UNIVERSIDADE FEDERAL DA PARAÍBA - UFPB
CENTRO DE CIÊNCIAS EXATAS E DA NATUREZA - CCEN
DEPARTAMENTO DE INFORMÁTICA - DI

PROJETO

OpenCTI: Software de uma Central de Telemedicina para Apoio à Decisão Médica em Medicina Intensiva

PLANO

Implementação de Arquitetura de Segurança Baseada em Security Patterns para o OpenCTI

João Filho Matos Figueiredo

Orientador:
Gustavo Henrique Matos Bezerra Motta

João Pessoa – PB
2009

1. Cronograma

Atividade 1				
Atividade 2				
Atividade 3				
Atividade 4				
	1º Trimestre	2º Trimestre	3º Trimestre	4º Trimestre

2. Atividades Realizadas

De acordo com as metas propostas no plano de trabalho, estão concluídas as atividades previstas para os dois primeiros trimestres e, atualmente, tem-se desenvolvido o projeto de arquitetura de segurança (Atividade três). As subseções seguintes apresentam, de forma concisa, tais atividades.

2.1 Revisão Bibliográfica em Telemedicina e Security Patterns Para Aplicações na Internet

A prestação de cuidados de saúde, uma vez executados usufruindo de meios de telecomunicações, onde as distancias dos participantes envolvidos são relevantes, caracterizam um cenário de telemedicina. Não diferente do cenário real, no que diz respeito a segurança da informação, a telemedicina também deve atender a requisitos, todavia, este novo ambiente se depara com os desafios de segurança que englobam as redes de computadores, os quais podem ser divididos nas seguintes áreas interligadas: sigilo, autenticação, não-repúdio e controle de integridade (Tanenbaum, 2003).

No contexto da telemedicina, o sigilo está relacionado ao fato de manter as informações longe de usuários não-autorizados. A autenticação gerencia o processo que determina com quem você, ou as aplicações, estão se comunicando, antes de revelar informações críticas. O não - repudio é outro requisito imprescindível, uma vez que trata das assinaturas, evitando que indivíduos neguem determinadas ações, como prescrições precipitadas, negligencia ou qualquer conduta errônea. O controle de integridade responsabiliza-se em identificar tentativas de adulteração do conteúdo das informações, impedindo, desta forma, falsificação e fraudes.

Todas essas questões são amplamente estudadas no campo da segurança computacional, que possui vasta literatura sólida, com soluções reconhecidamente eficazes e largamente utilizadas. Por conseguinte, foram considerados relevantes os seguintes padrões de segurança:

Canais Seguros: Criação de canais seguros, criptografados fim-a-fim, instigando o sigilo das informações trocadas em sessões de telemedicina[1].

Known Partners (Parceiros Conhecidos): Utilização de mecanismos que possam garantir a identidade dos envolvidos nas sessões. Desta forma, pode-se trocar dados com maiores níveis de confiabilidade, uma vez que as partes envolvidas passam pelo processo de autenticação[1].

Zona Desmilitarizada: Separação dos serviços com acesso público (tais como HTTP, SVN,

sFTP, Correio Eletronico) da rede local. Para tanto, tais servidores de aplicações publicas não deverão ter rotas para a rede local, limitando, desta forma, possíveis danos nos demais pontos da rede caso um destes serviços seja comprometido[1].

Protection Reverse Proxy: A DMZ eleva a proteção na rede local, isolando-a dos servidores públicos, porém, esses também precisam elevar seus níveis de segurança, muito embora continuem susceptíveis a ataques pela internet. Desta forma, este padrão funciona como um filtro de pacotes no nível de rede. Além disso, proporciona proteção às aplicações ao nível de protocolo[1].

Integration Reverse Proxy: Nos sistemas distribuídos robustos, é importante que a existência de muitos servidores, interoperando entre si, seja abstraída aos usuários. A utilização de proxys reversos busca fornecer uma visão homogênea de um conjunto de servidores[1].

Intrusion Detection Requirements: O IDS é um serviço de segurança que automatiza o acompanhamento dos eventos que ocorrem em servidores ou na rede. Ele é capaz de tomar decisões, como modificar configurações do firewall, baseado na ocorrência dos eventos, além de funcionar como um importante mecanismo capaz de impor o cumprimento de algumas políticas de segurança.[1]

2.2 Especificação dos Requisitos da Arquitetura de Segurança do OpenCTI

Nas sessões de telemedicina, eventualmente utiliza-se informações multimídia, tais como videoconferências, sinais e exames de alta definição, requerendo assim uma rede com qualidade de serviço, que possibilite o trafego do grande volume de dados de maneira eficiente.

Além disso, o Conselho Federal de Medicina [2] estipula que o prontuário eletrônico pertence ao paciente e deve ser usado apenas por ele ou pelo médico a fim de assisti-lo. Por tanto, os requisitos anteriormente mencionados, que visam garantir o sigilo, autenticação, não - repudio e controle de integridade, são indispensáveis no contexto da telemedicina e do OpenCTI. Mais especificamente neste contexto, deve-se atentar também as peculiaridades de cada instituição, tais como a cultura organizacional e limitações tecnológicas, a fim de alcançar resultados homogêneos, embora lidando com instituições culturalmente diferente e distribuídas.

Com base nas especificações objetivadas para o OpenCTI, os seguintes requisitos fundamentais foram levantados:

- ***Escalabilidade:*** a quantidade total de serviços oferecidos ou o total de participantes pode crescer arbitrariamente;
- ***Flexibilidade:*** a entrada/saída de membros deve ser feita de modo transparente e sem necessidade de grande esforço, mantendo a fora do qualidade do serviço;
- ***Segurança dinâmica:*** além de possíveis canais seguros e exclusivos, previamente criados, deve-se prover mecanismos de autenticação e autorização através de meios de comunicações não confiáveis, como a Internet;
- ***Descentralização:*** as relações de confiança entre as organizações podem ser desenvolvidas e estabelecidas de forma descentralizada, gerando uma rede de confiança, que contribui para diminuir a sobrecarga de um elemento central e para aumentar a eficiência dessas relações;
- ***Confiança mútua:*** todas as partes envolvidas devem possuir níveis de confiança similares, apesar das discrepâncias existentes entre as organizações[1].

Com exceção da camada física, quase toda segurança se baseia em princípios criptográficos [3], portanto, este assunto deve ser cuidadosamente aplicado, visto que a utilização inadequada de padrões (algoritmos e protocolos) pode levar a exposição crítica do sistema.

Na camada de enlace, os pacotes podem ser codificados à medida que saem de uma

estação, e decodificados quando atingem o destino. No entanto, quando os pacotes têm de atravessar vários roteadores, essa abordagem se mostra ineficiente, pois se faz necessário descriptografa
-los em cada roteador, possibilitando ataques dentro dos mesmos. Para contornar essa situação, pode-se utilizar a combinação de VPNs e IPSec, criando o já mencionado *canal seguro.*

Na camada de rede, podem ser instalados os *Protection Reverse Proxy, firewalls, Integration Reverse Proxy, Intrusion Detection Requirements,* além da segurança do IP. Na camada de transporte, é possível criptografar conexões inteiras fim a fim, processo a processo, obtendo segurança máxima. Finalmente, na camada de aplicação, são tratadas as questões como autenticação e não repúdio.

Na prática, haverá um framework, o MACA [4], que deverá gerenciar a autenticação e a autorização multidomínio, baseado no modelo RBAC [5], no qual privilégios são associados a papéis e papéis são associados a usuários. Neste processo, é importante salientar que a literatura mostra a importância da utilização de algoritmo forte (mas público) e de uma chave longa, a fim de garantir o sigilo. Algoritmos fortes, de chaves simétricas, geralmente são mais rápidos que algoritmos de chaves públicas, porém esses normalmente serão usados apenas para o compartilhamento das chaves simétricas. O MACA também não deverá usar algoritmos que possibilitem "ataques de aniversário", ou seja, igual ou inferior ao MD5, ou "ataque por reflexão", devendo, para tanto, obedecer a quatro regras essenciais[3]:

1. *Fazer com que o transmissor prove quem é antes de o receptor.*
2. *Fazer com que o transmissor e o receptor utilizem chaves especificas para provarem quem são, mesmo que isso signifique ter duas chaves compartilhadas, K_{ab} e K_{ba}.*
3. *Fazer com que o transmissor e o receptor extraiam seus desafios de conjuntos distintos. Por exemplo, o transmissor deve usar números pares e o receptor deve usar números impares.*
4. *Tornar o protocolo resistente a ataques que envolvam uma segunda sessão paralela, no qual as informações obtidas em uma sessão sejam usadas em uma sessão diferente.*

Além disso, o famoso algoritmo de Diffie-Hellman também deve ser evitado, por ser sujeito a ataques de "homem ao meio". O uso da autenticação bidirecional, com protocolo de desafio-resposta abreviado é uma boa implementação prática que atende as necessidades do OpenCTI, desde que atenda as regras anteriores.

2.3 Projeto e Implementação de um Protótipo da Arquitetura de Segurança para o OpenCTI

O projeto da arquitetura vem sendo desenvolvido, o qual já foi apresentado em um trabalho produzido no âmbito dessa pesquisa. Foram logradas tecnologias consagradas e reconhecidas na área de segurança, das quais temos: VPNs, IPSec, VLANs, IDS e Clusters. Afora, tem-se os security patterns, que hão de proporcionar níveis elevados de confiabilidade ao sistema como um todo. Uma abstração da arquitetura pode ser vista nas figuras abaixo:

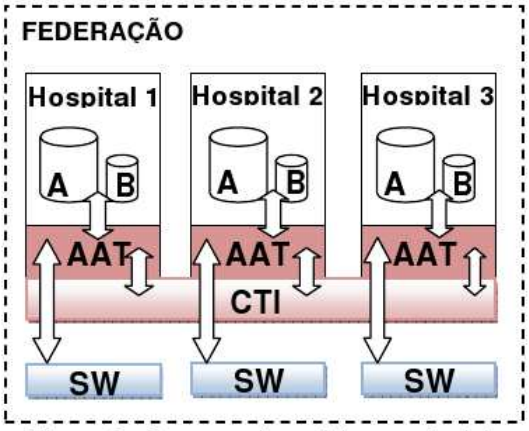

Figura 2 – Esquema do modelo conceitual da arquitetura

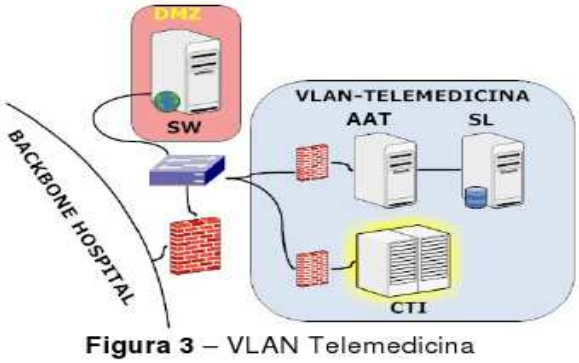

Figura 3 – VLAN Telemedicina

Os SW são servidores com acesso públicos; CTI é um cluster distribuído, abstraído por VPNs; AATs são aplicações avançadas em telemedicina. Todos os elementos vem sendo projetados com base nos padrões e requisitos já descritos, desde a camada de rede, até a camada de aplicação.

3. Dificuldades

Proporcionar segurança em ambientes multidominios, com particular uso de autorização baseada em papéis, tem sido campo de vastos estudos e pesquisas, não se mostrando uma tarefa trivial. Recentemente o framework MACA[4] disponibilizou um modulo para suporte multiorganizacional, fruto de recentes pesquisas, que oferece uma solução para autenticação coletiva de usuários em diferentes organizações. Esta solução ainda será analisada nessa pesquisa, a fim de se certificar quanto aos níveis de segurança oferecidos, com base nos requisitos do OpenCTI.

4. Outras Atividades Desenvolvidas

Foram apresentados seminários com os seguintes títulos:

- Estruturação da Evolução Clinica Para o Prontuário Eletrônico do Paciente.
- TimeLine Visualizing Integrated Patient Records.
- Modelo Conceitual de Segurança Para Uma Arquitetura Multidominio em Telemedicina.

Participação no XI Congresso Brasileiro de Informática em Saúde, em Campos do Jordão – SP, onde foi publicado um artigo[1] produzido no contexto da pesquisa, o qual foi selecionado como Finalista ao Prêmio de melhor publicação no CBIS2008.

[1]**MODELO CONCEITUAL DE SEGURANÇA PARA UMA ARQUITETURA MULTIDOMÍNIO EM TELEMEDICINA** – João F. M. Figueiredo, Eduardo P. Serafim, Walber J. A. Silva, Diego S. A. Pizzol, Gustavo H. M. B. Motta. (artigo: http://www.sbis.org.br/cbis11/arquivos/953.pdf).

A exposição do artigo, em forma oral, está disponível em: http://video.google.com/videoplay?docid=-6281250557996704708

Implantação de um ambiente colaborativo, MediaWiki, para dar suporte a documentação e gerenciamento de resultados do OpenCTI.

5. Referencias Bibliográficas

[1] SCHUMACHER, M.; BUGLIONI, E. F.; HYBERTSON, D.; BUSCHMANN, F.; SOMMERLAD, P. **Security patterns:** integrating security and systems engineering. England: John Wiley & Sons, 2006.
[2] Conselho Federal de Médicina (Brasil). Resolução CFM Número 1.821/2007. Brasília, DF: CFM, 11 jul. 2007.
[3] TANENBAUM, A. S. **Redes de Computadores.** tradução Vandenberg. D. S., 4ª Edição. Rio de Janeiro: Elsevier, 2003.
[4] MOTTA, G. H. M. B. **Um modelo de autorização contextual para o controle de acesso ao prontuário eletrônico do paciente em ambientes abertos e distribuídos.** São Paulo: USP, 2004. 213 p. Tese (Doutorado) – Programa de Pós-graduação em Engenharia Elétrica, Escola Politécnica da

Universidade de São Paulo, São Paulo, 2004.
[5] FERRAIOLO D. F.; KUHN, D. R.; CHANDRAMOULI, R. **Role-Based Access Control**. Boston: Artech House, 2003.