Evolution of Cloud Computing
Delivering assurance into the world of tomorrow

Raj Samani
EMEA CTO McAfee, CIO Cloud Security Alliance
SOA is Cloud Computing?

End customers for cloud will demand an SOA approach

Demands for greater assurance
The Connected Home – The Last Decade
Typical Connected Home, Year 2000

- Master Bedroom
- W.I.R.
- Laundry
- Master Bathroom
Typical Connected Home, Year 2000

2013
In fact the cloud will be MORE!

...forget just using it for ‘dumb’ storage

it has to be MUCH more...
M-Cloud services usage by public authorities

- IaaS
- PaaS
- SaaS

- Mosty This
- Not Much of These Yet
- Lots of This

- REHOST
- REFACTOR
- REVISE
- REBUILD
- REPLACE
Some applications

251M smart meters installed - 535M by 2015...

Lots of Data to be analysed...
Peak = 7.18 kW
Mean = 0.49 kW
Daily load factor = 0.07
Energy consumption = 11.8 kWh
Everything is Connected!
Further stakeholders include those that exert pressure on security and privacy within the ‘Grid’. Implementation of an end-to-end secure solution within the modern energy infrastructure is complicated with the number of natural and technical participants and system components within the ‘Grid’. At appropriate levels, standards need to be “Smart Grid” ready in order to ensure, that remaining SGIS related risks are acceptable at all times.

Supply Chain

Grid Operators

- Suppliers of Grid Hardware
- Smart Grid Customers
- Comms Providers
- ICT Providers
- ISVs
- Testing Organizations
- Internet Service Providers
- Energy Suppliers
- Installation Companies

Stakeholders that facilitate the broader metering infrastructure

Stakeholders that comprise of the advanced metering infrastructure

Responsible for installation of meters, managing the network and ensuring security and privacy requirements set by broader stakeholders
Extending the McAfee 3x3 model we see multiple layers of data types which may not only traverse the multiple zones but also rest or transmit through multiple stakeholders enforcing the need for strong data control.
Objective: To protect confidential, and personal information establishing trust relationships with third parties.

- Identity across deployment platforms
- End-to-end message security required as messages can may traverse across trust zones.
- Access to be provided to information (and systems) based on business drivers.
- Various aspects of security need to be enforced at the ESB to ensure valid and secure access to systems and data.
- To consider the appropriate governance, risk, and compliance measures to address a variety of legal and regulatory aspects.
## Future requirements

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>SOA</th>
<th>CC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Linking</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Standard Protocols for Access</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Dynamic Discovery</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Relative Autonomy</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Trust Chain</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Federation</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>On-demand self-service</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Ubiquitous Network Access</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Multi-tenancy</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Rapid Elasticity</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Measured Service</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

Source: IBM
Future Security

- Dynamic Attestation
- 3rd Party Access
- End to End validation
- Real-time assurance
- CSP
- Internal
Whose role is it?

The lower down the stack the Cloud provider stops, the more security the consumer is tactically responsible for implementing & managing.
Contact

• Help us secure cloud computing
• www.cloudsecurityalliance.org
• info@cloudsecurityalliance.org
• LinkedIn: www.linkedin.com/groups?gid=1864210
• Twitter: @cloudsa

• Twitter: @Raj_Samani    @CyberGridBook