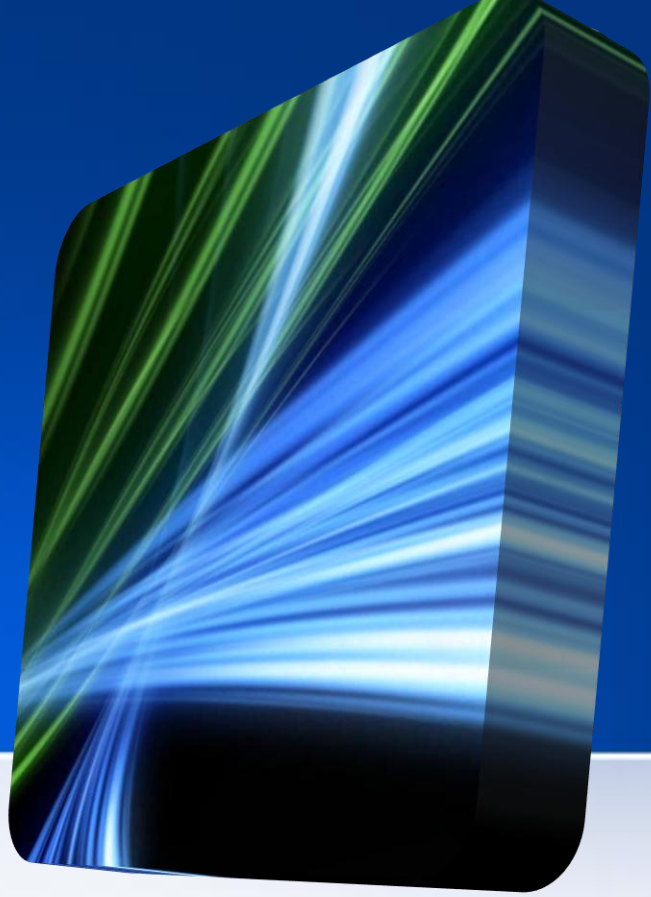
Aspectos Legais do Software



Introdução à Ciência da Computação

Professor Rodrigo Mafort

PURO
PÓLO UNIVERSITÁRIO DE RIO DAS OSTRAS

Avisos

1. O primeiro dia de apresentação dos seminários será 21/05/2012 (próxima segunda-feira)
2. Cada grupo terá direito a 20 minutos
3. A ordem da apresentação de um determinado dia será sorteada no início da mesma aula
4. Todos devem estar presentes, pois a avaliação conterá perguntas sobre as apresentações.

Importância da Informação

- A informação é a base da tomada de decisões. Desde as mais simples:
  - Vou levar guarda-chuva ou não?
  - Devo levar casaco?

  Até as mais complexas:
  - Qual é o melhor investimento?
  - Qual ação devo comprar?
- Devido a sua importância, cada vez mais tem se discutido a sua segurança.

Hacker

- Quando se fala em segurança, logo vem a mente o nome “HACKER”.
- Mas o que e quem são hackers?
  - Hackers são pessoas com enorme interesse e conhecimento no funcionamento interno de algum sistema.
  - Tem excepcional conhecimento de programação e de sistemas operacionais.
  - Não se dedicam a destruir, danificar ou roubar dados e sistemas.
  - Seu objetivo é descobrir falhas em sistemas, para depois publicá-las e corrigi-las.
  - Normalmente tem entre 16 e 24 anos.
  - Geralmente se tornam grandes especialistas na área de segurança da informação.

Cracker

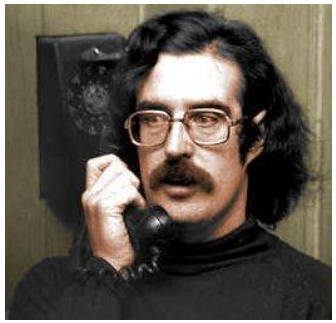
- E quando se ouve a notícia de que um hacker roubou milhares de cartões de crédito?
- Isso é um erro! Quem invade sistemas com intenções maliciosas são os CRACKERS.
- Assim como os hackers, os crackers tem um enorme conhecimento em programação e Sistemas Operacionais.
- Pode-se simplificar o conceito, afirmando que um cracker visa lucro e destruição. Enquanto um hacker visa buscar e corrigir erros em sistemas computacionais, jamais se dedicando a danificar ou roubar dados intecionalmente.

Cracker

- O termo cracker, além da definição já apresentada, é utilizado também para se referir àquele individuo que se dedica à arte de contornar as proteções de softwares e dispositivos. Exemplos: “Cracks” para programas e jogos, desbloqueios para consoles de video game, dentre outros.

Breve Histórico

- 1872 – John Draper, ou Capitão Crunch, descobriu que um apito de brinquedo que era oferecido como brinde em caixas de cereal, de mesmo nome, produzia um sinal sonoro com frequência de 2,6 kHz que lhe permitia fazer chamadas telefônicas de longa distância sem ter que pagar. Feito isso, desenvolveu em conjunto com Steve Wozniak, fundador da Apple, um aparelho que permitia emular todas as frequências usadas pelo sistema telefônico. Isto forçou os EUA a trocar todo o seu sistema telefônico. Draper foi preso por fraude em 1972 e condenado a cinco anos de prisão.



Breve Histórico

- 1980 – A predecessora da internet entra em colapso devido a um vírus acidentalmente distribuído.
- 1986 – Na Universidade de Berkeley, o gestor de rede descobriu um erro de 75 centavos nos registros da universidade. Uma investigação foi realisada e culminou com a prisão de 5 crackers alemães.
- 1988 – Robert Morris lança um programa verme (worm), que rapidamente se espalha por 6000 servidores, levando a rede a quase fechar. Morris foi condenado a pagar U$ 10.000 e 400 horas de serviço comunitário.

Breve Histórico

- 1989 – Kevin Mitinick é condenado a 1 ano de prisão por ter roubado software de uma companhia e códigos para linhas de longa distância de computadores da US Telephone.
- 1993 – Kevin Poulsen, Ronald Austin e Justin Perterson são acusados de terem adulterado a linha telefônica de uma estação de rádio, fraudando esta, de modo que apenas suas ligações passavam. Os 3 ganharam 2 Porches, U$ 20.000 e férias no Havaí.
- 1994 - Um estudante de 16 anos é preso e acusado de ter invadido os computadores de uma base área, da NASA e do Instituto Coreano de Investigação Atômica. Neste mesmo ano, um grupo de 6 crackers russos invadiu os servidores do Citibank e transferiu 10 milhões de dólares das contas.

Breve Histórico

- 1995 – Kevin Mitnick é preso pela 2ª vez. Foi acusado de ter roubado 20.000 números de cartão de crédito. Ainda neste ano, Cristopher Pile tornou-se a primeira pessoa a ser presa por criar e distribuir um vírus.
- 1999 – O vírus Melissa criou pânico por toda a internet. O FBI investigou e prendeu o seu criador.
- 2000 – O vírus ILOVEYOU atacou computadores por todo o mundo. Os mais populares sites da internet ficaram sobrecarregados. Além disso, a Microsoft admitiu ter sido atacada e que os códigos do futuro Windows haviam sido vistos.

Ferramentas dos Hackers - Scanner

- Programa que permite investigar e detectar automaticamente todas as vulnerabilidades de um sistema.
- Este programa vasculha toda uma faixa de endereços, buscando portas abertas que respondem por algum determinado serviço.
- Caso sejam muito agressivos e repetitivos, o administrador da rede pode desconfiar da iminência de um ataque.

Ferramentas dos Hackers – Password Crackers

- Qualquer programa que consiga realizar a quebra de senhas ou inutilizar as proteções destas.
- Atualmente, as senhas são armazenas utilizando um sistema de criptografia que não permite obter a senha em texto plano depois de que esta foi criptografada. A solução para descobrir uma senha é um ataque que busque um texto, cujo resultado da criptografia seja igual ao armazenado.
- Existem duas maneiras:
  - Ataque dicionário: São testadas todas as combinações de palavras em um dicionário.
  - Ataque forca bruta: São testadas todas as combinações possíveis de letras, números e caracteres especiais. Pode levar muito tempo para encontrar um resultado, dependendo do tamanho da senha. Porém, caso o ambiente não conte com uma proteção para evitar esse ataque, a senha será descoberta.

Ferramentas dos Hackers - Trojan

- Um trojan é um programa que executa uma operação ilegal em um computador. Normalmente, os trojans abrem uma porta no computador afetado, permitindo ao Hacker o acesso ao sistema por meio desta.
- Seu nome se deve ao fato de que este “código secreto” está alojado dentro de um programa inofensivo, como um jogo, por exemplo. Assim como na mitologia, onde guerreiros se esconderam dentro de um cavalo que foi dado de presente para um outro reino, e, ao cair da noite, devastaram todo o reino.

Ferramentas do Hackers – Sniffer

- Um sniffer é um programa que coloca o dispositivo de rede em um modo conhecido como promíscuo. Neste modo, todos os dados que trafegam na rede, mesmo para outro destinatário, são entregues ao programa.
- Com isto, o programa consegue capturar indevidamente todos os pacotes da rede, processá-los e comprometer a segurança da rede.
- Com estes programas, pode-se obter, por exemplo, senhas, emails e mensagens instantâneas enviadas de um computador para outro.

Ferramentas do Hackers – Vírus e suas variantes

- Um vírus é um programa com capacidade de se auto propagar por uma rede ou pela internet.
- Normalmente, tem um objetivo nocivo ao ambiente, seja danificar o sistema, o roubo de informações ou mesmo o sequestro de todo o sistema.
- Normalmente, quando infectado por um vírus o computador em questão se torna um escravo do criador deste. Ficando a disposição para ataques em grupo contra um alvo determinado. Devido ao “uso” secreto, percebe-se que o sistema apresenta lentidão anormal, sendo esse o principal sintoma da contaminação.

Pirataria

- Após a apresentação dos Cracker, nota-se que um dos feitos destes é a criação de ferramentas que permitem burlar a proteção de sistemas e dispositivos. Em geral, os sistemas afetados são então pirateados, isto é, distribuídos sem a devida licença.
- Esse “desbloqueio” e distribuição são considerados crimes, passíveis de multas e até prisão.
- A lei que tornou crime a pirataria no Brasil é a Lei Nro 10.695/03

Pirataria – Legislação

- O artigo 184 do Código Penal considera como crime a violação ao direito do autor.
- Além disso, qualquer adulteração de informação ou acesso indevido a ela pode ser considerado um ato de piratear informação.
- Pode-se então definir pirataria como uma prática ilícita, caracterizada pela reprodução e uso indevido de programas e softwares legalmente protegidos.
- Calcula-se que para cópia legítima em uso, pelo menos uma é produzida sem autorização.

Pirataria – Formas Mais Frequentes

- Existem 4 formas mais frequentes de pirataria:
  - Cópia para o utilizador final: Simples cópia não licenciada por particular ou empresa. O número de licenças é menor do que o números de instalações.
  - Pré-instação do disco: Computadores comercializados com software ilícito pré-instalado. Os revendedores adquirem uma licença válida e a instalam em vários computadores. Esses computadores são vendidos para usuários finais que desconhecem essa situação. Em geral, o computador segue sem a mídia, a licença e a documentação do sistema para o comprador.

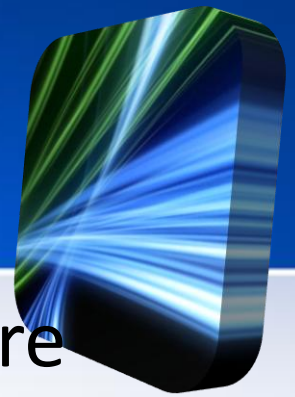
Pirataria – Formas Mais Frequentes (cont)

- Falsificação: Prática mais comum. Um software e sua embalagem são copiados e distribuídos em larga escala de forma ilegal, frequentemente por organizações criminosas, como um produto legal.
- Canais não autorizados: Software fornecido com condições especiais para um determinado fim, que depois é redistribuído para empresas e pessoas que não possuem as qualificações necessárias para estas licenças. Exemplo: Software para fins acadêmicos, que são distribuídos e utilizados por empresas.

Licenciamento

- Até o momento, se falou apenas do lado ilegal do software. Mas e o lado legal?
- Em primeiro lugar é necessário estabelecer o que é vendido para o comprador.
- Não é o sistema que é vendido!!! Mas o direito de uso do mesmo!!!

Formas de Licenciamento



- O licenciamento para o uso de um software pode ser encontrado nas seguintes formas:
  - Uso de uma cópia única;
  - Uso de múltiplas cópias até um valor limite;
  - Licença Geográfica: Permite o uso de um número ilimitado de cópias em uma organização dentro de uma localização geográfica definida. Exemplo: Filial de uma empresa.
  - Licença Institucional: Concede direito de uso de um número ilimitado de cópias à uma instituição. Exemplos: Uma universidade ou uma empresa inteira

Formas de Distribuição

- Um software pode ser distribuído de várias formas:
  - Domínio Público: Não demanda nenhuma obrigação de licenciamento. Em geral, são softwares cujo direito de propriedade tenha sido liberado. Em geral, softwares oriundos do mundo acadêmico.
  - Proprietários: Estes demandam, na maioria dos casos, a necessidade de obter uma licença. Podem ocorrer casos, onde isso não é necessário.

Sistemas Proprietários

- Os sistemas proprietários podem ser distribuídos de formas distintas:
  - Freeware
  - Shareware, Demo e Trial
  - Beta e Release Candidate
  - Adware
  - OpenSource, GPL e GNU
  - Update e Upgrade

Freeware

- São softwares gratuitos
- Podem ser utilizados livremente.
- Podem ser destinados apenas para pessoas físicas ou uso acadêmico.
- Embora o uso seja livre, a empresa continua sendo proprietária do sistema.
- Exemplos:

  Google Chrome, Firefox

Shareware, Demo e Trial

- Sofwares que podem ser copiados livremente para **avaliação**;
- Constituem uma versão de avaliação do produto em si;
- Normalmente estabelecem um prazo máximo de uso, como por exemplo, 30 dias;
- Requerem licenciamento em caso de uso continuado;
- Normalmente, contam com limitações em relação a sua versão paga;
- O conceito Demo é mais aplicado a Jogos, que podem ser distribuídos até em CDS, porém somente para avaliação e com certas limitações.

Beta e Release Candidate

- São versões ainda em desenvolvimento;
- Muitas vezes possuem aspectos de freeware;
- Precedem a versão oficial.
- Em geral, possuem erros que devem ser reportados à criadora do sistema.
- Antes de um lançamento oficial do sistema, normalmente são lançados betas do mesmo.
- Normalmente, não possuem todas as funções presentes no sistema concluído.

Adware

- São programas suportados por banners.
- São gratuitos enquanto o banner estiver rodando no programa.
- Existe a possibilidade de adquirir uma licença e retirar os banners.
- Esses banners estão contidos na tela do programa e exibem propagandas dos mais diversos tipos. Com o valor arrecadado por esta propaganda, o sistema se mantém funcionando.
- Em geral, não é possível escolher quais propagandas serão exibidas, o que pode ser um problema...

Opensource, GPL e GNU

- Opensource é um tipo de distribuição no qual o programa é um freeware e seu código fonte também está disponível para download.
- Desenvolvedores podem utilizar este código, adaptando e reaproveitando-o, porém o resultado final também deverá ser distribuído nos mesmos padrões.
- GPL e GNU são os contratos para esta forma de distribuição.
- A principal vantagem deste modelo é a facilidade para encontrar e resolver erros, tendo em vista que o mundo todo compartilha o mesmo código-fonte.

Opensource, GPL e GNU: Linux

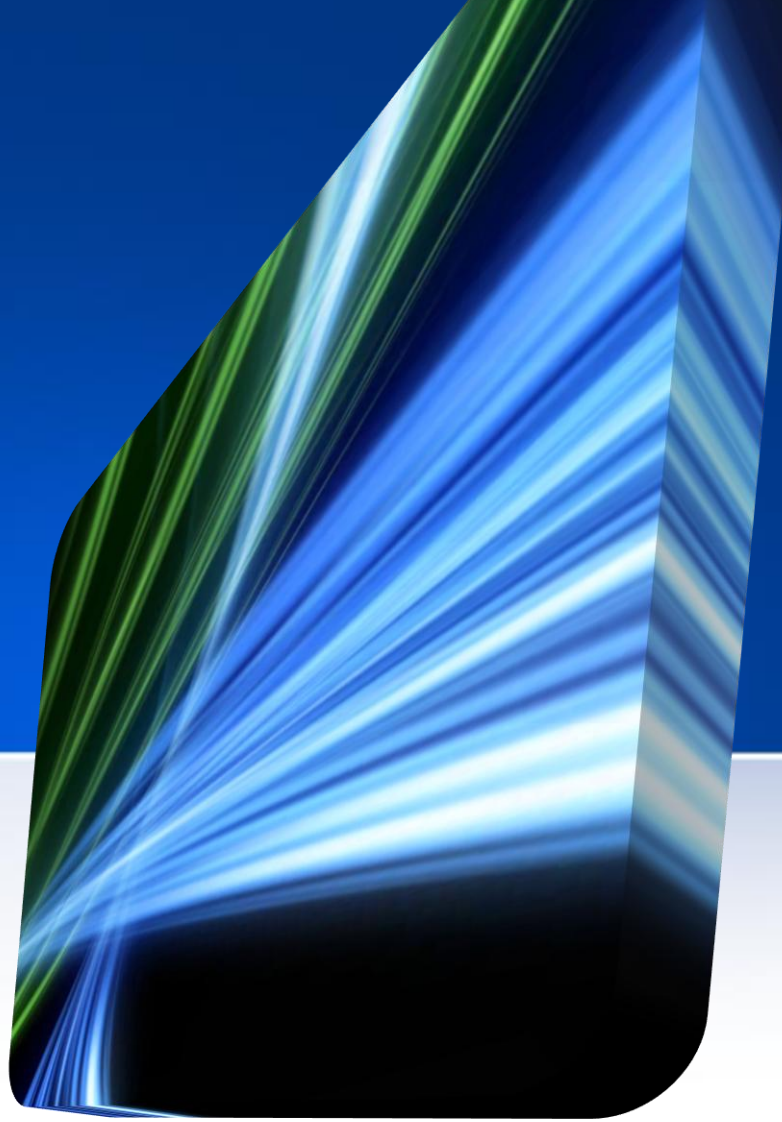
- O maior exemplo de um sistema que segue as regras do opensource é o Linux.
- Seu código fonte é amplamente distribuído e adaptado, formando as distribuições.
- Uma vez que essas distribuições seguem a regra do opensource elas não podem ser cobradas.
- Porém, as empresas que as desenvolvem podem cobrar pela manutenção e suporte a estas distribuições. É daí que vem o seu “sustento”.

Update e Upgrade

- Update: Nome dado a uma atualização de um programa. Os programas antivírus são os que mais necessitam de updates. Em geral, estão embutidos na licença adquirida. A maioria dos sistemas fazem updates automaticamente.
- Upgrade: Nome dado a real mudança de versão. Por exemplo, ao trocar o sistema operacional do Windows XP para o Windows 7. Entende-se que isto deve acarretar melhorias no sistema.

Bibliografia

- GUIMARÃES, Ângelo M; LAGES, Newton A. C.; Introdução a Ciência da Computação. LTC – Livros Técnicos e Científicos. Edição Atualizada.
- MOKARZEL, Fábio C.; Introdução à Ciência da Computação. Editora Campus
- TANENBAUM, Andrew S.; Sistemas Operacionais Modernos, Editora Pearson PTR, Terceira Edição
- FEDELI, Ricardo D. *et al.*; Introdução à Ciência da Computação, Editora Cengage Learning, Segunda Edição



FIM