5
Avaliação

Neste capítulo, descrevemos a metodologia e os resultados da avaliação qualitativa de uso e de desempenho do CoPS. A primeira parte deste capítulo trata dos experimentos realizados para avaliar como os usuários entrevistados utilizariam e controlariam o acesso à sua localização em cenários de um jogo fictício entre duas equipes competidoras. A segunda parte deste capítulo descreve alguns resultados da análise de desempenho do processamento de consultas de autorização de acesso ao contexto implementado pelo CoPS, com o intuito de estimar o quanto o tempo despendido nesse processamento pode influenciar no tempo total de aquisição ao contexto.

5.1
Avaliação qualitativa de uso

Nesta seção, descrevemos a metodologia, os cenários e os resultados da avaliação qualitativa do CoPS. Ela foi realizada através de entrevistas e experimentos com usuários em um ambiente de simulação de um jogo fictício (descrito no Apêndice A) no qual a informação de localização pode ser utilizada pelos usuários para coordenarem suas atividades e conseguirem atingir o objetivo de encontrar os equipamentos perdidos pelo Campus da PUC-Rio. Nos experimentos realizados, avaliamos os aspectos de uso do CoPS com o intuito de identificar como os usuários interpretam e manejam alguns dos controles de privacidade discutidos no Capítulo 3 (e.g., controle de visibilidade de localização, notificação e relatório de acesso, *plausible deniability*) para controlar o acesso à informação de localização. Nós não avaliamos todos os mecanismos de controle de privacidade (e.g., as políticas de controle de acesso, a hierarquia das políticas de privacidade, restrição temporal, dentre outros) por causa da complexidade de implementação do ambiente de simulação do jogo, da complexidade de projetar uma boa interface de gerenciamento da política de privacidade que ofereça todos os recursos providos pelo CoPS, e do tempo disponível para realização dessa pesquisa.

A redução do escopo de avaliação dos mecanismos de controle de privacidade oferecidos pelo CoPS simplificou o projeto da interface, visando a possibi-

litar que o seu projeto pudesse interferir o mínimo possível nos resultados dos experimentos. Uma boa interface, neste caso, é fundamentalmente necessária para que se possa isolar, as dificuldades ligadas à complexidade ou filosofia "da tecnologia", das dificuldades ligadas apenas (ou em primeira instância) à complexidade e projeto da interface. Para os experimentos realizados, a interface foi refinada (e redesenhada) várias vezes para estar tão sintonizada quanto possível com as expectativas dos usuários. Ainda assim, como mostrarão os testes, algumas questões levantadas sugerem a possibilidade de ter havido interferência da interface na apreciação da solução tecnológica.

5.1.1 Controle de privacidade na visão de usuários

Toda proposta tecnológica não pode perder de vista aqueles que vão em última instância decretar o seu valor e a sua relevância - os usuários. Por esta razão, essa pesquisa inclui um estudo sobre como os usuários interpretam e manejam alguns dos mecanismos de controle de privacidade propostos neste trabalho.

Dado que privacidade representa um conceito subjetivo e pessoal, nós temos o interesse de avaliar como um conjunto representativo de usuários (dentro de seu contexto social, cultural e princípios) expostos a situações que suscitam questões de privacidade usam os controles de privacidade do CoPS. O objetivo da avaliação é o de entender em maior profundidade o problema, e não o de prever e generalizar como "todos" os usuários (ainda que classificados em perfis diferentes) interpretarão as questões de privacidade e usarão a tecnologia. Como já colocado nos capítulos iniciais desta tese, esta generalização não faz sentido quando o assunto é privacidade.

5.1.2 Experimentos com usuários

O paradigma adotado para esta pesquisa foi o da pesquisa qualitativa. Denzin & Lincoln (92) resumem desta forma a essência da pesquisa qualitativa, comparada à quantitativa (p. 23): "A palavra qualitativa implica uma ênfase sobre as qualidades das entidades e sobre os processos e os significados que não são examinados ou medidos experimentalmente (se é que são medidos de alguma forma) em termos de quantidade, intensidade, volume ou freqüência." Os autores ainda ressaltam que os pesquisadores que aderem ao paradigma qualitativo estão focado na natureza socialmente construída da realidade, o que é particularmente pertinente para o foco da pesquisa desta tese. Uma pesquisa quantitativa sobre privacidade requereria a capacidade de medirmos

e analisarmos as relações causais entre variáveis, e não trataria dos processos - especialmente dos perceptivos e interpretativos, tão essenciais para as questões aqui discutidas. O paradigma qualitativo tem diferentes métodos a sua disposição, dentre os quais as entrevistas, a observação em campo, e a análise do discurso. Para efeitos desta tese, utilizamos o método de entrevista, com questões abertas, apenas motivadas por situações relativas a uma situação de jogo hipotético, como passamos a descrever. Nossos experimentos envolveram cinco usuários que realizaram entrevistas e testes em um simulador de um jogo fictício. Nosso intuito foi avaliar se esses usuários têm percepções que convergem ou divergem de algumas hipóteses de usabilidade do CoPS. Os experimentos realizados visaram especificamente descobrir se os mecanismos de controle de privacidade do CoPS são interpretados como efetivos (i.e., funcionam) e úteis (i.e., atendem às expectativas dos usuários) para os usuários "gerenciarem" a sua privacidade ao usarem uma aplicação sensível à localização.

Assim, pudemos obter indicações qualitativas sobre a "relevância percebida" dos recursos de privacidade oferecidos pelo CoPS. Alguns recursos foram selecionados entre os mais comumente oferecidos por serviços similares (30, 93, 94) e por aplicações de comunicação mediada por computador (por exemplo: chat, email, fóruns eletrônicos) e telefonia digital. Outros, porém, são específicos do CoPS, tais como políticas de controle de acesso, hierarquia de políticas de privacidade e o algoritmo de especificidade, o qual é usado como base para o gerenciamento de granularidade fina das demais funcionalidades, entre elas: perfis de privacidade, notificações de acesso, controle de precisão da localização divulgada, dentre outros.

Indicações quantitativas estatisticamente válidas sobre a usabilidade do CoPS não foram cogitadas na avaliação por duas razões principais: a) primeiramente, aplicações que usam o CoPS ainda não estão efetivamente implementadas em dispositivos práticos que possam ser usados extensamente em situações realistas de avaliação (por exemplo, em *Personal Digital Assistants* - PDAs); b) outra razão é que o tempo e a complexidade para elaborar e executar uma pesquisa quantitativa estatisticamente válida sobre o modelo conceitual do serviço dependem de pesquisas qualitativas que indiquem quais variáveis podem e devem ser significativamente quantificadas em uma pesquisa desta natureza, e isto extrapola os limites de prazo desta pesquisa.

Os principais aportes de indicações qualitativas sobre a relevância percebida dos recursos de privacidade oferecidos pelo CoPS são:

1. indicar significados de aspectos e dimensões de privacidade oferecidos pelo serviço;

2. sugerir questões para pesquisas mais aprofundadas sobre o significado e o uso de mecanismos de controle de privacidade; e

3. indicar alguns tipos de reações que o CoPS poderá suscitar em usuários do serviço.

Discussão sobre a metodologia de avaliação

Dado que privacidade é um conceito (psicologicamente muito) abstrato, variável (13, 31, 33), e acima de tudo, completamente dependente de contexto, um dos principais desafios com que nos deparamos para realizar os experimentos está relacionado à forma em que coletamos e interpretamos as evidências sobre as opiniões dos usuários a respeito da utilidade e efetividade dos mecanismos de controle de privacidade oferecidos pelo CoPS. Vale ressaltar que as evidências obtidas serão sempre "parciais", jamais generalizáveis. Ou seja, em nenhuma hipótese poderemos afirmar que, a partir das evidências coletadas, é possível comprovar que para todo X tal que X é uma pessoa e para todo Y tal que Y é uma situação que envolve controle de privacidade, é verdade que X saberá controlar sua privacidade na situação Y através do CoPS ou de qualquer outro serviço/arquitetura.

Tendo em vista que não conseguiremos colher evidências que tenham valor universal sobre as opiniões dos usuários, realizamos experimentos que expõem as nossas hipóteses, crenças ou expectativas (no sentido qualitativo) sobre a efetividade e a utilidade das funcionalidades do CoPS à refutação. As hipóteses avaliadas são descritas sucintamente a seguir, no entanto, elas estão mais detalhadas e elaboradas no Apêndice B.

Hipótese 1: Há situações em que o usuário deseja manter um compromisso entre sociabilidade e privacidade, disponibilizando a sua localização com diferentes granularidades (i.e., precisão) em função do dia/horário e dos usuários/grupos de requisitantes.

Hipótese 2: Existem usuários que não querem se ater a detalhes de configuração da política de privacidade para usar uma aplicação LBS. No entanto, eles desejam saber quais informações pessoais a seu respeito estão sendo divulgadas, como e para quem.

Hipótese 3: Existem usuários que não se preocupam se a sua localização é divulgada ou não.

Hipótese 4: Existem usuários que desejam criar, a priori, perfis de privacidade para diferentes papéis sociais que desempenham com a mediação,

necessária ou opcional, de uma tecnologia sensível a privacidade (e.g., professor, aluno, orientador, amigo).

Hipótese 5: Há situações em que, para não prejudicar o seu relacionamento social, o usuário deseja negar acesso à sua localização para um grupo de requisitantes, em um período pré-determinado, sem que os mesmos tenham conhecimento de tal atitude.

Visto que só nos resta avaliar se os usuários têm interpretações convergentes ou divergentes em relação às hipóteses definidas, estruturamos o processo de avaliação da seguinte forma: (a) enunciamos as hipóteses de usabilidade e efetividade do CoPS; (b) associamos a cada hipótese um cenário de avaliação possível; (c) elaboramos um teste em que pessoas "representativas" do público-alvo ao qual a tecnologia deve servir possam, por intermédio de sua ação, adotar atitudes e produzir julgamentos alinhados ou desalinhados com as nossas hipóteses.

Como a tecnologia ainda não está em produção (pois precisa provar o seu valor para justificar o investimento), tivemos que fazer concessões e trabalhar em condições artificiais de contorno, por exemplo, usando simulação em terminais de computadores ao invés de experimentos reais com *Palmtops/Laptops*.

Naturalmente, tais concessões e condições podem afetar a expressividade e interpretação dos resultados obtidos, pois os usuários estarão controlando a divulgação da sua localização em cenários hipotéticos que, comparados a situações reais de uso de uma tecnologia baseada em localização, não suscitam questões de privacidade que podem de alguma forma comprometer, lesar ou prejudicar o usuário, social ou financeiramente, por exemplo. Em função disto, definimos que os usuários entrevistados tinham que ser pessoas capazes de "abstrair" simulações em terminais e, além disto, decidimos que o simulador devia ser projetado e implementado na forma de um "jogo", que é uma maneira extremamente difundida de engajar as pessoas em um processo de abstração, motivadas por uma situação irreal, mas verossímil (ou análoga a uma situação verossímil). Esta prática é bastante difundida em pesquisas com usuários (95), e, a despeito da artificialidade dos contextos de observação, tipicamente produzem importantes indicadores de como os usuários reagirão em uma situação real.

Perfil dos participantes

O jogo simula a disputa entre duas equipes de três pessoas, todas elas atendendo ao seguinte perfil mínimo:

– Pessoas com idades entre 20 e 35 anos;

- Pessoas familiarizadas com simuladores em ambientes computacionais;
- Pessoas familiarizadas com o(s) espaço(s) físico(s) do Departamento de Informática da PUC-Rio;
- Pessoas que têm uma atitude favorável a jogos em grupo (como gincanas, por exemplo);
- Usuários de telefonia móvel;
- Usuários de serviços de chat;
- Usuários freqüentes de email.

Descrição dos testes com o simulador do jogo

Os testes realizados com os usuários através do simulador do jogo consistem da análise de alguns cenários específicos (descritos no Apêndice C) que fazem parte de um jogo fictício (descrito no Apêndice A) em que duas equipes concorrentes usam as suas informações de localização para se coordenarem na busca de alguns equipamentos perdidos no Campus da PUC-Rio. No jogo, os membros de cada equipe adotam diferentes estratégias para vencer a equipe adversária e/ou acomodar suas atividades e objetivos pessoais no contexto da competição que se desenrola.

Nesse experimento, o usuário tem que desempenhar o papel de um dos personagens do jogo em uma série de cenários distintos. Em cada cenário, o objetivo do usuário é contribuir para que sua equipe encontre os brindes perdidos por "Lévy Meses", fornecedor de equipamentos do Departamento de Informática da PUC-Rio, antes que a equipe concorrente o faça. Para fazer isto, o usuário deve utilizar o simulador do jogo implementado na ferramenta LoMC (*Location-based Mobile Collaboration tool*). Os cenários são comunicados ao usuário pelo sistema. O usuário também pode simular que está "andando pelo Campus", no RDC ou em outros prédios para encontrar os brindes perdidos, conforme apresentado no "*filme tutorial*" do jogo. O único meio de contato do usuário com os demais participantes é através do simulador. Através dele, o usuário pode também controlar e monitorar o acesso de outros à sua localização, bem como (tentar) obter a localização dos demais participantes de uma e outra equipe.

Metodologia de avaliação

Os experimentos foram realizados com cada usuário separadamente, em quatro etapas, seguindo duas técnicas comuns em IHC (Interação Humano-Computador): entrevistas abertas e experimentos do tipo "Mágico de Oz" (55, 56, 95) (simulação conceitualmente fidedigna de aspectos relevantes de uma tecnologia que ainda não está em produção). Essas etapas foram organizadas da seguinte forma:

- Primeiro, fizemos uma entrevista cujo objetivo foi determinar como os usuários lidam com as questões de privacidade presentes em aplicações de bate-papo (e.g., *Instant Messaging*) e telefones celulares;
- Segundo, averiguamos como os usuários acham que gerenciariam a privacidade da informação de localização em alguns cenários específicos do jogo. As opiniões dos usuários obtidas nessa etapa foram contrastadas com suas ações desempenhadas através do simulador. Isso nos permitiu avaliar o quanto as opiniões dos usuários obtidas na entrevista divergem de suas ações desempenhadas no simulador;
- Terceiro, realizamos testes com os usuários através do simulador do jogo, confrontando-os com cenários específicos através dos quais eles poderiam reforçar ou enfraquecer algumas hipóteses de usabilidade do CoPS; e
- Por fim, na quarta etapa, realizamos uma entrevista para investigar se o usuário conseguiu manejar o simulador, se as funcionalidades de controle de privacidade foram úteis para gerenciar o acesso à localização, quais foram as principais dificuldades encontradas, quão difícil seria utilizar os mecanismos de controle de privacidade em uma situação real do cotidiano em que outros usuários podem ter acesso à informação de localização, dentre outros.

Nos experimentos realizados através do simulador, o usuário tinha a função de desempenhar o papel de um dos personagens do jogo em 7 cenários distintos. Em cada cenário, o usuário recebia uma mensagem do sistema estimulando-o a desempenhar uma determinada tarefa, por exemplo, obter a localização de um outro usuário do mesmo grupo ou do grupo oponente, alterar a política de privacidade ou interagir com outros usuários. O administrador do simulador do jogo era responsável por desempenhar o papel dos usuários do grupo adversário e fazer consultas à localização do usuário entrevistado. Tais mensagens e consultas tiveram o propósito de "provocar reações" no usuário que o motivasse a alterar as suas preferências de privacidade, analisar as notificações e relatórios de acesso.

Os experimentos realizados com cada usuário duraram aproximadamente 90 minutos. Para analisar os resultados obtidos, gravamos o áudio das entrevistas e capturamos em vídeo (no formato .avi) os testes realizados através do simulador. Além disso, todas as ações dos usuários realizadas através do simulador (e.g., alteração na política de privacidade, mensagens recebidas e enviadas, comandos para obter a localização de outros usuários) foram registradas em um banco de dados para facilitar a geração de relatórios. O áudio e o vídeo foram gerados através do software de captura de tela *SnagIt* (96) e o simulador foi implementado em Java e está disponível em (97, 98).

5.1.3 Resultados

A seguir, discutimos as principais conclusões das entrevistas e experimentos com usuários. Nós mostramos como as opiniões e atitudes dos usuários em relação ao controle de privacidade da sua localização reforçam ou enfraquecem as hipóteses de usabilidade do CoPS.

Principais conclusões dos experimentos

Nas entrevistas realizadas nas duas primeiras etapas, *os usuários reportaram que se preocupam com privacidade "on-line" em relação ao acesso a seus dados pessoais ou em situações em que terceiros podem derivar conclusões a seu respeito.* Por exemplo, deduzirem que estão no trabalho, ou que estão descansando, namorando, etc. Entretanto, em alguns cenários do jogo, houve usuário que, apesar de afirmar que se preocupa com a sua privacidade, não restringiu o acesso a sua localização para o grupo adversário, mesmo em situações em que os seus adversários pudessem inferir as suas ações. Esta é uma evidência real que demonstra que nem sempre as pessoas *reagem* em certas circunstâncias (e.g., dentro do contexto do jogo) como elas *acham que reageriam* fora delas (e.g., fora do jogo). Este é um dos pontos importantes da pesquisa qualitativa - revelar estas contradições e ir "além dos números".

No geral, *os usuários controlaram o acesso e a visibilidade à sua informação de localização,* reforçando a viabilidade da Hipótese 1 sobre a usabilidade do CoPS que considera que há usuários que desejam manter um compromisso entre sociabilidade e privacidade, disponibilizando a sua localização com diferentes granularidades para diferentes grupos de requisitante.

Nós também identificamos que *os usuários disponibilizaram a sua localização exata para os membros do seu próprio grupo e se preocuparam em restringir o acesso a esta informação somente para os membros do grupo oponente.* Isso nos leva a crer que em cenários reais a relação pessoal, social e

profissional entre os usuários pode determinar quais informações e em que condições os usuários as divulgariam.

Além disso, todos *os usuários afirmaram que normalmente usam a identificação do requisitante (chat ou telefone celular) como parâmetro de decisão para estabelecer ou não uma comunicação.* Isso vai ao encontro da nossa hipótese do modelo conceitual sobre a necessidade da garantia de autenticidade da identidade do usuário.

Em geral, *os participantes dos experimentos afirmaram que seria muito difícil manter as suas preferências de privacidade atualizadas em função das inúmeras opções de controles de privacidade que podem ser re-configuradas e das diferentes situações que podem requerer essas atualizações.* Eles relataram que muito provavelmente esquecerão de atualizá-las e poderão ser expostos a situações constrangedoras ou embaraçosas, como, por exemplo, deixar explícito para o professor orientador que ele estava na lanchonete enquanto deveria estar participando de uma reunião. Como uma solução paliativa, a maioria dos entrevistados disse que o uso de perfil de privacidade (e.g., Em Reunião, Descansando, ...) facilitaria o gerenciamento da política de privacidade, principalmente se a seleção dos perfis fosse realizada de forma automática e eles pudessem alterar as exceções quando for necessário. Como um dos entrevistados reportou, *"Eu gostaria de criar perfis para gerenciar a política de privacidade. Controlar as propriedades de privacidade individualmente pode fazer com que o usuário cometa erros e divulgue a sua localização indevidamente".* Dessa forma, as sugestões de uso de perfis de privacidade para o gerenciamento da política de privacidade reforçam a aplicabilidade dos benefícios apontados pela Hipótese 4.

Entretanto, *um dos participantes disse que apesar da seleção automática de perfis ser útil, ele não consegue imaginar como o sistema poderia adivinhar sempre corretamente qual perfil deve ser selecionado nas mais diversas situações do dia-a-dia.* Nesse caso, podemos concluir que o próprio usuário teria ressalvas com relação à eficácia da tecnologia. Além disso, estamos cientes de que, apesar dos usuários terem afirmado que o uso de perfis pode facilitar o gerenciamento da política de privacidade, nós não sabemos o quanto essa solução seria eficaz. Ou seja, se o usuário conseguiria criar e associar nomes coerentes aos perfis de seu interesse. No entanto, acreditamos que este seja um desafio para o projeto da interface, e não da implementação dessa funcionalidade no sistema.

Alguns usuários adotaram uma abordagem mais liberal, disponibilizando a informação de localização para todos os demais usuários. No entanto, no decorrer dos testes com o Simulador, estes usuários com atitudes mais

liberal utilizaram demasiadamente as notificações e relatórios de acesso para identificar e prevenir-se de possíveis infrações. Sendo assim, nós acreditamos, conforme proposto pelas Hipóteses 2 e 3, que há usuários que não se preocupam se a sua localização é divulgada ou não, mas gostariam de identificar os acessos maliciosos e aplicar uma medida corretiva, como, por exemplo, bloquear um acesso específico ou desativar o uso da tecnologia quando necessário, ficando, por exemplo, invisível para todos os participantes. Ou seja, a tecnologia tem que tratar algumas exceções e/ou permitir que o usuário a desative de uma maneira rápida e simples.

Dentre os usuários entrevistados, *somente um deles manifestou o interesse de "mascarar" o seu status de disponibilidade, negando o acesso à sua localização sem que o requisitante tenha ciência da ação tomada.* Essa abordagem em IHC, conforme argumentado em (40), é comumente conhecida como *face-saving strategies*. Em suma, são estratégias que "oferecem uma saída educada" para quem quer tomar uma atitude que, se comunicada diretamente, seria uma falta de educação ou consideração com os outros e desgastaria as relações pessoais entre as pessoas. No CoPS, apelidamos essa funcionalidade como *plausible deniability*. A partir dos experimentos realizados, constatamos que a maioria dos usuários nos forneceu elementos que enfraquecem a Hipótese 5, pois, mesmo diante de cenários que despertavam a necessidade de uso dessa funcionalidade, eles não a utilizaram na maioria das vezes. Nas entrevistas feitas após os experimentos, os usuários disseram que não se lembraram ou entenderam essa funcionalidade do sistema. Isso também pode ter ocorrido por causa de algum problema de comunicação da interface ou por causa da falta de expressividade ou importância dessa funcionalidade no contexto do jogo.

Nós também identificamos em algumas etapas dos experimentos que os usuários podem expressar percepções (através de suas opiniões e ações) que enfraquecem e reforçam várias das hipóteses de usabilidade do CoPS, dependendo da situação. Por exemplo, se o participante considera que o momento não representa muito risco, ele divulga a sua localização e acompanha os relatórios de acesso e notificações (convergindo para as Hipóteses 2 e 3, e divergindo da Hipótese 1). Em uma situação oposta, ele bloqueia explicitamente o acesso e controla o nível de visibilidade da localização a ser disponibilizada (convergindo para a Hipótese 1 e divergindo das Hipóteses 2 e 3). Essa configuração dependente de contexto também pode ser evidenciada a partir do comentário de um dos participantes: *"Eu não me preocupo que a minha localização seja divulgada inadvertidamente para outros usuários. Quando for necessário gerenciar o acesso a uma informação importante ou em um cenário sensível/delicado, eu vou lembrar de atualizar as minhas preferências de privacidade."*

Essas evidências significam para nós que esse usuário é representante de um grupo de pessoas para quem as questões de privacidade são extrema e complicadamente dependentes do contexto em que se encontram. Ou seja, não podemos partir para soluções generalizantes. E se partirmos para uma variedade de controles de privacidade em que as pessoas podem escolher usá-los ou não de acordo com o contexto, temos de estar atentos para o fato de que este contexto pode mudar muito e, portanto, o leque de opções utilizadas a cada momento pode também variar na mesma proporção. Com isto, os controles e as interfaces das aplicações LBS e da aplicação de gerenciamento da política de privacidade constituirão, provavelmente, um desafio não trivial de interação.

Limitações e diretrizes futuras

Nós identificamos através dos experimentos algumas questões de privacidade que não estamos tratando ou que ainda não investigamos em profundidade. Por exemplo, a maioria dos participantes questionou a perda de controle da informação divulgada, evidenciando ainda mais as discussões de Grudin (8) sobre essa questão. Como discutido na proposta do modelo conceitual de privacidade, a funcionalidade de "Contrato de uso de contexto" não representa uma solução efetiva para esse problema. De qualquer modo, não faz parte do escopo deste trabalho tratar do controle do tempo de vida da informação divulgada pela rede.

Uma outra funcionalidade requisitada pelos usuários que não é tratada pelo CoPS é a pré-configuração de perfis, que entra em vigor quando determinadas condições informadas pelos usuários são satisfeitas. Dada a impossibilidade de antever ou deduzir corretamente quando e como os perfis dos usuários devem ser selecionados, pretendemos, a curto prazo, projetar uma abordagem mais simples na qual o usuário configura, a priori, a seleção de seus perfis de acordo com a sua localização. Por exemplo, ao entrar em alguma sala de aula do prédio RDC, o perfil "In Classroom" deve ser selecionado, ao entrar no auditório 1 do prédio LEME, o perfil "Meeting", etc.

As notificações de acesso à localização foram apresentadas aos participantes na forma de caixas de diálogo. *A maioria dos usuários achou que a notificação de acesso a cada requisição é muito intrusiva.* Um dos entrevistados sugeriu a criação de uma "abstração" da apresentação da notificação, por exemplo, notificar o usuário somente se houver "várias" tentativas de acesso do mesmo requisitante, ou se ocorrerem n tentativas em um curto espaço de tempo, etc. Nos trabalhos futuros, pretendemos incorporar ao CoPS essa abstração de notificação ao usuário.

Os usuários relataram nas entrevistas realizadas após os testes com o

Simulador do jogo que gostariam de configurar diferentes controles de acesso para diferentes grupos de requisitantes. Este controle de granularidade fina é provido pelo CoPS através do algoritmo de especificidade. No entanto, apesar da sua aplicabilidade, os usuários mencionaram que têm receio de que essa especificidade na configuração das regras aumente muito a complexidade de configuração da política de privacidade. Sendo assim, podemos presumir que o projeto da interface de gerenciamento da política de privacidade representará um fator crítico para a usabilidade do CoPS. Como trabalho futuro, pretendemos interagir com os pesquisadores do grupo de IHC do laboratório SERG (99) da PUC-Rio para trabalharmos no projeto de uma interface que ofereça diferentes níveis de abstração para a configuração da política de privacidade, pois estamos cientes de que uma interface mal projetada desmotivará o usuário a utilizar o CoPS e, conseqüentemente, os serviços de provisão de contexto que o utilizam.

5.2 Avaliação de desempenho

Nesta seção, descrevemos alguns testes de desempenho que realizamos com o propósito de avaliar a escalabilidade e a vazão do CoPS na avaliação de requisições de acesso ao contexto. Nestes testes, usamos duas máquinas, uma para executar o servidor CoPS e outra para executar os clientes, ambas tinham a seguinte configuração: Pentium IV 2.4Mhz, 512MB de RAM, executando *WindowsXP Professional* em uma rede local *Fast-Ethernet*.

Para facilitar a implementação dos testes de desempenho, usamos o AspectJ (100) para instrumentar o código do CoPS com instruções que registrem em arquivos de log o tempo de processamento de alguns de seus métodos/procedimentos. Em nossos experimentos, nós não utilizamos a *cache* da API CAA e medimos o tempo de resposta do processamento das requisições de acesso ao contexto com e sem a latência de rede. Além disto, em nossos testes, utilizamos a autenticação simétrica (usando UITs, como explicado na Sub-Seção 4.2.1) para obter resultados de desempenho mais realísticos.

Nos experimentos realizados, analisamos três questões principais. Primeiro, medimos o quanto o tempo de resposta do CoPS aumenta em função do número de regras de privacidade selecionadas para avaliar uma requisição, levando em conta que essas regras possuem o mesmo nível de especificidade em todos os campos avaliados (i.e., as regras selecionadas são avaliadas em todas as fases de especificidade). Com base neste experimento, definimos para o segundo e terceiro experimentos a quantidade de regras de privacidade que devem ser analisadas em todas as fases de especificidade para o processamento

das requisições dos clientes. Segundo, identificamos o quanto o tempo de resposta percebido pelos clientes (e.g., serviço de contexto) aumenta em função do número de clientes concorrentes. Terceiro, refinamos o experimento anterior para medir somente o tempo de processamento do algoritmo de especificidade em função do número de clientes concorrentes, desconsiderando a latência da rede.

Em nosso primeiro experimento, populamos a base de dados do CoPS com um conjunto pré-selecionado de regras de privacidade, de uma forma que fosse possível selecionar a mesma quantidade de regras em cada fase de especificidade para avaliar uma dada requisição. Este experimento teve o objetivo de avaliar como o aumento do conjunto de regras mais específicas (i.e., regras de privacidade que se aplicam em cada fase de especificidade, incluindo a análise dos campos *temporal restriction, precision, application* e *result*) selecionadas para avaliar uma requisição influencia o tempo de processamento do algoritmo de especificidade. A Figura 5.1 ilustra os resultados deste experimento. Neste teste, a latência de processamento do algoritmo de especificidade foi estimada a partir da média do tempo de processamento de 100 requisições consecutivas (com os mesmos parâmetros) realizadas por uma aplicação cliente. Nós configuramos cuidadosamente os parâmetros das requisições e os campos das regras na base de dados do CoPS de tal forma que cada teste pudesse selecionar uma quantidade específica de regras para ser analisadas em todas as fases da análise de especificidade.

A partir deste teste, identificamos que o número total de regras na base de dados do CoPS não tem impacto direto na latência do tempo de resposta, porque as consultas SQL filtram de forma rápida as regras que "casam" com os campos *subject, requester, context variable* da requisição e descartam aquelas que não se aplicam. Além disso, conforme descrito nas Sub-Seções 4.1.5 e 4.2.2, cada fase da análise de especificidade pode eliminar algumas regras para as análises posteriores. Sendo assim, é importante notar que o principal "gargalo" do algoritmo de especificidade não está relacionado com a quantidade de regras selecionadas via a consulta SQL para avaliar uma dada requisição, mas, sim, com o número de regras de privacidade avaliadas em cada fase do algoritmo de especificidade. Conforme é mostrado na Figura 5.1, o tempo de processamento do algoritmo de especificidade é linear em relação ao incremento do número de regras avaliadas em todas as fases de especificidade. A partir deste experimento, nós podemos ver que quando o conjunto de regras mais específicas é grande (aproximadamente 200 regras analisadas em todas as fases de especificidade para avaliar uma única requisição) o tempo de processamento é de aproximadamente 20ms. Entretanto, acreditamos que

na prática o algoritmo de especificidade não selecionará e avaliará mais do que 15 regras de privacidade para cada requisição em cada fase. Para que isso ocorresse, o usuário teria que atribuir a todos os campos das regras selecionadas valores que as configurassem no mesmo nível de especificidade, de uma forma que nenhuma delas fosse descartada pelo algoritmo. Baseando-se nesta premissa, realizamos os testes seguintes (mostrados na Figura 5.2) usando um conjunto pré-definido com 15 regras que serão analisadas em todas as fases do algoritmo de especificidade para avaliar as requisições recebidas.

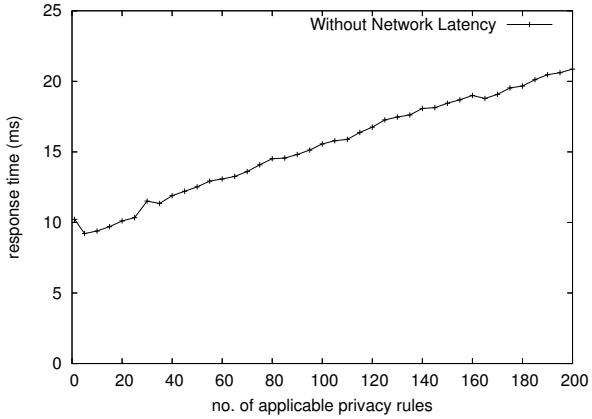

Figura 5.1: Tempo de processamento vs. Número de regras de privacidade aplicáveis à requisição

A Figura 5.2 mostra os resultados do segundo e terceiro experimentos, nos quais analisamos a média do tempo de resposta variando o número de clientes concorrentes. Nestes testes, populamos a base de dados do CoPS com 301 usuários: 300 possíveis *Requesters* e um usuário *Subject* 'S1'. Para reduzir o número de regras de privacidade, associamos os 300 possíveis *Requesters* ao grupo 'MyFriend' e criamos 15 regras de privacidade com os campos *Subject* e *Requester* contendo 'S1' e 'MyFriend', respectivamente. Todas essas regras foram configuradas na hierarquia de política de privacidade do Usuário e nós assumimos que a política de acesso padrão "Liberal" foi escolhida. Nós também configuramos cuidadosamente os campos das regras para que todas elas sempre fossem selecionadas/analisadas em todas as fases de especificidade para cada requisição. Em seguida, executamos um número incremental de clientes concorrentes, onde cada cliente fez a mesma requisição 100 vezes. Depois, medimos os tempos de resposta com e sem a latência da rede.

A única diferença entre esses dois experimentos é que o último avalia o tempo de processamento do algoritmo de especificidade e não considera a latência da rede. A diferença entre o tempo de processamento do algoritmo e o tempo de resposta percebido pelos clientes pode ter sido aumentada em

função da configuração do ambiente de teste, no qual executamos os clientes concorrentemente em uma mesma máquina.

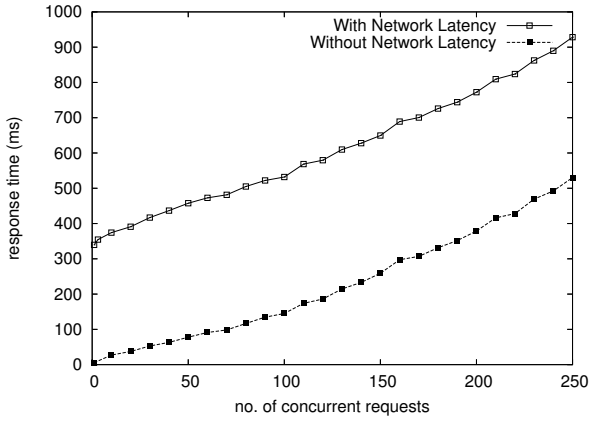

Figura 5.2: Tempo de resposta vs. Número de clientes concorrentes

Os resultados (Figura 5.2) mostram um aumento linear do tempo de resposta e do tempo de processamento do algoritmo a medida que o número de clientes concorrentes é incrementado. Os resultados mostram que o tempo de processamento do algoritmo de especificidade tem pouca influência no tempo de resposta total de uma requisição de autorização de acesso ao contexto.

5.3 Discussões

Neste capítulo, discutimos a metodologia e os resultados da avaliação qualitativa de algumas hipóteses de usabilidade do CoPS e descrevemos, em linhas gerais, os resultados dos experimentos da análise de desempenho realizada com o serviço de privacidade proposto.

Os testes de desempenho demonstraram que o tempo gasto pelo CoPS no processamento de requisições de autorização de acesso ao contexto representa somente uma pequena parcela do tempo total gasto no processo de aquisição da informação de localização. Com base nisto, acreditamos que o uso do CoPS não representaria um ponto crítico para o desempenho do serviço de contexto, podendo assim, em relação a esse aspecto, ser utilizado em um ambiente real.

Os testes das avaliações qualitativas, normalmente, trabalham com amostras pequenas, se comparadas às amostras estatisticamente representativas utilizadas nos estudos quantitativos. Isso se deve entre outros fatores, ao fato das pesquisas qualitativas serem, em geral, extremamente trabalhosas e de lenta execução (101, 102). "Cada um de seus passos - a delimitação precisa de seus objetivos, o conhecimento do contexto no qual a questão de estudo se insere, a coleta minuciosa dos dados, a análise artesanal, aprofundada e iterativa do

material coletado, etc. - envolve freqüentes tomadas de decisão e denso trabalho de análise e interpretação dos dados coletados" (101). Por essas razões, as pesquisas qualitativas costumam trabalhar intensivamente com poucos participantes ao invés de extensivamente com grandes amostras.

A partir dos experimentos realizados, pudemos identificar opiniões e atitudes dos usuários que reforçam a viabilidade de usabilidade do CoPS, uma vez que foi expresso o desejo de manter um compromisso entre sociabilidade e privacidade, disponibilizando a sua localização com diferentes granularidades para diferentes grupos de requisitante. Além disso, de acordo com os usuários, as aplicações LBS podem ser muito úteis, entretanto, sem os controles de privacidade que lhes permitem gerenciar o acesso e a visibilidade da sua localização, essas aplicações apresentariam riscos à perda de privacidade que poderiam ser mais evidentes e impactantes do que os seus benefícios.

A noção de privacidade é individual, havendo substancial variação na atitude que as pessoas têm em relação à privacidade como um todo e a situações de proteção ou divulgação de informações privativas. Sendo assim, há usuários pouco ou muito preocupados com questões de privacidade. Em função disto, acreditamos que para atender as demandas e necessidades dos usuários, o serviço de privacidade deve fornecer um conjunto significativo de recursos de controle de privacidade flexíveis que lhes permitam adotar uma postura mais conservadora, por exemplo, negar o acesso à sua localização (ou à informação de contexto em geral) ou, uma postura liberal (porém, moderada), por exemplo, divulgar a informação requerida e monitorar os acessos para identificar e a inibir os eventuais abusos.

Nos experimentos realizados, nós avaliamos somente um sub-conjunto das funcionalidades providas pelo CoPS em função da complexidade em desenvolver uma interface que contemple todos os controles de privacidade oferecidos e do tempo disponível para realizar esta pesquisa. No entanto, foi possível obter resultados muito interessantes, como, por exemplo: identificar as percepções (i.e., opiniões e atitudes) dos usuários em relação às hipóteses de usabilidade do CoPS; auferir novas idéias de trabalhos futuros (e.g., abstração da apresentação das notificações, seleção automática dos perfis); e ainda pudemos adquirir experiência na execução de testes de avaliação qualitativa com usuários, o que nos permitirá avaliar outras características do serviço de privacidade proposto. No próximo capítulo, faremos uma comparação da nossa proposta de trabalho com outros trabalhos relacionados à nossa pesquisa.