

# Essential Considerations for Architecting Secure Federal Data Centers

Doc Shankar

IBM Distinguished Engineer

Federal CTO Office

[dshankar@us.ibm.com](mailto:dshankar@us.ibm.com)

# Security ... It's simple, really...

MILS VPN SOX Physical  
DAC HIPAA Laptop Encryption IPSEC Access  
Password Smart Card SAML Identity Management  
Token FIPS 140-2 Smart Card PCIDSS MLS SaaS  
Trusted Computing XML Gateways Biometrics  
Kerberos Thin Clients Accreditation PKI Cross Domain Systems  
Trusted OS LSP/EAL4+ MAC H/W Crypto  
Wireless Secure Blades Guards Digital Certificate  
Cyber Security Cloud Tripwire Hardening SABI/TSABI  
Federation TCP Wrapper RSBAC Secure Collaboration  
Compliance SOA Security FISMA

11/17/2009

Doc Shankar

2

\* Not a complete collection

# Agenda

1. What are the security concerns in an enterprise?
2. What are the security concerns in a cloud?
3. What is the enterprise security problem?
4. How does one get attacked?
5. Have security requirements changed with time?
6. What are the essential considerations for secure data centers?
7. What's different about federal data centers?
8. Does the customer have any role?
9. Is open source more secure?

# Enterprise Security Concerns

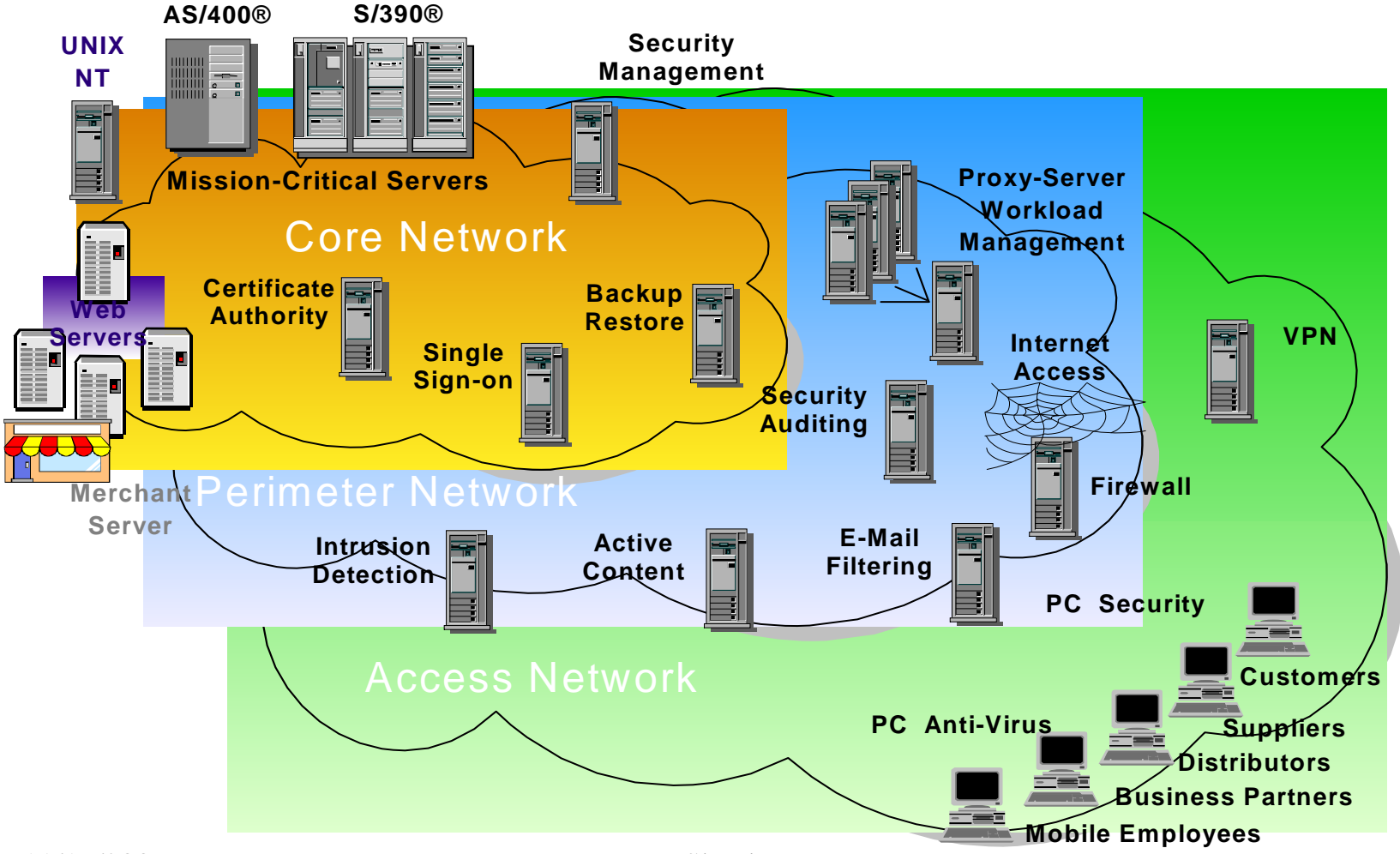
- “I am concerned about the increasing vulnerabilities and exploits”
- “I would like to monitor the enterprise security from one console”
- “I am seeing more attacks internally from privileged users”
- “I need a way to prevent data leakage & loss”
- “I have a hard time defining and meeting the privacy requirements”
- “I am confused about all the compliance requirements”
- “I am not sure how to handle a major DDoS attack”
- “I seem to be always behind in patch management”
- “I am never really sure I have adequate physical security”
- “I worry about directory security which enables dynamic discovery”
- “I am not sure what to do about federated identity management”
- “I am asked to connect my data center with others”

# CC Security Customer Concerns

- “I am nervous about someone else controlling my data”
- “My data is on the same disks as data from other users. If another customer’s data is raided by FBI, could mine go with it?”
- “I am not willing to say that the copy of the data in the cloud is the only copy I’ve got”
- “I am fearful of vendor lock-in”
- “I am still responsible for demonstrating compliance”
- “I don’t know where my data is stored – in which country?”
- “I don’t understand how my data is kept separate from others”
- “I don’t see how I recover my data in case of a disaster”
- “I want to investigate any illegal activity over my data”
- “I want to ensure my data is available when I need it”

Some say, Cloud security fears are overblown!

# Enterprise Security Problem



# Attack Categories

- Misconfigured Programs
- Buggy Programs
  - Buffer Overflows
  - Parsing Errors
  - Formatting Errors
  - Bad input to cgi bin
- Malicious Programs
  - Trojans
  - Virus
  - Worms
  - Root kits
  - Botnets
- Unsafe Programs
- Identity Theft
- Applications
  - Cross site scripting
  - Injection flaws
  - Malicious file execution
- Eavesdropping
- Spamming
- IP Spoofing
- Phishing
- Pharming
- DoS/DDoS
- People
  - Social Engineering
  - Weak passwords
  - Sloppy Admins.

# Customer Pain Points

- **P** - Privacy (Confidentiality)
- **A** - Authorization (Authentication)
- **I** - Integrity
- **N** - Non-Repudiation

The fundamentals of security haven't changed for a long time. However, in the last few years due to viruses, worms, intrusions & DDoS attacks, another one has been added called "Assured Information Access".

# Security Issues

1. Data Security
2. Identity Management
3. Single Sign On
4. Applications Security
5. Secure Multi-tenancy
6. Logs/Audit Trails (Forensics)
7. Cyber Security (DPI)
8. Encryption & Key Management
9. Virtualization Security
10. Storage security
11. Information Lifecycle Management
12. Portability & interoperability
13. US Federal Specific Issues
1. Governance & Risk Management
2. Compliance
3. Vulnerability & Patch Management
4. Physical/personal Security
5. Operational security
6. Availability
7. Incident response
8. Privacy
9. Business Continuity
10. Legal Issues

# US Federal Specific Issues

- How will the cloud meet my information assurance requirements?
- If multiple Govt. agencies need to share information, do they need to be in the same cloud? How do I build a community cloud?
- How is sharing done across different security domains in the cloud? e.g. Multiple Independent Levels of Security (MILS), Multilevel Security (MLS), Cross domain,..
- Mission criticality is key in certain DoD operations. How is this guaranteed in the cloud?
- What cyber security requirements should I impose on cloud providers?
- In case of a cloud cyber attack, how is the attack contained?
- How do I know/control the other tenants?
- How would my end point encryption change, if I move to cloud?
- How will I meet Certification and Accreditation (C&A) requirements in the cloud?

# Customer Role

- Define Security Policy
- Implement Secure Solution to meet policy
- Ensure Secure Configuration
- Patch Management Strategy/Execution
- Secure Administration
- Client Policy Enforcement
- User Training
- Ensure adequate physical security
- Disaster preparedness & recovery plans
- Personnel recruitment and separation strategies
- Automated tools to help user community

# Is Open Source More Secure?

- Security implications of Linux
  - Source code availability
  - Patch speed
  - Community participation
  - Cryptography & Secure Protocol comparison
- Simply publishing code does not mean people will examine it for security flaws.
- Bad guys have access to code.
- So, while Open Source is a good thing, it is NOT a guarantee for security.
  - On the other hand, Linux has been looked at by a lot of very good security engineers.
- End user empowerment
  - Autonomy in resolving security issues
- Diversity inoculates against class breaks
- Linux offers the rock-solid security tradition of Unix

**Advantages are there – one must take advantage of them!**