Engenharia de Proteção

Objetivos

- Apresentar tópicos que devem ser considerados na especificação e no projeto de software seguro
- Discutir o gerenciamento de riscos de proteção e a derivação de requisitos de proteção de análise de riscos
- Descrever boas práticas de projeto para o desenvolvimento de sistemas seguros
- Explicar a noção de capacidade de sobrevivência de sistemas, e apresentar um método de análise da capacidade de sobrevivência

Tópicos abordados

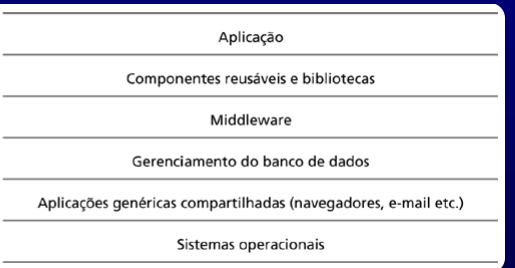
- Conceitos de proteção
- Gerenciamento de riscos de proteção
- Projeto para proteção
- Capacidade de sobrevivência de sistemas

Engenharia de proteção

- São ferramentas, técnicas e métodos para apoiar o desenvolvimento e a manutenção de sistemas que podem resistir aos ataques maliciosos, que tem a intenção de danificar um sistema baseado em computador ou seus dados.
- É um subcampo de um campo amplo de proteção de computadores.

Camadas de sistema

Figura 30.1
Camadas de sistema onde a segurança pode ser comprometida.



Proteção de aplicações/infra-estrutura

- A proteção de aplicações é um problema de engenharia de software em que o sistema é projetado para resistir aos ataques.
- A proteção de infra-estrutura é um problema de gerenciamento de sistemas, em que a infra-estrutura é configurada para resistir aos ataques.
- O foco deste capítulo é a proteção de aplicações.

Conceitos de proteção

Tabela 30.1 Conceitos de proteção

Termo	Descrição
Ativo	Recurso de sistema que possui um valor e deve ser protegido.
Exposição	Possível perda ou dano que pode resultar de um ataque bem-sucedido. Pode ser uma perda ou dano em dados ou uma perda de tempo e esforço, caso seja necessária uma recuperação depois de uma brecha de proteção.
Vulnerabilidade	Ponto fraco em um sistema baseado em computadores que pode ser explorado para causar perda ou dano.
Ataque	Exploração de uma vulnerabilidade do sistema. Geralmente, é externo ao sistema e constitui uma tentativa deliberada de causar algum dano.
Ameaça	Circunstâncias com potencial para causar perda ou dano. Você pode pensar nelas como uma vulnerabilidade de sistema sujeita a ataque.
Controle	Medida de proteção que reduz uma vulnerabilidade de sistema. A criptografia pode ser um exemplo de controle que reduz uma vulnerabilidade de um sistema fraco em controle de acesso.

Exemplos de conceitos de proteção

Tabela 30.2 Exemplos de conceitos de proteção

Termo	Descrição
Ativo	Os registros de cada paciente que está recebendo ou recebeu tratamento.
Exposição	Prejuízo financeiro potencial devido a futuros pacientes que não procurarão tratamento por não confiarem na clínica para manter seus dados. Prejuízo financeiro devido a ação jurídica movida pelo astro do esporte. Perda de reputação.
Vulnerabilidade	Sistema fraco em senhas que permite aos usuários criarem senhas que podem ser descobertas. IDs de usuário iguais a seus nomes.
Ataque	A imitação de um usuário autorizado.
Ameaça	Um usuário não autorizado ganhará acesso ao sistema descobrindo as credenciais (nome de login e senha) de um usuário autorizado.
Controle	Um sistema de verificação de senhas que desautoriza senhas definidas pelos usuários que sejam nomes próprios e palavras normalmente incluídas em um dicionário.

Ameaças de proteção

- Ameaças à confidencialidade de um sistema ou de seus dados.
- Ameaças à integridade de um sistema ou de seus dados.
- Ameaças à disponibilidade de um sistema ou de seus dados.

Controles de proteção

- São controles que se destinam a assegurar que os ataques sejam mal sucedidos. É análogo à prevenção de defeitos.
- São controles que se destinam a detectar e repelir os ataques. É análogo à detecção e tolerância de defeitos.
- Controles que se destinam a apoiar a recuperação de problemas. É análogo à recuperação de defeitos.

Gerenciamento de riscos de proteção

- O gerenciamento de riscos está relacionado à avaliação de possíveis perdas que poderiam ser resultados de ataques ao sistema, e ao balanço dessas perdas em relação os custos de procedimentos de proteção que podem reduzí-las.
- O gerenciamento de riscos deve ser dirigido por uma política de proteção organizacional.
- O gerenciamento de riscos envolve:
  - Gerenciamento de riscos preliminar;
  - Avaliação de riscos de ciclo de vida.

Avaliação de riscos preliminar

Figura 30.2
Avaliação de riscos preliminar.

Análise de ativos

Tabela 30.3 Análise de ativos em um relatório de avaliação de riscos preliminar

Ativo	Valor	Exposição
Sistema de informações	Alto. Necessário para dar suporte a todas as consultas clínicas. Potencialmente crítico em segurança.	Alta. Prejuízo financeiro, na medida em que as consultas podem ser canceladas. Custos de restauração de sistema. Possível dano ao paciente se o tratamento não puder ser prescrito.
Banco de dados de pacientes	Alto. Necessário para apoiar todas as consultas clínicas. Potencialmente crítico em segurança.	Alta. Prejuízo financeiro, na medida em que as consultas podem ser canceladas. Custos de restauração de sistema. Possível dano ao paciente se o tratamento não puder ser prescrito.
Registro individual de paciente	Normalmente baixo, embora possa ser alto para pacientes específicos de perfil alto.	Baixos prejuízos diretos, mas possível perda de reputação.

Análise de ameaças e de controle

Tabela 30.4 Análise de ameaças e controles em um relatório de avaliação de riscos preliminar

Ameaça	Probabilidade	Controle	Viabilidade
Usuário não autorizado ganha acesso como gerente de sistema e torna o sistema indisponível	Baixa	Permitir somente o gerenciamento do sistema com base em localizações específicas fisicamente protegidas.	Baixo custo de implementação, mas devem ser tomados cuidados com a distribuição de chaves e assegurar que estas estejam disponíveis no caso de uma emergência.
Um usuário não autorizado obtém acesso como usuário de sistema e acessa informações confidenciais	Alta	Requerer que todos os usuários se autentiquem usando um mecanismo biométrico. Fazer o log de todas as mudanças de informações de pacientes para acompanhar o uso do sistema.	Tecnicamente viável, mas uma solução de alto custo. Possível resistência do usuário. Simples e transparente de implementar e também dá suporte para a recuperação.

Requisitos de proteção

- As informações do paciente devem ser baixadas, no início de uma sessão clínica, para uma área segura do sistema cliente que é usado pelo pessoal clínico.
- As informações do paciente não devem ser mantidas em sistemas cliente depois que uma sessão clínica terminou.
- Um log deve ser mantido, em um computador separado do servidor de banco de dados, com todas as mudanças efetuadas no banco de dados de sistema.

Avaliação de riscos de ciclo de vida

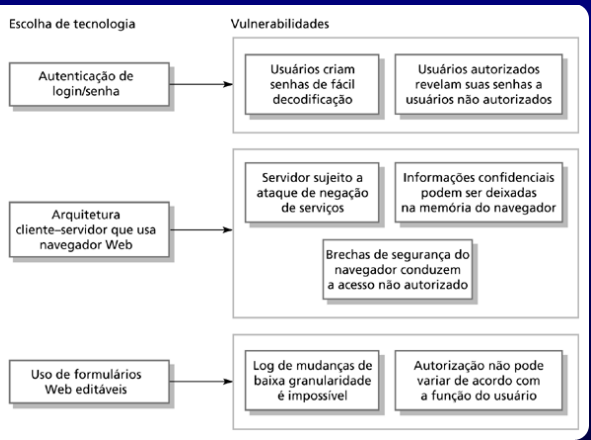
- É a avaliação de riscos enquanto o sistema está sendo desenvolvido, e após ele ter sido implantado.
- Mais informações são disponíveis – plataforma de sistema, middleware, a arquitetura de sistema e a organização de dados.
- As vulnerabilidades que surgem das escolhas de projeto podem, portanto, ser identificadas.

Exemplos de decisões de projeto

- Usuários de sistema autenticados usando uma combinação de nome/senha.
- A arquitetura de sistema é cliente-servidor, com clientes acessando o sistema por meio de um web browser padrão.
- As informações são apresentadas como um formulário de Web editável.

Vulnerabilidades de tecnologia

Figura 30.3
Vulnerabilidades associadas a escolhas de tecnologia.



Projeto para proteção

- Projeto de arquitetura – como as decisões de projeto de arquitetura afetam a proteção de um sistema?
- Boas práticas – o que é aceito como boa prática quando se projeta sistemas seguros?
- Projeto para implantação – qual apoio deve ser projetado nos sistemas para evitar a introdução de vulnerabilidades quando um sistema for implantado para uso?

Projeto de arquitetura

- Proteção
  - Como o sistema deve ser organizado de modo que ativos críticos possam ser protegidos contra ataques externos?
- Distribuição
  - Como os ativos de sistema devem ser distribuídos de modo que os efeitos de um ataque bem sucedido sejam minimizados?
- Conflitos potenciais
  - Se os ativos são distribuídos, são mais onerosos para proteger.

Proteção

- Proteção no nível de plataforma
- Proteção no nível de aplicação
- Proteção no nível de registro

Proteção em camadas

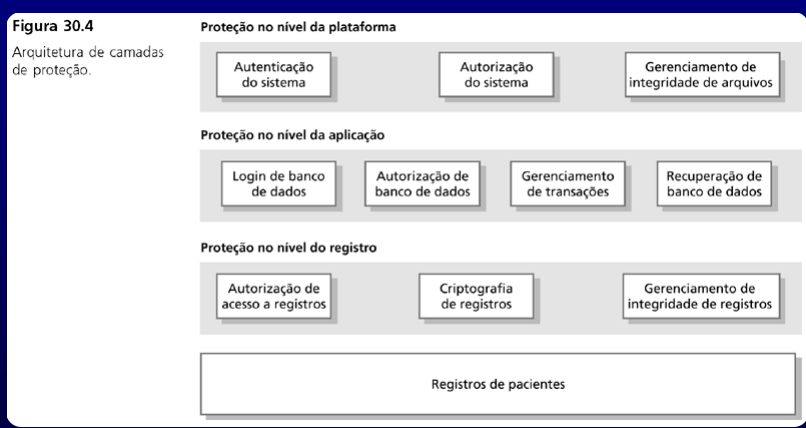
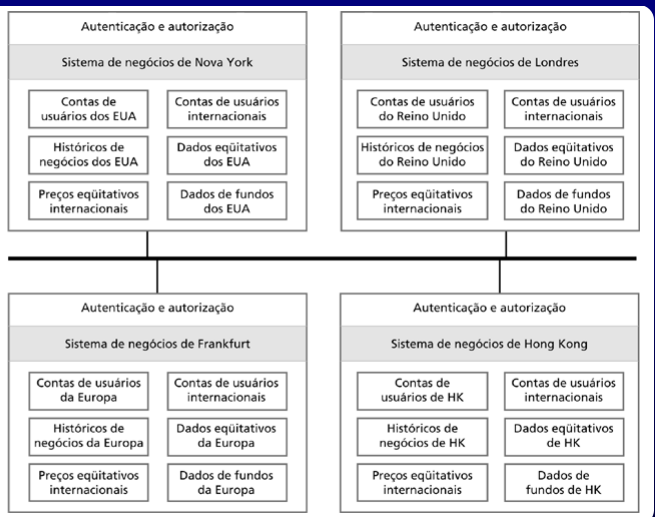


Figura 30.4 Arquitetura de camadas de proteção.

Um sistema distribuído eqüitativamente

Figura 30.5
Ativos distribuídos em um sistema de negócios eqüitativo.



Diretrizes de projeto

- As diretrizes de projeto englobam boas práticas em projetos de sistemas seguros
- Diretrizes de projeto servem para dois propósitos:
  - Aumentam a consciência sobre questões de proteção em uma equipe de engenharia de software;
  - Podem ser usadas como base de um checIklist de revisão que é aplicado durante o processo de validação de sistema.

Diretrizes de projeto 1

- Basear as decisões de projeto em uma política de proteção explícita
- Evitar um ponto único de falha
- Falhar de maneira protegida
- Equilibrar proteção e usabilidade
- Estar ciente da possibilidade de engenharia social

Diretrizes de projeto 2

- Usar redundância e diversidade para reduzir riscos
- Validar todas as entradas
- Compartimentar seus ativos
- Projetar para implantação
- Projetar para capacidade de recuperação

Projetar para implantação

- Implantação envolve a configuração de software para funcionar em seu ambiente operacional, a instalação do sistema e sua configuração para a plataforma operacional.
- Vulnerabilidades podem ser introduzidas neste estágio como um resultado de erros de configuração.
- Um projeto de apoio de implantação no sistema pode reduzir a probabilidade de vulnerabilidades serem introduzidas.

Implantação de software

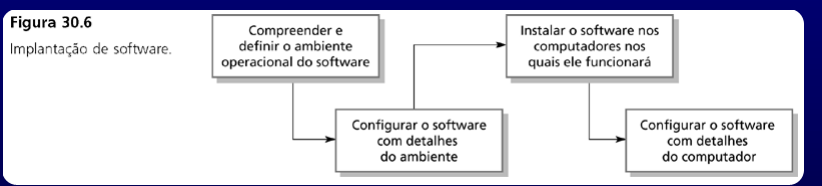


Figura 30.6
Implantação de software.

Apoio à implantação

- Incluir apoio para visualização e análise de configurações
- Minimizar privilégios default e, portanto, limitar o dano que poderia ser causado
- Localizar parâmetros de configuração
- Prover formas simples para reparar a vulnerabilidades de proteção

Capacidade de sobrevivência de sistemas

- Capacidade de sobrevivência é uma propriedade emergente de sistema que reflete a sua habilidade de continuar a fornecer serviços essenciais enquanto está sob ataque, ou depois que parte do sistema tenha sido danificada.
- A análise e projeto de capacidade de sobrevivência deve ser parte do processo de engenharia de proteção.

Disponibilidade de serviços

- Quais serviços de sistema são os mais críticos para um negócio?
- Como esses serviços poderiam ser comprometidos?
- Qual é a mínima qualidade de serviço que deve ser mantida?
- Como esses serviços podem ser protegidos?
- Se um serviço se torna indisponível, com que rapidez ele pode ser recuperado?

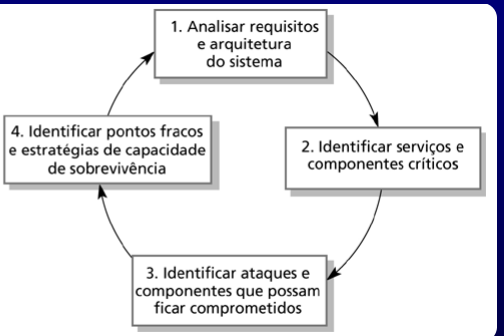
Estratégias de capacidade de sobrevivência

- Resistência
  - Evitar problemas por meio da implementação de capacidades no sistema para repelir ataques.
- Reconhecimento
  - Detectar problemas por meio da implementação de capacidades no sistema para detectar ataques e falhas e avaliar os danos resultantes.
- Recuperação
  - Tolerar problemas por meio da implementação de capacidades no sistema para fornecer serviços enquanto está sob ataque.

Método de capacidade de sobrevivência de sistema

Figura 30.7

Estágios de análise de capacidade de sobrevivência.



Atividades principais

- Compreensão de sistema
  - Revisar objetivos, requisitos e arquitetura.
- Identificação de serviços críticos
  - Identificar serviços que devem ser mantidos.
- Simulação de ataques
  - Inventar cenários de ataque e identificar componentes afetados.
- Análise de capacidade de sobrevivência
  - Identificar estratégias de capacidade de sobrevivência a ser aplicadas.

Capacidade de sobrevivência de sistemas de negócio

- Contas de usuário e preços eqüitativos replicados entre servidores e, assim, mais provisão de capacidade de sobrevivência é feita.
- O serviço principal a ser mantido é a capacidade de colocar pedidos de produtos.
- Os pedidos devem ser precisos e refletir as vendas/compras feitas pelo negociador.

Análise de capacidade de sobrevivência

Tabela 30.5 Análise de capacidade de sobrevivência em um sistema de negócios eqüitativos

Ataque	Resistência	Reconhecimento	Recuperação
Usuário não autorizado envia pedidos maliciosos	Exigir uma senha de negócio diferente da senha de login para enviar pedidos	Enviar cópia do pedido por e-mail para um usuário autorizado com número de telefone de contato (assim eles podem detectar pedidos maliciosos). Manter o histórico de pedidos do usuário e verificar padrões de transação incomuns.	Fornecer mecanismo para 'desfazer' automaticamente as transações e restaurar contas de usuários. Ressarcir usuários por perdas devido às transações maliciosas. Proteger-se contra as conseqüências de perdas.
Corrompimento de banco de dados de transações	Exigir que os usuários privilegiados sejam autorizados a usar um mecanismo de autenticação robusto, como certificados digitais.	Manter cópias somente para leitura de transações de um escritório em um servidor internacional. Comparar periodicamente as transações para verificar se foram corrompidas. Manter checksum criptográfico em todos os registros de transações para detectar corrompimento.	Recuperar o banco de dados com base em cópias de back-up. Fornecer um mecanismo para reproduzir as transações de um período específico para recriar banco de dados de transações.

Pontos-chave

- A engenharia de proteção enfoca como desenvolver sistemas que podem resistir a ataques maliciosos.
- Ameaças de proteção podem ser ameaças à confidencialidade, à integridade ou à disponibilidade de um sistema e seus dados.
- O gerenciamento de riscos de proteção envolve a avaliação de perdas possíveis provenientes de ataques, e a derivação de requisitos de proteção para minimizar as perdas.
- Projeto para proteção envolve projeto de arquitetura, seguindo boas práticas de projeto e minimização de introdução de vulnerabilidades do sistema.

Pontos-chave

- Questões principais ao projetar uma arquitetura segura incluem a organização de estrutura para proteger ativos e distribuição de ativos para minimizar as perdas.
- Diretrizes gerais de proteção sensibilizam projetistas para questões de proteção, e servem como checklists de revisão.
- Visualização de configuração, localização de parâmetros e minimização de privilégios default ajudam a reduzir os erros de implantação.
- A capacidade de sobrevivência reflete a habilidade de um sistema em continuar a fornecer serviços enquanto está sob ataque, ou após uma parte do sistema ter sido danificada.