JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A proactive architectural model for cloud computing security

Kamlesh Tiwari[1]

Senior Research Fellow, MPUAT, Udaipur, India

***Abstract*—Industries are increasingly adopt cloud computing because it is a new technology which is cut IT costs. Cloud computing is technique to store a large amount of data on a centralized server and user can access his data from anywhere through web. All users use the same centralized storage so there are many security challenges arises. In this paper, we analyse security problems and propose an architectural model for handle these security issues.**

***Keywords*— cloud computing, security, cloud policy, security cloud**

I. INTRODUCTION

Organizations around the world have reaped tremendous benefits of Information Technology as a new driver for change and innovation. But the human quest for innovation never ends and a promising new technology on the anvil is Cloud Computing.

Cloud computing is defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, applications, storage, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1].

The cloud technology is a growing trend. Organizations around the world are sitting up and taking notice of this new phenomenon which promises huge cost benefits, agility and scalability to the businesses either big or small. Researchers have forecast a tremendous growth in the coming years.

Despite the promises however, Cloud Computing has a problem: security. Because Cloud is a new paradigm, it involves careful execution and planning. It would be detrimental to the cause of the organization to just jump on the bandwagon, without proper planning and strategy in place. This concern is indeed reflected in surveys which single out security as the biggest concern.

The DCUG Spring survey 2010 shows that the key concern towards adoption of cloud was security as echoed by 60% of the respondents. [3]

Section II analyzes the problem of security in cloud computing. Section III details the architecture based on the proactive model we propose. Section IV shows the advantages of proposed solution. Finally the references of the paper is concluded.

II. PROBLEM OF SECURITY

A. Background

According to NIST [1], the cloud model is built of five crucial characteristics, three service models, and four deployment models. The five crucial characteristics are as follows:

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

Following are the service models:

- Software as a Service (SaaS): It provides applications over a network for e.g., Google Docs.
- Platform as a Service (PaaS): It provides a platform to deploy applications which is customer-created to a cloud for e.g., Microsoft Azure.
- Infrastructure as a Service (IaaS): It provides Storage, network capacity, Rent processing, and other computing resources e.g. Cloud hosting [4]-[6]

The deployment models, summarized by NIST presentation which can be implemented either internally or externally, as follows:

- Private cloud—Leased or owned Enterprise.
- Community cloud—Shared infrastructure for a particular community sharing common interests
- Public cloud—Sold to the public, large-scale infrastructure
- Hybrid cloud—Combination of two or more clouds

Multi-tenancy although, not covered directly is regarded as an important feature of the paradigm. [7]

It must be noted that the benefits of cloud listed above predominantly accrue when a Public Cloud Model is chosen. The cloud service providers (CSPs) leverage the economy of scale resulting from usage of the underlying infrastructure by many clients. The resultant reuse of the infrastructure enables them to pass on the benefits of reduce the cost for customers.

B. Analysis of Cloud Security

For the purpose of the analysis, we consider two primary cloud deployment models, private and public and analyze their suitability for adoption in an enterprise environment. Community and hybrid clouds are a derivative of the above two. Hence, we limit our concern to private vs. public cloud model.

The cloud computing paradigm opens up new avenues of attack and hence several security issues crop up in case of its

adoption. The top cloud security issues according to the Cloud Security Alliance [8] are:

1) Abuse and Nefarious Use of Cloud Computing

The Cloud Service Providers typically offer IaaS and PaaS solutions to multiple clients. This enables them to distribute the cost of infrastructure across many organizations. It is strictly an economy of scale phenomenon. The larger the number of clients, more economical it is for the provider. To improve business prospects, often free trials are offered to prospective client, in many cases with a requirement of only a valid Credit Card.

It has led to cyber criminals taking advantage and using the vulnerable CSPs infrastructure for nefarious purposes like spamming, phishing and botnets. This may result in the entire IP address range of the Service Provider, ending in a Blacklist.

Thus, a public cloud is plagued by such issues, often exacerbated by the Conflict of Interest of the Service Provider into having such trial offers.

Public Cloud: Affected
Private Cloud: Not affected

2) Insecure Interfaces and APIs

CSPs provide various APIs for the provisioning, management, orchestration and monitoring of the cloud to the clients. The security of the cloud depends on the set of APIs performing robustly. Any bug can wreak havoc and compromise the security of the cloud altogether. Cyber criminals may even be able to log in anonymously. Needless to say, it presents a threatening prospect to the security posture of an organization. Both public and private clouds are subject to this threat.

Public Cloud: Affected
Private Cloud: Affected

3) Malicious Insiders

According to the CERT Insider Threat Center 2010 Cyber Security Watch Survey, more than 67% of the respondents admitted to the fact that Insider incidents are more costly than external breaches. [9]

The best prevention against Insider Threat is a strong and effective organization Security Policy. Any non-compliance must be punished severely. Litigation is an effective deterrent in this case. The security of an organization using cloud services is often dictated by the type of people being hired by the Cloud Service Provider. Clients have no direct say in the hiring policies of such providers. Incidents of corporate espionage in which a competitor intentionally implants a mole in the Provider network cannot be completely ruled out. Unfortunately, Public Clouds are seriously affected by this flaw.

Public Cloud: Affected
Private Cloud: Not affected

4) Shared Technology Issues

IaaS vendors adopt multiple-tenant architecture in order to achieve economy of scale in their operations. Virtualization and specifically the Hypervisor based products are used for the purpose. This results in a scenario where the infrastructure is shared by many different clients. The security requirements often are dependent on the robustness of the underlying hypervisor. Research has shown that it is possible for malicious attacker to bypass the validation and security of the hypervisor in order to manipulate the other guest virtual machines running and effecting a DoS attack. Additionally, a total compromise cannot be ruled out which may jeopardize the data security of the client in question. Again, Public Clouds come to the fore as being affected directly by this threat. Private clouds, on the other hand, may be vulnerable as well. Typically, a private cloud runs only the virtual machines belonging to one security domain of an organization.

Public Cloud: Affected
Private Cloud: Affected

5) Data Loss or Leakage

Data loss or unauthorized leakage to a third party is a biggest threats in Cloud Computing. Due to the way Cloud Computing model is structured, an organization's data may end up in servers in some other nation. This is a significant concern for some organizations. Another issue is for how long the data may be retained by the Cloud Service Provider. The data may continue to remain on the provider's servers even after it has been deleted by the client. Also, a provider may unethically retain additional copies of the data in order to sell it to interested third parties. Surely, encryption can be employed as a solution but it does not solve all the issues. Privacy and Regulatory compliance may require data not to cross the jurisdiction of a country. Additionally, the prospect of data being confiscated by a foreign government cannot be ruled out. Geo-political situation governing the safety of data is not very inviting either. Public Clouds definitely are affected by all of the above threats.

Public Cloud: Affected
Private Cloud: Not affected

6) Account or Service Hijacking

Typically, an authenticated web interface can access a cloud in form of passwords. In a Public Cloud, the threat of an account being hacked is very high. Even two-factor authentication may not be effective in case of a malicious insider at the Service Provider's end colluding with the attackers. This may lead to a situation where the attackers may be able to gain access to the entire sensitive data. Again, Public Clouds are affected by this threat directly.

Public Cloud: Affected
Private Cloud: Not affected

7) Unknown Risk Profile

Cloud computing is an emerging technology and still not mature. The Public Cloud model is especially affected directly by the policies of the Service Provider. In some cases, the Service Provider may not act in good faith and hence jeopardize the prospects of the client. The internal policies regarding data handling is not revealed. A provider may not disclose a security event if it occurs.

Public Cloud: Affected
Private Cloud: Not affected

Hence we see that Private Clouds fare very well in face of top threats as outlined by the Cloud Security Alliance as opposed to Public Clouds as outlined in the following table:

TABLE 1: AFFECTED BY THREATS PUBLIC AND PRIVATE CLOUDS

Threats	Public Cloud	Private Cloud
Abuse and Nefarious Use of Cloud Computing	✓	×
Insecure Interfaces and APIs	✓	✓
Malicious Insiders	✓	×
Shared Technology Issues	✓	✓
Data Loss or Leakage	✓	×
Account or Service Hijacking	✓	×
Unknown Risk Profile	✓	×

The conclusion that can be drawn from above is that by the sheer number of additional threats, Public Clouds are more vulnerable than private clouds. This is reflected in the cloud adoption pattern by various organizations, showing more enthusiasm in adopting private clouds rather than public clouds.

A recent survey by Novell reveals widespread enterprise adoption of private clouds. [10] The writing on the wall is clear. Even though the Private Clouds provide for limited benefits as opposed to Public Clouds, enterprises are not willing to gamble with data security. They have opted for a middle way by adopting private clouds, despite the fact that the real benefits of this promising new technology like cost reduction, agility and flexibility are rather afforded by Public Clouds.

The problems of security as discussed above need to be addressed in a comprehensive manner before an enterprise is confident of security. Clearly, all the issues cannot be simply solved by any single technology. A comprehensive approach must be undertaken which involves both technology and management.

Normally, the clients have to repose their trust in the security practices of the CSP. The Service Level Agreement (SLA) is the only legal instrument between the CSP and the client. While dealing with Public Clouds, sole emphasis is on the SLA. There is no proactive monitoring by the client for any policy violation by the provider.

We propose an architecture based on a proactive methodology which monitors the CSP for any policy violation as mandated by the organization's Cloud Policy, which augments the Security Policy, using a Security Cloud running on top of the Private Cloud.

III. Proposed Solution

Information is vital to the survival of any organization and hence security is the first priority. As discussed above, a public cloud is vulnerable to many threats. The sole recourse is to rely on the vendor's good faith and ability to implement the security properly. Once, data is moved to the Public Cloud, there is little that the originating organization can do to secure it. We propose architecture based on the Security Cloud, running on top of the private cloud, which interacts with the Public Cloud in scenarios only when the service provider exhibits compliance to the organization's Cloud Policy.

Our solution is twofold:

- A Cloud Policy which augments the Security Policy of an organization
- A separate Security Cloud running as a subsystem on the Private Cloud infrastructure which proactively monitors and reports any policy violations.

A. Proactive Methodology

Once this is place, the organization just does not sit passively. Active monitoring is done continuously in order to detect any policy violations. This proactive methodology which we follow for the purpose is listed as under:

- Create a detailed Cloud Policy.
- Identify compatible Cloud Service Provider based on the Cloud Policy above.
- Draft a detailed Service Level Agreement with provisions for monitoring of the Cloud Service Provider network and services.
- Continuous monitoring by the Security Cloud for policy violation.
- The feedback is used to refine the Cloud Policy according to the emerging technology trends and solution.

The details of creation of the Cloud Policy and the Security Cloud are described in the later sections in detail.

B. Cloud Policy

As discussed above, the most common threats affect the Public Cloud computing paradigm which invariably adds an element of a third party in form of the Cloud Service Provider. Traditional Security Policies are custom made for the traditional IT infrastructure model which centers on a data center. Adoption of cloud computing is a paradigm shift in the IT usage by an organization. Hence we argue that a separate Cloud Policy would do justice to the case. Among others, the benefit shall include the management's focused effort and understanding that is required for such a change. This cloud policy will augment organization's Security Policy.

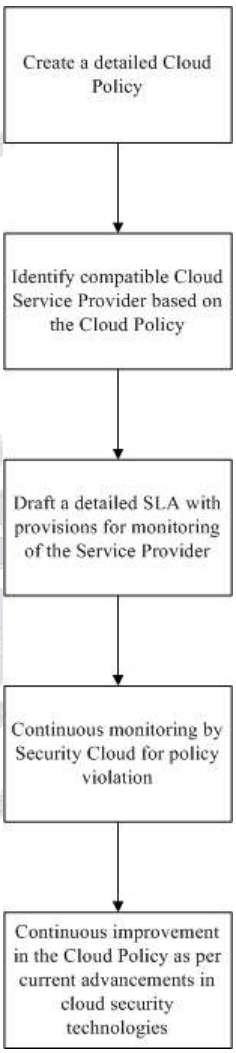

Fig. 1: The Proactive Methodology

As discussed previously, many of the threats simply arise due to Conflict in Interest in the business goal of the provider versus security requirement by the organization.

An example could be choosing a provider which does not allow the practice of giving free trial offerings which open the door for various malpractices and misuse by the cyber criminals. Secondly, due care must be taken to ensure that the Service Provider has a compatible Hiring Policy which compares well to the HR(Human Resources) Policy of the organization. This ensures that the disgruntled employees of the provider do not affect the organization indirectly. Lastly, a very specific SLA (Service Level Agreement) needs to be drawn which clearly outlines the level of security required including periodic threat assessments of the provider network and information in case of a security event. A commitment of

due care by the provider must be sought. The service provider demonstrates this by implementing best security practices for installation and configuration and sending out a periodic report to the client. Strong encryption algorithms and security Protocols must be used in order to provide an acceptable level of security.

The Cloud Policy aims to address such lacunae and strives to map the exact security requirements of an organization as it adopts cloud computing.

Having a separate Cloud Policy provides the benefit of specifying all the Cloud Security issues in one place which is affected by the overall Organization Security Policy.

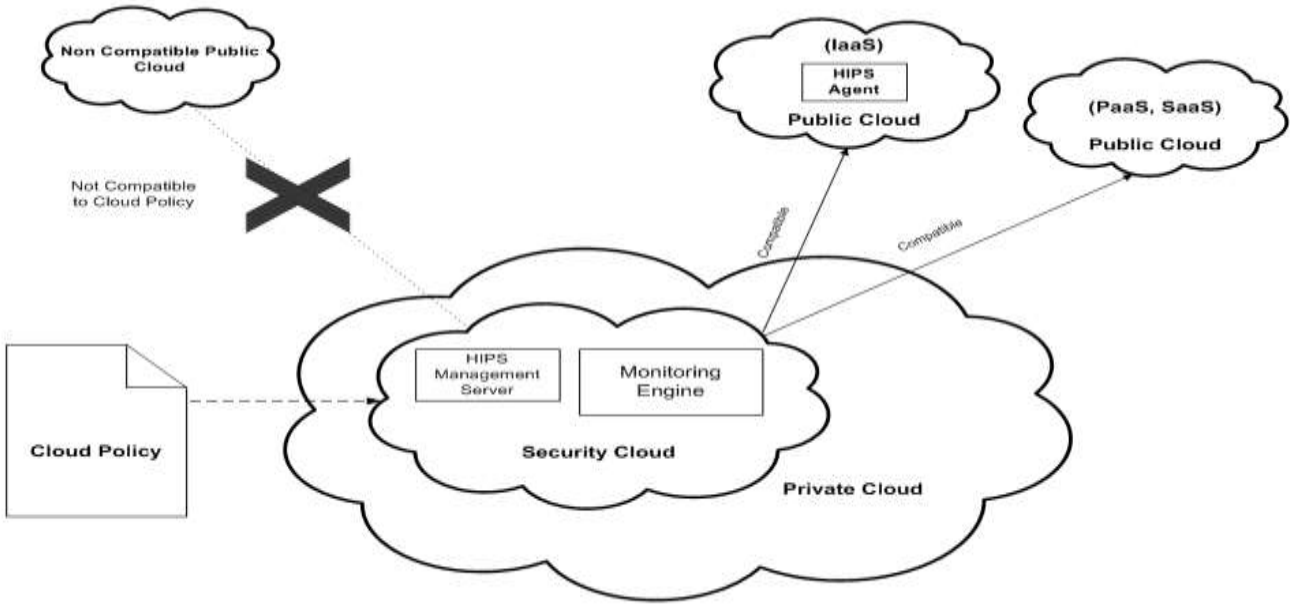

Fig. 2: Architecture based on the proactive methodology

C. Creation of the Cloud Policy

As discussed in the paper Cloud computing security issues and challenges [11], the vast number of security threats and challenges must be kept in mind while drafting the policy. Management support is necessary. Without commitment from the management, any change in any organization is doomed to

A failure. Identify key personnel which should include the network administrators, security administrators and developers too. To understand the end user perspective, end-users should be included as well.

- *Privileged user access:* The provider needs to be accountable for people who are hired to manage an organization's data. Only providers with a compatible HR policy must be contracted.
- *Regulatory Compliance:* The provider must be willing to allow for third party audits and exhibit due care for regulatory concerns. In case of PCI DSS, data logs must be provided to regulators and security managers.
  - *Data Location:* Data in a public cloud infrastructure may travel far and wide. Location independence is in fact one of the tenets of cloud computing. [1] The provider should allay concerns if any of the organization regarding location of data. If need be, the provider should exhibit willingness to limit the flow of data beyond the boundaries of the nation in question.
  - *Data Segregation:* Experts must assess the encryption schemes in use and certify them as safe. The cloud provider should use only standardized encryption algorithms and protocols.
- *Recovery:* In event of a disaster, data must be recoverable from multiple sites, if need be. This requires the service provider to have a comprehensive Business Continuity and Disaster Recovery Planning Policy in place. Also, the time it requires to recover from an incident must be sought after and a guarantee elicited.
- *Investigative Support:* Investigation of illegal activity in a cloud environment is especially difficult. Gartner suggests that it may be impossible to get support from the provider for the cause. Hence, if required, inquire whether the provider has provided for such requests in the past.
- *Long Term Viability:* Acquisition and mergers at the service provider end may create logistical problem of data accessibility. A clear mandate of what actually happens to data in such a situation should be sought.

Additionally, the following must be accounted for:

- *Non-proprietary technologies:* This is to prevent vendor lock-ins. Some clouds are incompatible to others. For example, Microsoft Clouds are incompatible to Google ones. In the interest of greater flexibility only a provider which supports OVF (Open Virtualization Format) should be opted for.
- *Data management:* This should describe the exact data management policies adopted by the service provider. Complete details regarding who has access to data, what actions can be performed must be revealed transparently.
- *Application security:* There should periodic application security tests. The security features and requirements defined must be adhered to by the provider. Security requirements for the application should be provided to the developers by the security team.
- *Security model of cloud provider interfaces:* As discussed above, insecure APIs pose a grave security threat. Hence, the security model of the interfaces must be assessed in detail.
- *Provider HR Policy*: As discussed earlier, it is extremely necessary to investigate the HR Policy of the provider in question.
- *Secure data deletion:* In public clouds, because of multi-tenancy, it is possible for an attacker to obtain a large pool of disk space and analyze it for data remnants. Hence, it must be required for the provider to securely wipe persistent data in accordance with industry standard guidelines like the NIST Special

Publication 800-88: Guidelines for Media Sanitization [13]

- *Defense in Depth.* Defense in depth strategy should be applied wherever applicable. For example, 2-factor authentication should be used where possible.
- *Information from Provider.* The provider must commit to provide an insight into the infrastructure technologies being used and disclose appropriate logs and data. This is to ensure due care criteria being fulfilled.

D. Security Cloud

Private Cloud computing is being increasingly adopted by large enterprises. The feature of elasticity accounts for extra compute resources which are allocated as and when need arises. The Security Cloud is initially provisioned on the underlying private cloud as per requirement. It then is allowed to scale up dynamically and utilize the extra resources available. The process is strictly dynamic so as to not affect availability for cloud users. The Security Cloud readily releases the resources if need be.

A security cloud will logically run as a separate entity on top of the underlying Private Cloud architecture.

The Security Cloud performs the important function of monitoring the Public Cloud Service Provider. Rather than passively relying on the claims of the CSP about the ability to implement security, this proactive architectural approach ensures that the organization will remain secure when a disaster strikes. Needless to say, the Security Cloud is a step forward in that direction.

The Security Cloud shall perform the following functions:

- *Monitoring public blacklists for one's own network blocks*: As discussed in the Top Threats to Cloud Security, this step is vital to ensure that the network block used by the CSP does not end up in a public black list due to illegal spam activity, creating a Denial of Service situation for the client.
- *Vulnerability Assessment*: Using automated tools the Vulnerability Scanning of the CSP network resources ensures that the current health of the provider network can be gauged.
- *Penetration Testing:* Automated penetration testing tools like the Metasploit Framework [14] can be deployed to test the CSP network. Care must be taken to not to cause any disruption of service in the provider network, which would defeat the purpose of the entire exercise. In order to ensure a comprehensive test, Open Source Penetration Testing framework like the OSSTMM can be adopted. [15]
- *Log Analysis:* The disclosure of applicable logs and relevant data by the CSP is mandated by the Cloud Policy. This log analysis is performed by the security cloud which reports any violation to the management.
- *Host Based Intrusion Prevention System:* In the IaaS model, the CSP provides only for the basic resources like storage and networking. The client is expected to provide for Operating Systems and applications. Taking advantage, a HIPS (Host Based Intrusion Prevention System) can be deployed as a defense in depth approach. Using anomaly detection and stateful protocol analysis, an effective system can be designed. [16]

The Security Cloud can be used to provide security services to the internal Private Cloud as well, in accordance to the organization's security policy. In addition to vulnerability scanning and penetration testing, it can be used to perform password audits employing offline password crackers like John the Ripper[17], to even online brute forcing by tools like Hydra[18] in order to check for weak passwords.

IV. ADVANTAGES OF THE PROPOSED ARCHITECTURE

The problem of underutilization in the traditional private clouds is solved to a large extent, with the utilization of the spare power in creation of the security cloud.

The two phased approach prepares the network administrators and the developers with key insight into the cloud paradigm, thus avoiding the culture shock that may arise if public Cloud is adopted all at once, thereby exposing the organization to unknown threats.

The Security Cloud provides a defence in depth solution to not only the instances when Public Cloud is being used but also to the Private Cloud infrastructure. Additional services provided like Vulnerability Scanning and Penetration Testing improve overall security.

A compatible Public Cloud Service provider is guaranteed in accordance with the Cloud Policy. The Cloud Service Provider's due diligence and due care is strictly monitored which improves the overall security posture of the client.

Finally, continuous improvement of the Cloud Policy as per the current advancements in the cloud security technologies assures that this architecture remains relevant in catering to the needs of the latest threats to security.

CONCLUSION

Cloud computing as a technology is still evolving. The industry waits with a baited breath while the experts iron out the flaws. Owing to the issues which are prevalent, a proactive approach to the adoption of the Cloud Computing is advised.

The continuous monitoring for any policy violations bodes well for the organizations as now they have more control over the security of the Public Cloud rather than just rely on the assurances by the vendor.

We are confident that this approach will improve the security posture of the public clouds and will go a long way in speeding up its adoption by the organizations around the world.

REFERENCES

[1] National Institute of Standards & Technology (NIST), http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc, November 2010

[2] Gartner Newsroom, http://www.gartner.com/it/page.jsp?id=1389313, January 2011

[3] The Data Center Users' Group DCUG Spring survey 2010, http://www.datacenterug.org/profiles/blogs/data-center-users-group-survey, January 2011

[4] Windows Azure, http://www.microsoft.com/azure/whatisazure.mspx, November 2010

[5] Google Docs, http://docs.google.com/, November 2010

[6] Salesforce.com, http://www.force.com/, November 2010

[7] Ronald L. Krutz and Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley Publishing, Inc. 2010

[8] Cloud Security Alliance, Top Threats to Cloud Computing V1.0, http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, December 2010

[9] CERT Insider Threat Research, 2010 CyberSecurity Watch Survey, http://www.cert.org/archive/pdf/ecrimesummary10.pdf/, December 2010

[10] Novell survey, http://www.informationweek.in/Cloud_Computing/10-10-05/Novell_survey_reveals_widespread_enterprise_adoption_of_private_clouds.aspx , January 2011

[11] Popovic, Kresimir and Hocenski, Zeljko, "Cloud computing security issues and challenges," in Proceedings of the 33rd International Convention, MIPRO 2010

[12] Gartner Seven Security Risks of Cloud Computing, http://www.networkworld.com/news/2008/070208-cloud.html, January 2011

[13] NIST Special Publication 800-88: Guidelines for Media Sanitization http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf, February 2011

[14] Metasploit Framework, http://www.metasploit.com/framework/, December 2010

[15] Open Source Security Testing Methodology Manual, www.isecom.org/osstmm/, January 2011

[16] The NIST Guide to Intrusion Detection and Prevention Systems (IDPS) http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf, January 2011
[17] John the Ripper Password Cracker, http://www.openwall.com/john/, January 2011
[18] THC-Hydra Network Logon Cracker, http://thc.org/thc-hydra/, January 2011