

Aula 08

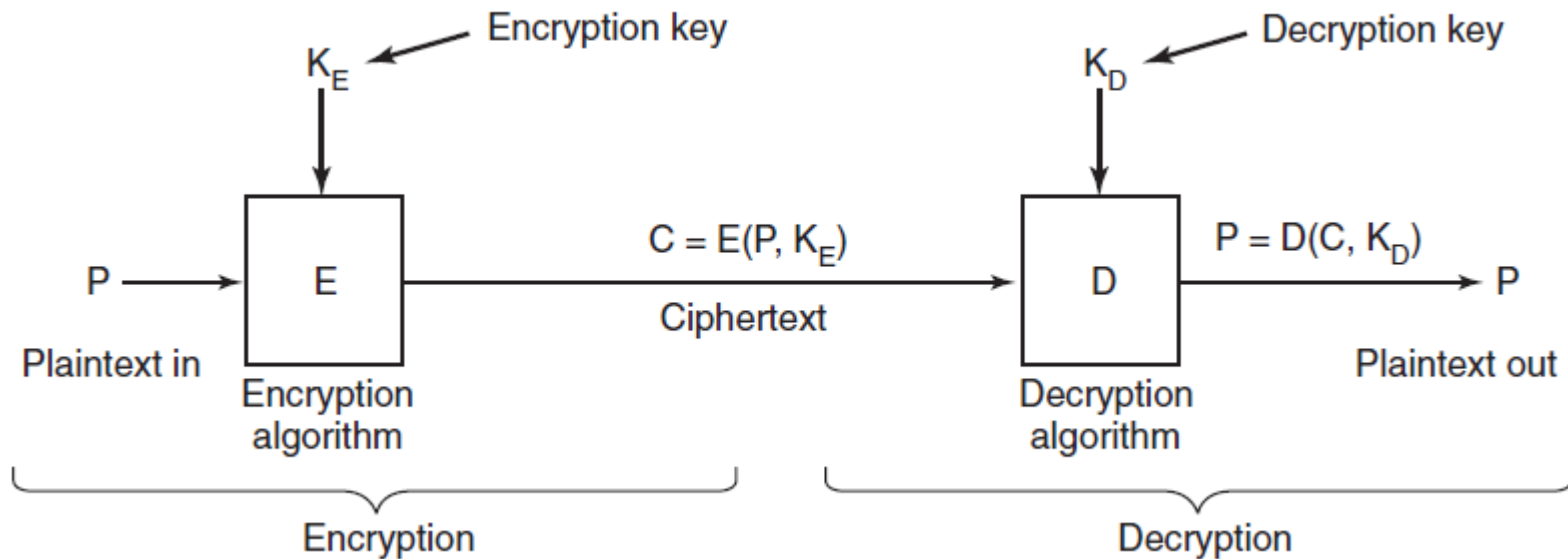
Segurança

Introdução

- Segurança visa:
 - Confidencialidade dos dados
 - Ameaça: Exposição de dados
 - Integridade dos dados
 - Ameaça: Adulteração de dados
 - Disponibilidade do Sistema
 - Recusa de serviço

Criptografia

- Segurança por obscuridade



Criptografia

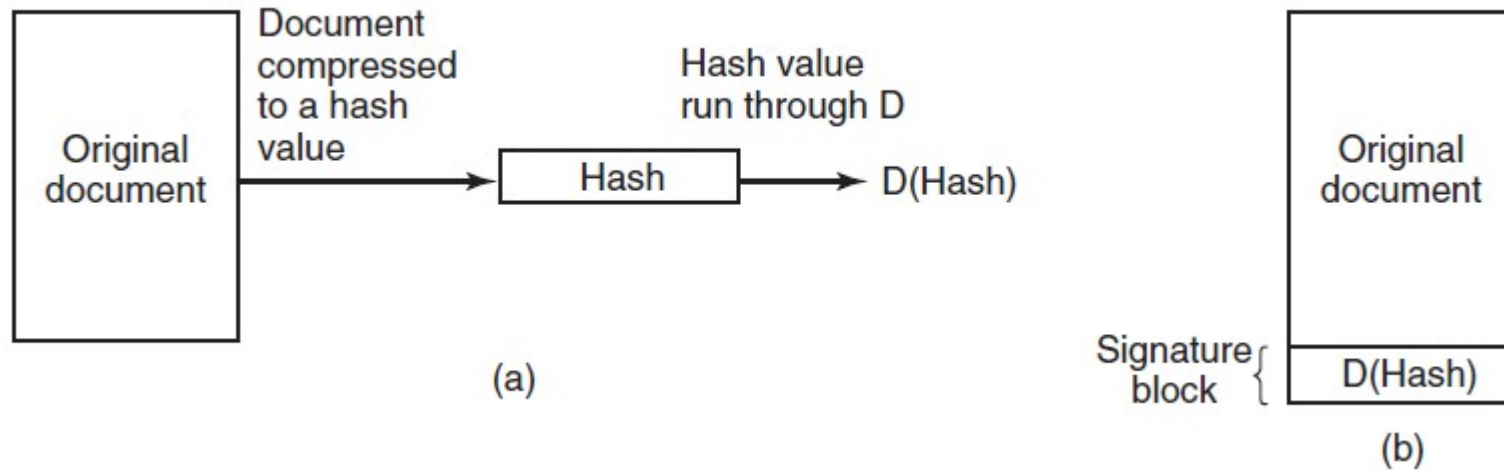
- Por chave secreta
 - Criptografia simétrica
- Relativamente seguros
 - Chaves suficientemente longas

Criptografia

- Por chave pública
 - Criptografia assimétrica
 - $314159265358979 * 314159265358979$
 - Raiz de 3912571506419387090594828508241
 - RSA
 - Multiplicação de grandes números é mais fácil que a fatoração de grandes números

Assinatura Digital

- Garantir integridade
 - MD5 (16 bytes) ou SHA (20 bytes)



Autenticação de Usuário

- Autenticação usando senhas
- Unix
 - Senha → chave criptográfica de um bloco fixo
 - Arquivo de senhas: usuário + bloco criptografado
- Nem superusuário tem acesso as senhas

Autenticação de Usuário

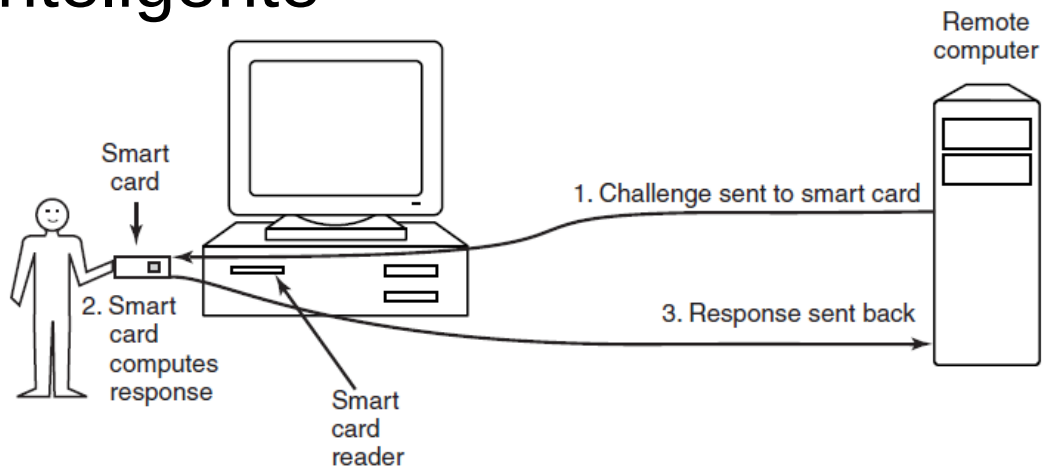
- Senhas de uma vez de uso
 - Livro de senhas
 - A cada acesso, usar a próxima senha do livro

Autenticação de Usuário

- Autenticação por resposta a desafio
 - Quem é a irmã da Mariana?
 - Em qual rua ficava sua escola primária?
 - O que o professor Pitoli ensinava?

Autenticação de Usuário

- Autenticação usando um objeto físico
 - Cartões com valores armazenados
 - Senha criptografada com uma chave conhecida
 - Cartão inteligente



Autenticação de Usuário

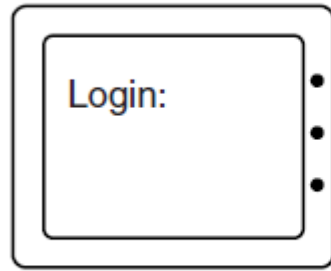
- Biometria
 - Digital
 - Reconhecimento de voz
 - Reconhecimento facial
 - Digitação → **Laboratório**

Ataques de Dentro do Sistema

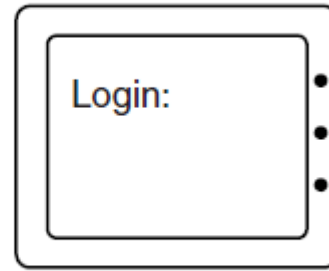
- Cavalo de Troia
 - Programa aparentemente inocente
 - Possui trecho de código malicioso
 - Função inesperada e indesejável

Ataques de Dentro do Sistema

- Conexão impostora (Login Spoofing)
 - Emula tela de login para captura da senha



(a)



(b)

Ataques de Dentro do Sistema

- Bomba lógica
 - Programa alimentado com uma senha por dia
 - Se deixar de receber a senha → executa código maléfico ao sistema

Ataques de Dentro do Sistema

- Alçapões (Back doors)
 - Código inserido no sistema
 - Desviar de verificação ou autenticação

```
C while (TRUE) {  
    printf("login: ");  
    get_string(name);  
    disable_echoing();  
    printf("password: ");  
    get_string(password);  
    enable_echoing();  
    v = check_validity(name, password);  
    if (v) break;  
}  
execute_shell(name);
```

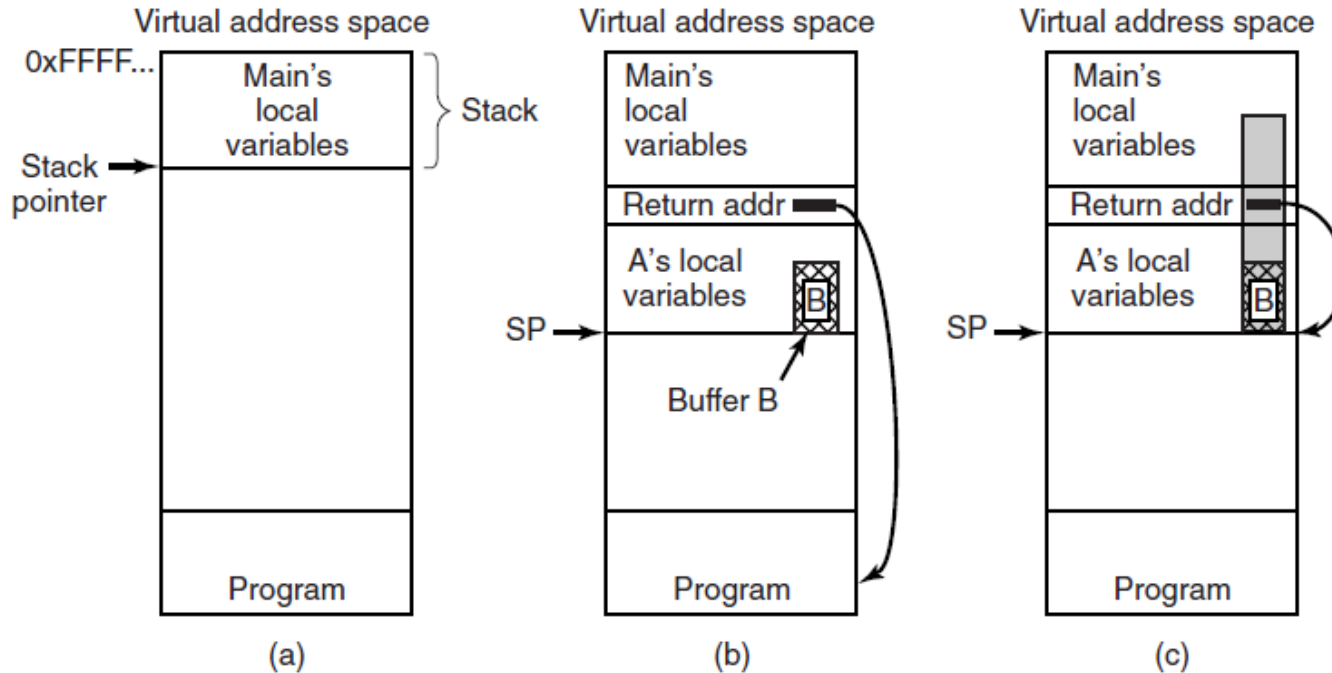
(a)

```
while (TRUE) {  
    printf("login: ");  
    get_string(name);  
    disable_echoing();  
    printf("password: ");  
    get_string(password);  
    enable_echoing();  
    v = check_validity(name, password);  
    if (v || strcmp(name, "zzzzz") == 0) break;  
}  
execute_shell(name);
```

(b)

Ataques de Dentro do Sistema

- Transbordo de buffer (Buffer Overflow ou Stack Overflow)



Ataques de Dentro do Sistema

- Injeção de código (Command Injection)

```
int main(int argc, char *argv[])
{
    char src[100], dst[100], cmd[205] = "cp ";
    printf("Please enter name of source file: ");
    gets(src);
    strcat(cmd, src);
    strcat(cmd, " ");
    printf("Please enter name of destination file: ");
    gets(dst);
    strcat(cmd, dst);
    system(cmd);
}
```

/* declare 3 strings */
/* ask for source file */
/* get input from the keyboard */
/* concatenate src after cp */
/* add a space to the end of cmd */
/* ask for output file name */
/* get input from the keyboard */
/* complete the commands string */
/* execute the cp command */

Ataques de Fora de Sistema

- Vírus
 - Vírus companheiro (executa no lugar de um outro programa)
 - Programa executável

Ataques de Fora de Sistema

- Vírus residente na memória
 - Permanece na memória
 - Captura instruções de desvio de controle
 - Desviando para o próprio código

Ataques de Fora de Sistema

- Vírus de setor de boot
 - Bios lê MBR
 - Vírus substitui código de inicialização

Ataques de Fora de Sistema

- Vírus de drivers de dispositivo
 - Drivers → programas executáveis
- Vírus de Macro
 - Word/excel
- Vírus de código fonte
 - Buscar arquivos .c ou .py por exemplo e faz inserção no código