

Cloud Computing Security

Interlocking Moats & Camouflage



by Bernadette Reiter

Bernadette@xavit.com 303-800-4220

Overview – Securing a Cloud

- Fuzzy know-how in how to achieve it
- It's my space - Virtual Fence
 - Economy of scale diminished
- Accountability and Identity of user
- Legal and illegal threat
- Support staff – access to physical h/w
- Theory versus Reality
 - Cost reduction outweighs risk
 - Someone else's problem to solve
 - Big guys have the solution
 - Standards lemming
 - Underlying technologies are unsecured

Elements of Security (1)

- **Hard breach (disruption of service)**
 - Physical access
 - Power
 - Network (local inter-processor and wide area)
 - One big sitting duck (air strike)
- **Soft Breach/Access**
 - O/S
 - Application
 - Drivers (api)
 - Database
- **Data corruption**
 - Existing
 - Data entry

Elements of Security (2)

- Data theft
- Disruption of service
 - Vulnerability to corporation or government agency
 - Cyber loads
 - Network overload
 - Processor overrun
 - Disk I/O hyper demand
- Distribution through email
- Thin-client architecture
 - Cross contamination

Cloud built on brute force approaches

- Luxury of Moore's Law
- Huge floor space requirement
- Miles of cabling
- Large support staff
- High failure rates
- Large communication bandwidth requirements
- Infrastructure exponential growth & redundancy
- Bloat = cost (incorporated into cost of service)
- Approach is unsustainable and not securable
- Migration effort daunting

Issues with Cloud Computing (1)

- Same as old time-share with added exasperation
 - Has inherent security issues
 - Hack-able
 - High resource consumption
 - Disk I/O, therefore, growing disk arrays
 - Internal memory (bloated applications)
 - Communication bandwidth (multi-media)
 - Consumption norm may make breaches undetectable for some time
 - Open-source – open hidden access
 - Too many notes
 - Too many hands in the innovation
 - Off-shore contributors

Issues with Cloud Computing (2)

- **Loss of control**
 - **Technology**
 - Infrastructure is what vendors support
 - 40,000 lbs. gorillas – me too
 - **Data**
 - **Architecture**
- **Barriers to Innovation**
 - **Technology and architecture controlled by 3rd party**
 - **Standards that address small facet versus totality**

A Closer Look at Cloud Security

- Mainframe vs. Open Architecture
 - Mainframe & mini proprietary
 - Unix, Linux, and MSWindows
 - Security sieve
 - Virus, worm, malware – vulnerability to loss
 - Outsourced – too many hands in the equation
- Too many disparate non-securable O/Ss & components
- Holes in support technologies
- Share-ware open-source
- Vulnerability of Internet disabled or regulated
 - One-stop-subpoena
- Impractical unattainable hyper-visor security
- Weak db access
- Ubiquitous user access
- Accountability and access to source-code
 - In-house or outsourced

Security Measures

- Responsibility of Architecture and Developer
- Part of development initiative
 - Secure DB Schema, Meta-data, Dictionaries
 - Refined db access parameters
 - Location and ID of user
 - Partition/isolation
 - Non-human readable
- Published standards vs. black-box
 - Xml – we're beyond the punch card
 - Semi-structured blobs – intelligence on both ends
- Nested measures

Common Sense Approaches

- **Non-human readable**
 - Program is key cipher
 - Compression
 - Encryption
 - Codification
 - Variable length structure
- **Permission based I/O**
- **Enhanced DB security**
 - DB and strategic files registered with O/S as protected
- **Multi-layered**
 - No one human point of compromise
 - Insider job vs. clever hacker

New Technologies and Architectures (1)

- Cooperative Computing
- Hybrid O/S (proprietary – open) – Protected Kernel
- Permission-based I/O
- Synthetic Intelligence of Infrastructure
 - Device driver with device
 - Immune system
- Front-end application server – smart back-end
 - xStar cooperative computing
 - Real-time update
 - Vetted data-entry
 - Infrastructure immune system
 - Multiple moats to the castle
 - Data formats , game-changing encryption, compression, encoding
 - Multiple levels of knowledge to compromise

New Technologies and Architectures (2)

- **Resource conservative technologies**
 - Programming tools
 - Tight non-redundant
 - No GOTO
 - Communication – photon-based
 - Internet 3
 - Database with FIND/search
 - Compact formats
 - Encoded references
 - Interpretation embedded with data (messaging)
- **Access key**
 - Know who and where user is
 - What are you authorized to touch
- **Server farm in a form factor of a Kleenex box**
 - Air cooled
 - One power outlet
 - Less is more
- **Reclaiming control – cheaper than time-share**

New Cloud – little puff versus Hurricane

- Network centric applications
- Network is an extension of the bus
- Massively parallel (controlled)
- Synthetic Intelligence – integration of cloud elements
- You are a component of the “New Cloud”
- New hack-proof technology
 - Proprietary extensibility
- Less is more technology and architecture
- Tiny CO₂ footprint (why and how)

Summary

- Cloud is old concept in new marketing clothes and expanded vulnerabilities
- Anchored on non-securable infrastructure
- Massive and growing CO₂ footprint – increasing points of vulnerability
- User's shoulder escalating costs
- Loss of control with increased points of malicious exposure
- Cumbersome migration back in-house
- New cloud with new technologies, architectures and approaches
- Everyone is an element of the Cloud
- Internet 3 – New opportunities
- Winning strategies ahead of hacker games and pulling away
- Proprietary yet open with security expandable and changeable security moats
- Anchored on common sense technology solutions
- Retrieving the baby from the bathwater