Banco Digital

Análise dos Requisitos Funcionais

Sara Ferreira, Tiago Carvalho

O nosso trabalho assenta sobre uma simples aplicação que visa simular a operação de um banco digital. O leque de funcionalidades deste sistema abrange a capacidade de aceder ao banco ou a uma ATM, cada uma destas partes com características diferentes. Uma vez registado, o utilizador através da sua conta bancária pode, então, consultar o seu saldo, depositar e levantar dinheiro, ou ainda fazer uma transferência para outro utilizador do sistema.

1 Casos de uso

Quando um utilizador do sistema acede ao banco, são-lhe apresentadas as opções de criar uma nova conta, alterar os dados da sua conta existente, consultar o saldo ou depositar dinheiro; por conseguinte se deduz que os os atores deste sistema são os clientes do banco, a entidade bancária e a(s) caixa(s) ATM.

1.1 Criar uma conta bancária:

Depois do utilizador selecionar a opção relativa à ação de criar uma conta no banco, ser-lhe-á pedido o seu nome completo, morada de residência ou local de trabalho e o seu número de telefone para distinguir o cliente e proceder ao envio do seu cartão bancário. O banco imprime então uma mensagem com o estado de sucesso da operação requerida; em caso de sucesso, imprime o número de cliente no ecrã e envia o novo cartão do cliente para a morada inserida; já em caso de erro, imprime a sua causa.

1.2 Alterar dados de uma conta bancária:

O utilizador acede ao sistema, por meio do seu cartão bancário; seguidamente, no menu que aparecerá no seu ecrã, escolhe a opção referente à alteração de dados da sua conta bancária.

Posteriormente, ser-lhe-á dado um conjunto de opções que eventualmente poderá alterar na sua conta. Após selecionar o dado pretendido, o utilizador insere o novo valor que o substituirá. Numa fase final, o banco recebe o pedido de alteração dos dados do respetivo utilizador, e envia um payload com o estado de sucesso da operação requerida; se for bem sucedido, imprime os dados da conta do utilizador com a alteração efetuada; já em caso de erro, imprime a sua causa.

1.3 Consultar saldo:

O utilizador acede ao ATM e seleciona a opção relativa à consulta de saldo da sua conta. O ATM seguidamente envia um payload com o saldo do utilizador do número de conta em questão.

1.4 Depositar dinheiro:

O utilizador acede ao banco digital e terá de escolher a opção no menu relativa ao depósito de dinheiro na sua conta. Seguidamente ser-lhe-á pedido a quantia a depositar e o banco envia um payload com o estado de sucesso da operação requerida; em caso de sucesso imprime a quantia depositada e o saldo do utilizador depois do depósito; em caso de erro, imprime a sua causa.

1.5 Transferir para outro utilizador:

O utilizador acede à ATM e, posteriormente, escolhe a partir do menu dado, a opção respectiva. Ser-lhe-á então pedido a quantia a transferir e o número de conta do destinatário. Depois do utilizador digitar esses dados, a ATM envia um payload com o estado de sucesso da operação requerida; em caso de sucesso imprime a quantia transferida, o destinatário da transferência e o saldo do utilizador depois da transferência; em caso de erro, imprime a sua causa.

2 Arquitetura

2.1 Arquitetura cliente-servidor

- As caixas ATM vão ser modeladas como um nó cliente, as quais se ligam a um único nó servidor, centralizado, correspondente ao banco.
- O banco terá um serviço *daemon* dedicado à escuta de pedidos de caixas ATM, ou de acessos ao próprio.

2.2 Base de dados SQL para guardar os utilizadores

Será usada a seguinte tabela para guardar os utilizadores do sistema:

```
CREATE TABLE IF NOT EXISTS users(
    id int NOT NULL AUTO_INCREMENT,
    saldo float,
    telephone varchar(16) NOT NULL,
```

```
    name varchar(128) NOT NULL,
    address varchar(512) NOT NULL,
    PRIMARY KEY (id));
```

2.3 Frontend com duas interfaces distintas (ATM e banco)

A aplicação final terá uma interface textual simples que permitirá aceder tanto ao banco, como a uma caixa ATM; no momento em que se inicia a aplicação, será dada a escolha ao utilizador, que o redireciona para a interface relevante.

3 Fluxo de dados e ativos

Assumimos que existe uma caixa fechada que faz tudo o que precisamos do ponto de vista de hardware e comunicação com o utilizador e com o banco.
Para cada um dos casos de uso, os números no fluxo serão substituídos pelo seu significado naquela situação.

Em todos os casos o cliente necessita de inserir um cartão para poder aceder à caixa fechada (ATM), essa situação não está representada no fluxo de dados acima porque é uma operação feita fisicamente e da qual não temos nenhum controle.

3.1 Criar uma conta bancária:

A criação da conta bancária é feita fisicamente num posto do banco; para esse efeito, o utilizador fornece o seu nome completo, número de telemóvel e o PIN secreto desejado para autenticação nas ATM. Além disso, ser-lhe-á pedido que instale no seu smartphone uma app que permite gerar OTP para efeitos de autenticação de dois fatores.

3.2 Alterar dados de uma conta bancária:

Para alterar os dados de uma conta bancaria, o cliente necessita de repetir o processo acima descrito no banco, semelhante aquando da criação da conta bancária.

3.3 Transferir para outro utilizador:

Os ativos, neste caso, são representados pelas transações feitas, ou seja, pelos dados do destinatário e do remetente da transferência bancária em questão. O banco e o destinatário da transferência valorizam esta informação como ativo. Se a segurança em qualquer dado da transação for quebrada, é possível alterar a quantia a transferir e/ou o destinatário da transferência. Esta quebra leva a um possível roubo do emissor da transferência fazendo com que o atacante possa transferir para a sua conta o dinheiro que iria ser transferido para um outro destinatário. Desta forma, é possível verificar que o cliente valoriza também esta informação como ativo.
Neste caso, tendo em conta o fluxo de dados acima, o 1 representa o pedido do cliente ao banco para transferir dinheiro para outro utilizador indicando a quantia da transferência e o destinatário da mesma. O 2 e o 4 representam a resposta dada ao pedido do cliente. O 3 representa a comunicação entre a caixa fechada e o banco.

3.4 Depositar dinheiro:

Os ativos presente neste fluxo de dados são idênticos aos do fluxo de dados anterior, correspondente à criação de uma conta bancária.

4 Estrutura de dados:

4.1 Cliente

- Saldo: float
- Nome completo: string
- Número de telefone: string
- PIN : hash 512 bits

4.2 Caixa ATM

Numa fase preliminar, definimos uma caixa ATM da seguinte forma:

- Identificador: inteiro
- Localização: coordenadas geográficas

4.3 Banco

Numa fase preliminar, definimos o banco da seguinte forma:

- Número de utilizadores: inteiro
- Caixas ATM: lista das caixas ATM instaladas

5 Modelo de confiança:

5.1 Banco digital

É dado como pressuposto que o Banco digital é uma entidade neutra, que não alterará qualquer tipo de dados em si confiados pelos clientes; porém, o mesmo não poderá ser dito de um ator malicioso que ganhe acesso aos dados, seja por que meio for. Assumimos então que o processo de criação de conta e/ou alteração de dados é seguro.

5.2 Clientes

É dado como pressuposto que é atribuído ao cliente um cartão físico único, enviado pelo banco aquando da criação da sua conta bancária.
Assumimos ainda que o cartão bancário é inserido quando um utilizador acede a uma caixa ATM ou fornecido fisicamente ao balcão de um banco.

5.3 Caixas ATM

Assumimos que as caixas ATM fazem aquilo que lhes é instruído, e nada mais, de acordo com o que definimos, sem perturbações.

5.4 Cartão bancário

Assumimos que os cartões bancários fazem aquilo que lhes é instruído, e nada mais, de acordo com o que definimos, sem perturbações.

6 Modelo de ameaças:

6.1 Ameaças

A maior parte dos utilizadores não vão procurar informação que não lhes está visivelmente disponível na interface do banco. Estes utilizadores não vão mudar o seu comportamento ao usar o banco digital ou o ATM de modo a aprender mais sobre o mesmo, portanto, não representam uma ameaça.

Agentes externos ao sistema como *hackers* constituem uma ameaça visto que conseguem aceder ao *backend* do banco e alterar dados de uma transferência de dinheiro para seu proveito ou até alterar os dados de um cliente de forma a prejudicá-lo.

Os administradores do *backend* têm acesso a toda informação guardada pelos servidores, mas não vão modificar essa informação ou tentar prejudicar alguém (tal como foi discutido no modelo de confiança), e, portanto, não constituem uma ameaça para o sistema.

Vamos ignorar a ameaça relativa a algum cliente ser roubado fisicamente, ou até perder o seu cartão uma vez que este está protegido por autenticação de dois fatores, e sem a sua OTP (gerada a partir do tempo atual e de uma chave simétrica armazenada no seu smartphone) e PIN secreto é impossível aceder à conta bancária.

Vamos também ignorar ameaças relativas a ataques ou danos (intencionais, acidentais, naturais ou estruturais) físicos, tanto nas instalações dos servidores como nos vários equipamentos ATM distribuídos por várias localizações.

6.2 Vectores de ataque e vulnerabilidades

Como na arquitetura não considerámos servidores *backup* nem bases de dados de *backup,* estamos perante uma vulnerabilidade do nosso sistema, visto que um atacante pode executar um ataque DOS (denial of service) mandando os servidores do banco abaixo, potencialmente corrompendo os dados armazenados dos utilizadores.

A comunicação aberta na rede também constitui uma vulnerabilidade visto que um atacante ao observar uma comunicação entre o cliente e o banco consegue, por exemplo, interceptar uma transferência e mudar o destinatário para o seu próprio proveito.

É de salientar que qualquer operação no fluxo de dados (representadas pelos números de 1 a 4) mostrado anteriormente constitui também um vetor de ataque.

7 Analise de Risco

Outros utilizadores que não os administradores, acederem ao backend do banco constitui um risco elevado para o sistema, algo que será considerado na mitigação dos riscos.

Outros utilizadores podem ainda intercetar comunicações entre o ATM e o banco, como por exemplo, uma transferência, que constitui de igual forma um risco muito elevado para o sistema, e vamos tentar mitigar.

Outros utilizadores podem tentar autenticar-se como outra pessoa para a prejudicar, algo que será considerado na mitigação dos riscos e tem um risco elevado.

Resumidamente, é necessário garantir autenticação e confidencialidade dos dados que são comunicados entre a ATM e o backend do banco.

Aceitamos o risco dos administradores que têm acesso ao backend poderem alterar os valores, porque acreditamos que não o vão fazer, tal como explicado no modelo de confiança.

Aceitamos também o risco dos servidores poderem ser prejudicados por um desastre natural sendo que não podemos proteger desses mesmos desastres.

O risco de um utilizador poder executar um ataque DoS e mandar os nossos servidores abaixo é elevado, algo que naturalmente prejudica o acesso contínuo aos nossos serviços, então vamos tentar mitigar.

8 Mecanismos de Seguranca

- Servidores backup;
- Backups mantidos offline;
- Criação de um canal de comunicação seguro e autenticado;
    - Negociação de conexões com TLS;
    - Backend possui um certificado emitido por uma AC de raíz;
- Emissão de cartões com chaves privadas neles armazenados;
    - 512 bytes aleatórios;
- Emissão de chave privada para a verificação de tokens OTP;
- Autenticação de 2 fatores;
    - É calculado o valor do hash BLAKE2b do pin com a chave privada do cartão do utilizador, posteriormente enviado ao backend, que garante mais bits de segurança do que as 10000 combinações possíveis de pins de 4 dígitos;
    - O utilizador verifica o próximo token OTP refrescado a cada 30 segundos, que é enviado ao servidor;
- Encriptação dos dados do backend;
    - O backend armazena o hash BLAKE2b do hash do pin com a chave privada do cartão, com um valor salt de 512 bytes lidos aleatoriamente;

Ameaça	Mecanismo de segurança
DoS	Servidores backup; Backups mantidos offline;
Comunicações interceptadas por hackers	Canal de comunicação seguro; Comunicação autenticada por criptografia assimétrica;
Tampering na backend	Não é armazenado diretamente o hash dos pins dos cartões;
Roubo de identidade	Autenticação de dois fatores com OTP

Verificamos assim que os mecanismos de segurança são **suficientes**, porque para cada ameaça há um mecanismo de segurança que a tenta mitigar.

Mecanismo Seguranca	Ameaça
Servidores backup	DoS
Backups mantidos offline	DoS
Canal de comunicação seguro e autenticado	Intercetar comunicações
Dados encriptados	Tampering na backend
Autenticação de dois fatores com OTP	Roubo de identidade

Verificamos assim que os mecanismos de segurança são **necessários** porque cada mecanismo mitiga pelo menos uma ameaça.