Análise de Segurança de um Servidor Chat
Segurança de Sistemas Informáticos

Helder Gonçalves, João Gomes
{pg28505, pg27761}@alunos.uminho.pt

Julho 2015

Contents

1 Introdução

O presente relatório apresenta a análise de segurança de um serviço de chat trabalhado durante o segundo semestre do Mestrado em Engenharia Informática, no âmbito da Unidade Curricular de Segurança de Sistemas Informáticos.

A conclusão deste projeto concretiza a implementação de um servidor de chat e uma componente de utilização cliente. O serviço de chat tem como visões primárias a segurança de comunicação entre os clientes e o servidor baseada maioritariamente, mas não só, em conceitos criptográficos.

A análise foi elaborada estudando os documentos facultados aos alunos pela equipa docente mas também dos conhecimentos resultantes da experiência empírica do grupo de trabalho.

Esta análise consiste noa identificação de assets, na análise de risco, na definição de objectivos de segurança, na descrição de mecanismos de protecção e a sua justificação tendo como base o conhecimento adquirido pelo grupo de trabalho.

2 Contextualização

Foi pedido ao grupo de trabalho que elabora-se uma análise de segurança relativo a um projecto anterior, acontece que o grupo decidiu avançar com o projecto referente a esta mesma unidade curricular, o servidor de chat.

Sucede este sistema consiste primariamente na segurança do canal de comunicação entre os utilizadores e o servidor e o processo de criação deste canal já seguia um procedimento de forma a garantir que este era o mais seguro possível.

O grupo de trabalho concentrou-se então em descobrir novas vulnerabilidades e a criar novos mecanismos de segurança para estas, encontrando descritas posteriormente neste presente e explicando a sua utilidade e necessidade.

2.1 Engenharia de Segurança de Sistemas

Engenharia de Segurança de Sistemas consiste essencialmente na avaliar a susceptibilidade a ameaças, identificar e avaliar vulnerabilidades, identificar especificar e desenvolver medidas para tratar vulnerabilidades, garantir medidas de segurança de forma a que o sistema se torne de confiança.

3 Common Criteria for Information Technology Security Evaluation

Common Criteria for Information Technology Security Evaluation (CC) foi uma das bases desta análise e permite comparar resultados de avaliações de segurança independentes. Faz isso fornecendo um conjunto comum de requisitos para a funcionalidade de segurança de produtos de TI e para medidas de garantia aplicadas a esses produtos de TI durante uma avaliação de segurança.

O processo de avaliação estabelece um nível de confiança que a funcionalidade de segurança dos produtos de TI e as medidas de garantia aplicadas a esses produtos atendem estes requisitos.

A CC é útil como guia para desenvolver, avaliar e/ou obter produtos de TI com funcionalidades de segurança.

É intencionalmente flexível, permitindo uma variedade de métodos de avaliação para serem aplicados.

3.1 Target of Evaluation(TOE)

Target of Evaluation(TOE) é o produto ou sistema que é alvo de avaliação. Este pode ser um produto TI, uma parte de um produto, um conjunto de produtos, uma única tecnologia que até pode nunca vir a ser um produto, ou combinação destes.

Quanto à CC, a relação entre um TOE e qualquer produto TI só é relevante num aspecto: a avaliação de um TOE contendo uma parte de um produto de

TI não deve compreendido como a avaliação de todo o produto de TI.

No caso de estudo no nosso TOE será então toda a aplicação de software criada, mais concretamente o servidor de chat.

O nosso sistema consiste num conjunto de clientes/utilizadores em que lhes é permitido comunicar entre si num servidor de chat. Cada cliente enviará mensagens aos outros clientes e receberá mensagens destes também. No entanto, esta comunicação é centralizada numa outra entidade, o Servidor, que tratará de receber as mensagens que os utilizadores desejam enviar e cabe também a este propagar as mensagens para todos os utilizadores.

A comunicação entre cada cliente e o servidor é segura na medida em que nenhum atacante, sendo activo ou passivo, consegue interpretar os dados que passam na rede e altera-los sem que o sistema tenha conhecimento.

3.2 Novos mecanismos de segurança implementados

Cada cliente para utilizar o serviço terá que se encontrar logado. Para efectuar o login terá que saber a sua palavra-passe, e em determinados casos ter acesso ao seu e-mail visto estar implementada uma autenticação multi-factor no sistema para garantir a identificação de cada utilizador.

A autenticação multi-factor é um dos elementos da estratégia de segurança mais eficazes. Esta estratégia atenua os ataques que ameaçam a confiança dos utilizadores, tais como roubo de identidade. Esta implementação é motivada por vários factos, salientando os seguintes:

- Os Hackers facilmente utilizam as credenciais mais fracas dos utilizadores ou credenciais roubadas em 76% dos ataques à rede;
- O roubo de identidade é muito mais rentável do que qualquer outro crime, correspondendo actualmente a 24,7 biliões de dólares;
- Os hackers estão sempre à procura de formas mais eficazes de roubar passwords via pharming, keylogging, phishing e outros.

A autenticação multi-fator é um elemento-chave da estratégia de segurança cibernética global de uma organização que adiciona uma camada adicional de proteção de dados.

O Servidor ficará também com a responsabilidade de aceitar ou não as tentativas de autenticação por parte dos clientes.

Cada evento considerado relevante no sistema será referido num ficheiro de log de sistema. Este ficheiro permite ao administração retirar informação acerca

do que se passa no sistema e se acontecer alguma falha catastrófica associar determinada falha a um acontecimento no sistema.

Serão guardados num sistema de base de dados a informação referente aos utilizadores (nome de utilizador, palavra-passe e e-mail) bem como o histórico de mensagens trocadas entre os utilizadores.

4 Activos(Assets)

Para garantir segurança o temos que nos preocupar com a proteção dos activos. Os activos são entidades que são tidas como valiosas para o sistema.

Os activos que do nosso sistema são, os seguintes:

- os conteúdos armazenados na base de dados, sejam o histórico de mensagens ou as informações relativas ao user;
- a autenticação do canal de comunicação entre cliente e servidor, a garantia do não repúdio e validade das mensagens recebidas por cada cliente (uma mensagem recebida foi efectivamente enviada por o user indicado)
- a disponibilidade e não congestionamento da rede.

Com o principal ambiente operacional e ser a máquina onde o programa Servidor está a correr.

5 Análise de Riscos/Ameaças

Gerenciar riscos é um passo essencial em qualquer sistema.

Uma ameaça é algo que pode afectar a confidencialidade, integridade ou disponibilidade de um sistema. Existem ameaças por actos humanos, naturais ou do ambiente, neste relatório apenas nos iremos ficar nas ameaças por actos humanos.

Para diminuir-mos os riscos aos nossos activos será necessário impor-mos contra-medidas.

Os principais riscos do nosso sistema são de um utilizador fazer-se passar por outro, roubando a sua identificação. A alteração, remoção ou visualização de dados presentes na base de dados, a descoberta dos cálculos a serem efectuados pelas máquinas a realizar processamento e o congestionamento da rede.

6 Objectivos de Segurança

Os objectivos de Segurança têm o objectivo de mascarar ou eliminar ou diminuir as vulnerabilidades enfraquecendo os riscos.

Os objectivos de segurança do nosso sistema passam por garantir:

- A autenticação de o utilizador.
- A autenticação do canal de comunicação entre servidor e cada cliente.
- A segurança dos dados.
- A disponibilidade de rede.
- Que em caso de falha catastrófica a entidade de administração sabe onde ocorreu o erro.

7 Mecanismos de Segurança

Os mecanismos de segurança implementados referentes aos dados guardados consistem em guarda-los num sistema de base de dados em que apenas a entidade de administração tem acesso.

Se apenas a entidade administradora tiver acesso à base da dados e esta for replicada a possibilidade de ocorrer qualquer tipo de falha é nula. Como apenas os administradores têm acesso, somente estes alterar os dados. Numa fase posterior seria relevante replicar a base da dados de forma a que qualquer erro ou perda teríamos sempre uma replicação de forma a que as falhas fossem ultrapassadas.

Em relação à autenticação do canal de comunicação todo a configuração no que toca à troca de mensagens é estabelecida tendo como base a construção de um canal seguro.

A autenticação do canal de comunicação é assegurada implementando vários métodos aprendidos na aulas para a construção de um canal seguro. Iniciando pelo protocolo de acordo de chaves Diffie-Hellman, acordando uma chave para parametrizar a chave simétrica a ser utilizada e acordando também a chave para assinar as mensagens seguida de uma implementação do protocolo Station-to-Station para verificar que de facto não existe a presença de um atacante do tipo Man-in-the-middle e posteriormente, após o canal seguro estar construído, passar à efectiva troca de mensagens.

A autenticação de o utilizador consiste neste mostrar a sua identificação.

Como referido anteriormente, a autenticação de o utilizador consiste neste mostrar a sua identificação, consistindo na apresentação do seu username e password, bem como de um código de activação baseado na autenticação multi-factor enviado para o seu e-mail que acrescenta uma camada adicional de protecção de identidade.

A disponibilidade da rede é garantida restringindo o número máximo de utilizadores. Em caso de alguma falha inesperada o administrador tem sempre acesso ao ficheiro de log do sistema podendo visualizar quais foram os últimos acontecimentos relevantes ao sistema e podendo inferir aquele ou aqueles que

causaram a falha, ou simplesmente para permitir observar que ocorrências estão a acontecer no sistema.

8 Considerações Finais

Em prol do desenvolvimento do software e da análise de segurança do mesmo, o grupo organizou-se no sentido da melhor produção final do produto, nomeadamente na calendarização e distribuição de tarefas.

A análise de segurança ao sistema em causa foi concluída identificando os principais pontos de ataque e tratando-os adicionando mecanismo de segurança, bem como a analise de mecanismos de segurança já implementados verificando a sua utilidade, necessidade e suficiência sobre a aplicação primeiramente desenvolvida.

Finalizando, tratando-se de uma análise de segurança a um sistema, com pouca semelhança a algum projecto realizado pelo grupo de trabalho e realizado num ambiente académico e com tempo limitado e reduzido, no geral, os resultados são tidos como conclusivos, informativos e satisfatórios.