DoD Cloud Computing Security Challenges

Chris Kubic

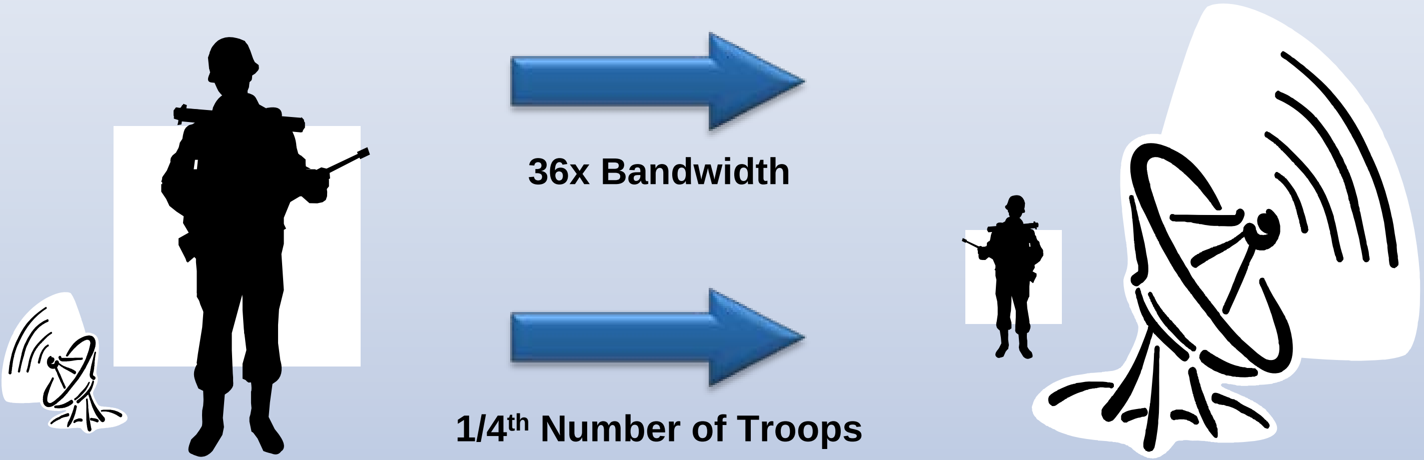
Chief Architect, Information Assurance Architecture and Systems Security Engineering Group

National Security Agency

This Briefing is Unclassified

Improved Situational Awareness Enables Small Agile Force

Growth of the Information Environment



99 Mb/s

3.6 Gb/s

36x Bandwidth

1/4th Number of Troops

500,000 Troops
1991

123,000 Troops
2003-2004

Source: Defense Systems “filling the SATCOM Gap” May 2008

Right Information, at the Right Time, at the Right Place, and Displayed in the Right Format

DoD’s Use of the Cloud

- 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

DoD’s Use of the Cloud

- Potential Implementation Models
  - – Use of commercially provided cloud services
  - – DoD deployment within DoD networks (build our own)
    - “Monolithic” cloud (serves a single purpose), statically provisioned

    ---

    - Dynamically provisioned across DoD clouds
  - – Multi-agency “Federated” processing and storage
  - – DoD/Commercial “Mashup”
- From a security perspective, above the line is hard – below the line is really hard!

DoD’s Use of the Cloud

- Early Adopters
  - trooptube.tv
    - “YouTube” for troops and their families
  - Rapid Access Computing Environment
    - Computing Capacity on Demand
    - Virtual Machine based
  - Many more in the works

TroopTube Powered by Military OneSource

DISA

RACE

RAPID ACCESS COMPUTING ENVIRONMENT

DoD Cloud Computing Security Challenges

- "Gartner Group" security risks certainly apply to DoD
  - Protection of sensitive data, regulatory compliance, data location, data segregation, recovery, etc…
- Other things to consider
  - Security standards for cloud computing (SAML, WS* equivalent)
  - Secure provisioning of applications into the cloud
    - Ensuring integrity of applications
    - Controlling/restricting what applications can run in which cloud instances
    - Binding specific platforms/virtual machines to applications
    - Ability to control how many resources an application can consume
  - Protecting the cloud computing platforms from cyber attack
  - Ability for cloud to attest to its security configuration/properties

DoD Cloud Computing Security Challenges (Cont)

- 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 trust system to enforce a security policy and accredit the policy