Introdução à Segurança Computacional: Princípios Básicos

André R. A. Grégio
gregio@inf.ufpr.br

Departamento de Informática
UFPR

Aula Anterior

- História do hacking

> "Aqueles que não conseguem lembrar o passado estão condenados a repeti-lo"
>
> – George Santayana, A Vida da Razão, 1905

… *bug loop!*

- No ano 2000, um invasor podia “quebrar” o Windows 95 e 98 por meio de uma URL especialmente codificada:

... bug loop!

- No ano 2000, um invasor podia “quebrar” o Windows 95 e 98 por meio de uma URL especialmente codificada:

```
<HTML>
<BODY>
<A HREF="c:\con\con">crashing IE</A>
<!-- or nul\nul, clock$\clock$ -->
<!-- or aux\aux, config$\config$ -->
</BODY>
</HTML>
```

... bug loop!

- No ano 2000, um invasor podia “quebrar” o Windows 95 e 98 por meio de uma URL especialmente codificada:

```
<HTML>
<BODY>
<IMG SRC="c:\con\con”>
<!-- or nul\nul, clock$\clock$ -->
<!-- or aux\aux, config$\config$ -->
</BODY>
</HTML>
```

… *bug loop!*

- Em 2013, *crash* similar no OSX afetou quase todas as aplicações:
  - File:/// em vez de file:///
- Em 2015, Google Chrome podia ser quebrado com um mero *mouse over* em URL terminada por:
  - "%%30%30"

Objetivos da Aula

- Apresentar conceitos básicos de segurança
- Introduzir os princípios de confidencialidade, integridade e disponibilidade
- Discutir ameaças, problemas e mecanismos

Motivação

- Sistemas seguros, aplicações seguras, hardware seguro…
  - *Seguro de quem?*
  - *Seguro contra o quê?*
- Um telefone criptografado é seguro contra:
  - Ouvintes casuais?
  - Atacantes motivados com poder financeiro?
  - Uma agência de inteligência governamental?
- A urna eletrônica brasileira é segura?

Motivação

- Segurança deve ser contextualizada:
  - Tipo, motivação e ferramental do atacante
  - Avanços temporais/matemáticos
- Sistemas são complexos:
  - Compostos por diversos dispositivos e programas
  - Dispositivos e programas precisam interagir
  - Sistemas podem precisar interagir com outros sistemas!
  - Possuem propriedades emergentes
  - Contêm *bugs*

Sistemas e Segurança

- "*Em teoria, não há diferença entre teoria e prática. Na prática, há.*" (Yogi Berra???)
- Segurança adequada considera o relacionamento entre:
  - Prevenção (lacres, cofres, políticas e regras de bloqueio)
  - Detecção (provisão de alarmes)
  - Reação (procedimentos de mitigação, remediação e forenses)

Da Natureza dos Ataques

- O ciberespaço é uma versão da sociedade:
  - Pessoas interagindo entre si
  - Correio, compras, relacionamentos
  - Vândalos, ativistas
  - Tarados, *voyeurs*
  - Aproveitadores, fraudadores, ladrões
    - Grampo, roubos diversos, pirâmides (Ponzi)
- O *exploit* serve como pé-de-cabra

Da Propriedade dos Dados

- Exposição extrema na Internet
  - Usuário “comum” dissocia sua persona virtual
- Dados pessoais não pertencem ao indivíduo:
  - Seu Gmail pertence ao Google
  - Seu perfil é do Facebook
  - Sua informação financeira é do banco
  - Suas informações de saúde são do médico

Scams e violação da privacidade

- Golpes ontem e hoje:
  - Mães e viúvas da guerra pagavam para um larápio cuidar do túmulo do falecido além-mar
  - Príncipes nigerianos enviam e-mail querendo dividir uma fortuna conosco
- Utilidade pública:
  - Usam sistemas telefônicos para medir luz, água...
    - Quando a pessoa sai de férias, o medidor muda
  - IoT (fechadura eletrônica, alarmes, monitoração)
    - Acessíveis via *apps* ou câmera na rede com cred. *default*

Da Natureza dos Ciberataques

- Ameaças são as mesmas, já o ambiente…
  - Alcance mais amplo (disseminação mundial)
  - Mais comuns com o tempo (seguro ao atacante)
  - Mais difícil de traçar a origem
    - Tecnologias para ofuscação, anti-forense
    - Uso de *proxies* e anonimizadores de tráfego
    - Trampolins, *botnets*
    - Legislação não-uniforme
- Automação, distância, propagação de técnicas

Das Necessidades de Segurança

- Privacidade:
  - Democracia é construída sobre ela (voto secreto)
- Segurança multinível:
  - Classificação da informação; compartimentalização
- Anonimidade:
  - Política, religiosa, de saúde, policial/jornalística
- Autenticação:
  - Estabelecimento de relações de confiança

Princípios Básicos

- Segurança computacional reside em
  - Confidencialidade
  - Integridade
  - Disponibilidade
- Interpretação pode variar
  - Ambiente
  - Necessidade do indivíduo
  - Costumes
  - Leis ou políticas vigentes

Confidencialidade

- Segredo, ocultação, encobrimento de informações ou recursos
- Necessária em áreas sensíveis:
  - Instituições civis ou militares (governamentais) compartimentalizam informações -> *need to know*
  - Acesso restrito àqueles que necessitam dela
- Ex.: companhias com projetos proprietários

Confidencialidade

- Mecanismo de suporte:
  - Controle de acesso
- Implementação do mecanismo de suporte:
  - Criptografia
    - A chave controla o acesso
    - Precisa-se proteger a confidencialidade da chave!
    - Problemas… Ex.: WEP
- Aplica-se à existência de dados
  - Comunicações cifradas de extra-terrestres
    - Saber que esse tipo de comunicação existe pode superar a necessidade de conhecer o conteúdo!!!

Confidencialidade

- Aspecto importante: ocultação de informações
  - Equipamentos de uma organização
  - Configurações
  - Versões de sistemas e aplicações
- Mecanismos para garanti-la dependem de
  - Serviços de suporte confiáveis e premissas:
    - *kernel* é capaz de lidar com o serviço
    - agentes proveem dados corretos
    - ambiente não comprometido

Integridade

- Confiança nos dados ou recursos
- Relacionada à prevenção de mudanças impróprias ou não-autorizadas
- Integridade dos dados:
  - O conteúdo da informação não foi alterado
- Integridade da origem:
  - Fonte de dados (autenticação)
    - Precisão, credibilidade e confiança na informação

Integridade

- Aspecto importante: credibilidade!
- Ex.: jornal imprime informação obtida de um vazamento do Palácio do Planalto e atribui a fonte errada (integridade dos dados, mas não da origem)
- Mecanismos podem ser divididos em 2 classes:
  - Prevenção
  - Detecção

Integridade

- Mecanismos de prevenção:
  - Mantêm a integridade pelo bloqueio de qualquer tentativa não-autorizada de modificação dos dados ou tentativas de modificar o dado de maneira não autorizada
    - Usuário tenta mudar dado sem autoridade para tal
    - Usuário autorizado tenta mudar dado de outras maneiras não correspondentes a sua autorização
- Ex.: intruso mexer nos registros de um contador vs. contador sonegar impostos

Integridade

- Mecanismos de detecção:
  - Alertam que a integridade dos dados não foi preservada (sem credibilidade)
- Garantia depende de premissas sobre a fonte e confiança nesta fonte
- Avaliação inclui corretude e confiança do dado
  - Como e de quem foi obtido?
  - O caminho do dado foi protegido?
  - O destino do dado é protegido?

Disponibilidade

- Habilidade de se usar a informação ou recurso desejado
- Aspecto importante da confiabilidade e projeto de um sistema:
  - Sistema indisponível é tão ruim quanto um sistema inexistente
  - Alguém pode deliberadamente negar acesso a um dado ou serviço, tornando-o indisponível

Disponibilidade

- Ex.: projetos de sistemas podem assumir um modelo estatístico para analisar padrões de uso esperado (garantidos por mecanismos)
- Se esse uso é manipulado (tráfego de rede), a premissa não é mais válida -> falha
  - Mecanismo para manter o recurso/dado disponível não suporta um ambiente para o qual ele não foi projetado
  - Ex.: conexões do Apache

Disponibilidade

- Tentativas de bloquear a disponibilidade são difíceis de se detectar:
  - O padrão de acesso incomum é uma anomalia momentânea, uma falha de dispositivo/recurso ou um ataque propositalP
- Se um sistema indisponível é essencial para o funcionamento de outro, a negação do serviço ocorre em cascata (e.g., interface de consulta e banco de dados remoto)