Segurança em Sistemas de Computação

Davidson Rodrigo Boccardo

flitzdavidson@gmail.com

Segurança

- Segurança deve considerar o ambiente externo do sistema, e proteger de:
  - Acesso não autorizado
  - Alteração ou destruição maliciosa

- Mais difícil proteger os objetos de um sistema contra ações maliciosas do que evitar que acidentes violem o esquema de segurança

Segurança

- É indiferente se tratada do ponto de vista de uma rede ou de uma máquina isolada, visto que o problema é o controle de acesso (autenticação e controle de permissões)

- Salientando algumas diferenças em relação ao escopo de atuação e vulnerabilidade

Ataques a Sistemas de Computação

- Tem a função de corromper, degradar, negar ou destruir informações residentes ou serviços oferecidos
- Ataques conhecidos:
  - Spoofing, modificação, recusa ou impedimente de serviço (DoS), códigos maliciosos, sniffing , brechas do sistema (uso de scanners)

Comunicação segura

- Envolve sigilo, autenticação (máquina ou rede) e integridade da mensagem
  - Sujeito a quais tipos de ataques?
    - Sniffing (placa de rede em modo promíscuo), spoofing (falsificação IP), modificação
  - Autenticação
    - Procedimentos distintos (procedimentos simples envolvendo somente o acesso físico ao equipamento, ou mais complexos como timbre vocal, iris, impressão digital, DNA)

Comunicação segura

- Solução?
  - Através de criptografia
    - Permite o remetente disfarçar os dados de modo que um intruso não consiga obter informação com base nos dados interceptados.
    - Técnicas de codificação da mensagem são conhecidas, por isso tem um pedaço de informação secreta contida nas mensagens (as chaves)

Criptografia

- Dois tipos de chaves
  - Chaves simétricas (as chaves dos sistemas comunicantes são idênticas e secretas)
  - Chaves públicas (utiliza de um par de chaves, uma pública e outra privada)
- Chaves simétricas
  - Cifra de César (deslocamento no alfabeto por um índice k, e.g. (a letra a seria a letra d)), somente 25 valores possíveis de chaves

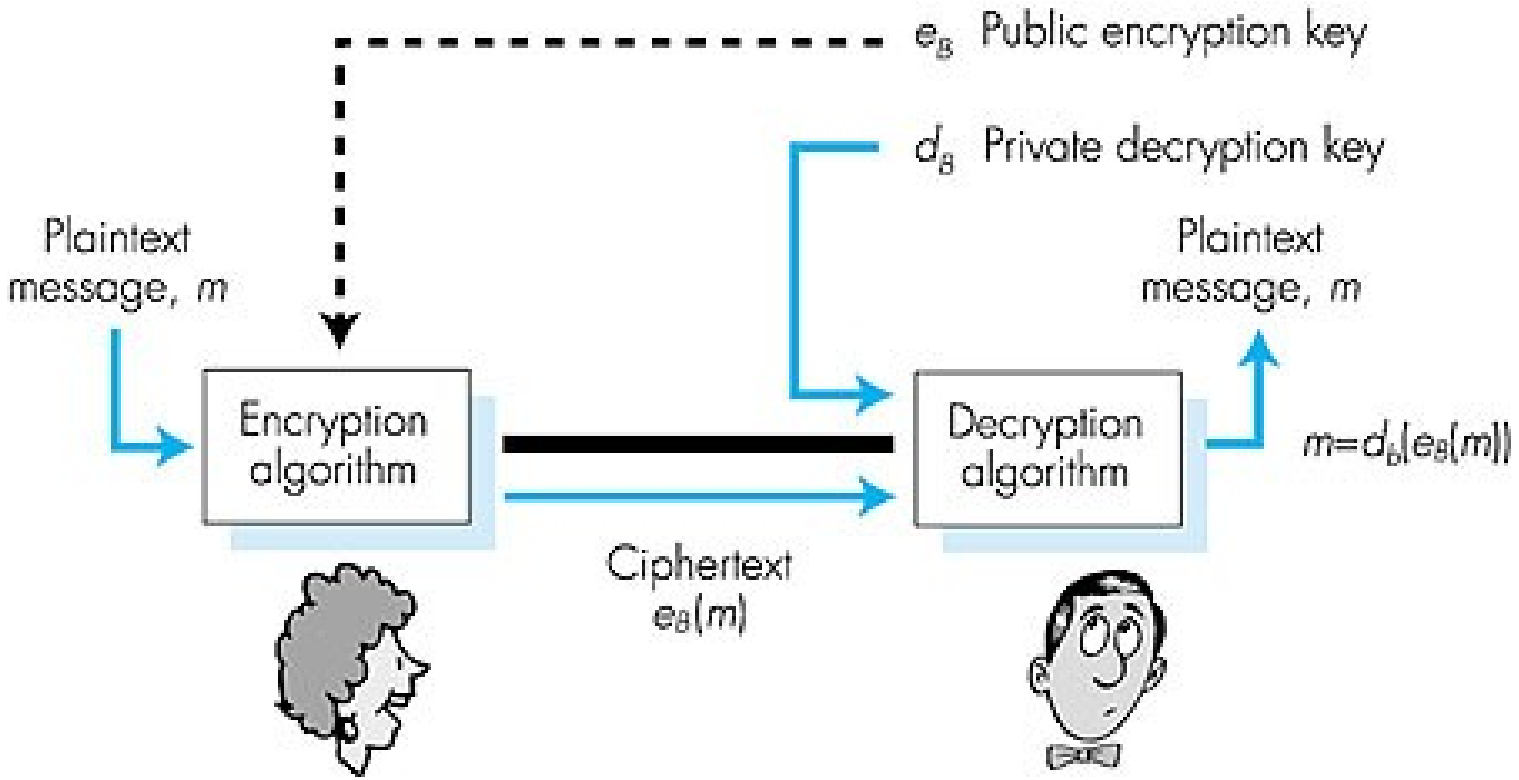
Criptografia

- Chaves simétricas
  - Cifra monoalfabética (qualquer letra pode ser substituída por qualquer outra)
  - Cifras polialfabéticas (Cifras de Vigenere), utilizam de múltiplas cifras monoalfabéticas
- Atualmente:
  - DES (Data Encryption Standard) e 3DES
  - Usa chave de 64 bits
  - 1997 (Uma equipe demorou quase 4 meses para quebrar uma mensagem, prêmio $ 10.000)
  - 1999 (menos de 22 horas em um computador que custa 250 mil dólares (“Deep Crack”)

Criptografia

- Chaves públicas (1976)
  - Dificuldade da chave simétrica?
    - Como entregar a chave com segurança
  - Utilizada não somente em criptografia, como autenticação e assinatura digital (será visto em slides posteriores)
  - Um dos algoritmos (RSA, nome dos autores)
  - Funcionamento?
  - Como autenticar o remetente da mensagem?
  - DES é 100x e entre 1000x a 10.000x mais rápido do que o RSA (software e hardware respectivamente)
  - Por isso na prática é usado em combinação com o DES (envio da chave DES através de criptografia RSA)

Criptografia por chaves públicas



Autenticação

- É o processo de provar a própria identidade, permitindo que o acesso lógico ao sistema seja habilitado para cada usuário.
- Baseada na posse (chave ou um cartão), conhecimento (um nome e uma senha), ou atributo (impressão digital, padrão de retina ou assinatura)

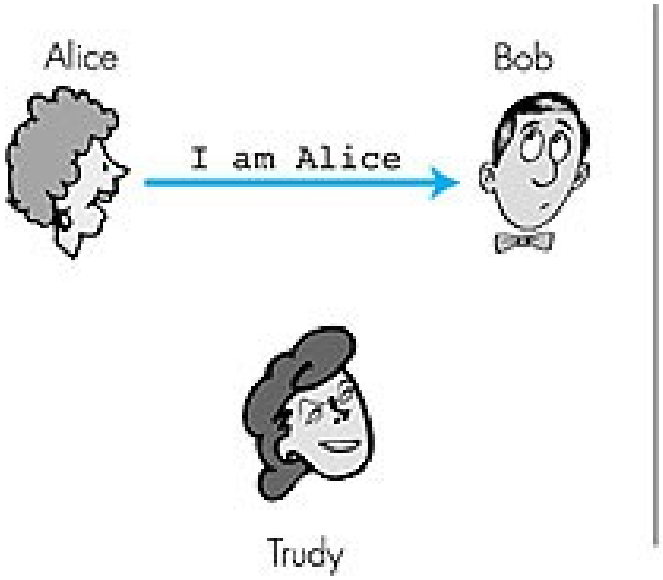
Autenticação

- Numa rede, as partes comunicantes não podem confiar em informações biométricas, a autenticação deve ser feita na base de mensagens e dados trocados como parte de um protocolo de autenticação
- O uso de senhas é extremamente comum, porque são fáceis de utilizar, porém tem vários problemas associados
  - Um outro usuário com a senha
    - Por descuido, por senhas fracas ou por força bruta
    - Por escuta da rede (sniffing), obtendo a senha

Autenticação

- Métodos preventivos:
  - O sistema pode gerar senhas (difícil para o usuário lembrar, ao contrário de senhas que o usuário cria que geralmente são fracas) ou alertar que a senha é fraca
  - Podem exigir troca de senha a cada período de tempo
  - Qual seria uma boa técnica para geração de senha?
- UNIX grava senhas criptografadas em um arquivo (força bruta poderia comparar estas senhas e descobrir alguma senha)

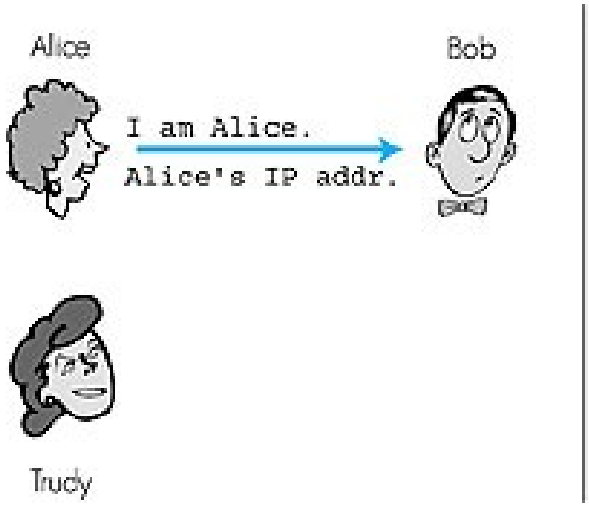
Autenticação de rede (Cenários)



Falha?

Trudy pode passar-se como se fosse a Alice

Autenticação de rede (Cenários)



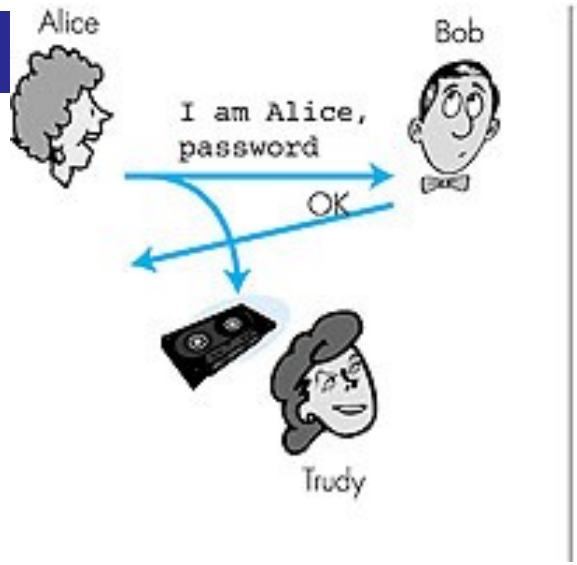
Falha?

Trudy poderia usar a técnica de spoofing para dizer que seu IP é igual o IP do computador de Alice

Solução?

Roteadores poderia verificar isso e não repassar IP falsificado

Autenticação de rede (Cenários)



Esquemas de autenticação (senha) são usados em HTTP, FTP e Telnet. Falha?

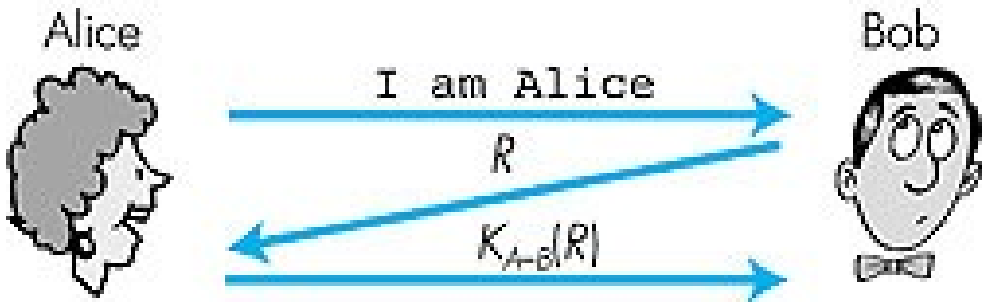
Trudy poderia usar a técnica de sniffing para capturar a senha de Alice

Solução?

Usar criptografia?

Não garante autenticação, porque Trudy poderia passar a senha criptografada e se passar por Alice

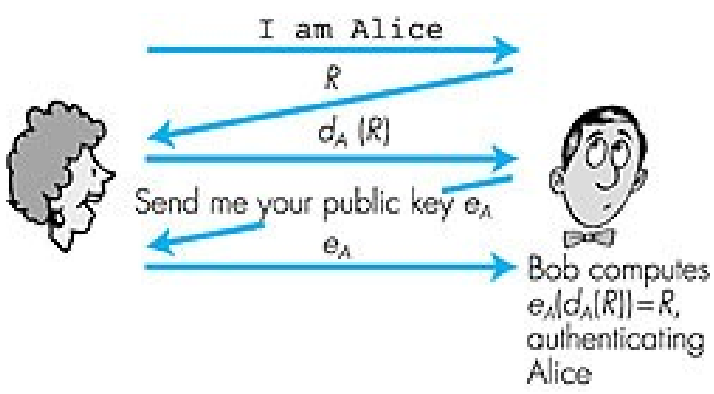
Autenticação de rede (Cenários)

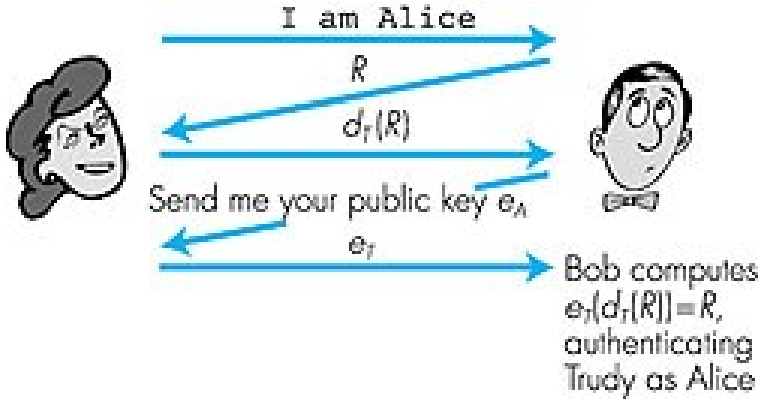


Bob envia um número (cada vez é diferente), Alice codifica este número R (chave simétrica) e envia a Bob, Bob decodifica e autentica a Alice usando a chave secreta

Não há cenário de falha

Autenticação de rede(Cenários)





E se fosse usar o esquema de chave pública?
R. Poderia ocorrer o caso de Trudy interceptar as mensagens que iam para Alice e se autenticar-se como se fosse Alice
Solução?
Distribuição segura das chaves públicas

Integridade

- Assinaturas atestam o fato que a pessoa conhece o conteúdo ou concorda com ele.
- No mundo digital, frequentemente quer indicar o dono ou criador de algum documento, a assinatura digital é uma técnica criptográfica que tem esta finalidade
- Assinatura digital é facilmente feita através de chaves públicas

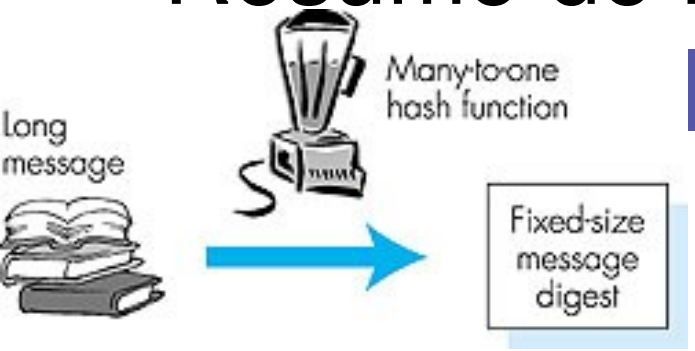
Integridade

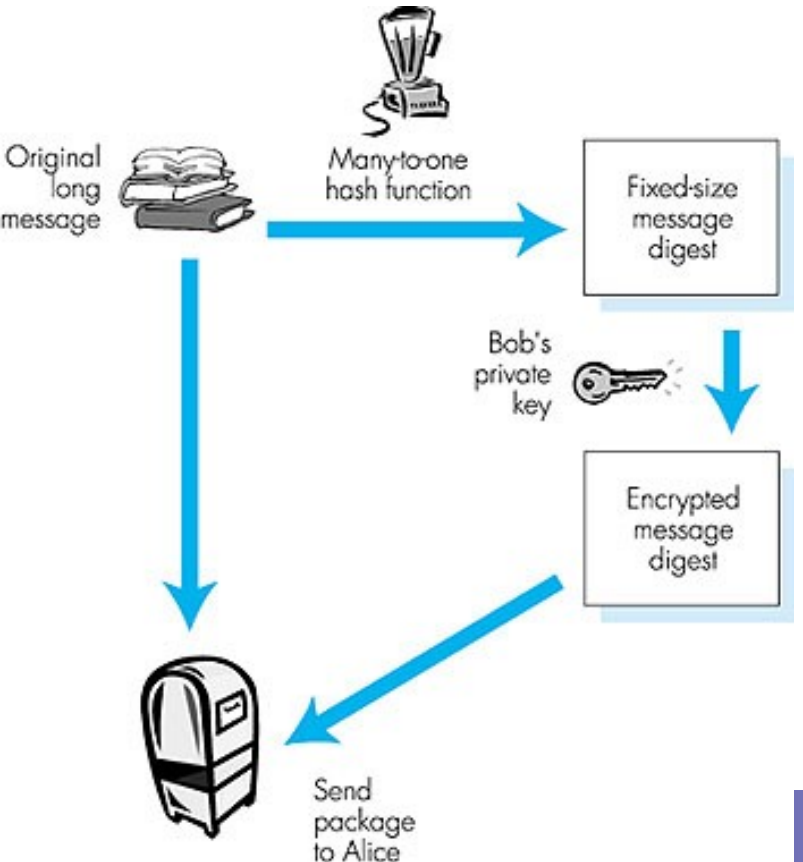
- Funcionamento:
  - Suponha que Bob quer transmitir uma mensagem para Alice
  - Bob codifica a mensagem com sua chave secreta e envia a Alice
  - Alice aplica a chave pública de Bob e verifica que ele é o autor daquela mensagem (a não ser que a chave secreta foi roubada de Bob ou Bob passou ela a alguém)
  - Evita também futuras modificações no documento

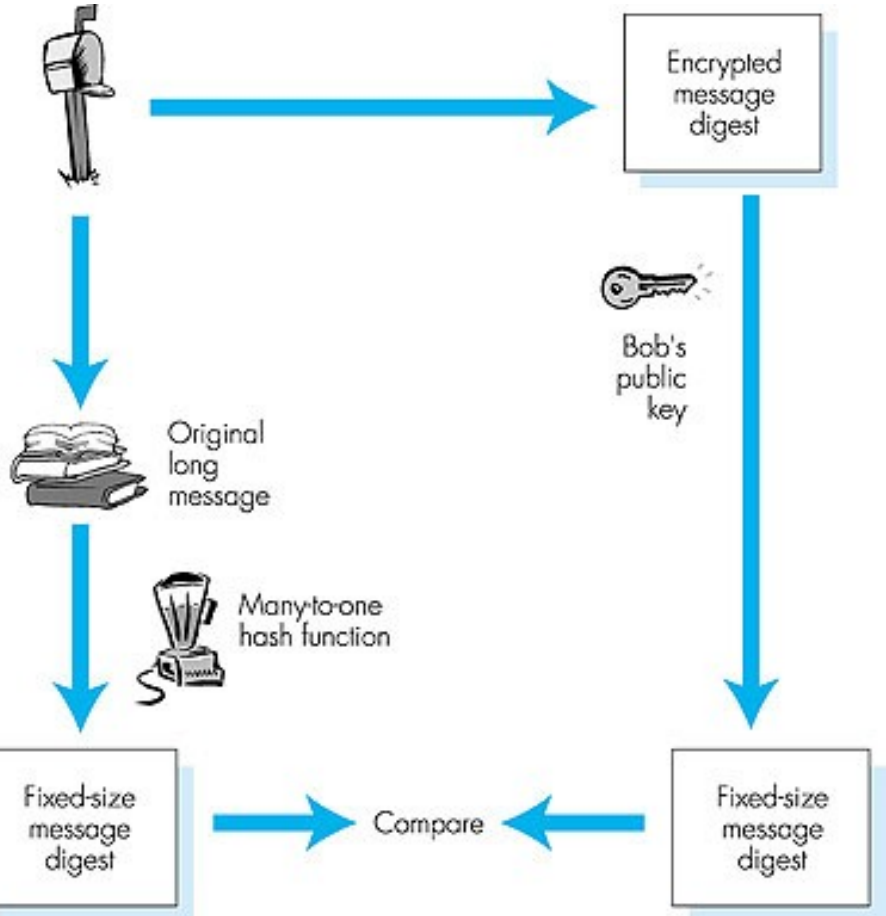
Integridade

- Assinar toda mensagem pode gastar muito tempo dependendo da aplicação, por isso existem os resumos de mensagem
- Resumo de mensagem é muito parecido com uma soma de verificação, pegam uma mensagem de comprimento arbitrário e calculam uma impressão digital
- Vantagem: Menos tempo para codificar, e garante a integridade da mensagem
- Algoritmos: MD5, SHA-1

Resumo de mensagem







Exemplo (E-mail seguro)

- Características para um e-mail seguro ?
  - Sigilo, autenticação do remetente, integridade da mensagem
- O que fazer para obter sigilo?
  - Para sigilo pode-se usar chaves simétricas (problema na distribuição), por isso uso de chaves públicas (ineficiência para mensagens longas)
  - Com isso uso de chave de sessão (criptografa uma chave simétrica com a chave pública)

Exemplo (E-mail seguro)

- O que fazer para autenticação do remetente e garantir a integridade da mensagem?
  - Assinaturas digitais e resumos de mensagem
  - Único problema é o fato de uma pessoa intervir na distribuição das chaves
- PGP
  - Em essência garante sigilo, autenticação do remetente e integridade da mensagem. Utiliza 3DES ou Idea para chaves simétricas, RSA para chaves públicas, MD5 ou SHA para resumos e oferece compressão de dados

Controle de permissões

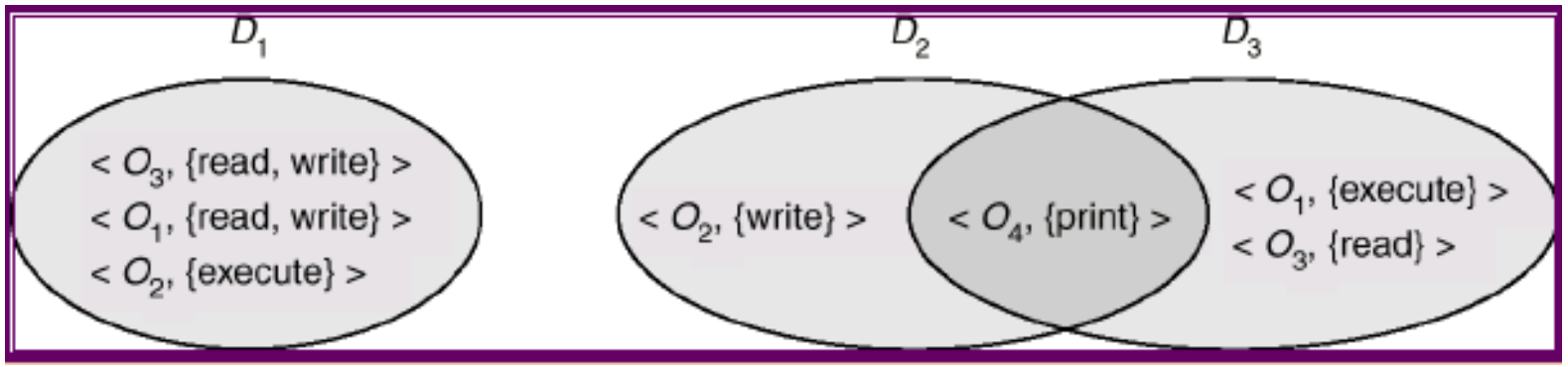
- Uma vez que o usuário tenha ganho acesso ao sistema ainda é preciso controlar suas ações dentro dele
- Um mecanismo de segurança é usado para controlar o acesso de programas, processos ou usuários aos dispositivos ou componentes de um sistema operacional
- Estes mecanismos variam de sistema para sistema e de recurso para recurso

Segurança

- Um sistema operacional consiste de uma coleção de objetos de hardware e software
- Cada objeto tem um único identificador e pode ser acessado através de um conjunto de operações bem definidas
- Objetivo do mecanismo?
  - Assegurar que cada objeto é acessado corretamente e somente por processos permitidos

Estrutura de domínios

- Direito de acesso = <nome-objeto, conjunto-de-operações>, onde conjunto-de-operações é um subconjunto de operações válidas que podem ser realizadas naquele objeto
- Domínio = conjunto de direitos de acesso



Implementação de domínio (UNIX)

- No caso de arquivos (diretórios)
  - Controle é feito sobre informações armazenadas sobre cada arquivo, que dizem o tipo de acessibilidade que o mesmo tem (RWX)
- Para o acesso a máquinas, é utilizada mecanismos de autenticação explícita, ou ainda, como no UNIX, fazer uso de arquivos que delimitam o acesso de cada máquina (arquivos .allow e .deny)

Matriz de acessos

- Acessibilidade vista como uma matriz
- Linhas representam domínios e colunas os objetos
- Acesso (i,j) é o conjunto de operações que o processo executando no Domínio i pode chamar no Objeto j

object / domain	F_1	F_2	F_3	printer
D_1	read		read	
D_2				print
D_3		read	execute	
D_4	read write		read write	

Uso da matriz de acessos

- Se um processo no domínio Di tenta realizar uma operação “op” no objeto Oj, então “op” tem que estar na matriz de acesso
- Pode ser estendida para proteção dinâmica
  - Operações de adicionar, deletar direitos de acesso
  - Direitos de acesso especiais
    - Proprietário do Oi
    - Copiar “op” de Oi para Oj
    - Controle – Di pode modificar direitos de acesso do Dj
    - Transferência – mudança do domínio Di para Dj

Uso da matriz de acessos

domain \ object	F_1	F_2	F_3	laser printer	D_1	D_2	D_3	D_4
D_1	read		read			switch		
D_2				print			switch	switch control
D_3		read	execute					
D_4	write		write		switch			

Ameaças de programas

- Cavalo-de-Tróia (Trojan Horse)
  - Programa que aparenta ser benigno, porém contêm funcionalidade escondida
- Porta de Escape (Backdoor)
  - Programador pode deixar uma porta de escape em um programa para não precisar passar pelos controles de segurança
- Stack Overflow e Buffer Overflow
  - Programas mal escritos que proporcionam exploração pelos atacantes

Ameaças ao sistema

- Worms
  - Programas auto-replicáveis com propagação via rede (geralmente com intuito malicioso)
- Vírus
  - Fragmentos de código embutidos em programas legítimos (podendo ter ações destrutivas ou perturbativas)
- Denial of Service
  - Sobrecarregamento do computador alvo evitando-o de realizar trabalho útil

Monitoramento de ameaças

- Deve analisar suspeitos padrões de atividade, por exemplo, tentativas mal sucedidas de autenticação (ataque por força bruta)
- Auditoria – gravar os horários, usuários e todos tipos de acesso aos objetos, útil para verificação e tomadas de melhores medidas de segurança
- Varrer o sistema periodicamente para encontrar buracos na segurança

Monitoramento de ameaças

- Checar:
  - Senhas curtas ou fracas
  - Programas não autorizados em diretórios do sistema
  - Processo rodando a muito tempo
  - Proteções de diretórios ou dados do sistema impróprias
  - Mudanças nos programas do sistema: monitorar valores de checksum

Firewall e IDS

- Firewall
  - Um firewall é colocado entre hosts confiáveis e hosts não confiáveis
  - Tem o papel de restringir o acesso a rede entre estes dois domínios de segurança
- Detecção de intrusos (IDS)
  - Tem o papel de detectar tentativas de intrusão
  - Métodos: através de auditoria e registros (logs)
  - Ex. Tripwire (checa a alteração de arquivos e diretórios)
  - Monitoramento de chamadas de sistema

Dúvidas?