Security@OSG

Aashish Sharma
OSG Security Team
security@opensciencegrid.org

OSG All Hands Meeting, March 2009


Credit Card Protection
Card
Check
Has your credit card number been STOLEN on the Internet?
card number
/
expires
Check It

Open Science Grid

Fire Box Traps Pranksters

Demonstrated above is a new fire signal box that locks the hand of alarm sender until released by a policeman or fireman with a key, thus deterring the sending of false alarms.

THE sending of false fire alarms by mischievous persons may be eliminated through use of a newly developed call box. To use the device, the sender of an alarm must pass a hand through a special compartment to reach the signal dial. Once the dial has been turned, the sender's hand is locked in the compartment until released by a fireman or policeman with a key.

Open Science Grid


"The chain is no weaker than its strongest link"
Photo by ToHell, 2003-09-23 in Slagsta, SE

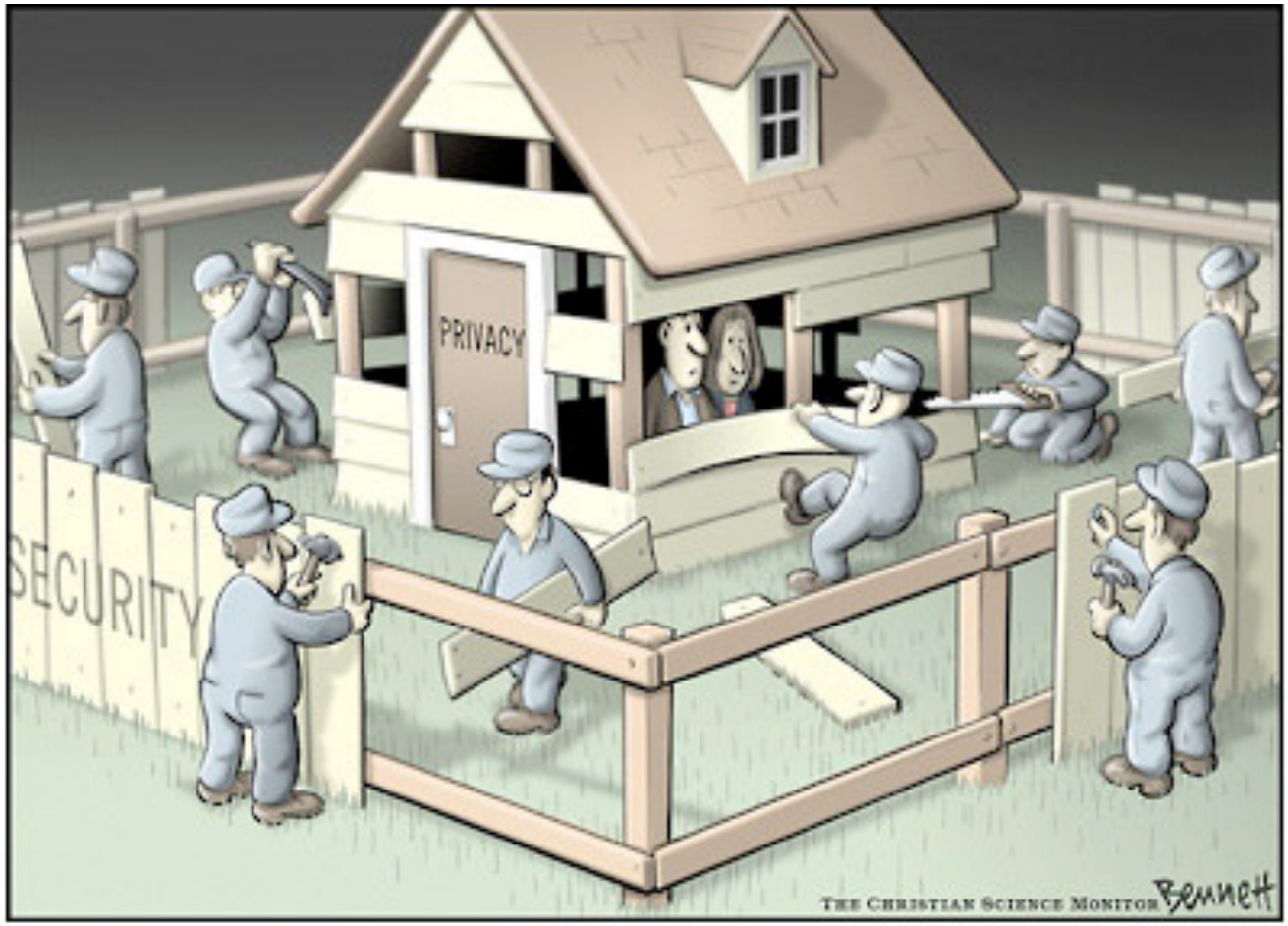
You have requested http://rapidshare.com/files/104063280/978-1588295019.rar (3940 KB).

- Download via GlobalCrossing #2
- Download via GlobalCrossing
- Download via Level(3) #4
- Download via Cogent #2
- Download via TeliaSonera #2
- Download via Level(3) #2
- (•) Download via Teleglobe
- Download via Level(3)
- Download via Level(3) #3
- Download via Cogent
- Download via TeliaSonera

No Premium User. Please solve the Riemann Hypothesis.

$$\pi(x) - \int_0^x \frac{\mathrm{d}t}{\ln(t)}\Bigg| = \mathcal{O}(x^{1/2+\varepsilon}),$$

Solution: [ ] Download via Teleglobe


PRIVACY
SECURITY
THE CHRISTIAN SCIENCE MONITOR
Bennett


Open Science Grid

Open Science Grid

OSG Security

- Security Philosophy
- Security Architecture
- Players involved
- Incident Response

OSG Team Members

- Mine Altunay
- Jim Basney
- Doug Olson
- Anand Padmanabhan
- Ron Cudzewicz
- Aashish Sharma

OSG Security Team Tasks

- Establish policies and procedures
- Identify Risks and Threats
- Determine ways to mitigate these threats and risks
- Co-ordinate the process
- In an event of any incident - Respond appropriately
- Determine extent of incident & damage
- Mitigation and recovery

Security Goals and Purpose

- provide a security framework that
  - enables science
  - promotes autonomous and open science collaboration [VO's, sites, and software providers]
- Keep the balance between
  - openness, which is necessary for science,
  - security is at the core of our work.

Security Team's Roles and responsibility

- OSG security team helps OSG members by providing examples, templates, services and tools

- Ultimate responsibility lies with the member entity to ensure its security.

Operational Security

- Keep an active dialogue with our members
- Evaluating the security of our software stack and releasing timely patches for identified vulnerabilities
- Observing the practices of our VOs and sites, and sending alerts when we detect abnormalities
- Continually performing fire drills to measure readiness and security awareness

Open Science Grid

Education

- Security training of our members
- Teaching best practices
- Learning from our users about difficulties of security practices

Open Science Grid

Site

- Maintain security hygiene of the resources
- Diligence to apply security patches
- cooperating during a security incident
- Notify security team about incidents

A site not meeting their responsibilities may be barred from OSG membership.

Users roles and Responsibilities

As a user of OSG, you are responsible for three aspects of security:

- Protecting your grid identity token
- Abiding by the policies of your Virtual Organization (VO) that authorizes access to resources
- Reporting known or suspected breaches of security

Users: Protecting grid identity token

- PKI X509 digital certificate with a lifetime of one year
- Private key to which only the user has access
  - Typically the private key is stored in a file called $HOME/.globus/userkey.pem.
  - The (public) certificate needs to be accessible to parties and resources to which user will authenticate. It is typically stored in a file called $HOME/.globus/usercert.pem.

Users: Securing Certificates

- Copy userkey.pem to and/or store it only in a file that is accessible to user alone, i.e., to which no one else has privileges. In particular, observe the following:
  - Do not keep unnecessary copies of it.
  - Do not copy it to or store it in AFS or other shared file system.
  - Do not copy it to or store it in a directory that is accessible to the network.

- The private key must be encrypted with a suitably complex passphrase that only you know.
- Typical Unix permissions should be 0400, readable only by owner.

Users: Certificates and key revocation

- You may also keep a copy of your certificate and private key in your web browser.
  - the private key must be encrypted using the features of your browser for encrypting keys and passwords.

  [For Mozilla Firefox this is called the Master Password of the Software Security Device.]
- If your private key is compromised
  - Revoke your certificate immediately and get a new one
- If your VO does not provide instructions on revoking certificate
  - contact the registration authority (RA) that issued the certificate, or directly contact the certificate authority (CA) that issued it.

Service Certificate

- Service itself needs certificate
- Private key not encrypted
- Site admin can request
- More vulnerable
- Sits in root / site admin account
- Which cases use service certificates
  - Job submissions [not recommended]
  - How quickly can you notify CA
  - Revoke Certificates / regular personal proxies
- Cross Job submission

Securing service certificates

- Don't use same certificate for different hosts
- Revoking certificates
  - https://pki1.doegrids.org/ca/ [DoE grids]

Security issues with OSG

- Compromise user accounts
- Compromise certificates
- Vulnerable software/security update
- Disclosure of information [Google cache/Google index - search engines]

Incident Discovery and Reporting

- Always report security incidents to your local/home organization's incident response team.
- Please promptly report security incidents involving OSG resources using any of the following methods:
  - Submit a Ticket
  - Call the Grid Operations Center (GOC) at +1 317-278-9699.
  - Send email to security@opensciencegrid.org.

- If you would like to submit encrypted information
  - User ID: Open Science Grid Security <security@opensciencegrid.org>
  - Key ID: 0x66F456CC
  - Expires: 2009-08-03
  - Fingerprint: 90D3 9626 E6AF CE96 40FB 15FC B399 2A3F 66F4 56CC

Incident discovery and reporting

- Please include the following information in your report:
  - Your name:
  - Your email address:
  - Your phone number:
  - An alternate number such as a cell phone:
  - What is your affiliation with the OSG? Which Virtual Organization are you a member of?
  - Did this incident occur on a Site machine or on a VO machine or on your personal computer? Please provide detailed information (names, IPs, URLs, etc.):
  - Is your grid identity (certificate and/or proxy) compromised?
  - Incident description, including time(s), systems involved and their description:
  - Any additional comments or questions?

Incident Response: Requirement

- Basic questions concerning any incident
  - who, what, where, when, and how ?
- Retaining all relevant information,
  - Timestamps
  - the digital identity of the user
  - sufficient to identify for each service instance
- Every security event including at least the following: connect, authenticate, authorize (including identity changes) and disconnect.

Incident Response

- Confirmation
- Communication
- Containment
- Eradication
- Recovery
- Closure

When you get an incident notification

- Different site
- OSG Security Team
- Administrators [support center, VO]
- Users [grid users]
- Developers

Incident Response: Analysis

- IRT member confirms and acknowledges the incident
- Start collecting relevant data and contact the notification site if more information is needed
- Bring in additional persons as per requirement [software providers, partners, other fellow groups]

Checklist for compromised account

- Notification of account compromise from a VO or partner grid site
  - Verification that user credentials are also stored on compromised host (s)
  - Get the date of compromise and verify the lifetime of certificates issued
- Verification that certificate was used by the user / miscreants
- Disable/Revoke certificate
- Contact user with a 'questionnaire'

Checklist (2)

- Questionnaire :
  - Do you have notification from any other site ?
  - What all different certificates/credentials do you use ?
  - What all hosts have you stored your certificates on ?
  - When was the last use of certificate ?
  - do you have same password/pass-phrase used on certificate used at other places ?
  - Have you verified integrity of all hosts (including personal machines) ?
  - Do you know how someone may have got your credentials ?
  - If you can provide security contact information for your site ?

Open Science Grid

Checklist (3)

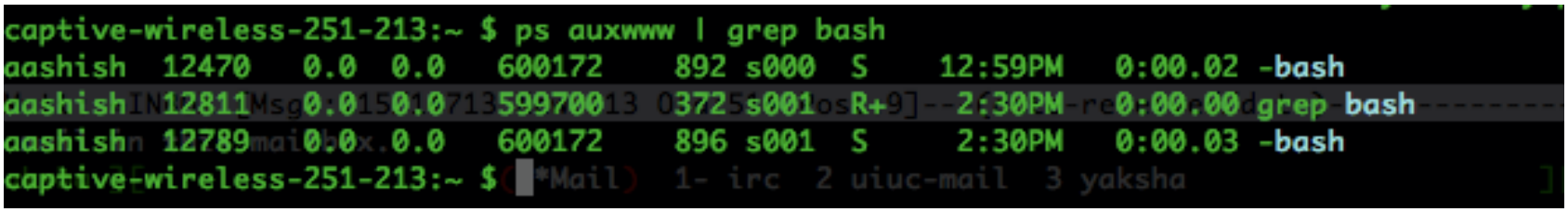
- Gather the list of IP/hostname the compromise user account [miscreants] are coming from
- cross check these IP's with relevant logs to determine if other accounts are compromised
- Issue new certificate once user confirms clean up has been done.

Incident Response: Analysis

- Things to records
  - Initial notification alert
  - Assessment
  - Status information
  - Incident timeline
  - Other technical details
- Actions are based on classification of urgency and severity

Determining compromise

- Look for running process/unusual process
- # ps –auxwww
- Detail investigation for a process
  - lsof –P -i –n



Detailed process information

```
captive-wireless-251-213:~$ lsof -P -i -n
COMMAND     PID   USER   FD   TYPE             DEVICE SIZE/OFF NODE NAME
SystemUIS   245 aashish   10u  IPv4 0x3b53518       0t0  UDP *:*
Adium       276 aashish   10u  IPv4 0x3f8066c       0t0  TCP 141.142.251.213:58289->209.85.201.125:5222 (ESTABLISHED)
Adium       276 aashish   11u  IPv4 0x3b536c8       0t0  UDP *:49186
Adium       276 aashish   12u  IPv4 0xc92466c       0t0  TCP 141.142.251.213:58290->66.163.181.178:5050 (ESTABLISHED)
Adium       276 aashish   15u  IPv4 0x8f66270       0t0  TCP 141.142.251.213:58291->66.163.181.178:5050 (ESTABLISHED)
iChatAgen   284 aashish    4u  IPv4 0xbbc4288       0t0  UDP 127.0.0.1:55812->127.0.0.1:55812
iChatAgen   284 aashish    7u  IPv4 0xa00566c       0t0  TCP 141.142.251.213:58297->209.85.201.125:5222 (ESTABLISHED)
iChatAgen   284 aashish   11u  IPv4 0xb37de64       0t0  TCP 141.142.251.213:58318->205.188.9.238:5190 (ESTABLISHED)
Mail        728 aashish   15u  IPv4 0x87b9270       0t0  TCP 141.142.251.213:53637->74.125.93.111:993 (CLOSE_WAIT)
Mail        728 aashish   24u  IPv4 0x99a2a68       0t0  TCP 141.142.251.213:58302->64.233.183.111:993 (ESTABLISHED)
Mail        728 aashish   25u  IPv4 0xc924270       0t0  TCP 141.142.251.213:58309->64.233.183.111:993 (ESTABLISHED)
Mail        728 aashish   29u  IPv4 0x87bba68       0t0  TCP 141.142.251.213:58313->64.233.183.111:993 (CLOSE_WAIT)
Mail        728 aashish   30u  IPv4 0x9ca966c       0t0  TCP 141.142.251.213:58330->64.233.183.109:993 (CLOSE_WAIT)
Mail        728 aashish   31u  IPv4 0x9d35270       0t0  TCP 141.142.251.213:60001->64.233.183.111:993 (ESTABLISHED)
Mail        728 aashish   32u  IPv4 0xd37fa68       0t0  TCP 141.142.251.213:59570->64.233.183.111:993 (ESTABLISHED)
Mail        728 aashish   33u  IPv4 0xc927e64       0t0  TCP 192.168.2.5:53470->74.125.47.109:993 (ESTABLISHED)
Mail        728 aashish   34u  IPv4 0x9651270       0t0  TCP 141.142.251.213:53639->74.125.93.111:993 (ESTABLISHED)
Mail        728 aashish   37u  IPv4 0xb37d270       0t0  TCP 141.142.251.213:58314->64.233.183.111:993 (ESTABLISHED)
Mail        728 aashish   38u  IPv4 0xc924e64       0t0  TCP 192.168.2.5:53481->74.125.47.109:993 (ESTABLISHED)
Mail        728 aashish   41u  IPv4 0x87b966c       0t0  TCP 141.142.251.213:58303->64.233.183.111:993 (ESTABLISHED)
Mail        728 aashish   42u  IPv4 0x9ca9270       0t0  TCP 141.142.251.213:58304->64.233.183.111:993 (ESTABLISHED)
Mail        728 aashish   45u  IPv4 0x8f66a68       0t0  TCP 141.142.251.213:58310->64.233.183.111:993 (ESTABLISHED)
Mail        728 aashish   46u  IPv4 0x99a266c       0t0  TCP 141.142.251.213:58312->64.233.183.111:993 (ESTABLISHED)
Mail        728 aashish   51u  IPv4 0x9651a68       0t0  TCP 141.142.251.213:58311->64.233.183.111:993 (ESTABLISHED)
iTunes      820 aashish   23u  IPv4 0x5ae8270       0t0  TCP *:3689 (LISTEN)
Safari    11435 aashish   28u  IPv4 0x87b9a68       0t0  TCP 127.0.0.1:51534->127.0.0.1:8118 (CLOSE_WAIT)
Safari    11435 aashish   32u  IPv4 0x9ca9e64       0t0  TCP 192.168.2.2:51531->141.142.2.140:443 (CLOSED)
Safari    11435 aashish   39u  IPv6 0xdbfdbe8       0t0  TCP [::1]:60091->[::1]:60090 (TIME_WAIT)
ssh       12489 aashish    3u  IPv4 0xa005a68       0t0  TCP 141.142.251.213:58321->141.142.228.5:22 (ESTABLISHED)
captive-wireless-251-213:~$
```

Finding unusal services

- chkconfig --list

```
NetworkManager  0:off  1:off  2:off  3:off  4:off  5:off  6:off
NetworkManagerDispatcher  0:off  1:off  2:off  3:off  4:off  5:off  6:off
acpid           0:off  1:off  2:off  3:on   4:on   5:on   6:off
amd             0:off  1:off  2:off  3:off  4:off  5:off  6:off
anacron         0:off  1:off  2:on   3:on   4:on   5:on   6:off
apmd            0:off  1:off  2:on   3:on   4:on   5:off  6:off
arptables_jf    0:off  1:off  2:on   3:on   4:on   5:on   6:off
arpwatch        0:off  1:off  2:off  3:off  4:off  5:off  6:off
atd             0:off  1:off  2:off  3:on   4:on   5:on   6:off
auditd          0:off  1:off  2:on   3:on   4:on   5:on   6:off
autofs          0:off  1:off  2:off  3:on   4:on   5:on   6:off
avahi-daemon    0:off  1:off  2:off  3:on   4:on   5:off  6:off
avahi-dnsconfd  0:off  1:off  2:off  3:off  4:off  5:off  6:off
bgpd            0:off  1:off  2:off  3:off  4:off  5:off  6:off
bluetooth       0:off  1:off  2:on   3:on   4:on   5:off  6:off
```

Unusual files

- Look for unusual suid/sgid root files
  - find / -uid 0 –perm -4000 –perm 2000 –present
- Files with names “dots” and “spaces” (…, “.. “, “ “, “. “)
  - find / -name “ “ –print
- Always always : ls –a

Open Science Grid

More unusual files

- Finding unlink binaries
  - Attacker runs a backdoor and then unlinks the binary so that regular “ls” won’t show it
  - lsof +L1
- Look for files with link count less then 1
- rpm verify –Va [especially files in /bin/, /usr/bin/, /usr/sbin]

Unusual network usage

- netstat –antupe

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User       Inode      PID/Program name
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      0          8075       2346/portmap
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      0          7300334    25226/cupsd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      0          8710       2524/sendmail: acce
tcp        0      0 127.0.0.1:6010          0.0.0.0:*               LISTEN      500        12574630   21606/14
tcp        0      0 127.0.0.1:6011          0.0.0.0:*               LISTEN      500        12580587   22275/15
```

Unusual scheduled tasks

- Look for cron jobs scheduled to be run as the user/ root
  - Crontab –u root –l
- Look for system wide cron jobs
  - cat /etc/crontab
  - ls /etc/cron.*

Unusual accounts

- /etc/passwd for new/unexpected accounts
- Accounts with uid and gid 0
  - grep :0: /etc/passwd
- Files left with non-existent user as the owner
  - find / -nouser –print

Incident Response: Mitigation/ Containment

- Actions to take
  - Banning the user [remove mapping]
  - blacklist of users
  - Revoke certificates
  - Disable services
  - Patch/update/upgrade/offline
- Monitor progress
- Affected parties list
- Response times
- Definition of end of event

Update about CRL's

- CA managemnt tools
- User certificate is revoked
  - How to update CRL's (vdt-control –list)
  - vdt-update-certs
  - fetch-crl
  - gums-host-cron

Incident Response: Eradication /Recovery

- Eradicate vulnerability
- Recovery
  - Affected users obtain new credentials
  - Accounts and services are re-enabled.

Update CRL's

- First line of defense
- Don't have banning capabilties
- Rely on CA's and how to do that
- Which CRL's are updated and which are not

What can/could have helped

- Log collection
  - Central syslog server
- Network flow logs
- IDS/Firewall logs
- Relevant logs for grid computing

Log Collection: Purpose

- Identify the source of all actions
  - executables
  - file transfers
  - pilot jobs
  - portal jobs
- The individual who initiated them.

Log Collection: Action

- fine-grained controls
  - blocking the originating user
  - monitoring to detect abnormal behavior

- It is essential to be able to understand the cause and to fix any problems before re-enabling access for the user.

What can/could have helped

GRAM	globus-gatekeeper.log	contains authentication and job state change information for jobs submitted to the CE
GRIDFTP	gridftp-auth.log	has authentication information for files transferred through the gridftp server
WS-GRAM	container-real.log	has authentication information for jobs submitted through the web services GRAM service

Open Science Grid

Monitoring

- Samhain/trip wire - file integrity monitoring software
- Log archives [Simple event correlator]
- Netflows [argus, nfdump/nfsen]
- IDS Bro [www.bro-ids.org]

Monitoring: Samhain

- **Host-based intrusion detection system (HIDS)**
  - client/server architecture allows central logging, central storage of baseline databases and client configurations, and central updates of baseline databases.
  - Web-based management console
  - Multiple logging facilities
  - Offers PGP-signed database and configuration files, a stealth mode, and several more features to protect its integrity.

Monitoring: Logwatch

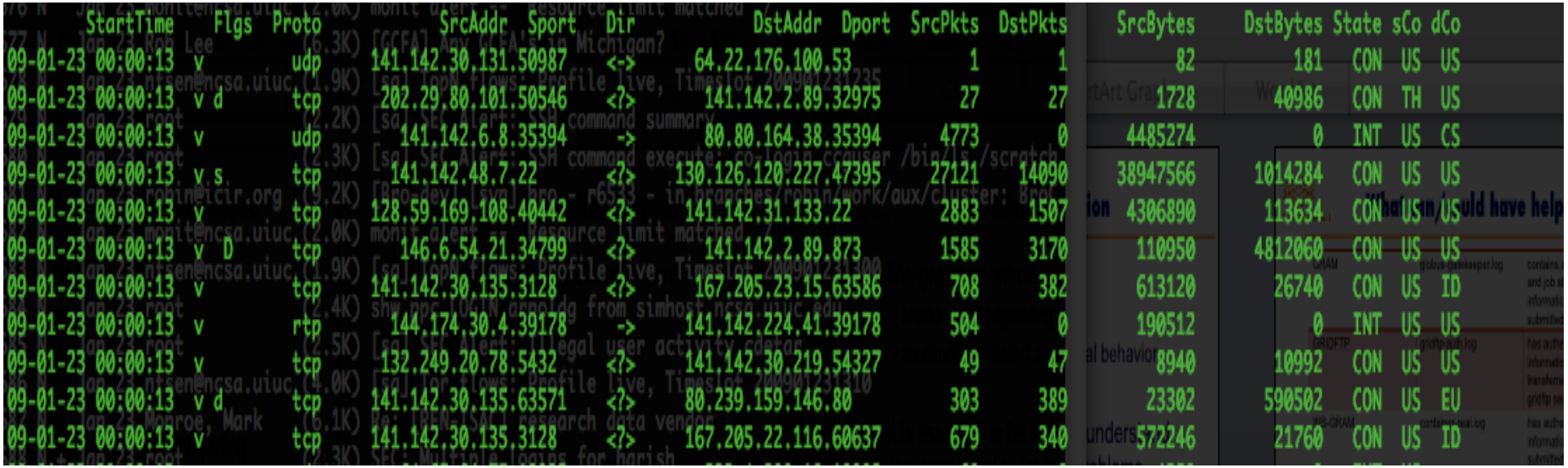
- Simple Event Correlation
  - Aggregates, normalizes, correlates and analyzes event log data
  - Alert based on thresholds/defined events
  - Account creation
  - Direct root logins
  - Multiple logins [hosts/ips/users]

Monitoring: IDS

- Network Intrusion Detection System (NIDS)
  - passively monitors network traffic
  - protocol analysis
  - detection of attacks [signature based, event based]
  - unusual activities [running of certain services, failed login attempts, clear text passwords]

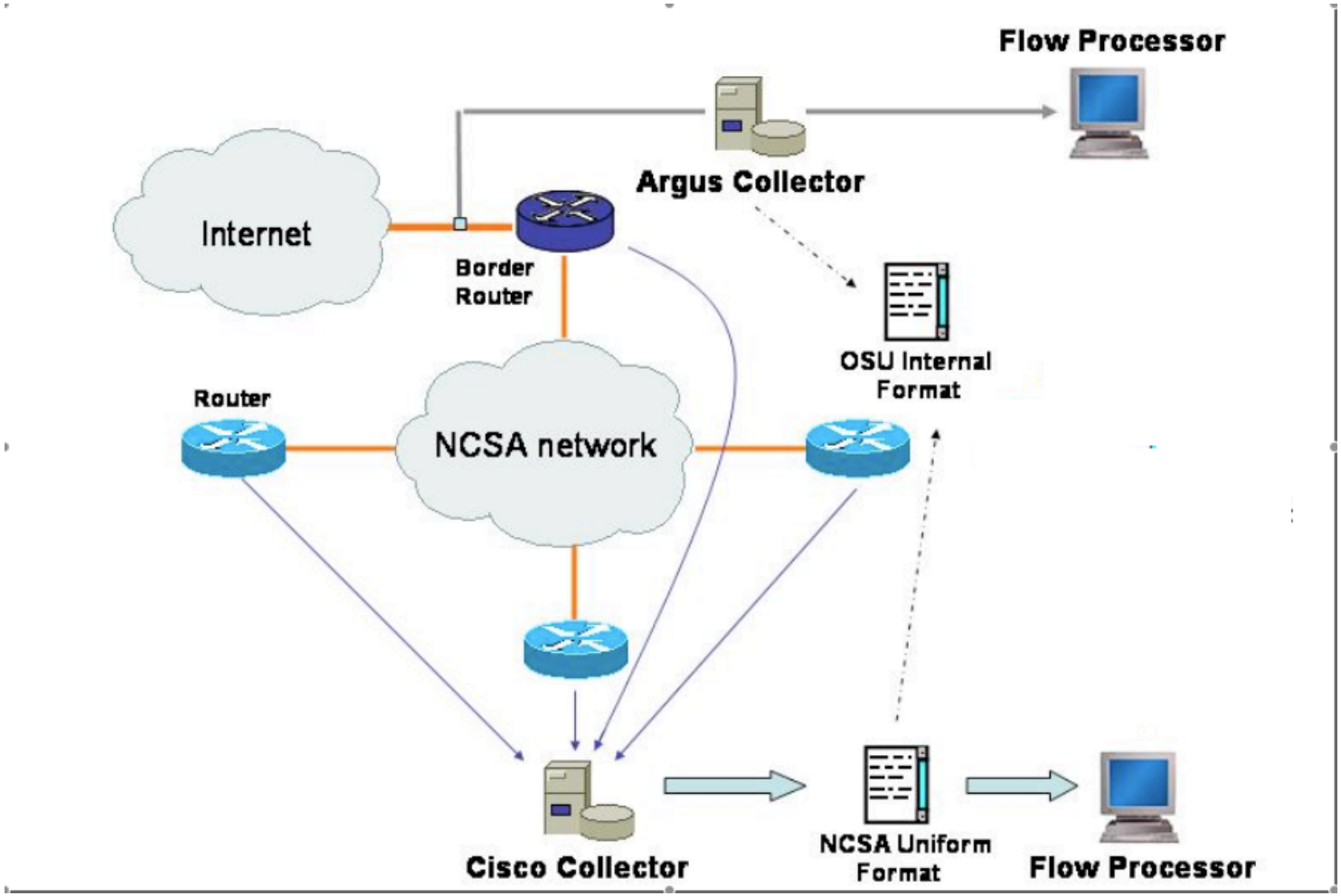
Monitoring: Netflows

- Netflows: network traffic logs
  - timestamps, ip addres, protocols, ports
- Scalable for catching all the traffic
- Good for forensic time lines
- Real time alerts on blacklist IP address



StartTime	Flgs	Proto	SrcAddr	Sport	Dir	DstAddr	Dport	SrcPkts	DstPkts	SrcBytes	DstBytes	State	sCo	dCo
09-01-23 00:00:13	v	udp	141.142.30.131.50987		<->	64.22.176.100.53		1	1	82	181	CON	US	US
09-01-23 00:00:13	v d	tcp	202.29.80.101.50546		<?>	141.142.2.89.32975		27	27	1728	40986	CON	TH	US
09-01-23 00:00:13	v	udp	141.142.6.8.35394		->	80.80.164.38.35394		4773	0	4485274	0	INT	US	CS
09-01-23 00:00:13	v s	tcp	141.142.48.7.22		<?>	130.126.120.227.47395		27121	14090	38947566	1014284	CON	US	US
09-01-23 00:00:13	v	tcp	128.59.169.108.40442		<?>	141.142.31.133.22		2883	1507	4306890	113634	CON	US	US
09-01-23 00:00:13	v D	tcp	146.6.54.21.34799		<?>	141.142.2.89.873		1585	3170	110950	4812060	CON	US	US
09-01-23 00:00:13	v	tcp	141.142.30.135.3128		<?>	167.205.23.15.63586		708	382	613120	26740	CON	US	ID
09-01-23 00:00:13	v	rtp	144.174.30.4.39178		->	141.142.224.41.39178		504	0	190512	0	INT	US	US
09-01-23 00:00:13	v	tcp	132.249.20.78.5432		<?>	141.142.30.219.54327		49	47	8940	10992	CON	US	US
09-01-23 00:00:13	v d	tcp	141.142.30.135.63571		<?>	80.239.159.146.80		303	389	23302	590502	CON	US	EU
09-01-23 00:00:13	v	tcp	141.142.30.135.3128		<?>	167.205.22.116.60637		679	340	572246	21760	CON	US	ID

A typical netflow collector setup



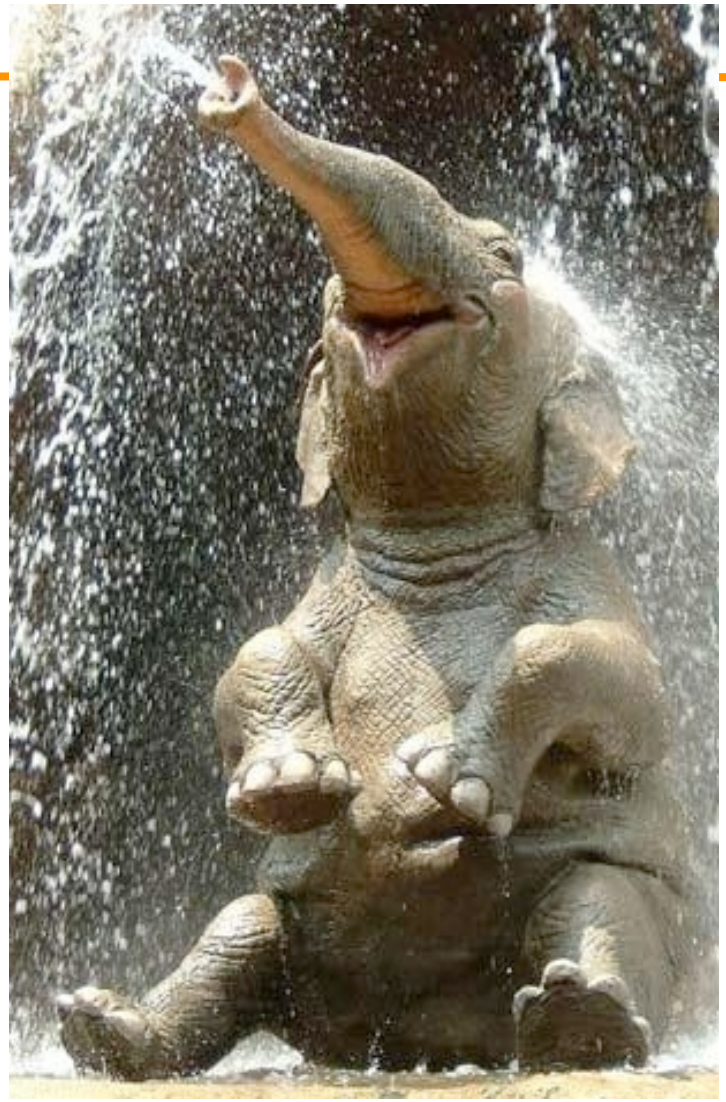
Avoiding an incident

- Patch/update/upgrade
- Avoid administrative mistakes
  - [leaving IP tables off]
  - [creating test account]
- Remember production machines are important but administrative machines are as important too
- Don’t forget test machines

RANT

Otherwise its just a way to carry an elephant


CHHINA FARM



Open Science Grid

Questions?

?

aashish@ncsa.uiuc.edu