Engenharia de Segurança 2017/1

Definição do Trabalho 1

(Data de entrega: 29/05/2017 - 23h:55)

A *Smart Home* do João

João decidiu melhorar seu dia a dia implementando algumas automatizações em sua própria casa para torná-la uma *smart home*. Para isso, João acoplou sensores e transmissores Wi-Fi (IEEE 802.11) às lâmpadas, ao ar-condicionado e às câmeras de monitoramento dispostas em locais estratégicos da casa. Todas as informações coletadas pelos sensores são enviadas a uma estação central que mantém estatísticas, efetua monitoramentos e permite controlar a luminosidade, as temperaturas e visualizar as imagens das câmeras. Estas informações são disponibilizadas localmente no computador de João.

Você é vizinho de João e descobriu acidentalmente que a rede da *smart home* está completamente aberta e decidiu comunicá-lo sobre isso, oferecendo ajuda para implementar algumas melhorias em sua rede, afinal, você é um engenheiro de segurança e grande amigo de João. Como primeiro passo, você deverá aplicar algum método de criptografia para assegurar que os dados trocados entre os dispositivos da casa estejam seguros. Depois, com mais calma, você pretende sugerir a implementação de mais algumas medidas que melhorem a *smart home* do João, ampliando principalmente a segurança.

Primeira tarefa

Escreva, na linguagem de programação de preferência da dupla, um algoritmo de criptografia que permita codificar e decodificar uma mensagem de texto. O algoritmo pode ser simétrico ou assimétrico. Na codificação, o programa deverá aceitar como entrada a chave e um arquivo de entrada, no formato texto, com a mensagem a ser criptografada e gerar um arquivo de saída criptografado. Na decodificação, o arquivo criptografado deverá ser lido como entrada e o arquivo legível deverá ser gerado.

Não preocupe-se, neste momento, com a implementação da rede. Efetue prioritariamente a implementação do algoritmo de criptografia e garanta o seu correto funcionamento. Caso queira, posteriormente, criar uma pequena rede e testar o seu algoritmo enviando dados de um dispositivo para outro, a parte de inovação/criatividade do seu trabalho também será considerada na avaliação.

Os critérios de avaliação desta tarefa serão:

- Originalidade do algoritmo (baseie-se em um algoritmo pré-existente, mas faça alguma alteração para tentar torná-lo mais forte; ou, ainda, escreva seu próprio algoritmo - quanto mais simples seu algoritmo mais simples será sua nota);

- Complexidade do algoritmo;
- Qualidade da documentação (interna e relatório);
- Funcionamento correto (obtenção da mensagem original após as duas operações).

Segunda tarefa

A implantação de criptografia já melhora bastante a segurança da *smart home*, mas você, como bom engenheiro de segurança, sabe que isso não é suficiente e decide dar alguns conselhos ao João para o futuro da *smart home*.

De modo detalhado e usando os termos técnicos corretos, descreva as possíveis medidas de segurança que o João deveria implementar em sua *smart home* futuramente. Sugira abordagens para melhorar a segurança das informações trocadas (podem ser técnicas associadas ao seu algoritmo de criptografia, por exemplo) e sugira também maneiras de assegurar as informações armazenadas na estação central (por exemplo, efetuar periodicamente um *backup* e armazenar as informações em um banco de dados). Como garantir integridade, disponibilidade, confidencialidade e autenticidade?

Considere que, atualmente, a *smart home* armazena as informações no computador de João e não as disponibiliza para acesso remoto. Qual seria a melhor abordagem para a disponibilização de acesso remoto à *smart home*? Efetue uma análise de risco e descreva a criticidade das informações armazenadas pela unidade central da casa; em seguida, avalie se a melhor abordagem seria o uso de serviços de nuvem para armazenar as informações e torná-las acessíveis remotamente ou se a implementação de um servidor em casa já seria suficiente para o cenário. Lembre-se de efetuar uma análise de custo também e esteja ciente dos possíveis ataques de segurança que a casa pode sofrer.

Sugestões de recursos adicionais a serem considerados:

- Adição de novos dispositivos à rede:
    - O que mais poderia ser monitorado/controlado na casa de João?;
    - Com um número elevado de dispositivos conectados à rede, é interessante que todos enviem as informações a uma unidade central? Imagine a possibilidade de criar subestações de monitoramento, cada uma responsável por um segmento (por exemplo, uma estação para monitorar a temperatura, outra para a luminosidade etc.).
- Desenvolvimento de um aplicativo para controle da *smart home*:
    - Que recursos deveriam estar disponíveis no aplicativo?
    - Alguns desses recursos deveriam ser habilitados/desabilitados quando acessando a casa remotamente?

Sobre a entrega

Envie, via Moodle, um arquivo compactado contendo:

1. Código fonte documentado (compilável);
2. Relatório contendo as seguintes seções:
    a. Execução da primeira tarefa
        i. Explicação do algoritmo, identificando a função da chave;
        ii. Restrições do algoritmo;
        iii. Estratégia sugerida para a troca de chave;
        iv. Instruções para compilação:
            1. Deve conter a versão do compilador utilizado;
            2. No caso do uso de bibliotecas, especificar a fonte onde a mesma pode ser obtida e a versão utilizada;
            3. Sequência de passos para compilação, caso não exista um Makefile;
            4. Parâmetros da linha de comando caso não exista interface iterativa (modo texto ou gráfico).
    b. Execução da segunda tarefa
        i. Instruções: organize esta seção em subtópicos de sua preferência se achar necessário. Inclua figuras que demonstrem as abordagens propostas (se usar figuras de terceiros não esqueça de citar a fonte).

Esclarecimentos

- Bibliotecas: não deve ser utilizada nenhuma biblioteca/*framework*/código disponível na internet que faça a criptografia em si. Podem ser utilizadas bibliotecas livres para qualquer outra função (ex: fazer uma UI opcional, facilitar a leitura e escrita do arquivo, cálculo de números primos ou de números grandes, etc.).
- Compilação: se o código fonte não compilar o trabalho não será considerado entregue! (zero)
- Sobre restrições do algoritmo: a correção inicialmente é feita por meio da comparação do arquivo decrifrado com o arquivo original. Se seu algoritmo possui alguma restrição que impeça que eles sejam idênticos, especifique estas restrições no relatório.

Data de entrega

O trabalho deve ser feito em ***duplas***, entregue via ***Moodle*** até dia ***29/05/2017*** às ***23:55***. Trabalhos entregues fora do dia e data terão a nota diminuída gradativamente de acordo com o atraso.