[34] Constituição Portuguesa, Lei 31/08 (2008)

[35] Constituição Portuguesa, Portaria 701-G/2008 (2008)

[36] D. Carneiro, R. Costa, P. Novais, J. Neves, J. Machado, and J. Neves, "Simulating and Monitoring Ambient Assisted Living," in ESM 2008, Le Havre, France, 2008., 2008, pp. 175182.

[37] R. Costa, P. Novais, J. Machado, C. Alberto, and J. Neves, "Inter organization Cooperation for Care of the Elderly," in Integration and Innovation Orient to ESociety Volume 2. vol. 252/2008 Boston: Springer, 2008, pp. 200208.

[38] R. Costa, P. Novais, J. Neves, G. Marreiros, C. Ramos, and J. Neves, "VirtualECare: Group Decision Supported by Idea Generation and Argumentation," in Pervasive Collaborative Networks, 2008, pp. 293300.

[39] P. Novais, R. Costa, D. Carneiro, J. Machado, L. Lima, and J. Neves, "Group Support in Collaborative Networks Organizations for Ambient Assisted Living," in Towards Sustainable Society on Ubiquitous Networks, 2008, pp. 353362.

[40] O. Alliance, OSGi Service Platform: The OSGi Alliance: IOS Press, 2003.

[41] Osgi Alliance, 2003. OSGi Service Platform: The OSGi Alliance. Riva, Gg. 2003. "Ambient Intelligence in Health Care". In Cyberpsychology & Behavior, vol. 6, 295-301

[42] G. Weiss, "Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence", The MIT Press (March 19, 1999), ISBN-13: 978-0262232036

[43] S. Garfinkel, G. Spafford, "Web Security & Commerce", O'Reilly Nutshell, 1997, ISBN-13: 978-1565922693

[44] SANS Institute Reading Room site, http://www.sans.org/, Men in the Middle Attack

[45] National Cyber Alert System, Cyber Security Tip ST04-015, "Understanding Denial-of-Service Attacks", http://www.us-cert.gov

[46] M. Stevens, "Fast Collision Attack on MD5", Department of Mathematics and Computer Science, Eindhoven University of Technology, The Netherlands.

[47] Christian Gehrmann (Bluetooth SIG Security Expert Group), "Bluetooth™ Security White Paper", http://grouper.ieee.org

[48] ZigBee Alliance, "ZigBee Specification" 2008, ZigBee Document 053474r17

[49] "Wireless specification 802.11", IEEE 802.11-2007

[50] Domain Name System Security Extensions, http://www.dnssec.net/

[51] RFC2133, "Basic Socket Interface Extensions for IPv6", http://www.ipv6.org/

[52] RFC3031, "Multiprotocol Label Switching Architecture"

[53] I. Pepelnjak, J. Guichard, “MPLS and VPN Architectures”, Cisco Press 2000, ISBN-13: 978-1587050022

[54] C. Gerg, K. J. Cox, “Managing Security with Snort and IDS Tools”, O'Reilly Media (2004), ISBN-13: 978-0596006617

[55] J. M. Stewart, E. Tittel, M. Chapple “Certified Information Systems Security Professional Study Guide”, Sybex Inc, ISBN 13: 9780782144437[56] KnopflerFish, http://www.knopflerfish.org/

[57] Felix, http://felix.apache.org/

[58] Concierge, http://concierge.sourceforge.net/

[59] Equinox, http://www.eclipse.org/equinox/

[60] Openssl, http://www.openssl.org/

[61] Chang. N. Zhang, Cungang Yang, "An Object-Oriented RBAC Model for Distributed System," wicsa, pp.24, Working IEEE/IFIP Conference on Software Architecture (WISCA'01), 2001

[62] Parrend P., and Frenot S., 2006. “A Security Analysis for Home Gateway Architectures”. World Academy of Science, Engineering and Technology Volume 16 November 2006 – ISSN 1307-6884

[63] Eugene H. Spafford - Director of the Public Center for Education and Research in Information Assurance and Security