Segurança na Internet partes 1 & 2

Prof. Elias P. Duarte Jr., *Ph.D.*
DInfo – UFPR
Itaipu 11/07/2003

Roteiro

- Por que preocupar com segurança?
- Ataques & Vulnerabilidades
- Medidas de segurança
- Sigilo & Privacidade, Integridade, Autenticidade, Disponibilidade
- Criptografia: chaves secreta, chave pública resumo digital (*hash*)
- Panorama de ferramentas de segurança

Uma Necessidade

- Perigo!
- As redes de empresas e organizações têm sido atacadas constantemente
  - Roubos: recursos, informação
  - Vandalismo
  - Ignorância
- Os ataques vêm de dentro e de fora
- Além de vulnerabilidades físicas e naturais

Problemas Diversos...

- Um erro de software alterou as contas de um banco de tal forma que foi necessário pedir um empréstimo de bilhões de dólares até a situação se resolver
- Os vírus que alteram a taxa de refrescamento de um monitor de vídeo podem levar a uma explosão
- Sites da CIA (EUA) e de governos ao redor do mundo já foram vandalizados

O "Verme"

- Na Internet, o alerta começou com o *worm*, de 1988
- O programa afetou 6000 computadores
  - Após se instalar em uma máquina, o verme se reproduzia, consumindo recursos locais, e se expandindo para máquinas vizinhas
  - Alvo: servidores BSD-UNIX fingerd, sendmail
- Mostrou que a rede, na época acadêmica, não era segura

O que é segurança?

- O objetivo é proteger o computador, a rede e tudo a eles associado
- Os *invasores* e *impostores* que querem obter informações ou bens ou auto-afirmação; NÃO são as únicas ameaças
- Medidas de segurança: sigilo & privacidade, autenticidade, integridade e disponibilidade

Sigilo & Privacidade

- Somente pessoas & processos *autorizados* devem ter acesso aos diversos recursos do computador e da rede
- Deve ser possível manter e transmitir *informações secretas*
- É necessário controlar os níveis de acesso e o que cada um pode fazer
- Criptografia é a chave do sucesso

Integridade & Autenticidade

- As informações armazenadas e em trânsito não podem ser corrompidas, alteradas de forma acidental ou maliciosa
- Deve ser garantida a integridade das informações armazenadas e transmitidas
- Devem haver meios de pessoas & processos garantirem a autenticidade de sua identidade

Autorização & Não-Repúdio

- Um usuário autenticado deve ter associado um esquema que identifica os tipos de acesso para os quais está autorizado
- Níveis de autorização diversos podem ser definidos: leitura, execução, escrita
- Um usuário que realizou uma ação não pode negar que tal ação tenha sido realizada

Disponibilidade

- Também é parte da segurança: a rede deve funcionar ininterruptamente
- Capacidade de recuperação imediata após desastres e ataques
- Impedir que usuários, por ignorância ou malícia, impeçam o trabalho de outros esgotando os recursos disponíveis

Definindo Termos

- Vulnerabilidades: pontos do sistema suscetíveis ao ataque
- Ameaça: um perigo potencial, pode ser pessoa, processo, informação, “coisa” ou evento
- Medidas de segurança: visam proteger o sistema

Vulnerabilidades

- Comunicação - mensagens podem ser forjadas, interceptadas, desviadas, repetidas
- Falhas e *armadilhas secretas* em hardware & software
- Vulnerabilidades Físicas (fio da rede...)
- Naturais (incêndio...)
- A mais difícil: *pessoas*, especialmente os administradores do sistema

Quais os componentes de um sistema seguro?

- Controle de acesso ao sistema
- Quem acessou fez o que? (*logging*)
- Controle de permissões, acesso de pessoas e programas às informações armazenadas
- Administração de segurança: incluindo monitoramento contínuo, treinamento de usuários

Controlando o Acesso ao Sistema

- Quem pode logar no sistema?
- Indentificação + Autenticação
- Métodos de Autenticação incluem:
  - passwords
  - chaves, cartões magnéticos, smart cards
  - impressão digital, reconhecimento de voz, retina, assinatura, padrões de digitação

Passwords

Passwords e seus riscos...

"*A password should be like a toothbrush. Use it everyday; change it regularly; and DON'T share it with friends*"

- A alternativa de autenticação mais comum
- Para serem efetivas, é necessário:
  - escolher boas passwords
  - elas devem ser protegidas
- Sempre sujeitas a um ataque de força bruta
  - o invasor tenta todas as combinações, uma de cada vez

Ataques a Passwords

- Existem 2.800.000.000.000 combinações possíveis de 8 caracteres
- Levaria 45 anos para um computador checar todas as possibilidades, se ele checasse 1 milhão de alternativas por segundo
- O problema é que muitos usuários não escolhem boas passwords...

Passwords Fáceis de Descobrir

- Estudos mostram que grande quantidade de usuários escolhem passwords extremamente simples de descobrir
- Os invasores podem usar um dicionário de passwords comuns
- Entretanto se a password for bem escolhida, fica muito difícil ela ser descoberta, com ou sem um dicionário

Dicas para Escolher uma Boa Password

- Não selecionar palavras da língua inglesa, portuguesa, ...
- Misturar caracteres alfabéticos com numéricos e especiais (&%@...)
- Misturar letras maiúsculas e minúsculas
- Melhor escolher passwords mais longas - mínimo de 8 caracteres
- Escolha passwords diferentes para sistemas diferentes
- Não escreva sua password num papel ou arquivo!

Ainda sobre Passwords:

- Uma boa alternativa é escolher as iniciais de uma frase que faça algum sentido F@$Sntd0
- Não mandar a password por e-mail
- Qualquer suspeita: mude a password imediatamente
- O sistema deve incluir providências para diminuir a probabilidade de sucesso de ataque

Armazenando a Password

- Em geral, os sistemas armazenam passwords criptografadas
- Não é necessário DES-criptografar, usam algoritmos para "*one way encription*"
- O arquivo de passwords deve ter a maior restrição de acesso que o sistema puder oferecer (*shadow password files*)

Programas Perigosos

Vírus

- Fragmento de código que invade um programa maior, que faz cópias de si próprio, e invade outros programas
- Todos os dias novos vírus são criados, descobertos...

Vírus: Estrutura

- `Trocar uma instrução numa posição x, por um jump para a posição y`
- `O código do vírus começa nesta posição`
- `A instrução originalmente na posição x deve seguir o código do vírus, com jump x+1`

Vírus: Antídotos

- Como podemos descobrir a existência de um vírus?
- Os antídotos mais comuns conhecem o código dos vírus, e checam todo o disco rígido procurando padrões em todos os arquivos
- É necessário atualizar tais checadores constantemente, pois novos vírus surgem a todo momento

Para Driblar os Antídotos...

- Foram criados os vírus *polimórficos*
- A cada vez que tais vírus criam cópias de si próprios, eles alteram a ordem de suas instruções, ou alteram algumas instruções para outras com funcionalidade similar
- Existem antídotos para estes também, mas a busca de padrões tem que ser mais sofisticada...

Para Driblar os Novos Vírus

- Foram criados antídotos que tiram "fotografias" dos diretórios e, tomando como base parâmetros como o tamanho de arquivos podem descobrir contaminação
- Aí surgiram os vírus que comprimem parte do programa, para que o tamanho total permaneça inalterado!
- Outros antídotos checam a autenticidade de cada arquivo

Trojan Horses

- Disfarce para programas invasores
- O usuário pensa que se trata de um programa, mas a verdade é diferente
- Mais comum: para capturar *passwords*
- Outras classificações de pestes incluem: bactérias (vírus que é um programa independente), bombas lógicas (vírus com data-hora para atacar, etc...

Medidas Preventivas

- Não executar programas vindos de fontes suspeitas (cartões, email-anônimo, etc...)
- Executar checadores periodicamente
- Fazer backups periódicos
- Limitar ambientes (jogos, trabalho, ...)
- Não inicializar computador com diskette de origem desconhecida
- Se os sistemas operacionais fossem projetados de forma mais defensiva...

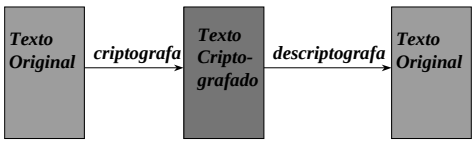
Introdução à Criptografia

Conteúdo

- Criptografia: a base de TODA a segurança
- O que é criptografia?
- Substituição & Transposição
- Algoritmos de Chave Secreta
- Algoritmos de Chave Pública
- Algoritmos de Resumo Digital (*hash*)
- Assinaturas Digitais

O Que É Criptografia?

- A palavra vem do grego: segredo + escrita
- Arte da escrita secreta
- Esquema geral:



Criptografia: def.

- O texto criptografado é aparentemente uma sequência de caracteres aleátorios, sem nenhum sentido
- Só quem conhece o método e a *chave adequada* pode descriptografar
- Desta forma, a informação flui entre emissor e receptor sem que ninguém mais possa entender o conteúdo

Em outras palavras...

- Seja T o texto original da mensagem;
- Seja $C_k( )$ o algoritmo de critpografia, parametrizado pela chave k
- $C_k(T)$ é então o texto criptografado
- Seja $D_k( )$ o algoritmo para descriptografar, ele usa a mesma chave k; então:

$$T = Dk(Ck(T))$$

Usos da Criptografia

- Além de permitir a manutenção e comunicação de informações *sigilo*sas,
- se usa criptografia para garantir:
  - A *integridade* de uma mensagem
  - A *autenticidade* de um usuário (ou processo)

Algoritmos & Chaves

- Criptografia envolve um algoritmo e um valor secreto - a *chave*
- O algoritmo é muitas vezes público
- Assim, podemos dizer que os algoritmos são parametrizados pela chave secreta
- Não é trivial obter um *bom* algoritmo de criptografia

Fácil & Difícil

- Um algoritmo de criptografia deve ser razoavelmente eficiente para que seus usuários legítimos possam usá-lo
- Por outro lado, para os criminosos, deve ser computacionalmente inviável descobrir o texto original a partir do criptografado
- Nem só criminosos: cripto-analistas

"Computacionalmente Difícil"

- É ***sempre*** possível tentar testar todas as chaves até encontrar a correta
- Entretanto, se fazê-lo demoraria 10 milhões de anos usando todos os computadores existentes na Terra, temos um bom algoritmo de criptografia
- O número de bits da chave é um fator importante neste sentido

Comprimento da Chave

- 1 dígito => 10 possibilidades
- 2 dígitos => 100 possibilidades
- 3 dígitos => 1000 possibilidades
- 6 dígitos => 1000000 possibilidades
- Possibilidades crescem exponencialmente
- Para e-mail seguro: chaves de 64 bits OK
- Para aplicações militares: no mínimo 256 bits

Algoritmos Publicados

- Uma boa estratégia para testar um algoritmo é publicá-lo
- Diversos cripto-analistas de todo o mundo vão testar o algoritmo de graça
- Por outro lado, se além da chave, o algoritmo também for secreto, pode ficar mais difícil quebrar um código
- Entretanto: é difícil manter segredo sobre um algoritmo muito usado

Algoritmos Secretos

- Hoje em dia, algoritmos de criptografia militares ainda são secretos
- Os sistemas comerciais usam algoritmos publicados - mas são bons algoritmos

Substituição & Transposição

- ***Todos*** os algoritmos de criptografia são baseados nestes dois princípios
- Estes métodos têm sido usados, na sua forma mais simples, desde a antiguidade
- São também encontrados em revistas de passatempo e jornais...

Substituição

- Consiste em *substituir* cada letra ou grupo de letras por outra letra ou grupo
- Considere o mapeamento A->s, M->A, E->B, I->I, X->O
- **AMEIXA**
- Pode substituir palavras, sílabas também
- O Método de César, usado pelo imperador romano é um exemplo típico

Substituição

- Consiste em *substituir* cada letra ou grupo de letras por outra letra ou grupo
- Considere o mapeamento A->s, M->A, E->B, I->I, X->O
- **SABIOS**
- Pode substituir palavras, sílabas também
- O Método de César, usado pelo imperador romano é um exemplo típico

O Método de César

- Atribuído ao imperador romano Júlio César
- É uma substituição de letras, a -> D, b -> E, c-> F,....., z -> C
- Por exemplo: **APRENDER**
- Há uma *chave*, que é o deslocamento, no caso acima k=3
- Para descriptografar é necessário saber o deslocamento, isto é, a chave

O Método de César

- Atribuído ao imperador romano Júlio César
- É uma substituição de letras, a -> D, b -> E, c-> F,....., z -> C
- Por exemplo: **DSUHQGHU**
- Há uma *chave*, que é o deslocamento, no caso acima k=3
- Para descriptografar é necessário saber o deslocamento

Será Difícil Quebrar o Método?

- Como fazer para descobrir a chave usada?
- Lembre-se: sempre é possível tentar testar todas as possibilidades
- Neste caso, são quantas possibilidades?
- Resposta: 26
- Tente quebrar o código do texto no qual aparece: **ZLNBYHUJH**
- Qual a chave usada?

Será Difícil Quebrar o Método?

- Como fazer para descobrir a chave usada?
- Lembre-se: sempre é possível tentar testar todas as possibilidades
- Neste caso, são quantas possibilidades?
- Resposta: 26
- Tente quebrar o código do texto no qual aparece: **SEGURANÇA**
- Qual a chave usada? K=7

Substituição Monoalfabética

- Para melhorar o método da substituição
- Idéia: substituir cada letra por outra aleatória
- O que é a chave neste caso?
- A sequência de 26 caracteres do mapeamento

Subst. Monoalfabética: Ex.:

- Podemos fazer o seguinte mapeamento:
- ABCDEFGHIJKLMNOPQRSTUVWXYZ
- KRMZWATDCEVJFGBHILNOPQSUXY
- A segunda sequência é a chave
- Neste caso, quantas possibilidades devem ser testadas no total?
- Resposta: 26! ~ $4x10^{26}$
- Testando uma possibilidade por micro-segundo: 10^{13} anos

Quebrando a Substituição Monoalfabética

- O que será a palavra abaixo?
- **LWZWN**
- Solução: **REDES**
- Busca de palavras prováveis, e *padrões* prováveis
- Exemplo: em inglês as letras mais comuns são *e, t, o, a, n, i, ...*, nesta ordem

Propriedades Estatísticas das Linguagens Naturais

- Deve-se começar procurando a letra mais comum, por exemplo ‘‘e’’ (em inglês)
- Depois pode-se procurar a segunda letra mais comum “t”
- Se houverem muitos “tXe”, provavelmente X -> h, e então “thZt” Z-> a
- A busca de palavras prováveis em um documento específico é outra boa estratégia

Transposição

- Neste método, as letras são *reordenadas*, *trocadas de lugar*, mas não são substituídas
- Assim, a transformação seguinte pode ocorrer **AMEIXA**
- Trocamos as letras da palavra de lugar, seguindo um algoritmo que permite a volta
- A chave neste caso foi a palavra *CHAVES*

Transposição

- Neste método, as letras são *reordenadas*, *trocadas de lugar*, mas não são substituídas
- Assim, a transformação seguinte pode ocorrer **EAXMAI**
- Trocamos as letras da palavra de lugar, seguindo um algoritmo que permite a volta
- A chave neste caso foi a palavra *CHAVES*

Transposição por Colunas

- Nesta transposição fizemos:

C	H	A	V	E	S
2	4	1	6	3	5
A	M	E	I	X	A

Transposição por Colunas

- Para descriptografar:

C	H	A	V	E	S
2	4	1	6	3	5
E	A	X	M	A	I

Transposição por Colunas - cont.

- A chave não pode conter letras repetidas
- Usando-se a chave, as colunas são numeradas pela ordem léxica das letras da chave; a letra mais próxima do início do alfabeto = 1, etc.
- Para descriptografar, basta fazer um mapeamento de posições

Transposição - Descriptografia

- Assim, no exemplo anterior, "X'' está agora na terceira posição, aquela da letra A-1, mas a terceira letra é a letra E, que está na quinta posição, é a posição correta de "X"

1	2	3	4	5	6
C	H	A	V	E	S
2	4	1	6	3	5
E	A	X	M	A	I

Transposição - Exercício

- Criptografar e Descriptografar a palavra SEGURO com a chave CHAVES

1	2	3	4	5	6
C	H	A	V	E	S
2	4	1	6	3	5
S	E	G	U	R	O

- Lembre-se a letra que está na posição da 1a letra da chave deve ir para a posição da 3a letra

1	2	3	4	5	6
C	H	A	V	E	S
2	4	1	6	3	5
G	S	R	E	O	U

Transposição de Textos

- No caso de um texto, procedemos da seguinte forma:

1	2	3	4	5	6
C	H	A	V	E	S
2	4	1	6	3	5
E	S	T	E	É	U
M	E	X	E	M	P
L	O	D	E	T	R
A	N	S	P	O	S
I	Ç	Ã	O		

Transposição de Textos - cont.

- O texto
- ESTEÉUMEXEMPLODETRANSPOSIÇÃO
- Se transforma em
- TXDSÃEMLAIEMTOSEONÇUPRSEEEPO
- Descriptografar como exercício

Quebrando a Transposição

- Usando as propriedades estatísticas das linguagens naturais -> frequencia de *letras*
- Depois é necessario descobrir quantas colunas existem -> onde é que as letras de uma palavra provável se encontram?

S E G
U R O

S E
GU
RO

Concluindo a Transposição

- Depois de descobrir o número de colunas, é necessário *ordená-las*
- Para uma chave pequena, não é difícil tentar todas as possibilidades
- Outro método de transposição: criptografa um bloco fixo de caracteres, e tem a ordem
- Exemplo: 4 caracteres, ordem = 3241

Um Método Poderoso
One-Time Pad

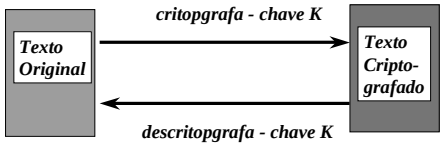
- Basta que a chave seja uma sequência totalmente aleatória de bits do tamanho exato da mensagem a ser transmitida
- É feito um XOR (ou-exclusivo) da mensagem com a chave
- Por exemplo: 1010 xor 0011 = 1001
- Neste caso todo bit é aleatório!
- Problemas: transmitir msg+*nova* chave

Os Três Tipos de Funções Criptográficas

- *Funções de Chave Secreta*
- *Funções de Chave Pública*
- *Funções Hash*

Algoritmos de Chave Secreta

- Envolve o uso de uma única chave
- O algoritmo para descriptografar é o reverso do algoritmo para criptografar



Usos de Criptografia com Chave Secreta

- Para manter o *sigilo* de informações transferidas em canal inseguro
- Para armazenar informações *sigilosas*
  - Cuidado! Se você esquecer a chave as informações estarão irremediavelmente perdidas!
- Checagem de *Integridade*
  - Checksums secretos

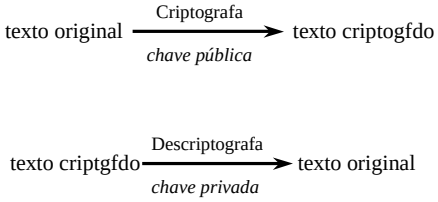
Algoritmos Criptografia Chave Secreta

- Existem várias soluções publicadas: DES, AES, BlowFish, IDEA...
- Estes algoritmos aplicam vários passos de substituições e transposições do texto, parametrizadas pela chave secreta

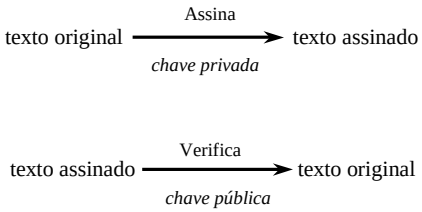
Algoritmos de Chave Pública

- Chamados assimétricos, enquanto os algoritmos de chave secreta são simétricos
- Todos os usuários tem *DUAS* chaves:
  - Chave Pública, conhecida por todos
  - Chave Privada, que não é distribuída
- O texto é criptografado com uma chave e descriptografado com a outra!

Criptografia com Chave Pública



Criptografia com Chave Pública *Assinando Mensagens*



Usos da Criptografia com Chave Pública

- Para armazenar informações sigilosas: deve-se criptografar com a chave *pública* (não com a privada)
- Para transferir mensagens sigilosas -> emissor criptografa com a chave pública do receptor
- Autenticação: desafio deve ser criptografado com a chave pública
- Assinatura de mensagens

Algoritmos de Hash

- Não usam chave alguma!
- Os algoritmos em si *não* são secretos
- Mas são usados em segurança!!
- É uma função matemática que
  - recebe uma entrada de tamanho arbitrário
  - produz um número (pequeno) como saída
- É possível que várias mensagens gerem o mesmo hash, mas deve ser *difícil* encontrar tal par

Algoritmos de Hash - Usos

- Armazenamento de passwords: o sistema guarda um hash
- Geração de checksums secretos
- Antídotos de vírus
- Os algoritmos de hash são mais eficientes que os algoritmos de chave pública

Assinaturas Digitais

- O RG (carteira de identidade) da Internet
- Quando voce faz uma compra pela rede, como pode se certificar da identidade do servidor?
- Cada “entidade” que tem uma assinatura digital deve criar duas chaves:
  - Chave Privada: usada para assinar os dados
  - Chave Pública: usada para verificar a assinatura

Cartórios Digitais

- *Public Key Infrastructure*
- Como é que o usuário vai ter certeza de quem são as chaves públicas?
- Uma autoridade independente, idônea, deve emitir um certificado de autenticidade
- Como funciona?
- A autoridade assina o certificado digital do usuário

Ataques & Quebra de Códigos

- *A partir de Texto Criptografado*
  - é fácil de obter texto criptografado
  - o objetivo é descobrir o texto original
  - quando é que se sabe que se achou tal texto?
- *A partir de <Txto Original, Txto Criptgfd>*
  - um espião conseguiu obter um par
  - em alguns casos (subst. monoalf.) tudo perdido!
- *Texto Escolhido pelo Hacker*

Segurança em Todos os Níveis

Segurança nas Camadas OSI

- Segurança Física
- Segurança de Enlace
- Segurança a Nível de Rede:
  - Firewalls
  - IPsec
- Segurança de Transporte: *Secure Socket Layer*
- Segurança de Aplicação

Aspectos Legais & Importação

- Governos consideram criptografia uma tecnologia perigosa
- Nos EUA, diversas tecnologias de segurança são patenteadas e...
- existem restrições quanto à exportação de diversos produtos (criptg. = munição)
- Leis específicas têm sido desenvolvidas, desde copyright até crimes digitais

Conclusões

- Segurança: uma necessidade
- Sigilo & Privacidade, Autenticidade, Integridade e Disponibilidade
- Vulnerabilidades, Ataques
- Programas perigosos; passwords perigosas
- Criptografia: os três tipos
- Aspectos Legais