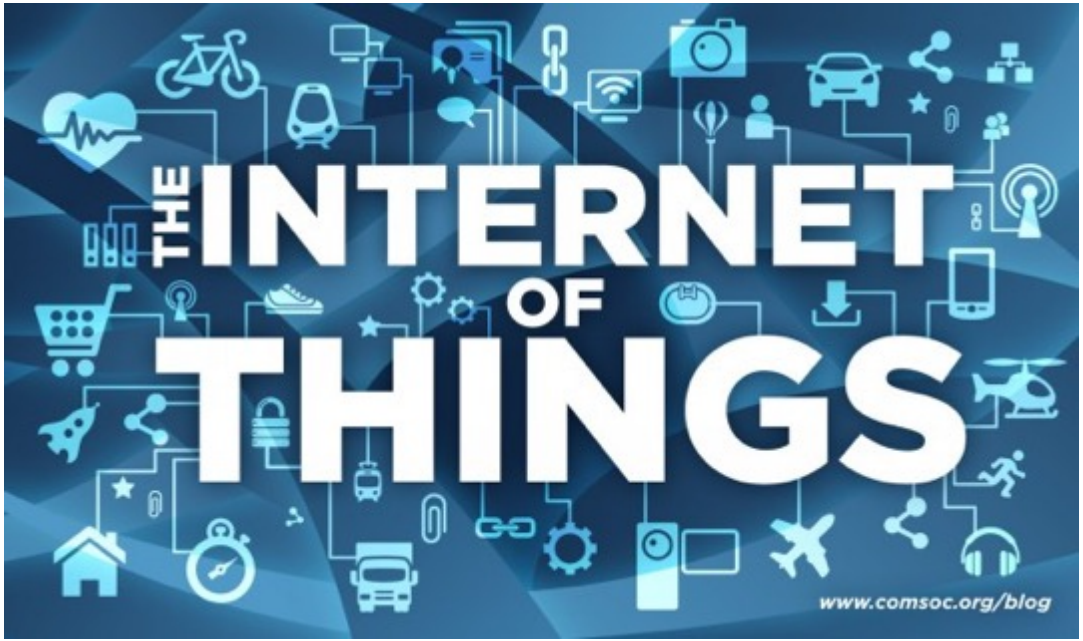
Gestão de Identidades na IoT: Desafios e Tendências

Profa. Dra. Michelle S. Wangham
Laboratório de Sistemas Embarcados e Distribuídos
Programa de Mestrado em Computação Aplicada
UNIVALI – Santa Catarina
wangham@univali.br

Internet das Coisas (IoT)



Infraestrutura de hardware, software e serviços que conectam objetos físicos, denominados como coisas, à rede.

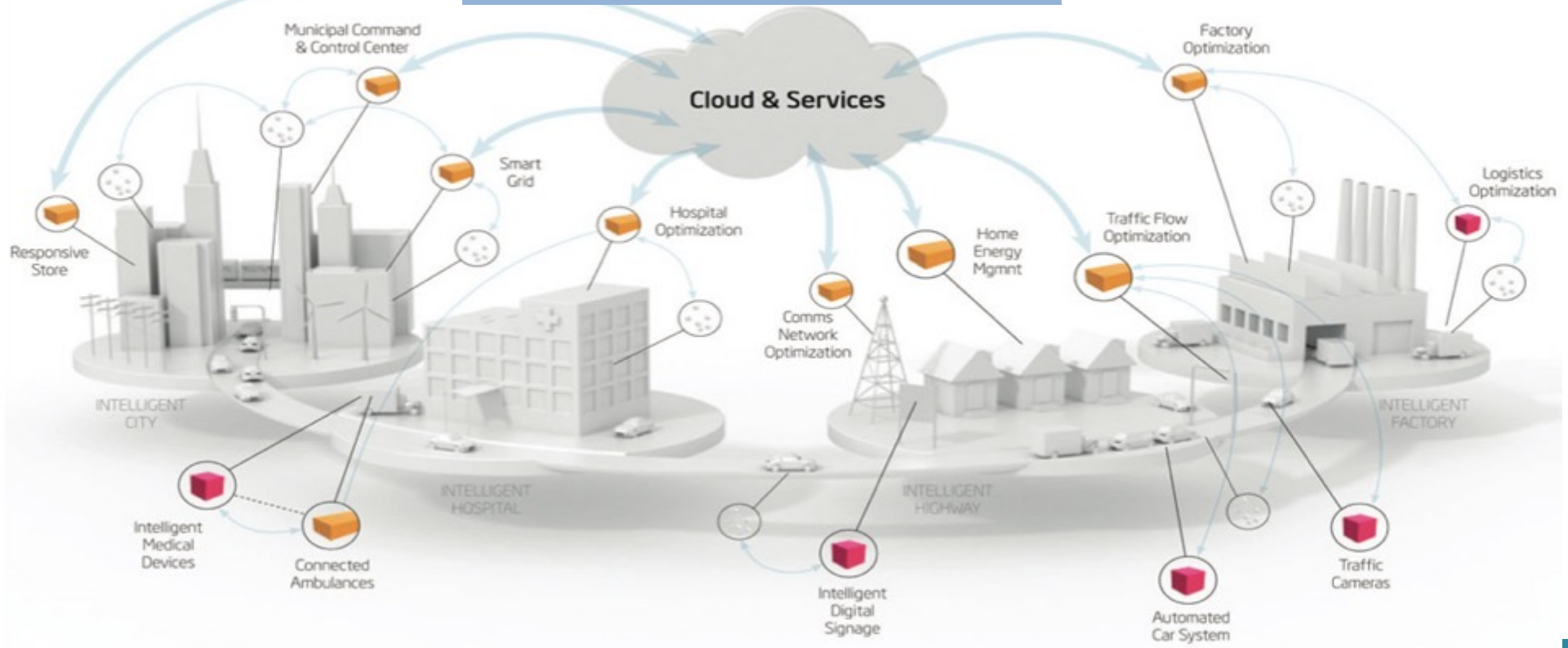
Coisas que interagem e cooperam entre si a fim de atingir um objetivo comum (métodos de endereçamento e protocolos padronizados)

Características das “Coisas”

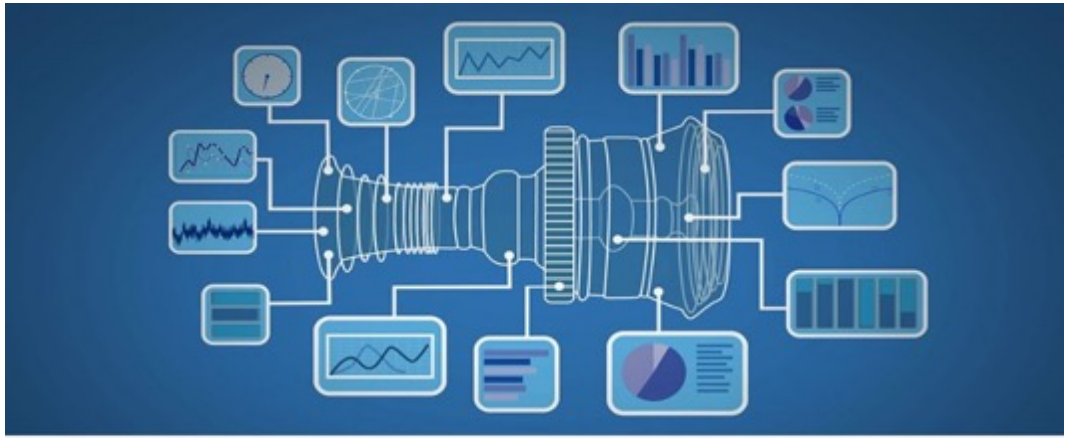
- Existência: existem no mundo real e virtual (CPS)
- Auto conhecimento: se comportam de maneira autônoma (*smart devices*)
- Conectividade (sem fio)
- Interatividade: D2D (M2M), D2P
- Dinamicidade: qualquer momento, lugar ou maneira. Entrar e sair da rede.
- Ciência do Ambiente: sensores para perceber as características dos ambientes

Cloud completa o conceito de IoT

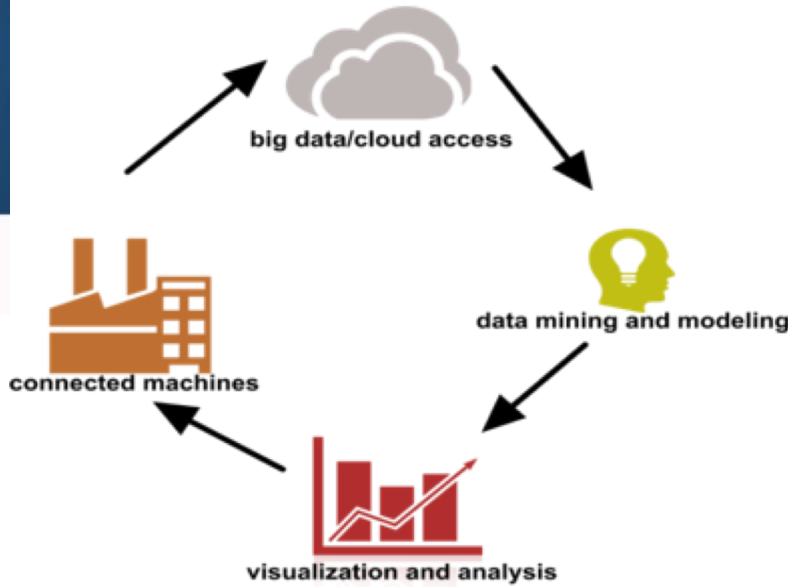
Sensoriamento ubíquo



IoT -> Big Data



200 sensors across the turbine generate 300 data points per second of performance and operation every hour.



Internet das Coisas:
Um Plano de Ação para o Brasil

- BNDES com o apoio do MCTIC: estudo para o diagnóstico e a proposição de plano de ação estratégico para o país em Internet das Coisas
- Conduzido pelo Consórcio McKinsey/Fundação CPqD/ Pereira Neto Macedo
- "Acelerar a implantação da Internet das Coisas como instrumento de **desenvolvimento sustentável** da sociedade brasileira, capaz de aumentar a competitividade da **economia**, fortalecer as **cadeias produtivas** nacionais, e promover a melhoria da **qualidade de vida.**"

https://bit.ly/2kfqRJ4

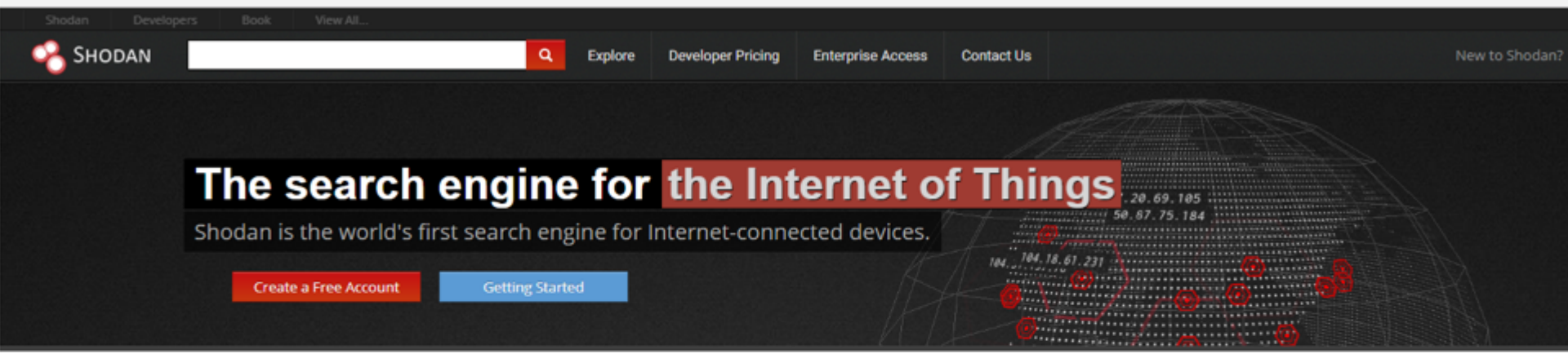
Regulatório, Segurança e Privacidade

- Endereçar questões da **regulamentação de Telecom** com vistas a acelerar o desenvolvimento de aplicações IoT
- Estruturar a criação de um **marco regulatório de proteção de dados pessoais** adequado para fomentar a inovação e a proteção aos direitos individuais
- Identificar e tratar **questões regulatórias específicas nas verticais priorizadas**
- Estabelecer desenho institucional adequado para enfrentar os desafios em **privacidade e segurança** para IoT

FONTE: Point

Segurança na Internet das Coisas

Nossas coisas e dados estão seguros na Internet das Coisas?



The search engine for Power Plants

The search engine for Webcams

The search engine for Refrigerators

The search engine for Buildings

Segurança e Privacidade na IoT

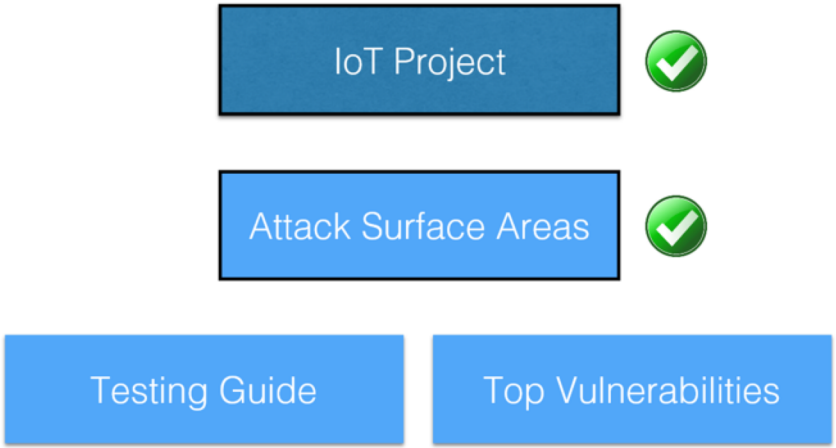
- Comportamento autônomo das coisas, recursos computacionais restritos, comunicação sem fio
- Propriedades de Segurança
  - Confidencialidade
  - Integridade
  - Disponibilidade
  - Autenticidade
- Privacidade
- **Segurança deveria ser um grande obstáculo!**

Por que as “coisas” são tão vulneráveis?

- **Segurança não é prioridade mesmo em dispositivos de segurança!**
- Sistemas operacionais simples: não possuem mecanismos adequados de proteção **e não sofrem atualizações**
- Inúmeras vulnerabilidades nos softwares embarcados (Aidra, Bashlite e Mirai botnets, veículos, *smartphones*, dispositivos médicos, centrais de alarmes, sistema aquecimento, sistemas elétricos)
- Desejo das empresas fabricantes de equipamentos de manter *backdoors*
- Monitoramento governamental em larga escala
- Protocolos sem criptografia ou mal implementados
- Dispositivos expostas diretamente na Internet (IPv6)
- **Falta ou falha de autenticação e controle de acesso**

The **Open Web Application Security Project** (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications and APIs that can be trusted.

*The **OWASP Internet of Things Project** is designed to help **manufacturers, developers, and consumers** better understand the **security issues** associated with the Internet of Things, and to enable users in any context **to make better security decisions** when building, deploying, or assessing IoT technologies.*



https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

HELPING SECURE THE INTERNET OF THINGS WITH THE

OWASP INTERNET OF THINGS TOP 10

VULNERABILITY CATEGORIES

Main | OWASP Internet of Things Top 10 for 2014 | Project Details

The OWASP Internet of Things Top 10 - 2014 is as follows:

- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

I2 | Insufficient Authentication/Authorization

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
Consider anyone who has access to the web interface, mobile interface or cloud interface including internal and external users.	Attacker uses weak passwords, insecure password recovery mechanisms, poorly protected credentials or lack of granular access control to access a particular interface. Attack could come from external or internal users.	Authentication may not be sufficient when weak passwords are used or are poorly protected. Insufficient authentication/authorization is prevalent as it is assumed that interfaces will only be exposed to users on internal networks and not to external users on other networks. Deficiencies are often found to be present across all interfaces. Many Issues with authentication/authorization are easy to discover when examining the interface manually and can also be discovered via automated testing.		Insufficient authentication/authorization can result in data loss or corruption, lack of accountability, or denial of access and can lead to complete compromise of the device and/or user accounts.	Consider the business impact of compromised user accounts and possibly devices. All data could be stolen, modified, or deleted. Could your customers be harmed?

I2 | Insufficient Authentication/Authorization | Testing

Is My Authentication/Authorization Sufficient?

Checking for Insufficient Authentication includes:

- Attempting to use simple passwords such as "1234" is a fast and easy way to determine if the password policy is sufficient across all interfaces
- Reviewing network traffic to determine if credentials are being transmitted in clear text
- Reviewing requirements around password controls such as password complexity, password history check, password expiration and forced password reset for new users
- Reviewing whether re-authentication is required for sensitive features

Checking for Insufficient Authorization includes:

- Reviewing the various interfaces to determine whether the interfaces allow for separation of roles. For example, all features will be accessible to administrators, but users will have a more limited set of features available.
- Reviewing access controls and testing for privilege escalation

- Lack of Password Complexity
- Poorly Protected Credentials
- Lack of Two Factor Authentication
- Insecure Password Recovery
- Privilege Escalation
- Lack of Role Based Access Control

I2 | Insufficient Authentication/Authorization | Make It Secure

How Do I Make My Authentication/Authorization Better?

Sufficient authentication/authorization requires:

1. Ensuring that the strong passwords are required
2. Ensuring granular access control is in place when necessary
3. Ensuring credentials are properly protected
4. Implement two factor authentication where possible
5. Ensuring that password recovery mechanisms are secure
6. Ensuring re-authentication is required for sensitive features
7. Ensuring options are available for configuring password controls

Please review the following tabs for more detail based on whether you are a Manufacturer, Developer or Consumer

I5 | Privacy Concerns

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
Consider anyone who has access to the device itself, the network the device is connected to, the mobile application and the cloud connection including external and internal users.	Attacker uses multiple vectors such as insufficient authentication, lack of transport encryption or insecure network services to view personal data which is not being properly protected or is being collected unnecessarily. Attack could come from external or internal users.	Privacy concerns generated by the collection of personal data in addition to the lack of proper protection of that data is prevalent. Privacy concerns are easy to discover by simply reviewing the data that is being collected as the user sets up and activates the device. Automated tools can also look for specific patterns of data that may indicate collection of personal data or other sensitive data.		Collection of personal data along with a lack of protection of that data can lead to compromise of a user's personal data.	Consider the business impact of personal data that is collected unnecessarily or isn't protected properly. Data could be stolen. Could your customers be harmed by having this personal data exposed?

I5 | Privacy Concerns | Testing

Does My Device Present Privacy Concerns?

Checking for Privacy Concerns includes:

- Identifying all data types that are being collected by the device, its mobile app and any cloud interfaces
- The device and it's various components should only collect what is necessary to perform its function
- Personally identifiable information can be exposed when not properly encrypted while at rest on storage mediums and during transit over networks
- Reviewing who has access to personal information that is collected

- Collection of Unnecessary Personal Information

I5 | Privacy Concerns | Make It Secure

How Do I Prevent Privacy Concerns?

Minimizing privacy concerns requires:

1. Ensuring only data critical to the functionality of the device is collected
2. Ensuring any data collected is properly protected with encryption
3. Ensuring the device and all of its components properly protect personal information
4. Ensuring only authorized individuals have access to collected personal information

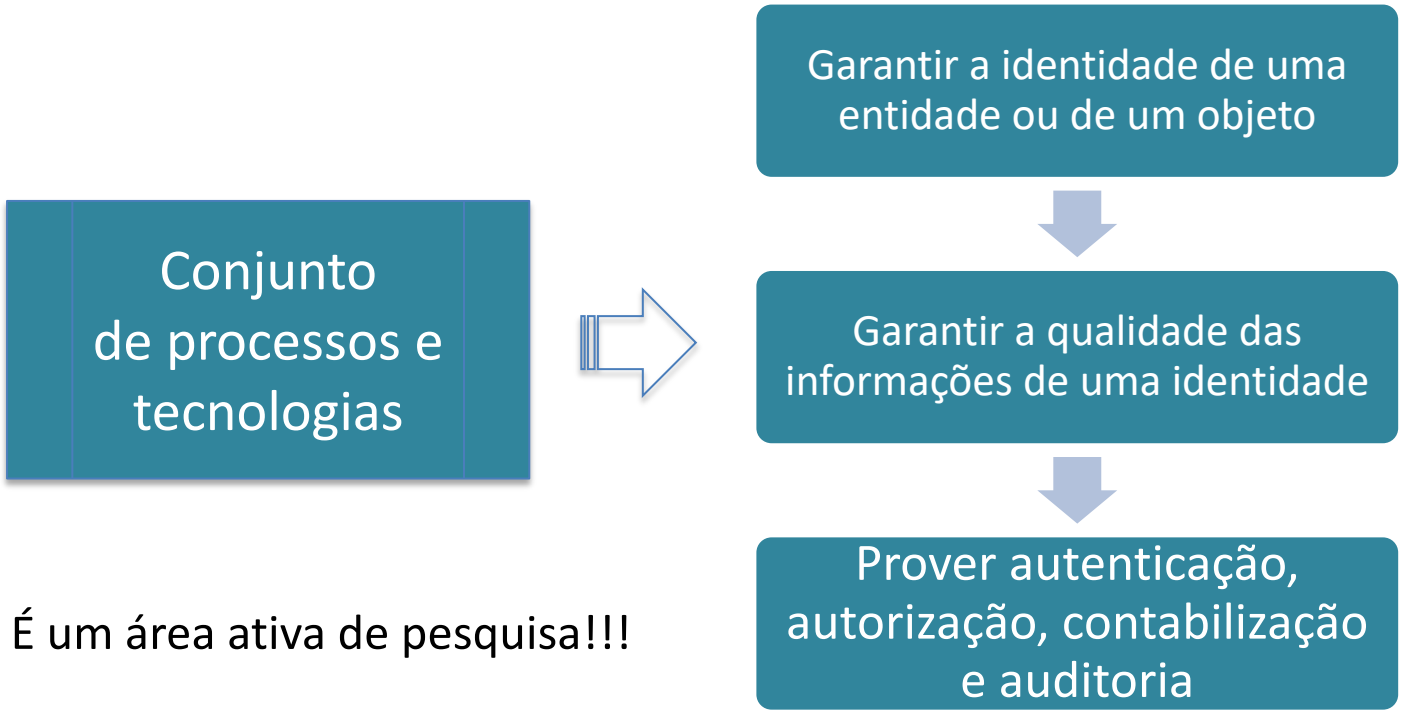
Please review the following tabs for more detail based on whether you are a Manufacturer, Developer or Consumer


SECURITY
DELEGATION
APPLICATIONS
PLATFORM
AUTHORIZATION
DIGITAL
IDENTITY
PROTECTION
INCREASE
COST
MANAGEMENT
SERVICES
AUTHENTICATION
SYSTEM
ACCESS
ROLES
PRODUCTIVITY
TECHNOLOGY
ENTITY
PRIVILEGES
CERTIFICATES
DECREASE

Identidades Digitais

- Uma identidade pode consistir de:
  - **Identificador**: conjunto de dígitos, caracteres e símbolos usado para identificar unicamente uma identidade.
- **Credenciais**: um objeto que pode ser usado para provar uma identidade. Ex: certificados X.509, senhas, tokens entre outras.
- **Atributos**: um conjunto de dados que descreve as características fundamentais de uma identidade.

Gestão de Identidade (Identity Management – IdM)



É um área ativa de pesquisa!!!

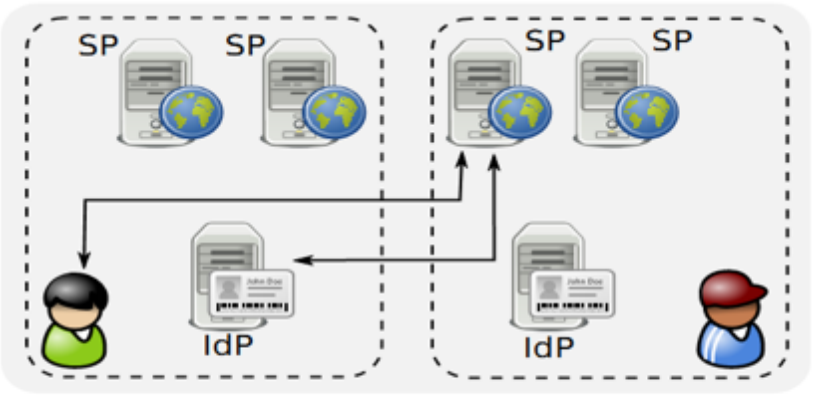
Preservar a Privacidade

Sistema de Gestão de Identidades

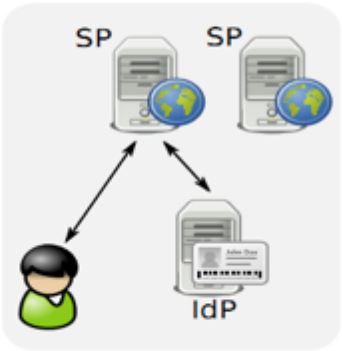
- Elementos
  - Usuários ou Objetos
  - Identidades
  - Provedores de Identidades
  - Provedores de Serviços

Modelos de Gestão de Identidades

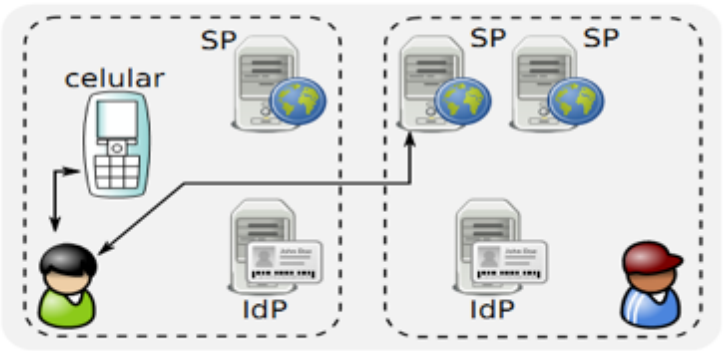
(a) Tradicional



(b) Federado



(c) Centralizado



(d) Centrado no usuário

Identidade de Objetos/CPS

- Identificador? Único? Relacionado com o fabricante? Endereço IPv6?
- Atributos diversos
  - Nome de exibição
  - Contato do administrador
  - Organização e unidade organizacional
  - Descrição
  - Tipo de dispositivo
  - Referência de localização física, latitude, longitude, altitude
  - Fixo ou móvel
  - Exposição (indoor ou outdoor)
  - Status (online ou offline)

Faltam padrões!

Garantir a qualidade da identidade

- Registro de dispositivos em um Provedor de Identidade (IdP) ou em um SP
  - Fabricação (alguns atributos, credenciais)
  - Dono do usuários (complementar atributos)
- Definição de credenciais (PIN, senhas, segredos, chaves)
- Proteção das credencias (elemento seguro, TEE)

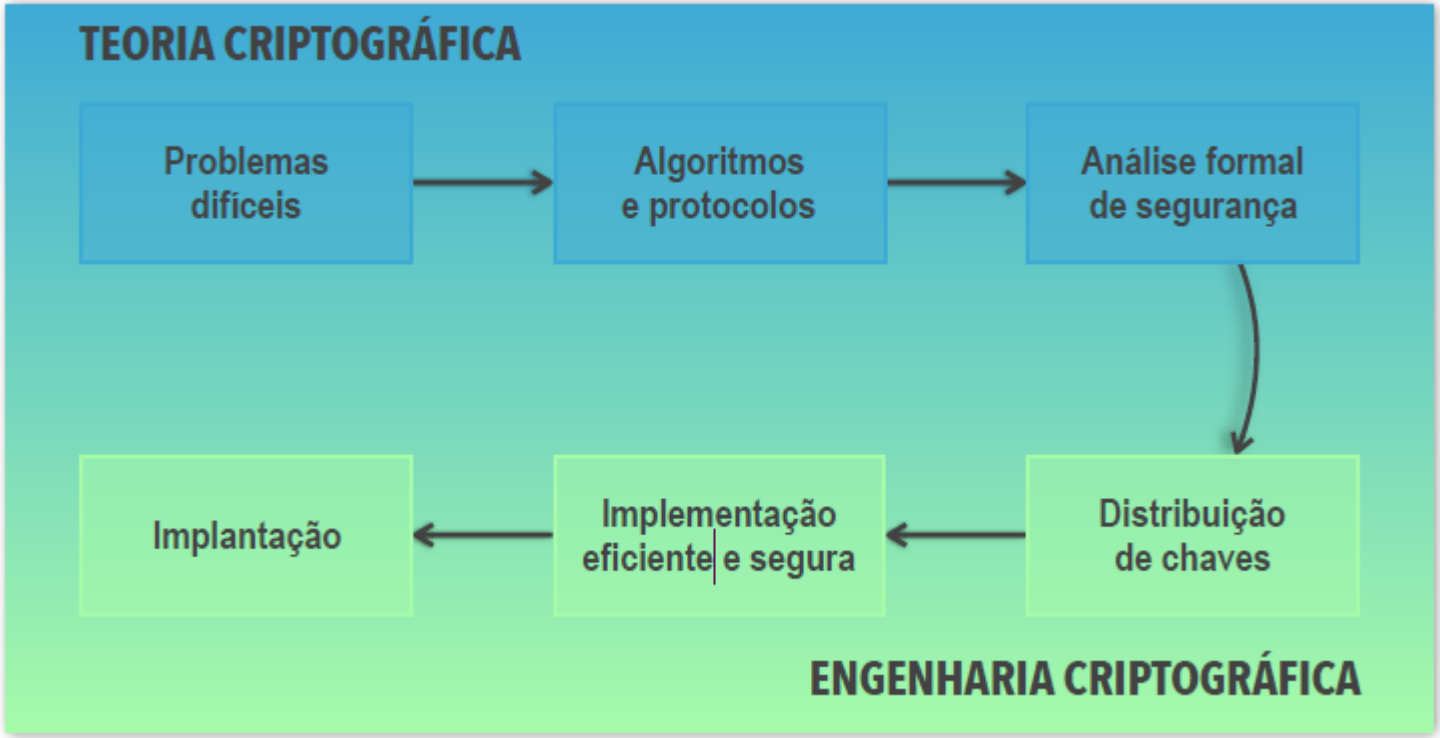
Autenticação de usuários na IoT

- **Autenticação tradicional (silo) baseado em PIN, ou senha** e chaves (certificados).
- Autenticação centralizada baseada em uma terceira parte confiável (IdP ou um KDC)
- Autenticação federada (nem sempre cliente e SP estão no mesmo domínio e confiam no mesmo IdP): baseada no OpenId Connect e no SAML
- Recomendação para o uso de **autenticação multifator e autenticação contínua**

Autenticação de Dispositivos (D2D)

- Certificados digitais X.509 (cripto assimétrica)
- *Tokens* assinados com chaves compartilhadas (Azure IoT)
- Criptografia simétrica (baseado ou não em KDC)
- Criptografia assimétricas alternativas (*certificateless* e *Identity-based cryptograph*)
- Autenticação multifator?

Aspectos em relação a criptografia



Fonte: https://bit.ly/2x4ypr5

Criptografia Leve

- Técnicas criptográficas customizadas para uma aplicação específica e cuidadosamente projetadas para serem eficientes
- Encriptação simétrica: LS Designs [Grosso et al. 2014], redes modernas de Feistel e Adição-Rotação-Soma (ARX) [Dinu et al. 2016], **PRESENT** [Reis et al. 2017]
- MACs curtos usando SipHash OU assinaturas digitais construídas a partir de funções de resumo com entradas curtas (não resistentes a colisão) ou funções resistentes à colisão como BLAKE2.
- Criptografia assimétrica de curvas elípticas (ECC)

Fonte: https://bit.ly/2x4ypr5

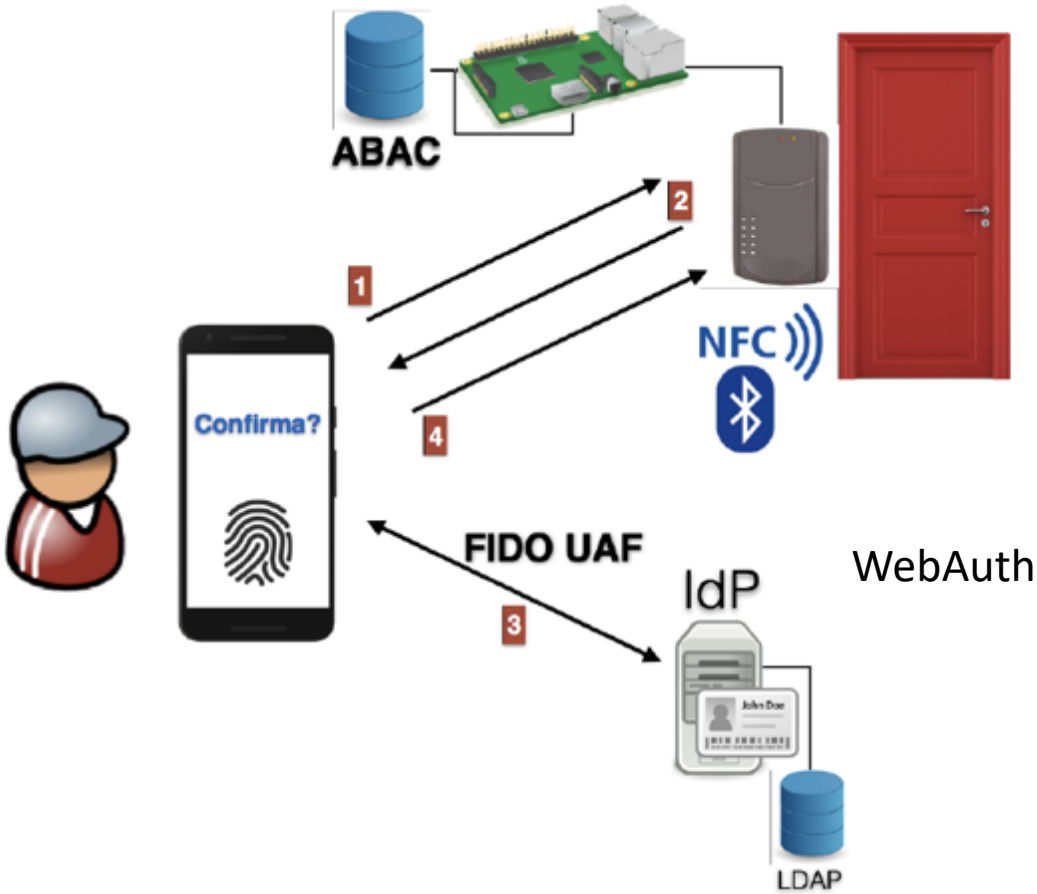
Autorização

- Dispositivos que oferecem serviços (SP)
- Se um dispositivo for acessado de forma indevida, há uma chance de que essa violação afete o mundo físico arriscando o bem-estar das pessoas e até mesmo a vida
- Modelos de controle de acesso: DAC (ACL), RBAC, ABAC
- Modelo de gestão de políticas de acesso aos dispositivos (*outsourcing* ou *provisioning*)
  - PDPaaS na nuvem
  - PDP no dispositivo
- **Uso do OAUTH 2.0** na IoT: HTTP, MQTT
- Uso do SAML/XACML (HTTP)

Privacidade na IoT

- Questão que ainda precisa ser mais discutida!
- É preciso proteger informações sensíveis nos dispositivos (dados pessoais - atributos da identidade)
  - Segurança jurídica para a proteção de dados pessoais (não vai resolver a questão)
- Como implantar o **consentimento do usuário** na manipulação de seus dados pessoais na IoT?
- Canais seguros, Autenticação e controle de acesso robustos: evitar vazamento de dados sensíveis
- Registro de eventos para responsabilização (SIEM)
- Certificação de dispositivos (auto)

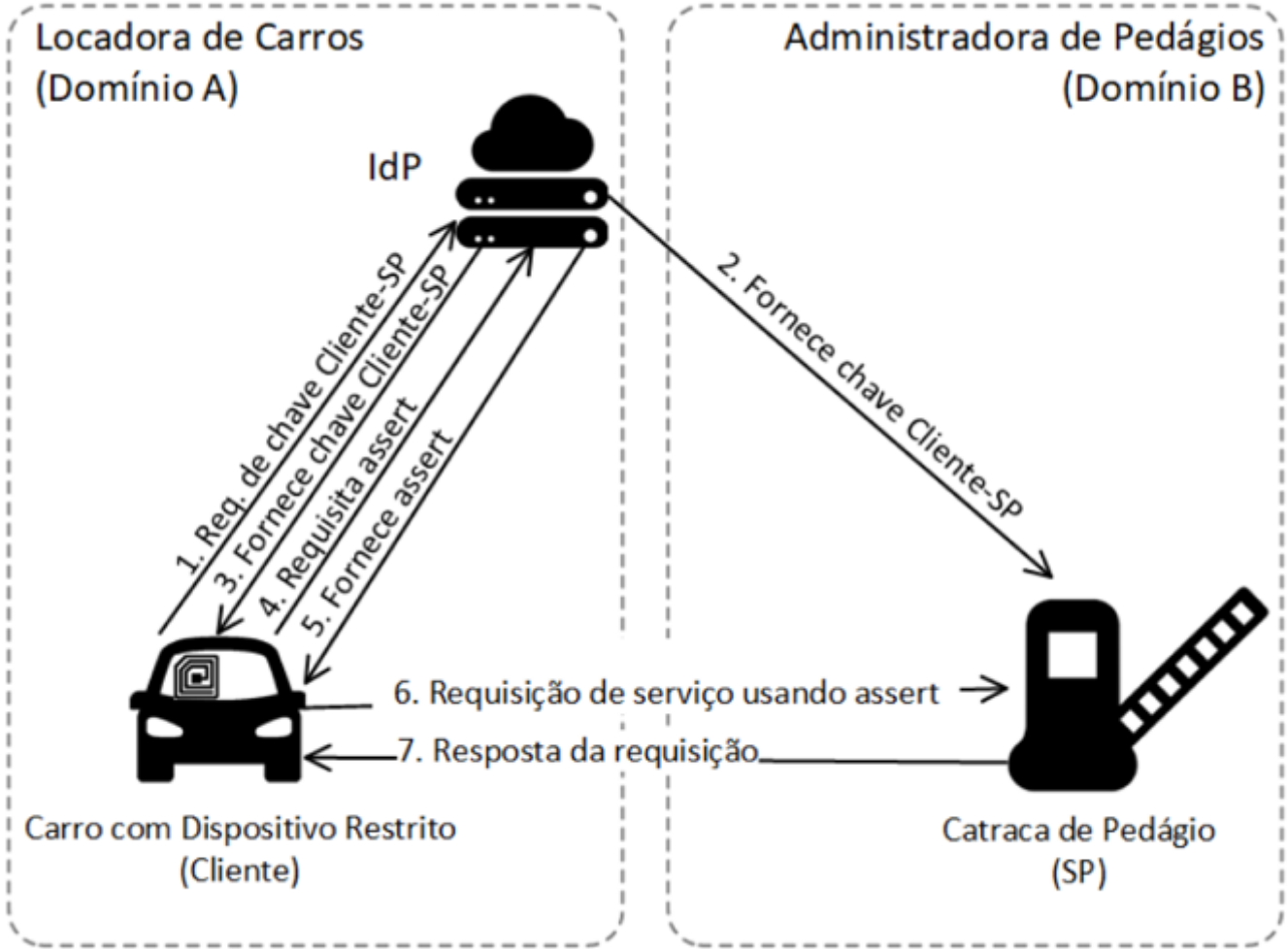
Estudo de Caso Projeto GT-Ampto (RNP)



WebAuthn (W

Estudo de Caso Protocolo FLAT (GT - RNP)

https://bit.ly/2KNkpEf



Conclusão

- Autenticação: existem soluções faltam ser utilizadas + pesquisas exploratórias (novas)
- Autorização: faltam pesquisas exploratórias
- Privacidade: ampliar a discussão academia, industria, judiciário, agências privadas certificadoras, agências reguladoras.
- IdM testbed: GidLab (RNP)
- *Startups*: prover soluções de IdM para IoT

Gestão de Identidades na IoT: Desafios e Tendências

Profa. Dra. Michelle S. Wangham
Laboratório de Sistemas Embarcados e Distribuídos
Programa de Mestrado em Computação Aplicada
UNIVALI – Santa Catarina
wangham@univali.br