Segurança de Redes e Sistemas de Computadores 2017/2018
Trabalho Prático nº 1 (v1.0, 22/Mar/2018)

Resumo

Neste trabalho pretende-se desenvolver um protocolo de segurança para comunicação em grupo que designaremos por STGC (Secure Transport for Group Communication) tendo em vista proteger comunicações IP em modo multiponto (IP Multicast - IPMC). A implementação permitirá estabelecer numa pilha STGC/UDP/IPMC uma camada genérica de segurança para transporte UDP de mensagens UDP suportado em IPMC. A proteção do protocolo STGC defenderá permitirá defender quaisquer aplicações de tipologias de ataques às comunicações tendo em conta algumas das tipologias de ataques definidas na framework de referência X.800. Um dos aspectos relevantes do trabalho é a concepção do protocolo STGC como serviço de segurança genérico, com comprovação de prova de conceito e a demonstração dessa generalidade com base numa uma aplicação concreta que será usada como demonstrador.

1. Contexto

A segurança de canais de comunicação em aplicações distribuídas suportadas em redes TCP/IP (ou Internet) podem ser asseguradas por protocolos de segurança normalizados e que visam proteger as comunicações a diferentes níveis dos serviços da pilha TCP/IP (o que se estudará em mais detalhe ao longo da disciplina).

Por exemplo, a implementação do padrão 802.11i garante proteção logo ao nível data-link, com autenticação de dispositivos (com base no subprotocolo EAP), controlo de acesso ao meio (com base no protocolo 802.1x) bem como autenticidade, integridade e confidencialidade de *frames* 802.11 em redes WiFi (com base nos protocolos WEP, TKIP ou CCMP). O protocolo IPSec fornece garantias de segurança para autenticidade de *endpoints* IP a partir do protocolo IKE/ISAKMP) bem como para confidencialidade e/ou integridade de pacotes IP (com base nos subprotocolos ESP ou AH). Finalmente, protocolos como por exemplo TLS ou WTLS, asseguram propriedades de segurança ao nível transporte, com proteção de autenticidade, confidencialidade e integridade de segmentos TCP encapsulados em records TLS, em canal fixo ou móvel (wireless). Todos os protocolos mencionados utilizam primitivas e algoritmos criptográficos e *ciphersuites* normalizadas parametrizáveis que usadas adequadamente em cada caso garantem as respetivas propriedades de segurança em bases de normalização. Dependendo do nível de suporte, garantem o estabelecimento de canais de comunicação seguros, aos diversos níveis da pilha TCP/IP com proteção das comunicações entre principais envolvidos.

No contexto do presente trabalho pretende implementar-se um novo protocolo de segurança (que se designará por **STGC** – ***Secure Transport for Group Communication***). O desenvolvimento deste protocolo, como camada genérica de segurança no empilhamento STGC/UDP/IPMC, permitirá que possa ser usado por qualquer aplicação que utilize comunicação UDP suportada em IPMC (por exemplo suportada em *sockets multicast*). Para implementação e demonstração da generalidade da solução será usada uma de duas aplicações (suportadas em UDP/IPMC) que podem ser encontradas nos materiais da aula prática (ver em http://asc.di.fct.unl.pt/~hj/srsc - labs), designadamente:

- **MCHAT.tgz**: Uma aplicação para suporte de sessões de CHAT em grupo, onde os participantes se juntam a sessões de CHAT associadas a grupos (endereços) IP Multicast;
- **STREAMING-STUFF.tgz**: Uma aplicação para suporte de disseminação de *media-streaming* (na forma de filmes/*trailers*), enviados por um servidor de *streaming* e que podem ser recebidos por um *proxy* local (cliente) que por sua vez os disponibiliza em tempo real para visualização com uma ferramenta, como por exemplo o VLC (https://www.videolan.org/index.pt.html).

Independentemente de cada grupo optar por uma ou outra das anteriores aplicações, como demonstradores de prova de funcionamento correto dos desenvolvimentos do trabalho, pode também usar o código fornecido em ***testMulticast.tgz,*** como aplicação mais simples que pode ser usada nos testes iniciais dos desenvolvimentos do protocolo STGC, antes de se usarem as outras aplicações anteriores.

2. Introdução

O protocolo STGC a implementar no TP1 deverá ser implementado como serviço genérico. Isto significa que pode ser adoptado para proteção genérica de qualquer aplicação que comunique via transporte UDP e IPBC (usando *sockets multicast*). A melhor forma de comprovar a generalidade da sua implementação é conseguir uma implementação em que a conversão de uma aplicação inicial (como as acima indicadas) que usa sockets UDP/IPmulticast (não seguros) passará a ficar protegida se usar o seu protocolo STGC. Para o efeito a conversão ser muito simples, obrigando ao menor número de alterações no código inicial. Como inspiração, isso poderá ser feito por substituição do uso de *sockets multicast* (MulticastSockets de acordo com o suporte java.net.MulticastSocket) por sockets seguros Multicast (que se poderão definir como STGCMulticastSockets). Estes últimos podem estender os primeiros, de acordo com o suporte da especificação de segurança do protocolo STGCM. Outra possibilidade é adoptar uma classe STGCDatagramPackets que estenderá a noção de DatagramPacket e conterá a proteção transparente dps pacotes transmitidos por UDP.

Deste modo, o trabalho será tanto mais conseguido:

- quanto menor for o impacto da conversão do código de uma aplicação não protegida (quer no número mínimo de linhas de código alteradas quer na minimização das alterações envolvidas);
- quanto mais flexível e parametrizáveis sejam os mecanismos de segurança subjacentes ao suporte criptográfico e parametrizações adoptadas para operação do protocolo STGC.

3. Modelo de adversário para o protocolo STGC

O protocolo STGC permitirá proteger de adversários que desencadeiam ataques às comunicações, tendo e conta a seguinte tipologia de ataques definidos na *framework* X.800 (estudado nas aulas teóricas). Estes ataques podem ser concretizações de ameaças por parte de potenciais oponentes com capacidade de acesso ao canal de comunicação e fluxos de tráfego (pilha UDP/IPMC/DataLink Layer):

- *Masquerading of principals (and their IDs)*
- *IDs will be established as identifiers in the form: "<Username>:<RFC 822 Email-Address>*
  Ex., "Henrique Domingos":"hj@fct.unl.pt"
- *Message Release*
- *Message Tampering*
- *Message-Replaying*

Garantindo necessariamente as seguintes propriedades de segurança:

- *Peer-Entity Authentication*
- *Data-Origin Authentication*
- *Access-Control*
- *Connectionless confidentiality*
- *Connectionless Integrity and Selective-Field Connectionless*

4. Protocolo STGC e seus componentes

O protocolo STGC é constituído por duas partes distintas (a seguir apresentados como dois subprotocolos específicos e ortogonais, embora complementares e integráveis) que designaremos por: STGC-TLP (STGC *Transport Layer Protocol*) e STGC-SAP (STGC – *Session Authentication Protocol*).

Para a implementação do trabalho os anteriores subprotocolos serão implementados de forma independente e em fases distintas:

FASE 1: desenvolvimento do subprotocolo STGC-TLP

A fase 1 é obrigatória para efeitos de entrega do trabalho prático nº 1, valendo até 15 valores.

FASE 2: concepção e implementação do subprotocolo STGC-SAP

A fase 2 não é obrigatória para efeitos de entrega do trabalho prático nº 1 mas a sua implementação e entrega será valorizada até 5 valores.

A implementação dos subprotocolos indicados será feita com base na utilização de sockets datagrama para IPMC e com recurso às primitivas criptográficas do suporte JAVA JCA/JCE (*Java Cryptographic Extension*) bem como respetivos provedores criptográficos compatíveis, particularmente o provedor BouncyCastle, de acordo com o contexto das aulas práticas / laboratórios.

As especificações iniciais de referencia para os subprotocolos STGC-TLP (Fase 1) e STGC-SAP (Fase 2) podem ser consultadas no documento: SRSC-TP1-Especificacoes.

5. Entrega do trabalho

Data de entrega. A partir de 9/Abril/2018 e com Data-Limite de entrega: 13/Abril/2018.

Sugere-se que os grupos organizem as agendas de trabalho antecipando a entrega a partir de 9/Abril/2018 (2ª feira) de modo a prepararem também o teste teórico a 14/Abril/2018. De qualquer modo cada grupo pode planear a realização do trabalho de acordo com a agenda mais adequada ao grupo.

Materiais a entregar. Os alunos receberão oportunamente (via CLIP) indicações complementares para entrega do trabalho, mas resumidamente, a entrega envolverá os seguintes elementos:

- Preparar um arquivo TP1-SRSC.tgz (tar gzip) com a implementação (código do projeto), com duas subdiretorias separadas, uma com a implementação da fase 1 (diretoria STGC-F1) e outra com a implementação completa da FASE 2 e FASE 1 (STGC). Se ambas as fases tiverem sido concluídas bastará existir a diretoria STGC e neste caso ambas as fases serão avaliadas na sua correção global.
- Ter o código (projeto) e o arquivo TGZ anterior disponíveis em repositório GITHUB ou BITBUCKET. Na data de entrega o projeto terá que estar partilhado (só em leitura) com o docente de modo que possam ser clonados (para verificação e teste pelo docente) a partir do respetivo URL do projeto, na data limite. A partilha será feita com:
- hj@fct-unl.pt no caso do GitHub
- henriquejoaolopesdomingos no caso do BitBucket
- Produzir um relatório (TP1-REPORT.pdf). Este será feito com base num formato do tipo ficha-resumo ou formulário, cujo *template* será publicado no sistema CLIP) e que deverá também ser colocado no repositório do projeto numa diretoria **docs.**
- No repositório do projeto, deverá ser incluída toda a informação (README) para se proceder à clonagem e teste de execução da implementação bem como indicações necessárias para o efeito.

Após análise das implementações e respetivo *reporting*, podem haver trabalhos e grupos selecionados que podem ser objeto de discussão/demonstração. Neste caso isso ocorrerá com base num escalonamento a indicar.

Entrega formal do trabalho. A partilha dos repositórios com as entregas finais deverá ser feita APENAS NA DATA DE 13/MARÇO/2018.

- *No* dia do teste (14/MAR/2018) os alunos terão que indicar (**na folha de resposta do teste**) qual o URL para clonagem no repositório do projeto. No repositório deverão estar todos os anteriores elementos. A não indicação do URL no teste de 14/Abril/2018 será penalizada na avaliação dos alunos que se não o fizerem. Caso não existam os elementos indicados no repositório do trabalho na data de 13/Março/2018 será considerado que o trabalho não foi entregue.
- Deve ter-se em conta que no teste (parte com consulta – teste prático) haverá questões relacionadas com o contexto de realização do trabalho bem como detalhes da sua implementação, por parte de cada grupo. Não esquecer que os testes são individuais.
- Será afixado depois no sistema CLIP a comunicação dos grupos que não entregaram o trabalho.