

Security Risks in the Grid

Elisa Heymann

Computer Architecture and
Operating Systems Department
Universitat Autònoma de Barcelona

elisa@cs.wisc.edu

Barton P. Miller

James A. Kupsch

Computer Sciences Department
University of Wisconsin

bart@cs.wisc.edu

UW-Madison
July 22, 2010

Who we are



**Bart Miller
Jim Kupsch
Rohit Koul
Wenbin Fang**



**Elisa Heymann
Eduardo Cesar
Jairo Serrano
Guifré Ruiz**

What should you expect

- > Users
 - Understand the risks
 - Prevention
- > Administrators
 - Understand SW configuration
 - Manage processes, resources, privileges
- > Developers
 - Secure programming techniques

What do we do

- > Make grid software more secure
- > Make a good assessment more automated
- > Teach tutorials:
 - Security risks
 - Vulnerability assessment
 - Secure programming

Roadmap

- > Introduction: Some fun?
- > Talk the talk
- > What the bad guys can do to you
- > What can you do?

Why do we do it

The Washington Post

Computer System Under Attack

Commerce Department Targeted; Hackers Traced to China

By Alan Sipress

Washington Post Staff Writer

Friday, October 6, 2006

Hackers operating through Chinese Internet servers have launched a debilitating attack on the computer system of a sensitive Commerce Department bureau, forcing it to replace hundreds of workstations and block employees from regular use of the Internet for more than a month, Commerce officials said yesterday.



Open Science Grid

Why do we do it

Security on  msnbc.com

U.S. eyes N. Korea for 'massive' cyber attacks

South Korean security company expects additional wave of attacks

msnbc.com staff and news service reports
updated 7/9/2009 12:31:50 AM

SEOUL, South Korea — U.S. authorities on Wednesday eyed North Korea as the origin of the widespread cyber attack that overwhelmed government Web sites in the United States and South Korea, although they warned it would be difficult to definitively identify the attackers quickly.

The powerful attack that targeted dozens of government and private sites underscored how unevenly prepared the U.S. government is to block such multipronged assaults.



WISCONSIN
MADISON



Autònoma
de Barcelona




Why do we do it

TechCrunch

Google Defends Against Large Scale Chinese Cyber Attack: May Cease Chinese Operations

by **Michael Arrington** on Jan
12, 2010

Google is **releasing**  information about a "highly sophisticated and targeted attack" on their corporate infrastructure that occurred last month. The attack originated in China and resulted in the "theft of intellectual property from Google." In light of the attack Google is making sweeping changes to its Chinese operations.

o



C

Home > Security

News

Over 75,000 systems compromised in cyberattack

Kneber botnet used to gather wide range of corporate, personal data, NetWitness says

By Jaikumar Vijayan

February 18, 2010 07:19 AM ET

COMPUTERWORLD

Computerworld - *Correction: An earlier version of this story incorrectly said the cyberattacks began in 1998. They began in 2008.*

Security researchers at Herndon, Va.-based NetWitness Corp. have unearthed a massive botnet affecting at least 75,000 computers at 2,500 companies and government agencies worldwide.

The Kneber botnet, named for the username linking the affected machines worldwide, has been used to gather login credentials to online financial systems, social networking sites and e-mail systems for the past 18 months, according to NetWitness.

A 75GB cache of stolen data discovered by NetWitness included 68,000 corporate login credentials, login data for user accounts at Facebook, [Yahoo](#) and Hotmail, 2,000 SSL certificate files and a large amount of highly detailed "dossier-level" identity information. In addition, systems compromised by the botnet also give attackers remote access inside the compromised network, the company said.



WISCONSIN
MADISON



Autònoma
de Barcelona



Why do we do it

- Machines belonging to a grid site are accessible from the Internet
- Those machines are continuously probed:
 - Attackers trying to **brute-force passwords**
 - Attackers trying to break **Web applications**
 - Attackers trying to break into servers and **obtain administrator rights**

Why do we do it

- > SW has **vulnerabilities**
- > Grid SW is **complex** and **large**
- > Vulnerabilities can be exploited by legal users or by others

Why do we do it

- > **Attacker** chooses the time, place, method, ...
- > **Defender** needs to protect against all possible attacks (currently known, and those yet to be discovered)

Security

- Security is a **permanent process**
- Security **cannot** be proven
- Security is **difficult to achieve** and **expensive**, and only to $100\% - \epsilon$
- Security involves:
 - Managers
 - Developers
 - Admins
 - **Users**

Admin Perspective

Just to get a feeling ...

- Condor configured to track processes
- When the job exits no processes are left behind

```
SLOT1_USER = condor_user1
```

```
SLOT2_USER = condor_user2
```

```
STARTER_ALLOW_RUNAS_OWNER = False
```

```
DEDICATED_EXECUTE_ACCOUNT_REGEX =  
condor_user1 || condor_user2
```

Admin Perspective

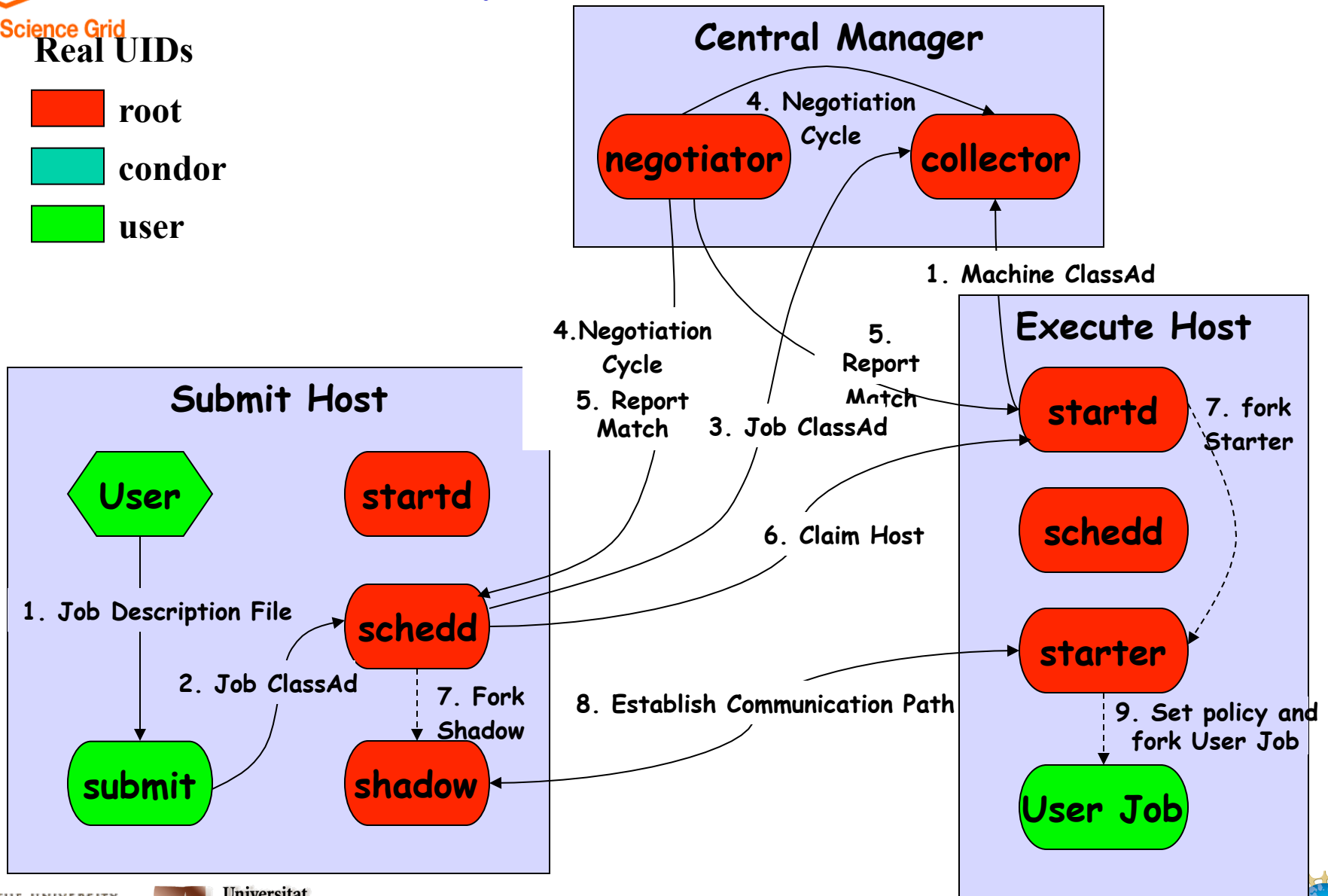
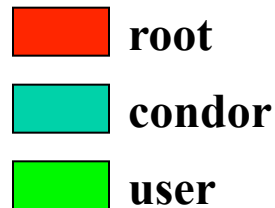
Just to get a feeling ...

- Depending on how Condor is installed, daemons run as root or as a non-root user



Open Science Grid

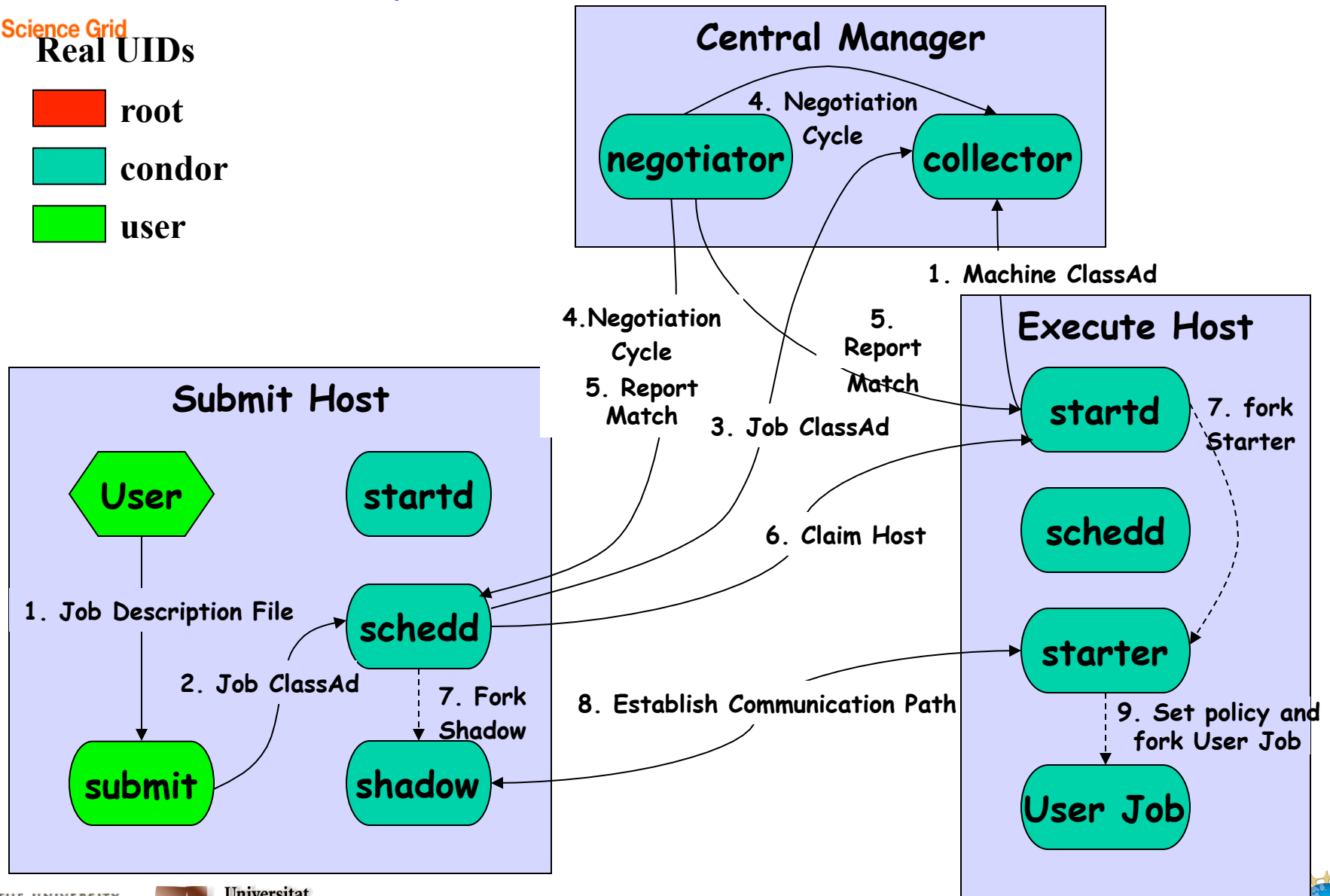
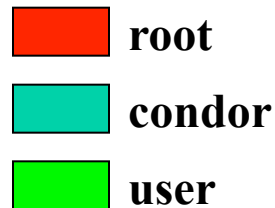
Real UIDs



Admin Perspective. Non-Root Install

Open Science Grid

Real UIDs



Developer Perspective

Just to get a feeling ... An example

- > Find as many potential vulnerabilities as you can (there may be more than one)
- > Assume:
 - pointer arguments are never NULL
 - strings are always NULL terminated

```
/* Safely Exec program: drop privileges to user uid and group
 * gid, and use chroot to restrict file system access to jail
 * directory. Also, don't allow program to run as a
 * privileged user or group */
```

```
1. void ExecUid(int uid, int gid, char *jailDir,
2.             char *prog, char *const argv[])
3. {
4.     if (uid == 0 || gid == 0) {
5.         FailExit("ExecUid: root uid or gid not allowed");
6.     }
7.
8.     chroot(jailDir); /* restrict access to this dir */
9.
10.    setuid(uid);      /* drop privs */
11.    setgid(gid);
12.
13.    fprintf(LOGFILE, "Execvp of %s as uid=%d gid=%d\n",
14.            prog, uid, gid);
15.    fflush(LOGFILE);
16.
17.    execvp(prog, argv);
18. }
```

Security in a Nutshell

Basic Concepts

- › Authentication
- › Cryptography
- › Certificates
- › Authorization Delegation

Authentication

- > Ability to identify each user of the system
- > Ability to identify the processes running
- > Prove identity using
 - What you have (key, card)
 - What you know (password)
 - What you are (fingerprint, retina pattern)

Cryptography

- Limits the potential senders and receivers of a message
- Based on secrets (keys)
- Used for authentication
 - Enables the receiver to verify that the message was created by some specific sender
 - Digital signature
 - Allows to check if the message was modified (integrity)
 - Public key, Private key (sender private key and receiver sender's public key)

Cryptography

> Encryption

- Enables the sender to ensure that only a specific receiver can read the message (confidentiality)
 - Symmetric encryption (secret shared key)
 - Asymmetric encryption
 - Public key, Private key (using the receiver's public key)

Certificates

- Obtained and signed from a **Certification Authority**
- Used to verify the **validity** of a public key
- Comparable to **capabilities**
 - List the access rights of the holder over resources
 - Identity, attribute, value
- Should be protected by a digital signature
- Hierarchical trust model
- Certificate Revocation List
- Restricted lifetime of certificates

Delegation

- Passing identity and access rights from one process to another
- Implemented through a **proxy**
 - Token associated to privileges and restrictions
- Chain of delegations

User Perspective




What the bad guys can do

> Attacks from inside The Argus

BRIGHTON NEWS

Rude awakening for dawn drivers

7:38am Friday 27th October 2006

 Print  Email  Share

By Louise Acford »

Early morning motorists got a shock yesterday when digital car park signs were tampered with by computer hackers and were left displaying an obscene message.

The message appeared on all similar signs around Crawley at about 6.45am.

Thousands of motorists travelling into the town would have been subjected to the unsavoury advice.




User Perspective

What the bad guys can do

> Attacks from outside

Page last updated at 11:54 GMT, Tuesday, 20 January 2009

 [E-mail this to a friend](#)

 [Printable version](#)

Clock ticking on worm attack code

Experts are warning that hackers have yet to activate the payload of the Conficker virus.

The worm is spreading through low security networks, memory sticks, and PCs without current security updates.

The malicious program - also known as Downadup or Kido - was first discovered in October 2008.

The worm can also spread via USB flash drives.

Although the spread of the worm appears to be levelling off, there are fears someone could easily take control of any and all of the 9.5m infected PCs.

User Perspective

What the bad guys can do

- Gain root access
- Privilege escalation
 - Gain other user access (admin, condor)
- Hijack machines
 - Attack the process running there

User Perspective

What the bad guys can do

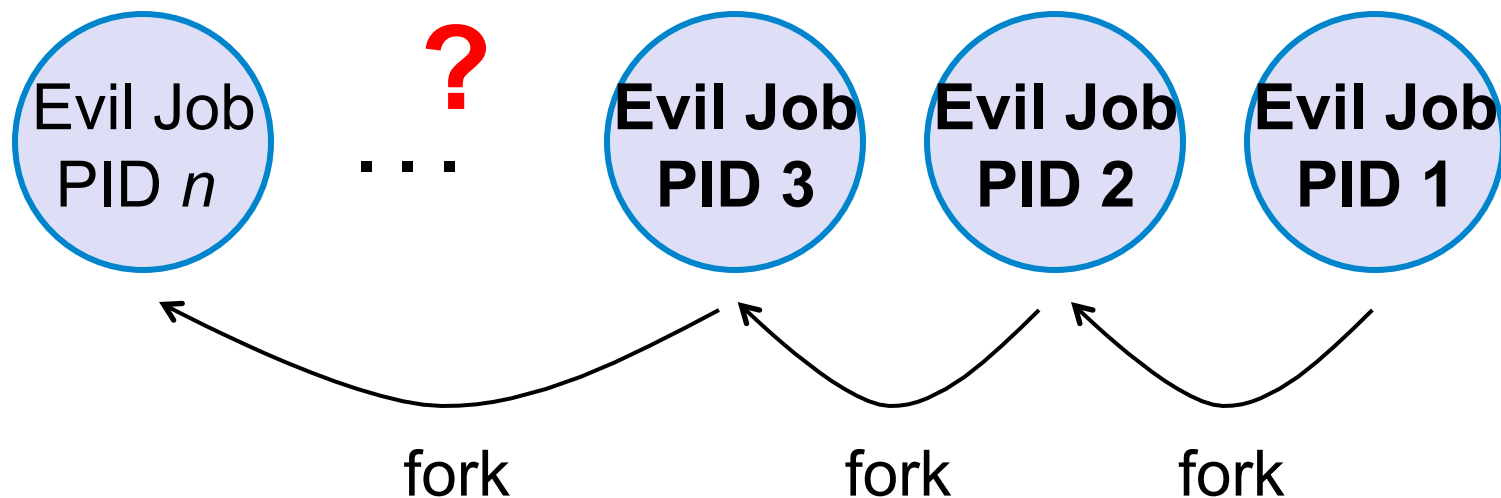
- > Injections
 - Command
 - SQL
 - Directory traversal
 - Log
- > Denial of Service (DoS)

User Perspective

What the bad guys can do

> Hijack machines

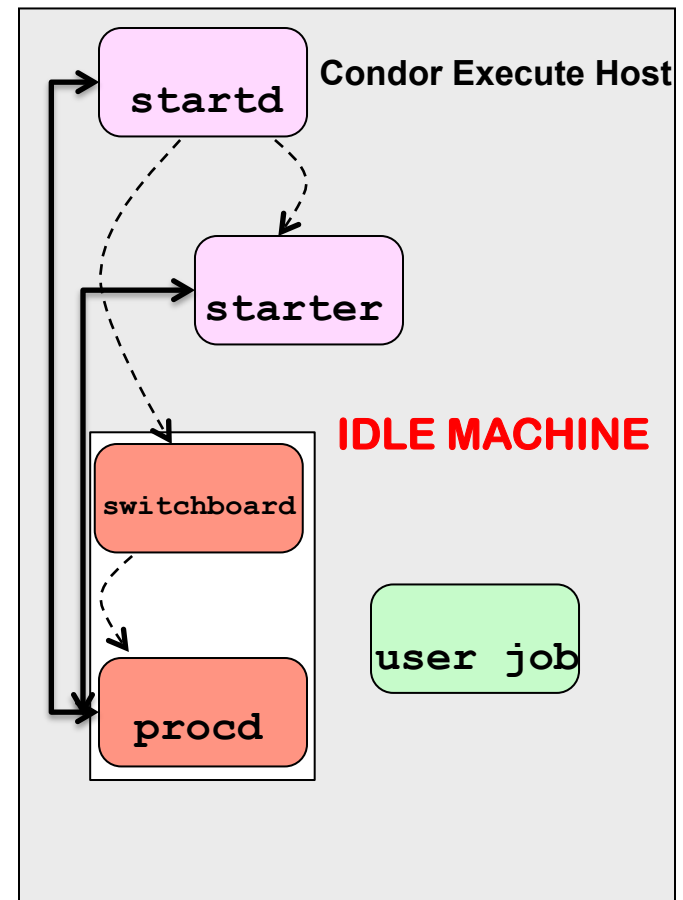
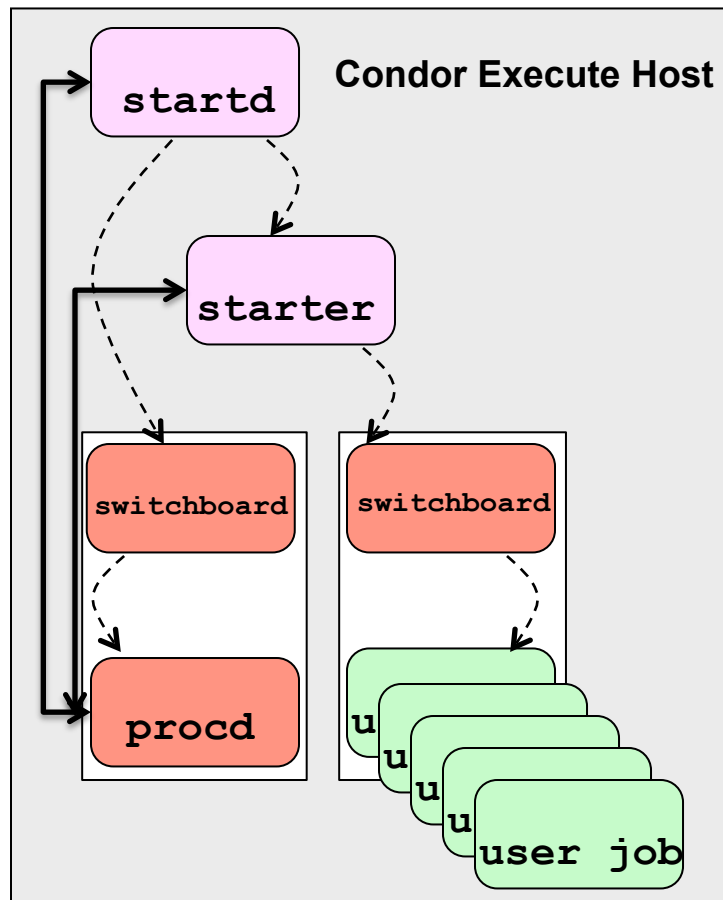
- Process escapes Condor control: keep forking and exiting to escape detection.



User Perspective

What the bad guys can do

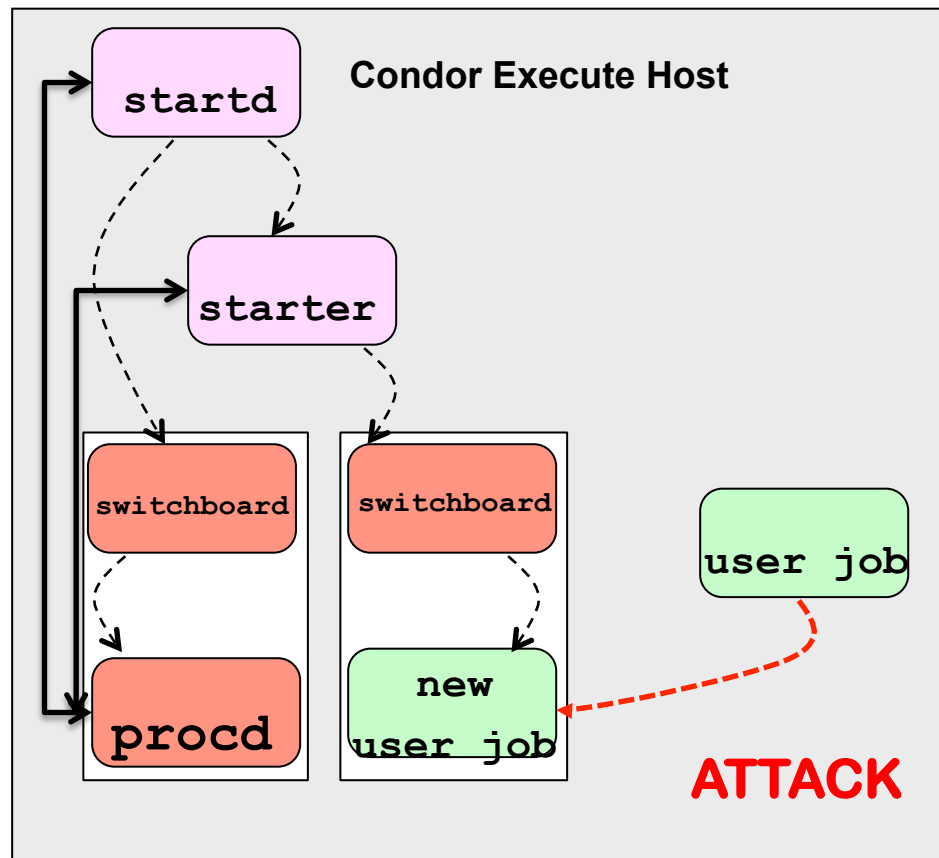
> Hijack machines



User Perspective

What the bad guys can do

- > Hijack machines



User Perspective

What the bad guys can do

- Hijack machines (con'd):
 - Condor believes the job is gone
 - The remaining process can do anything to new user jobs running on that machine
 - This is the same problem that the Condor team fixed years ago

User Perspective

What the bad guys can do

- Denial of Service
 - An attacker can prevent updates in the Condor-Quill database

```
condor_qedit 1.0 `perl -e 'print "x"x2001'` foo
```

User Perspective

What the bad guys can do

- > **GRATIA**: The OSG Accounting System
 - Maintains a Grid-wide view of resource utilization.
 - Job Submission (Priority in the batch queue, CPU time, Memory usage)
 - Storage (Disk usage, Tape storage)
- > Accounting Information *easily* available to people (web interface) and to applications (Web Services)

User Perspective

What the bad guys can do

- > Background
 - Gratia Condor Probe deletes debug files in /tmp, does some computation and then re-creates the debug files in /tmp.
 - Gratia Condor Probe has weak validation mechanism (does not validate the job parameters properly)
 - Symbolic links and Open
 - If files are created using `O_CREAT` without `O_EXCL` flag and the final component of the file path is a symbolic link, the file is created where the symbolic link points.

User Perspective

What the bad guys can do

> Background

- Gratia Condor Probe deletes debug files in /tmp, does some computation and then re-creates the debug files in /tmp.

What happens if we create a symbolic link to the pathname after the operation that deletes the files, but before the one that opens and creates them. Can we win this race?

- Symbolic links and Open
 - If files are created using `O_CREAT` without `O_EXCL` flag and the final component of the file path is a symbolic link, the file is created where the symbolic link points.

User Perspective


What the bad guys can do

Can we exploit the weakness in validation mechanism to make it write something “meaningful” to a “useful” system file?

- Gratia Condor Probe has weak validation mechanism (does not validate the job parameters properly)
- Symbolic links and Open
 - If files are created using `O_CREAT` without `O_EXCL` flag and the final component of the file path is a symbolic link, the file is created where the symbolic link points.




Gratia-Probe-2010-002

Open  rohit@localhost:~

```
[rohit@localhost ~]$ su 'r.TimeDuration('
sh-3.2#
```



Gratia-Probe-2010-002

Open  rohit@localhost:~

```
[rohit@localhost ~]$ su 'r.TimeDuration('
sh-3.2#
sh-3.2#
sh-3.2# chfn
Changing finger information for root.
Name [root]: █
```


What can you do?

> Users

- Choose good passwords
- Take care of your certificates
- Never share identities
- Report strange behavior

> Sys Admins

- Minimal privileges
- Configuration settings
- Check log files
- Upgrades

What can you do?

- > **Developers**
 - Learn secure programming
- > **Managers**
 - Prioritize security, invest in it, and have assessment and response strategies

Security Risks in the Grid

Elisa Heymann

Computer Architecture and
Operating Systems Department
Universitat Autònoma de Barcelona

elisa@cs.wisc.edu

Barton P. Miller

James A. Kupsch

Computer Sciences Department
University of Wisconsin

bart@cs.wisc.edu

UW-Madison
July 22, 2010



Studied Systems



Condor, University of Wisconsin
Batch queuing workload management system



SRB, SDSC
Storage Resource Broker - data grid



MyProxy, NCSA
Credential Management System



glExec, Nikhef
Identity mapping service



CrossBroker, Universitat Autònoma de Barcelona
Resource Manager for Parallel and Interactive Applications



Gratia Condor Probe, NCSA
Feeds Condor Usage into Gratia Accounting System



Condor Quill, University of Wisconsin



Studied Systems



Wireshark (in progress)
Network Protocol Analyzer



Condor Privilege Separation, University of Wisconsin (in progress)
Restricted Identity Switching Module



VOMS Admin, Istituto Nazionale di Fisica Nucleare (in progress)
Virtual Organization Management Service