Aula 10
Internet das Coisas

Segurança em IoT

Prof. Julio Cezar Estrella
jcezar@icmc.usp.br

Roteiro

- Aspectos importantes da Segurança
- Segurança
  - Dispositivos
  - Comunicação
  - Informação

Aspectos Importantes da Segurança

- A segurança é um ponto crucial em qualquer projeto de IoT. Como destacamos em aulas anteriores, ela é transversal em todas as camadas de IoT
- Vamos abordar os riscos mais comuns de segurança em projetos de de IoT uma organização/empresa
- Há também opções de ferramentas para reduzir riscos de ataques aos dispositivos, comunicação e aos dados transmitidos da solução

Aspectos Importantes da Segurança

- Alto índice de ataques às redes, dispositivos, base de dados
- Necessidade de controle de tráfego
- Garantir integridade aos serviços
- Alta demanda dos serviços da Internet
- Milhões de acessos ao dispositivos de IoT

Aspectos Importantes da Segurança

- Mas por onde começar?
  - Dispositivo: É de onde vem os dados coletados pelos sensores. Como protegê-los?
  - Transmissão/Comunicação: Como garantir que no canal de comunicação não teremos intrusos interceptando os dados transmitidos?
  - Informação: Como garantir o acesso adequado (autenticação e autorização) à informação armazenada em bases de dados/storages

Segurança de Dispositivos

- Os dispositivos sofrem ataques especificos e precisam garantir o envio e recepção das informações aos gateways, brokers, nuvem
- Alguns ataques conhecidos são:
  - *Injeção de código mal intencionado*
  - *Interceptação da comunicação*
  - *Privação do sono*
  - *Criptoanálise*

Segurança de Dispositivos

- Injeção de código mal intencionado
  - Inserção de código (um script) que pode reprogramar o *dispositivo* para parar de enviar mensagem ou enviar mensagem errada, ou tentar algum acesso que ele não deveria ter, etc.
  - Inserir um software dentro do dispositivo de modo que com esse acesso seja possível controlá-lo e roubar informações.

Segurança de Dispositivos

- Interceptação da comunicação
  - Interceptar o que está sendo enviado/recebido. Um dispositivo consegue ler o que está sendo transmitido e se a informação não for encriptada, isso pode comprometer a privacidade e a integridade do sistema

Segurança de Dispositivos

- Privação do Sono
  - Muito comum quando dispositivos tem apenas a bateria como fonte de energia primária (para garantir sua autonomia).
  - Eles são programados para funcionar em intervalos bem definidos para enviar somente o que é necessário e com o intuito de economizar energia

Segurança de Dispositivos

- Privação do Sono
  - Este ataque consiste em derrubar o dispositivo movido a bateria e não deixá-lo entrar em modo sono.
  - Exemplo:
    - Quando criamos um sensor que dura 2 anos movido a bateria, é fundamental só enviar o que precisa, agregar informações, compactar, porque o objetivo é consumir o mínimo de energia.
    - O ataque força o sensor a computar, a enviar informações, que nada agregam e o sensor morre. Uma vez ocorrendo isso, todo o sistema fica comprometido.

Segurança de Dispositivos

- Criptoanálise
  - Consiste em quebrar as chaves de criptografia e ler as mensagens enviadas pelos dispositivos.
  - Encriptamos para proteger as mensagens e a criptoanálise atua no sentido de quebrar essa proteção
  - Isso compromete a privacidade
    - De usuários
    - Das organizações

Segurança da Comunicação

- Além da garantia da segurança do dispositivo, temos que nos preocupar com a segurança da comunicação.
- Há dispositivos que podem se passar por outros e isso pode comprometer o projeto de IoT, colocar em risco as informações da organização, expor o funcionamento de equipamentos, etc.

Segurança da Comunicação

- Lista de problemas mais comuns em IoT
  - Denial of Service
  - Spoofing
  - Uso não autorizado
  - Roteamento de informações
  - Man-in-the-Middle

Segurança da Comunicação

- Denial of Service
  - Consiste em gerar muita carga de trabalho para o sensor, muito além de sua capacidade de processamento. O conjunto (dispositivo/sensor) não consegue transmitir o que é relevante pois não possui recursos computacionais suficientes.
  - Isso leva:
    - Perder Informações
    - Congestionar a rede

Segurança da Comunicação

- Spoofing
  - O atacante mascara a informação.
  - Faz um dispositivo se faz passar por outro
  - Exemplo:
    - Um dispositivo que tem o mesmo IP do outro, se passando por ele, disfarçando sua identidade, com o objetivo de confundir outros dispositivos no mesmo ambiente de comunicação

Segurança da Comunicação

- Uso não autorizado
  - Um dispositivo passa a tentar acessar recursos que não deveria ter permissão.
  - Um dispositivo que só envia dados, passa a receber dados que estão no mesmo servidor que grava as suas informações.
  - *Este ataque explora problemas de permissão de acesso a recursos.*

Segurança da Comunicação

- Roteamento de informações
  - Um dispositivo infectado/hackeado altera as informações de roteamento e gera loops de roteamento. Um dado que sai do dispositivo para o gateway não chega nele, porque houve alteração da tabela de roteamento
  - Trata-se de um ataque ao protocolo de roteamento utilizado, pois trabalha de uma forma maliciosa
  - Impede que a informação chegue ao destinatario, ao usuário, ao gateway, ao servidor na nuvem, à base de dados na cloud, etc.

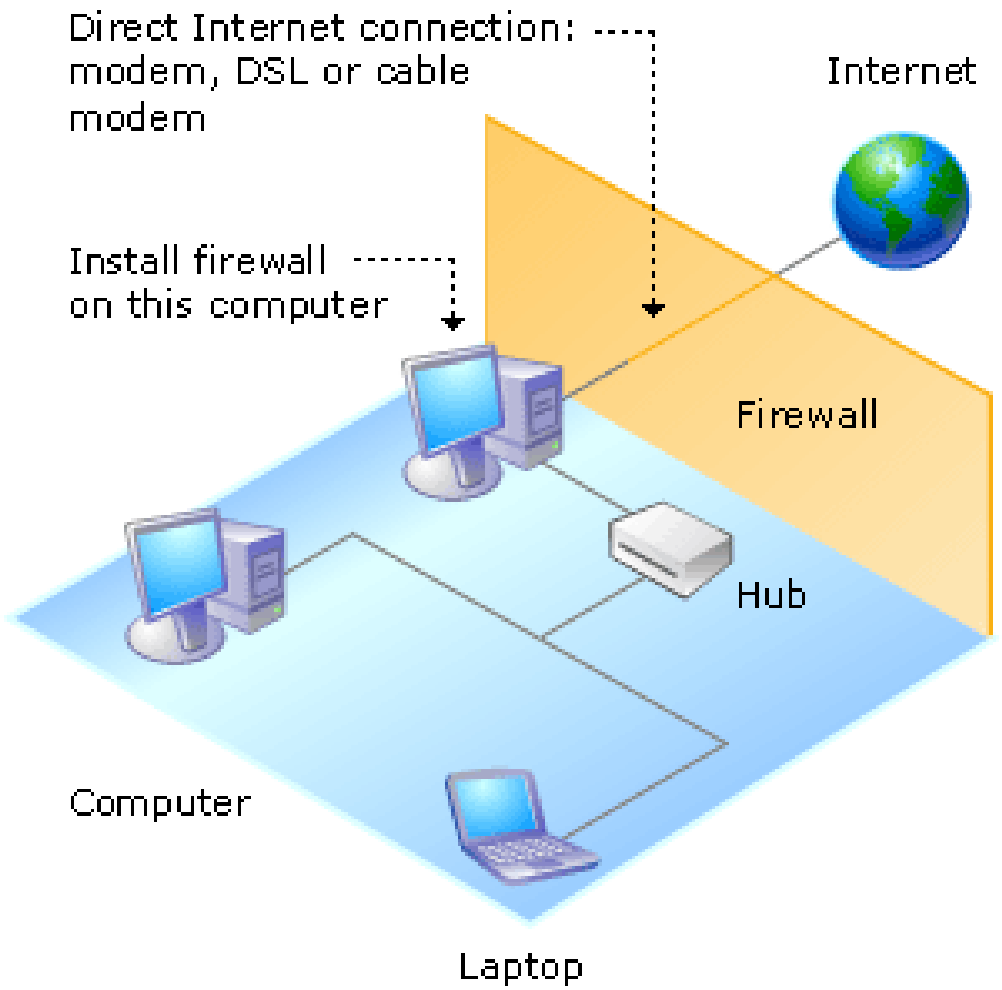
Segurança da Comunicação

- Man-in-the-Middle
  - O atacante coloca um novo elemento (dispositivo computacional) entre a origem e o destino dos dados transmitidos/recebidos
  - Exemplo: Comunicação entre um dispositivo e um gateway
    - O atacante “ouve” a comunicação quando o dispositivo inicia o envio de dados e se passa por ele encaminhando tudo para o gateway e outros vizinhos.
    - Ele compromente as mensagens enviadas pela rede, pois são de alguém que não é a origem verdadeira

Segurança da Comunicação

- Medida para lidar com a segurança da comunicação
  - Firewall
    - Significa parede Corta Fogo
      - Regula tráfego entre redes existentes
      - Impede a propagação de dados nocivos

Segurança da Comunicação



Segurança da Comunicação

- **Firewall**
  - É um foco para a tomada de decisões
  - Pode ser usado como um ponto de partida para a política de segurança da organização
  - Pode gravar requisições
  - Limita a exposição da rede

Segurança da Comunicação

- **O que um firewall não pode fazer?**
  - Proteger uma rede contra usuários internos
  - Proteger uma rede contra conexões que não passam por ele
  - Proteger contra ameaças completamente novas
  - Proteger contra vírus

Segurança da Comunicação

- **Firewall**
  - Principais características
    - Toda solicitação chega ao Firewall
    - Somente tráfego autorizado passa pelo Firewall
    - O próprio Firewall deve ser imune a penetração
    - Bloqueia o recebimento de dados baseado em uma fonte ou destino
    - Bloqueia o acesso a dados baseado em uma fonte ou destino
    - Bloquear dados baseado em conteúdo
    - Permite conexões com uma rede interna
    - Reporta o tráfego na rede e as atividades do Firewall

Segurança da Comnicação

- **Firewall**
  - Deve ter pelo menos as 4 funções a seguir:
    - Filtragem de pacotes
    - NAT (Network Address Translation)
    - Proxy de Aplicação
    - Monitoramento e registro

Segurança da Comunicação

- **Firewall**
  - Estratégias gerais:
    - Allow-All
    - Deny-All

Uma boa opção é misturar ambas!

Segurança da Comunicação

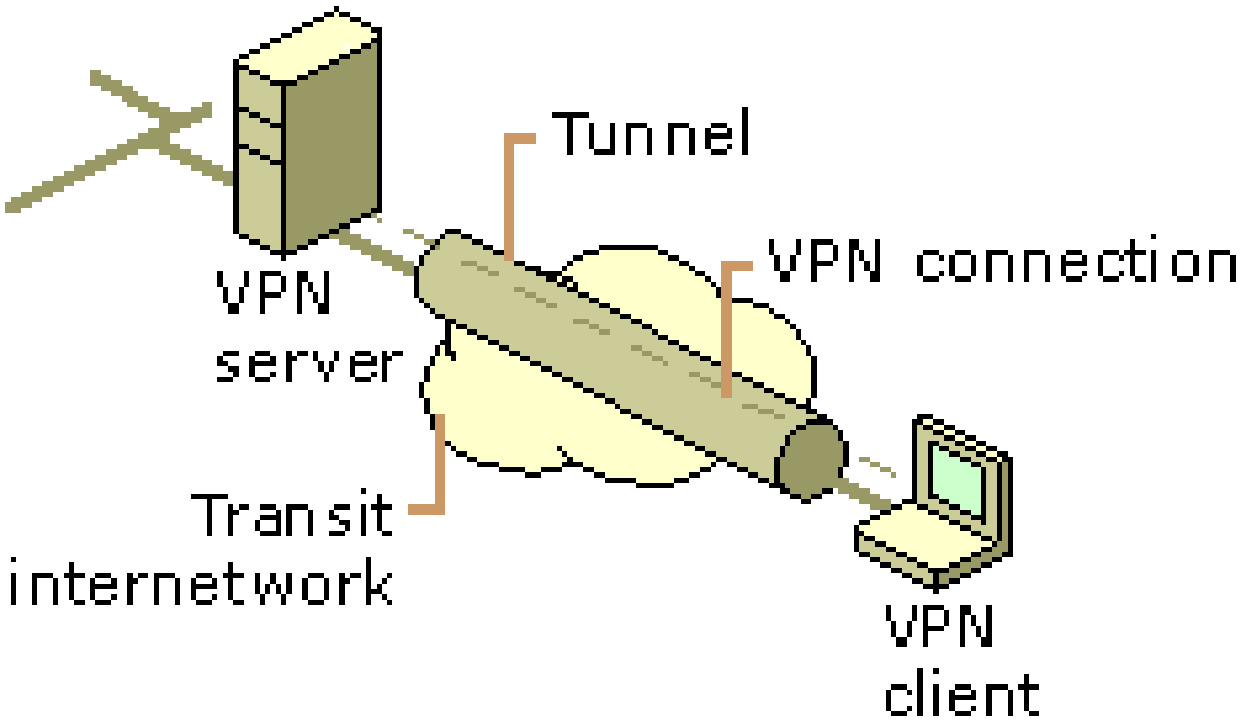
- *Deny network traffic on all IP ports.*
- *Except, allow network traffic on port 80 (HTTP).*
- *Except, from all HTTP traffic, deny HTTP video content.*
- *Except, allow HTTP video content for members of the Trainers group.*
- *Except, deny Trainers to download HTTP video content at night.*

Segurança da Comunicação

Medida para lidar com a segurança da comunicação

- **VPN**
  - É uma conexão onde o acesso e a troca de dados somente é permitido a usuários e/ou redes que façam parte de uma comunidade de interesse, que ocorre sobre uma infra-estrutura compartilhada.
  - É uma rede de comunicações privada construída sobre uma rede de comunicações pública (como por exemplo, a Internet).

Segurança da Comunicação



Segurança da Comunicação

- **VPN**
  - Motivação
    Redução de custo
- Rede Tradicional
  - Taxa de instalação
  - Custo mensal fixo
  - Tarifas por Km
  - Servidores de Acesso
  - Manutenção
  - Vários equipamentos

Segurança da Comunicação

- **VPN**
  - **Vantagens**
    - Facilmente Escalável
    - Rapidez na instalação de novos sites
    - Facilidade para aumentar a capacidade do link de comunicação
  - Gerenciamento/Controle
    - Autenticação de usuários
    - Privilégios de acesso
    - Segurança
    - Mudanças na Rede

Segurança da Comunicação

- **VPN**
  - Tunelamento
    - Permite tráfego de dados de várias fontes para diversos destinos em uma mesma infraestrutura
    - Permite trafegar diferentes protocolos em uma mesma infraestrutura a partir de encapsulamento
    - Permite garantia de QoS (Quality of Service) - tráfego de dados pode ser direcionado para destinos específicos

Segurança da Informação

- Como garantir a segurança da informação em IoT?
  - Confidencialidade
  - Integridade
  - Disponibilidade
  - Identificação/Autenticação
  - Privacidade
  - Confiança

Segurança da Informação

- Confidencialidade
  - Dispositivos não podem revelar informações protegidas a outros dispositivos próximos
  - Um dispositivo que detecta presença de pessoas, deve garantir que isso seja confidencial para não expor a outros que não tenha acesso/direito.
  - A transmissão para servidores deve ser feita considerando apenas o serviço de encaminhamento.
    - Não pode ler, não pode alterar

Segurança da Informação

- Integridade dos dados transmitidos
  - Um emissor que envia dados para o gateway (temperatura)
  - É preciso garantir que o dado da temperatura não seja alterada no meio do caminho até ser gravada em uma base de dados
  - A informação vista pelo usuário deve ser produto daquele dado coletado lá pelo sensor acoplado ao dispositivo

Segurança da Informação

- Disponibilidade
  - Exemplo: Se for necessário reprogramar um dispositivo com N sensores, preciso de garantias de que consigo acessá-lo.
  - *Digital twin* pode armazenar o comando antes de enviar, de atualizar algum programa armazenado no dispositivo, desligá-lo, reiniciá-lo, etc.

Segurança da Informação

- Identificação e Autenticação
  - Quem vai fazer o quê, como e onde?
  - Garantir identificar o dispositivo, e quem não autenticou não vai ter acesso à minha rede e aos meus dispositivos.
  - Em um ambiente não controlado com milhares de sensores, precisamos identificar quem envia, recebe, etc.
  - Se identifico um risco e comportamento estranho na rede preciso retirar a permissão de acesso àquele sensor

Segurança da Informação

- Privacidade
  - É o principal desafio da segurança do projeto de IoT
    - Quem está sendo monitorado no ambiente?
    - Quem interage com as máquinas?
      - Preciso garantir que somente coleto e acesso se tenho autorização
      - Somente as pessoas com essa autorização vai poder acessar a informação.

Segurança da Informação

- Confiança
  - O dispositivo que está enviando os dados é ele mesmo?
  - Aquela comunicação que o dispositivo faz até que o dado chegue ao servidor é garantida?
    - A mensagem não está sendo alterada, roubada.

Conclusão

- A segurança não é um software que vai ser instalado no sistema quando tudo estiver pronto
- Não é um módulo acoplado que vai garantir a segurança do projeto, das pessoas, dos dados, das informações
- Os dados e as informações coletadas e transmitidas
  - não deve comprometer a integridade de uma pessoa,
  - não pode derrubar um projeto em execução.
  - O dispositivo não vai ficar exposto, ficando acessível para outras pessoas e consequentemente vulnerável.

Referências

- KUROSE, J.; ROSS,K. W. **Redes de Computadores e a Internet,** 2016
- Zwicky, E; Cooper, Simon **– Contruindo Firewalls para a Internet.** O´Reilly, 2000
- **Internet Firewalls – UFRGS -** http://penta.ufrgs.br/redes296/firewall/fire.html

Atividade

- Disponível no Moodle conforme consta no cronograma da disciplina

Atividade

- Disponível no Moodle conforme consta no cronograma da disciplina