From misconceptions to a failure – security and privacy in US cloud computing FedRAMP program

Special research prepared by Rubos, Inc. team:
Mikhail Utin, PhD, CISSP and Daniil Utin, MS
(We do independent research on security matters in various domains)

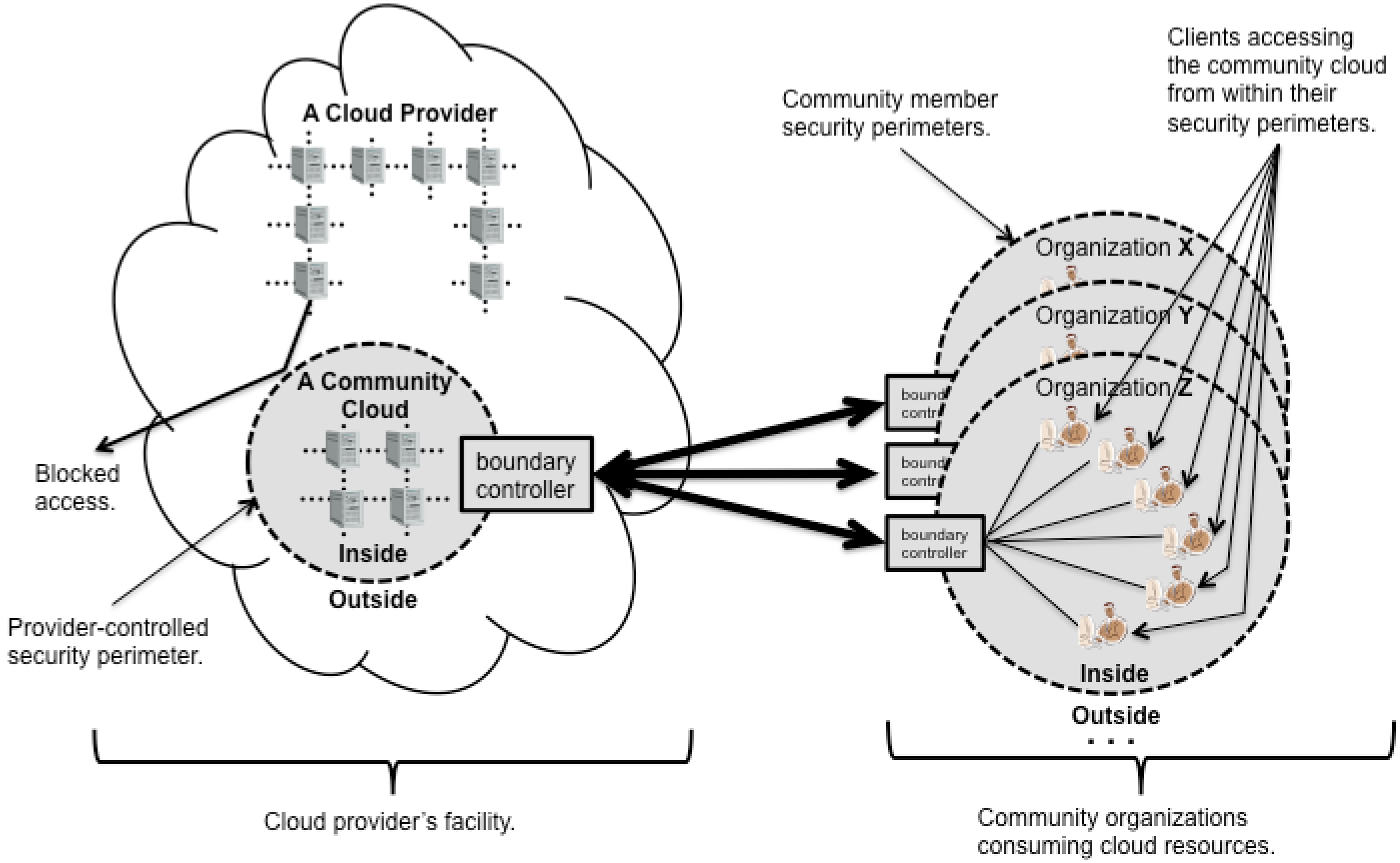
Prepared for DeepSec 2013
Presented by Mikhail Utin

(Questions will be answered after the presentation. Please, submit them to the speaker in writing)

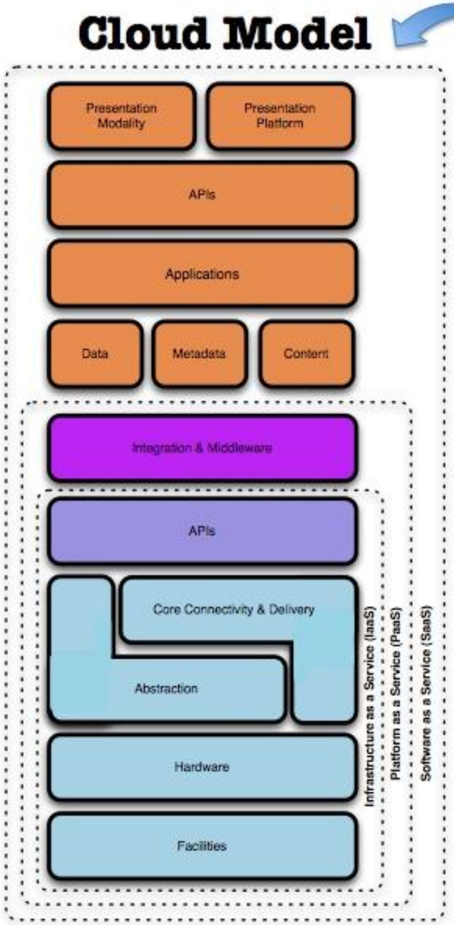
1.1. Introduction – Concerns over Cloud Computing (CC) and CC Services CCS) security

- Our research [1, 2b] shown inefficiency of CC models and questionable CCS security (slides 1.2 and 1.3) in implementation of Complex privacy protection regulations [3] requiring simple models (slides 1.4 and 1.5) instead of overlaying complex structures
- No concerns – future FedRAMP [4] (Federal Risk and Authorization Management Program) announced at NASA on Sept. 15, 2009

1.2. Introduction - Example - The Outsourced Community Cloud Scenario NIST SP 800-146


A Cloud Provider
A Community Cloud
boundary controller
Inside
Outside
Blocked access.
Provider-controlled security perimeter.
Community member security perimeters.
Clients accessing the community cloud from within their security perimeters.
Organization X
Organization Y
Organization Z
bound contr
bound contr
boundary controller
Inside
Outside
. . .
Cloud provider's facility.
Community organizations consuming cloud resources.

1.3. Introduction - Typical CC security model



Cloud Model

Presentation Modality

Presentation Platform

APIs

Applications

Data

Metadata

Content

Integration & Middleware

APIs

Core Connectivity & Delivery

Abstraction

Hardware

Facilities

Infrastructure as a Service (IaaS)

Platform as a Service (PaaS)

Software as a Service (SaaS)

Find the Gaps!

Security Control Model

Applications	SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
Information	DLP, CMF, Database Activity Monitoring, Encryption
Management	GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
Network	NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
Trusted Computing	Hardware & Software RoT & API's
Compute & Storage	Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
Physical	Physical Plant Security, CCTV, Guards

Compliance Model

PCI

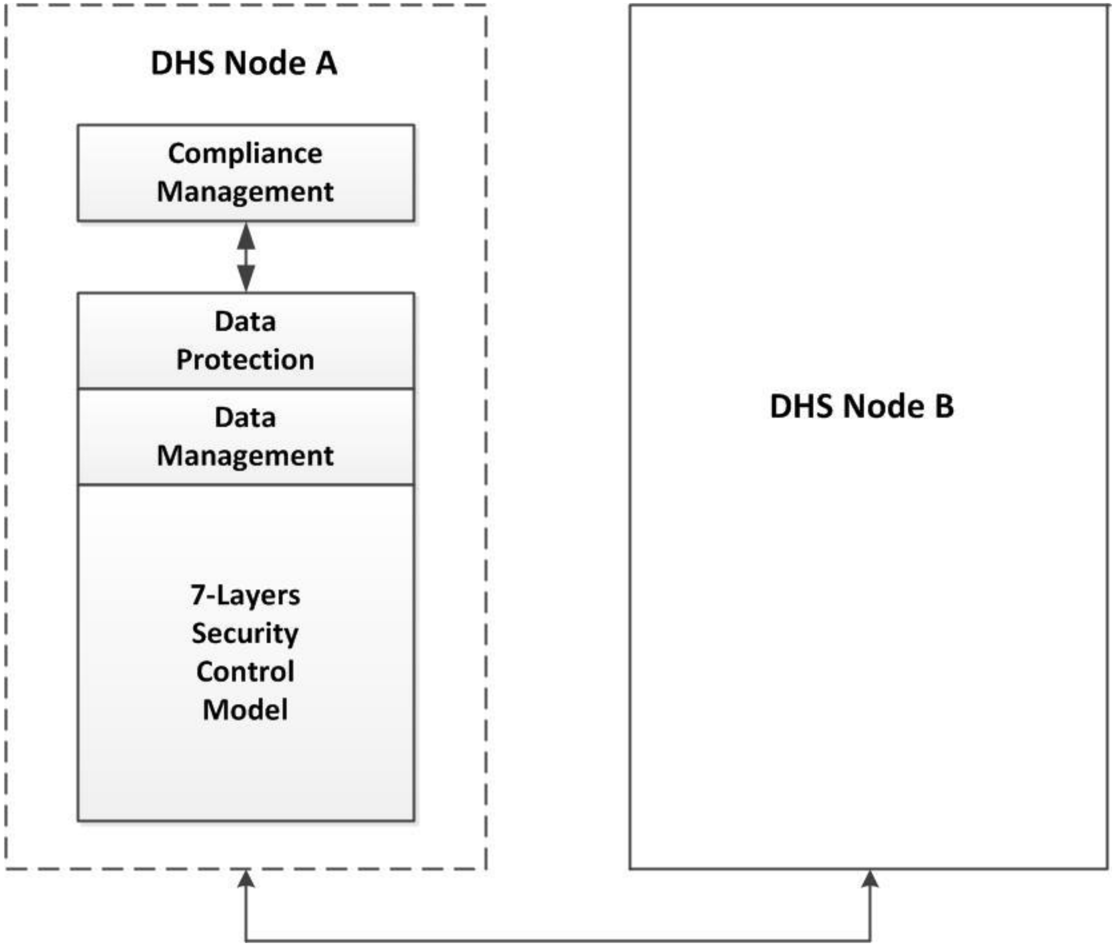
- ☑ Firewalls
- ☑ Code Review
- ☑ WAF
- ☑ Encryption
- ☑ Unique User IDs
- ☑ Anti-Virus
- ☑ Monitoring/IDS/IPS
- ☑ Patch/Vulnerability Management
- ☑ Physical Access Control
- ☑ Two-Factor Authentication...

HIPAA

GLBA

SOX

1.4. Introduction - PI Protection 9-layer Security and Compliance Model (PIP9 Model) (2)



1.6. Introduction – What we did in our research

Analysis of NIST CC and CCS related documents:

1. **Guidelines on Security and privacy of Cloud Computing – NIST SP 800-144, December 2011 [5]**
2. **The NIST Definition of Cloud Computing – NIST SP 800-145, September, 2011 [6]**
3. **Cloud Computing Synopsis and Recommendations – NISt SP 800-146, May 2012 [7]**

(pay attention to dates – official announcement – September, 2009)

4. **Official risk management concept – Guide for Applying Risk Management Framework to Federal Information Systems – NIST SP 900-37 R1, February, 2010 [8]**
5. **Security controls for federal information systems – Security and Privacy Controls in fderal Information systems and organizations – NIST SP 800-53 R4, April, 2013 [9]**

1.7. Introduction – FedRAMP Documents and available audit documents

FedRAMP:

1. FedRAMP Concept of Operations (CONSOPT), v.1.0, February, 2012 [4]
2. FedRAMP Security Controls – FedRAMP Security Controls Preface document [10]
3. FedRAMP_Baseline_Security_Controls_01_05_2012 table [11]

Audits:

1. NASA's Progress in Adoption Cloud-Computing Tecgnologies, NASA Office of Inspector general, July 29, 2013 – simply – failure to address security [12]
2. Audit of GSA Transition from Loyus Notes to the Cloud, Office of GSA Inspector general, September 28, 2012 – no record on any costs saving [13]

2. Where did "Cloud Computing" come from?

2.1. The history of CC goes back to the Internet Bubble, which required a lot of datacenters hosting a rapidly growing number of web sites. After the Bubble has burst, such datacenters became useless. Some sources refer to as low as 10% were is use only. Amazon.com in 2006 came up with the idea of hosting applications in the same way as web hosting – Amazon Web Services (AWS) is the predecessor of CC services.
2.2. Amazon was not using "cloud" in AWS. Neither Google meant "cloud" when started so named Academia Cluster Computing Initiative (ACCI) [14] in 2007 with the pure focus on Clusters and Distributed Parallel Processing (DPP) [15].
There is no "cloud" computing term in Computer Science, nor CC is equal to Distributed parallel Processing.
2.3. "Cloud" term and depicting it image of a cloud have been in use for years in communications, and late moved in general networking to represent networking, basically – communication environment.

2.4. Conclusion

2.3.1. The term “cloud” appeared more likely within IBM affiliated circles [16]. It stated by replacing in Google originated program name “Academic Cluster Computing Initiative (ACCI)” “Cluster” term by “Cloud”. Incorrect name of ACCI program still exists in Wikipedia article and on IBM affiliated web sites.

2.3.2. “Cloud” came from communications, not computer science. There is no such computing. The nature of “cloud” is communications and delivery of information, for instance, as a hosting service.

3. Models and CC concept

“Cloud” is communications term, and “computing” belongs to computer science. Connecting two words was brilliant finding to introduce “new” service of “cloud computing” as new computing concept.

CC, to be claimed as “new computing concept”, required some sort of science behind it. It needed a model, as a standard science attribute.
Do CC models have any value?

There are two models, which are used to describe CCS implementation – Deployment Model (DM) and Service Model (SM). First relates to computing, actually to networking infrastructure, and the other – to services within such infrastructure

3.1. CC services models (1)

Reference sources: NIST SP 800 [5, 6, 7] and Wikipedia "C;pod Computing" article [17] having more recent information (for instance, NaaS).

There are currently four models - NaaS, IaaS, PaaS and SaaS:

3.1.1. Network as a Service (NaaS)

"NaaS concept materialization also includes the provision of a virtual network service by the owners of the network infrastructure to a third party". We translated that in : "NaaS is a virtual network which is provided to CCS customer", or shortly "Hosting of a virtual network", i.e. Hosting Service.

3.1.2. Infrastructure as a Service (IaaS)

"…providers offer computers, as physical or more often as virtual machines, and other resources". what is IaaS? It is again – Hosting of a customer network on a vendor premises, whether virtual or physical.

3.1. CC services models (2)

3.1.3. Platform as a Service (PaaS
Quote from Wikipedia [17]: “cloud providers deliver a computing platform, typically including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform”. Shortly, a vendor provides application development environment where the customer can host development process. Nevertheless, it is Hosting again

3.1.4. Software as a service (SaaS)
It is simply applications’ hosting environment, where a customer can run various applications – office software, email, games, etc. It is the same kind of Hosting service, which has been introduced as AWS by Amazon.com in 2006

Considering that CC services in question have dynamic nature (service can move between infrastructure nodes), we can name “Cloud Computing” as Dynamic Hosting Service

3.1. CC services models (3)

There was no need to invent service Models.
The following table represents an interpretation of Service Models in simple and understandable old hosting services terms:

Model	CCS	Dynamic Hosting
NaaS	Network as a service	Dynamic Virtual network hosting
IaaS	Infrastructure as a Service	Dynamic Network hosting
PaaS	Platform as a Service	Dynamic Development hosting
SaaS	Software as a Service	Dynamic Application hosting

3.2. CC infrastructure Deployment Models (DMs) and terminology

CC Deployment Model idea is to explain how networking infrastructures is installed, or in general, about vendor's resources. First question is **why a customer needs to know how a CC Service supporting infrastructure is installed** and what resources are.

The second question, are Deployment Models adequate and useful?
Since 1985, when we got first AppleTalk as first Local Area Network (LAN), we used to just a few terms describing the evolution of networking. **There are two fundamental – LAN and WAN** (Wide Area Network [18] with a few technological sub-types like WLAN.

When somebody says to us "LAN" or "Wireless LAN", we definitely know what it means

3.2. CC infrastructure Deployment Models (DMs) and terminology (2)

1. “Public Cloud” – quote: “*…It is owned and operated by a cloud provider delivering cloud service to customers*”. Basically, “owned and operated by a provider” implies to a **WAN providing Hosting Service infrastructure**. However, do we really need a new model such as “Public Cloud” to explain what we know since 1990s as “WAN”?

2. “Private Cloud” – quote: “… *is operated exclusively for a single organization. It may be managed by the organization or by a third party, and may be hosted within the organization’s data center or outside of it.*” If Private Cloud is comprised from customer's equipment an managed by the organization, – it is either LAN or WAN, depending on whether it is geographically distributed or not. If the organization’s LAN or WAN is operated by an external entity, it is called “outsourcing”. So, again we can easy explain new “Private Cloud” model in old and easily understood terms – LAN, WAN, or Outsourced LAN or WAN

3.2. CC infrastructure Deployment Models (DMs) and terminology (3)

"Community Cloud" – quote: *Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them"*

This definition is wrong in legal context. There is no such legal entity as a "community", thus any legal representation within or outside of such community is not possible, and services cannot be provided.

A "community" cannot sign an agreement, unless organizations within form such entity legally. In this case, we again see one-to-one relationship, and "public cloud" – WAN/Hosting Service.

Real life example – try to get internet service from an ISP as a 'community"

3.2. CC infrastructure Deployment Models (DMs) and terminology (4)

"Hybrid Cloud" – it is a composition: "*… more complex than the other deployment models, since they involve a composition of two or more clouds (private, community, or public). Each member remains a unique entity, but is bound to the others through standardized or proprietary technology that enables application and data portability among them.*" As far as services are concerned, this model is a combined WAN (private cloud), WAN/hosting service (public cloud), and "Community", as we discussed above, cannot legally exist.

CC DMs	What is it concerning networking and services?
Public Cloud	WAN/Hosting Service
Private Cloud	LAN, or WAN, or Outsourced LAN or WAN
Community Cloud	Legal Nonsense, or becomes Public Cloud – WAN/Hosting Service
Hybrid Cloud	Combined WAN, or WAN/Hosting Service, or Legal Nonsense

3.2. CC infrastructure Deployment Models (DMs) and terminology - Conclusion (1)

1. **It was no need to invent and use "CC Service Model"; all processes can be more easily explained using traditional "Hosting Service"** term and its utilization in each case.

2. **So named "Deployment Models" are useless for services customers, because explain the installation of CCS. Old terminology or LAN/WAN and Hosting Service much better explain processes and do not confuse service providers and users. Such model as "Community Cloud" is legal nonsense, and using it "Hybrid Model" is either legal nonsense as well or becomes WAN-based services**.

3. NIST, which discusses SLA and the importance of agreements and contracts with CCS providers throughout its documents [5, 6, 7], has not identified legal absurd of the "Community Cloud" model.

4. US Government NIST SP 800 documents identifying information security for CCS

There is Information Security Special Publication series SP 800. All standards are mandatory to implement in federal information systems.
There are currently 151 documents available on NIST web site, and some of them have additional versions as well (see http://csrc.nist.gov/publications/PubsSPs.html).

There are five NIST documents, which we should consider and analyze to understand US government position on Cloud Computing security. First three are about the object – CC/CCS and its security:
- NIST SP-800-145 - The NIST Definition of Cloud Computing, September, 2011 (current version) [6];
- NIST SP-800-146 - Cloud Computing Synopsis and Recommendations, May, 2012 (current version) [7];
- NIST SP-800-144 - Guidelines on Security and Privacy in Public Cloud Computing, December, 2011 (current version) [5].

4. US Government NIST SP 800 documents identifying information security for CCS (2)

Next document is about risk management for federal information system, and should help us in understanding risks in CCS:
- NIST SP-800-37 R1 - Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010 [8].

Final document should identify security controls to be used in government CCS implementation:
- NIST SP-800-53 R4 - Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 [9].

4.1. NIST SP-800-145 - The NIST Definition of Cloud Computing

This document has the total of 7 pages, and 2 pages (!) of technical material.

It contains definitions of Services and Deployment Models, and Essential Characteristics. We already analyzed both models above and gave our conclusion. Characteristics are irrelevant to our research, so we skip them

This very short document provides what is well-known from other source4s, and actually does not correspond to the advertised purpose of the document: "…and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing". We did not find within two pages of its text any baseline and anything to help "…how to best use cloud computing".

4.2. NIST SP-800-146 - Cloud Computing Synopsis and Recommendations, May, 2012 (current version)

This document has the total of 81 pages and 74 pages of technical text including 5 appendixes.

The purpose and the scope of the document is (quote):" … to explain the cloud computing technology area in plain terms, and to provide recommendations for information technology decision makers. "

In Executive Summary (quote): "Economical consideration: … Whether or not cloud computing reduces overall costs for an organization depends on a careful analysis of all the costs of operation, compliance, and security, including costs to migrate to and, if necessary, migrate from a cloud."

What is considered in the document (next slides):

4.2. NIST SP-800-146 - Cloud Computing Synopsis and Recommendations, May, 2012 (current version) (2)

- **Cloud computing definition** – the same as SP 800-145
- Typical commercial terms of service - NIST consideration and advising on the legal part of CCS, what a customer should know and do; very basic consideration of contracts and Service Level Agreement.
- **Agreements** – nothing new. There is one we like the most: (quote): “Compliance. Consumers should carefully assess whether the service agreement specifies compliance with appropriate laws and regulations governing consumer data. “ That is great advice! But if the provider claims the compliance, how could the customer be sure about that? There is no NIST advising.
- **General cloud environments** – does not contain any new and valuable technical consideration of “clouds”, basic consideration of Service and Deployment models all together.

4.2. NIST SP-800-146 - Cloud Computing Synopsis and Recommendations, May, 2012 (current version) (3)

- Open Issues (a list of 25):

Latency
Off-line data synchronization
Scalable programming
Cloud reliability
Network dependence
Cloud provider outages
Safety-critical processing
Risk of business continuity
Service agreement evaluation
Portability of workloads
Interoperability of cloud providers
Disaster recovery
Lack of visibility (operations)
Physical data location
Jurisdiction and regulation

4.2. NIST SP-800-146 - Cloud Computing Synopsis and Recommendations, May, 2012 (current version) (4)

Support for forensics
Risk of unintended data disclosure
Data privacy
System integrity
Multi-tenancy
Browsers
Hardware support for trust
Key management

While the most of issues used to be known in LAN/WAN environment, “cloudization” adds a lot of specifics to be resolved in addition to known issues.

- General recommendations – there are **the total of 30 recommendations in five groups**. Some recommendations follow Open Issues list, but some not.

4.2. NIST SP-800-146 - Cloud Computing Synopsis and Recommendations, May, 2012 (current version) (5)

Groups of General recommendations: **Management, Data Governance, Security and Reliability, Virtual Machines, and Software and Applications.** Following are a few recommendations as an example:

- Having a plan for migrating data in cloud to start CCS and from cloud for termination of services. The problem is to get data back from the "cloud"
- Compliance – a customer should be sure of CCS provider compliance and security status; however, it is very hard to get CCS provider internal security information

.- Provider should have operating policies for an external audit, security certification, etc. It is very unlikely that CCS providers have such in place or would be willing to have and to use unless that is required by a law.

- Data recovery – quote "Consumers should be able to examine the capabilities of providers with respect to: (1) data backup, (2) archiving, and (3) recovery". We cannot understand how a customer can verify these three CCS provider activities..

4.2. NIST SP-800-146 - Cloud Computing Synopsis and Recommendations, May, 2012 (current version) (6)

Conclusion:

1. The document is deeply affected by NISTS's necessity to consider everything together – cloud models, services, implementation, applications, etc. Recommendations do not correspond to outlined issues, and are too general and questionable considering current US laws and regulations.
2. Readers of the document more likely will be discouraged whether to go "cloud", because numerous outlined issues and recommendations create a sense of uncertainty and confusion. Instead fo managing internal LAN and applications, they need to create "cloud", get all issues and then resolve them.
3. When it comes to a discussion of economical advantages of CCS, NIST is very cautious and advises to take into consideration all factors and issue before going "vloud". However, such advising is very difficult to follow, because CCS providers limit access to services' internals and documents.

4.3. NIST SP-800-144 - Guidelines on Security and Privacy in Public Cloud Computing, December, 2011 (current version) (1)

This document has the total of 80 pages and 75 pages of technical text including 5 appendixes.

The purpose of the document (quote): ” The purpose of this document is to provide an overview of public cloud computing and the security and privacy challenges involved. The document discusses the threats, technology risks, and safeguards for public cloud environments, and provides the insight needed to make informed information technology decisions on their treatment.”

The most important here is that NIST gave up all models and services and is going to provide security advising for “public cloud”, i.e. hosting service.

The reason is that previous document is almost impossible to use, and adding advising on security controls will make writing difficult and using almost impossible.

4.3. NIST SP-800-144 - Guidelines on Security and Privacy in Public Cloud Computing, December, 2011 (current version) (2)

What is in the document:

1. Key security and privacy issues (10 issues)
2. Public Cloud Outsourcing – how to move:

- General concerns - 7 concerns
- Preliminary activities – 9 activities
- Technology areas to be reviewed -17
- Initiating and coincident activities – 10
- Areas to clarify – 8
- Conclusive activities – 3

Total including Key Issues : 64 security processes and serious issues to consider. Each requires consideration of numerous NIST SP 800 documents. NIST provides numerous tables and documents' lists.

NIST therefore created a roadmap document, which requires step by step considerations, analysis, planned activities, and development of possibly 60+ supporting documents.

4.3. NIST SP-800-144 - Guidelines on Security and Privacy in Public Cloud Computing, December, 2011 (current version) (2)

1. The first and very interesting distinction is that **the document considers “public cloud”, i.e. hosting service only**. While numerous models of CCS exist, practically only one is used
2. **“Cloudization” in a form of models did not affect the document**, it is thorough and logical. While we can question some NIST opinion, the entire document provides a roadmap to outsourcing and hosting.
3. **NIST is very cautious in advising whether to move in to a “cloud”.** Fortunately, NIST does not follow “Cloud First”, because people who wrote the document do understand the complexity of moving an information system into completely different environment, and in particular, government systems
4. **We believe that this road can be walked out**. If a government organization decided to go “cloud”. **But How Much Will It Cost**? Will it save or waste money?

4.4. NIST SP 800-37 R1 - Guide for Applying the Risk Management Framework to Federal Information Systems, February, 2010 (current version) (1)

Unfortunately, the entire document contains only a few very general statements, the most of them we have seen in NIST SP-800-144. The document is about risk management process inside of an organization, and considers risks in distributed computing systems very briefly.

Conclusion:

1. Organization's accountability for risks associated with external (i.e. hosting or "cloud") services; we have seen that in other, including SP 800-144, documents
2. "Chain of Trust" concept is new in the consideration of legally bound distributed computing systems in NIST documents; however, we independently developed better term explaining such bindings in [2] – "Delegation of Trust". It identifies dynamic legal process of moving a trust between distributed nodes, and thus establishing legal relationship based on mutual agreements and information sharing.

4.4. NIST SP 800-37 R1 - Guide for Applying the Risk Management Framework to Federal Information Systems, February, 2010 (current version) (2)

This document does not consider the fundamental difference between CCS models (or hosting services) – different context of information and data. Therefore, associated risks will be different as well.

Short conclusion: this is pure framework managerial document. NIST provides very limited, almost none, analysis of risks in CCS even comparing to what we found in SP 800-144. The most discouraging is that there are no ideas concerning distributed systems. **Therefore, there is no official standard representing methodology of estimating and managing risks in distributed system.**

4.5. NIST SP 800-53 R4 - Security and Privacy Controls in Federal Information Systems and Organizations, April, 2013 (1)

This is the final version of SP 800-53 R4 document. It has been slightly changed comparing to the draft version released in February, 2012. It has 457 pages total. It has three chapters and 10 appendixes A – J). General conceptual part contains only 63 pages. The appendixes D, E, F and J are related to security controls consideration with detailed description of security controls in Appendix D and privacy controls in Appendix J. There are 224 security controls and 26 privacy controls..

Our analysis was extremely brief considering the volume of the document, because NIST did not include any recommendations for utilization of security and privacy controls in distributed (or cloud) information systems, including federal. NIST intentionally avoids labeling “for cloud” any of security and privacy controls, thus leaving such to users of the document

4.5. NIST SP 800-53 R4 - Security and Privacy Controls in Federal Information Systems and Organizations, April, 2013 (2)

Conclusion:

1. **Even considering NIST self-escape from "cloud" advising, new document has definite value and can be successfully used for security and privacy implementation**.

2. It is very helpful that NIST included in the standard the mapping of 800-53 security controls to ISO 27001, and vice versa, but we do not use that in our current research.

3. **FedRAMP is using old version of SP-800-63**. It may happen because while changing and modifying security controls in new version, NIST decided to simplify its job and leave thing on "cloud" matter unchanged.

4. From our point of view, NIST should include consideration of applicability of SP-800-53 R4 security and privacy controls to its own seven (currently 8) "cloud" models. The organization should prove that models and security controls can co-exist.

5. US Federal CCS FedRAMP program

It started as no program of such magnitude should start, and continues in controversy.

There were several very influencing factors, which defined how it started and current outcome of the program, and may be the future of the US government information technology as well:

- **US government loves outsourcing** whatever is possible to outsource expecting to decrease or at least not to increase federal budget
- **Short term of US presidency**, which forms a desire to do something different and remarkable
- **Enormous marketing pressure from US IT industry** promoting CCS (HP, IBM, Intel, Microsoft, etc.)
- **Personalities of the president and his office**
- Etc.

5.1. How "cloudization" reform has started (1)

We have the following dates of important events, which explain what exactly happened:

- **March, 2009 – new federal CIO** Vivek Kundra started his tenure after working for local Virginia and DC government as leading IT manager; his experience included a few web hosting projects of government systems; pure IT, no security experience
- **September, 2009 – Announcement of CCS government program at NASA Ames Reseach center** [19] "… administration's first formal efforts to roll out a broad system designed to leverage existing infrastructure and in the process, slash federal spending on information technology, especially expensive data centers"
- **December, 2010 – "25 Points Implementation Plan" [20] and the announcement of CIO resignation** within 7 months

5.1. How “cloudization” reform has started (2)

- **February, 2011- Draft of NIST SP 800-144** Guidelines on Security and Privacy in Public Cloud Computing
- **December 2011 - SP 800-144** Guidelines on Security and Privacy in Public Cloud Computing
- **February, 2012 – FedRAMP Concept of Operations** (CONOPS)
- May 2012 – NIST SP 800-146 Cloud Computing Synopsis and Recommendations

We see that **Federal CIO announced extremely ambitious program without ANY supporting official documents from such reputable source of government standards as NIST**.

Announcement of CCS program happened without any plan development, and such “25 points” plan appeared only one year later. What was the point to rush?

5.2. First federal cloud proiect and its audit

First “cloudization”: result:
The project:
Federal CIO initiated a project to migration of e-mail/Lotus Notes to the Gmail and Salesforce.com's platform in the middle of 2009, which expected to reduce operational costs.
The result:
However, September 2012 GSA Inspector General report [13] found the savings and cost analysis not verifiable and recommended GSA update its cost analysis. GSA office of CIO was unable to provide documentation supporting its analysis regarding the initial projected savings for government staffing and contractor support. Quote: “*The audit found that the agency could neither verify those savings nor clearly determine if the cloud … migration is meeting agency expectations despite initial claims that indicated 50% cost savings.*”

5.3. FedRAMP initiating “25 Points” plan

This plan was named “25 Points Implementation Plan to Reform Federal Information Technology management” [20], **and is not about a research for feasibility, but implementation.** Federal IT administration had no doubt about applicability of “cloudozation” to federal IT.

The document has 40 pages. It indeed has 25 Point, i.e. short paragraphs briefly explaining what the author means.

Conclusion:

1. The plan of 25 “points” how to re-build entire government IT and move it to utilize commercial web hosting **does not contain any security consideration.** The author is unaware of security issues and treats associated with web hosting and sharing resources.
2. **The plan to reduce the number of Federal data centers by at least 800 by 2015 is not explained at all**.

Reference to future NIST standards outlines the fact that the plan has been crafter without NIST security standards.

5.4. FedRAMP Concept of Operations (CONOPS) document analysis (1)

FedRAM was established by OMB memorandum on December 8, 2011. There are various documents supporting FedRAMO program. Concept of Operations (CONOPS) [4] identifies (quote); "… a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services."
CONOPS fixes the major gap of "25 Points" – lack of security management in the program.
The following quote explains how the program and its participants (government agency, CCS provider, FedRAMP and third party assessor) will work together:
1. Federal agency customer – has a requirement for cloud technology that will be deployed into their security environment and is responsible for ensuring FISMA compliance
2. Cloud Service Provider (CSP) – is willing and able to fulfill agency requirements and to meet security requirements

5.4. FedRAMP Concept of Operations (CONOPS) document analysis (2)

3. Joint Authorization Board (JAB) – reviews the security package submitted by the CSP and grants a provisional Authority to Operate (ATO)
4. Third Party Assessor (3PAO) – validates and attests to the quality and compliance of the CSP provided security package
5. FedRAMP Program Management Office (PMO) – manages the process assessment, authorization, and continuous monitoring process
System owner, i.e. agency-customer, has a word only at final stage – reviews the proposed security package and can authorize it.
While from managerial point of view CONOPS plan seems will work, from security perspective it has serious deficiency - the system owner is involved only at final stage, and may formally agree to what has been approved by other parties.

5.4. FedRAMP Concept of Operations (CONOPS) document analysis (3)

Conclusion:

1. **The CONOPS represent thorough developed plan, which sets the protocol of security management process** between the government (customer- agency, and FedRAMP management), CSP and third party assessor. The document identifies responsibilities and activities of all parties.
2. **However, the deficiency of this conceptual document is the role of the customer-agency. By all government regulations, it is responsible for secure operations of its systems. By CONOPS the customer is excluded from the participation in the beginning of the process** and has a role of final consideration and approval. Such stage as assessment and testing by 3PAO (Third Party Assessor) does not mitigate the problem.

6. Auditing of results of NASA;s implementation of FedRAMP program in progress (1)

Initiators of FedRAMP claimed that CCS will decrease various IT costs and at the same time will improve information security. There is nothing new in such claims – CCS industry promoters always claimed that.

However, first audit of GSA “cloud” email project found no savings, and even more interesting – no documents. Basically, federal CIO and his team simply lied about expected cost savings – they never estimated them.

Now, there is NASA turn to prove by its internal audit [12] the results of “cloudization”. The following are quotes from the audit report:

1. “We found that the **Agency OCIO was unaware of two of the eight companies providing cloud services to NASA organizations** and that **two Centers had implemented cloud services**. In addition, **only 3 of 15 NASA organizations surveyed indicated that coordination with the Agency OCIO was required** before moving systems and data into public clouds.”

6. Auditing of results of NASA;s implementation of FedRAMP program in progress (2)

#1 represents both NASA administration and FedRAMP management failure to handle security processes. More likely that FedRAMP was simply ignored. It also may show the personnel attitude towards administration initiated "cloudization"

2. "**None of the five contracts came close to meeting recommended best practices. The standard contracts failed to include Federal privacy, IT security, or records management requirements and the individualized service contract failed to address many of the best practices discussed earlier**. As a result, the NASA systems and **data covered by these five contracts are at risk of compromise, which could adversely affect Agency operations or result in the loss of data**. In addition, because none of the contracts specified how a provider's performance would be measured, reported, or enforced, "

6. Auditing of results of NASA;s implementation of FedRAMP program in progress (3)

#2 shows that FedRAMP simply does not work – contractors do what they want to do – minimal or no security, and the customer simply does not care about contracts and security controls.

3. “We reviewed documentation provided by eTouch and RightNow, including systems security and contingency plans, authorization to operate the system, and the results of annual system control tests. **We found that NASA’s internal and external portal, which includes more than 100 websites, was operating without system security or contingency plans and with an operating authorization that expired in 2010**. Even more troubling, **a test of security controls on the IT services provided by the NASA Portal had never been undertaken to determine whether the system’s controls were implemented correctly**.”

6. Auditing of results of NASA;s implementation of FedRAMP program in progress (4)

Conclusion:

1. **It was no time synchronization between issuing NIST SP 800-144 and 800-53 R4, FedRAMP CONOPS and NASA process of moving services to “cloud”**. We believe that it was no estimate at all what to move and what not, because such process would take years. NASA started the process at the end of 2011.
2. **Neither NASA administration nor personnel were prepared to such project. NIST SP 800-144 and FedRAMP CONOPS describe very complex security management processes, which cannot be implemented “ad-hock”**, it requires a few years of education and planning.
3. **NASA audit did not perform financial part of the audit for unknown reason. We believe that if carefully done, it would not show any saving but extra expenses.**

7. Analysis of FedRAMP NIST SP 800-53 R3 security controls

Just to be consistent, we did brief analysis of FedRAMP proposed security controls. Here are our conclusions:

1. **FedRAMP uses outdated version of SP800-53**, which does not have recommendations for distributed computing environment, and neither has privacy controls
2. **FedRAMP's table of security controls [11] has no explanation why a lot of controls have been excluded, and neither has comments for included.**
3. **CONOPS misconception of excluding customer-agency from "security assessment" process leads to inconsistent security controls** when **all decision making and implementation is moved to service provider** and JAB, and the customer-agency is unaware what and how is implemented. Having final approval status does not fix the problem. In many cases customer-agency will formally approve security controls implementation and finally will get security problems.

8. Our own financial “audit” – NASA budget analysis (1)

The quote from the NASA audit above [12], which did not do financial part, but is very sure about savings:

“NASA spends about $1.5 billion annually on its portfolio of information technology (IT) assets, which includes more than 550 information systems…

The adoption of cloud-computing technologies has the potential to improve IT service delivery and reduce the costs associated with managing NASA’s diverse IT portfolio.

Specifically, cloud computing offers the potential for significant cost savings through faster deployment of computing resources, a decreased need to buy hardware or build data centers, and enhanced collaboration capabilities.”

We checked a few NASA budgets specific expenses, which could be associated with moving in “cloud” [21, 22].

8. Our own financial "audit" – NASA budget analysis (1)

The following table represents total NASA budget for 2009 – 2014 (projected). It is pretty flat with some plans to decrease it in 2014. This gives us the value of the agency budget – approximately 17 billion.

n

Year	2009	2010	2011	2012	2013	2014
Budget, billions	17.78	18.72	18.45	17.77	17.7	16.6

Our own financial “audit” – NASA budget analysis (2)

The following table represents NASA IT detailed budget as it was planned in 2011 for 2011 - 2017. We see that 2013 and following years budget for Infrastructure was expected to increased by 19 million. Actually, “cloudization” of the agency has started in 2012 (or the end of 2011) and we should see a decrease in infrastructure budget. The budget for IT Management was planned to decrease, but logically it should increase, because “cloud” requires more management than internal services.

	2011 Actual	2012 Estimate	2013 Request	2014 Notional	2015 Notional	2016 Notional	2017 Notional
Agency IT Services	145.0	159.1	152.0	152.0	152.0	152.0	152.0
- IT Management	15.0	14.6	10.5	10.5	10.5	10.5	10.5
- Applications	75.3	67.8	67.8	67.8	67.8	67.8	67.8
- Infrastructure	54.7	76.6	73.7	73.7	73.7	73.7	73.7

7. Our own financial "audit" – NASA budget analysis (3)

Next table is for years 2012 – 2018, but we see that Infrastructure budget is planned to increase for yet another 18.8 million (comparing to 2012), or 39.9 million comparing to one year ago (2011) plans. That cannot represent CCS budget savings! As NASA plans to progress in CCS adoption, infrastructure, as we see numbers, requires more and more!

	2012 Actual	2013 Estimate	2014 Request	2015 Notional	2016 Notional	2017 Notional	2018 Notional
Agency IT Services	158.5	-	168.4	168.4	168.4	168.4	168.4
- IT Management	14.6	-	17.6	17.6	17.6	17.6	17.6
- Applications	68.7	-	56.0	56.0	56.0	56.0	56.0
- Infrastructure	76.0	-	94.8	94.8	94.8	94.8	94.8

7. Our own financial “audit” – NASA budget analysis (4)

Conclusion:

1.By simple checking of NASA budget plans **we identified that Infrastructure, i.e. clous-based services require more and more. We do not see that as expected budget savings, but pure budget gap**. During two years each year planned expenses increased by approximately 20 million.

2. Even more interesting how IT infrastructure budget affects the entire agency budget. **The Infrastructure is only 0.44% of the agency budget. Any savings in Infrastructure will be invisible. The same conclusion is if we compare total IT budget to total NASA budget. It is only 0.9 %.**

We do not see any point of NASA going to “cloud” based on expected savings. They will be invisible! ***However, extra expenses definitely happened, and NASA operations were disturbed, not mentioning security problems.***

9. References (1)

1. Mikhail A. Utin, Daniil Utin. Cloud Computing: a new approach to securing personal information and addressing new EU regulations. DeepSec 2012, Vienna, 2012.
2. Mikhail A. Utin, Daniil Utin. Private Information Protection in Cloud Computing – Laws, Compliance and Cloud Security Misconceptions, OWASP AppSec DC 2012, April, 2012.
3. Proposal for a regulation of the European parliament and of the Council on the protection of individuals with regards to the protection of personal data and on the free movement of such data (General Data Protection Regulation); COM(2012) 11 final, Brussels, 25.1.2012
4. FedRAMP Concept of Operations (CONOPS), Version 1.0, February 2, 2012.
5. Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication 800-144, December 2011.

9. References (2)

6. The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September, 2011.

7. Cloud Computing Synopsis and Recommendations, NIST Special Publication 800-146, May 2012.

8. Guide for Applying the Risk Management Framework to Federal Information Systems, NIST Special Publication 800-37 R1, February, 2010.

9. Security and Privacy Controls in Federal Information Systems and Organizations, NIST Special Publication 800-53 Revision 4, April, 2013.

10. Federal Risk and Authorization Management Program (FedRAMP) Security Controls - FedRAMP Security Controls Preface.PDF document, see http://www.gsa.gov/portal/category/102375

11. FedRAMP_Baseline_Security_Controls_01_06_2012_v1.0 - MS Excel spreadsheet file, see http://www.gsa.gov/portal/category/102375

9. References (3)

12. NASA’s Progress in Adopting Cloud-Computing Technologies. NASA Office of Inspector General, REPORT NO. IG-13-021 (ASSIGNMENT NO. A-12-022-00), July 29, 2013.

13. Audit of GSA Transition from Lotus Notes to the Cloud, September 28, 2012. Office of Audits, Office of Inspector General, US General Services Administration, Report Number A120131/O/F/F12004.

14. Let a Thousand servers bloom – Google official post, Posted by Christophe Bisciglia, October 8, 2007 http://googleblog.blogspot.com/2007/10/let-thousand-servers-bloom.html

15. Academic Success in Cluster Computing, Google Research Blog, posted by Alfred Spector, VP of Research, Decenber 22, 2011. http://googleresearch.blogspot.com/2011/12/academic-successes-in-cluster-computing.html

16. IBM/Google Academic Cloud Computing Initiative (ACCI) , see http://www.cloudbook.net/directories/research-clouds/ibm-google-academic-cloud-computing-initiative

9. References (4)

17. Cloud Computing, see Wikipedia, http://en.wikipedia.org/wiki/Cloud_computing

18. Wide Area Network, see Wikipedia http://en.wikipedia.org/wiki/Wide_area_network

19. White House unveils cloud computing initiative; Daniel Terdiman, CNet.com, Sept. 15, 2009, see http://news.cnet.com/8301-13772_3-10353479-52.html

20. Vivek Kundra, US CIO. 25 Points Implementation Plan to Reform Federal Information Technology Management. December 9, 2010.

21. FY 2013 Presidents Budget Request Summary, see http://www.nasa.gov/sites/default/files/659660main_NASA_FY13_Budget_Estimates-508-rev.pdf

22. FY 2014 Presidents Budget Request Summary, see http://www.nasa.gov/pdf/750614main_NASA_FY_2014_Budget_Estimates-508.pdf

Thank you!

All questions will be answered:

- mikhailutin@hotmail.com

or

- mutin@rubos.com

Rubos, Inc. (presentations, texts, articles, etc.)

- This presentation will be available on DeepSec site