UNIVERSIDADE DE BELAS
FACULDADE DE ENGENHARIA

ENGENHARIA INFORMÁTICA

Programação IV

Enunciado do trabalho do 4º Ano – Anual - 2019

KEROBIN.AO

O grupo KEROBIN.AO está interessado em alargar os seus negócios na área da saúde e pretende que seja concebido um sistema de informação hospitalar de modo a estabilizar a situação financeira do grupo. O objetivo do sistema é auxiliar a gestão de toda a informação clínica e administrativa de uma instituição hospitalar, e melhorar a qualidade da prestação de cuidados de saúde.

Interessada em aumentar as suas receitas, o grupo KEROBIN.AO pede então que desenvolvam um aplicativo, SIS – Sistema de Informação de Saúde, direcionado para três tipos de utilizadores: utentes, pessoal administrativo e pessoal clínico (médicos). Um estudo preliminar identificou os principais requisitos estruturais e funcionais que estão associados a cada tipo de utilizador:

Utente

- Efectua o registo no sistema (nota 1)
- Visualiza quais as especialidades, médicos e/ou exames complementares de diagnostico existentes numa instituição (nota 2)
- Marcar consultas e/ou exames (nota 3)
- Insere informação de carácter pessoal no registro clínico de utente – RCU (nota 4)
- Consulta e actualiza o seu RCU (nota 5)

Pessoal Clínico

- Consulta e actualiza a informação referente ao seu registro (nota 6)
- Efectua a gestão de informação de carácter não pessoal do RCU

Pessoal Administrativo

- Efectua a criação e actualização do registro do pessoal clínico
- Especifica as especialidades e horários de atendimento para o pessoal clínico
- Efectua a gestão de marcação de consultas e /ou exames (nota 3)
- Consulta e actualiza os RCU (nota 7)
- Envio automático e atempado de informação útil ao utente através de e-mail ou de outro canal de distribuição (por exemplo: aviso de uma consulta com um dia de antecedência).

Devido a importância do projecto, o processo de avaliação seguirá regras rigorosas definidas à priori, e que são apresentadas na secção seguinte. Este processo será muito exigente, e assim sendo, o grupo KEROBIN.AO reserva-se o direito de anular o contrato caso o vosso projecto não respeite os requisitos considerados necessários.

Notas:

1 – O formulário de registro de um utente inclui a seguinte informação obrigatória: número de utilizador (login), uma palavra-chave (password), nome de utilizador, data de nascimento, morada, localidade, código postal, telefone de contacto, endereço de correio electrónico, entidade financeira responsável (por exemplo: seguradora) e número de utente na entidade responsável. O login e password permitir-lhe-á realizar a marcação de consultas e /ou exames e gerir o seu RCU.

2 – A consulta das especialidades, médicos e exames existentes não exige que o utente esteja registado. Todas as restantes funcionalidades exigem a autenticação do utente.

3 – Existem determinados exames complementares de diagnóstico que podem ser requeridos pelo pessoal administrativo ou pelo utente mediante a existência da respectiva prescrição médica no RCU. Por exemplo: para que um utente possa realizar a mercação de uma radiografia é exigido que, no seu RCU e na especialidade de ortopedia esteja a permissão médica para o efectuar.

4 – O RCU, para além da informação de carácter administrativo definida pelo utente aquando do seu registo no SIS, contém ainda:

Dados médicos fixos (ocorrências singulares): sexo; grupo sanguíneo e alergias;

Outros dados médicos (ocorrências múltiplas de dados ou dados temporais): história clínica, consultas/exames efectuados e respectivos resultados, diagnósticos, procedimentos e terapêutica;

Dados de caracter pessoal relevante para a saúde: história familiar de saúde, boletins de vacinas, histórico das suas actividades relativas às suas consultas e exames.

5 – O utente apenas pode actualizar a informação de carácter pessoal e visualiza apenas a parte pública dos outros dados médicos do RCU (por exemplo: terapêutica e diagnóstico, exames e consultas efectuados).

6 – O pessoal clínico apenas pode alterar o seu horário com um mês de antecedência e no caso de não existir nenhuma consulta já marcada.

7 – O pessoal administrativo não pode consultar a informação de caracter pessoal do RCU, à excepção da administrativa, e apenas pode actualizar determinadas informações (por exemplo: o pessoal administrativo não pode alterar a terapêutica administrativa por um médico).

Segurança

Dada a importância da informação numa organização, espera-se que neste projecto, se aplique os conceitos fundamentais de segurança computacional no sentido de estabelecer uma comunicação mais segura, protegendo as informações contra qualquer tipo de ataque conhecido, eliminando do sistema todas as vulnerabilidades que possam ser exploradas pelos maliciosos. Concretizando as propriedades de segurança como autenticidade, integridade, disponibilidade e confidencialidade.

Deverá se utilizar todas as técnicas e ferramentas apreendidas durante as aulas de segurança computacional para a criação do sistema de informação de eventos obedecendo os critérios e explicações listadas abaixo:

Controlo de Acesso

O SIS deverá possuir primeiramente uma interface para autenticação dos utilizadores onde será informado os seus credenciais (nome de utilizador e a palavra-passe). Depois do utilizador ser autenticado pelo sistema ele poderá efectuar diversas operações usufruindo das funcionalidades do das funcionalidades do sistema como registro de um novo utente, a edição ou até mesmo a consulta de eventos.

Nem todo evento será de acesso público, por razões de privacidade alguns utilizadores poderão optar em restringir um certo grupo de pessoas para terem acesso aos seus eventos, também delegar à estas pessoas algumas das funcionalidades administrativas sobre o utente, alteração de informações do evento, autorizar outras pessoas a acederem o SIS, ect.

Uma boa prática de segurança computacional para o controlo de acesso não seria somente a utilização de uma interface de autenticação, mas sim a utilização dos mecanismos de controlo e acesso rigoroso como *Matriz de Controlo de Acesso*, onde o acesso aos recursos do sistema (objectos que podem ser exames, utilizadores, etc.) devem ser pré definidas na matriz de controlo de acesso associados a um processo (utilizador).

Secure Socket Layer (SSL)

O servidor quando gera a página que contem as informações sobre o Exames, normalmente está página estará composta de diversos atributos textos do Exame como data de marcação, data de realização, o médico que examinou, etc., mas também poderá conter imagens e/ou arquivos anexados, relacionado a este Exame ou a página gerada. Todo este conteúdo será transmitido atrvés da Web.

O protocolo HTTP realiza a transferência de informações do mesmo jeito que a página foi gerada, destacando uma vulnerabilidade no caso da transmissão de páginas de Exames de acesso restrito, embora o texto possa estar previamente criptografado antes da transmissão, mas os outros tipos de conteúdos (imagens por exemplo) estarão inseguros.

Foi desenvolvido um novo protocolo que gere a encriptação das informações na camada de transporte denominado Secure Socket Layer (SSL), consequentemente o protocolo

da camada de aplicação HTTPS. O sistema desenvolvido deve suportar este mecanismo de segurança para garantir a segurança total na transmissão das páginas, principalmente as páginas com informações sobre eventos com acesso restritos.

Ataques Comuns aos Sistemas

O Sistema de Informação de Saúde irá interagir com diversas pessoas, dentre elas poderão existir pessoas com intenções maliciosas e, caso combinem as suas habilidades computacionais com as simples funcionalidades disponibilizadas pelo sistema em uma vulnerabilidade.

Através de qualquer inteface do sistema que envia as informações passadas para a base de dados do sistema, um malicioso poderá realizar o ataque SQL *Injection*; Das funcionalidades como adicionar e visualização de anexos ou imagens de um Exame poderá surgir um ataque PHP *Injection*. A ignorância do controlo de requisições enviadas ao servidor também poderá originar um ataque de Negação de Serviço (DoS) violando assim a propriedade de disponibilidade.

Para evitar estes ataques comuns aos sistemas, principalmente aplicações web, recomenda-se a utilização da classe PDO para desenvolvedores em PHP ou uma outra classe ou API semelhante para outras linguagens que possam combater o ataque SQL *Injection*; Como uma alternativa à prevenção do sistema contra o ataque de negação de serviço (DoS) é a utilização do *Message Digest* para reconhecer requisições repetitivas.

Criptografia

Para evitar o forjamento de dados e principalmente a compreensão da informação caso a comunicação esteja comprometida e acedida de forma indevida, deve-se implementar a criptografia de chave pública como RSA à todas informações durante a transmissão, dificultando a sua compreensão caso caia sob um ataque homem no meio.

Certificado Digital

O servidor de segurança deve possuir um Terceiro Confiável “Certificate Autority (CA)” com um documento eletrónico (Certificado Digital) contendo as informações individuais, a fim de certificar se alguém é o que diz ser. O certificado digital estabelece uma associação entre a identidade do indivíduo e uma chave pública. Existem CA´s públicos como a VeriSign, Entrust, Baltimore, etc. e também existem CA´s privados (in-house) que são desenvolvidos pela própria organização, mas para o caso deste sistema interno requer a utilização de um CA in-house. Os arquivos de Certificados Digital devem possuir uma das seguintes extensões (*.crt, *.cert, *.cer, *.pem ou *.der).

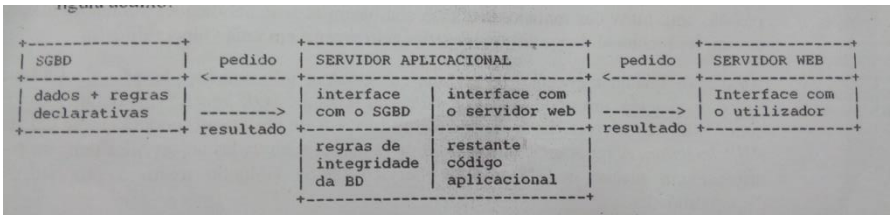
Assinatura Digital

As assinaturas digitais estão relacionadas às criptografias de chave pública, mas invertem o papel de chaves públicas e privadas. Um remetente pode encriptar e assinar digitalmente uma mensagem com sua chave privada. Quando a mensagem é recebida, o destinatário pode desencripta-la coma chave pública do remetente. Como o remetente é a única pessoa com acesso à chave privada o destinatário pode estar relativamente certo de que a mensagem que veio é do remetente esperado e a mensagem não foi alterada.

Visto que a utilização do Certificado Digital armazena as informações sobre os indivíduos assim como a sua chave pública, como boa prática o sistema deve reultilizar estas informações evitando assim redundâncias, deve utilizar Message Digest em vez de uma assinatura de dimensão variável (poderá ser de conteúdo muito grande).

Aspectos técnicos

- Os projectos utilizarão preferencialmente servidores com as tecnologias ASP.NET MVC, PHP, JAVA, SqlServer, Mysql e Oracle. Os clientes terão obrigatoriamente de ser browsers Web.
- É obrigatório estruturar o código do sistema de informação nos módulos apresentados na figura abaixo.



- É necessário utilizar as técnicas de Inteligência Artificial (por exemplo: o sistema deve ter a capacidade de aprender).

Muito importante:

- Outras variantes de servidores, por exemplo Mysql, PostgreSQL e tecnologias podem ser utilizados, mas o corpo docente poderá não garantir o apoio técnico.
- O nome do ficheiro do relatório deve ser o seguinte: kerobin_2019_XX.pdf e onde XX é o número do grupo.
- O relatório em papel + pdf+ficheiro extensão .mpp do Mapa de Gantt.
- Os grupos são encorajados a fazerem o desenvolvimento nos seus PCs, mas devem assegurar-se antes das demonstrações que o código deselvolvido funciona em qualquer servidor.

Entrega

- As características deste projecto requerem uma equipa composta obrigatoriamente por quatro elementos, com competências e responsabilidades bem definidas e distintas, que serão posteriormente avaliadas. **Excecionalmente**, se o número de elementos inscritos não permitir que todos os grupos tenham quatro alunos, poderão ser considerados grupos comum número inferior de alunos. Isto é, individual, dois ou três elementos, mas nunca cinco elementos.
- O relatório final deve conter a descrição da arquitetura utilizada. As listagem de todo o código desenvolvido e uma análise crítica de todas as opções tomadas ao longo do projecto (especialmente as destinadas a optimizar o acesso aos dados), apresentado os resultados das medidas de desempenho efectuadas.
- Deve ser entregue um relatório do trabalho em formato A4, escrito com letra do tipo ***Times New Roman*** ou semelhante. Um tamanho de letra de 12pt, à excepção de títulos, identificação e início de secções (14pt carregado – bold - é suficiente). O relatório NÃO deve ser entregue com a encadernação (e.g. argolas, cola, furos, …) excepto calha. As folhas

que constituem o relatório não devem ser agrafadas. Convidam-se os alunos a serem sucintos, sendo penalizados relatórios exageradamente longos. O relatório deverá conter:
O nome da disciplina, ano, a identificação do grupo e de cada um dos seus elementos.
Deve ocupar no máximo ¼ do topo da 1ª página – exemplo:

Programação IV, 4º Ano
SIS – Sistema de Informação de Saúde
Grupo nº 0001
Emanuel Cândido
Fabiana Joaquim
Funete Xindome
Helena Miguel

Penalizações

- Para além da entrega do relatório do trabalho em papel no formato A4, deverão entregar também o relatório numa Pendrive até às 12:00 de 29 /07/2019. Também podem utilizar o seguinte email para entrega: brentsuares22@hotmail.com até 24:00 de 29/07/2019. E para cada dia de atraso será descontado 20% da cotação total do trabalho.
- Projectos com ficheiros desnecessários na PenDrive terão uma penalização na nota de 20%. Consideram-se desnecessários os ficheiros gerados automaticamente na compilação.

Avaliação dos trabalhos

- As avaliações dos trabalhos serão realizadas na semana que tem início a 09 de Agosto devido a a importância do projecto, o processo de avaliação seguirá regras rigorosas. Todos os elementos do grupo terão de comparecer à avaliação e a avaliação é feita individualmente. Deste modo, cada elemento do grupo deve estar preparado para responder a qualquer questão relacionada com os trabalhos e com a matéria das aulas teórico-práticas.
- O trabalho entregue será avaliado com visualização e discussão. Após as discussões, cada aluno terá uma nota individual da disciplina que refletirá a sua participação no projecto.

.