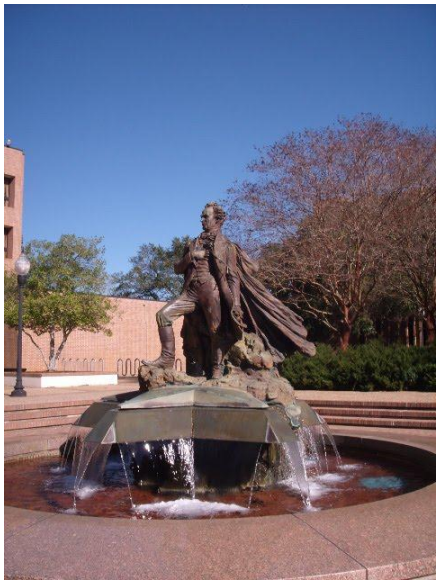
Security in the Cloud - Now and Around the Corner

Dr. Eugene W.P. Bingue
U. S. Navy
Eugene.bingue@navy.mil

Dr. David A. Cook
Stephen F. Austin State University
cookda@sfasu.edu




WE CAN'T MOVE FORWARD UNTIL YOU GET INPUT FROM ALLEN.
AND THAT WON'T BE EASY. ALLEN IS AN AMORPHOUS CLOUD OF GAS.
HE ONCE WAS HUMAN LIKE US.
ALLEN WAS AFRAID TO GIVE HIS OPINION OR MAKE A DECISION.
HE PUT SO MUCH EFFORT INTO AVOIDING COMMITMENT THAT HIS MOLECULES STOPPED BINDING TOGETHER.
NOW HE EXISTS AS NOTHING BUT A SUBTLE ODOR NEAR THE COPIER ROOM.
HOW CAN I GET HIS INPUT?
DON'T MAKE ME MICRO-MANAGE YOU.
ALLEN? IS THAT YOU?
SORRY.
E-mail: SCOTTADAMS@AOL.COM
© 2008 Scott Adams, Inc./Dist. by UFS, Inc.
www.dilbert.com

The purpose of this presentation is to investigate issues with security and using the Cloud.

Currently, rather than “trust the network to handle security end-to-end”, there are several options that an individual can use to protect his/her personal data.

Unfortunately, the new paradigm of Cloud Computing will make some of these methods impractical.

In the Cloud, we need to examine what is the best method of security and encryption that makes sense, given that data and application may not be stored locally. Is there a single solution? Will multiple solutions need to be considered. Are current synchronous and asynchronous algorithmic methods feasible?

In addition, the advent of Cloud Computing and Quantum Computing might make today's strong encryption methods unsafe. Current methods that guarantee "protect your data for 25 years in the future" are harder to find given the potential technological changes over the next 25 years.

We will discuss approaches that make sense now, and examine ways that individual users and enterprise users can help ensure that their data can be secured for the future.

Topics

- Cloud Environments Security Challenges
- Data-In-Motion & at Rest security
- Trust across DoD Clouds
- Vulnerabilities on the horizon
- The way ahead

The Focus of Cloud Computing

- Cloud computing comes into focus only when you think about what IT needs: a way to increase or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software.
- Cloud computing encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends IT's existing capabilities.

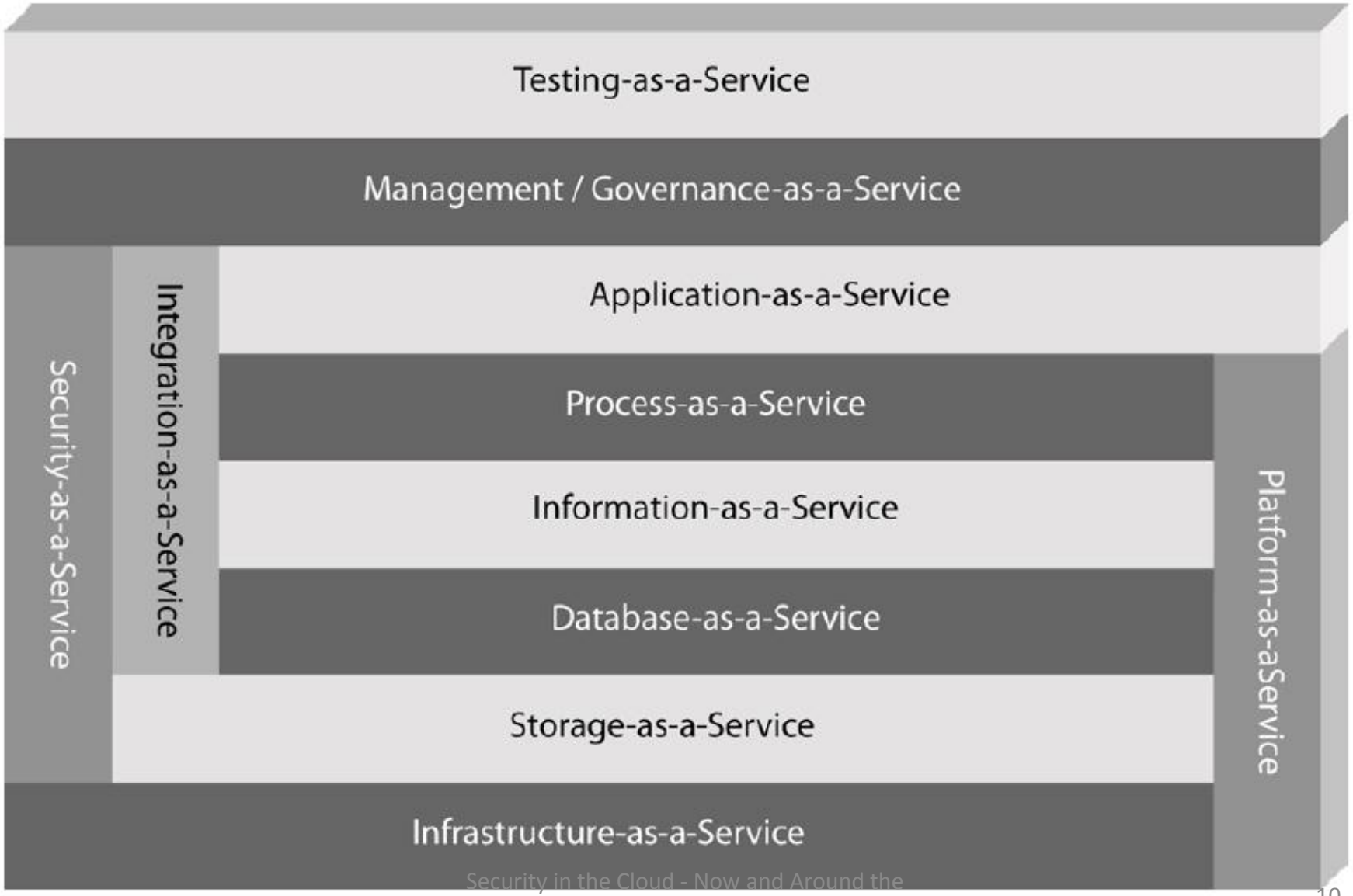
Granularity in the Cloud

- Fine-grained services include
  - storage
  - database
  - information
  - process
  - integration
  - security
  - management/governance
  - testing

Granularity in the Cloud

- Coarse-grained services
  - Application
  - Platform
  - infrastructure

Cloud Environments Security Challenges



Cloud Environments Security Challenges

- **Software-as-a-Service** - Software-as-a-Service is defined as software that you access via the Internet. It is deployed and maintained by the provider. There is no up front investment; rather, you pay for use as needed. You lose the ability to control the software – instead, you rely on others to maintain and update it as needed.

- **Infrastructure-as-a-Service** - Infrastructure-as-a-Service offers core infrastructure, such as servers, switching, storage, etc., on an on-demand basis. The infrastructure is maintained by the provider. There is no up front investment; rather, you pay for use as needed. You lose control of where your data is, and how it is secured. You also lose control of how it is distributed.

Security Challenges in the Cloud

- **Platform-as-a-Service - Platform-as-a-Service offers a platform for building your** own cloud applications. All infrastructure is deployed and maintained by the vendor. Further, a set of APIs is provided to build your application. There is no up front investment; rather, you pay for use as needed. You rely on tools to provide all your needs. You only use the tools – you do not maintain nor control them.

- **Private cloud - Private cloud is a deployment model for things like Infrastructure-as-a-Service**. It describes a model where an organization deploys the cloud service privately to its stakeholders only. Higher costs, better service.

Security Challenges in the Cloud

- **Public cloud - Public cloud is a deployment model for things like Infrastructure-as-a-Service**. It describes a model where a vendor deploys cloud services publically for any company to use (for a fee).

- **Hybrid cloud - Hybrid cloud is a deployment model for things like Infrastructure as-a-Service**. It describes a model where an organization deploys both private cloud and public cloud services.

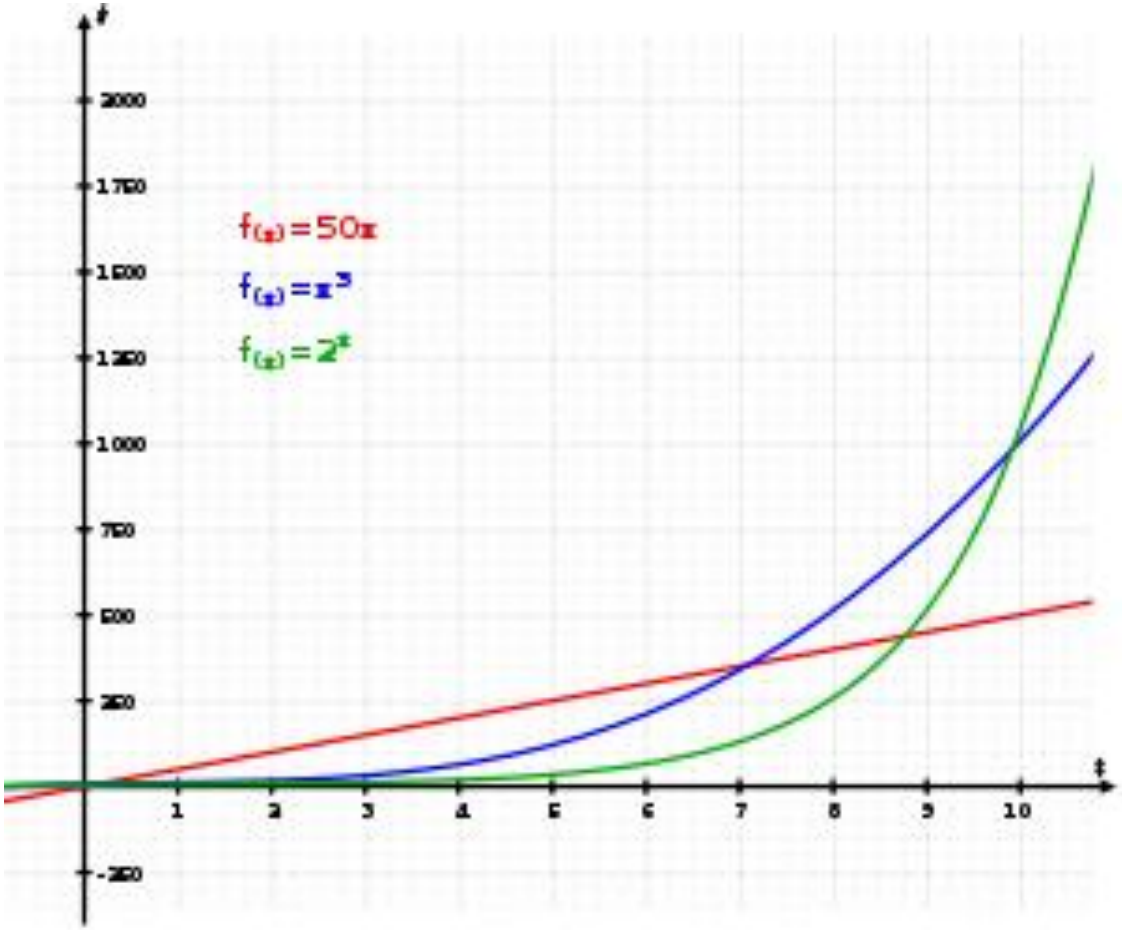
Cloud Environments Security Challenges

- Top five Cloud Services
  - Email services (including management and security)
  - Security management
  - Web and IM security
  - Virtual desktop capability and security
  - Log and/or incident management

Data-In-Motion & at Rest Security

- Computer security is in barely in equilibrium "Ying&Yang" balance daily
  - New Attack generates New Defense
- Cryptography has inherent mathematical properties that greatly favor the defender
  - Adding a single bit to the length of a key adds only a slight effort for the defender, but doubles the amount of effort the attacker has to apply
  - Doubling Key increases Attacker effort ***exponentially***

Data-In-Motion & at Rest Security



.

Exponential growth

Linear growth

Cubic growth

Moral of the story

- You need STRONG keys – think 4096 or above for older asymmetric keys.
- You need REALLY good security – do NOT think asymmetric (PGP). Use AES or Blowfish. Trust that symmetric keys are a necessity. Consider using non-electronic deliver for keys. Or – use VERY STRONG asymmetric codes to exchange symmetric codes – and then switch to symmetric.
- Use GOOD keys.

Data-In-Motion & at Rest security

- In many cases, the databases are queried so often that they are left in plaintext to avoid significant performance degradation.

- In other cases, cost are cut by giving each customer their own table space in the same database – which would allow any customer to see any other's customer's data.

- Solution? Redesign databases with distributed and cloud-based security in mind. Re-examine schemas, subschemas, relationships and access.

Trust across DoD Clouds

- How can we verify an authorized user

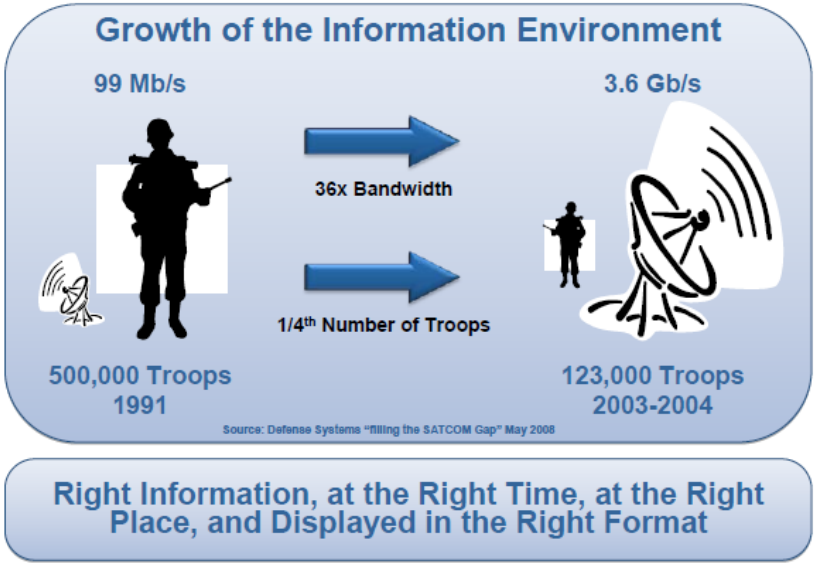
Potential Cloud Applications (lots of them!)
Cyber Network Defense Sensor, data storage, analysis, situational awareness

- Battlespace Awareness -- Common Operating Picture Status of troops, missions, vehicles, weapons, supplies
- In the future – autonomous (unmanned) weapons systems

- Storage/processing of tactical Intelligence, Surveillance, Reconnaissance (ISR) feeds
- Creating a tailored picture based on a user's access privileges

- Simulation and Visualization Mission planning and training

Plus all the emerging "corporate/business" applications



Trust across DoD Clouds

- Unique DoD Challenges
  - Processing information at multiple classification levels and under multiple authorities (e.g. DoD, DHS)
    - Sanitization/purging of local storage
    - Data labeling
    - Privilege-based access control to data stored in the cloud
    - Tailoring “common operating picture” presented to a user based on their privileges
  - Certification and Accreditation
    - Approves system Hardware/Software configuration
    - Extremely difficult in dynamically provisioned environment
    - Must have a trustworthy (and non-optional) system to enforce a security policy and accredit the policy

2012 National Defense Authorization Act

- The 2012 National Defense Authorization Act directs the DoD to transition from private clouds controlled by the DoD to public, commercial clouds.
- The idea is that commercial clouds can provide better service at a lower cost to the taxpayers.
- But critics say that in passing this law "Congress has now increased costs, delays, and security risks for the DoD."

Vulnerabilities on the horizon

- Transition from IPv4 to IPV6
  - Tunneling IPv4 over IPv6
  - Not allocating sufficient memory of longer IPv6 addresses, could lead to remote code execution
- Available data and applications 24/7 in the cloud, is a war chest of information for our adversaries.
- endpoint is now more secure, the situation is that the data is in a more risky place and it will be much easier to silently steal it.

- Most of the attacks nowadays focus on infecting the machine and then hiding the presence of the malware for as much time as possible to intercepting information

Vulnerabilities on the horizon

- With Cloud-centric OS'es, the race will be towards stealing access credentials. Once this occurs, it's "game over".

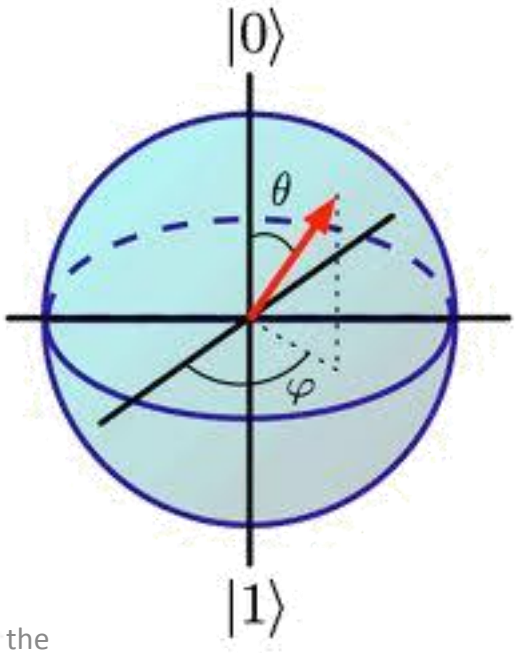
- Google Chrome has already been hacked
- Chrome OS has been designed in such a way that it's extremely resilient to modifications and has a good self healing capability.
  - However, VUPEN Security (French company) that they've cracked the security protections built into Chrome
    - Now able to infect a computer through a malicious page when it's browsed.

One Way Ahead

- IPv6 could lead to more secure networks.
  - Just by planning and prudent approach to deployment
- The problem – we are looking at tomorrow's technology with an understanding limited by today's capabilities
- Quantum computing could make cloud secure
  - Users' qubits –> quantum server (which entangles the qubits according to a standard but private and encrypted scheme
  - Resulting Qubits –> return to sender in a state known only to the user
  - By any practical approach, uncrackable with today's understanding of technology and capabilities

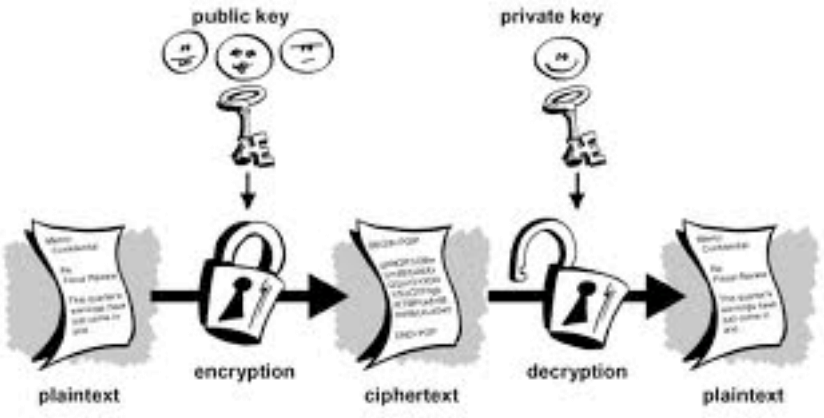
Another Way Ahead

- A 30-qubit quantum computer would equal the power of today's Harvard architecture computer that could run at 10 **teraflops** (trillions of floating-point operations per second).
- Today's typical desktop computers run at speeds measured in gigaflops (billions of floating-point operations per second).
- Of course – the realistic question is "How do you build qubits?"



Quantum Computing

- This has the potential to change security. Right now, state-of-the-practice is asymmetric keys (public-private key encryption), at least to set-up initial security.
- Quantum computers have the potential to factor large numbers into their prime factors very quickly. This will change security in the future.



Summary

- It’s very hard to plan when you can’t see the road ahead, and the maps are all under construction.
- Be sure that “whatever cloud you use” has adequate security. REALLY know.
- Plan for very strong security on your own. Don’t neglect backups. Have contingency plans.

Final Words

- Any new technology has “growing pains”.
- You don’t want to be in too much pain. Let non-critical applications pave the way, and use the new technology appropriately.
- Security is of primary concern in the DoD. You need to aggressively plan for security in the Cloud, and not trust it as a deliverable.

References

- **Quantum Computing Could Make Cloud Secure,** http://www.tgdaily.com/security-features/60908-quantum-computing-could-make-cloud-secure

- **Google Chrome hacked with sophisticated exploit** http://bx.businessweek.com/windows-7/view?url=http%3A%2F%2Fc.moreover.com%2Fclick%2Fhere.pl%3Fr4608179379%26f%3D9791

- **The Defense Department's forced march to the public cloud, http://www.infoworld.com/d/cloud-computing/the-defense-departments-forced-march-the-public-cloud-183890**

- **Don't Panic About, or Ignore, IPv6 Security, http://www.itbusinessedge.com/cm/blogs/weinschenk/dont-panic-about-or-ignore-ipv6-security/?cs=49775**

- **DoD Cloud Computing Security Challenges, http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2008-12/cloud-computing-IA-challenges_ISPAB-Dec2008_C-Kubic.pdf**