

# Discussions on Policy in a trusted computing environment



# Selection of applications for analysis

---

For this assignment, I have chosen to select two applications of Trusted Computing.

1. Secure Data Storage.
2. Network Access Control.

These are generic applications and which have been proposed and implemented.



# Secure Data Storage applications

---

There are the following application for secure data storage:

1. DriveTrust technology from Segate.

I have used this as the basis of analysis.



# Network Admission Control applications

---

These are the solutions available for implementation who use Trusted Computing aided Network Admission Control:

1. Juniper Network's Unified Access Control.
2. Cisco's NAC (Network Admission Control)

I have used these as the basis of analysis.



# Strengths of Secure Data Storage applications

---

According to my observations, following are the strengths of the policies implemented in Secure Data Storage applications:

1. Primary function is to protect drive data, but also ensures there is a trusted path between the drive and the application, this policy prevents data leaks on the way from the harddisk to application.
2. The on drive security feature of separation of partitions gives the basic tool for implementation of strong separation of processes even when on static or permanent storage.
3. Support for full disk encryption facilitates secure transport of data.
4. This particular application (DriveTrust) addresses the problem of portable data devices such as USB keys, by implementing a technology called drive pairing. Which enables the content on the portable device to be authenticated with the harddisk before data transfer.



# Weaknesses of Secure Data Storage applications

---

1. Forensic analysis of data for investigative purposes is also an important use of data, these policies fail to address this special issue and may hinder the recovery of evidence.
2. The operation of the drive is such that once the credentials are supplied the data is unlocked and will stay unlocked until the power is supplied, there are concerns about this technologies support for OS hibernation/standby.
3. Recovery of critical data from a failing harddisk is almost impossible. This is usually the case when a computer harddisk is concerned.
4. There is no consideration in the policies to support applications such as RAID, NFS, ISCSI, etc.



## Strengths of Network Admission Control applications

---

According to my observations, following are the strengths of the policies implemented in Trusted Computing aided Network Admission Control:

1. Main intention is to guard the network and the connected resources from the internal users of the network. To ensure that the integrity and the health of each machine joining the network is guaranteed.
2. Policies prevent already infected or unhealthy machines joining the network and infecting other resources.
3. The policies facilitate the movement of hosts inside the network, so that the host can connect to any point in the network, but the policies that govern the access to the resources is the same.
4. The policies provide limited but sufficient access to guests, they prevent access of the internal resources such as the databases, but will allow access of the generic internet.



## Strengths of Network Admission Control applications

---

5. Worm containment can be addressed by eliminating the problem causing host rather than shutting down the switch port.
6. The policies address the issue of intrusion detection and provide continuous monitoring of host traffic for suspicious activity. And then the host can be eliminated based upon the seriousness of the offence.
7. Efficient network flow management issues can be addressed, high network consuming resources could be identified and segregated in a particular high bandwidth network.



## Weaknesses of Network Admission Control applications

---

According to my observations, following are the weaknesses of the policies implemented in Trusted Computing aided Network Admission Control:

1. The whole NAC concept is heavily dependant on the “agent”, which is responsible for reporting the status of the host it is running upon. This heavily exploits the remote attestation function of Trusted Computing for its functionality. Also this forms a single point of failure, compromise of this agent or the malfunction of it can render the host isolated or give it unrestricted access.
2. The “agent” typically checks for the Operating system patch level and Antivirus version, they do not define any criteria about the Unix based systems which may render these operating system based hosts always untrusted and only allowed to access limited resources.
3. Network Access Control systems typical warrant the complete overhaul of the networking infrastructure, which is not trivial.
4. The policies require the hardware to be compliant to certain strict regulations, which may render perfectly good old hardware useless.



## Weaknesses of Network Admission Control applications

---

5. Also if the particular network policies require the agent to be active throughout, it may well consume a lot of resources on the host computer which would adversely effect the efficiency of portable systems such as laptops.
6. A fully patched operating system and an updated version of the Antivirus do not guarantee system integrity and that the system is devoid of any malware.
7. There may be serious compatibility issues between solution offered by different or competing companies, so if we use a particular companies solution it may require the same hardware to be installed all over the network.



## Points for potential improvements in the TVSA policies

---

According to my observations, following are the points which could be considered for improvement of the TVSA policies:

1. Define rules, policies for a system to spawn its own virtual system.
2. There should be special limiting policies on systems which are the part of more than 'x' (a particular threshold) number of systems. As these are most liable to leak information between systems.
3. Policies should be defined for the containment of a rouge virtual system, so that the damage is limited due to such an incidence.
4. Due to the structure of TVSA, data is flowing through multiple trust domains, and multiple components. Policies will be enforced at different levels in this architecture, so the specification of policies should be such that they translate well into the building specifications of that particular device so that the required policies can be effectively enforced.

The above points are a result of my own limited understanding of the TVSA, they are not necessarily a required addition to TVSA.



# Resources

---

1. [http://www.seagate.com/docs/pdf/whitepaper/TP564\\_DriveTrust\\_Oct06.pdf](http://www.seagate.com/docs/pdf/whitepaper/TP564_DriveTrust_Oct06.pdf)
2. [http://www.cisco.com/en/US/netsol/ns466/networking\\_solutions\\_package.html](http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html)
3. <http://www.juniper.net/company/presscenter/pr/2006/pr-061113.html>
4. [http://www.juniper.net/products\\_and\\_services/unified\\_access\\_control/index.html](http://www.juniper.net/products_and_services/unified_access_control/index.html)
5. <http://www.juniper.net/products/ua/dsheet/100137.pdf>
6. [http://blogs.eweek.com/brooks/content/print/nac\\_is\\_whack.html](http://blogs.eweek.com/brooks/content/print/nac_is_whack.html)
7. [http://en.wikipedia.org/wiki/Network\\_Access\\_Control](http://en.wikipedia.org/wiki/Network_Access_Control)



# Resources

---

8. [http://en.wikipedia.org/wiki/Trusted\\_Computing](http://en.wikipedia.org/wiki/Trusted_Computing)
9. “Some weaknesses of the TCB model”, B. Blakley, D. M. Kienzle, Proceedings of the 1997 IEEE Symposium on Security and Privacy, Page: 3, 1997
9. “Secure Data Management in Trusted Computing”, Ulrich Kühn, Klaus Kursawe, Stefan Lucks, Ahmad-Reza Sadeghi, Christian Stübke, Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005)