Forces at Work
Distributed Systems Industry Perspectives

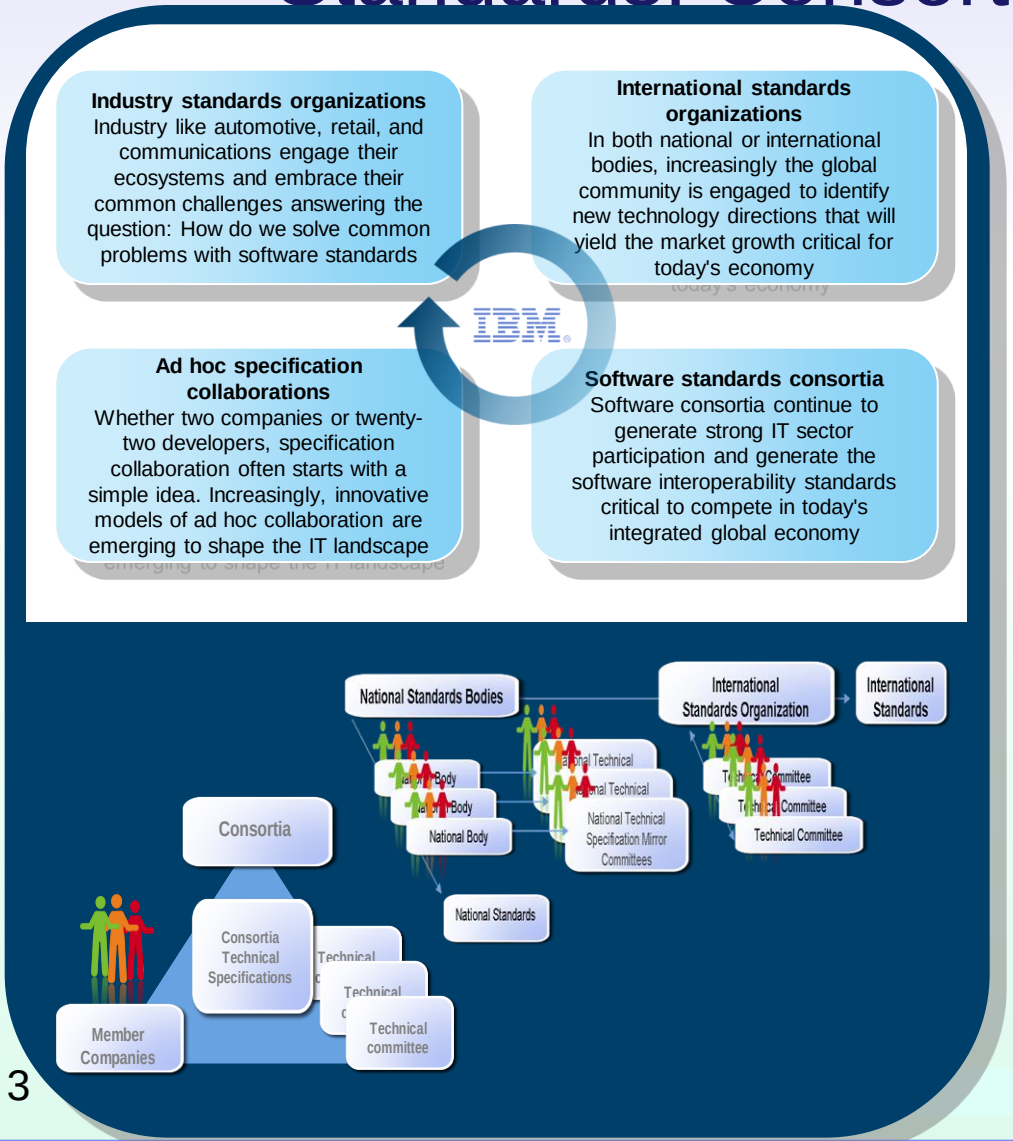
Standards Challenges and Cybersecurity: Implications for Distributed Systems (Business Infrastructure, Cloud Computing, Smart Grid/Smart Cities) and User Privacy

Heather Kreger
CTO International Standards, IBM
Nov 20, 2014

Agenda

- So Many Kinds of Standards
- Cloud Standards – the land grab
- Collaboration on New Cloud Computing Vocabulary Cloud Reference Architecture
- Changing drivers for Cloud standards
- Observations
- Standards education challenges

So many ways to create Standards International Standards, Consortia, Open Source



- There are many ways to develop standards ranging from very informal, adhoc work to very formal international standards.
- **Most standards orgs we work with are consortia** – W3C, OASIS, Open Group, etc,
  - Participate as IBM experts
- There are only **3 International Standards** organizations, *de jure,* as recognized by the UN:
  - **ISO, IEC, and ITU.**
  - Participate as national body experts
- Consortia and International technology discussions often run concurrently
- Competitive landscape grabbing for new trends in Cloud, Big Data, IoT, etc.
- Alignment of consortia and International efforts can influence outcomes
- International standards activity continues to attempts to anticipate IT industry developments ´JTC1 & ITU-T)

ISO/IEC and ITUT Cloud Activities

Land grab for any shiny new trends – Need to ensure common base for Regulation, Communication, SLAs, Standards, and Interoperability

ISO/IEC Cloud Activities

ISO/IEC JTC1 SC38 DAPS – WS, SOA, Cloud Cloud & ITU-T

- Cloud RA & Vocabulary –
- Cloud services SLA standard in progress
- Cloud Interoperability and Portability
- Cloud Data and its Flow

- **ISO/IEC JTC1 SC27 –Security**
  - 27017 and 27018 on cloud security and privacy
- **ISO/IEC JTC1 SC07 – SW Engineering**
  - ITIL and Cloud Governance

- JTC1-ITUT Joint work: Cloud Vocabulary & Cloud RA - 2014!
- Cloud Security (SC27-SG17) joint initiating
- Consortia – DMTF, Open Group, OASIS,

ITU-T Cloud Activities

ITU-T SC13 WP6 Cloud Computing (FTO)

- **JOINT** - Cloud computing ecosystem & Cloud functional architecture, infrastructure & networking
- **NOT JOINT** - Cloud computing resource management & virtualization
- New Questions (projects) Proposed – overlaps SLA & IoT

SG17 Security (not joint) - Cloud security Specs under development

No influence on: Resource Management, Cloud Security in ITUT

ITU-T & ISO/IEC SC38 Joint CCRA and Vocabulary

Agreed on by ISO/IEC JTC1 and ITUT as foundation for Cloud Computing in IT and Telecommunications industries.

NIST CCRA and IBM CCRA V2 submitted as input

Now published:

Cloud Computing Reference Architecture (ISO/IEC 17789)

Cloud Computing Vocabulary (ISO/IEC 17788)

Defines roles, activities they perform, functional architecture that identifies technical components needed to perform activities.

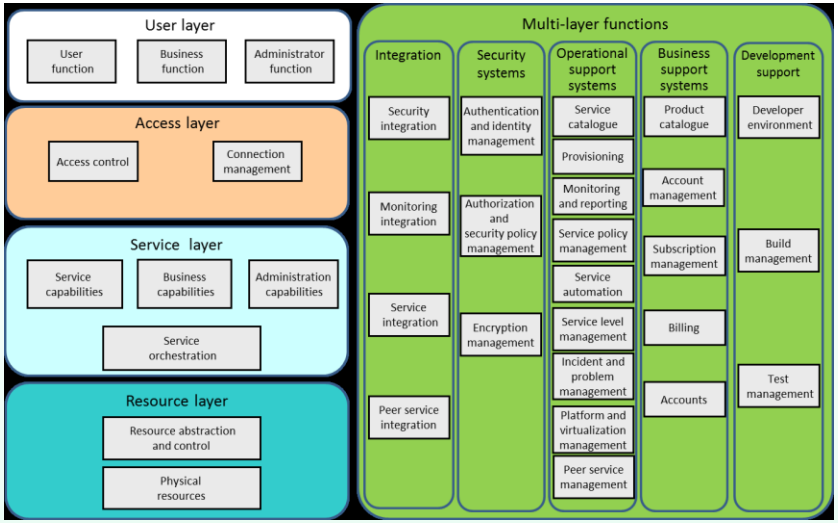
Activities map to common patterns and use cases.

Aspects adopted include auditability, availability, governance, interoperability, maintenance & versioning, performance, portability, protection of PII, regulatory, resiliency, reversibility, security.

Components to support Aspects categorized in *Multi-layer functions* under Integration, Security systems, OSS, BSS, Development

Cloud Computing Vocabulary (ISO/IEC 17788)
http://standards.iso.org/ittf/PubliclyAvailableStandards/c060544_ISO_IEC_17788_2014.zip

Cloud Computing Reference Architecture (ISO/IEC 17789)
http://standards.iso.org/ittf/PubliclyAvailableStandards/c060545_ISO_IEC_17789_2014.zip



Suppliers, customers, and consortia around the world were involved in the development of these standards, including Microsoft, Oracle, VMWare, HP, Dell, Fujitsu, Cisco, EMC, Hitachi, CA, Huawei, France Telecom Orange, AT&T, China Mobile, Intel, Open Group, DMTF, and government organizations from the US (NIST), China and Korea

Changes in Drivers for Standards

Cloud Computing is Catalyzing Governments

Governments using Cloud **NEED** and are driving:

- Cloud (security) certification
- Enforceable SLA terms
- Privacy measures

Shared observations:

- Local computing and physical security measures no longer assured
- Significant increase in visible and publicized security & privacy concerns

- Countries look to protect both government and citizen data
- Cloud offers significant cost benefits leading to government mandates to use cloud services
  - but **SAFELY**
- Lack of Cloud SLA, Privacy & Security standards cited

Governments establishing requirements:

- Requirements range from guidelines to compliance & certification
- Potential impact on businesses in all countries
  - impact **NOW** in Europe, China

Industry doesn't **NEED** standard SLAs like Governments

- Current SLAs very custom or boiler – SLAs don't impact ability to compete or change providers.
- Causes lag in consortia work
- Death by a thousand SLAs

Observations

- Standards essential for business and distributed computing landscape for Industry and Governments
- Standards and regulation will be part of every business's day to day operations
- Standards on the bleeding edge – shiny syndrome
- Challenges
  - Managing influence and control across countries and cultures
    - Competing interests – eg control of WWW
  - Coordinating international, consortia and … open source
    - Competing interests for industry and governments

- Shiny drivers and land grabs under way–
  - Big Data and analytics – everyone needs but some trepidation about about access to data, value from analytics, privacy…
  - Smarter everything – Cities need
  - IoT – foundation for Smarter* and drives Big Data

How can education help

We spend an in ordinate amount of time educating executives and new players on standards

Lack of appreciation of value

Its an expense.. Not perceived as driving value

Standards are not part of the default set of memes and tools we look at as part new shiny opportunities and challenges

Standards expertise is being lost – retiring, reducing standards staffing

Need unbiased education

QUESTIONS?