Uma infraestrutura baseada em certificados digitais para efetuar autenticação de cliente

Leonardo Schäffer

Supervisor:
Prof. Dr. Alfredo Goldman vel Lejbman

Introdução

O Nubank é uma *startup* que emite cartões de crédito e oferece todo o controle financeiro através de seu aplicativo móvel.

Nesse trabalho o objetivo é encontrar uma forma de aumentar o nível de segurança em geral para clientes do Nubank, e minimizar prejuízos causados por fraudes, cortando classes inteiras delas, através de uma maneira eficiente com o uso de tecnologia.

Mais especificamente, o objetivo é garantir que operações perigosas por parte do cliente (como movimentar dinheiro, por exemplo), venham apenas dos aplicativos móveis, dificultando diversos tipos de ataques comuns em sistemas não móveis e navegadores web.

Dessa forma, qualquer fraude que dependa do acesso às contas dos clientes se torna muito difícil de ser realizado.

A solução escolhida foi realizar autenticação forte dos clientes, através de certificados digitais, na hora que a conexão entre os serviços do Nubank e o aplicativo inicia.

Principais metas

1. Aumentar a segurança dos clientes
2. Buscar uma maneira eficiente de combater fraudes
3. Restringir operações perigosas aos aplicativos móveis
4. Afetar o mínimo possível a usabilidade dos aplicativos

Serviços *web* no Nubank

A infraestrutura do Nubank se baseia em microserviços rodando na nuvem (AWS).

A comunicação entre os serviços acontece através de mensagens HTTPS.

HTTPS, TLS, certificados digitais e autoridades certificadoras

HTTPS é nada mais que HTTP em cima de TLS.

TLS é o protocolo que dá segurança às conexões, oferecendo confidencialidade e integridade.

Ao se iniciar uma conexão TLS, o cliente verifica a identidade do servidor através da validação de seu certificado digital.

O certificado digital é um documento que garante a identidade de seu dono.

Certificados digitais são emitidos por entidades de alta credibilidade, chamadas de autoridades certificadoras.

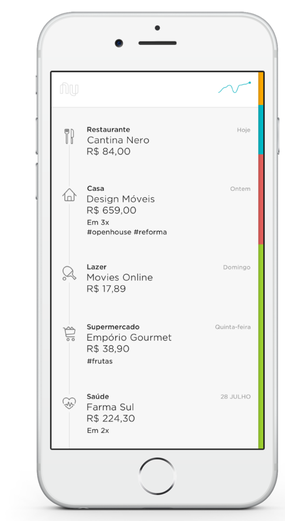
É possível que o servidor também verifique a identidade do cliente, se este também apresentar um certificado. Isso se chama autenticação de cliente.

A solução

A solução desenvolvida foi realizar autenticação de cliente nos aplicativos móveis. Ou seja, os aplicativos, ao fazerem requisições HTTPS aos serviços, precisam apresentar um certificado digital de cliente, para que o servidor possa autenticar o cliente também. Sem o certificado as requisições são negadas.

Os certificados são gerenciados por uma autoridade certificadora própria interna do Nubank.

Eles são emitidos para o cliente no processo de aquisição, o processo pelo qual um possível cliente se torna de fato cliente.



Eles ficam armazenados no celular do cliente, e inicialmente apenas esse celular poderá se comunicar com os serviços.

Se o celular for perdido, ou os dados do aplicativo do Nubank forem apagados, o cliente precisa passar por um processo de recuperação, que exige a verificação de identidade pela equipe de atendimento.

O aplicativo utiliza os certificados automaticamente, sem que isso seja exposto para o cliente, assim sua usabilidade não é afetada.

Possibilidades futuras

Além de fazer autenticação de cliente nos aplicativos móveis, é possível utilizar a mesma estrutura para também emitir certificados aos funcionários e fazer autenticação de cliente nos serviços internos da empresa. Dessa forma, não basta comprometer as credenciais de um funcionário para acessar indevidamente os serviços, é necessário possuir o certificado, que é muito mais difícil de se obter.

Outra vantagem é o fato de o cliente ter um par de chaves seu. É possível utilizá-lo para encriptar dados importantes, assim como assiná-los digitalmente. Isso abre diversas possibilidades, pois assinaturas digitais garantem autenticidade, integridade e não-repúdio.