Apreciação Subjetiva

A motivação do trabalho

A falta de privacidade na internet sempre me deixou incomodado. O relato de alguns amigos de falsos sequestros que eram feitos com dados obtidos através das redes sociais agravava isso. Quando tive contato com criptografia, vi que existia, de alguma maneira, uma solução para tal problema. Foi então que me motivei a fazer um estudo sobre criptografia para redes sociais.
Um "detalhe" importante do trabalho foi a busca por garantir privacidade de fato. Então foi que incluí no estudo o ponto de "não confiança no provedor de serviço". Os casos de espionagem dos Estados, dentro os quais os EUA são o maior exemplo, vem justamente na contramão disso. Um bom exemplo foi a luta "anti-terrorista" depois dos ataques às torres gêmeas que foi usada como justificativa para quebrar a privacidade de qualquer um.
Em suma, minha motivação foi a de que as pessoas pudessem usar as redes sociais com a liberdade que têm na vida real, sem ter que se preocupar com ser espionadas por estarem no meio virtual.

O desafio

Quando pensei em começar o trabalho tive a ilusão de que seria possível, se não implementar todo o software para tal tipo de rede, pelo menos apontar o caminho. Quando comecei os estudos vi que o "detalhe" da não confiança no provedor de serviço era um problema em aberto e que a dificuldade de alcançar isso era grande. Era quase como o último teorema de Fermat, com um enunciado simples e de fácil entendimento, mas de resposta muito complexa.

O estudo

Iniciei os estudos com o que eu conhecia do trabalho feito por um amigo. Ele havia implementado um sistema de criptografia para o *Facebook* através de um complemento para o *Google Chrome*. Então comecei a estudar a criptografia de *broadcast*. O conceito é simples, porém exige um conhecimento básico do que é criptografia. Já neste início percebi que a disciplina optativa eletiva que fiz no IME de criptografia foi fundamental.
Ainda no primeiro semestre de 2014 ocorreu em São Paulo um evento de criptografia que foi importante ao meu trabalho: a *Cryptorave*. Foi um ciclo de palestra e oficinas que tratava sobre como um usuário comum poderia ter privacidade na rede com o que existe de criptografia implementada hoje e qual é o estado da arte de criptografia. Foi meu primeiro contato com o protocolo OTR, que fez parte do meu estudo.
Passado tal evento, foi pesquisar sobre redes sociais seguras. Foi quando percebi o que já desconfiava: não existia nenhuma rede social com as características que eu buscava. A *Diáspora**, única rede social que encontrei com a preocupação com a privacidade dos usuários, se baseava na distribuição dos provedores de serviço para garantir a segurança. Ou seja, parte da segurança da rede era delegada aos usuários, que poderiam adicionar um servidor próprio. Como meu estudo já havia mostrado que é praticamente impossível garantir segurança permanente confiando que um determinado servidor não será invadido, a *Diáspora** fugia do que eu almejava.
Tive bastante dificuldade em encontrar exatamente o que precisava para redes sociais. Demorei para encontrar a criptografia baseada em atributos e entende-la. Apesar disso, foi justamente ela o que mais estudei e o que mais me ajudou com o trabalho. Foi com ela que consegui entender melhor o que era simples e o que era mais complexo quanto a criptografia. Por exemplo: a junção em um sistema de criptografia da propriedade de não ter um servidor central que tenha conhecimento das informações com a propriedade de poder adicionar e excluir membros torna o problema

criptográfico a ser resolvido muito complexo.

Sobre a disciplina do trabalho de conclusão

Muitos estudantes já sabiam o que gostaria de fazer em seu trabalho antes mesmo de se matricular na disciplina e já tinham conversado com os professores que iriam orientá-los. Outros, como foi o meu caso, passaram a pensar nisso somente quando se matricularam na disciplina. Ao final do ano fizemos nossas apresentações com o que conseguimos fazer, com o fruto do trabalho do ano todo. Acredito que esse momento seria muito útil para aqueles que pretendem fazer a disciplina no próximo ano, pois poderiam ver os trabalhos e conversar com as pessoas sobre a experiência que tiveram (desde as dificuldades, até o estilo de trabalho de cada orientador), enriquecendo assim os futuros trabalhos de conclusão de curso.
Outro ponto que me pareceu importante foram as entregas parciais. Talvez se houvesse uma primeira apresentação do trabalho de cada um no meio do ano isso potenciaria os trabalhos e ajudaria aqueles que têm dificuldades com as apresentações.

As conclusões pessoais

A maior experiência que ganhei com o trabalho foi justamente fazer algo que não era um trabalho pré-fabricado por um professor, mas algo que foi uma ideia própria (mesmo que não original). Para aqueles que pretendem fazer um mestrado, essa é uma experiência importante, pois é a primeira experiência “autônoma” do estudante.
Ainda considero muito importante a pesquisa que iniciei. Porém, vejo que o desenvolvimento matemático necessário para conseguir resolver o problema proposto me foge às capacidades atuais. Há possibilidade de continuação da pesquisa, pois nem toda a literatura sobre o tema eu pude esgotar e a cada dia novos *papers* sobre o tema têm surgido. Mesmo diante das dificuldades, vejo que as redes sociais seguras ainda são uma necessidade geral.