Universidade do Porto
FEUP Faculdade de Engenharia

Mestrado Integrado em Engenharia Informática e Computação

5ºAno - Segurança em Sistemas Informáticos
Professor José Magalhães Cruz

"Android Secure Mesh"
Especificação

31 de outubro de 2013

Autores:
Fernando Guilherme Ferreira Sousa, ei09153@fe.up.pt
João Domingos Afonso Anes, ei09007@fe.up.pt

Introdução

O “Android Secure Mesh” irá ser uma aplicação que permitirá a diversos dispositivos android comunicarem entre si, proporcionando um serviço de chat sobre um canal seguro, trocando entre si actualizações.
Construindo uma rede descentralizada sobre uma rede Wifi já existente (ou estabelecendo uma rede mesh, pelos limites da plataforma Android), e criando um túnel seguro baseado num segredo partilhado, ou uma chave ou estabelecendo um protocolo de decisão, os dispositivos irão poder trocar mensagens entre si, sendo estas enviadas para uma interface em comum, onde todos podem ler e todos podem enviar mensagens

O principal objetivo é que a implementação da rede seja realmente confidencial e íntegra, permitindo apenas aos utilizadores envolvidos acederem e manipularem essa informação, resistindo a ataques “man-in-the-middle”, repetição e outros.

Motivação

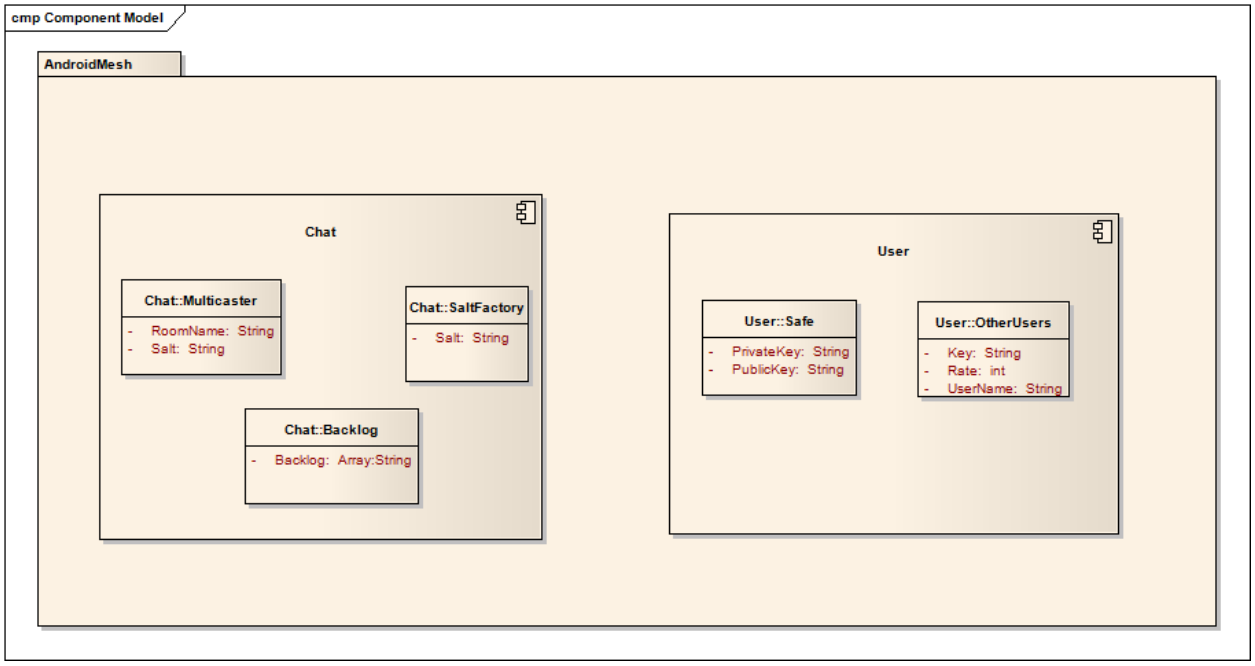
Os dispositivos móveis já fazem parte do dia-a-dia de cada um de nós e já entraram nas nossas vidas, tornando difícil que seja viver sem eles.
Tendo em conta todo este crescimento e com o facto que o conceito de segurança e privacidade é cada vez mais importante, achamos interessante esta abordagem descentralizada para tratar este problema. Também estaríamos a resolver um problema, que é a falta de aplicações desta área na plataforma em questão (Android).

Objetivos

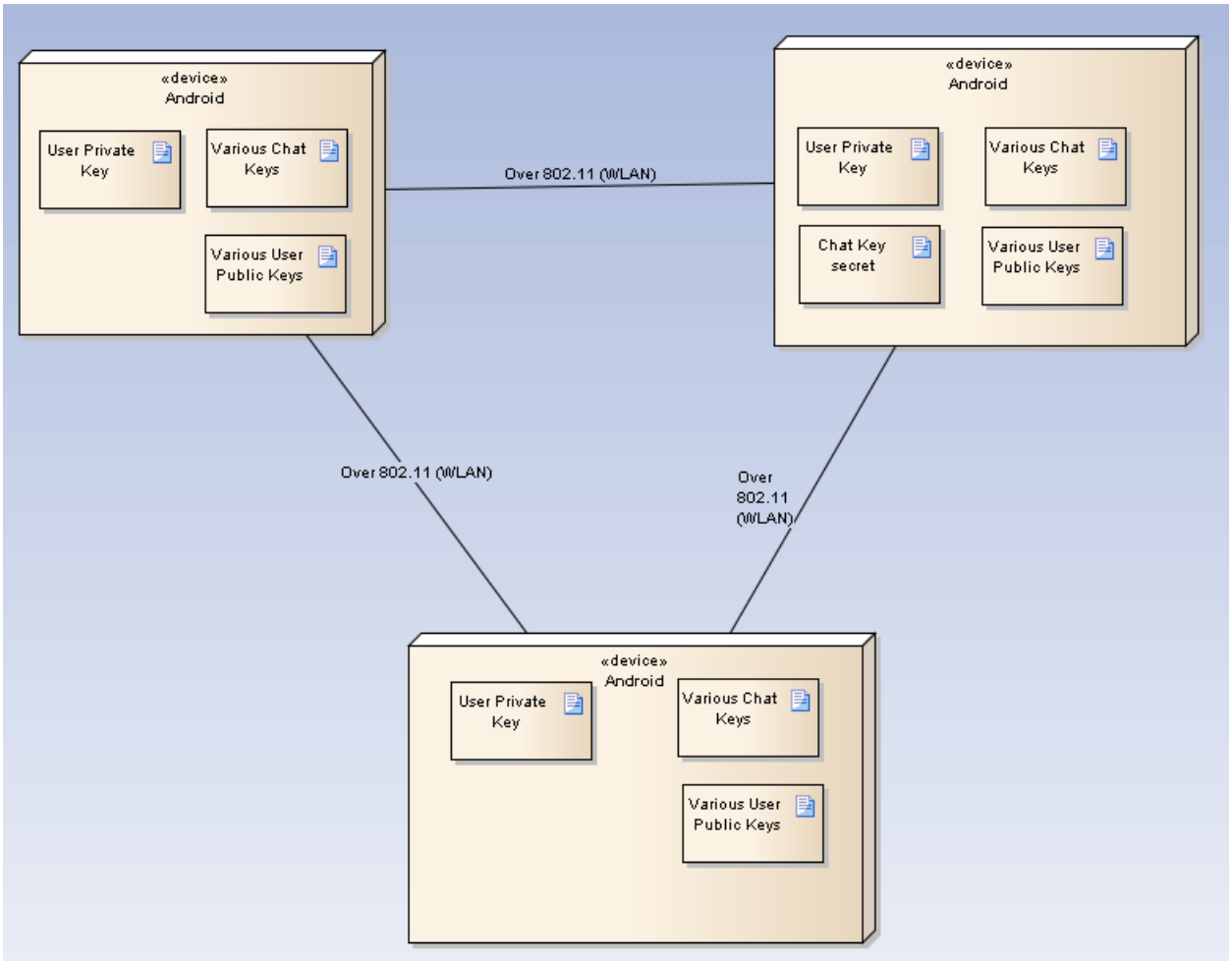
O principal objetivo é desenvolver uma aplicação nativa em Android, onde só os utilizadores da aplicação consigam aceder à informação, recebendo e enviando mensagens.
A aplicação irá então ter uma interface semelhante a um chat, onde é visível uma lista de mensagens que todos os utilizadores estão a enviar, desde o instante em que se entra na aplicação, tendo também uma caixa de texto que permita enviar uma nova mensagem para a conversa. Para tudo isto será necessário um registo na sala de chat. Tudo isto deve ser o mais transparente possível ao utilizador, exigindo apenas o seu input em momentos cruciais, como para preservar um segredo.

Arquitetura do Sistema

Neste “Component Model” pode-se ver que o component “Chat”, que representa todo o sistema de conversação segura que irá haver na aplicação tem um “Multicaster”, que tem um nome da Sala que será difundido em toda a gama de IP’s da rede. Existe também uma “SaltFactory” que contém um “Salt” e ainda um “Backlog” que irá guardar uma série de notas sobre tudo o que se passa nessa sala de chat.
Existe um outro componente “User” uma espécie de cofre onde contém uma “PrivateKey” e uma “PublicKey” e os outros utilizadores que ele irá interagir, guardará a respetiva “Key”, um “Rate” que contém a cotação desse utilizador (se é um utilizador com boa ou má reputação) e um “Username”.



No diagrama de “Deployment” vemos a forma como os dispositos móveis Android irão interagir entre si. Vê-se aqui que o sistema é descentralizado, porque todos interagem com todos, trocando as mensagens e chaves entre si.



Principais Casos de Utilização

- Criar um chat: Criar uma sala de chat com um nome próprio, que tem a sua chave (automaticamente e transparentemente gerada).
- Entrar no chat: inserir alguns dados necessários para entrar no chat, tais como username e uma chave.
- Avaliar utilizador: o utilizador pode sugerir uma avaliação positiva ou negativa a outro utilizador. As tabelas de reputação de toda a gente no sistema actualizam-se em resposta a este acontecimento. Caso um utilizador, numa sala de chat, receba muitas avaliações negativas, será expulso, por ter sido considerado um intruso.
- Troca de mensagens: permite que o utilizador possa interagir com os outros, na mesma sala de chat, através do envio e da receção de mensagens, através de um canal protegido por criptografia.

Bibliografia

- Android Security OverView - Android Developers, 2013. http://source.android.com/devices/tech/security/ (consultado em outubro de 2013)

- How Secure is Android, Really, 2013. http://lifehacker.com/how-secure-is-android-really-1446328680 (consultado em outubro de 2013)

- Android Cryptography, 2013. http://developer.android.com/reference/javax/crypto/package-summary.html (consultado em outubro de 2013)

- Mobile Phone Security, 2011. http://www.mayrhofer.eu.org/downloads/presentations/2011-10-19_Mobile_Phone-Security-Android.pdf (consultado em outubro de 2013)