Topic Paper Title: **Utility Computing Security Issues**

Author: **Justin Klvac**

Date: **6th September 2002**

Reading Instructions: Numbers, within the text, denotes Literature references (e.g.: "(1)"). Security terms unexplained within the text are contained within the glossary and are denoted with letters (e.g.: "Firewalls (a)").

Introduction

With the increasing developments as regards "Utility Computing" it is important to consider relevant security aspects.

This paper will seek to discuss the characteristics of Utility Computing as it is emerging within the IT industry. At this stage relevant security considerations will be highlighted (Risk, Threat, Vulnerability analysis). Discussions of the core technologies that Utility Computing will be based upon will be highlighted. In conclusion an opinion will be offered as to an appropriate security architecture (in general terms).

It should be noted however, that Utility Computing detailed architecture; its actual security product recommendations and their configuration, are beyond the scope of this paper. The aim of this paper is to discuss the overall security Risk and approach to be employed in mitigation against this Risk. This will be done while considering the unique aspects of Utility Computing security issues in this emerging and important field of interest within the IT industry.

Utility Computing: What is it?

Utility Computing is an overall new methodology and technical architecture for the implementation of computing infrastructure services. This series of initiatives involves significant changes to current practices as regards the actual implementation, configuration and redesign of Data Centre technologies. Utility Computing is at the moment a focus of development for IBM, SUN and HP. IBM uses the term "Autonomic" Computing (13), whereas HP use the term Utility Computing (5), while SUN has coined the term "Public Utility Computing" (6).

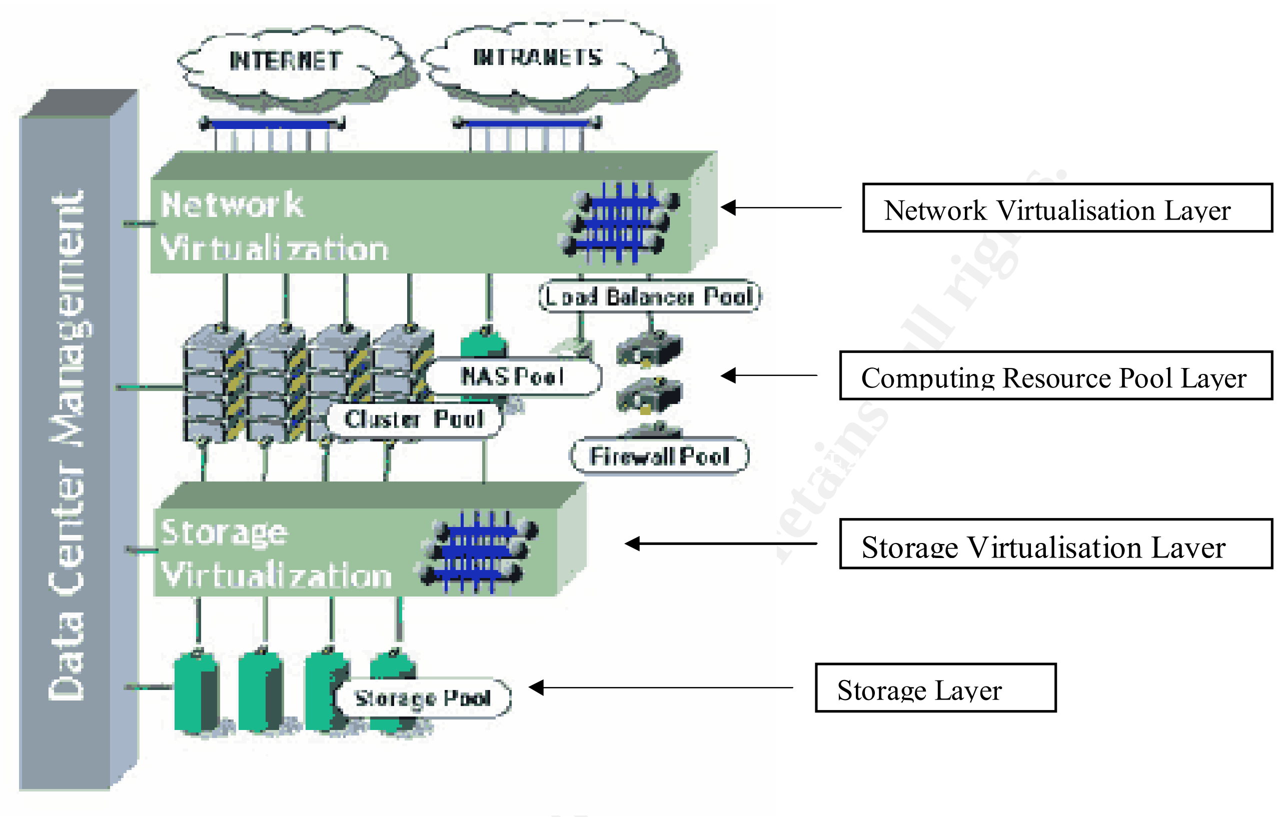
An analysis of marketing material reveals that they are all three of the companies initiatives are on the same track (HP's current offering is UDC, where as IBM's is eLiza). However, it should be noted that initiatives and terms such as "grid computing", "pervasive computing", "service centric computing", or "Planetary Scale Computing" seem at this stage to be synonymous (1,2,11,14).

Utility Computing Characteristics

The key logical characteristics of Utility Computing involves:

- Virtualization of all servers, network connections and data (i.e.: all data is separated from their servers - fungible servers) (5)
- Automatically configured and reconfigured servers and storage based upon predefined policy (4)
- “Drag & Drop” configuration and re-configuration of application infrastructures, in many cases not requiring systems reboot (5)
- Multi-tiered, clustered applications with each tier based upon load balanced redundant modules (12)
- Horizontally and vertically scalable application architecture support (5)
- Data Center and Enterprise wide VLAN, VPN, or VEN (Virtual Enterprise Network) implementation (facilitating anywhere, anytime secure access to corporate computational facilities) (6)
- Centralized control and management of the service via “utility controller software” (5)
- "Fabric" software facilities allowing for a wire once, redeploy many data centre implementation (5)
- "Pay for what you use" vendor financial models (8)
- A complete set of integrated Data Management software monitoring and management services (i.e.: performance monitoring, accurate usage data collection, end to end application SLA reporting, trouble ticketing, configuration management, etc.) (3, 11, 12)
- Higher utilization of servers possible due to ease and speed of redeployment (5, 12)
- High availability due to the load balanced, intermeshed nature of the deployed architecture (i.e.: self healing) (12)
- The option of this service being provided as a complete managed, or outsourced service (2)
- Complete Internet, remote corporate facilities access (6)

The following diagram illustrates a conceptual logical visualisation of a Utility Computing Data Center. Note how the virtualization layers (network and storage) provide for a highly intermeshed interconnected network of computing, management and storage infrastructures.



Source: Hewlett-Packard (5)

The overall literature research (listed at the conclusion to this document) combined with the above diagram indicates that the a Utility Computing Solution will comprise the following physical, or architectural characteristics:

1. A DMZ (e) where web servers can be safely located and portioned
2. The Data Centre Management layer will have to provide for such capability as; Systems Performance Monitoring, Usage Mediation and Billing, Auditing Software/Solutions, Server and Storage Configuration tools, Network and Systems troubleshooting tools (eg: OpenView solution set), Backup Configuration tools and Systems Operations toolsets.
3. The servers and alternate equipment within the Computing Resources Pool layer would have to be redeployable on an ongoing basis to provide for alternate “Application Groups”, or “departmental computing” facilities within the overall Data Centre / Utility Computing facility conglomeration.
4. The Storage Layer would be comprised of a single, over perhaps multiple SAN implementations (eg: EMC technology accessed over a network of fibre connections and configurations). Tape as well as disk SAN implementations could be implemented here.
5. Both the Network and Storage Virtualisation Layers (5) provide for multiple physical channels to the same devices allowing for complete redundancy and the promise of “wire once”, “deploy many”.
6. Load balancers and content caching (3) could be deployed to allow for various application-processing layers to have their own redundancy.

7. Firewalls (a) could be allocated to each “Application Group”, to facilitate higher degrees of security.

The Promise of Utility Computing

The promise of Utility Computing can be expressed in the following quote (2):

“Tapping into compute resources with a simplicity equal to plugging a lamp into an outlet has been a goal of pervasive computing efforts from the start. Known as utility computing, the idea is to provide unlimited computing power and storage capacity that can be used and reallocated for any application - and billed on a pay-per-use basis.” Dan Neel.

Furthermore the key aspects of the Utility Computing promise is:

1. To allow for higher degrees of automation to be achieved leading to increased service levels, reducing downtime (planned and unplanned) and enabling quicker time to market. This is to be achieved by the wire-once deploy many “utility controller / management” technology.
2. To deliver superior financial performance (i.e.: reduced costs). This is to be achieved as less people will be required to run, design and configure the facility as a whole and higher utilisation can be achieved due to the ease of deployment and re-deployment of servers, storage and network capacity.
3. To deliver continual computing services (highest availability), due to the geographically and component redundant nature of the infrastructure.
4. To deliver the highest levels of end user perceived performance due to the dynamic nature of this self healing, self-deploying, self-configuring infrastructure.

Note of Caution

The author notes that detailed technical architectures are not available at this stage, in many cases product inventory information is also not available at this stage (IBM and HP are the exceptions here). Initial, or embryonic Utility Computing examples are prevalent (e.g.: HP Labs UDC Implementation, IBM’s American Express transaction) (2, 9). However, implementations consistent with the above stated Utility Computing Characteristics delivering on the promise of Utility Computing are not in operation at the moment.

Components of utility computing exist today and in fact have exited for numerous years. For example; load balancers, network attached storage, clustered computers and applications (WebSphere), geographical redundant network configurations, etc. In the near future, various hybrid models incorporating components of Utility Computing will become more prevalent (10). As such, it is the author's opinion that Utility Computing is still very much a developing field of endeavour as regards commercial deployment.

Rich Friedrich (Hewlett-Packard Principal Architect Internet Computing) estimates that that the utility computing model will be firmly established within the general industry in a 5 – 7 year time frame (1). Forrester Research state "estimates for the arrival of global utility computing extend out as far as 10 years with some analysts" (2).

It is suffice to say that the marketing publications and statements are yet to be proved deliverable at this stage, or at any stage in the near future. In some ways the literature seems to describe a computing environment similar to the 70s style bureau computing model (7). As such, due to the amount, detail and quality of information available, it is incumbent upon the author to partially speculate as to the required security design aspects.

Utility Computing Security In General

It is important to note from the outset that Utility Computing will be nothing magical. The facility will still comprise of networking equipment componentry, Unix, Linux and Intel based compute servers, computer electrical wiring, computer racks located on floors within data centres, commercially available and well-known application packages, telecommunications facilities and Internet access.

Furthermore, these facilities will still be managed, used and implemented by human beings. The data that resides within these infrastructures will still have the same sensitivities, or value attached to them. As such, motivation to obtain and manipulate these repositories of data will still be the same as today.

As such the following tasks and issues will need to be addressed:

(i) Completion of a thorough Security Policy
(ii) Implementation of a complete Incident Management procedure
(iii) Completion of a Risk Assessment report
(iv) Completion of a Threat / Vulnerability Analysis
(v) Development of an audited Security Architecture
(vi) Appropriate deployment of Network Intrusion Detection (b) systems
(vii) Appropriate deployment Host Intrusion Detection (c) systems
(viii) Appropriate deployment of "locked-down" (d) operating systems
(ix) Anti Viral Software Policy & Implementation
(x) Network Architecture and Configuration policy
(xi) Password Management Policy
(xii) Establishment & Conduction of rigorous Auditing procedures
(xiii) Staff screening
(xiv) Operating Systems patching diligence

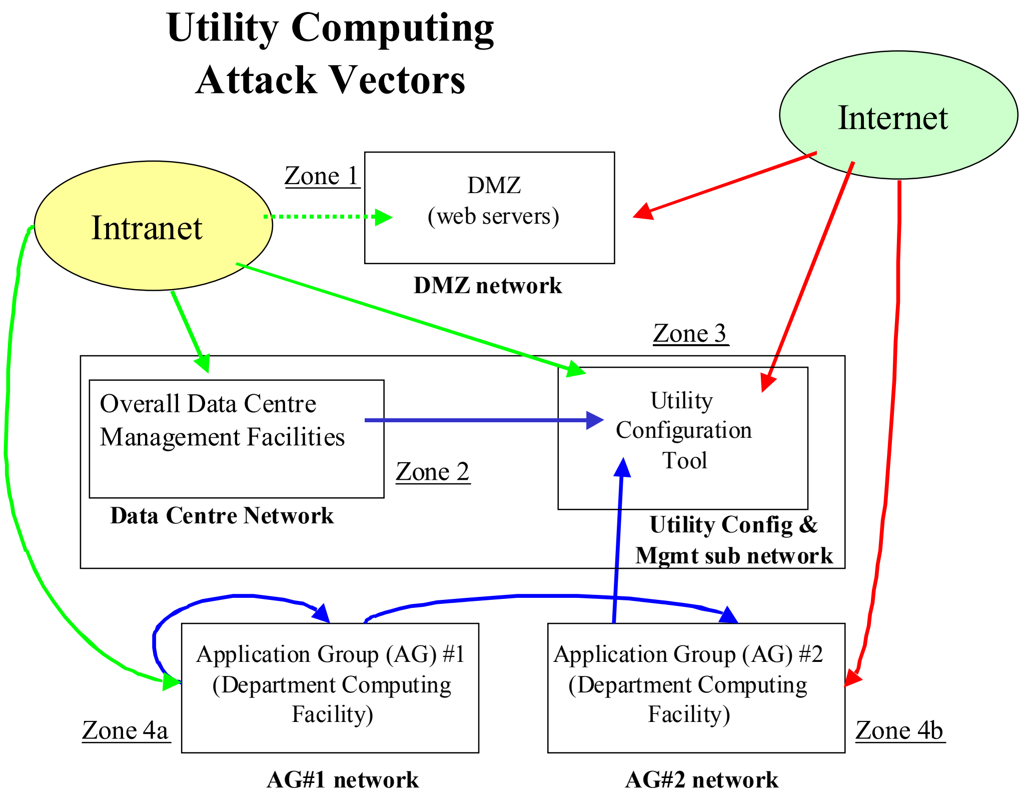
(xv) “Benign” attack (authorised attack) security testing
(xvi) Authentication mechanisms
(xvii) Authorisation mechanisms
(xviii) Repudiation mechanisms
(xix) Encryption mechanisms

In other words, traditional computing security concerns and considerations cannot be ignored.

Utility Computing Attack Vectors

Attack vectors refer to the pathways, or avenues, an attack may take. It is important to consider these attack vectors as it relates to Utility Computing as it allows for a more considered approach to security architecture. If it is known where the utility facility can be attacked from and via what pathways, it is easier to work out how a likely attack would be mounted. As such to plan a defensive strategy is easier and more likely to be successful.

The following diagram details the Utility Computing logical structure, with indications as to likely attack vectors. Note that red lines indicate attacks from outside the organisation, green lines indicate attacks that originate from actors within the organisation, but not configured within the Utility Computing infrastructure, while blue lines indicate attack vectors from users within the Utility Computing facility itself.


Utility Computing
Attack Vectors
Internet
Intranet
Zone 1
DMZ
(web servers)
DMZ network
Zone 3
Overall Data Centre Management Facilities
Zone 2
Utility Configuration Tool
Data Centre Network
Utility Config & Mgmt sub network
Application Group (AG) #1 (Department Computing Facility)
Application Group (AG) #2 (Department Computing Facility)
Zone 4a
Zone 4b
AG#1 network
AG#2 network

Notes:

- It is assumed that the users of the Utility Configuration Tools have complete access to the Application / Department Group computer servers and data.
- It is assumed that the networks are TCP/IP based.

It is beyond the scope of this paper to outline the actual methods of attack possible. However, it is considered suffice to mention that the various forms of attack that could be expected would include such episodes as; denial of service attacks, virus software infection, buffer overflow attacks, Trojan software, password hacking, etc.

It is the author's opinion that the Utility Computing model will have four major areas, or "Zones", to consider as far as security planning is concerned. These Zones can be briefly described as:

1. The DMZ where Internet facing (and possibly Intranet facing) web servers reside, providing access to various applications and associated data.
2. The Overall Data Centre Management facility which provides such services as; network monitoring, trouble ticketing, performance management, billing, etc.
3. The Utility Configuration Tool, which provides the hardware, software and data required for configuring the whole Utility Computing Service. This Zone will contain the data that relates all application code / usage to actual hardware (including storage).
4. The Application Groups, which provide the actual computing power and associated data for the computing using entity (i.e.: a government department, or a company division / functional entity).

Threat / Vulnerability Analysis - Utility Computing Specific Characteristics

This section of the paper seeks to detail a Threat / Vulnerability analysis as regards utility computing from the perspective of understanding if associated Risk of establishing and running a Utility Computing environment is greater than current, more traditional Data Centres.

So, firstly what is a Threat in security terms?

"A Threat is an activity that represents possible danger. Danger can be thought of as anything that would negatively affect the confidentiality, integrity, or availability of a computing service." (15)

Secondly, what is Vulnerability in security terms?

"A Vulnerability is a weakness in your system, or processes, that allows a Threat to occur." (15)

Threats when combined with Vulnerabilities increase the likelihood of actualised Risk (Risk = Threat x Vulnerability). For an example, an IT employee is in financial troubles and has made the decision he is willing to sell confidential company information to competitive organisations. This employee is the Threat. Say that as the Data Centre manager, I allow all IT employees access to systems "super user", or administrative logons. This would be a flaw in security procedures and would be termed a specific Vulnerability. If all employees act as they are expected to (with confidentiality and integrity) there would be no undue Risk. However, in this case there is the Threat (malicious intent) combined with a specific Vulnerability (opportunity to gain undetected access to sensitive information), leading to significant Risk increase.

The following table seeks to outline Threats and Vulnerabilities specific to the changing computing technology and usage characteristics inherent with Utility Computing.

Threat or Vulnerability	Description / Notes	Increase or Decrease?
Threat	Acts of God Physical Threats (e.g.: fire, major power blackouts, floods, earthquakes, storm damage). Due to the heavily intermeshed, redundant configuration and self-healing nature of the Utility Computing environment, this Threat is considered to decrease.	Decrease in Threat expected
Threat	Equipment Failure Physical Threats (e.g.: disk failures, systems failures, telecommunications and network equipment failure). Due to the heavily intermeshed, redundant configuration and self-healing nature of the Utility Computing environment, this Threat is considered to decrease.	Decrease in Threat expected
Threat	Malicious Attack Threat (e.g.: hackers, vandals, protesters, sabotage, viruses, random acts of violence) Due to the more pervasive nature of the computing resource and the greater the extent it would be relied upon, a Utility Computing facility is expected to present greater motivation to potential malicious attack perpetrators.	Increase in Threat expected

Threat or Vulnerability	Description / Notes	Increase or Decrease?
Vulnerability	Higher Degree of Availability (14) Utility Computing proposes to provide continuous transaction processing, eliminating planned and unplanned downtime. Higher degrees of availability do not in themselves present an increased Vulnerability. However, higher availability does present greater opportunity to perpetrate attacks.	Slight increase in Vulnerability expected
Vulnerability	Higher Degree of Automation Utility Computing proposes to automate many more data centre tasks than currently performed. Increased Automation does not in itself present an increase in Vulnerability. If the automated task is correctly designed, then security is enhanced as tasks are completed in a regular, fast and consistent manner. If task automation is not well designed, or inappropriately used then Vulnerability can be increased. *Note:* *Rigorous testing of the environment and training of staff would be required to assist in the mitigation of this Vulnerability.*	Neutral as regards Vulnerability analysis
Vulnerability	Higher Degree of Interconnectivity In traditional Data Centres, all computers, storage and peripheral devices are not interconnected physically. Physical detachment is a significant security enhancement. Utility Computing promises to interconnect all devices, allowing for easy software based redeployment. This point is further reinforced when it is considered that this infrastructure is connected to the Internet.	Significant increase in Vulnerability expected
Vulnerability	Higher Degree of Complexity Utility Computing promises to be easier to run, allowing for automated allocation and reallocation of computing infrastructure either via drag and drop configuration tasks, or even policy driven. However, the interconnectivity and associated equipment configuration and Utility Computing rules must be very complex.	Significant increase in Vulnerability expected

Threat or Vulnerability	Description / Notes	Increase or Decrease?
	It is the author's opinion that complexity of infrastructure is a contributing factor to human error in both monitoring and on-going management.	
Vulnerability	Reuse of Computer Servers and Storage (2) One of the key promises of Utility Computing is the fast, automated reuse of computing resources including; servers, firewall, networking components and disk storage. How do we make sure that data is "cleaned up" once the disk space it used has been allocated to another department, or worse another company?	Significant increase in Vulnerability expected
Vulnerability	Security by Obscurity As Utility Computing architectures become better understood, the knowledge required to compromise a Utility Computing environment would become more prevalent.	Some increase in Vulnerability expected

It is impossible at this stage to calculate in qualitative and quantitative terms the actual increases or decreases in Risk expected, as operational and specific architectural information is not available. However, it is the author's opinion that the introduction of Utility Computing environments will significantly increase expected Risk, especially in relation to internal and external originating malicious attacks. This should be actively considered when planning Utility Computing security architectures.

There are three ways of dealing with Risk. One is to accept the Risk, another is to transfer the Risk (insurance model), the last is to mitigate (i.e.: reduce) the Risk. It is the author's opinion that in this case a Risk mitigation strategy be pursued.

Utility Computing Security Architecture Recommendations

The following Utility Computing security related architectural recommendations are offered in consideration of the following:

- Overall Utility Computing Security requirements (highlighted previously in this paper)
- The updated Utility Computing relative Threat / Vulnerability analysis (highlighted previously in this paper)

- Possible attack vector and overall Zones of Utility Computing (highlighted previously in this paper)
- The provisioning of a multiple layered defence model, providing appropriate “defence in depth” (15) (i.e.: defences at the physical, network, host, application and data layers presenting multiple barriers to pass for any would-be attacker).

The following table illustrates the Zones (as previously discussed) with associated general security implementation recommendations. Specific product recommendations and configuration parameters are beyond the scope of this paper.

Zone	**Security Recommendations & Notes**
1 DMZ	• VPN (f) (1, 3, 6) Implementation for remote access to Utility Computing facility • Securely configured routers with appropriate ACL (h) configuration • Firewall protection (probably a Stateful Inspection Firewall) (mitigates against Internet and Intranet originating attacks) • Network Intrusion Detection system implementation • Host Based Intrusion Detection system implementation • All servers to be “Locked-down” at the operating system level • The DMZ to itself be configured as a VLAN (g) • Appropriate logging to be enabled for auditing purposes • Single Sign On software (providing authentication and authorisation), or Web Server based authentication (at least) • Application level authorisation • The use of digital certificates (j) and associated encryption services is to be considered. Alternatively SSL (k) could be considered as an encryption (l) method, increasing data privacy. • Security Patches to be installed and updated on a regular basis • Switched Networks (i) to be used to decrease the opportunity of broadcast attacks, or reconnaissance information gathering. *Notes:* *Key gateway to the Internet and as such a source for many attacks. The DMZ should be treated as a very sensitive area.* *These recommendations should mitigate against external attack vectors from the Internet (and to a certain extent the Intranet). It should be noted that all external attacks against the Utility Computing environment would have to proceed via the DMZ.*

Zone	Security Recommendations & Notes
2 Data Centre Management	• The Data Centre Management Zone is to be configured as a VLAN • Server to be "locked-down" as appropriate • Appropriate logging to be enabled for auditing purposes • Securely configured routers with appropriate ACL configuration • Firewall protection (against Internet and Intranet traffic) • Network Intrusion Detection to be considered • Host based Intrusion Detection to be considered • Security Patches to be installed and updated on a regular basis • Switched Networks to be used to decrease the opportunity of broadcast attacks, or reconnaissance information gathering. *Notes:* *Not as sensitive an area, due to the lack of application data stored within the Zone. However, could be used as a staging point for further attacks on other more sensitive Zones.* *Possible consideration necessitating greater security requirements could be related to:* • *Auditing, Billing and mediation data being regarded as sensitive data.* • *Accessibility to any backup data would need to be considered.*

Zone	Security Recommendations & Notes
3 Utility Configuration Tool	• Utility Configuration Zone is to be configured as a separate VLAN • Servers to be "locked-down" as appropriate • Security Patches to be installed and updated on a regular basis • Appropriate logging to be enabled for auditing purposes, especially including detailed audit data gathered on the Utility Configuration Database • Securely configured routers with appropriate ACL configuration • Firewall protection (against Internet, Intranet, Data Centre Management & Application Group based attacks) • Database security to be configured (especially for the Utility Computing Configuration database) • Network Intrusion Detection system to be implemented • Host based Intrusion Detection to be implemented • Switched Networks to be used to decrease the opportunity of broadcast attacks, or reconnaissance information gathering. *Notes:* *Regarded as the most sensitive Zone in a security sense, due to the core nature of the Utility Configuration Tools to the whole Utility Computing environment and all its data.*
4a, 4b, etc. Application Group/s	• Each Application Group "x" Zone is to be configured as a separate VLAN • Server to be "locked-down" as appropriate • Security Patches to be installed and updated on a regular basis • Appropriate logging to be enabled for auditing purposes • Anti-Viral software to be associated with e-mail servers • Firewall protection (against Internet, alternate Application Group and Intranet based attacks) for each Application Group to be implemented • Securely configured routers with appropriate ACL configuration • Database security to be configured (for application database/s) • Network Intrusion Detection system to be considered • Host based Intrusion detection to be considered • Switched Networks to be used to decrease the opportunity of broadcast attacks, or reconnaissance information gathering.

Each Zone is considered highly sensitive. The DMZ is the gateway to the Internet and an absolute key pathway for attack. The Utility Configuration Tool facility is the "map" of how the whole Utility Computing environment is established and interconnected. The Application Groups are the repositories of the actual application code and data that requires protection. The Data Centre Management facility is probably the least sensitive area with a Utility Computing environment.

It is important to note that the scale of security architecture implementation will depend largely upon the sensitivity of data stored and the actual expected loss should; data theft, data destruction, or denials of service occur. This calculation will drive the actual resources that are to be deployed towards the security architecture (i.e.: time, money and people) should a Risk Mitigation strategy (as suggested) be pursued.

In addition end user performance requirements, overall manageability and the associated costs of the Infrastructure as a whole should be considered. For example, host based Firewalls increase overall security capability, but also might well impact on overall application based performance.

Conclusion

Utility Computing is an emerging concept and architecture that is anticipated to be adopted by more and more Computing Facilities, as time allows for appropriate technical developments to occur.

It is considered that the overall Risk, incurred with the adoption of a Utility Computing model, will increase.

Due to the highly automated, highly interconnected and organisationally pervasive nature of the Utility Computing model, keen attention should be paid to the possible attack vectors and overall unique security Threats and Vulnerabilities of this technical architecture. This should be considered when deciding upon aspects of overall Utility Computing security architecture, without loosing focus on the traditional, or common, aspects of security architecture relevant to all computing environments.

Glossary & Brief Explanation of Security Terminology

a. Firewall - A logical or physical discontinuity in a network to prevent unauthorized access to data or resources. The four basic types of Firewalls are; Packet filtering, circuit-level gateway, application level gateway and stateful inspection.

b. Network Intrusion Detection – A security management system for network traffic monitoring. A Network Intrusion Detection system gathers and analyzes information from the network traffic to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

c. Host Intrusion Detection – Host Based Intrusion Detection is a specific software installation and configuration that allows for host-specific intrusion detection. Its primary purpose is to detect suspicious activity or known attack patterns on the specific host it is installed on.

d. Locked-down operating systems – The configuration of operating systems and related tools, in conjunction with the installation of security related patches, in a manner consistent with the elimination (or reduction) of vulnerabilities at the operating system level of key hosts.

e. DMZ – DeMilitarised Zone. A DMZ is a frontline network, when protecting valuable information and computing facilities from direct exposure to an un-trusted environment (usually the Internet). Typically implemented in the form of an additional separate network layer between Internal trusted networks and an External un-trusted network.

f. VPN – A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network. For example, if a corporation has LANs at several different sites, each connected to the Internet by a firewall, the corporation could create a VPN by (a) using encrypted tunnels to connect from firewall to firewall across the Internet and (b) not allowing any other traffic through the firewalls. A VPN is generally less expensive to build and operate than a dedicated real network, because the virtual network shares the cost of system resources with other users of the real network.

g. VLAN – The partitioning at a network layer 2 level of logical separation of machines into different logically separated LANs. Server association with a particular LAN as a result can be made without overriding consideration as to geographical locality. Refer to (f).

h. ACL – A mechanism that implements access control for a system resource by listing the identities of the system entities that are permitted to access the resource.

i. Switched Networks – A communications network, such as the public switched telephone network, in which any user may be connected to any other user through the use of message, circuit, or packet switching and control devices. A Switch in computing context is a network device used to connect multiple hosts to a network segment. However, it only forwards packets to the specific port that belongs to each host on the switch. Thus, any given host on the switch only sees traffic addressed to it.

j. Digital Certificates – A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. A certification authority issues it. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

k. SSL – A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection.

l. Encryption - Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.

Source: Based upon SANS “Security Essentials Glossary of Terms” © 2001

References

1. Cowen, Amy, “Utility Computing On A Planetary Scale”, mpulse (a cooltown magazine), Hewlett-Packard Company, August 25, 2002, URL: http://www.cooltown.com/mpulse/0102-thinker.asp
2. Neel, Dan, “The Utility Computing Promise”, InfoWorld, Special Reports, April 12, 2002, URL: http://www.infoworld.com/articles/fe/xml/02/04/15/020415feutility.xml
3. Barlas, Demir, “IBM Extends Utility Computing”, Line56, E-Business News, June 7, 2002, URL: http://www.line56.com/articles/default.asp?ArticleID=3739
4. Jareva Technologies Inc., “Utility Computing: IT Resources Always Available When Needed”, August 26, 2002, URL: http://www.jareva.com/solutions/utility.asp
5. Hewlett-Packard Company, “Utility Data Center: Overview”, 20 August, 2002, URL: http://www.hp.com/large/infrastructure/utilitydata/overview/
6. Sun Microsystems, “Beyond Firewalls: Public Utility Computing for Private Networks”, Sun Corporate Web Site, 27 August, 2002, URL: http://research.sun.com/features/puc/
7. Leyden, John, “IBM’s Utility Computing Push”, The Register, July 1, 2002, URL: http://www.theregister.co.uk/content/23/25975.html
8. Hurwitz Group, “Utility and Service-Centric Computing”, Hurwitz Group Corporate Web Site, 21 August, 2002, URL: http://www.hurwitz.com/coverageareas/uscc.htm
9. Shread, Paul, “HP Connects Its Utility Data Center to the Grid”, Grid Computing Planet. COM, April 10, 2002, URL:http://www.gridcomputingplanet.com/news/article/0,,3281_1006551,00.html

10. Martorelli, Bill, “Utility Computing Goes Mainstream”, ZDNet Tech Update (as contributed by the Hurwitz Group), April 8, 2002, URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2860061,00.html
11. Schwartz, Ephraim, “HP Makes Play for Utility Computing”, InfoWorld, News, April 8, 2002, URL: http://www.infoworld.com/articles/hn/xml/02/04/08/020408hndatacenter.xml
12. IBM Company, “eLiza on IBM Servers”, IBM Corporate Web Site, August 15, 2002, URL: http://www-1.ibm.com/servers/eserver/introducing/eliza/
13. Scannell, Ed, “Paul Horn directs IBM Research into autonomic computing development”, InfoWorld, Interviews, March 14, 2001, URL: http://www.infoworld.com/articles/hn/xml/01/03/13/010313hnhorn.xml
14. Andriole, Steve, “What You Need To Know About Pervasive Computing”, DataMation, IT Management Update, August 23, 2002, URL: http://itmanagement.earthweb.com/columns/bizalign/article/0,,2711_1449951,00.html
15. SANS GSEC Course Notes; Security Essentials (Day 2), “Defence In Depth”, SANS © 2001