SafeTrail: um modelo para controle de acesso baseado em perfis, contextos e trilhas

Márcio Ferreira da Silveira[1]
Jorge Luis Victória Barbosa[2]
Kleinner Farias[2]
Sandro Rigo[2]

Resumo: A computação móvel, a cada dia, está mais difundida, verificando-se uma quantidade crescente de pessoas utilizando seus recursos e interagindo a partir de seus dispositivos, de qualquer lugar e a qualquer momento. Muitas dessas interações envolvem informações e conteúdos confidenciais ou restritos, o que exige um nível de segurança para proteção dos usuários e de seus dados: a autenticação. Nesse sentido, soluções tradicionais de autenticação, pelo uso de um login e uma senha, vêm sendo substituídas por um novo modelo chamado de autenticação implícita, no qual o dispositivo reconhece o usuário a partir de seu histórico de acessos e de seu comportamento. As soluções de autenticação implícita existentes não oferecem um nível de segurança capaz de limitar o acesso a contextos e recursos específicos, combinando validações tanto da trilha de acessos dos usuários quanto dos seus perfis e permissões atuais. Com base nesse cenário, este artigo propõe o SafeTrail, um modelo para autenticação implícita com um controle de acesso, baseando-se em contextos, trilhas e perfis. O SafeTrail analisa os padrões comportamentais dos usuários, garantindo que cada um acesse apenas os recursos previamente autorizados. Este artigo descreve um protótipo que serviu como base para realizar uma avaliação por meio de cenários, na qual foram obtidos resultados positivos, com a liberação dos acessos apenas para usuários com os perfis necessários e adequados para os contextos e recursos em questão.

Palavras-chave: Computação ubíqua. Autenticação implícita. Contextos. Trilhas.

Abstract: *Mobile computing is every day more widespread, with an increasing number of people using its resources and interacting from their devices, from anywhere and at any time. Many of these interactions involve information and confidential or restricted content, which requires a specific level of security to protect users and their data: authentication. However, traditional authentication solutions, through a login and password, are being replaced by a new model called the implicit authentication, where the devices recognize the users from their history of access and behavior. The implicit authentication solutions already presented do not offer a level of security able to actually limit access to specific contexts and resources only to users authorized to do so by combining validations of the user's trail of the access and their current profiles,. Based on this scenario, this paper proposes the SafeTrail, a model for implicit authentication with access control based on contexts, tracks and profiles. The SafeTrail analyzes the behavioral patterns of users, ensuring that each one access only the resources previously authorized. It has implemented a prototype to validate the access requested by users through scenarios in which positive results were obtained, allowing access only to users with the correct profiles.*

Keywords: *Ubiquitous Computing. Implicit Authentication. Contexts. Trails.*

[1] Graduação em Sistemas de Informação, Universidade do Vale do Rio dos Sinos – Av. Unisinos, 950 – São Leopoldo, RS, Brasil
{marcio.f.silveira@gmail.com}
[2] Programa de Pós-Graduação em Computação Aplicada, Universidade do Vale do Rio dos Sinos – Av. Unisinos, 950 – São Leopoldo, RS, Brasil
{jbarbosa@unisinos.br; kleinner@gmail.com; rigo@unisinos.br}

http://dx.doi.org/10.5335/rbca.2015.5559

1 Introdução

Controlar o acesso físico (ou mesmo virtual) é uma das preocupações fundamentais quando se constrói ambientes reais como hospitais, grandes corporações, instituições financeiras e universidades, nos quais pessoas com diferentes tipos de permissão poderão circular. Em um hospital, por exemplo, é crítico controlar o acesso às salas de resultados de exames, aos consultórios e às salas de cirurgias, visto que, nesses ambientes, informações confidenciais de pacientes são geradas e armazenadas, recursos e materiais particulares dos médicos são utilizados e atividades envolvendo risco de morte ocorrem. Por isso, várias técnicas de controle de acesso foram desenvolvidas nas últimas décadas, tais como o controle de acesso usando login e senha ou dados biométricos.

Paralelamente, os dispositivos móveis também estão passando a apresentar uma tendência de interconectividade maior a cada dia. Combinado a isso, há a transferência de dados por meio da internet também em franco crescimento, pois mais e mais as informações estão acessíveis em qualquer lugar, a partir de qualquer dispositivo. Nesse contexto, com a crescente adoção da computação ubíqua [1], passou-se a receber informações relevantes de forma proativa. Isso é possível por intermédio do registro e da análise de contextos, que, segundo a visão de Anind Dey [2], nada mais são do que "qualquer informação que pode ser utilizada para caracterizar a situação de uma entidade". E por entidade compreende-se que possa ser uma pessoa, um lugar ou mesmo um objeto, desde que seja relevante para a interação do usuário com a aplicação a ser utilizada. Isso permite que as informações sejam recebidas no momento em que elas são necessárias e no local onde elas são realmente importantes. Com o avanço na utilização da computação ubíqua [1], expande-se o uso dessas tecnologias para viabilizar a autenticação de usuários nesses ambientes [3].

Um formato tradicional de autenticação de usuários é o de credenciais simples: um login e uma senha. Nesse modelo, existem perfis previamente criados, e cada usuário é relacionado a um ou mais desses perfis, determinando quais funções ele poderá exercer no ambiente, a que locais ele terá acesso, que diretórios e arquivos poderão ser utilizados em uma rede, e se eles poderão ser alterados ou excluídos. A autenticação com o uso de credenciais abre espaço para alternativas, como a autenticação [4] e o controle de acesso [5,6] a partir de contextos [2]. Essa opção consiste em aplicar conceitos e recursos propostos pela computação ubíqua [1], permitindo que os dispositivos registrem o histórico das pessoas e analisem seus comportamentos, seus arquivos acessados, locais e frequência em que ocorrem esses acessos, determinando quais usuários podem ter acesso a determinados conteúdos ou recursos. Esse histórico de contextos é chamado de trilha [7,8] e reúne informações sobre as últimas ações dos usuários, cada contexto registra o que o usuário acessou, além de quando e de onde ocorreu esse acesso. Com base nesse conjunto de contextos, obtém-se um histórico detalhado do usuário e seus comportamentos [9]. No entanto, a autorização de acesso dos usuários só é possível por meio da análise do perfil de cada uma das permissões pré-estabelecidas para cada perfil, e não apenas pelo histórico de acessos.

Diante dessa necessidade de controlar o acesso usando informações de contexto, este artigo propõe o SafeTrail, um modelo de autenticação por contextos [2], trilhas [7] e perfis [9], em que se aprimorou o controle de acesso dos usuários em relação aos modelos semelhantes estudados, garantindo que cada indivíduo tenha as permissões corretas para acessar apenas os contextos e recursos adequados. O fator principal desse modelo é o uso de trilhas para controlar os novos acessos, baseando-se no histórico de cada usuário [7]. Combinado a isso, o modelo considera o perfil do usuário para validar e conceder um novo acesso a um contexto já utilizado assim como para autorizar o acesso a um contexto novo.

O modelo propõe dois níveis de controle de acesso. O primeiro avalia as permissões do usuário a um determinado contexto, ao passo que o segundo verifica o acesso aos recursos disponíveis nesse contexto. E mesmo que o usuário tenha em sua trilha o registro de um acesso anterior a um determinado contexto ou recurso, o modelo verifica se tanto o usuário quanto o contexto ou recurso se mantêm ainda com os mesmos perfis e permissões. Caso tenha ocorrido alguma alteração em pelo menos um dos perfis, o SafeTrail verifica novamente se o usuário de fato tem as permissões adequadas para acessar o contexto ou recurso solicitado. Dessa forma, é possível garantir que cada indivíduo acesse apenas os contextos e os recursos para os quais tem permissão, sem a necessidade de uma autenticação adicional por meio de login e senha. Alguns cenários foram sintetizados para avaliar o modelo proposto. Os resultados obtidos mostram a utilidade e a efetividade para controlar o acesso de usuários em um ambiente hospitalar.

O artigo está organizado em seis seções, com esta introdução. Na seção 2, são discutidos os trabalhos relacionados ao tema proposto. A proposta do modelo SafeTrail para autenticação sensível ao contexto, trilhas e

perfis é apresentada na seção 3. Na seção 4, são apresentados os resultados obtidos com os cenários montados para avaliação do modelo SafeTrail. Na seção 5, são apresentadas as considerações finais.

2 Trabalhos relacionados

Os trabalhos estudados apresentam em suas estruturas alguns recursos que permitem o controle de acesso em ambientes sensíveis ao contexto, com características próprias e que são utilizados em diversas áreas.

A infraware [10] é uma plataforma que atua com o recebimento e o tratamento das requisições das aplicações e do controle de acesso e de privacidade dos usuários por intermédio de um módulo específico para isso. O modelo também soluciona o problema do acesso e da integração dos dados, utilizando uma infraestrutura dedicada, manipulando as informações de contexto de diversos domínios.

O UbiCOSM (Ubiquitous Context-based Security Middleware) [11] é um middleware desenvolvido com foco no controle de acesso sensível ao contexto. Com ele é possível que administradores de segurança de uma empresa ou ambiente qualquer definam quais diretivas do sistema de controle de acesso querem utilizar para impedir o acesso indevido aos seus serviços locais. Além disso, o middleware permite que os usuários determinem os requisitos de privacidade que deverão ser atendidos ao divulgar informações pessoais no exato instante em que acessam um novo contexto [11]. Em sua arquitetura estão presentes os módulos responsáveis pelo controle do sistema. Além deles, também há o módulo gerenciador de políticas, o módulo gerenciador de instalação de políticas, o gerenciador de autorizações e, ainda, o gerenciador de segurança sensível ao contexto. O UbiCOSM baseia-se no contexto para determinar o nível de segurança empregada na especificação das políticas de execução. Diferente de outros modelos de controle de acesso, nele, as permissões estão ligadas diretamente aos contextos, e não à identidade de usuários e funções [11].

O AWARENESS (Context-AWARE NEtworks and ServiceS) [12] é um modelo desenvolvido em conjunto por instituições holandesas – incluindo o governo – que tem como objetivo a criação de uma infraestrutura para suporte a serviços e aplicações que sejam sensíveis ao contexto, com foco no controle de acesso dos usuários [12]. Para esse projeto, alguns cenários reais e específicos da área médica foram utilizados para demonstrar a aplicação, com o intuito de validar o modelo. Esse sistema visa à integração entre os serviços a partir dos conceitos da computação ubíqua, além de utilizar técnicas de processamento de informações contextuais e de aplicações proativas e aplicar ontologias para a descoberta de novos serviços. Sua estrutura prevê o suporte à mobilidade do usuário em ambientes também sensíveis ao contexto [10].

O middleware SOCAM (Service-Oriented Context-Aware Middleware) [13] utiliza a ontologia conhecida como CONON (*Context Ontology*), que permite às aplicações se comunicar e compartilhar dados. Ele foi concebido para oferecer suporte a tarefas, como aquisição de contexto, compartilhamento, análise do contexto, armazenamento de informações e disseminação dos contextos, além de serviços em locais que tenham um controle de acesso sensível ao contexto [13]. A aquisição do contexto é realizada pelos componentes *Context Providers*, que abstraem os contextos a partir de diferentes fontes externas ou internas, e os convertem na representação formal da ontologia CONON.

O EasyConn4All [14] é um modelo desenvolvido para executar o controle de acesso de usuários a partir do uso de contextos e trilhas, combinado com o papel do usuário. O modelo é organizado em cinco módulos que controlam o armazenamento de informações, que são comparadas pelos módulos responsáveis especificamente pelo controle de acesso. Esses módulos têm seus próprios recursos voltados a armazenamento, exclusão, alteração e inativação de registros. Em relação às atividades, o EasyConn4All gerencia somente aquelas que estão registradas em sua base de dados. Nenhuma atividade externa ao modelo ou não registrada pode ser controlada, uma vez que não possui regras cadastradas. Especificamente sobre o controle de acesso, o modelo o faz utilizando papéis e trilhas de acesso de cada usuário. Somado a isso, outro critério utilizado é a troca de confiança entre as entidades. Caso uma entidade confie em outra e queira compartilhar uma atividade para a qual ambas apresentem condições de realizar, a delegação de confiança do modelo permitirá o acesso.

Nenhum desses modelos combina a validação da trilha do usuário com seu perfil atual e também com o perfil do contexto ou recurso ao qual o usuário está solicitando acesso. No SafeTrail, caso o usuário tenha em sua trilha o registro de um acesso anterior a um determinado contexto ou recurso em um momento em que ambos tinham os perfis adequados para tal acesso, o modelo verifica se atualmente o usuário e o contexto ou recurso ainda possuem os mesmos perfis. Em caso positivo, o acesso é concedido. No entanto, uma vez que ao menos

um dos perfis, seja do usuário, do contexto ou mesmo do recurso tenha sido alterado, o SafeTrail realiza uma nova validação dos perfis para garantir que somente um usuário autorizado receba o acesso solicitado. Esse recurso torna o SafeTrail mais robusto, se comparado aos outros modelos aqui apresentados.

Na Tabela 1, pode-se verificar a comparação feita entre os modelos, considerando algumas características consideradas mais relevantes.

Tabela 1: Comparação entre os trabalhos relacionados e o modelo SafeTrail

Modelo	Sensível ao contexto	Baseado em trilhas	Baseado em perfis	Mobilidade	Contextos dinâmicos	Domínio	Controle de alteração de perfis
Infraware	Sim	Parcial	Sim	Não	Sim	Genérico	Não
UbiCOSM	Sim	Não	Não	Sim	Sim	Genérico	Não
AWARENESS	Sim	Não	Não	Sim	Sim	Médico	Não
SOCAM	Sim	Não	Não	Sim	Sim	Genérico	Não
EasyConn4All	Sim	Sim	Sim	Sim	Sim	Genérico	Não
SafeTrail	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**	**GENÉRICO**	**SIM**

Fonte: elaboração dos autores com base nos dados da pesquisa.

3 O modelo SafeTrail

Esta seção apresenta a descrição do modelo SafeTrail. Para isso, a seção 3.1 introduz os princípios e conceitos básicos considerados na elaboração dos modelos. A seção 3.2 apresenta a arquitetura do SafeTrail. A seção 3.3 discute as regras de acesso aos contextos e aos recursos. E, por fim, a seção 3.4 descreve detalhes sobre como o modelo foi implementado.

3.1 Princípios e conceitos básicos

O modelo de controle de acesso SafeTrail foi projetado a partir dos seguintes princípios básicos:

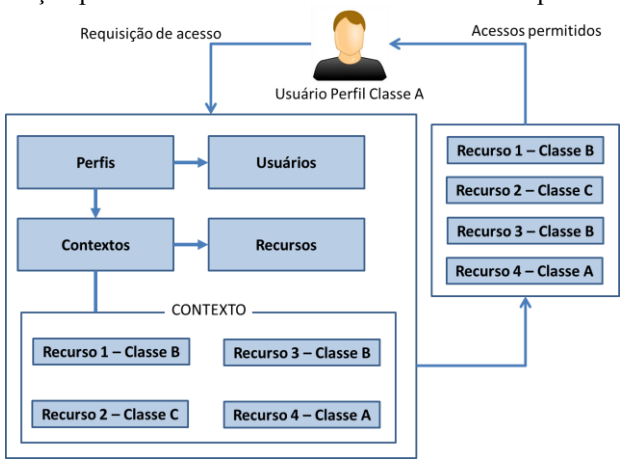
a) controle de acesso: cada acesso a determinado recurso dentro de um contexto tem um nível de controle que mantém a integridade das permissões concedidas aos usuários. Essa verificação é feita por módulos responsáveis pelo controle de acesso que analisam o histórico de contextos acessados e o perfil do usuário, validando se o acesso solicitado está de acordo com as permissões desse perfil, assim como com sua trilha;

b) perfis: cada usuário tem associado um perfil, utilizado no sistema para registrar e reunir os contextos e recursos que podem ser utilizados por cada um dos usuários. Os perfis cadastrados têm três níveis de segurança:

   - perfil classe A: é o nível mais alto, com acesso autorizado a todos os contextos e recursos disponíveis,
   - perfil classe B: nível intermediário, com acesso autorizado apenas aos contextos e recursos das classes B e C,
   - perfil classe C: trata-se do nível mais baixo, com acesso restrito aos contextos e recursos classificados como C.

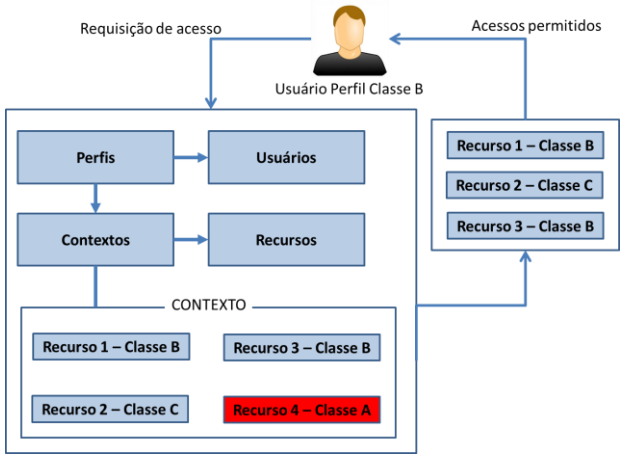
   É por meio da classe do perfil que o sistema identifica quais recursos estão disponíveis para o usuário quando ele faz uma requisição de acesso a um determinado contexto. Na Figura 1, apresenta-se uma requisição de acesso feita por um usuário de perfil classe A, em que todos os recursos lhe são disponibilizados, ao passo que na Figura 2, vê-se o mesmo acesso sendo solicitado por um usuário de perfil classe B e a restrição de acesso aplicada ao recurso classe A;

Figura 1: Autorização para acesso aos recursos de um contexto – perfil classe A



Fonte: elaboração dos autores com base nos dados da pesquisa.

Figura 2: Autorização para acesso aos recursos de um contexto – perfil classe B



Fonte: elaboração dos autores com base nos dados da pesquisa.

c) contextos: dentro de um determinado ambiente existem diversos contextos disponíveis. Por ambiente compreende-se uma rede de computadores com servidores, diretórios e arquivos, ou mesmo instalações físicas como a sede de uma empresa com diversas salas e equipamentos. Cada diretório ou arquivo de uma rede são recursos, assim como as salas de uma empresa também o são. Cada contexto armazena internamente dados, como os usuários o acessaram anteriormente, os perfis desses usuários, a classe do contexto e os recursos disponíveis. Os contextos classificam-se quanto ao seu nível de segurança:

   – contexto classe A: trata-se do contexto mais restrito, autorizado apenas para usuários de perfil classe A,
   – contexto classe B: contexto com nível médio de restrição, em que todos os usuários com perfis de classes A e B podem acessar os dados,
   – contexto classe C: é o contexto com o menor nível de restrição de acesso. Pode ser acessado livremente pelos usuários de todos os perfis.

   Esses níveis podem ser alterados por meio de uma configuração do sistema. Existe uma parametrização que relaciona faixas de horário ao longo do dia com a classificação que o contexto deve receber em cada um desses períodos, fazendo com que um determinado contexto tenha, por exemplo, um nível

mais restrito pela manhã (classe A), um nível intermediário de segurança na parte da tarde (classe B) e um nível sem restrição à noite (classe C). Por se tratar de um parâmetro do sistema, essa relação entre período do dia e classificação do contexto pode ser alterada no SafeTrail a qualquer momento. Como exemplo prático, pode-se considerar a sala do presidente de uma empresa. Para o período da manhã, compreendido entre 8h e 12h, essa sala recebe a classificação A, permitindo que somente o próprio presidente e seus diretores tenham acesso em caso de uma reunião do comitê diretor, que seria realizada das 10h às 11h. À tarde, das 12h às 18h, a classificação é alterada automaticamente para B, pois o presidente tem um encontro às 15h com todos os gerentes, que têm perfis também de classe B. Por fim, a partir das 18h, a sala recebe a classificação C, para que colaboradores de serviços gerais possam acessá-la e realizar a limpeza e organização do recinto;

d) recursos: cada contexto tem seu conjunto de recursos, que também são classificados de acordo com o nível de segurança necessária para cada um:
   - recurso classe A: trata-se do tipo de recurso mais crítico, destinado exclusivamente aos usuários de perfil classe A,
   - recurso classe B: com um nível médio de restrição, esses recursos podem ser acessados por usuários com perfis de classe A e B,
   - recurso classe C: com acesso autorizado a todos os usuários, esse tipo de recurso não oferece restrição de acesso.

   A relação dos níveis do perfil do usuário que solicita acesso e dos níveis dos contextos e recursos requisitados será determinante para a aprovação ou reprovação do acesso;

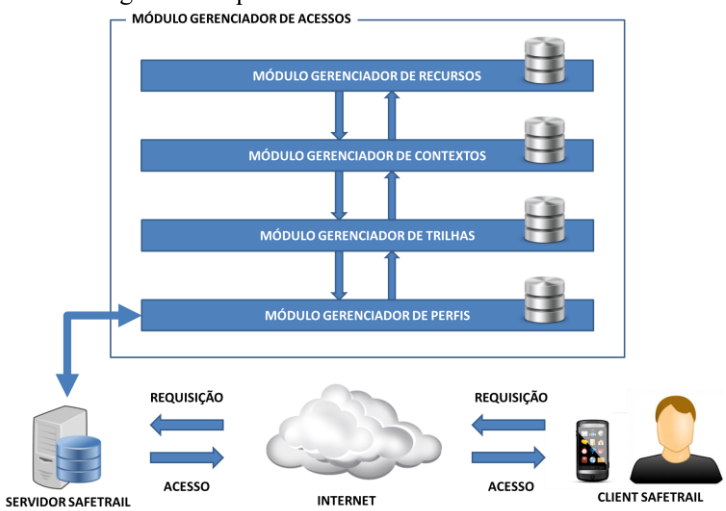
e) gerenciamento de trilhas: o sistema realiza um controle dos acessos feitos, contextos e recursos que o usuário utilizou, assim como níveis, data, horário e local de cada acesso, e registra tudo em uma trilha de contextos que será posteriormente consultada para controlar novamente o acesso aos mesmos contextos e recursos. Essas trilhas são analisadas em conjunto com o perfil do usuário para autorizar o acesso a contextos ainda não utilizados por ele;

f) definição de regras: o modelo permite que o administrador do sistema defina as regras para a concessão de acesso aos usuários, seja para contextos e recursos já utilizados seja para novas permissões baseadas em histórico e níveis de perfis, contextos e recursos.

3.2 Arquitetura SafeTrail

O modelo SafeTrail foi projetado usando uma arquitetura do tipo cliente-servidor, na qual o usuário poderá utilizar um dispositivo móvel com um aplicativo enquanto o sistema é executado em um servidor, com módulos de controle e bases de dados. A Figura 3 mostra a arquitetura do modelo.

Figura 3: Arquitetura do modelo SafeTrail



Fonte: elaboração dos autores com base nos dados da pesquisa.

A arquitetura projetada para o modelo SafeTrail inclui cinco módulos, detalhados a seguir:

a) módulo gerenciador de acessos: é o principal e engloba os demais módulos. É responsável por receber as requisições de acesso aos contextos dos usuários. Após a realização das validações necessárias em cada um dos módulos, o gerenciador de acessos responde para o usuário, concedendo-lhe ou não o acesso ao contexto solicitado e a seus recursos, de acordo com as permissões pertinentes ao perfil desse usuário;
b) módulo gerenciador de perfis: é responsável por identificar o perfil de acesso do usuário e seus dados;
c) módulo gerenciador de trilhas: é responsável por buscar as trilhas de acessos do usuário, identificando locais e horários em que ocorreram. Cada novo acesso é registrado e passa a fazer parte da trilha do usuário, sendo também analisado no momento em que um novo acesso for requisitado. Uma vez localizadas as trilhas do usuário, ocorre a análise dos contextos presentes nessas trilhas para identificar o histórico de contextos já acessados por esse usuário, utilizando-se o gerenciador de contextos;
d) módulo gerenciador de contextos: é responsável por identificar na trilha quais contextos especificamente foram acessados pelo usuário, assim como a sua classificação. Nesse ponto, ocorre a comparação entre a trilha e o contexto que está sendo solicitado no momento. Por fim, sabendo quais contextos foram acessados e qual está sendo o acesso requisitado no momento, chega-se aos recursos disponíveis;
e) módulo gerenciador de recursos: é responsável pelo controle dos recursos disponíveis em cada contexto. Um contexto, independente da sua classificação, pode conter diferentes tipos de recursos, de níveis distintos.

3.3 Regras para acesso aos contextos e aos recursos

A partir do momento em que um usuário requisita acesso a um determinado contexto, o modelo SafeTrail inicia um processo de validação em diferentes etapas. Primeiramente identifica o perfil desse usuário e sua classificação: A, B ou C. O modelo o reconhece a partir do seu login, que pode ser consultado em uma base externa, como o cadastro de colaboradores da empresa ou do local em questão. Com base nesse login, tem-se o perfil do usuário, que pode ser comparado aos três níveis de perfis registrados no SafeTrail.

Em seguida, o modelo consulta sua trilha de acessos anteriores e verifica quais contextos e quais recursos já foram acessados previamente pelo usuário e suas classificações. Ao localizar na trilha um acesso com sucesso ao contexto solicitado, o modelo busca também os recursos já acessados nesse contexto, e compara as suas classificações com o perfil do usuário. Todos os recursos já acessados nesse contexto que tenham a mesma classificação atribuída ao perfil do usuário estão automaticamente liberados para um novo acesso. O uso da trilha nesse momento tem como principal benefício a agilidade na identificação dos acessos autorizados para o usuário, baseado no seu histórico, pois a consulta à trilha é feita apenas no momento em que o usuário solicita acesso a determinado contexto.

Além da autenticação baseada em perfis e trilhas para avaliar o acesso do usuário a contextos já utilizados anteriormente, o SafeTrail também permite o acesso a um novo contexto, ainda não acessado pelo usuário. Esse acesso é concedido da mesma forma, desde que as regras do modelo sejam atendidas: a classe do perfil do usuário deve ser igual ou superior à classe do contexto e à classe do recurso que se quer acessar.

3.4 Aspectos de implementação do protótipo SafeTrail

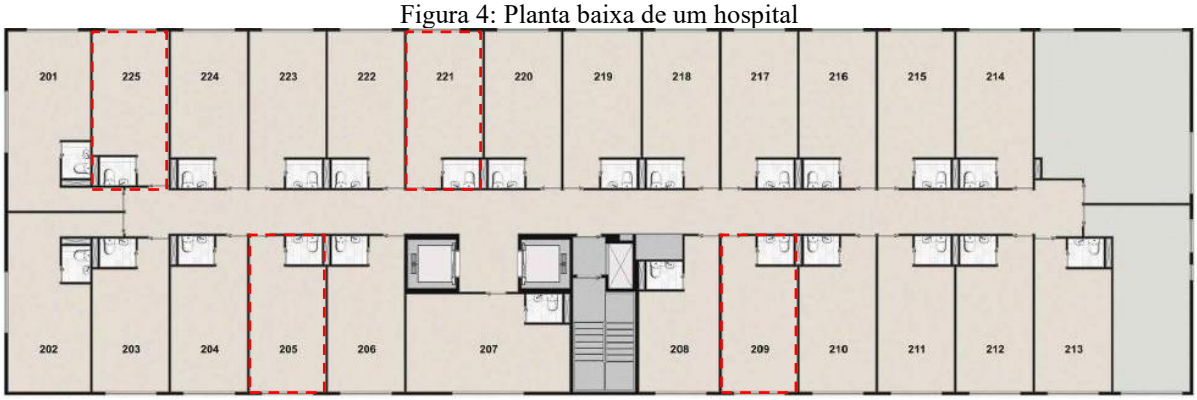
Um protótipo do modelo foi desenvolvido para smartphones com plataforma Android utilizando a linguagem Java, também denominado SafeTrail. Esse protótipo envolveu a criação de um banco de dados por meio da ferramenta MySQL Workbench 6.3, que fica hospedado em um servidor virtual da Amazon. Para permitir a comunicação entre o cliente Android e o servidor, foi desenvolvido um *web service*, responsável pela validação dos dados informados pelos usuários e pelos retornos do servidor, com as autorizações ou negações de acesso aos contextos e recursos. Novos usuários, contextos, recursos e informações de trilhas são incluídos no banco de dados também por intermédio do *web service*.

4 Avaliação

Com o intuito de avaliar os conceitos propostos pelo modelo SafeTrail, foi utilizado um ambiente hospitalar fictício para a criação de cenários. Em um ambiente como esse, existem diversas salas e itens que são tratados pelo modelo como contextos e recursos, respectivamente. O objetivo desses cenários é avaliar as funcionalidades do modelo ao acompanhar as tentativas de acesso de diferentes funcionários de um hospital a contextos e recursos do local.

A Figura 4 apresenta a planta baixa de um hospital de pequeno porte, representado no modelo SafeTrail, com a distribuição dos ambientes, aqui tratados como contextos, e dos equipamentos e móveis, vistos como recursos. Os contextos e recursos utilizados nos cenários foram cadastrados diretamente na base de dados do SafeTrail. Também foram cadastrados usuários com diferentes níveis de perfis, com o objetivo de validar algumas das possíveis combinações de acesso: nível maior ou igual ao do contexto ou recurso e nível mais baixo. Logo após a conclusão dos cadastros, o sistema – conectado ao banco de dados – foi executado em um smartphone, e as execuções dos cenários foram iniciadas.

Figura 4: Planta baixa de um hospital



Fonte: elaboração dos autores com base nos dados da pesquisa.

A Tabela 2 apresenta a lista dos contextos mapeados para o protótipo e utilizados durante os testes, destacados na representação da planta baixa do hospital (Figura 4).

Tabela 2: Contextos mapeados e cadastrados

Nome do contexto	Descrição do contexto	Perfil
Sala 205	Consultório Dr. Marcelo Rodrigues	A
Sala 209	Quarto hospitalar	B
Sala 221	Almoxarifado	C
Sala 225	Ambulatório	B

Fonte: elaboração dos autores com base nos dados da pesquisa.

A Tabela 3 apresenta a lista dos recursos mapeados e cadastrados para cada contexto no protótipo.

Tabela 3: Recursos mapeados e cadastrados

Nome do recurso	Nome do contexto	Perfil
Armário de medicamentos	Sala 205	A
Monitor cardíaco	Sala 205	A
Monitor cardíaco	Sala 225	A
Bomba de infusão	Sala 225	B
Cadeira hematológica	Sala 225	B
Oxímetro	Sala 225	B
Armário de insumos	Sala 221	C

Fonte: elaboração dos autores com base nos dados da pesquisa.

4.1 Cenário 1

Dr. Marcelo, médico do hospital, chega, portando seu smartphone, entra no prédio pela entrada principal no andar térreo e toma o elevador social até o segundo andar, onde fica seu consultório, na sala 205, em destaque na Figura 4. Ao sair do elevador e aproximar-se da porta de sua sala, Dr. Marcelo tem em mãos o seu smartphone e faz o login no aplicativo SafeTrail, de acordo com o apresentado na Figura 5a. Em seguida, ele verifica no aplicativo a lista de contextos cadastrados, como pode ser observado na Figura 5b. Nesse cenário, o sistema está exibindo a lista de contextos previamente registrados na base de dados, voltados exclusivamente para os testes. Não há identificação, nesse ponto, da localização do usuário dentro do hospital, e com base na exibição dos contextos, é indicado apenas o andar em questão. Dr. Marcelo seleciona, em um clique simples na tela do smartphone, seu consultório, conforme mostra a Figura 5c. Nesse momento, o SafeTrail verifica na trilha de acessos do usuário que ele já realizou com sucesso um acesso anterior ao mesmo contexto. Além disso, o modelo também identifica que não ocorreram alterações tanto no perfil do Dr. Marcelo (nível A ou *High*) quanto no perfil do contexto (também nível A ou *High*). Dessa forma, sem necessidade de validar as permissões do perfil do usuário em relação ao perfil do contexto, o SafeTrail libera novamente o acesso do Dr. Marcelo ao seu consultório, na sala 205, destrancando automaticamente a porta.

Figura 5a: Tela de login

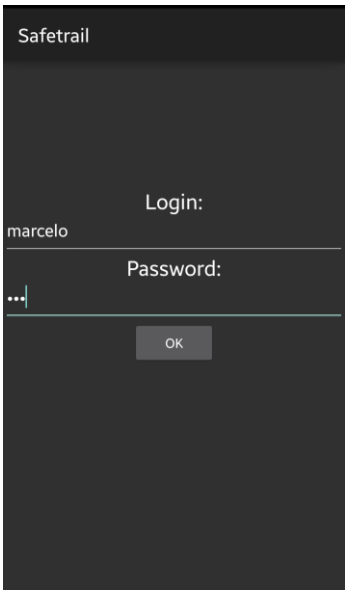


Figura 5b: Lista de contextos cadastrados

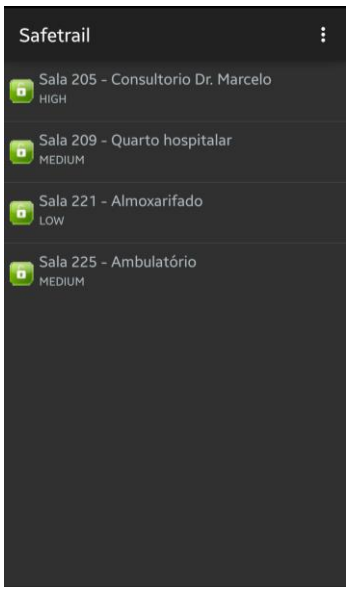
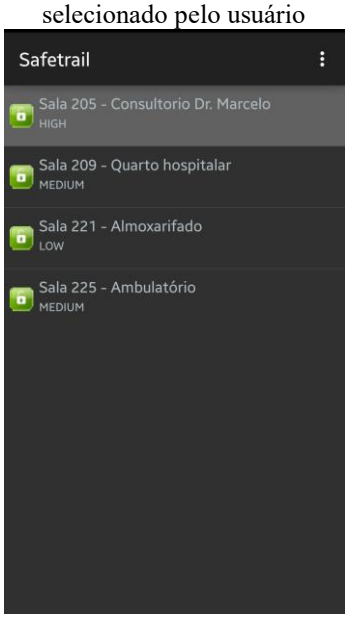


Figura 5c: Contexto selecionado pelo usuário



Após entrar no consultório, Dr. Marcelo consulta novamente o aplicativo SafeTrail e observa a lista de recursos disponíveis no contexto atual, conforme ilustrado na Figura 6a. Durante uma consulta, Dr. Marcelo precisa fazer um exame de monitorização dos batimentos cardíacos de um paciente. Dessa forma, mais uma vez acessa o SafeTrail em seu smartphone e seleciona o recurso Monitor cardíaco, como visto na Figura 6b. Nesse momento, o SafeTrail verifica na trilha do usuário que já houve um acesso positivo ao recurso solicitado assim como identifica que não foram realizadas alterações nos perfis do Dr. Marcelo (nível A ou *High*) e do Monitor cardíaco (também nível A ou *High*), concedendo novo acesso. O equipamento, que estava em modo *stand by*, é acionado automaticamente, liberando todas suas funcionalidades para o médico. A Figura 6c apresenta a mensagem exibida nesse momento, informando que o acesso foi autorizado.

Figura 6a: Lista de recursos cadastrados para o contexto acessado

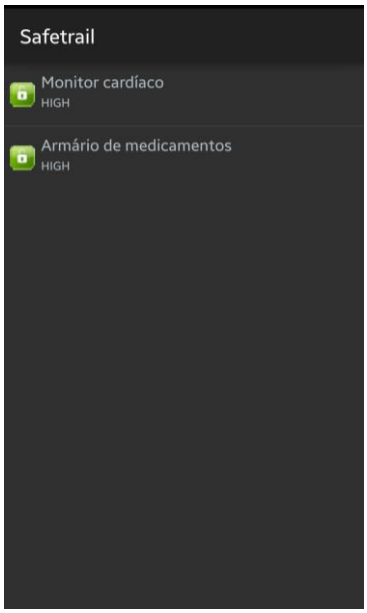


Figura 6b: Recurso selecionado pelo usuário

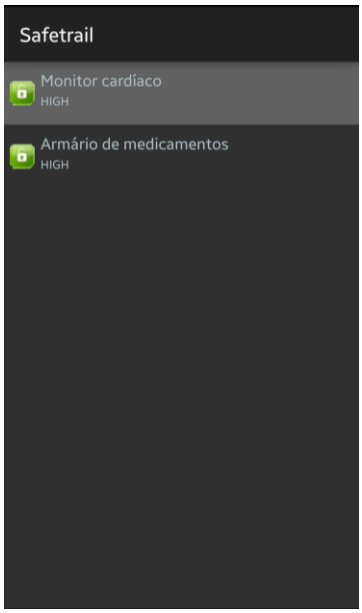
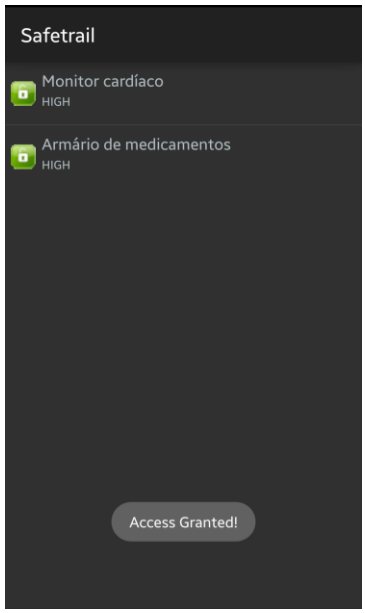


Figura 6c: Mensagem de autorização de acesso ao recurso solicitado



Ao final da monitorização dos batimentos cardíacos, Dr. Marcelo prescreve um medicamento ao paciente, e decide fornecer uma amostra grátis. Para isso, é necessário retirá-lo de seu armário de medicamentos. Com isso, ele acessa novamente o SafeTrail em seu smartphone e seleciona o recurso Armário de medicamentos, como demonstrado na Figura 7a. Como anteriormente, o modelo pesquisa na trilha do usuário e encontra um acesso prévio ao recurso informado com sucesso. Da mesma forma, identifica que não houve alteração nos perfis do Dr. Marcelo (nível A ou *High*) e do Armário de medicamentos (nível A ou *High*), liberando o acesso mais uma vez, de acordo com a Figura 7b. A porta do armário de medicamentos é destrancada automaticamente pelo sistema, e os remédios podem ser coletados.

Figura 7a: Recurso selecionado pelo usuário

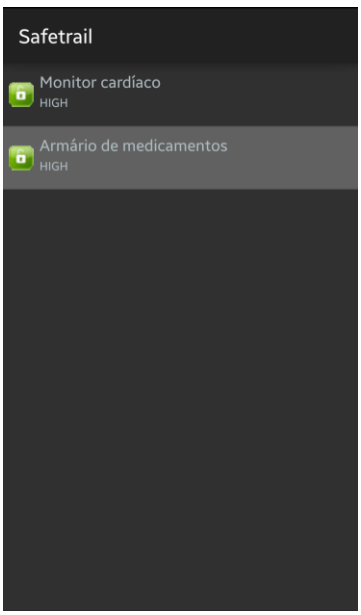
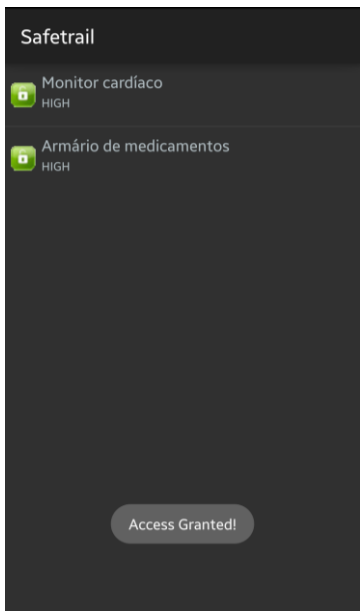


Figura 7b: Mensagem de autorização de acesso ao recurso solicitado



4.2 Cenário 2

Eduardo é enfermeiro e trabalha no mesmo hospital em que Dr. Marcelo atua. O enfermeiro chega ao prédio com seu smartphone, faz o login previamente no *client* SafeTrail, de acordo com a Figura 8a. Eduardo acessa o prédio pela entrada principal, no andar térreo, e toma o elevador social até o segundo andar, onde ficam os quartos destinados aos pacientes internados.

Ao sair do elevador, Eduardo verifica no aplicativo SafeTrail a lista de contextos cadastrados, como pode ser observado na Figura 8b. Em seguida, ele seleciona, por engano, em um clique simples na tela do smartphone, o consultório do Dr. Marcelo, conforme mostra a Figura 8c. Nesse momento, o SafeTrail verifica na trilha de acessos do usuário que ele não havia acessado com sucesso anteriormente esse contexto. Além disso, o modelo também identifica que o perfil do enfermeiro Eduardo (nível B ou *Medium*) não tem as permissões necessárias para acessar o consultório, uma vez que a essa sala foi atribuído o perfil de nível A ou *High*. Dessa forma, o SafeTrail não libera o acesso do enfermeiro ao consultório, mantendo a porta da sala trancada e exibe na tela a mensagem ilustrada pela Figura 8d.

Figura 8a: Tela de login

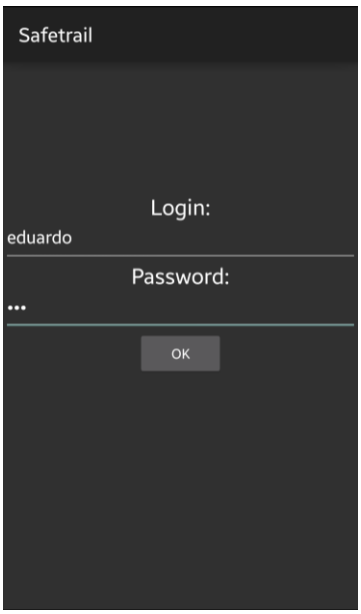


Figura 8b: Lista de contextos cadastrados

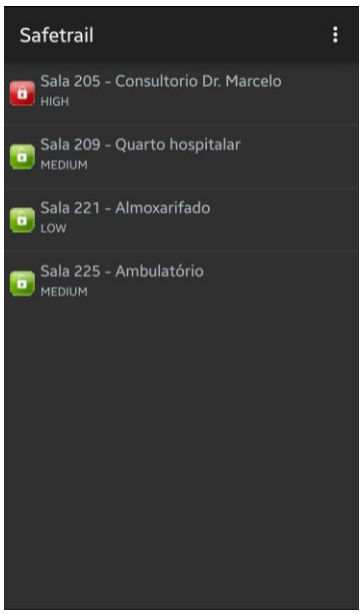
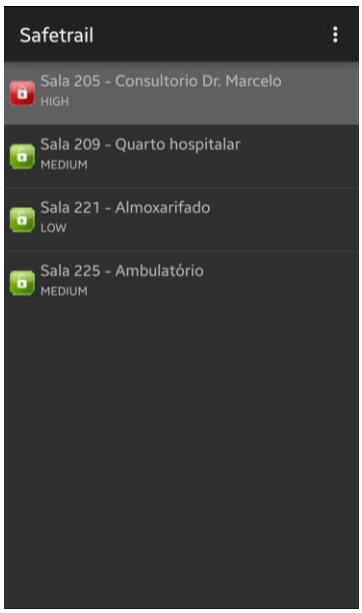
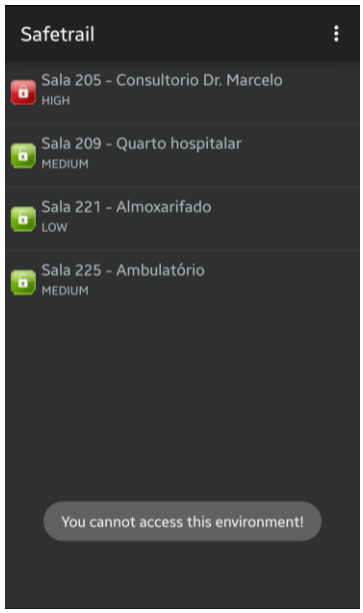


Figura 8c: Contexto selecionado pelo usuário

Figura 8d: Mensagem de restrição de acesso ao recurso solicitado





Em seguida, o enfermeiro continua pelo corredor central do segundo andar do hospital e aproxima-se do quarto 209, no qual ele precisa verificar a situação de um paciente. Eduardo consulta novamente a lista de contextos cadastrados, como pode ser observado na Figura 9a, e seleciona o quarto 209, conforme a Figura 9b. Nesse momento, o sistema verifica na trilha de acessos do usuário que ele já realizou com sucesso um acesso anterior ao mesmo contexto. Além disso, o SafeTrail também identifica que não ocorreram alterações, tanto no perfil do enfermeiro (nível B ou *Medium*) quanto no perfil do contexto (também nível B ou *Medium*). Dessa forma, sem necessidade de validar as permissões do perfil do usuário em relação ao perfil do contexto, o SafeTrail libera novamente o acesso do enfermeiro Eduardo ao quarto 209, destrancando automaticamente a porta.

Figura 9a: Lista de contextos cadastrados

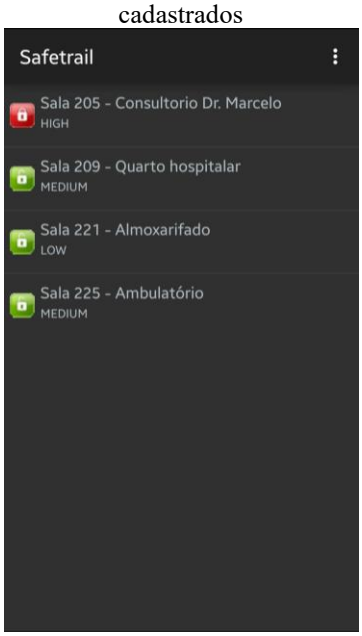
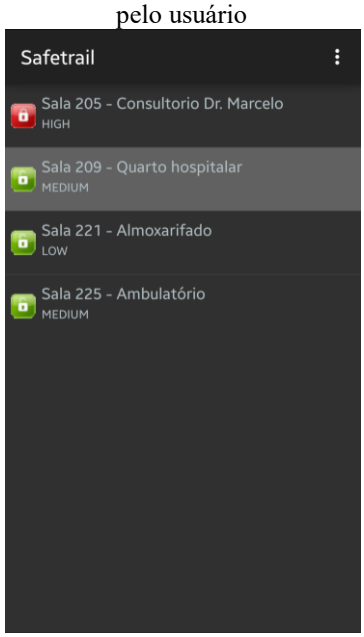


Figura 9b: Contexto selecionado pelo usuário



Após entrar no quarto, o enfermeiro Eduardo consulta novamente o aplicativo SafeTrail e observa a lista de recursos disponíveis no contexto atual, ilustrada pela Figura 10a. Ele deseja utilizar o monitor cardíaco

disponível no quarto para realizar a monitorização de batimentos do paciente. Eduardo seleciona o recurso por meio de um clique simples na tela do seu smartphone, como visto na Figura 10b. Nesse momento, o SafeTrail verifica na trilha de acessos do usuário que ele não realizou com sucesso um acesso anterior a esse recurso. Além disso, o modelo também identifica que o perfil do enfermeiro Eduardo (nível B ou *Medium*) não tem as permissões necessárias para acessar o monitor cardíaco, uma vez que a esse equipamento é atribuído o perfil de nível A ou *High*. Dessa forma, o SafeTrail não libera o acesso ao recurso, mantendo-o no modo *stand by*, e exibe na tela a mensagem ilustrada pela Figura 10c.

Logo após, Eduardo precisa acessar o Oxímetro para verificar os níveis de oxigênio no sangue do paciente. Para isso, ele seleciona o referido recurso por meio de um clique simples na tela do seu smartphone, conforme ilustra a Figura 10d. Então, o modelo verifica na trilha do usuário que já houve um acesso positivo ao recurso solicitado, assim como identifica que não foram realizadas alterações nos perfis do enfermeiro (nível B ou *Medium*) e do Oxímetro (também nível B ou *Medium*), concedendo novamente o acesso. O equipamento, que estava em modo *stand by*, é acionado automaticamente, liberando todas as suas funcionalidades. A Figura 10e apresenta a mensagem exibida, informando que o acesso foi autorizado.

Figura 10a: Lista de recursos cadastrados para o contexto acessado

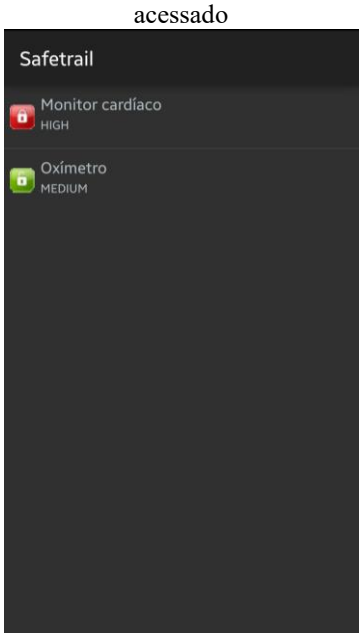


Figura 10b: Recurso selecionado pelo usuário

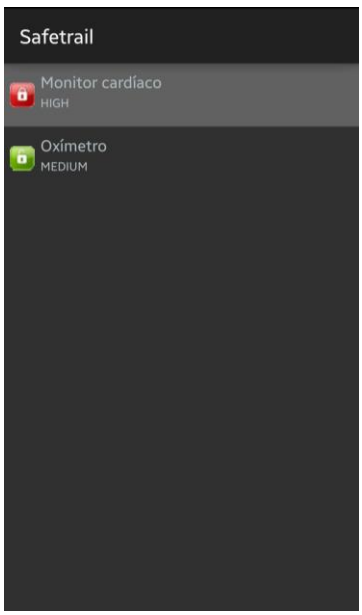


Figura 10c: Mensagem de restrição de acesso ao recurso solicitado

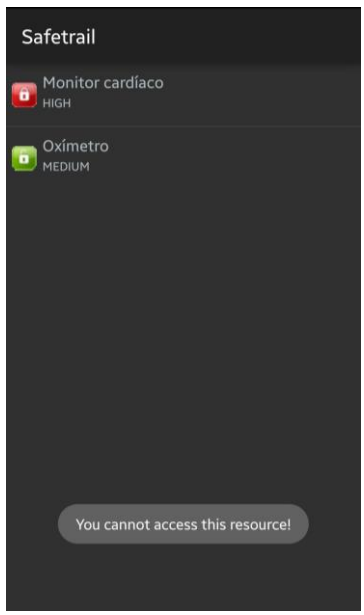


Figura 10d: Recurso selecionado pelo usuário

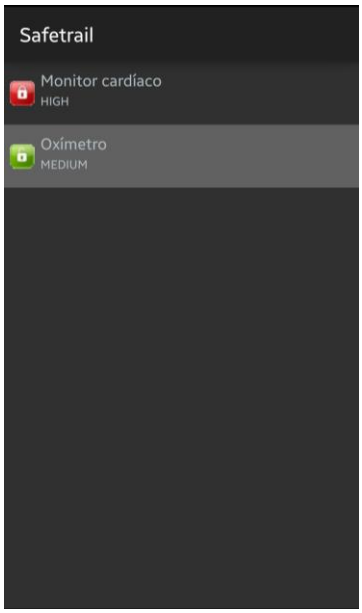
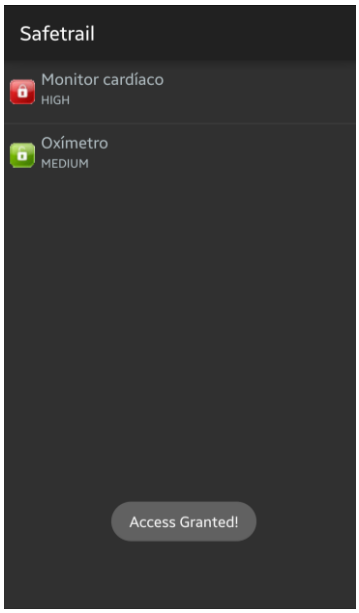


Figura 10e: Mensagem de autorização de acesso ao recurso solicitado



5 Conclusão

Este artigo apresentou o modelo SafeTrail para controle de acesso a partir de contextos, perfis e trilhas. Ao longo do texto, foram apresentados conceitos básicos, trabalhos relacionados, arquitetura do modelo e suas especificações. A partir da criação de cenários, foi possível testar o funcionamento do SafeTrail e concluir que o controle proposto é viável.

As avaliações mostraram que o modelo de fato exerce o controle de acesso proposto, autorizando os usuários a acessar contextos e recursos já utilizados por eles anteriormente, desde que estejam de acordo com o perfil do usuário que solicita tal acesso.

O principal ponto positivo do modelo SafeTrail está na segurança apresentada, ao permitir o acesso somente de usuários que realmente deveriam utilizar determinados recursos nos variados contextos disponíveis.

Como ponto fraco, o modelo exige o uso de um smartphone com o *client* em execução pelo usuário durante todo o tempo que os deslocamentos são feitos ao longo de toda a área coberta pelo controle de acesso, fazendo com que a liberação dos acessos não seja tão ágil.

Uma oportunidade futura de melhoria do modelo seria a utilização de crachás específicos para todos os usuários contendo etiquetas RFID (*Radio-Frequency Identification*) com os respectivos leitores posicionados junto às entradas das salas e dos equipamentos que exigem autenticação, validando a solicitação de acesso feita apenas pela presença do usuário em tais pontos. Dessa forma, o deslocamento dos usuários poderia ser mais livre, e a autenticação seria bem mais dinâmica, sem a necessidade de portar qualquer tipo de dispositivo extra. Para demonstrar tal aplicabilidade do modelo são necessários mais testes, com cenários mais complexos em ambientes reais.

Outro cenário de uso do SafeTrail seria na detecção de comportamentos anômalos dos usuários ou de configurações atípicas dos contextos para conceder ou não acesso a novos contextos ou recursos. Por exemplo, acontecendo um incêndio em um hospital ou corporação, o sistema de autenticação desenvolvido usando o SafeTrail reconfiguraria os privilégios previamente estabelecidos para atender à configuração da situação excepcional.

Referências

[1] WEISER, Mark. The computer for the 21st century. *Scientific America*, Armonk, v. l.l, p. 94-104, 1991. Disponível em: <http://dx.doi.org/10.1145/329124.329126>. Acesso em: 4 dez. 2015.

[2] DEY, Anind K. Understanding and using context. *Personal and Ubiquitous Computing*, London, v. 5, p. 4-7, 2001. Disponível em: <http://delivery.acm.org/10.1145/600000/593572/10050004.pdf>. Acesso em: 4 dez. 2015.

[3] LIMA, João Carlos Damasceno. *Uma abordagem de recomendação sensível ao contexto para apoio a autenticação implícita em ambientes móveis e pervasivos baseado em conhecimento comportamental do usuário.* 2013. Disponível em: <https://repositorio.ufsc.br/handle/123456789/107473>. Acesso em: 4 dez. 2015.

[4] ROCHA, Cristiano Cortez da. *Uma arquitetura para autenticação sensível ao contexto baseada em definições comportamentais*. 2010. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/94219/284315.pdf?sequence=1>. Acesso em: 4 dez. 2015.

[5] MEHRA, Pankaj. Context-aware computing: beyond search and location-based services. *IEEE Internet Computing*, v. 16, n. 2, p. 12-16, 2012. Disponível em: <http://ieeexplore.ieee.org/ielx5/4236/6159208/06159215.pdf?tp%3D%26arnumber%3D6159215%26isnumber%3D6159208>. Acesso em: 4 dez. 2015.

[6] SCHIAFFINO, Silvia; AMANDI, Analía. Intelligent user profiling: artificial intelligence an international perspective. *Lecture Notes in Computer Science*, Berlin, p. 193-216, 2009. Disponível em: <http://www.exa.unicen.edu.ar/catedras/knowmanage/apuntes/56400193.pdf>. Acesso em: 4 dez. 2015.

[7] SILVA, Jader M. et al. Content distribution in trail-aware environments. *Journal of the Brazilian Computer Society*, Porto Alegre, 2009. Disponível em: <http://dl.acm.org/citation.cfm?id=1858492>. Acesso em: 4 dez. 2015.

[8] ROSA, J. H. et al. A Multi-Temporal Context-aware System for Competences Management. *International Journal of Artificial Intelligence in Education*, v. 25, n. 4, p. 455-492. Disponível em: <http://dx.doi.org/10.1007/s40593-015-0047-y>. Acesso em: 4 dez. 2015.

[9] WAGNER, André; BARBOSA, Jorge Luis Victória; BARBOSA, Débora Nice Ferrari. A model for profile management applied to ubiquitous learning environments. *Expert Systems with Applications*, v. 41, p. 2023-2034, 2014. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0957417413007203>. Acesso em: 4 dez. 2015.

[10] PESSOA, Rodrigo Mantovaneli et al. Aplicação de um middleware sensível ao contexto em um sistema de telemonitoramento de pacientes cardíacos. In: SEMINÁRIO INTEGRADO E SOFTWARE E HARDWARE, Campo Grande: SBC, 2006. v. 1. p. 32-46.

[11] CORRADI, Antonio; MONTANARI, Rebecca; TIBALDI, Daniela. Context-based access control for ubiquitous service provisioning. *COMPSAC, IEEE*, Los Alamitos, v. 1, p. 444-451, 2004. Disponível em: <http://www.computer.org/csdl/proceedings/compsac/2004/2209/01/220910444.pdf>. Acesso em: 4 dez. 2015.

[12] WEGDAM, Maarten. *AWARENESS: a project on context-AWARE NEtworks and ServiceS*. In: MOBILE & WIRELESS COMMUNICATIONS SUMMIT, 14. *Proceedings*... [S. l.]: [S. n.], 2005. p. 19-23. Disponível em: <http://www.eurasip.org/Proceedings/Ext/IST05/papers/293.pdf>. Acesso em: 4 dez. 2015.

[13] GU, Tal. A middleware for building context-aware mobile services. In: IEEE VEHICULAR TECHNOLOGY CONFERENCE (VTC-Spring 2004). *Proceedings*... Milan: [S. n.], 2004. p. 2656-2660. Disponível em: <http://dx.doi.org/10.1109/VETECS.2004.1391402>. Acesso em: 4 dez. 2015.

[14] ALBARELLO, Paulo César; MARTINI, Bruno Guilherme; BARBOSA, Jorge Luis Victória. Controle de acesso baseado na inferência em trilhas. *Revista de Sistemas de Informação da FSMA*, Macaé, n. 15, 2015. Disponível em: <http://biblioteca.asav.org.br/vinculos/000007/0000071D.pdf>. Acesso em: 4 dez. 2015.