Security Models

From Corporate to ISP
On size does not fit all

Security Camp @ MIT

August 15, 2006

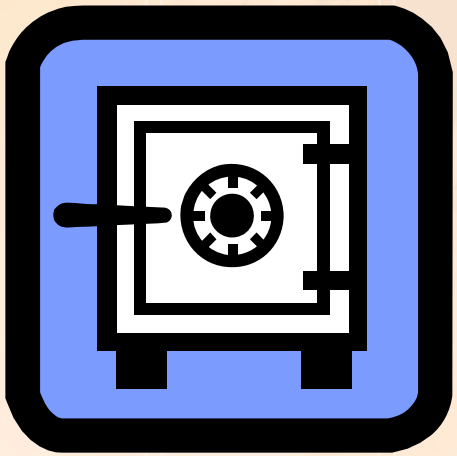
Joel Rosenblatt, Senior Security officer
Columbia University, CUIT

Security is a concept, not a device

- *It depends on*
  - *What needs to be secured*
  - *What risks are involved*
  - *What resources are available*

A Short history of security

- *Banks before ATM's*
  - *Big vault*
  - *Thick concrete walls*
  - *Huge door with lock*
  - *Guards with guns*



Mainframe Security

- *Glass House – The Data Bank*
  - *Monitored 24/7*
  - *Access limited to controlled terminals*
  - *Access was secured by people*

The ATM – Distributed Banking

- *A new security model was needed*
  - *Money not in locked rooms. No more vault*
  - *Protection needed to move closer to money*

The Banking model

- *Original assumptions*
  - *Monolithic computing model*
    - *Mainframe*
    - *Tight access controls – physical & logical*
    - *Trusted computing environment*
    - *Biggest or only threat was insiders*

Banking model – the new reality

- *Distributed access – How business gets done*
  - *Crunchy shell model doesn't work*
  - *Consumers and staff want access from everywhere*
  - *The Web provides a conduit for the bad guys to access the inside of a network*
  - *Any open port can provide a vector for attack*
- *Security in layers is needed to protect assets*

The ISP model – security concerns

- *An ISP is a collection of thousands of machines linked together by a common network with no one in control*
  - *Any machine can be owned by a bad guy*
  - *An ISP can be attacked internally (bandwidth abuse) or externally (DDOS attack) – sometimes they are the same*
- *Is not suited for*

  Corporate offices

The ISP model – security inside out

- *View all of the customers as "The Enemy"*
  - *Any machine can attack any other machine*
  - *The probability is that compromised machines in the address space of the ISP will be used to attack machines inside and outside of that space*
  - *Abusive behaviors to guard against*
    - *Bandwidth abuse*
    - *DDOS attacks*
    - *Scanning machines*

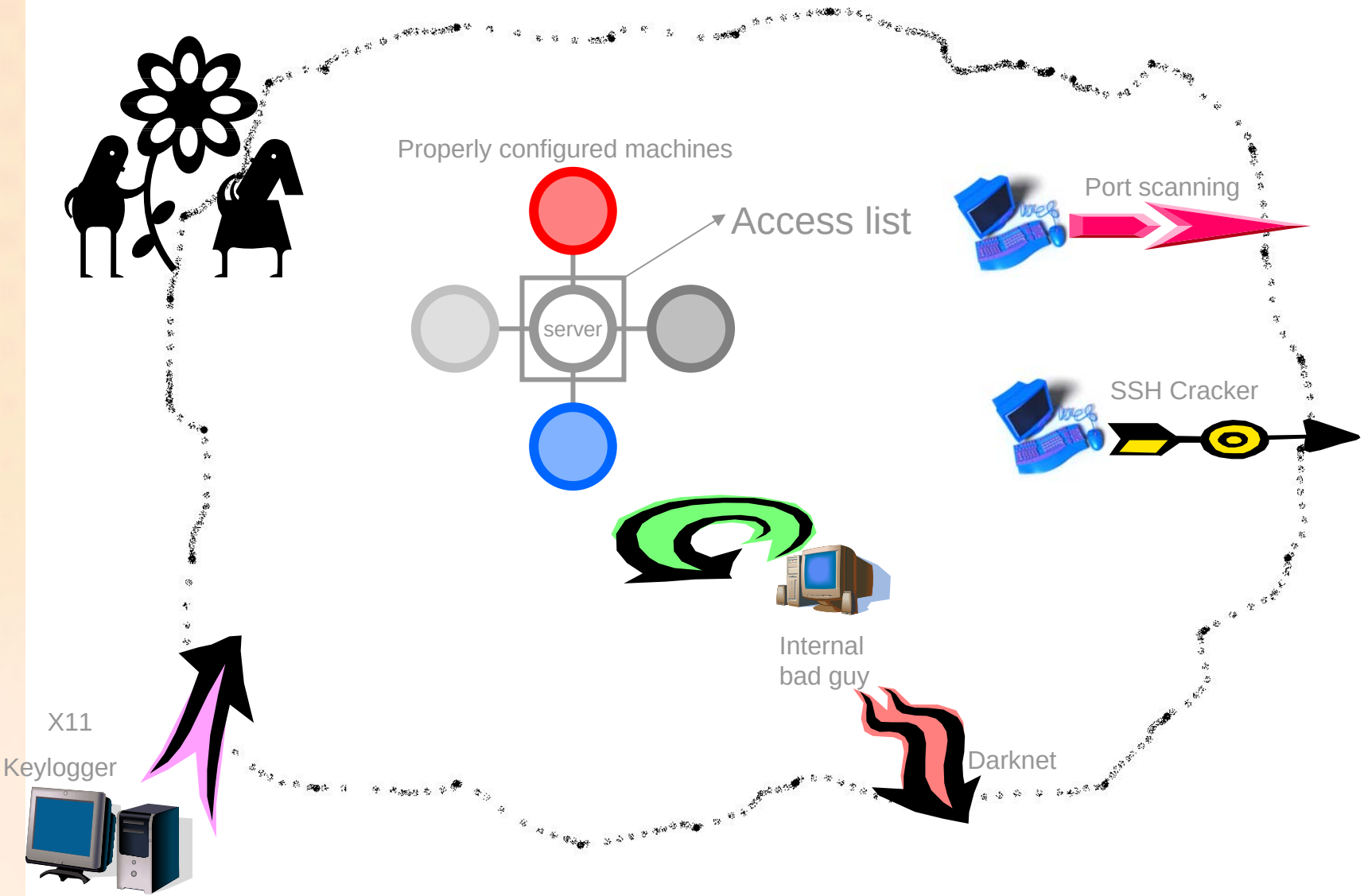
The ISP model - Assumptions

- *Policy – attack behavior is unacceptable*
- *Policy – each user is responsible for the behavior of their system*
- *There is a way to look at traffic entering and leaving the network*
- *There is an effective way to remove a machine from network*
- *A way is needed to educate machine owners so that they don't make the same mistake again*

The Columbia Model - environment

- *Large research University*
- *Decentralized management structure*
- *Over 60,000 network nodes*
- *Over 35,000 MAC address active on average*
- *Decentralized computer support*
- *No sniffing traffic or scanning machines allowed*
- *“Free Love” IP address assignments*
- *No University wide, corporate like, firewalls*

Columbia University Network



The Columbia Model - assumptions

- *There is no such thing as perfect security*
- *There are more bad guys outside the University than inside*
- *Telling people what they can't do at Columbia is hard*
- *We have a big network pipe and lots of fast hardware*
- *We own the campus network*
- *Security in layers works*

The Columbia Model - Philosophy

- *A security system that can protect the rest of the world from Columbia University will also protect Columbia from the rest of the world*
- *We may have some control over the attackers; the machines on our campus*

The Columbia Model - Caveats

- *One size does not fit all – even at Columbia*
  - *There are Banking model LANs around campus to support servers than need isolation security*
  - *Some departments use firewalls to try and slow down attacks*
- *These are the exceptions, not the rule*

The Columbia Model - Tools

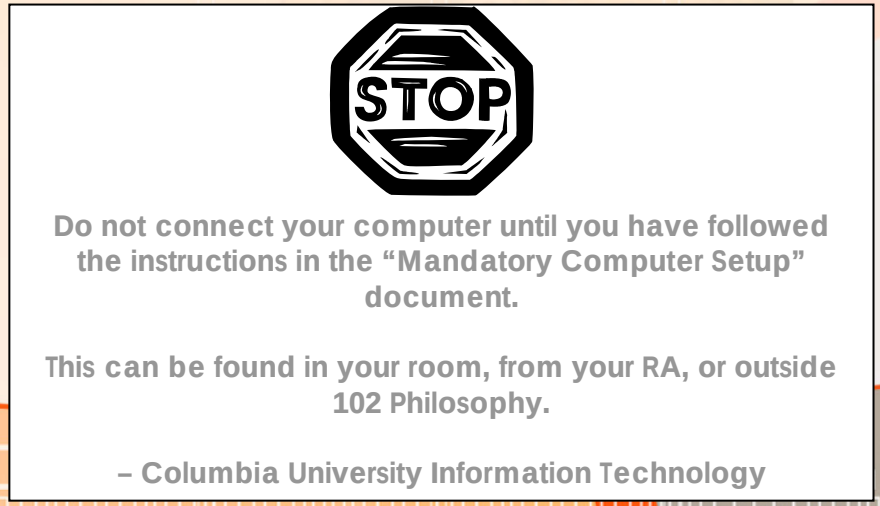
- *Policies & Practices*
- *User education*
- *Site license software*
- *Network management software*
- *Security software*

Policies & Practices

- *Each user is responsible for the security of their own computer*
  - *They get to rebuild their own system if it gets compromised*
  - *People learn from pain – after the ordeal of a full rebuild, most people learn about computer safety*

User education

- *Security web site*
  - *Cookbook on how to secure your computer and best security practices*
- *Back to school program*
  - *Packet of information sent home*
  - *Mandatory session for every new student*
  - *Pillow top information packet – Network jack covers*



Site license software

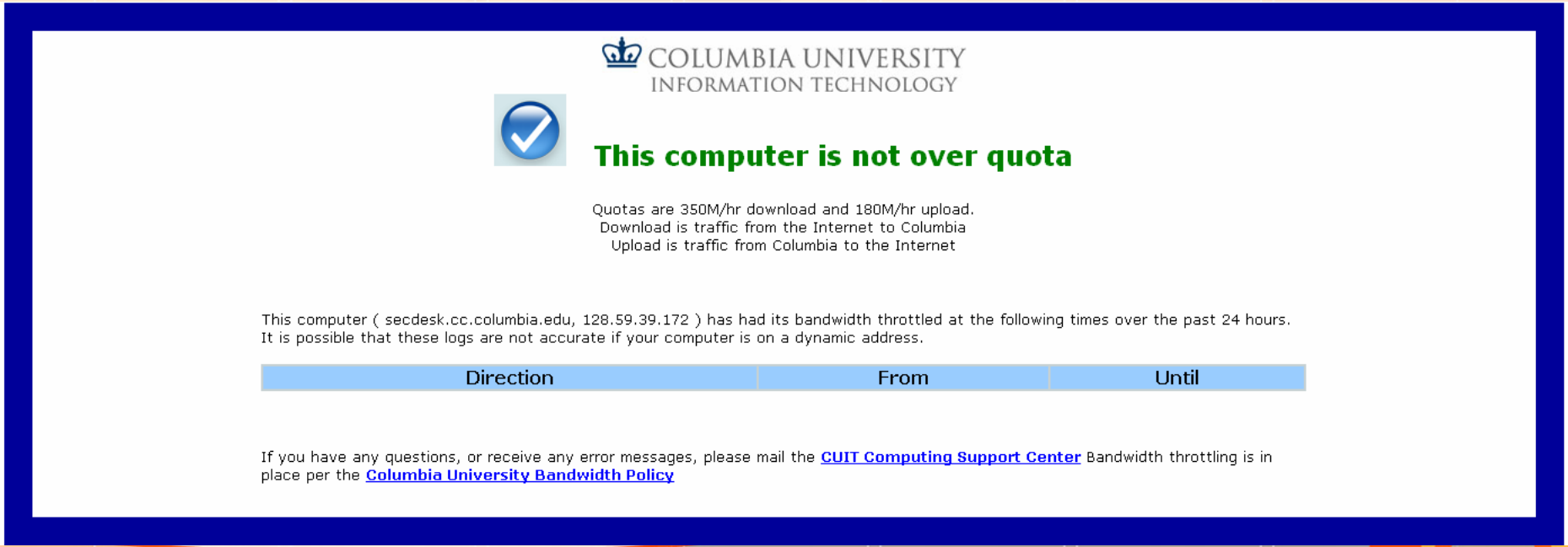
- *Free Anti-virus software*
- *Free Anti-spyware software*
- *Free PCPhoneHome software*
- *Secure SSH software - PuTTY*
- *Secure FTP software - WinSCP3*

Network Management

- *Bandwidth Quota*
  - *Each host computer on the Columbia network is assigned two quotas. One quota affects outbound usage, i.e., data sent to the Internet. The second affects inbound usage, i.e., data downloaded from the Internet. A host exceeding either limit in a given hour will have its bandwidth in that direction restricted to a lower rate for the remainder of the hour and the hour following if excessive bandwidth use continues*
  - *The quotas change from time to time in order to allow the highest traffic levels compatible with the overall performance of the network*
  - *The quota is protocol agnostic and not affected by encryption*
  - *Exceptions are granted for servers*

Bandwidth Quota

- *Users can check on their own computer to see its current status and history*
- *Since quota is based on number of bytes, it also works to limit DOS attacks*



Capture

- *Capture allows us to remove a machine from our network without turning off a network jack*
- *It works on wired or wireless connections*
- *It allows us to communicate the reason that the machine was taken off the network*
- *It allows the user to self repair and remove capture without help desk involvement*
- *It is integrated with our REMEDY ticket system*

Capture – Compromised system

COLUMBIA UNIVERSITY
INFORMATION TECHNOLOGY

Network Access Suspended

You must follow all these instructions

Internet connectivity to this machine has been disabled because of network traffic indicating that it has been compromised by an Internet worm/trojan.

Internet access **cannot** be restored until this activity stops. This will require that the hard drive be reformatted and the operating system reinstalled. You will need to back up any data on this machine and reinstall the operating system or run a system restore/recovery CD provided by the manufacturer, after which you will need to reinstall all the programs.

However, if you have been using an application that scans for open network shares, then there is a chance that your machine has not been compromised. If this is the case, remove the scanning application and click Restore Network Access below. Scanning for vulnerabilities or open shares is a violation of University policy.

Reformatting your machine removes all data from your computer. This is an irreversible process. If you do not back up a file, it will be lost forever.

We understand the inconvenience experienced by you in this case, but ask for your understanding. When a machine has been compromised in this manner, there is no way to know it is secure without returning it to a brand-new state.

In order to ensure that your machine does not become infected again after you reinstall the operating system, please review our basic information about rebuilding Windows computers.

Once you have reformatted the machine, you will need to do a series of updates in order to prevent it from becoming infected again. You can find the updates on this page. If you have a writable CD/DVD drive, you will need to download the files and burn them to a CD/DVD **before** you do the reformat.

Because the process is different for every computer manufacturer, CUIT is unable to provide assistance to users who need to reformat and reinstall an operating system. Any questions you have about this process should be directed to the manufacturer of your computer system.

CUIT has arranged a 10% discount with Techs in a Sec, a company that can assist in backing up, reformatting, and securing machines. Click here for more information about Techs in a Sec.

When you have followed all the above steps, you may restore network access for this computer.

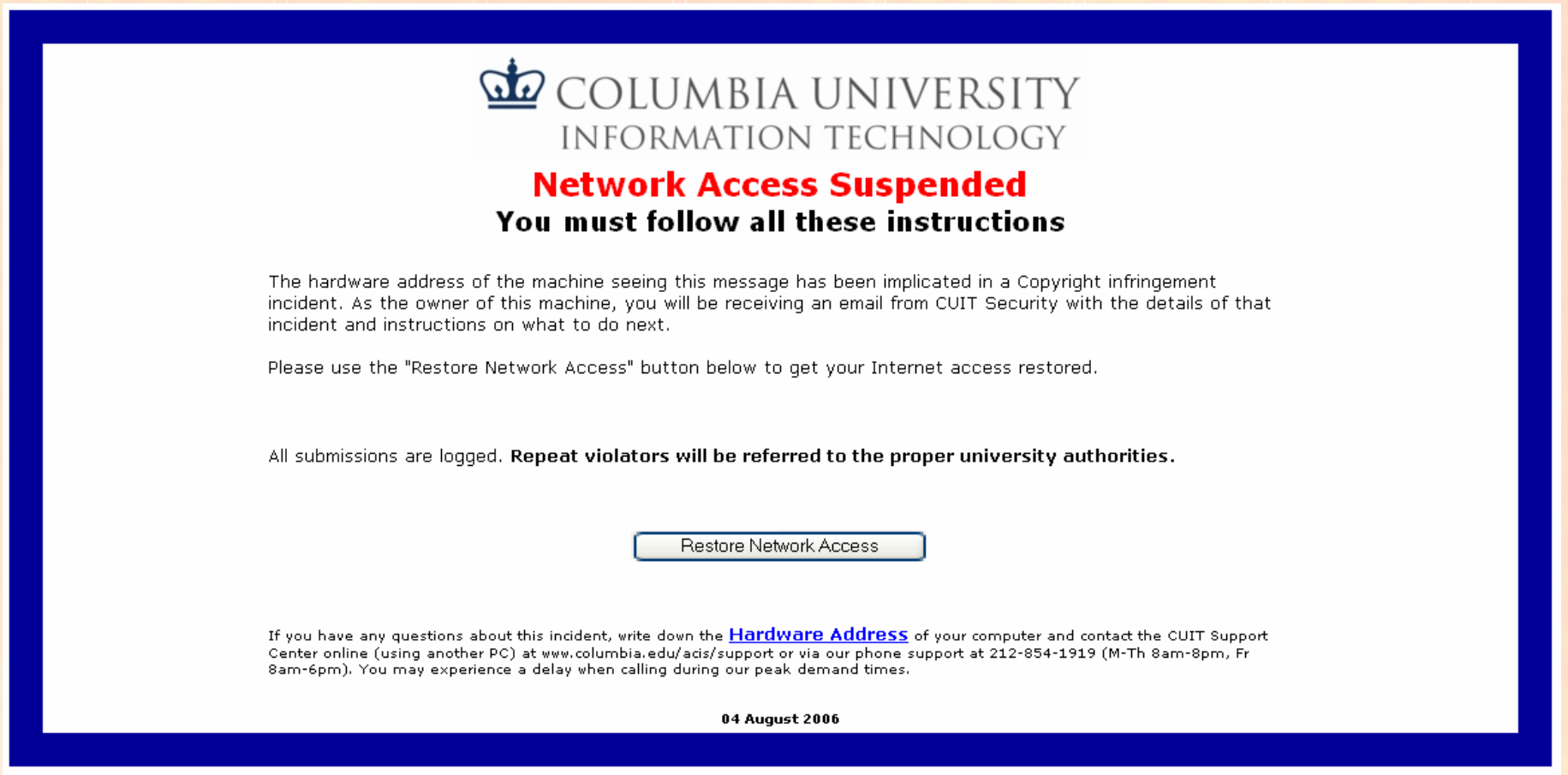
Note that by clicking below, you are affirming you have followed the above instructions. All submissions are logged. **Repeat violators will be referred to the proper university authorities.**

Restore Network Access

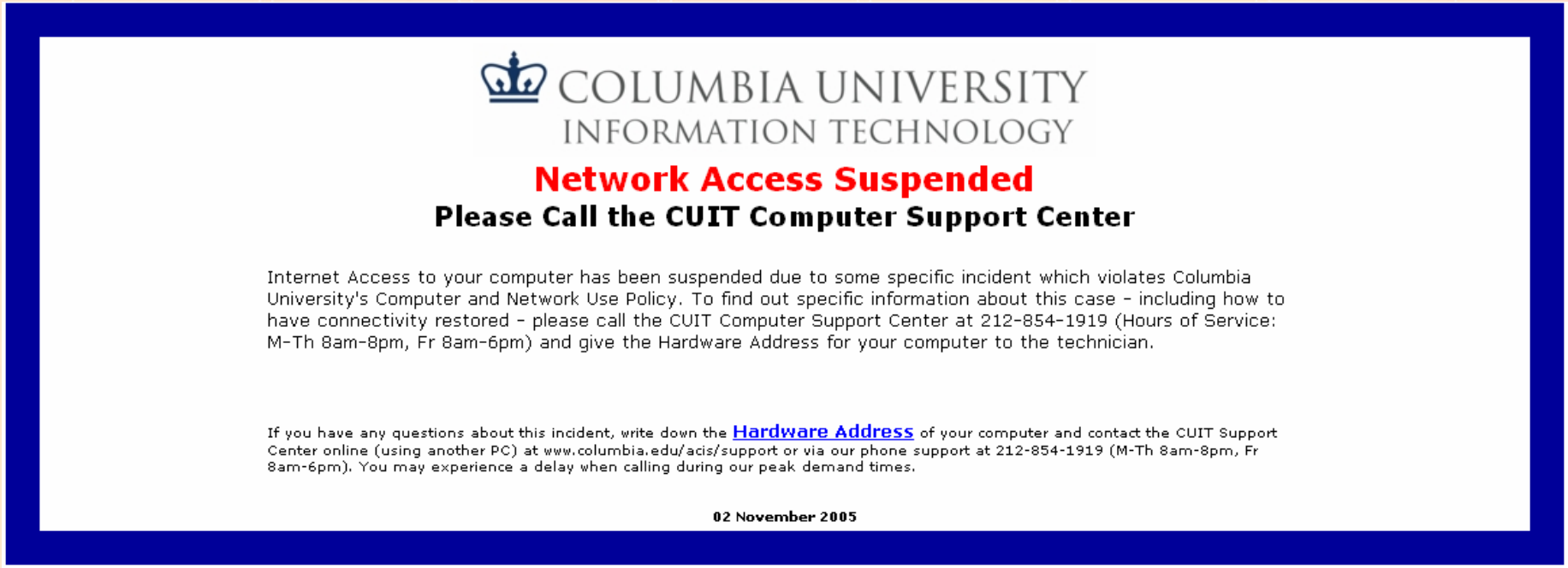
If you have any questions about this incident, write down the **Hardware Address** of your computer and contact the CUIT Support Center online (using another PC) at www.columbia.edu/acis/support or via our phone support at 212-854-1919 (M-Th 8am-8pm, Fr 8am-6pm). You may experience a delay when calling during our peak demand times.

23 September 2005

Capture – Copyright Infringment



Capture – Please call



COLUMBIA UNIVERSITY
INFORMATION TECHNOLOGY

Network Access Suspended

Please Call the CUIT Computer Support Center

Internet Access to your computer has been suspended due to some specific incident which violates Columbia University's Computer and Network Use Policy. To find out specific information about this case - including how to have connectivity restored - please call the CUIT Computer Support Center at 212-854-1919 (Hours of Service: M-Th 8am-8pm, Fr 8am-6pm) and give the Hardware Address for your computer to the technician.

If you have any questions about this incident, write down the Hardware Address of your computer and contact the CUIT Support Center online (using another PC) at www.columbia.edu/acis/support or via our phone support at 212-854-1919 (M-Th 8am-8pm, Fr 8am-6pm). You may experience a delay when calling during our peak demand times.

02 November 2005

GULP – Grand Unified Log Program

- *Problem – How do you know who is using an IP address without registration?*
  - *GULP processes the logs from 12 different services that require authentication*
  - *It processes information from the ARP cache to associate MAC address with IP address*
  - *GULP correlates all information*
  - *A user can be tracked by IP, MAC, or UNI – even if the IP is not on the Columbia network*
  - *The data is kept for 29 days and then purged*

GULP – screen shot

CUIT Security Management - Logged in as joel

Tools

Logout
Refresh
Security
Helpdesk

Wiki
SwitchMgr
CapturePage
IncDB

GULP
SULog
PollerPounce
PortHistory
Projects

IncDump
IncPage
MassCapture
CaptureAudit

PAIRSpanel
ContactDB

Search User Records

UNI	joel
IP	
MAC	
Service	
Server	
Start	
End	

Color code:
○ UNI ◉ IP ○ MAC

Search

- Fill out as many fields as you want.
- You can specify more than one value for UNI, IP or MAC, just keep a space between them.
- If you want to find records where a value is *not* present, start that value with a ! (ie, UNI: !wren !joel).
- For IP, you can use a % wildcard, but searches will take much longer unless you include most of the IP (128.59.31.% works fine, but 128.59.% does not).
- Valid services: Cunix, Pinex, POP, IMAP, Cyrus-POP, Cyrus-IMAP, SMTP, WWWS, WIND, CubMail, NNTP, SLAUTH
- Dates and times can be entered in most logical formats used in the US.

Joel L. Rosenblatt
Systems Programmer Lead
Information Technology
joel@columbia.edu

UNI	Service	Server	Login	Logout	IP Address	Hostname	MAC Address
joel	Cyrus-IMAP	mockduck	06-aug-2006 21:49:20		69.116.5.168	pool-457405a8.dyn.optonline.net	
joel	Cyrus-IMAP	tempeh	06-aug-2006 21:37:21		69.116.5.168	pool-457405a8.dyn.optonline.net	
joel	Cyrus-IMAP	veat	06-aug-2006 21:12:19		69.116.5.168	pool-457405a8.dyn.optonline.net	
joel	Cyrus-IMAP	unchicken	06-aug-2006 20:57:41		69.116.5.168	pool-457405a8.dyn.optonline.net	
joel	Cyrus-IMAP	veat	06-aug-2006 20:46:59		69.116.5.168	pool-457405a8.dyn.optonline.net	
joel	Cyrus-IMAP	veat	06-aug-2006 20:46:39		69.116.5.168	pool-457405a8.dyn.optonline.net	
joel	Cyrus-IMAP	seitan	06-aug-2006 20:31:56		69.116.5.168	pool-457405a8.dyn.optonline.net	
joel	Cyrus-IMAP	veat	06-aug-2006 19:55:32		69.116.5.168	pool-457405a8.dyn.optonline.net	
joel	Cyrus-IMAP	veat	06-aug-2006 19:40:16		69.116.5.168	pool-457405a8.dyn.optonline.net	
joel	Cyrus-IMAP	tempeh	06-aug-2006 19:30:44		69.116.5.168	pool-457405a8.dyn.optonline.net	
joel	Cyrus-IMAP	tofu	06-aug-2006 19:30:12		69.116.5.168	pool-457405a8.dyn.optonline.net	
joel	Cyrus-IMAP	veat	06-aug-2006 19:04:52		69.116.5.168	pool-457405a8.dyn.optonline.net	
joel	Cyrus-IMAP	unmeatball	06-aug-2006 18:40:02		69.116.5.168	pool-457405a8.dyn.optonline.net	
joel	Cyrus-IMAP	soysage	04-aug-2006 20:25:27		69.116.5.168	pool-457405a8.dyn.optonline.net	
joel	Cyrus-IMAP	tempeh	04-aug-2006 20:00:04		69.116.5.168	pool-457405a8.dyn.optonline.net	
joel	SMTP	brinza	04-aug-2006 15:49:13		128.59.39.172	secdesk.cc.columbia.edu	00123F466CDC
joel	SMTP	jalapeno	04-aug-2006 15:45:57		128.59.39.172	secdesk.cc.columbia.edu	00123F466CDC
joel	SMTP	brinza	04-aug-2006 15:41:02		128.59.39.172	secdesk.cc.columbia.edu	00123F466CDC
joel	SMTP	brinza	04-aug-2006 14:48:13		128.59.39.172	secdesk.cc.columbia.edu	00123F466CDC
joel	Cyrus-IMAP	mockduck	04-aug-2006 12:51:45		128.59.39.172	secdesk.cc.columbia.edu	00123F466CDC
joel	SMTP	serrano	04-aug-2006 12:44:04		128.59.39.172	secdesk.cc.columbia.edu	00123F466CDC

PAIRS – Point-of-contact And Incident Response System

- *Consists of three main modules*
  - *KnowScans – analyzes netflow data*
  - *Incident Analyzer – correlates incident data*
  - *ContactDB – informs systems administrators*
- *Incidents (Port scans, C&C communications, Darknet scans) are placed in Oracle DB by KnownScans*
- *Correlated incidents are assigned a score and machines are either Captured or Contacted*

PAIRS – additional functions

- *Additional processing done through PAIRS*
  - *SSH error logs*
  - *SNMP logs*
  - *Switch/Router logins*
  - *Scans from the outside world*
- *Inside attacks are processed through the ContactDB*
- *Outside attacks generate a “Please Stop” message to the ISP*

PAIRS - research

- *Use the Columbia network as a sensor to look for new attacks by developing a statistical model of ports being scanned*
- *Use external scans of our network to act as a passive network scanner. Find freshly compromised systems by looking for positive responses*

Summary

We view Columbia University as a blend of Corporate and ISP elements that as such, requires a security structure that covers these requirements. We believe that the security environment should not, as much as possible, interfere with the basic structure of the University's mission – to provide an open environment to allow the exchange of ideas. We strongly believe that the open network allows this exchange with a minimum of red tape and by using programs, such as GULP, PAIRS, and Capture; we can offer a secure environment for intellectual exchange