Segurança Informática

Aula 1

Docente: Ricardo Costa
rcosta@estg.ipp.pt

1. Conceitos introdutórios

Objetivos:

* Compreender conceitos básicos sobre segurança informática.

* Apresentar os principais conceitos relacionados com a segurança informática.

Princípios de Segurança Informática

- A evolução e a redução do custo de aquisição de computadores e outros aparelhos tecnológicos, tornou mais atraente a possibilidade de utilização destes quer em ambientes isolados ou em ambientes em rede.

- Esta possibilidade de conexão de computadores e outros aparelhos tecnológicos em redes trouxe consigo algumas vantagens e também desvantagens.

Princípios de Segurança Informática

- Um sistema informático é dito seguro se responde a três requisitos básicos relacionados aos recursos que o compõem:
  - Confidencialidade
    - Garantir restrições de acesso e divulgação da informação.
  - Integridade
    - Propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.
  - Disponibilidade (incluí hardware, software, recursos e utilizadores)
    - Propriedade de que a informação não esteja disponível a quem não tem autorização nem esteja credenciado.

Princípios de Segurança Informática

- A Confidencialidade, Integridade e Disponibilidade, representam os principais atributos que, atualmente, orientam a análise, o planeamento e a implementação da segurança informática.

- Outros atributos importantes são o controlo e auditoria.

  - Auditoria: Da mesma forma que um controlo deve ser feito para evitar o acesso não autorizado a um sistema, deve ser feito também o controlo de ações de utilizadores autorizados.

  - Controlos de auditoria devem permitir a criação de históricos de acessos válidos para uma eventual verificação de atividades irregulares executadas por utilizadores devidamente autorizados.

Segurança – conceitos básicos

- Dada uma troca de informação entre duas entidades através de um canal de comunicação:

A -(i) -> B

- Autenticação
  - Garantia que A e B são quem dizem ser.
- Confidencialidade
  - Garantia que só A e B têm acesso ao conteúdo da informação.
- Autorização
  - Garantia que B tem o direito a aceder à informação enviada por A.
- Integridade
  - Garantia que a informação enviada por A é a mesma que é recebida por B.

Segurança – conceitos básicos

- Não-repudiação
  - Garantia que a informação recebida por B foi mesmo enviada por A.
- Disponibilidade
  - A capacidade de A e B para trocarem informação não depende de terceiros.
- Privacidade
  - B garante que a informação recebida não será nunca disponibilizada a terceiros sem o acordo de A.

Segurança - implementação

- Autenticação
  - Passwords, certificados digitais
- Confidencialidade
  - Tecnologias de encriptação
    - Chaves simétricas e assimétricas
- Autorização
  - Políticas de Acesso:
    - Policy Enforcement Points (PEP)
    - Policy Decision Points (PDP)
    - Access Control Lists (ACLs)
    - Role Based Access Control (RBAC)

Segurança - implementação

- Integridade
  - geração de digest criado por algoritmo de hashing
  - envio do digest encriptado com chave privada (assinatura)
- Não-repudiação
  - validação da assinatura através de chave pública obtida em certificado:
    - Certification Authority (CA)
    - Public Key Infrastructure (PKI)
      - conjunto de hardware, software, pessoas, políticas e procedimentos necessários para criar, gerir, distribuir, usar, armazenar e revogar certificados digitais.
- Disponibilidade
  - autenticação dos intervenientes
  - rejeição de interações repetidas (firewalls)
- Privacidade
  - encriptação de informação armazenada
  - políticas de segurança efetivas

Desafios da Segurança Informática

- As tecnologias da informação e comunicação são hoje meios indispensáveis em qualquer atividade da sociedade.
- Ameaças contra a sua disponibilidade, integridade e confidencialidade podem resultar em ocorrências nefastas para o normal decurso das atividade das instituições.
- A segurança informática é também um tópico que tem vindo a merecer bastante atenção, por parte dos profissionais de TI em particular e no geral pela sociedade.

Desafios da Segurança Informática

- Alguns dos desafios de segurança de computadores são:
  - Complexidade
    - A segurança informática pode parecer fácil de implementar, porque as suas exigências são simples, temos confidencialidade, autenticação, não repúdio, integridade.
    - Mas os mecanismos utilizados para atender a esses requisitos podem ser bastante complexos.
  - Desenvolvimento e posse dos algoritmos de segurança
    - Mecanismo de segurança pode exigir mais de um algoritmo ou protocolo.
    - Isso traz um desafio de criação, distribuição e proteção dessas informações.
    - Também pode haver uma dependência de protocolos de comunicações, cujo comportamento pode complicar o processo de desenvolvimento do mecanismo de segurança.

Desafios da Segurança Informática

- Colocação de algoritmo de segurança
  - Se o algoritmo de segurança for bem sucedido, há um outro desafio que é saber onde usá-lo.
    - Isso é necessário tanto para colocação física (por exemplo, em que pontos de uma rede são necessários certos mecanismos de segurança) e num sentido lógico (por exemplo, em que camada ou camadas de uma arquitetura, tais como TCP / IP deve ser o algoritmo de segurança colocado).

- Possíveis ataques
  - Ao desenvolver um mecanismo de segurança específico ou algoritmo, deve-se sempre em primeiro lugar analisar os potenciais ataques sobre esses recursos de segurança.
  - No entanto, os ataques bem-sucedidos são projetados por analisar o problema de uma forma completamente diferente.

Desafios da Segurança Informática

- Desafio de conhecimentos
  - A segurança informática é normalmente uma batalha entre as mentes de uma pessoa que está a tentar encontrar falhas de segurança e o administrador que tenta reduzí-las ou eliminá-las.
  - A principal vantagem do atacante é que este só precisa encontrar uma única fraqueza, enquanto o administrador deve encontrar e eliminar todos os pontos fracos para alcançar a segurança perfeita.

- Ignorância
  - Há uma tendência natural por parte de utilizadores do sistema e alguns administradores em compreender a necessidade de investimento em segurança até que ocorra uma falha de segurança.

Desafios da Segurança Informática

- Falta de tempo
  - A segurança de um parque informático precisa de constante monitorização e isso às vezes é um grande desafio para algumas pessoas devido à falta de tempo devido a sobrecarga de tarefas.

- Mau planeamento
  - Segurança é na maioria das vezes incorporada num sistema depois que o projeto está concluído, em vez de ser uma parte integrante do processo de design.
  - Às vezes, é visto também como um obstáculo ao funcionamento eficiente e de fácil utilização de um sistema de informação ou uso da informação.

Modelo de Segurança Informática

- No modelo de segurança informática, precisamos de olhar para os recursos do sistema, ou ativos, que se deseja proteger.

- Pode listar os seguintes recursos do sistema:
  - Hardware
  - Software
  - Dados
  - Instalações e redes de comunicações
  - Utilizadores

Modelo de Segurança Informática

- Nos termos de segurança informática, estes recursos do sistema podem estar sob diferentes categorias de vulnerabilidades.

- As categorias gerais de vulnerabilidades de um dos recursos de sistema de computador ou recursos de rede são:
  - Vulnerabilidades
    - Os recursos do sistema de computador podem ser corrompidos, para que execute ações não solicitadas.
      - Por exemplo, dados armazenados podem ser indevidamente modificados.
      - Recursos do sistema ou rede podem tornar-se permeáveis.
      - Podem ficar indisponíveis ou muito lento.
  - Ameaças
    - Uma ameaça é o principal perigo de segurança para os recursos do sistema ou rede, pois é capaz de explorar as vulnerabilidades de segurança do computador.
    - Um ataque é um tipo de ameaça que, se realizado com sucesso pode levar a uma violação indesejável de segurança do computador, ou consequência ameaça.
    - Os ataques podem ser de dois tipos;
      - Ataque ativo que é uma tentativa de alterar os recursos do sistema ou afetar o seu funcionamento.
      - Ataque passivo que é uma tentativa de aprender ou fazer uso de informação do sistema que não afeta os recursos do sistema.

Modelo de Segurança Informática

- Estes tipos de ataques também podem ser classificados de acordo com a origem do ataque:
  - Ataque interno que é iniciado por uma pessoa/item dentro do perímetro de segurança (um "insider").
  - Ataque externo que é iniciado por uma pessoa/recurso fora do perímetro, por um utilizador não autorizado ou ilegítimo do sistema (um "estranho").
  - Esses tipos de ataques podem ser controladas no âmbito do processo conhecido como contramedida. Trata-se de prevenção, onde um ataque em particular é impedido de ser executado com sucesso.
  - Se a prevenção falhar, então o próximo passo é para detetar o ataque e, em seguida, recuperar dos efeitos do ataque.

Segurança na Internet

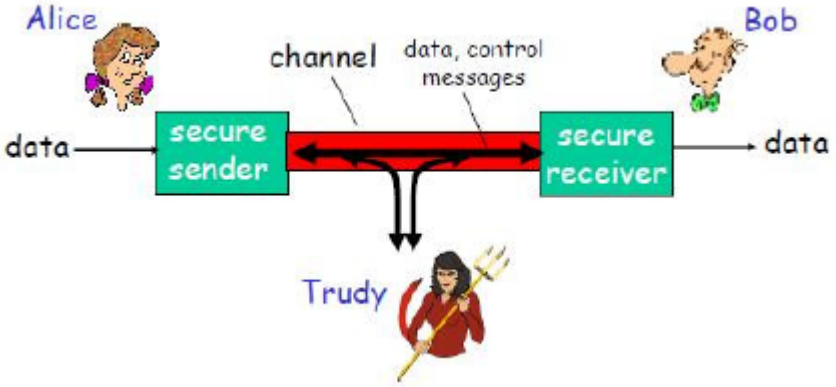
- Os requisitos associados ao eBusiness promoveram a adoção generalizada de protocolos de segurança.

- A segurança foi essencial na transformação da Internet num espaço de negócio:
  - Protocolos de encriptação de chave assimétrica
  - Distribuição de chaves através de certificados digitais (CA)
  - Implementação open source do SSL permite utilização generalizada
  - Suportado por todos os browsers e servidoresWeb

- Bem adaptados ao modelo de interacção do Business-to-Consumer (B2C):
  - Modelo de acesso single-hop

Segurança na Internet - Exemplo

- Amigos e Inimigos: Alice, Bob & Trudy.
- As personagens Alice e Bob, namorados, querem comunicar de forma "segura".
- Trudy, o intruso pode intercetar, apagar, modificar ou adicionar mensagens.



Segurança na Internet - Exemplo

- Quem pode ser a Alice e o Bob?
  - Podem ser Alices e Bobs da vida real!
  - Um Web browser e um servidor a realizar transações comerciais (ex., compras on-line)
  - Cliente e servidor de aplicação de Home banking
  - DNS servers
  - Routers a trocar atualizações de tabelas

Segurança na Internet - O que um intruso pode fazer?

- Eavesdrop
  - intercetar mensagens
- Inserir mensagens forjadas na ligação
- Impersonation
  - pode forjar (spoof) endereços de origem em pacotes (ou qualquer campo num pacote)
- Hijacking
  - "assaltar" uma conexão em curso retirando o remetente ou destinatário e tomar o seu lugar
- Denial of service
  - impedir serviços de serem utilizados por outros (ex., sobrecarregando os servidores)

QUESTÕES

?