

# Certificates Abound

Tim Rupp  
Computer Security Team  
December 2006

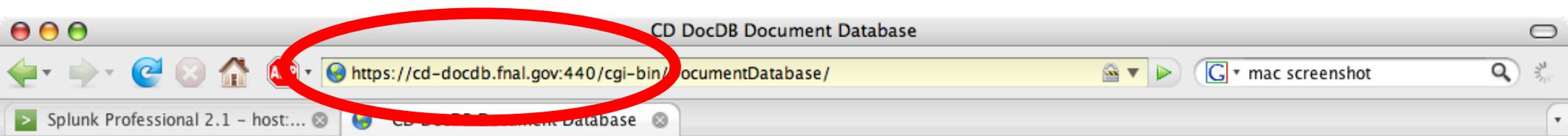
# A day in the life of...

- Surfing carefree
- Oh no! Blocked!
- Wait...which computer was it?
- Ok, why was it blocked?
- Scan the machine. Make sure it's good to go
- Jump on over to another Division to gather some information
- Time for vacation. Check my email before I go

So without a care in the world, I'm minding my own business,  
looking through DocDB for that critical document that I know my  
colleague added



# DocDB



Fermi National Accelerator Laboratory

## Computing Division

<a href="#">CD Home</a>	<a href="#">Search</a>	<a href="#">Documents</a>	<a href="#">Projects</a>	<a href="#">Help Desk</a>	<a href="#">MOUs</a>	<a href="#">At Work</a>
<a href="#">System Status</a>	<a href="#">Metrics</a>	<a href="#">Phonebook</a>	<a href="#">Security</a>	<a href="#">ES&amp;H</a>	<a href="#">Departments</a>	<a href="#">CD Internal</a>

## Document Database

[Create or change documents or other information](#)

Search for  ([Advanced](#) or [Cross Search](#))

Show CD-doc-#  -v

Show documents modified in the last  days

[Calendar](#) of events

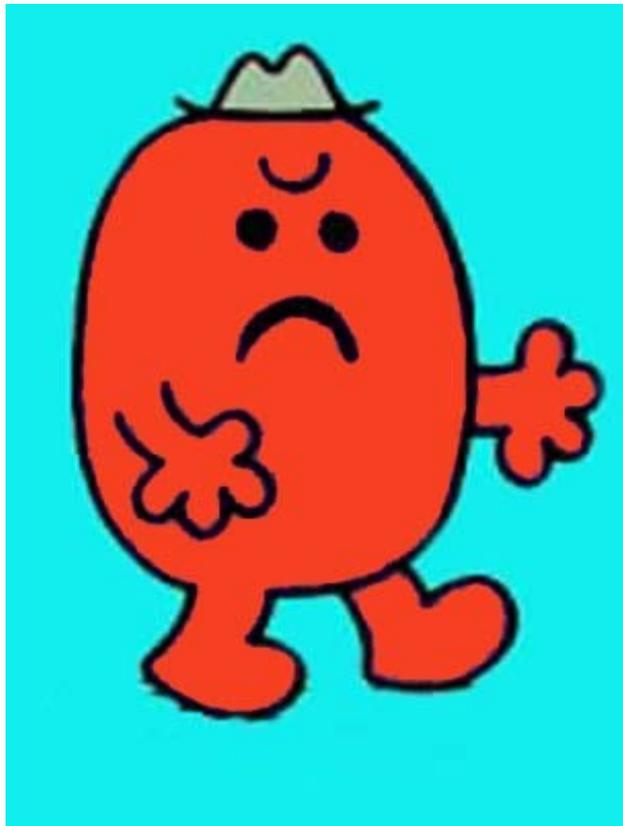
List:

- [Authors](#)
- [All documents](#)
- [Topics](#)
- [Groups](#)
- [Keywords](#)
- [Events](#)

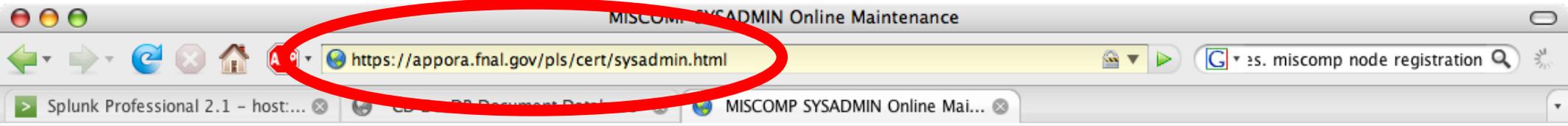
Documents modified in the last 7 days

CD-doc-#	Title	Author(s)	Topic(s)	Last Updated
<a href="#">1938-v2</a>	<a href="#">Lattice QCD Hardware Status</a>	<a href="#">Donald Holmgren</a>	<a href="#">Lattice QCD</a>	28 Nov 2006

When all of a sudden I'm perplexed by an email and a block notice. Curses! Is that machine even mine?



# SysAdmin DB



## MISCOMP SYSADMIN Online Maintenance

[Home](#) [Instructions](#) [Search](#) [Create a New Cluster](#) [Web Reports](#) [Systems With No Managers](#) [Systems With Expired Managers](#)

### Listing for Timothy Rupp

#### Authorized Administrator For Clusters

System Name	System Number	FNAL Property Tag	Class	Purpose	Location	SI #	SN
FERMISCANNERFARM	<a href="#">C01273</a>			Security scanners	FCC/2/218		
KDC CLUSTER	<a href="#">C00422</a>			KERBEROS SERVERS	FCC/2		

#### Authorized Administrator For Systems

Retire (remove from network & maintenance)	System Name	System Number	Node Name(s)	FNAL Property Tag	Class	Purpose	Location	SI #	SN
--		<a href="#">S04478</a>		087636	DELL: PE6400-P3X-700		SITE-38/W2		5FWR201

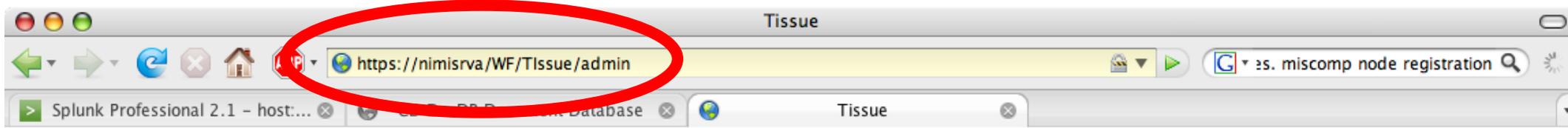
#### Primary System Manager For Systems

Retire (remove from network & maintenance)	System Name	System Number	Node Name(s)	FNAL Property Tag	Class	Purpose	Location	SI #	SN
<input type="checkbox"/>	ARCSIGHT	<a href="#">N53961</a>	arcsight		CPU BOX		FCC/3/360		
<input type="checkbox"/>	BANANA	<a href="#">S25811</a>		101501	HP: HX2490B		FCC/3/360		2CK6320NWC
<input type="checkbox"/>	CATBOT	<a href="#">S17380</a>		101124	DELL: DIM-9150-2200		FCC/3/360		8LSK9B1
<input type="checkbox"/>	FAZ	<a href="#">N37585</a>		088855	DELL: GX400-1700-MT	JOE KLEMENCIC LINUX DT	FCC/3/360		DXR6S01

Unbelievable, it is. Well, I'd hate to have my torrents stop downloading, so I better go remediate the issue



# Tissue



## Issue Tracking Database (Tissue)

Production v1.2 instance

- [Home](#)
- [Action codes](#)
- [Source classes](#)
- [Source codes](#)
- [Severity codes](#)
- [Machines](#)
- [Issue codes](#)
- [Events](#)
- [User Front](#)
- [Blocker Workflow](#)

### Events Summary

By status **Blocked: 460** **Open: 411** **Closed: 3763**  
By severity Warning (W): 531 Critical (C): 4452 Informational (I): 173

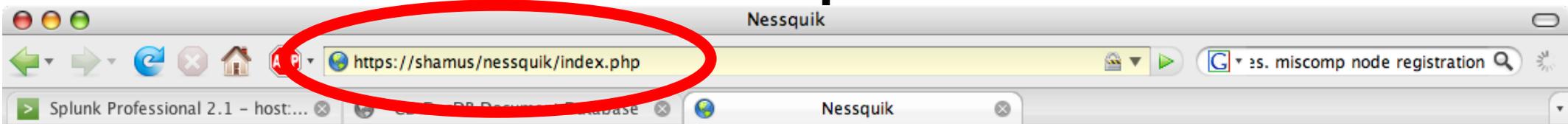
### Most recent events

ID	Issue	Severity	Event Status	Block Status	IP	Machine ID	Found	Updated	Blocked
7900	<a href="#">Open X Server</a>	C	Blocked	B	131.225.43.130	<a href="#">tdport52-vm</a>	11/30/06 10:55:27	12/01/06 11:02:01	12/01/06
7901	<a href="#">MS04-022</a>	C	Closed	UP	131.225.163.166	<a href="#">zhustian</a>	11/30/06 13:50:13	12/01/06 14:01:44	
7902	<a href="#">SSHD PasswordAuthentication</a>	C	Closed	UP	131.225.163.102	<a href="#">dudes-mac</a>	11/30/06 14:11:16	12/01/06 14:01:53	
7903	<a href="#">SSH-unKerb</a>	W	Closed	UP	131.225.163.102	<a href="#">dudes-mac</a>	11/30/06 14:11:38	12/01/06 14:02:02	
7904	<a href="#">Open X Server</a>	C	Blocked	BP	131.225.133.109	<a href="#">adrfltpj</a>	11/30/06 15:40:23	12/01/06 15:42:03	12/01/06
7909	<a href="#">Swap</a>	W	Open	U	131.225.217.220	<a href="#">REXPERIMENT</a>	11/30/06 19:58:28	11/30/06 19:58:29	
7910	<a href="#">Tel-unKerb</a>	W	Open	U	131.225.19.133	<a href="#">NPIE7CBC6</a>	11/30/06 23:33:05	12/04/06 04:59:42	
7911	<a href="#">Tel-unKerb</a>	W	Open	U	131.225.63.198	<a href="#">NPIE6DFD9</a>	12/01/06 00:54:26	12/04/06 06:16:59	
7912	<a href="#">Tel-unKerb</a>	W	Open	U	131.225.52.233	<a href="#">RANDOLPH</a>	12/01/06 02:03:22	12/01/06 02:08:10	
7914	<a href="#">MS06-040 (net chk)</a>	C	Closed	UP	131.225.94.102	<a href="#">nroch01</a>	12/01/06 09:30:05	12/01/06 14:02:13	
7915	<a href="#">SSHD PasswordAuthentication</a>	C	Closed	UP	131.225.88.147	<a href="#">miso</a>	12/01/06 10:51:14	12/01/06 14:02:25	
7916	<a href="#">Unregistered</a>	I	Open	U	131.225.16.90	<a href="#">BAGGINS</a>	12/01/06 13:00:47	12/01/06 13:00:49	
7917	<a href="#">Open X Server</a>	C	Blocked	BP	131.225.44.164	<a href="#">MTFPC31</a>	12/01/06 16:55:22	12/04/06 09:46:32	12/02/06
7918	<a href="#">Open X Server</a>	C	Closed	UP	131.225.162.223	<a href="#">NB-OCHANDO</a>	12/01/06 20:40:26	12/04/06 06:45:36	
7920	<a href="#">Unregistered</a>	I	Open	U	131.225.81.48	<a href="#">CDPLYCM4</a>	12/01/06 21:14:47	12/01/06 21:14:50	
7921	<a href="#">Unregistered</a>	I	Open	U	131.225.84.76	<a href="#">PATLX2</a>	12/01/06 21:16:24	12/01/06 21:16:33	
7922	<a href="#">Swap</a>	W	Open	U	131.225.139.2	<a href="#">TEL2VACINTLK</a>	12/02/06 12:48:31	12/02/06 12:48:34	
7923	<a href="#">Open X Server</a>	C	Blocked	BP	131.225.163.252	<a href="#">NB-OCHANDO</a>	12/02/06 17:40:42	12/03/06 22:57:18	12/03/06
7924	<a href="#">Unregistered</a>	I	Open	U	131.225.192.20	<a href="#">RPS-FE-V7</a>	12/02/06 19:08:16	12/02/06 19:08:17	
7925	<a href="#">Open X Server</a>	C	Closed	UP	131.225.243.140	<a href="#">McGill-CDF2</a>	12/02/06 21:50:22	12/03/06 23:08:49	
7926	<a href="#">MS06-040 (net chk)</a>	C	Blocked	BP	131.225.163.95	<a href="#">D-D0-WIRELESS-COMMENT</a>	12/03/06 12:40:16	12/03/06 12:41:31	12/03/06
7927	<a href="#">MS06-040 (net chk)</a>	C	Blocked	BP	131.225.163.199	<a href="#">NB-JAFFRE</a>	12/03/06 13:10:13	12/03/06 13:11:53	12/03/06
7928	<a href="#">Swap</a>	W	Open	U	131.225.225.230	<a href="#">FANNY-CLUEDO</a>	12/03/06 13:54:40	12/03/06 13:54:48	
7929	<a href="#">SSHD PasswordAuthentication</a>	C	Blocked	BP	131.225.88.241	<a href="#">D-FCC-COMMENT</a>	12/04/06 09:21:49	12/04/06 09:23:13	12/04/06
7930	<a href="#">Tel-unKerb</a>	W	Open	U	131.225.43.163	<a href="#">d-r15866</a>	12/04/06 09:43:32	12/04/06 09:47:43	

And just to be on the safe side, I'll run a Nessus scan against the offending machine to make sure that its vulnerability is fixed



# nessquik



Hello **Tim**, what would you like to scan?

[Home](#) | [Settings](#) | [Scans](#) | [Help](#)

[My registered computers](#)

[My whitelist entries](#)

[My saved scans](#)

[A list of computers](#)

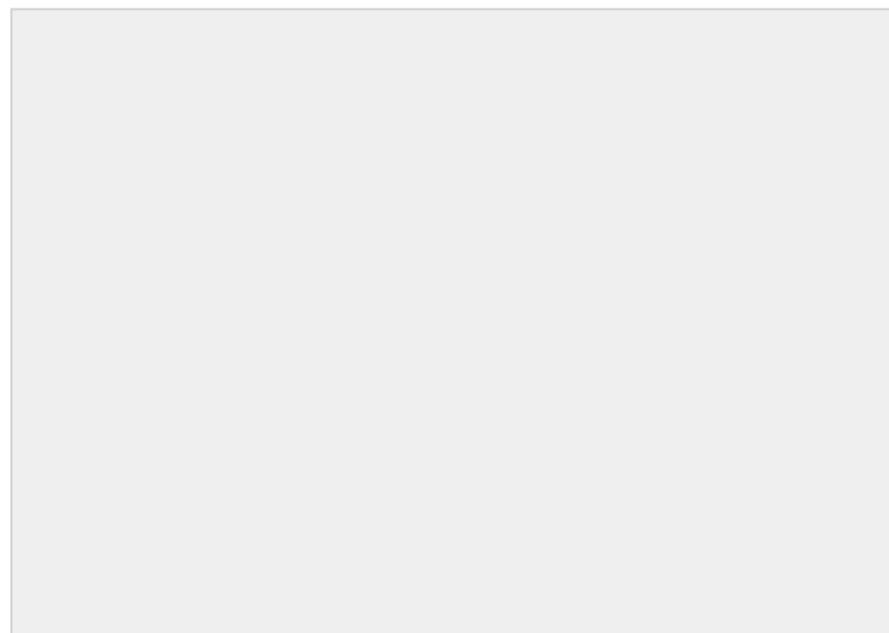
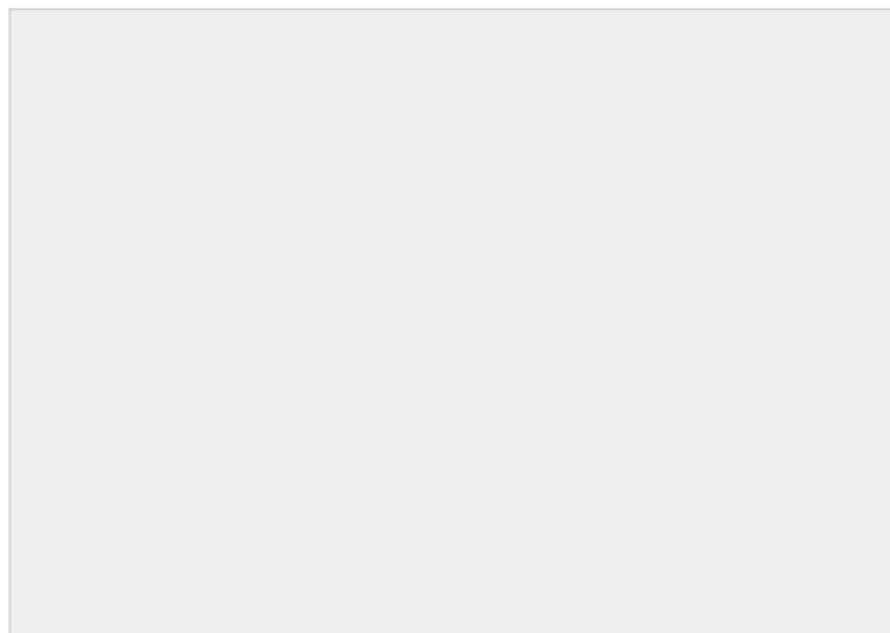
[A cluster of computers](#)

## Choose Plugins To Scan With

[By Family](#)

[By Severity](#)

[All Plugins](#)



Done. But being frustrated with the Window's policy of patching my machine, I decide I'd like to give the people who make these decisions a good thrashing, I don't know who to though contact. I know, I'll check out WinPol on Plone.



# Select CD Plone Sites

Welcome to the Windows Policy Site — Fermilab Windows Policy Site

https://plone4.fnal.gov/P1/WinPol

**Fermilab**

home news members

you are not logged in log in

you are here: home

## Welcome to the Windows Policy Site

The Windows Policy Committee oversees the site windows domain.

*Access to this page is controlled by KX.509 certificates (some one you use for nessus scans). If you have such a certificate and you are a windows OU manager or admin then use it to log in to this site and unlock the magic within!*

The Windows Policy Committee is responsible for setting policies for the top-level Fermilab Windows domain (win) and the child domain (fermi) containing users. The committee is responsible for approving win.fnal.gov and fermi.win.fnal.gov policy changes and for controlling creation of special domain accounts. Our charter is available [here](#).

Members of the Windows Policy Committee are appointed every two years by recommendation of their Division/Section/Experiment. In addition to voting members each OU may have additional technical managers (OU Managers). OU Managers provide technical feedback to the voting members. In most cases a voting member is also an OU manager.

**Voting Members:**

-----

**Committee Chair:** Jack Schmidt, [schmidt@fnal.gov](mailto:schmidt@fnal.gov)

**Accelerator Division:** Sam Jarocki, [jarocki@fnal.gov](mailto:jarocki@fnal.gov)

**Business Services Section:** Tom Ackenhusen, [tackenhu@fnal.gov](mailto:tackenhu@fnal.gov) Mike Rosier, [mrosier@fnal.gov](mailto:mrosier@fnal.gov)

**DO:** Greg Cisco, [cisco@fnal.gov](mailto:cisco@fnal.gov)

**CD, CDF, DIR, ESH, FESS, LSS, NUMI, SDSS:** Ken Fidler, [fidler@fnal.gov](mailto:fidler@fnal.gov) Al Lilianstrom, [lilstrom@fnal.gov](mailto:lilstrom@fnal.gov)

**Particle Physics Department:** Allen Forni, [forni@fnal.gov](mailto:forni@fnal.gov) Karen Carew, [carew@fnal.gov](mailto:carew@fnal.gov) Quinten Healy, [quint@fnal.gov](mailto:quint@fnal.gov)

navigation

- Home
- Security Exception Forms
- Windows Domain Policies
- Documentation
- DA Pager Schedule
- Meeting Minutes

log in

Name

log in

authentication note

You have an SSL Certificate, but it is not mapped to any local users. You should go to the [join form](#) to create an account that can use your SSL Certificate to log in.

December 2004

Su	Mo	Tu	We	Th	Fr	Sa
		3	4	5	6	7
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

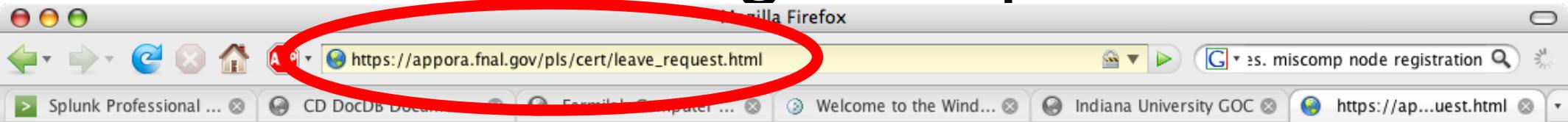
Done

plone4.fnal.gov

After all I've done today, I need to take some time off. Yellowstone probably looks pretty good this time of year. Vacation here I come!



# Leave Usage Requests



**Timothy Rupp**

- [New Request](#)
- [Personal Calendar](#)
- [Personal Request History](#)

**User Guide**

**View Calendars**

- [CD/CCF/CST](#)
- [CD/CCF](#)
- [CD](#)

**Travel Related Links**

- [Computing Division Travel Page](#)
- [Fermilab Holidays](#)

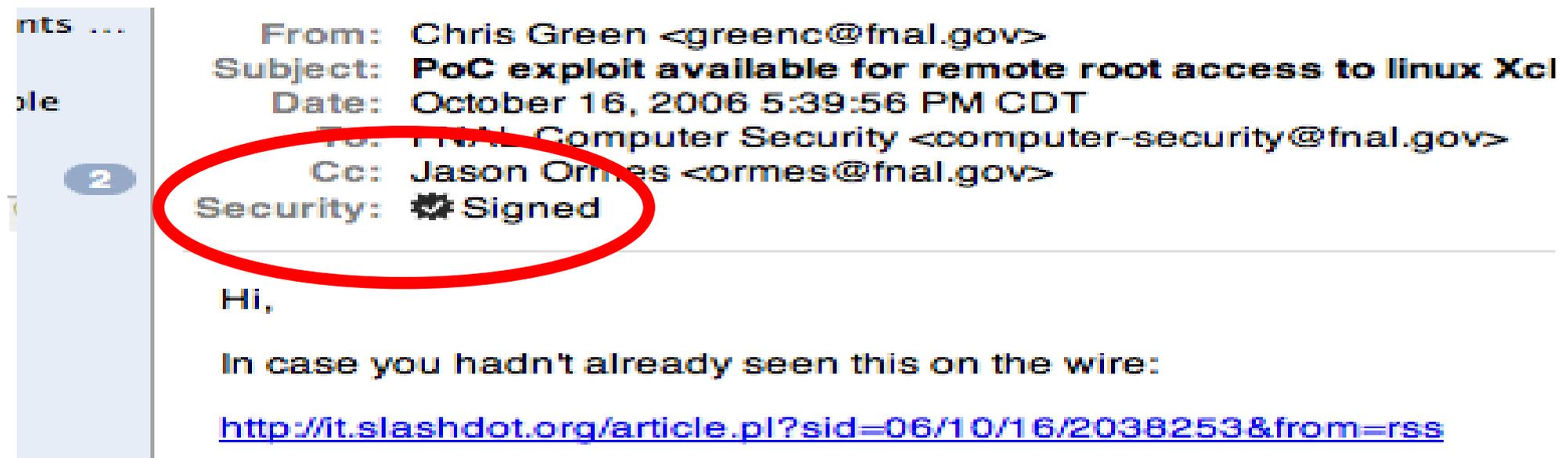
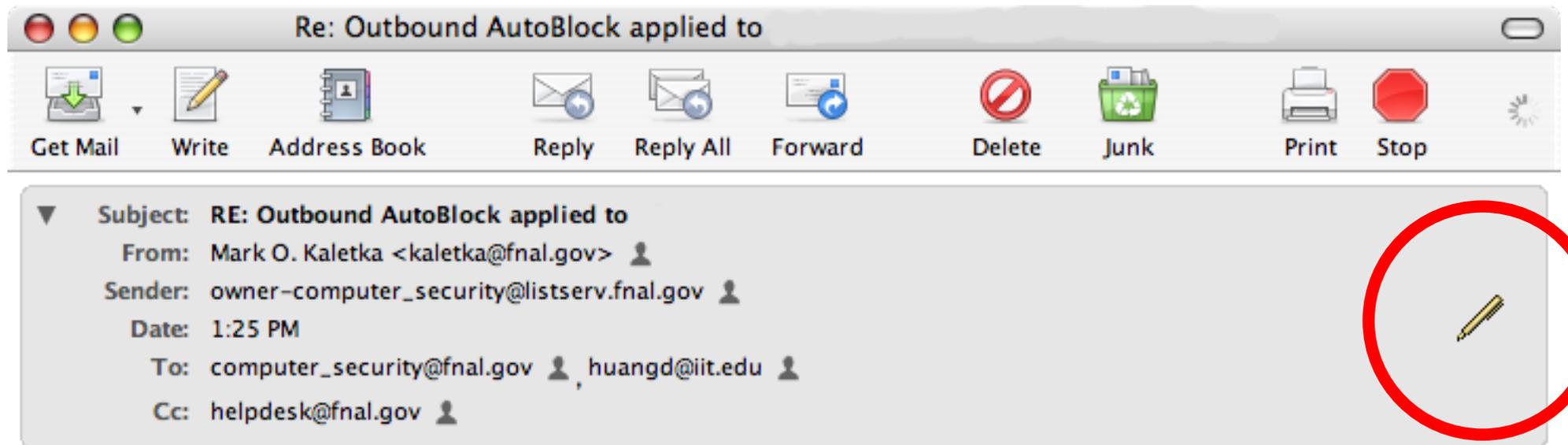
**Leave Usage Request System**

**No personal upcoming request item found**

Before I take off though, I'll check my mail. Wouldn't want to miss anything important.



# Signing Email



# So what about certificates?

- They were used in every example
- KCA and DOEGrids both have their uses
- No extra passwords were needed in any example, all it took was a quick run of get-cert and I was set
- I guarantee more areas of the lab use certs than what I touched on
- get-cert needed once per week

# roadblocks

- functionality of security tool is dependent on OSX release
- get-cert works best with Tiger 10.4.8
- Disconnect between Keychain and Firefox
- If you're mixing DOE and KCA certs, please pay attention to Keychain because Mail doesn't ask which cert to use for signing
- If you use get-cert with an existing kerberos cache, you may not get a week long certificate

# requirements

- Access should match the level of protection required by the data
- No authorization necessary for some read only applications
- Cert required for protected reads and all writes when used by collaborators
- No anonymous writes allowed
- No “self- adding” of accounts for write access

# authorization options

- Group account
- Individual accounts over SSL
- DOE Grid Certs
- KCA Certs

# least desirable

- Group account
  - Weak identity verification
  - Read only, can't publish information
    - Data that would otherwise be public to prevent spidering and indexing
  - Because all required termination of accounts must be managed by CNAS
    - Users who lose their affiliation must be assumed to continue reading
  - Password will be vulnerable: sniffing, from application server or phishing
  - It can be shared by people

# 2<sup>nd</sup> least desirable

- Individual accounts over SSL
  - Weak identity verification
  - Read or publish information
  - Because all required termination of accounts must be managed by CNAS
    - Users who lose their affiliation must be assumed to continue reading or publishing data
  - Password will be vulnerable: from application server, phishing
  - Sensitivity of information requires greater protection than group password

# recommended

- DOE Grid Certs
  - Strong identity verification
  - Read or publish information
  - User privileges can be revoked
  - No password vulnerability
  - Can support non FNAL usage
    - Organization based authorization
  - Long lifetime
  - Ideal for signing email because of long lifetime

# also recommended

- KCA certs
  - Strong identity verification
  - Read or publish information
  - User privileges can be revoked
  - No password vulnerability
  - Restricts usage to FNAL only
  - Requires frequent renewal
  - Short lifetime is bad for signing email. Don't use KCA certs to sign your email

# final words

- Use KCA for authenticated web access if no outside contributors will need access
- Use DOEGrid cert otherwise
- Use DOEGrid cert to sign email
- Support the get-cert development.
- We have an external developer working on a seamless Windows integration, so if there are people in the Mac community who wish to take the lead on seamless integration with Mac, we can hook you up with the developer