Universidade do Minho - Dep.to Informática
2º Semestre, 2021/2022
Mestrado em Engenharia Informática
Gestão e Segurança de Redes

Ficha de Trabalho Prático Nº1

SNMPv2cSec

Objectivos:

- Consolidação dos conhecimentos sobre os protocolos, mecanismos e filosofias da arquitetura de gestão *Internet-standard Network Management Framework* (INMF), dando especial relevo aos aspetos de segurança e controlo de acesso.

Observações:

- O trabalho deverá ser realizado ao longo de 30 a 40 horas efetivas de trabalho individual.

Requisitos:

- Acesso a sistema com, pelo menos, um pacote *freeware* instalado com suporte a SNMP (versão 2, no mínimo): **Net-SNMP**, CMU-SNMP, SCOTTY, etc.
- Utilização opcional de APIs de programação que facilitem a implementação de primitivas SNMPv2c ou SNMPv1.

AVISOS:

- Não serão tolerados atropelos aos direitos de autor de qualquer tipo de *software*...

Bibliografia específica e material de apoio

Material de apoio:

- Manuais/Tutoriais do *net-snmp*;
- MIBs em `/usr/share/snmp/mibs` (ou diretoria equivalente da instalação);
- Recurso `http://net-snmp.sourceforge.net/wiki/index.php/Tutorials/`;
- Recurso `http://www.simpleweb.org/`;
- Recurso `http://www.snmplinks.org/`.

Bibliografia:

- M. Rose, *The Simple Book*, Second Edition, Prentice Hall, 1996.
- B. Dias, *Gestão de Redes*, PAPCC, Universidade do Minho, 1996.
- W. Stallings, *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*, Addison-Wesley, 2000.
- D. Mauro, K. Schmidt, *Essential SNMP*, O'Reilly, 2001.
- Ver outros recursos na área de "Conteúdo" no BB da UC e no material fornecido no início do semestre.

Modelo SNMPv2cSec

A inclusão de mecanismos de segurança para garantia de privacidade, autenticação e verificação da integridade dos dados foram definidos na segunda versão do INMF. No entanto, a sua implementação era opcional pelo que as duas primeiras versões do modelo, que passaram a ser conhecidas como SNMPv1 e SNMPv2c, não oferecem mecanismos de segurança nativos. Esses mecanismos são apenas garantidos pela terceira versão do INMF, comumente conhecida como SNMPv3, sendo que, na prática, não existe razão para os equipamentos e aplicações implementarem uma eventual versão SNMPv2. Ou implementam uma versão que não suporta mecanismos de segurança (v1 ou v2c) ou implementam uma versão que os suporta (v3).

Quando o suporte nativo para os mecanismos de segurança do SNMPv3 não está disponível, ainda é possível garantir o mesmo nível de segurança (ou até níveis de segurança superiores), mesmo que se utilize o SNMPv1 ou SNMPv2c. Nesse caso, a segurança não está embebida no protocolo normalizado, mas tem de ser implementada indiretamente à custa da semântica de objetos duma MIB especial que o permita. Esta estratégia é usada nalguns ambientes industriais onde a mudança do protocolo para a versão 3 era mais complicada de se conseguir do que a adoção duma MIB especial que permita implementar, não só os mesmos mecanismos de segurança previstos no SNMPv3, mas também mecanismos de segurança adicionais, como por exemplo, o não repúdio.

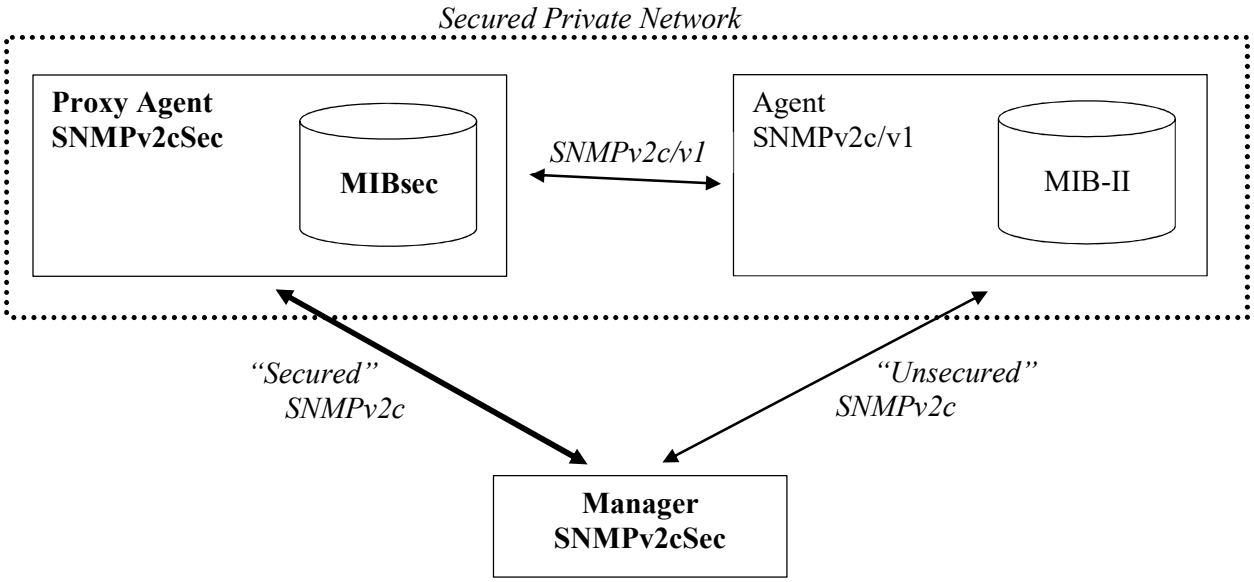

Figura 1: Interligação do agente proxy com um agente normal.

Assim, a forma mais simples de implementar esta segurança é acrescentar um agente proxy nativo SNMPv1 ou SNMPv2c que implementa esta MIB especial de segurança e que serve de interface seguro para um agente SNMPv1 ou SNMPv2c. Passaremos a designar o agente proxy como um agente SNMPv2cSec.

O agente proxy SNMPv2cSec fará de interface seguro para um agente SNMPv1 ou SNMPv2 normal, não seguro, conforme o esquema da Figura 1. Este agente normal pode ser independente e pode estar implementado e instalado numa máquina da rede interna/privada ou ser implementado na mesma máquina do agente proxy. Também pode ser um processo interno numa implementação integrada com o agente proxy, sendo esta opção ainda mais segura, mas menos modular.

Os objetivos principais deste trabalho é definir a MIBsec, construir um protótipo dum agente SNMPv2cSec e de um gestor SNMPv2Sec que implemente essa MIBsec e construir um protótipo dum gestor SNMPv2cSec que permita aceder de forma segura a alguns objetos da MIB-II dum agente normal para o qual o agente SNMPv2cSec faça de proxy. Não é necessário que o gestor e o agente SNMPv2cSec implementem todas as primitivas da norma SNMPv2c, mas é necessário a implementação de pelo menos a primitiva `get-request()` ou `get-next-request()` no gestor e a primitiva `response()` no agente proxy suportando a resposta às primitivas implementadas no gestor.

Comunicação SNMPv2cSec

A vantagem deste modelo é que não precisa qualquer alteração ao protocolo de comunicação SNMPv2c (ou SNMPv1). As alterações necessárias não são na sintaxe do PDU nem nas primitivas possíveis, mas sim na forma como os objetos da MIBsec são definidos e implementados.

Assim, a comunicação entre o gestor e o agente SNMPv2cSec pode ser feito utilizando as mesmas APIs do SNMPv2c já disponibilizadas por vários pacotes de software disponíveis publicamente (e utilizam a codificação normalizada BER) ou pode ser implementada de raiz para os protótipos do agente e do gestor como um protocolo aplicacional com uma codificação também a definir no contexto deste trabalho (e que seja mais simples do que o BER).

MIBsec

Esta MIBsec deve permitir definir mecanismos de segurança indiretos para manipulação segura dos objetos que são implementados nas MIBs normais dos agentes normais.

Assim, a MIBsec deve conter objetos que suportem a autenticação dos gestores, a encriptação dos valores dos objetos (e da sua identificação) acedidos indiretamente nas MIBs normais e a verificação da integridade dos dados trocados entre os agentes e o gestor. A MIBsec deve suportar também um mecanismo equivalente às vistas de controlo de acesso do SNMPv3. Opcionalmente, o agente SNMPv2cSec pode implementar mecanismos de segurança adicionais, comportamentais ou puramente tecnológicos.

Os protótipos devem suportar pelo menos operações seguras de leitura/monitorização dos valores das instâncias dos objetos das MIBs normais. Opcionalmente podem suportar operações seguras de escrita/configuração dos valores das instâncias dos objetos das MIBs normais.

No contexto do trabalho, deve ficar bem explícito a forma indireta de manipular com segurança os objetos duma MIB normal dum agente SNMPv2c normal, como por exemplo da MIB-II, através da manipulação direta dos objetos definidos para a MIBsec num agente proxy SNMPv2cSec.

Relatório e outras recomendações

O código dos protótipos do agente e do gestor devem utilizar, preferencialmente, apenas funções normalizadas da linguagem C, de preferência da norma 217 ISO (STD 17), e ou funções desenvolvidas pelo grupo de trabalho. Podem usar-se APIs, funções ou excertos de código de terceiros para implementar aspetos tecnológicos. Em caso de dúvida consulte o docente para verificar a adequação da sua utilização no contexto do trabalho.

Opcionalmente pode utilizar-se uma outra qualquer linguagem de programação que não a linguagem C. De qualquer forma, o código deve ser claro e usar convenções de nomeação de variáveis, tipos, funções

e constantes. O código deve ser estruturado duma forma o mais modular possível, sem complexidades desnecessárias, e permitir reutilização sempre que possível. A qualidade e correção do código não se mede pelo seu tamanho! Os alunos devem documentar/explicar o código criado através de comentários nas secções mais relevantes e no relatório. Todos os ficheiros do código devem ter um cabeçalho com a informação relevante que identifique os seus autores e explique as principais funções/classes criadas, tipos de dados e variáveis usadas, etc.

O relatório pode ser escrito no formato e no editor que for mais conveniente e deve incluir, no mínimo:

- Uma primeira página com o título do trabalho e a identificação do autor (incluindo fotografia), universidade, curso, unidade curricular e data de entrega;
- Um índice do conteúdo;
- Uma secção com a discussão das estratégias escolhidas, as opções tomadas, os mecanismos e tecnologias adotados, incluindo eventuais otimizações;
- Uma secção com a definição e explicação detalhada da MIBsec;
- Uma secção com a definição e explicação detalhada da forma de se atingir uma manipulação indiretamente segura dos objetos das MIBs dos agentes normais;
- Uma secção com a explicação e análise crítica das principais funções/classes implementadas, os seus principais méritos e a suas limitações mais importantes;
- Uma secção de conclusões que inclua uma eventual discussão sobre o que gostava de ter feito melhor ou de ter acrescentado e não conseguiu;
- Uma lista de eventuais referências bibliográficas, artigos científicos ou recursos informais na web e que tenham sido úteis.

O relatório é para ser avaliado pelo docente por isso não inclua informação genérica e irrelevante que o docente já conheça. Tente ser conciso e claro. Sempre que incluir uma afirmação importante no contexto do relatório e que seja de autoria de terceiros, ou que seja baseada diretamente em afirmações de terceiros ou concluída de informação retirada de recursos alheios, deve referenciar corretamente essas autorias ou proveniências e acrescenta-las na lista das referências.

O relatório pode incluir algumas partes relevantes do código quando estas ajudam às análises e justificações apresentadas. Não inclua código desnecessário no texto do relatório. Sempre que possível, comente antes o próprio código.

No material entregue inclua apenas dois ficheiros: um ficheiro PDF com o relatório e um ficheiro zip com todos os ficheiros do código do projeto dentro duma diretoria com o seguinte nome `GSR-21_22-Número_Aluno.zip`, como por exemplo, `GSR-21_22-83974.zip`.

Por fim, é recomendável que, durante a defesa do trabalho, tente responder honesta e concisamente apenas às questões colocadas por forma a que as sessões de apresentação não se arrastem muito para além dos 30-40 minutos.