Revisão

Segurança da Informação

Nesta revisão, abordaremos os principais tópicos relativos ao conteúdo da disciplina **Segurança da Informação**, para cada semana de aula que foi ministrada. Esta revisão deve ser utilizada como um guia para ajudá-lo(a) a rever os principais assuntos abordados na disciplina. Espera-se que você tenha realizado as leituras sugeridas dos textos-base, feito as atividades propostas no decorrer de cada aula, bem como, sempre que possível, ter assistido aos vídeos de apoio. Foram disponibilizados códigos de exemplo e diversos materiais adicionais para que pudesse utilizá-los para reforçar o aprendizado. Feito isso, tenho certeza de que terá sucesso na avaliação.

Na **primeira semana**, o objetivo foi apresentar alguns aspectos relacionados ao que se entende por segurança e o porquê de o tema ser abordado e relevante atualmente, em especial porque todos nós fazemos uso de algum serviço na internet, que envolve nossos dados pessoais e dinheiro (bancos *on-line*). Dessa forma, foi fundamental tratarmos de modelos de segurança de redes de computadores, conhecer os cinco principais serviços básicos de segurança e conseguir identificá-los em casos reais, bem como ter uma visão geral de criptografia e refletir sobre como esses mecanismos de segurança são presentes no nosso cotidiano, afetando-nos diretamente. Discutimos a importância de incidente no contexto da segurança, que é um evento adverso que foi confirmado ou está sob suspeita em um ambiente com diversos recursos computacionais. Tratamos os pilares da segurança da informação, sendo a integridade uma propriedade de que a informação não foi alterada de maneira não autorizada, citando, por exemplo, códigos de correção de erros como ferramentas para apoiar a integridade.

Na **segunda semana**, apresentamos os conceitos principais que envolvem confidencialidade e cifras simétricas, com destaque para o AES, que é atualmente a cifra simétrica mais importante e com uso mais amplo. Também foram levantadas questões relacionadas ao paralelismo durante a cifração/decifração, problemas, cuidados, ou seja, tudo o que é necessário considerar para uma solução de segurança. Foram apresentados modos de operação para cifragem de blocos como o CBC, que tem como característica evitar a revelação de padrões em uma sequência de blocos. Sua operação consiste em: dado um primeiro bloco de texto puro B1, é feito um ou exclusivo com um vetor de inicialização, **VI**, antes de ser encriptado e cada bloco de texto puro subsequente sofre um ou exclusivo com o bloco de texto cifrado anterior antes de ser encriptado.

Discutimos as operações que compõem as cifras modernas por meio da utilização de bibliotecas prontas de algoritmos de criptografia ao invés de sua implementação do zero. Vimos também exemplos atuais de aplicação da criptografia na internet, como a assinatura de documentos eletrônicos. Trouxemos também discussões sobre ataques, como o ataque de texto puro em que um criptoanalista tem acesso ao texto cifrado de uma ou mais mensagens, cujas mensagens foram encriptadas utilizando a mesma chave K.

Na **terceira semana,** apresentamos dois serviços de segurança, que são a integridade e a autenticidade. Aprendemos também sobre a geração de números aleatórios, o que é essencial para construir chaves criptográficas imprevisíveis e, assim, difíceis de serem adivinhadas por um atacante, sendo útil inclusive em cenários em que é necessário embaralhar informações, como no caso de jogos de cartas ou no embaralhamento de votos registrados em urnas eletrônicas. Aprendemos também que as cifras de blocos simétricas, cifras assimétricas e funções *hash* e códigos de autenticação de mensagens são três categorias de algoritmos criptográficos, e que para aplicações criptográficas a semente que serve como entrada do gerador de número pseudoaleatório (PRNG) deve ser segura. Na indicação de leitura dos textos-base, aprendemos que o pseudogerador de números aleatórios (PRNG) é determinístico. Em termos de aleatoriedade, um requisito para um PRNG é que o fluxo de *bits* pareça ser aleatório, embora seja determinístico. Aprendemos que dentre as características que um teste de aleatoriedade deve estabelecer, destacam-se a consistência, a uniformidade e a escalabilidade.

Na **quarta semana**, o assunto proposto foi criptografia assimétrica e certificação digital. Compreendemos o funcionamento básico desse tipo de criptografia e o papel de cada uma das chaves empregadas (pública e privada). Tratamos do método Diffie-Hellman, o qual permite que as partes que não se conhecem possam compartilhar entre si uma chave secreta por meio de um canal inseguro de comunicação, sendo, portanto, importante para ser usado no intercâmbio de chaves entre usuários. Tivemos também um breve contato com a parte matemática por trás dos algoritmos utilizados e entendemos como funciona o processo de certificação digital e para que ele serve. A criptografia assimétrica, também conhecida como “criptografia de chave pública”, é baseada em dois tipos de chaves de segurança (uma privada e outra pública) que são usadas para cifrar mensagens e verificar a identidade de um usuário. Aprendemos que, em relação à segurança do RSA, há técnicas como ataques baseado em falha de *hardware*, ataques de força bruta e de temporização que são usados para romper com a segurança proposta pelo RSA. Outro assunto abordado na semana foi sobre os certificados digitais, os quais servem como identidade virtual para uma pessoa física ou jurídica, uma vez que com ele podemos realizar transações *on-line*

com garantia de autenticidade e com toda proteção das informações trafegadas pela rede de dados.

Na **quinta semana,** aprendemos sobre mecanismos de autenticação de usuários e compreendemos e comparamos os aspectos positivos e negativos desses mecanismos de modo a entender sua aplicabilidade em contextos distintos. Também verificamos os cuidados a serem considerados ao desenvolver algum sistema que utilize mecanismos de autenticação, o que certamente auxilia a evitar erros e vulnerabilidades. Há quatro grupos básicos de mecanismos de autenticação, que se utilizam de: aquilo que você é (informações biométricas, como a sua impressão digital, a palma da sua mão, a sua voz e o seu olho), aquilo que apenas você possui (como seu cartão de senhas bancárias e um *token* gerador de senhas), aquilo que você sabe (senhas numéricas, alfanuméricas) e aquilo que você faz (biometria dinâmica, como métodos por análise de voz, assinatura manual ou andar). Também foi objeto de estudo os *botnets*, que se caracterizam por um número de dispositivos conectados à internet e cada um executa um ou mais *bots*. Os *botnets* podem ser usados para executar ataques DDoS, roubar dados, enviar *spam* e permitir que o invasor acesse o dispositivo e sua conexão. O *software* parasita pode ser instalado no computador da vítima por meio de um cavalo de Troia ou algum outro pacote de *malware.* A rede *botnet* é controlada de forma centralizada por um proprietário denominado “controlador de parasitas”.

Na **sexta semana**, abordamos os conceitos que envolvem *software* maliciosos (ataques e defesas), com objetivos que foram como: conhecer o inimigo, analisar o inimigo, combatê-lo e discutir se o inimigo do meu inimigo é meu amigo. Os *softwares* maliciosos são programas criados para executar ações danosas e atividades maliciosas em um computador e podem causar sérios danos aos usuários. Dentre os exemplos, destacaram-se: vírus, *worm*, *spyware*, *trojan*, *keylogger*, *ransomware*.

Para finalizar, chegamos à **última semana** do curso, na qual discutimos *firewalls* e sistemas de detecção de intrusão. Conhecemos as ações realizadas por atacantes como forma de preparação de ataques (descobrir IPs na rede, varrer portas, varrer vulnerabilidades), dando ao atacante informações sobre como esses serviços podem ser explorados. Também conhecido como IDS (*Intrusion Detection System*), um sistema de detecção de intrusão é um *software* (ou um *hardware*) que analisa o tráfego de uma rede, identificando ataques e tentativas de acesso não autorizados e alerta em tempo real. Quando ocorre um evento desse tipo, a principal desvantagem do IDS é que ele apenas detecta a intrusão. *Firewalls* são soluções de segurança baseada em *hardware* ou *software* que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede de entrada e saída para

determinar quais operações de transmissão ou recepção de dados podem ser executadas. No contexto dos *firewalls* como um mecanismo para garantir determinado nível de segurança da rede, temos a figura da DMZ que é uma rede em que estão os servidores que necessitam serem acessados também pela rede WAN.

Nesta semana, também abordamos o contexto da segurança em nuvens computacionais, apresentando o que é realizado nas nuvens da Amazon, Azure e GCP neste contexto. Vimos a importância do gerenciamento de identidade de acesso (IAM - *Identity Access Management*) da AWS, que assegura que a identidade de uma entidade seja verificada. Por outro lado, na nuvem da Azure, um *gateway* de VPM envia o tráfego criptografado em uma conexão rede pública. Apresentamos de forma complementar que no universo de IoT há preocupações com segurança, assim como há em outras tecnologias vigentes, como na nuvem e ambientes locais, sendo problemas típicos da IoT o baixo poder de processamento dos dispositivos, bem como sua heterogeneidade e escalabilidade.

De modo geral, sugiro que você revise as Atividades Avaliativas, bem como os textos-base, os códigos disponibilizados, os vídeos e as ferramentas que foram solicitadas que você interagisse durante as semanas. Tais materiais contêm informações importantes cujo entendimento é primordial e que podem aparecer na prova.

Como docente responsável pela disciplina, espero que os assuntos tratados possam complementar a sua formação profissional e que você tenha sucesso no decorrer da sua carreira que está apenas começando. Tenham em mente que todo o esforço será recompensado.

Desejo sucesso e uma boa prova!

Prof. Dr. Julio Cezar Estrella