

ESQUEMA DE GERENCIAMENTO DE CHAVES PARA GRUPO MULTICAST SEGURO, COM ESTRUTURA HIERÁRQUICA

Andrés A. Level M.

Dep. Engenharia de Sistemas e Computação,
Instituto Militar de Engenharia
Rio de Janeiro, Brasil
level@ime.eb.br

ABSTRACT

This work describes the concepts and technologies requested to develop videoconferencing systems, and it presents the proposal to make the management of keys for multicast safe groups, as solution to the problem of rekeying of for videoconferencing participants in groups thoroughly distributed.

Keywords: Videoconferencing system, management of key, multicast.

RESUMO

Este trabalho descreve os conceitos e tecnologias necessárias para desenvolver sistemas de videoconferências, e apresenta a proposta de um esquema de gerenciamento de chaves para grupos multicast seguros, como solução ao problema de redistribuição de chaves para participantes de videoconferências em grupos amplamente distribuídos.

Palavras Chave: Sistema de Videoconferência, gerenciamento de chaves, multicast.

1. INTRODUÇÃO

O constante crescimento da Internet implica que novos problemas têm que ser enfrentados pelas diferentes comunidades de usuários. Existe um grupo de novas aplicações (videoconferências, jogos de guerra, sistemas de informação distribuídos em tempo real, entre outros) cuja demanda na Internet aumenta a cada dia, que são baseadas no modelo de comunicação de grupos [15], isto é, requerem a entrega de informação (pacotes de dados) de um ou mais remetentes autorizados para um grande número de receptores autorizados. Como resultado, comunicações seguras de grupos (isto é, que fornecem sigilo, autenticação e integridade na entrega de mensagens entre os membros do grupo) estão se tornando um ponto crítico de discussão.

Dentro do contexto das telecomunicações são cada vez maiores as exigências, tanto nas áreas tradicionais (militar, diplomática e governamental) quanto nas áreas: educativa, comercial, industrial e de comunicação pessoal, relacionadas à segurança nas comunicações. Com o desenvolvimento da tecnologia digital, foi possível a integração de diferentes tipos de informação (basicamente áudio, vídeo e texto) dando origem aos Sistemas Multimídias, que referem-se à transmissão simultânea de duas ou mais mídias, isto é, mídias que devem ser processadas/armazenadas/transmitidas durante um certo intervalo de tempo bem definido, geralmente com alguma interação com o usuário [12]. Da combinação de diversas mídias resulta um processo de comunicação e aprendizado mais agradável e eficiente.

Para satisfazer a urgente e forte necessidade por segurança na Internet, diversas soluções estão sendo desenvolvidas. Contudo, estas soluções são isoladas, e nenhuma interoperabilidade é prevista para aproximações conceitualmente diferentes. Algumas destas soluções trabalham em cooperação estreita com as aplicações, outras são incorporadas aos Sistemas Operacionais ou até mesmo embutidas nas camadas de Enlace e de Rede e muitas dependem da existência de componentes de rede confiáveis.

Para garantir o sigilo dos participantes da videoconferência, o texto, o áudio e o vídeo podem ser cifrados. Os sistemas de videoconferência utilizam cada vez mais a Internet devido a sua popularidade e baixo custo em relação às redes de alta velocidade, mas a qualidade da imagem e o som dependem do desempenho local da conexão dos usuários, pois esta Rede não oferece garantias de Qualidade de Serviço (*Quality of Service – QoS*).