Resource Monitor

WELCOME

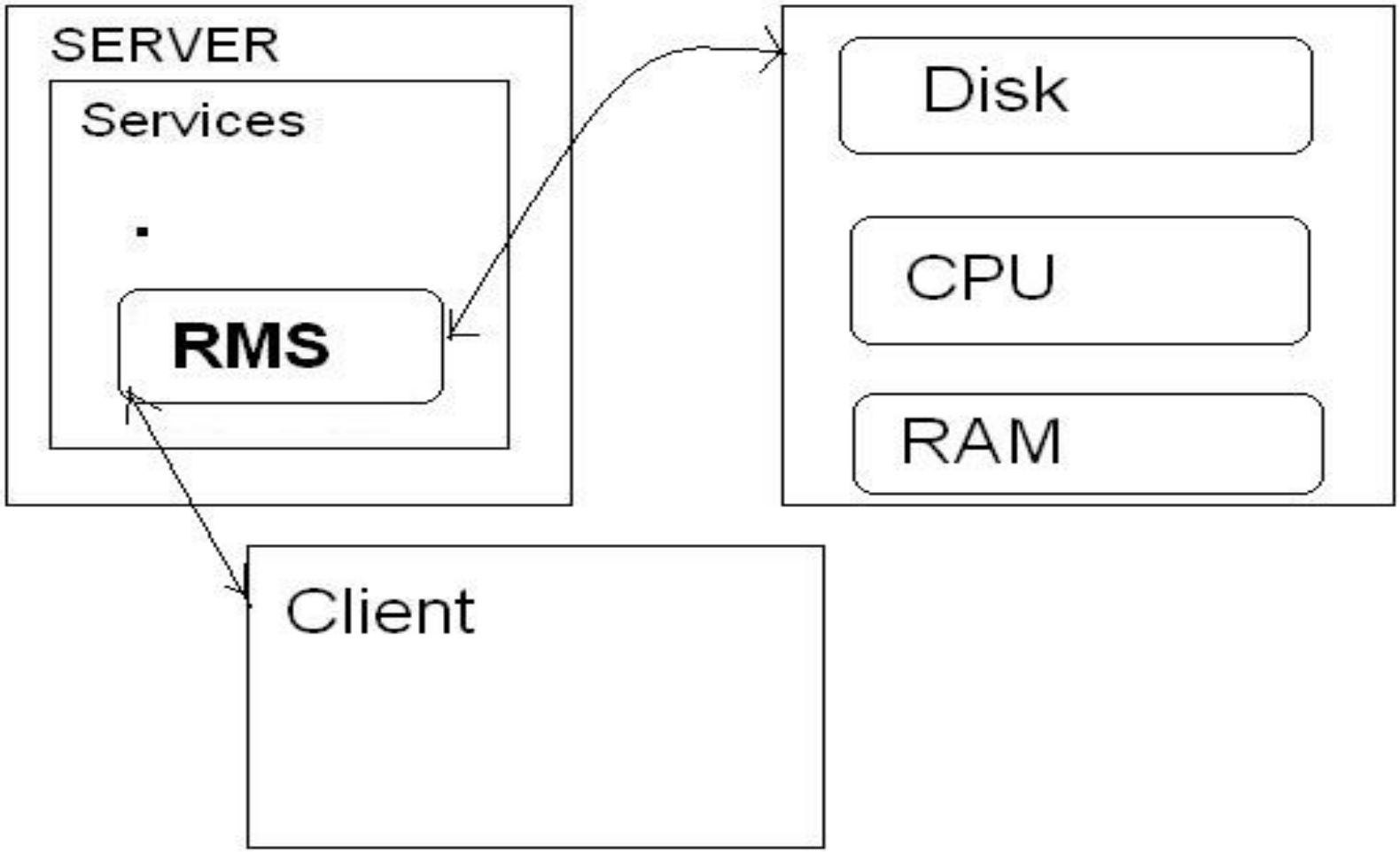
Sathya Prakash.K

www.boris-info.co.cc

Requirements

- It should not consume huge resource on the server where it is listening
- Availability of the program even during updating the program
- Client-Server model
- Threshold time
- Security
- Crash proof

Architecture



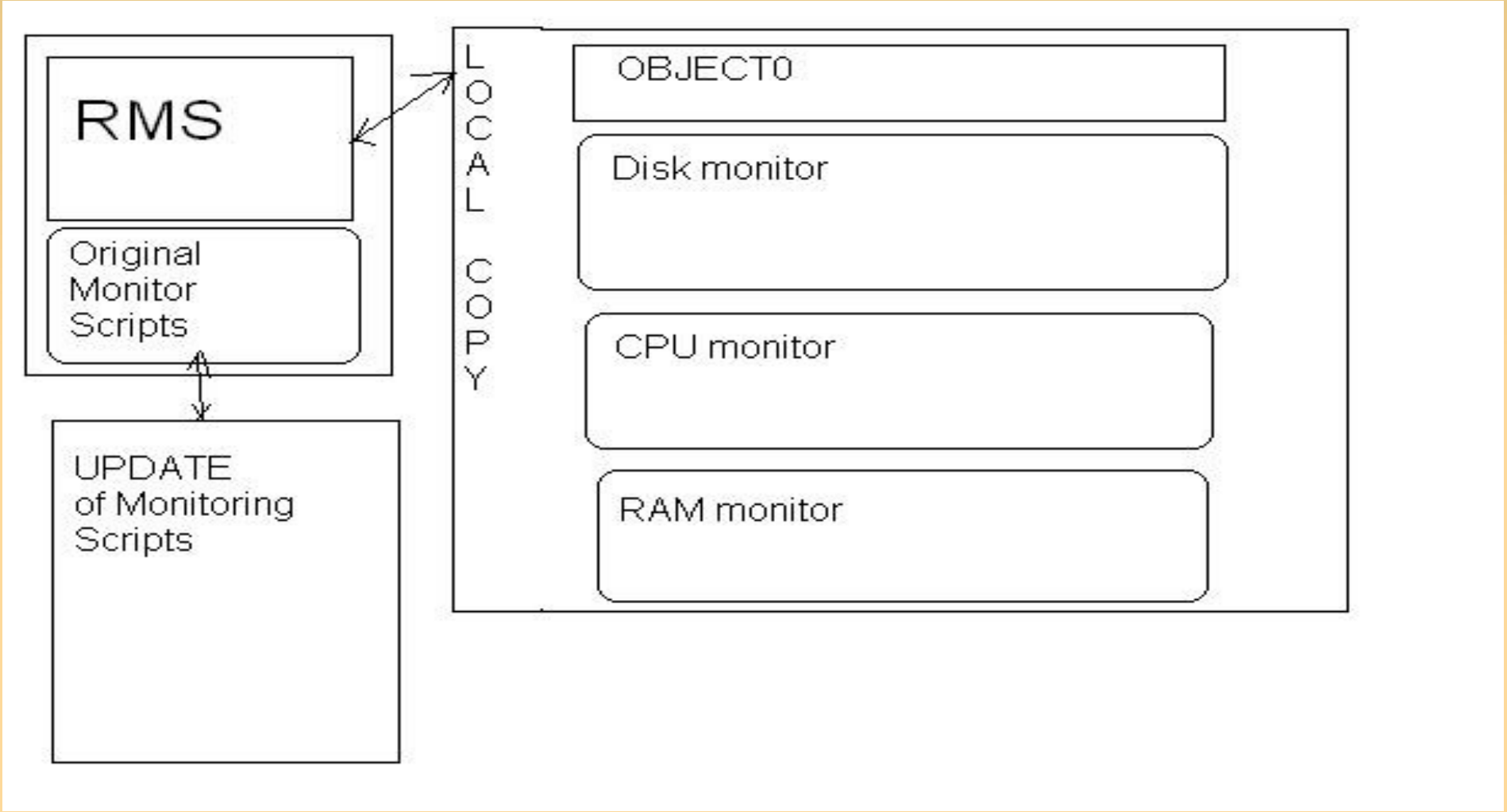
Resource Monitor Server(RMS)

- Instead of running all the monitoring services, which might consume more resources we apply the client - server model
- The Resource Monitor Server listens on a particular port of the server machine
- RMS handles the request from the client

Object Oriented Approach

- Whenever the RMS is started it creates a object of those monitoring scripts locally
- Hence in case of software updates, the local object will not face any problems
- And when the RMS is restarted after update, objects of new updated monitoring scripts are created

OO Approach


RMS
Original Monitor Scripts
UPDATE of Monitoring Scripts
LOCAL COPY
OBJECT0
Disk monitor
CPU monitor
RAM monitor

Server Side Config

- Listening port
- Threshold time for each resource monitor modules

  When the threshold time is crossed the RMS kills the running instance of the object

Security

Last but not the least

- Without guessing or testing the type of attacks that could be carried on a infrastructure, deploying various security functions,cipher algorithms makes the server bulky
- Authentication passwords are md5 encrypted

Attacks

What kind of attacks could be carried on ?

Attacks on Authentication

- Brute Forcing

  FPGA brute forcer

  GPU brute forcer

- Sniffing the network (MITM)

Brute Forcing

Olden method of Attack

- Slight changes in the authentication program can completely avoid this attack

Sniffing-MiTM

- MiTM is carried out by arp spoofing
- I'm not going to use any cryptographic functions

  Just setup static arp entry on both the sever & client the machines

- "arp -s 192.168.1.5 ff-ae-be-ef-ca-fe"

Deployed Security Measures

- Md5 encryption on password transfer
- Secured authentication coding to prevent brute forcing
- Static arp entries
- Displaying Fake Banner
- Skiddy Baiting

Thank You