Aula 20

Segurança

Segurança X Proteção

- Segurança:
  - Problema geral;
  - O que proteger? De quem?
- Proteção:
  - Mecanismos específicos implementados para proteger informação

- Segurança: o quê?
- Proteção: como?

Segurança – Causas de Perdas de Dados

- Catástrofes naturais
- Erros de hardware/software
- Erros humanos
- Erros **bizantinos** (!) - invasores.

Backup resolve os três primeiros problemas.
- Por que não o último?

Segurança - Invasores

Podem ser:

- passivos: leitura não autorizada
- ativos: modificação nos dados

Exemplos:

- invasores casuais, não técnicos (passivos);
- invasores internos ou externos, determinados, tecnicamente qualificados – hackers;
- ladrões;
- espionagem (militar ou comercial);
- violações de privacidade.

Segurança – Espionagem Comercial: Intel

Nos centros de desenvolvimento da Intel:

- Todo acesso de **fora** do prédio é negado;
- Todo acesso de **dentro** do prédio é logado:
  - ftp, telnet, mail
- Toda comunicação com o mundo exterior é feita através de um *firewall*.
- **Todo** funcionário tem seus pertences revistados na saída do prédio

Resolve o problema?

Segurança – Privacidade

- Seu chefe pode querer monitorar o que você faz!
  - Pessoas já foram demitidas por envio "inapropriado" de e-mail
  - Quem garante que o CRC não está te espionando?
- Operações com cartões de crédito, visitas a websites etc são:
  - logados
  - catalogados
  - vendidos!

Segurança – Privacidade

- Exemplo **sério**:
  - uma empresa de segurança pode conseguir sua ficha médica;
  - e baseado nisso cancelar seu seguro;
  - você pode até perder o emprego!
- Outro exemplo:
  - você cadastra preferências, fotos, gostos, amigos, onde estuda e onde trabalha Orkut?
  - como esta informação pode ser usada?

SOBE

Transplantes
No primeiro trimestre, o número de doadores de órgãos no Brasil subiu 28% em relação ao mesmo período de 2009

Topete
Foi adotado em versão meio aloirada pela candidata petista Dilma Rousseff

Tiago Splitter
O brasileiro foi eleito o melhor jogador de basquete em atividade na Espanha, que promove o segundo campeonato mais rico do mundo

DESCE

Paradinha
Serão punidos com o cartão amarelo os jogadores que baterem pênalti exagerando o truque inventado por Pelé para enganar os goleiros

Paquistão
O país de maioria muçulmana bloqueou o YouTube, o Facebook e restringiu a Wikipédia, por causa do "conteúdo sacrílego" desses sites

Google
Investigado por invasão de privacidade na Alemanha, admitiu ter colhido ilegalmente informações particulares de usuários

FOLHAONLINE
www.folha.com.br
Quinta-feira, 28 de janeiro de 2010Quinta-feira, 28 de janeiro de 2010

28/01/2010 - 14h15

Empresa lança serviço anônimo de busca

da **Reuters**, em Londres

A companhia de buscas on-line Startpage lançou um serviço que permite a usuários preocupados com sua privacidade executar pesquisas na web e clicar nas páginas de resultados sem que sejam identificados, rastreados ou registrados.

Ao contrário dos serviços de busca convencionais, que recolhem informações comercialmente valiosas sobre o comportamento dos usuários, a Startpage (www.startpage.com), uma empresa de capital fechado, se concentra na privacidade desde 2005.

"O acontecimento que me despertou surgiu no ano passado", disse Katherine Albrecht, que cuida de relações com a mídia e do marketing da Startpage nos Estados Unidos.

Ela diz ter percebido que o Google havia instalado um programa que monitorava os usuários que digitavam termos de busca indicativos de que estivessem sofrendo de gripe e que estava divulgando essas informações para o Centro de Controle de Doenças dos EUA.

O presidente-executivo do Google, que domina o mercado mundial de buscas, irritou os críticos com declarações em uma entrevista de TV, no mês passado. "Se existe alguma coisa em sua vida que você deseja que ninguém mais saiba, talvez o melhor seja que você não a faça", disse Eric Schmidt, em entrevista ao canal de notícias CNBC.

The New York Times

OP-ED CONTRIBUTOR

Search, but You May Not Find

By ADAM RAFF
Published: December 27, 2009

London

Related

Times Topics: Google

Room for Debate: Wh

One way that Google exploits this control is by imposing covert "penalties" that can strike legitimate and useful Web sites, removing them entirely from its search results or placing them so far down the rankings that they will in all likelihood never be found. For three years, my company's vertical search and price-comparison site, Foundem, was effectively "disappeared" from the Internet in this way.

Another way that Google exploits its control is through preferential placement. With the introduction in 2007 of what it calls "universal search," Google began promoting its own services at or near the top of its search results, bypassing the algorithms it uses to rank the services of others. Google now favors its own price-comparison results for product queries, its own map results for geographic queries, its own news results for topical queries, and its own YouTube results for video queries. And Google's stated plans for universal search make it clear that this is only the beginning.

Apple Moves to Tighten Control of App Store

By CLAIRE CAIN MILLER and MIGUEL HELFT
Published: February 1, 2011

SAN FRANCISCO — Apple is further tightening its control of the App Store.

Some application developers, including Sony, say Apple has told them they can no longer sell e-books within their apps unless the transactions go through Apple's system. Apple rejected Sony's iPhone application, which would have let people buy and read e-books from the Sony Reader Store.

> Apple is now saying the app makers must allow those purchases to happen within the app, not in a separate browser window, with Apple getting its standard 30 percent cut of the transaction. At the moment this applies only to e-book purchases.

Segurança – Furos de Segurança Famosos

- UNIX:
  - `lpr` com opção de remover o arquivo:
    - `lpr -r /etc/passwd`

  – link arquivo `core` com `/etc/passwd` força um core dump de um programa SETUID:
    - programa repõe passwd com o novo core
    - invasor tem novo arquivo passwd

Segurança – Furos de Segurança Famosos

- UNIX:
  - `mkdir foo`:
    - mkdir é SETUID cujo dono é root
    - mkdir := cria i-node; chown usuário i-node
    - pode-se remover o i-node **antes** do chown e link o i-node com /etc/passwd
    - usuário passa a ser dono de /etc/passwd!

Segurança – Furos de Segurança Famosos

- MULTICS:
  - Segurança adequada para time-sharing
  - Segurança não-existente para batch.

  Exemplo de (mau) uso:
  - Modifica-se um programa de uso comum para obter informações: p.ex. escreve um programa que imprime “login:” e coleciona senhas.
  - Usa batch para instalar o programa em `/bin`
  - Todo usuário agora usa o programa mau.
  - Exemplo de **cavalo de Tróia**.

Segurança – Furos de Segurança Famosos

- TENEX(DEC-10):
  - Usava paginação e permitia que page faults fossem tratados pelo usuário;
  - Usava senhas para proteger o acesso. Checava um caracter por vez e parava quando o primeiro não batesse;
  - Truque – alinhar a senha de tal forma que o **segundo** caracter estivesse em outra página:
    - Submete a senha AA. Se ocorrer um page fault, é porque o primeiro caracter da senha é A.
    - Após descobrir o primeiro caracter, realinha a senha: o **terceiro** caracter causa page fault;
    - Possível quebrar a senha com **128n** ao invés de **128^n** tentativas.

Segurança – Furos de Segurança Famosos

- Internet worm:
  - worm: verme
  - worm: self replicating program
  - Criado por Robert Tappan Morris Jr em 02/11/1988
  - Consiste de dois programas:
    - um bootstrap i1.c (99 linhas de código)
    - o worm

Segurança – Internet Worm

- Infecção pelo Internet Worm:
  - O bootstrap para a “vítima” e lá é compilado e executado.
  - O programa contactava o computador de origem e transferia o worm.
  - A partir daí o worm tentava contactar outras máquinas e infectá-las.
  - O worm também quebrava senhas para acessar máquinas que usuários podiam acessar.
  - O worm checava para ver se já estava instalado no computador, só se replicava uma vez a cada 7.
    - foi muito!
  - O worm **não** causava danos, só se multiplicava.

Segurança – Internet Worm

- O acesso às máquinas era feito:
  - Executar **remote shell**. Surpreendentemente fácil, muitas máquinas simplesmente aceitam!
  - **finger daemon:**
    - finger é chamado com um string especial de 536 bytes.
    - o tamanho do string causa um overflow do daemon, que **não o checava!** Excedente da string era escrito na **pilha** do daemon;
    - isto causava um **return** para **dentro** da string, que então executava `/bin/sh`.
  - sendmail:
    - um bug do programa permitia um envio de uma cópia do bootstrap e a sua execução.

Segurança – Internet Worm

Fim da história:

- foi feito um **teste** com o worm dentro de Cornell. Por causa de um erro na sua configuração ele se espalhou.
- **Parou a Internet!**
- O “criminoso” foi condenado:
  - US$ 10.000 de multa
  - 400h de trabalho comunitário
  - US$ 150.000 de advogados

Por quê???

Segurança – Internet Worm

- O problema foi o “Jr.”
- O pai do Robert é um dos maiores especialistas em segurança da NSA
- Diz a lenda que Robert queria mostrar ao pai que era bom!!!

Segurança – Como atacar SOs em 8 fáceis lições

1. Requisite páginas de memória, disco, etc. Muitos SOs não as apagam quando de sua desalocação.

2. Tente syscalls ilegais, ou legais com parâmetros ilegais, etc.: p.ex. no Mach: task_by_pid(-1).

3. CTRL+ALT+DEL ou CTRL+C durante login. Pode matar o programa que checa senha.

4. Tente mudar as estruturas de dados do SO mantidas no espaço do usuário

Segurança – Como atacar SOs em 8 fáceis lições

5. Escreva um programa “login:”
6. Procure em manuais a frase “Do not do X”. Just do it.
7. Convença o CRC a baixar a guarda. Invente desculpas, minta, etc.
8. Compre o pessoal técnico.

Notem como é importante pagar bem o pessoal técnico!!!!

Segurança – Vírus

- Diferente do worm porque é adicionado a outro programa
  - normalmente com más intenções
- Difícil de programar:
  - tem que ser pequeno, indetectável, eficiente
- Perigoso:
  - porque o usuário quer rodar o programa
- Melhor proteção:
  - Prevenção
- Comum em DOS/Windows. Por quê?

Um tormento recente: Worms + Vírus + Email

- Episódios Nimda e derivativos – 2001 – prova-de-conceito de uma forma cruzada de propagação:
  - Servidor MSoft contaminado:
    - Um worm ataca outros servidores e os contamina
    - Servidor ataca outros por meio de compartilhamento
    - Usuários que acessarem páginas web serão contaminados
  - Cliente Msoft contaminado:
    - Ataca servidores próximos por meio de compartilhamemento
    - Acata outros clientes por meio de email

Segurança – Princípios Seguros de Projeto

- Fazer um sistema aberto;
- Não dar acesso por default;
- Checar sempre pela permissão, p.ex. arquivo aberto por muito tempo;
- Dar o mínimo de privilégio possível
- Mecanismos de proteção devem ser simples, uniformes, e construídos nos mais baixos níveis possíveis.
  - Segurança não pode ser adicionada *a posteriori*.
- Esquema deve ser aceitável pelos usuários.