Especificação de requisitos para o sistema pessoal de controle de acesso (PACS)

1. Introdução

O propósito dessa especificação é prover detalhes suficientes para que o time de desenvolvedores projete, desenvolva, teste e integre o sistema pessoal de controle de acesso (PACS). É uma tradução do texto elaborado por Constance Heitmayer para a competição de desenvolvimento de sistemas ACM Score [1].

2. Descricão geral do Sistema PACS (*Personal Açess Control System*)

2.1 Conceito do sistema

O sistema PACS é uma versão simplificada de um sistema automatizado de acesso de pessoas (portão eletrônico) usado para fornecer acesso físico privilegiado a salas, edifícios, etc. O usuário insere seu cartão de identificação pessoal, que contém seu nome e CPF, em um leitor e o sistema verifica os dados contidos no cartão em um banco de dados. Este banco pode ser atualizado periodicamente pela administração. O usuário insere o número de identificação pessoal (PIN – Personal Identification Number), um código de 4 dígitos, usando um teclado de 12 posições simples. O sistema valida/invalida o código e permite/proíbe a entrada na sala/edifício. Uma tela de exibição de linha única fornece mensagens e instruccões ao usuário. Um agente de segurança monitora no seu console (um outro computador) as mensagens apresentadas ao usuário; ele pode alterar a decisão do sistema, seja para permitir, seja para negar o acesso ao usuário.

Existem seis componentes de hardware simples no sistema PACS: leitor de cartão, teclado, unidade de exibição de mensagem digital de linha única, console da segurança e portão (ver "interface externa" na Seção 3).

2.2 Ambiente operacional e confiabilidade esperada

O sistema de software deve ser entregue com o código fonte. Para manter a simplicidade, o software do PACS gerencia apenas um leitor de cartão/crachá que deve operar 24 horas por dia, sete dias por semana. Qualquer falha do sistema deve causar uma mensagem de "Acesso negado" no leitor de cartões e uma mensagem para o agente de segurança.

A carga do sistema varia de leve para pesada, dependendo do período do dia e do dia da semana. Uma falha de nível 1 ocorre quando o software fica travado, quando cartões e PINs válidos não são processados, quando usuários inválidos têm acesso ou quando o agente de segurança não consegue alterar uma decisão do sistema. Em resumo, uma falha de nível 1 conduz o sistema ao não funcionamento. A confiabilidade esperada é 0,99 por transação (ou seja, 99 de 100 transações devem executar sem uma falha de nível 1).

Uma falha de nível 2, por outro lado, não é crítica. O agente de segurança pode revogar falhas não-críticas e manter o sistema em execução. Falhas do sistema de nível 2 incluem anomalias tais como um

usuário com um pacote grande que precisa de mais tempo para poder entrar. Uma falha de nível 2 exige um trabalho operacional do agente para ser superada. A confiabilidade de destino será 0.9 por transação por falhas de nível 2.

Uma falha de nível 3 é uma falha do tipo "Don't care" e será corrigida na próxima versão do software. Um exemplo de uma falha de nível 3 é um erro de documentação.

2.3 Visão geral do projeto de alto nível

O sistema de software deve exibir a mensagem “Insira o cartão” e, em seguida, avaliar se o cartão inserido no leitor de cartões é válido (1 no registrador R6) ou inválido (0 no registrador R6) . No caso de cartão válido, o sistema deve ler os onze dígitos do CPF e o sobrenome que pode conter até 20 caracteres.

A validação será feita contra o arquivo chamado *Card.val*. Se os dados forem válidos, o software atualizará o arquivo *message.led* com o texto “Introduza PIN” que representa o LED de 20 dígitos ASCII. Se o cartão é ilegível, uma mensagem "Tente novamente" é gravada no máximo três vezes no arquivo representado o LED. Depois da terceira tentativa mal sucedida, o sistema deve gravar no *message.led* “Procure o segurança”.A mesma mensagem é enviada para o agente de segurança pelo software por meio da gravação no arquivo *Officer.led* e o registrador R8 é definido com o valor de 1.

O agente de segurança tem que *reiniciar* o sistema PACS antes de colocá-lo em funcionamento novamente; ele faz isto definindo o registrador R7 com o valor 1. O software deve ler este registrador e reiniciar o sistema. O PIN de 4 dígitos deve ser lido dos registradores R1 até R4 do teclado e comparado com os dados no arquivo *Card.val*. Observe-se que o primeiro dígito é armazenado no registrador R1, o segundo dígito no registrador R2, etc.. O software deve permitir o máximo de 5 segundos entre dígitos antes da mensagem "PIN inválido" ser exibida. Se o PIN introduzido falhar em três tentativas, uma mensagem “Procure o segurança” é gravada no arquivo chamado *Officer.led* e também exibida no LED do teclado gravando-a no arquivo *message.led*. Um PIN válido deve gerar a mensagem "Por favor, prossiga" para o usuário depois de o registrador R5 receber o valor 1, provocando a abertura da porta pelo hardware. Depois de 10 segundos, o sistema automaticamente se reinicia para outro usuário ou depois que um usuário passa pelo portão.

3. Requisitos (software)

3.1 Requisitos funcionais

1. Ler dados do cartão do usuário e validar dados do cartão.
2.Relatar e registrar as entradas bem sucedidas e mal sucedidas dos usuários.
3.Ler e validar o valores PIN entrados no teclado.
4.Relatar e registrar os valores de PIN bem sucedidos e mal sucedido.
5.Controlar a abertura e o fechamento do portão dependendo do resultado da validação.

3.2 Requisitos de desempenho

1.O software deve ler as teclas à medida que são digitadas.

2.A validação dos dados e a exibição das mensagens deve levar menos 1 segundo.

3.3 Requisitos de segurança

1.O sistema de software deve manter um *log* de todas as transações, bem-sucedidas e mal-sucedidas. O objetivo do *log* é atribuir responsabilidades quando da ocorrência de problemas.
2.Qualquer falha de nível 1 ou de nível 2 deve provocar o bloqueio do portão; o agente de segurança tem capacidade para desbloqueá-lo.
3.Qualquer incompatibilidade do banco de dados com os dados do cartão do usuário ou com o PIN inserido deve provocar:
3.1 Apresentação da mensagem “Insira o cartão/PIN" nas três primeiras tentativas.
3.2 Envio de mensagem para o agente de segurança depois da terceira tentativa mal sucedida; espera pelo reinício do sistema pelo agente de segurança ou liberação do portão.

3.4 Restrições de projeto

- A base de dados de usuários é limitada a 1000 triplas <CPF, nome, PIN>.
- Apenas uma combinação de cartão/teclado/portão deve ser tratada em um dado momento pelo software.
- O leitor de cartão, o teclado e o display são apenas uma unidade. O teclado possui 12 teclas: 0 até 9 mais # e *; os últimos dois caracteres permitem a deleção de teclas digitadas.
- O usuário tem 5 segundos para digitar cada tecla do seu número PIN; caso contrário, é apresentada a mensagem “PIN Inválido”.
- O sistema entre a apresentação da mensagem “Introduza o PIN” e a primeira tecla digitada; caso contrário, o sistema é reiniciado.

3.5 Interfaces externas com o usuário, hardware, software, comunicação

- parâmetros do leitor de dados do cartão ICAR (31)
- registradores para armazenamento do valor de PIN inserido: registradores R1 a R4
- registrador para reinício do sistema pelo agente de seguraça: registrador R7
- registrador de alerta de PIN inválido para o agente de segurança: registrador R8
- registrador de controle do portão: registrador R5
- registrador que informa que o cartão está no leitor de cartões: registrador R6
- registrador que informa o fim da leitura dos dados do cartão: registrador R10
- registrador que informa o fim da leitura do PIN: registrador R11.

3.6 Outras informações

- Mensagens apresentadas no LED do leitor de cartões: “Insira o cartão”; “Introduza PIN”; “Tente novamente”; “PIN inválido”; “Por favor, prossiga”; “Insira o cartão/PIN”; “Procure o segurança” e “Acesso negado”.

- Arquivos de dados:
  - Card.val – base de dados do sistema com o CPF do usuário, o sobrenome e o PIN (1000 registros, uma para cada usuário com a seguinte estrutura: CPF – cadeia de caracteres de

comprimento onze; sobrenome – cadeia de caracteres comprimento 20; cadeia de caracteres de comprimento 4.
    - Message.led – buffer para entrada de mensagem para o LED (vinte caracteres fixos)
    - Officer.led – buffer para entrada de mensagem para o LED do agente de segurança (vinte caracteres fixos).
    - Audit.act – tempo (clock do sistema); data; sistema; CPF do usuário e nome; transação sucesso/falha (i.e., 1 ou 0).

4. Objetivos do projeto

- Produzir os requisitos precisos;
- Produzir documentos de análise e projeto;
- Implementar o sistema;
- Desenvolver e executar casos de teste.

5. Referências

[1] Heitmayer, Constance. “Requirements Spec for the Personnel Access Control System (PACS)”, ACM Score Competition, 2009. Disponível em http://score.elet.polimi.it/projects/heitmeyer.pdf (Visitado em 19 de junho 2009).