

## Aula 6

### IoT – Internet das Coisas

Prof. Gian Carlo Brustolin

1

### Conversa Inicial

2

### Segurança em IoT

- Como há muitas incertezas sobre IoT, as vulnerabilidades não são plenamente conhecidas
  - Introdução à segurança da informação
  - Aspectos gerais de segurança para IoT
  - Privacidade e IoT
  - Segurança em MQTT
  - Segurança em *fog* e *edge*

3

### Introdução à segurança da informação

4

### Introdução à segurança da informação

- Dado, informação e valor da informação
- Característica da informação segura
- Vulnerabilidade e ameaça
- Risco
- Ataques
- Contramedidas e triplo A

5

### Dado, informação e valor da informação

- Uso de IA em *smart cities*: após as fases de pré-tratamento e análise, os dados ganham o status de informação
- Informação é um bem com valor econômico
  - Graus de sigilo: informações públicas, reservadas ou confidenciais
  - O valor da informação cresce a cada transição entre esses graus

6

### Dado, informação e valor da informação

- Ciclo de vida: produção, manuseio, armazenamento, transporte e descarte
- Incidentes de comprometimento da informação

7

### Características da informação segura

- Confidencialidade
- Integridade
- Disponibilidade
- Autenticidade
- Irretratabilidade (não repúdio)
- Privacidade
- Auditabilidade

8

### Vulnerabilidade e ameaça

- Vulnerabilidades são fraquezas no tratamento da informação que podem gerar incidentes de comprometimento
- Quando um agente é capaz de explorar uma vulnerabilidade, há uma ameaça possível
- Uma ameaça não é sempre intencional – ameaças naturais

9

### Risco e impacto

- Estando presentes uma ameaça e uma vulnerabilidade, existe o risco de que um incidente rompa as características da informação segura
- Risco é a probabilidade de sucesso de uma ameaça
- Incidentes têm impactos diferentes

10

### Risco e impacto

- Matriz de gestão quantitativa de risco

| PROBABILIDADE | 5       | 5 | 10 | 15 | 20 | 25 |
|---------------|---------|---|----|----|----|----|
|               | 4       | 4 | 8  | 12 | 16 | 20 |
|               | 3       | 3 | 6  | 9  | 12 | 15 |
|               | 2       | 2 | 4  | 6  | 8  | 10 |
|               | 1       | 1 | 2  | 3  | 4  | 5  |
|               | 1       | 2 | 3  | 4  | 5  |    |
|               | IMPACTO |   |    |    |    |    |

Fonte: De Paulo et al., 2007.

11

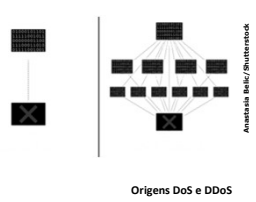
### Ataques

- Tipos de ataques
  - Ativos: buscam alterar características dos dados
  - Passivos: acessam indevidamente os dados, coletando informações reservadas ou confidenciais
- Contramedidas: além de reduzir o risco de ocorrência, caso haja sucesso, é preciso preparar técnicas de mitigação de impacto

12

### Ataques

- Ataques DoS e DDoS
  - Comuns em sites comerciais de internet, causando a "queda" do site
  - Tipos: volumétrico, de protocolo e de aplicação



Origens DoS e DDoS

Anastasia Balic/Shutterstock

13

### Contramedidas e triplo A

- Contramedidas: além de reduzir o risco de ocorrência, caso haja sucesso, é preciso preparar técnicas de mitigação de impacto
- Princípio do triplo A: autenticação, autorização e auditabilidade (*authentication, authorization, and accounting*)

14

### Aspectos gerais de segurança para IoT

15

### Confiabilidade, integridade e disponibilidade

- Confiabilidade: necessidade de que dados transmitidos entre dois dispositivos cheguem ao destino e possam ser decodificados
- Interface rádio eficiente e MAC capaz de recuperar a informação
- Integridade: garantia de que esses dados serão recebidos com o exato conteúdo que foram transmitidos
- Criptografia x simplicidade de alguns objetos IoT

16

### Confiabilidade, integridade e disponibilidade

- Disponibilidade
  - Modelos de modulação resilientes e por métodos de controle e correção de erros

17

### Segurança na camada de percepção

- Restrições de HW implicam limitações de software, impedindo implementações complexas voltadas à segurança
- Potencial de impacto de acesso indevido a sensores e atuadores é alto
- O risco foi comprovado pelo colapso da rede de distribuição de EE da Ucrânia em 2015
- Vulnerabilidades
  - HW – físicas ou lógicas (configurações)
  - SW – vulnerabilidade do SO em C

18

### Segurança na camada de rede

- Implementações de segurança clássicas são “pesadas” em demasia
  - Criptografia de dados na camada MAC
  - Autenticação na camada de aplicação

19

### Segurança e aplicação

- Não difere daquela para qualquer outro tipo de aplicação de nuvem
  - Com alta superfície de ataque
  - Alto impacto do acesso indevido a dados
  - Sub-redes não amistosas entre si
- Defesa do *data center* e das informações
  - LGPD

20

### Privacidade e IoT

21

### Privacidade e IoT

- Riscos envolvendo a camada de aplicação
  - Técnicos
  - Jurídicos, causados pela eventual quebra de privacidade de dados
- LGPD
- LGPD e IoT

22

### LGPD

- A LGPD estabelece limites à coleta e à utilização de dados pessoais no Brasil
  - Vincula a coleta e o uso de dados pessoais ao consentimento livre, informado e inequívoco, desde que expressamente utilizados para uma finalidade determinada (art. 2º)
  - Necessidade de que o cidadão tenha acesso livre e facilitado ao tratamento de seus dados, permitindo-se, a qualquer tempo, a reversão do consentimento (art. 9º)

23

### LGPD

- Dados que podem expor aspectos indesejados devem ser anonimizados (cap. II, seção II)
- Adoção de medidas de segurança, técnicas e administrativas de contenção (art. 46)
- Regras de boas práticas, de governança e mecanismos internos de supervisão e de mitigação de riscos compulsórios (art. 50)

24

### LGPD e IoT

- Dados são patrimônio privado individual e não podem ser coletados sem autorização
- Cidades inteligentes coletam dados não anônimos – devem ser descartados ou anonimizados de forma auditável
- Empresas envolvidas no fornecimento de serviços inteligentes precisarão de fortes investimentos em segurança e constantes avaliações de risco

25

### Segurança em MQTT

26

### Vulnerabilidades

- Foco em disponibilidade e não em integridade e confiabilidade não implementa
- Autenticação forte
  - ✓ Entidades espúrias podem autenticar
  - ✓ Ataque DoS derruba as válidas
- Nem criptografia
  - ✓ Vazamento
  - ✓ Contaminação por entidades espúrias

27

### Métodos de Hash

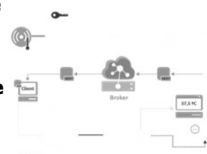
- Levam em conta as limitações dos dispositivos
- Rápidos e simples, podem garantir a integridade, não a confiabilidade
- Espúrio registrado pode mandar mensagens maliciosas desde que conheça o Hash
- Alternativa: HMAC (*keyed-hash message authentication code*)

Implementação de HMAC  
(Fonte: Dincoleand et al., 2019, p. 4)

28

### Métodos de Hash

- HMAC implica a troca de chave entre dispositivo e servidor
- Possível estender a segurança ao assinante final
- Distribuição da chave constitui-se em um novo problema



Implementação de HMAC fim a fim  
(Fonte: Dincoleand et al., 2019, p. 7)

29

### Métodos de Hash

- Distribuição de chave criptográfica para HMAC
- Estratégias clássicas utilizam chaves assimétricas
- Pré-distribuição de chave
  - ✓ Objeto novo sofrerá um login inicial, em uma entidade confiável, encarregada do pré-set dos dispositivos

30

### Predição de ataque

- Uso de processos de predição de anomalias na camada de percepção
- Distinguir um assinante malicioso daquele legítimo

31

### Predição de ataque

- Pequeno IDS residente no servidor próximo, evitando sobrecarga de processamento dos dispositivos
- Sem ACLs a solução baseia-se em IA e análise estatística
- Cria-se camada de segurança, antecessora da aceitação de solicitações MQTT, no servidor

32

### Segurança em modelos computacionais *fog* e *edge*

33

### Segurança em neblina

- Nesta arquitetura, a rede local de percepção se vê confinada em relação à WAN ou internet pelo concentrador
- O problema de segurança se vê dividido
  - É clássico entre concentrador e servidor de nuvem
  - Entre concentrador e objetos
    - ✓ Concentrador pode implementar contramedidas de firewall

34

### Segurança em borda

- O problema de segurança se vê dividido
  - É clássico entre concentrador e servidor de nuvem
  - Entre concentrador e objetos
    - ✓ Concentrador pode implementar contramedidas de firewall
  - Entre objetos
    - ✓ Há mais capacidade de processamento nos objetos, permitindo implementações de segurança

35

### Finalizando

36

Finalizando

- Buscamos examinar os desafios ligados à definição dos protocolos de análise de risco x impacto e na escolha de contramedidas
- O aspecto técnico está ainda sem soluções sedimentadas disponíveis
- O aspecto legal gera forte preocupação
- Ao concluirmos nossos estudos, entendemos que pode restar certa frustração, devido à impossibilidade de se oferecer certezas e métodos eficientes e consolidados

37

38