

Computer Forensics & Network Security

ISU Information Assurance Center
www.iac.iastate.edu

2006

Outline

- Issues
- What is Forensics
- Case studies
- What is Digital Evidence
- Considerations with Digital Evidence
- Data deletion & retrieval
- Data Loss
- Network Security

Core Problems

We have millions of systems out there in which:

- Interoperability is more important than security
- Poorly designed or tested software
- Users do not hold vendors accountable for developing secure systems and software
- Social/people problem
- Attackers have changed tactics (people)

Forensics in the Private Sector

- What are you trying to do?
 - Detect attackers
 - Catch attackers
 - Prosecute attackers
 - Protect company assets from internal actions
 - Protect private data
 - Enforce company policies

Computer Forensics

- Looking for data/evidence on the computer (internal issues)
- Looking for data/evidence after an attack (external issues)
- Types of data:
 - Deleted files
 - Network activity
 - Application installation

Computer Forensics

- Keeping log files
- Monitoring the systems
 - Local
 - servers

Network Forensics

- Looking for data/evidence of what the employees are doing on the network
- Looking for data/evidence of an attack using the network

Network Forensics

- Difficult to trace back traffic
- Multiple hops
- All hops would need to keep logs

Network Forensics

- **Criminal:**
 - Scan networks for CP
 - Estimated 2% of traffic is CP
 - Traceback from network attack
- **Civil: RIAA & MPAA**
 - Scan P-to-P networks for songs

My first Case

- Mang: July 1995
 - Noticed activity on a server
 - Was able to document activity
 - Helped obtain search warrant Aug 9th 1995
 - Helped serve search warrant
 - Found large amount of software

Next big case:

- Jan 27, 1997
- Warez server in the dorms
- Helped obtain and serve search warrant in the dorms
- Helped analyze the systems, found large amount of pirated software

Case work

- Backdoor software installed on lab of computers to capture password
 - Found files that contained text that was typed by users in a public lab
 - Determined the date and time that software was installed
 - Used Video tape of lab to catch the person

Case Work

- Password capture software installed on web server
- Part of a web design contest.
- Person never found

Other cases

- Death threats
- Child porn, IP theft, Software theft.
- Teacher surfing for Porn
- RIAA

Jason Lighthall

Child Pornography

From: "Randy...." <taz@tryforfree.com>
To: <online@iastate.edu>, <abuse@iastate.edu>, <root@iastate.edu>,
<webmaster@iastate.edu>, <admin@iastate.edu>
Subject: CHILD PORN!!
Date: Sun, 24 Mar 2002 22:09:04 -0500

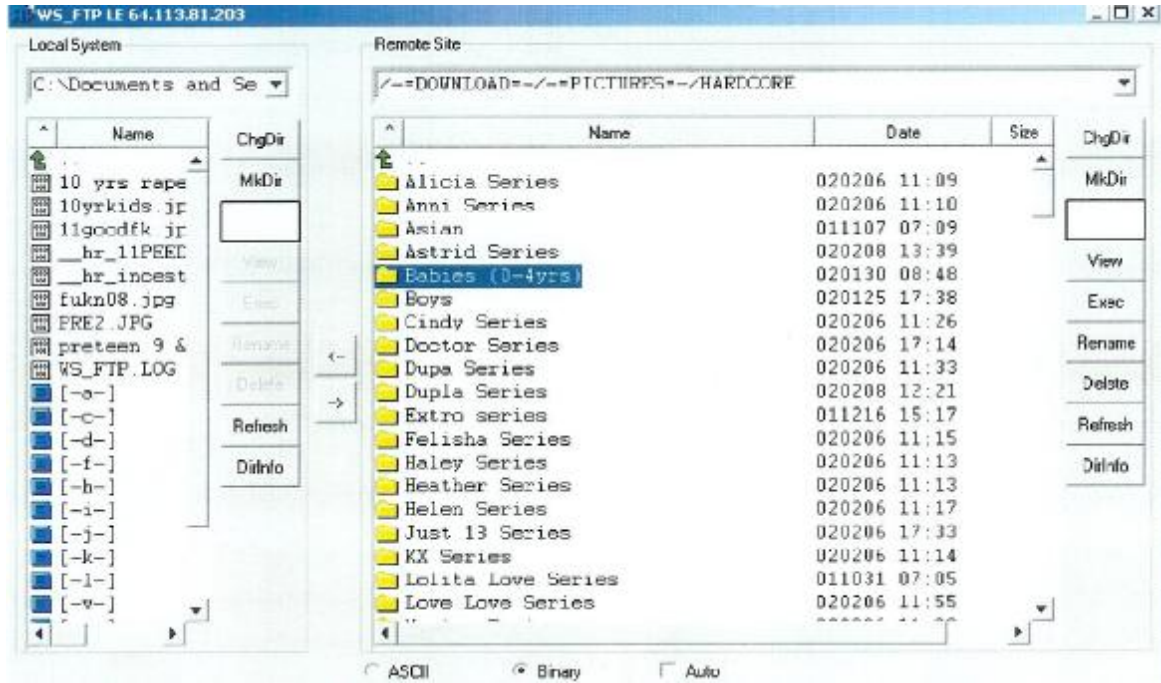
This IP listed below was submitted to my site advertising and distributing child porn. It was listed sometime sunday eve around 10pm EST. This IP seems to be tracked to your University. I hope you take the necessary action to catch and prosecute this offender. Listed below is the site and the description as entered onto my site. I have logs to prove it.

<ftp://upload:upload@jeanlucp27.dynip.com>

want child porn + preteen only
Which was submitted from 64.113.81.203
<ftp://upload:upload@64.113.81.203>

Warmest Regards,


TAZ....
www.WickedDownloads.com



Iris Fung

Computer Stalking/Unauthorized Access

The Email




X-Mailer: USANET web mailer (34FW.0700.17C.01)
Mime-Version: 1.0
Content-Type: text/plain; charset=US-ASCII

Dear Irwin,

I have had some lengthy discussions with my wife. She really likes to finish her master degree in information technology first before we move away from the DC area. Some bad experience she had recently with a web-based course has further convinced her that distance learning is not her cup of tea; on the other hand, transferring to a new program will essentially require her to start from scratch. Therefore, I would like to withdraw my name from the list of candidates for the FME position. I am truly sorry for whatever inconvenience I might have caused you.

Best regards,



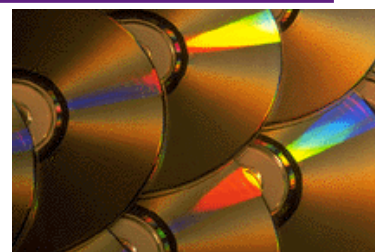
What is Digital/Electronic Evidence?

- Any kind of storage device
 - Computers, CD's, DVD's, floppy disks, hard drives, thumb drives
 - Digital cameras, memory sticks and memory cards, PDA's, cell phones
 - Fax machines, answering machines, cordless phones, pagers, caller-ID, scanners, printers and copiers
 - X-box, Playstation, etc.

Considerations with Digital/Electronic Evidence

- Digital evidence is fragile
- Recognizing potential evidence
- The role of the computer in the crime
- Consent Search vs. Search Warrant
- Forensic Analysis

Guidelines for Seizing Electronic Evidence



- Take all peripherals
- Obtain passwords, if possible
- Photograph scene
- Process scene for other storage devices

Examining Evidence

- Commercial Tools
- Public domain tools
- Disk copy/edit tools

Forensic Analysis

EnCase

Produced by

Guidance Software

Forensic and Enterprise
Investigation Solutions



Data deletion and retrieval

- A file is stored on the disk as three parts
 - Directory listing (the directory is a file that stores the file name)
 - Data usage table (shows which data blocks are used for the file)
 - File data (the data block that contain the data)

Data deletion

- Directory entry is changed to mark the file as deleted
- Data usage table – the blocks are marked as free in the table
- Data blocks – not altered

Data recovery

- Easy way
 - Find deleted file name in directory and then find first entry in data entry table.
 - Follow data entry table to put the data blocks together
- Hard way
 - Search disk for parts of files and try to put them back together
 - Drivelook (search hard drive and shows all words)

Other issues

- Tools are available that will delete all of the data
- The longer the time between deletion and recovery the lower the odds of recovery
- Wipe old drives before recycling

What to look for

- It depends on why we are looking
 - User files
 - Application files
 - Cookies
 - Internet history
 - Registry data
 - Email
- Issues:
 - Encrypted data
 - Computer authentication, can you prove who used the computer

Network forensics

- Content monitoring
- Email tracking
- Anonymous services

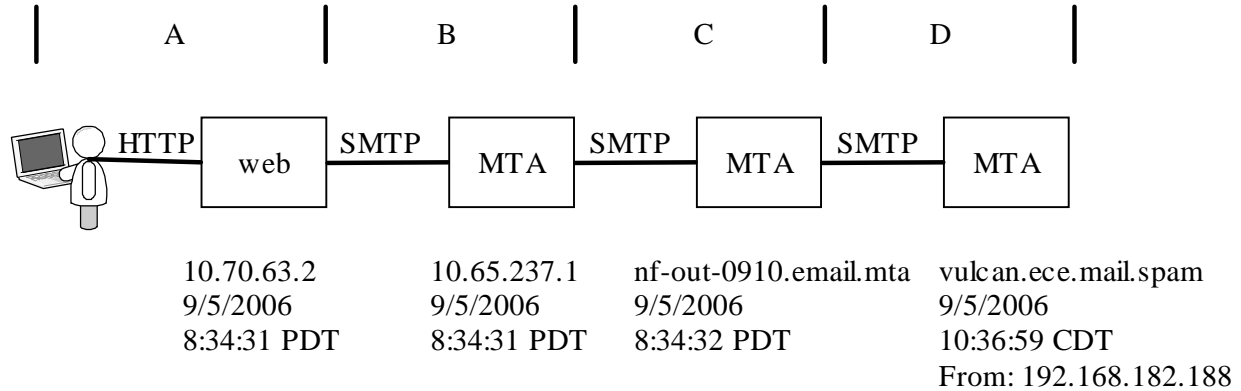
Outbound content filtering

- Used to keep private information from leaving
 - SS Numbers
 - Account Numbers
 - Medical records
- Will either log, stop, or encrypt violating emails

Bypassing a content filter

- Encryption
 - There are encrypted viruses
- Compression

Email Forensics

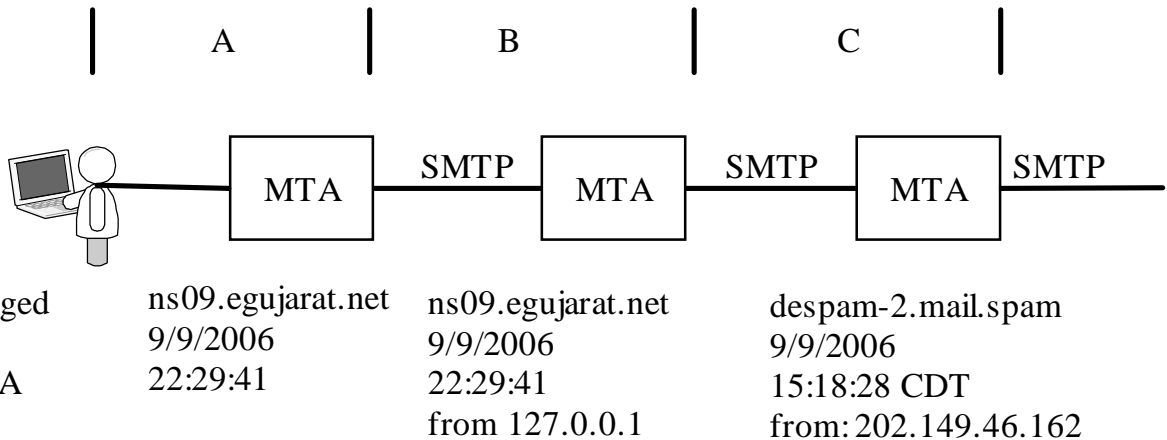


Email Forensics

```

D Received: from nf-out-0910.email.mta (nf-out-0910.email.mta
  [192.168.182.188])
  by vulcan.ece.mail.spam (8.12.8/8.9.3) with ESMTTP id
  k85FaxBT1486661
  for <john@ee.mail.spam>; Tue, 5 Sep 2006 10:36:59 -0500 (CDT)
C Received: by nf-out-0910.email.mta with SMTP id p77sol381355nfc
  for <john@ee.mail.spam>; Tue, 05 Sep 2006 08:34:32 -0700 (PDT)
  DomainKey-Signature: a=rsa-sha1; q=dns; c=noaws;
  s=beta; d=spammer.fake;
  h=received:message-id:date:from:to:subject:mime-
  version:content-type;
  b=BD9tHbNaozYZj9gNQqXmkrnHNA3N8+3W4NApcFJkKsKyX8DdOTS7Dp1VNunGx66SLcU5r
  YiDxCnY6SuVCktWq73DDH7MYEfWgaOtYdl/hILBIRVNcbLxGtyCoIT7I8use4F4RgCzZWc3
  Oc6fjqNzgGLE5s3RFQ9eVPhS+HxW+DA=
B Received: by 10.65.237.1 with SMTP id o1mr4809264qbr;
  Tue, 05 Sep 2006 08:34:31 -0700 (PDT)
A Received: by 10.70.63.2 with HTTP; Tue, 5 Sep 2006 08:34:31 -0700 (PDT)
  Message-ID:
  <ab156e9f0609050834v528b5b2eld9204458fe6409a1@mail.spammer.fake>
  Date: Tue, 5 Sep 2006 10:34:31 -0500
  From: "Harry Mudd" <Harry6502@spammer.fake>
  To: john@ee.mail.spam
  Subject: mail trace 2
  MIME-Version: 1.0
  
```

Email Forensics



```

(Removed local headers)
Received: from ns09.egujarat.net (202-149-46-162.static.exatt.net
[202.149.46.162] (may be forged))
D   by despam-2.iastate.edu (8.12.11.20060614/8.12.4) with ESMTP id
k89KIRCr017274
   for <dougj@iastate.edu>; Sat, 9 Sep 2006 15:18:28 -0500
C   Received: from ns09.egujarat.net (localhost.localdomain [127.0.0.1])
   by ns09.egujarat.net (8.13.5/8.13.5) with ESMTP id
k89H5sYI007263
   for <dougj@iastate.edu>; Sat, 9 Sep 2006 22:37:19 +0530
B   Received: (from administrator@localhost)
   by ns09.egujarat.net (8.13.5/8.13.5/Submit) id k89Gxf4q006335;
   Sat, 9 Sep 2006 22:29:41 +0530
A   Date: Sat, 9 Sep 2006 22:29:41 +0530
   Message-Id: <200609091659.k89Gxf4q006335@ns09.egujarat.net>
   To: dougj@iastate.edu
   Subject: Password change required!
   From: "eBay Inc." <admin@eBay.com>
   Content-Type: text/html
Spam Filter 2 X-egujarat-MailScanner-Information: Please contact the ISP for more
information
X-egujarat-MailScanner: Found to be clean
X-MailScanner-From: administrator@ns09.egujarat.net
Spam Filter 1 X-PMX-Version: 5.2.0.264296, Antispam-Engine: 2.4.0.264935, Antispam-
Data: 2006.9.9.124943
X-Perlmx-Spam: Gauge=XXXXXXXXXXXXXXXXXXXX, Probability=99%,

<p></p>
<BR>
Logo Dear sir, <BR>
<BR>
We recently have determined that different computers
have logged onto your eBay account, and multiple
password failures were present before the logons. We strongly advice
CHANGE YOUR PASSWORD. <BR>
<BR>
If this is not completed by <STRONG>September 15,
2006</STRONG>, we will be forced to suspend your
account indefinitely, as it may have been used for fraudulent purposes.
Thank you for your cooperation. <BR>
<BR>
Phishing Site <A
href="http://linux.net.zero.idv.tw/~ming/.change/index.php?MfcISAPIComma
nd=ChangeFPP"
target=_blank>Click here to Change Your Password</A></TD>

```

Email Forensics

Email Tracking

- www.readnotify.com
- Uses web bug tracking
- Keeps a log and emails you when the recipient opens the email.
- Looks like the email came from the sender, you send the email to:
 - user@domain.readnotify.com

Anonymous Email Services

- Login to a web site and send email from the site.
- Gmail, etc.
- Special sites for anonymous email
 - www.anonymousspeech.com

Privacy surfing the Internet

- Web servers can collect demographics about you
- www.privacy.net will show you all the things a webserver knows about you
- Examples:
 - Your browser type and Operating System
 - CPU type
 - whether JavaScript is enabled
 - Date/Time on your computer
 - Your IP address
 - Which plugins you have installed

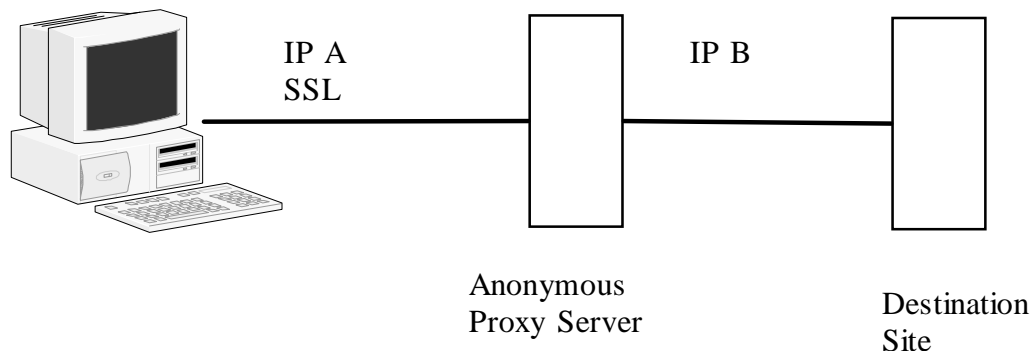
Privacy on the Internet

- Once you login and give your email address, you are no longer anonymous
- Some web sites share your email address with other sites
- This can lead to you receiving spam from sites to which you've never disclosed your email
- Some sites store cookies on your harddrive. Amazon.com does this to recommend books based on your previous purchases.
- One way to surf privately: connect through a proxy

Proxy Servers

- There are two reasons to be anonymous
 - Don't want webservers to know who we are
 - Don't want big brother (ie: your boss) to know what sites we are visiting
- A proxy can provide some amount of anonymity
- Examples of existing proxy servers used to provide anonymity:
 - anonymizer.com, safeweb.com, kaxy.com, the-cloak.com
- However, if your company does not wish you to be using these proxies, they can block access to them through their firewall.

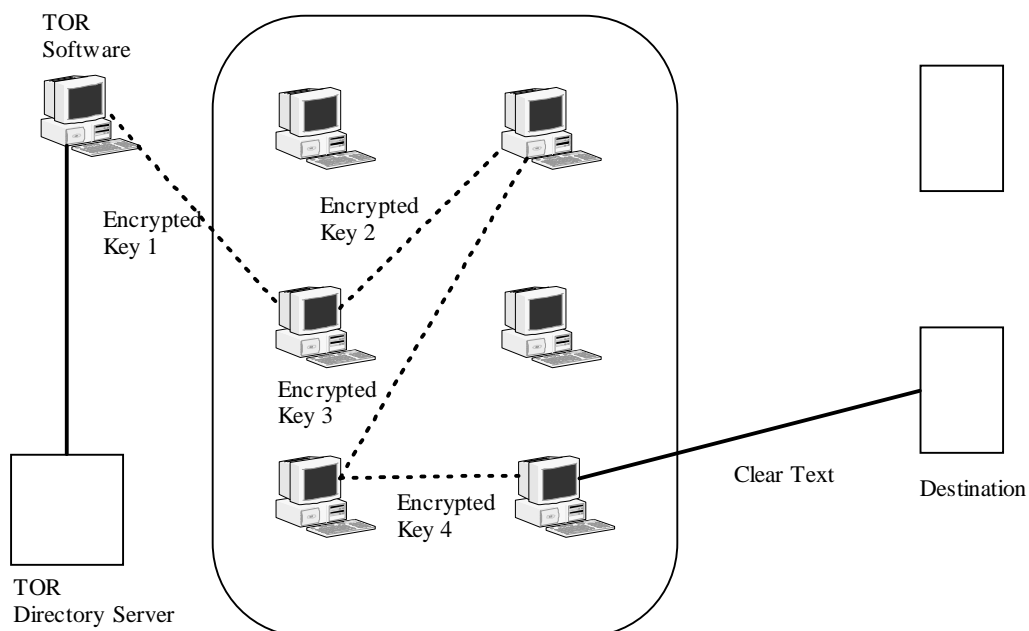
Secure Proxy Server



Proxy Servers

- However, TOR has a fix that prevents a company from blocking access to their site.
- It involves a system called onion routing
- See diagram next slide

TOR



Security Issues

- Bypass company security policies
- Hard to stop

Network Security

- Issues
- Employee Monitoring

Where are the problems

- Perimeter defenses
 - We build good walls
 - Strong technology in the market place
- Wireless
- Insider
 - Public places inside
 - Employee carelessness
 - Employee as a threat

Wireless (A world without perimeters)

- Wireless can create a new perimeter
 - Know access points
 - Unknown access points
- Treat your wireless access points the same as you would any remote access to your network.
 - Monitor it
 - Filter it
 - Protect it

Why is Wireless different?

- Most security models are based on a strong perimeter around an organization
- Wireless signals are not confined to the walls of an organization
- Wireless technology is plug and play
- Security makes wireless harder to use.

Other Defenses

- Secure Channels
- Perimeter defense
 - Firewalls
 - IDS
 - Egress monitoring
- Internal defense

Egress Monitoring

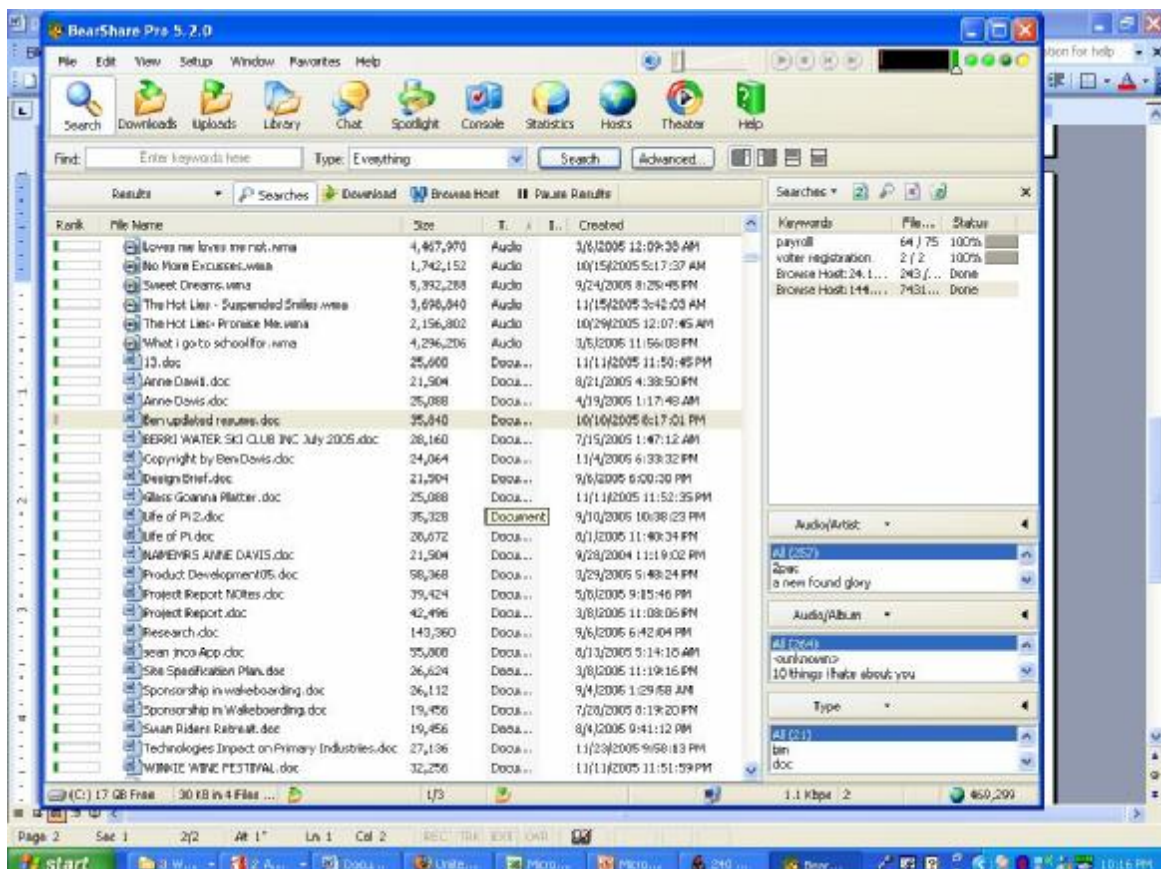
- We tend to focus on what is coming in.
It is easy to accidentally export data
- What is leaving your organization
 - Protocols
 - User installed applications
 - Confidential data

Careless Insider

- Attackers have shifted focus to the employees and home users
 - Phishing
 - Viruses
 - Spyware
- Using Email, peer to peer, IM, web sites, software downloads

Peer to peer problems

- Uses bandwidth
- Opens files up to sharing
- Good way to get viruses
- Possible legal action from RIAA



Insider defense

- Who can talk to what?
- Who has access to what?
 - Machines
 - Data
- Technologies
 - Access control
 - Internal honey pots
 - Internal firewalls

Where to start

- Make a Plan
- Start doing something now
- Decide what is most important
- Plan how to protect it
- Build the wall
 - Guard the wall
 - Watch the wall
- Don't forget to watch the inside activity

What's in a security policy?

- A security policy is a set of guidelines that help determine:
 - The need for security.
 - The categories of risk.
 - The responsibilities of the various members .
 - Appropriate levels of security based on risk.
 - Coordination and notification procedures.
- Risk = Threats x Vulnerabilities x Impact

Education

- Education is the key to strong security:
 - The attacker only needs to find one weakness while we must fix all holes.
 - Just like neighborhood watch we all have to take responsibility for security.
 - A policy is just a guideline.
 - No policy ever secured anything.

Personal Security

- Security starts at home
- Everyone needs to understand security
- Attacks are becoming people focused
 - Based on employment

What is safe?

- Ordering on-line
- Reading simple email
- Sending email
- Chat rooms
- Surfing the web

What is not safe?

- Reading email attachments
- Downloading programs
- Filling out forms on line
- Sending email
- Ordering on-line
- Chat rooms
- Surfing the web

What can I do?

- Virus scanning
- Personal firewall
- Be careful
 - Downloads
 - Email attachments
 - Sending info to a web site
 - Wireless
 - Peer to Peer
- Backups

Why is still a problem?

- If this was a technology issue only we could win.
- Information Assurance is a Social/human issue
- The information war **cannot** be won on technology alone
- **Everyone** must be involved

Questions
