Universidade do Minho

Licenciatura em Engenharia Informática

Unidade Curricular de Segurança de Sistemas Informáticos

Ano Letivo de 2023/2024

Concórdia

Serviço Local de Troca de Mensagens

Inês Marques[100606]

Maio de 2024

SSI

Índice

1. Introdução

Este relatório descreve o trabalho realizado no âmbito da disciplina de Segurança de Sistemas Informáticos do curso de Engenharia Informática da Universidade do Minho, no ano letivo de 2023-2024. O projeto teve como objetivo a criação de um serviço de conversação entre utilizadores locais de um sistema Linux, focando-se na segurança e robustez do programa, conforme abordado na matéria lecionada.

No contexto deste projeto, assume-se que os utilizadores já existem no sistema operativo, eliminando a necessidade de criação de novos utilizadores pelo serviço. Este serviço foi projetado para permitir a implementação de controles de acesso rigorosos e isolamento de processos. Estas características são cruciais para garantir que as mensagens sejam transmitidas e armazenadas de maneira segura, protegendo a integridade e a confidencialidade dos dados. Além disso, o sistema foi concebido para ser resiliente a falhas e capaz de operar eficientemente mesmo sob condições adversas.

Este relatório detalha todo o processo de desenvolvimento do projeto Concórdia, incluindo a arquitetura adotada, as práticas de segurança utilizadas, estrutura do código e sugestões de possíveis melhorias para futuros projetos semelhantes.

2. Solução desenvolvida

O projeto Concórdia foi desenvolvido para fornecer um serviço de conversação seguro entre utilizadores locais de um sistema Linux. Baseando-se nas práticas seguras observadas em sistemas como o qmail, o trabalho desenvolvido adota uma arquitetura modular onde os comandos dos utilizadores são separados do daemon de processamento. Essa separação é fundamental para a segurança, garantindo que cada componente opere com permissões mínimas e que uma falha num comando de um utilizador não comprometa o daemon.

Os utilizadores possuem permissões específicas para executar comandos do sistema Concórdia, processando informações e criando tarefas em formato de texto. No entanto, eles não têm permissão para executar estas tarefas diretamente, estas funções cabem ao daemon. As tarefas são enviadas para uma diretória comum, onde são armazenadas como arquivos de texto, aguardando o processamento pelo daemon.

Esta abordagem modular facilita a manutenção e a expansão futura do sistema, permitindo que o sistema incorpore novas funcionalidades de forma segura. As estritas permissões e o monitoramento contínuo do daemon garantem a integridade e a confidencialidade das mensagens, tornando o sistema resiliente a falhas e acessos não autorizados.

Em suma, embora a solução desenvolvida pelo projeto Concórdia seja inspirada por sistemas comprovados como o qmail, ainda há espaço para melhorias e ajustes. No entanto, demonstra como uma arquitetura bem planeada pode proporcionar um serviço de conversação seguro e eficiente, oferecendo uma base sólida para futuros desenvolvimentos.

3. Arquitetura do projeto

A arquitetura do projeto Concórdia é composta por vários componentes principais que interagem entre si para fornecer um serviço de conversação eficiente e seguro.

Os utilizadores possuem permissões específicas que lhes permitem executar os diferentes comandos do sistema Concórdia, fornecendo as informações necessárias para realizar as tarefas desejadas.

Os diversos programas Concórdia processam as informações dos utilizadores, convertendo-as em texto e registrando-as como tarefas. Essas tarefas são enviadas para uma diretória comum (/var/queue/new), que irá atuar como uma fila, onde ficam armazenadas, aguardando o seu processamento.

O deamon.c é um processo em segundo plano executado pelo utilizador “deamon” que monitora continuamente a diretoria /var/queue/new, aguardando a receção de novas tarefas. O funcionamento do deamon.c envolve verificar periodicamente a presença de novos arquivos na diretória, ler os arquivos quando novas tarefas são encontradas, verificar a validade das tarefas, realizar as ações necessárias e, por fim, eliminar as tarefas concluídas da diretoria. Além disso, o daemon mantém logs detalhados das tarefas processadas, garantindo a possibilidade de rastrear todas as ações realizadas.

4. Estrutura do código

O projeto Concórdia está organizado em várias pastas, cada uma com um propósito específico:

- **bin/:** Contém os binários gerados após a compilação.
- **includes/:** Armazena os ficheiros de cabeçalho (.h).
- **objetos/:** Guarda os ficheiros objeto (.o) gerados durante a compilação.
- **src/:** Nesta pasta encontram-se os ficheiros fonte (.c).
- **Makefile:** Script de automação para compilar o projeto.

Na diretoria src/, encontram-se diversos ficheiros fundamentais para o funcionamento do sistema. Os ficheiros concordia-*.c são responsáveis por receber comandos específicos e encaminhar as mensagens para o diretório de espera. O ficheiro deamon.c realiza a daemonização do processo e a identificação do tipo das tarefas a realizar. Além disso, task.c contém funções para processar as concordias gerais, group-task.c trata das concordias de grupos, e aux.c providencia funções auxiliares gerais, bem como funções de validação das tarefas. Estes ficheiros auxiliares (task.c, group-task.c e aux.c) organizam o código e suportam o deamon.c, permitindo uma melhor estruturação e manutenção do projeto.

O Makefile do projeto Concordia é um elemento essencial para gerar, construir e instalar o software. Este define como os diversos componentes do projeto são compilados e organizados em diretorias específicas. A estrutura do Makefile inclui a definição do compilador (gcc), flags de compilação e diretorias para os binários (bin), objetos compilados (objetos) e as diretorias de instalação (/bin/concordia). Além disso, garante a criação dos mesmos, caso não existam. O Makefile compila cada arquivo em src para arquivos objeto em objetos e, em seguida, liga esses objetos em executáveis na diretoria bin. Também define regras específicas para limpar arquivos compilados e para instalar os binários na diretoria final, com permissões apropriadas para segurança.

Esta abordagem modular e estruturada facilita o desenvolvimento, manutenção e segurança do projeto, garantindo que cada componente seja tratado de forma independente e organizada.

5. Segurança

Em seguida, irei explicar as medidas de segurança implementadas neste projeto. Estas medidas visam garantir a integridade, confidencialidade e disponibilidade das mensagens trocadas, bem como a proteção contra acessos não autorizados e outras ameaças, de modo a implementar uma programação defensiva.

No Makefile, as permissões e a propriedade dos ficheiros são cuidadosamente configuradas para garantir a segurança. Após a compilação, os binários são instalados na diretoria /bin/concordia com as permissões necessárias para que todos os utilizadores possam executar os programas concordia. No entanto, o programa mydeamon, que irá correr em background, é restrito ao utilizador deamon. As seguintes linhas do Makefile são responsáveis por isso:

```
# Alvo para instalar os binários em /bin/concordia
install: $(BINDIR)/mydeamon $(BINDIR)/concordia-ativar \
    $(BINDIR)/concordia-desativar $(BINDIR)/concordia-enviar \
    $(BINDIR)/concordia-ler $(BINDIR)/concordia-listar \
    $(BINDIR)/concordia-remover $(BINDIR)/concordia-responder \
    $(BINDIR)/concordia-grupo-criar \
    $(BINDIR)/concordia-grupo-remover \
    $(BINDIR)/concordia-grupo-listar \
    $(BINDIR)/concordia-grupo-destinatario-adicionar \
    $(BINDIR)/concordia-grupo-destinatario-remover

    sudo cp $(BINDIR)/mydeamon $(BINDIR)/concordia-* $(INSTALLDIR)/
    sudo chmod 755 $(INSTALLDIR)/concordia-*
    sudo chown deamon:deamon $(INSTALLDIR)/mydeamon
    sudo chmod 700 $(INSTALLDIR)/mydeamon
```

Ter um utilizador específico associado ao mydaemon oferece várias vantagens em termos de segurança. Por exemplo, isola o processo dos demais processos do sistema, protegendo outros processos e dados. Também facilita a monitorização das atividades do mydeamon, permitindo uma deteção rápida de atividades suspeitas. Além disso, as permissões de arquivos e diretórios são configuradas para que apenas o utilizador deamon tenha acesso, evitando modificações ou leituras não autorizadas (como será explicado mais detalhadamente a seguir). Por fim, reduz a superfície de ataque, pois o deamon não terá acesso a comandos ou recursos desnecessários do sistema. Estas vantagens contribuem para uma arquitetura de segurança mais robusta e eficiente.

No deamon.c, é criada a diretoria /var/quele/new caso não exista, com as permissões 0703. Isto permite ao proprietário (deamon) todas as permissões, impedindo que outros

utilizadores listem o conteúdo da diretoria, mas permitindo que possam adicionar tarefas. Os grupos não têm nenhuma permissão. Esta configuração garante que apenas o daemon pode gerir completamente a diretoria, enquanto outros utilizadores podem interagir limitadamente.

Na criação de tarefas pelo concordia-*.c, como os utilizadores são os criadores destas tarefas em formato texto, as permissões são definidas como 0004, permitindo apenas a leitura por outros utilizadores. O deamon, sendo o único com permissão para listar as mensagens na diretoria, sabe quais abrir para leitura.

Para as diretorias /mail/ e /grupos/, as permissões são 0700, permitindo que apenas o deamon possa modificá-las, visto que é ele quem cria os ficheiros, sendo por esse meio o seu proprietário. Esta configuração aplica-se também à criação de novas pastas referentes a grupos de utilizadores.

Ao criar ficheiros de texto que identificam mensagens recebidas de um utilizador específico, as permissões são definidas como 0400, significando que apenas o user deamon (o proprietário destas mensagens) pode ler esses ficheiros, sem permissão para alterá-los após o envio. Quando uma mensagem é lida, o nome do ficheiro .txt é alterado para "lido_", garantindo a integridade e proteção das mensagens.

Em relação às permissões para tarefas relacionadas com grupos, estas só foram possíveis graças às configurações feitas através do comando sudo visudo, que adiciona parâmetros específicos para que o deamon tenha as permissões necessárias para essas operações. As seguintes linhas do sudoers configuram estas permissões:

```
#includedir /etc/sudoers.d
deamon ALL=(ALL) NOPASSWD: /usr/sbin/groupadd, /usr/sbin/usermod, /usr/sbin/groupdel, /usr/bin/gpasswd, /usr/sbin/deluser
```

Resumindo, o facto de os utilizadores não poderem fazer modificações nas suas pastas nem nas dos outros utilizadores previne acessos não autorizados e garante a integridade dos dados. Esta separação de responsabilidades assegura que as operações são realizadas de forma controlada e segura, reduzindo o risco de falhas de segurança consequentes de ataques de outros utilizadores.

6. Conclusões

Ao longo do desenvolvimento deste projeto, enfrentei dificuldades específicas, como garantir ao daemon as permissões necessárias sem conceder todos os privilégios de root e encontrar uma maneira eficiente de organizar as mensagens de grupos para cada utilizador pertencente ao mesmo. Superar esses desafios exigiu muita pesquisa e estudo aprofundado.

No entanto, identifiquei algumas áreas onde melhorias poderiam ser implementadas para aumentar a eficiência e funcionalidade do sistema. Uma dessas melhorias seria a substituição da diretoria comum por FIFOs (First In, First Out) para a comunicação entre processos. Apesar de a utilização de uma diretoria comum para armazenar tarefas em formato de texto ser uma abordagem simples e direta, de fácil manutenção, o uso de FIFOs poderia melhorar a eficiência do processamento de tarefas, reduzir a latência na troca de mensagens e, em geral, ser mais adequado em sistemas de alta demanda.

Além disso, a implementação do comando concordia-resposta foi apenas parcialmente concluída, não sendo possível responder a grupos. Esta funcionalidade ampliaria significativamente as capacidades de comunicação do sistema, permitindo aos utilizadores enviar respostas não apenas a indivíduos, mas também a grupos dos quais fazem parte.

Outra melhoria potencial seria a criação de um ficheiro específico onde os utilizadores pudessem ver o resultado de comandos como concordia-listar ou concordia-ler, em vez de depender exclusivamente dos logs para listar essas respostas. Esta modificação tornaria a interação dos utilizadores com o sistema mais intuitiva e eficiente.

Apesar destas áreas de melhoria e dos desafios enfrentados, o projeto Concórdia alcançou os seus objetivos principais. A solução desenvolvida mostrou-se eficaz na criação de um serviço de conversação seguro e modular. Durante o processo de desenvolvimento, aprendi bastante sobre a importância da arquitetura modular, o gerenciamento de permissões e a segurança em sistemas de mensagens. Este projeto não só forneceu uma base sólida para futuros desenvolvimentos, mas também destacou a importância de contínuas melhorias e otimizações para atender às necessidades em evolução dos utilizadores.