Info Hacker

RESUMO QUINZENAL OFICIAL DA ACADEMIA HACKER

01: Capítulo 2: Computer Network Security Fundamentals

Capítulo 2: Computer Network Security Fundamentals

por Cauê Bittencourt

Neste capítulo do livro Guide to Computer Network Security de Joseph Migga Kizza, o autor aborda algumas formas de proteger objetos[1]. A prevenção de acesso não autorizado a recursos do sistema é obtida através de uma série de serviços que incluem controle de acesso, autenticação, confidencialidade, integridade e não-repudiação

Sistemas utilizam o serviço de controle de acesso, combinado com uma identificação prévia - como uma senha, para determinar quem utiliza o quê de seu sistema. O autor estabelece uma classificação desse serviço baseada em software e em hardware. O primeiro é dividido em monitoramento de ponto de acesso (ou POA do inglês point of access) e em monitoramento remoto, podendo um POA estar conectado à uma rede. Já para o último, o autor cita alguns exemplos como terminais de acesso, monitoramento de evento visual, cartões de identificação - magnéticos, códigos de barra, chips de contato ou uma combinação desses - identificação biométrica e vigilância em vídeo.

Autenticação é um serviço utilizado para identificar um usuário. Identificação de usuários, especialmente remotos, é algo complicado, pois muitos usuários - especialmente aqueles com intenção de causar danos - podem se passar por usuários legítimos quando na verdade não o são. Esse serviço fornece ao sistema a capacidade de verificar que um usuário é realmente quem ele ou ela diz ser, através da identificação de três pontos chaves: algo que o usuário é, algo que ele sabe e algo que ele tem. Fisicamente, podemos autenticar usuários checando um ou mais dos seguintes itens: username, senha, imagens de retina, digitais, localização física, cartões de identificação.

Um serviço de confidencialidade protege dados e informações do sistema de acessos não autorizados. Quando dados partem de uma das bordas do sistema, como por exemplo um computador cliente conectado na rede, ele passa a navegar por ambientes não confiáveis. Dessa forma, é razoável que o receptor desconfie que alguma aplicação de terceiro ou um man-in-the-middle (homem no meio, em português) possam ter interceptado esses dados, outra ameaça comum são os Sniffers. Sniffers (farejadores em português) são programas escritos para serem instalados em canais de comunicação com o objetivo de espionar o tráfego da rede.

Para proteger objetos dessas ameaças, esse serviço utiliza algoritmos de criptografia. O autor divide esses algoritmos em simétricos, que utilizam uma chave comum e o mesmo algoritmo de criptografia para criptografar e para descriptografar a mensagem, e assimétricos (mais conhecido como chave pública). Esse último utiliza duas chaves diferentes, uma pública e uma privada - conhecida apenas pelo emissor e pelo receptor. Tanto o emissor quanto o receptor possuem as duas chaves, para criptografar uma mensagem, o emissor utiliza a chave pública do receptor, e ao receber a mensagem, o receptor utiliza sua chave privada para descriptografá-la.

Integridade é um serviço utilizado para proteger os dados do sistema contra ameaças que podem modificá-los durante sua transmissão entre a origem e o destino. Enquanto a confidencialidade protege os objetos contra acessos não autorizados, a integridade protege contra a modificação - garantindo que a integridade dos dados transmitidos esteja intacta. Para isso, ele utiliza algoritmos de criptografia e de hashing. Uma função hash recebe como entrada uma mensagem e gera como saída um código (comumente chamado de hash) que funciona como uma assinatura da mensagem - algo parecido com a impressão digital para humanos. Essa assinatura é então acoplada na mensagem antes dela ser enviada ao receptor, promovendo assim a integridade e autenticidade da mensagem.

Por último, mas não menos importante, temos o serviço de não-repúdio, que tem como objetivo fornecer prova de origem e de entrega do serviço e/ou da informação. No mundo real, é possível que o emissor possa negar a autoria de uma troca de dados que originou dele. Esse serviço, através de assinatura digital e algoritmos de criptografia, garante que esses dados não possam ser repudiados (terem sua existência negada), fornecendo provas de origem que sejam irrefutáveis.

Segundo o autor, o termo não-repúdio tem dois significados, um no mundo jurídico e outro no mundo técnico da criptografia. No livro, o autor trabalha com este último significado, utilizando a definição dada por Adrian McCullagh e Willian Caelli[²]:

- Um serviço que fornece prova da integridade e da origem dos dados numa relação à prova de falsificação, a qual pode ser verificada por qualquer terceiro a qualquer momento.
- Uma autenticação que, com uma alta garantia, pode ser declarada como legítima e não pode ser refutada posteriormente.

Para atingir a não repudiação, usuários e ambientes de aplicação exigem que um serviço de não-repúdio colete, mantenha e disponibilize evidências irrefutáveis. Os melhores serviços de não repudiação são assinaturas digitais e encriptação. Esses serviços oferecem confiança através de geração de evidências de forma persistente, que podem ser usadas para resolver uma disputa.

[¹]: Segundo o autor, objetos são os recursos do sistema os quais queremos proteger. Para saber mais, consulte a edição 14 do Info Hacker
[²]: McCullagh A, Caelli W Non-repudiation in the digital environment. http://www.firstmonday.dk/issues/issue5_8/mccullagh/index.html#author

Desafios de Programação

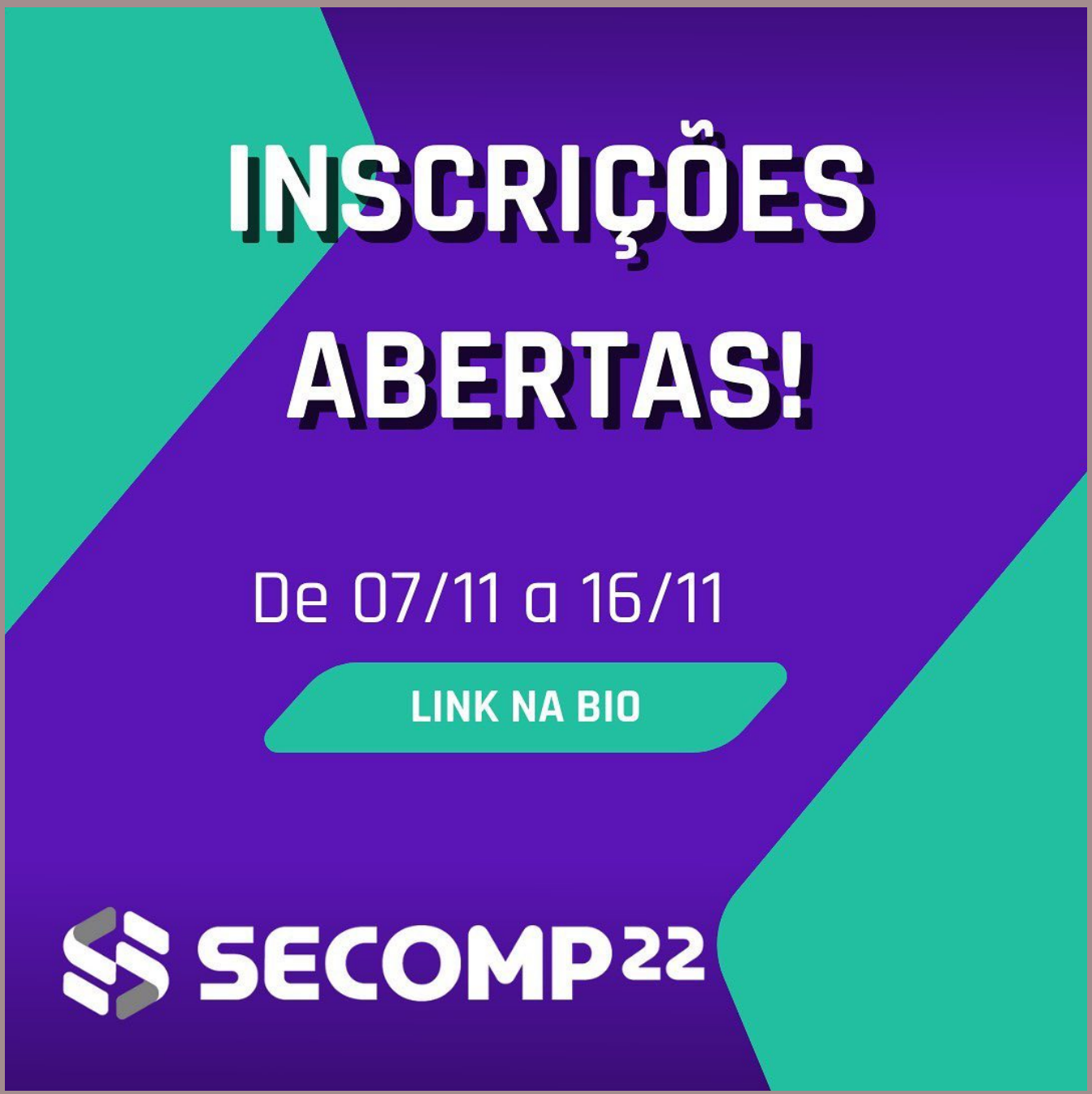
Em Python qual a saída dos trechos de códigos abaixo?

```
>>> round(1.5) == round(2.5)
>>>
```

a) 2
b) undefined
c) False
d) True
e) SyntaxError

```
>>> round(2.5) == round(3.5)
>>>
```

a) True
b) undefined
c) 3
d) False
e) SyntaxError



https://doity.com.br/secomp2022

secomp.ufal

Info Hacker - Edição 018
08/11/2022

Produção
Equipe Info Hacker

acha.ufal

Edições Anteriores

https://github.com/Academia-Hacker/Info-Hacker