

A User-Services-Driven Approach To Computer and Network Security

**A SIGUCCS Tutorial
November 6th, 1-4:30
Monterey, California**

Joe St Sauver, Ph.D. (joe@uoregon.edu)
Computing Center, University of Oregon
<http://www.uoregon.edu/~joe/siguccs/>

Introduction

Welcome to SIGUCCS in Monterey!

- Let me be among the first to welcome you to SIGUCCS and Monterey!
- I know this will be a great conference for everyone, and I appreciate your taking the time to attend this pre-conference tutorial.
- I hope you'll find it helpful as you work to help keep your users secure.

A Little About The Format of This Talk

- Because...
 - I tend to talk somewhat fast
 - I hate to be misquoted
 - this talk deals with technical material and has lots of URLs
 - some attendees may end up sharing this talk with others after this meeting is over
 - there may be audience members for whom English is not their primary language,
 - there may be hearing-impaired audience members (think of these notes as "closed captioning" for them), and because
 - I'm highly prone toward rambling and exceeding my allotted time if I'm not scripted...

I've gone ahead and prepared this talk in some detail; at this point you should each have a printed copy. I know that this will destroy the illusion that my talk is all just a spontaneous/extemporaneous reflection, but I hope you'll forgive me.

Attendee Introductions and Interests/Concerns

- What I'd like to do is begin by taking a few minutes to go around the room, giving each attendee a chance to...
 - 1) give their name and the institution they're from
 - 2) talk briefly about what they do there
 - 3) briefly mention their goals for this workshop
 - 4) tell us the biggest security-related problem they're currently wrestling with (or the issue they'd particularly like to make sure we cover today)
- but you can also feel free to just say "Hi" if you'd rather. :-)

My Background

- I've been at the University of Oregon Computing Center for about 18 years now, and that entire time has been in the User Services part of the organization. My current title is "Director, User Services and Network Applications," and I do understand what user services folks are facing because I've "been there and done that," and in fact I continue to work with my staff to help UO's users virtually every day.
- In addition to my work with the UO Computing Center, I also participate in some national efforts, including serving as co-chair of the Educause Security Effective Practices Working Group (with Gary Dobbins of Notre Dame), serving as an appointed member of the I2 Security at Line Speed (SALSA) working group, acting as one of three senior technical advisors to the carrier Messaging Anti-Abuse Working Group, etc.
- All opinions in today's talk, however, are strictly my own.

Today's Agenda

- What we'll talk about today will be driven in part by what you're interested in, but I've got a few ideas lined out in case you don't have any burning questions you'd like to talk about.
- I definitely want to hear what you've got to say, and share things that will be helpful and relevant to you.
- My goal is to focus on practical suggestions for stuff you can actually DO to improve your users'/your university's security.
- We've got about 3 1/2 hours this afternoon, and we'll take a break at about 2:30PM to give people a chance to stretch their legs and get some refreshments and make a pit stop.
- If we go late, I'll stay till people get bored, if we get done early, that's okay with me too.

Disclaimers

- While the suggestions in this presentation *may* improve your security, and reasonable care has been used in compiling this presentation, no brief presentation of this sort can substitute for an onsite, comprehensive and intensive security review done at your site by qualified professionals. We recommend you have one done.
- If you do elect to take any of the steps outlined in this document, you acknowledge that some of those steps may include inherent risks of their own, including but not limited to loss of data, or loss of functionality/usability.
- Make a complete backup of each system, including all personal files and the system's registry, before making ANY changes.
- You understand and acknowledge that even if you follow all the recommendations in this presentation, you and your campus network and/or systems may still be vulnerable to known and/or as-yet-unknown security threats.
- Mention of a particular hardware or software product in this presentation should not be taken to be a recommendation excluding equally capable equivalent products. Products change over time, and needs can vary dramatically, so always do your own evaluation before purchasing any product.

**Why Should User Services Worry
About System or Network Security?
Isn't That a "Network Thing" or a
"Systems Programmer" Thing?**

Does User Services Even Have a Dog in This Fight?

- Traditionally, if you look at an average IT organization, security often ends up as something that's been affiliated with the "networking guys," more or less by default, or perhaps it is something that's traditionally been the provenance of your large system systems programming folks.
- The networking guys, after all, are usually the ones who run the institution-wide firewall (if there is one), and the networking guys are also the ones who tend to run any intrusion detection system (such as Snort or Bro).
- The systems programmers, as professional system administrators, are accustomed to thinking about system security, patching and logging, authentication, etc.
- But what about the user services folks? How do we end up in the "security" biz?

User Services and Security

- I believe that increasingly security IS a user services issue:
 - network traffic is getting firewalled, encrypted, tunneled ("everything over port 80"), and otherwise becoming difficult to deal with exclusively at the network layer
 - fewer and fewer users work directly on large local systems; most users have never used anything except a personal computer... and 1000's of web sites off campus (so they may never even work with your local systems folks)
 - we ARE the ones who work directly with the users who are struggling to help them keep their desktop systems safe
 - we ARE the ones who respond to abuse complaints
 - we ARE the ones who work with users to deal with compromised systems
 - we ARE the ones who do the training and documentation
 - we ARE the ones who act as defacto user advocates, and
 - of course user services always gets the really ugly jobs. :-)

And Trust Me, The Problem *IS* Ugly...

- One of my favorite quotes:

‘I'm here to tell the security pros reading this that we are in deeeeeep trouble when it comes to securing the computers of [your typical American computer user].

‘Security is just not a concept that "normal" folks focus on. It's not even on the radar screen. It's just not thought about at all.’

“Joe Average User Is In Trouble”

By Scott Granneman Oct 22, 2003

<http://www.securityfocus.com/columnists/193>

While Users May Not Be Worrying About Security, College and University IT Officials Sure Are...

- "College and university IT officials identify 'network and data security' as the 'single most important IT issue affecting their institutions over the next two-three years' according to new data from the Campus Computing Project [the 2005 National Survey of Information Technology in Higher Education]."

<http://www.campuscomputing.net/>
October 2005

- This is another reason why security is user services job – when something's the top issue we're confronting, by default that issue becomes everyone's job (including ours).

Balancing Risks, Costs and Usability

Low Hanging (Ripe) Fruit First

- As we think about dealing with security issues, we need to recognize that there are some security risks which will be extremely difficult (or extremely expensive) to eliminate.
- Our general approach will be to deal with the easy stuff first, and then tackle the harder stuff as we go along.
- We'll also try to handle the issues that are ripe/currently important before we handle the theoretical issues that aren't currently causing critical problems.
- This approach is consistent with the pragmatic emphasis of things like the SANS Top 20 list, <http://www.sans.org/top20/>

Mundane Issues, Many With Easy Solutions

- Fortunately, many security issues are mundane and tractable, and quite easy to deal with, IF people are paying attention.

“Gartner reports that more than 90% of security exploits are carried out through vulnerabilities for which there is a known patch.”

<http://www.nwfusion.com/news/2002/1111bigfix.html>

A Boat's Safe In The Harbor, But That's Not What a Boat's For...

- You should also be clear that our goal is not to make things "**100% safe**" -- being perfectly safe keeps you from doing a lot of things that may have substantial payoff and a small/tolerable amount of associated risk.
- Our goal is to help you operate in a reasonable and prudent way, intelligently assessing and balancing risks and rewards, without being paranoid. You should have locks on your door and maybe a burglar alarm, but probably not a minefield.

Focusing on the Unmanaged Environment

- While we know that some of you may be running in a managed desktop environment, for the most part, we don't believe that's where your issues will reside – we believe that most of your problems will come from the unmanaged systems that are controlled by end users.
- These may be personally owned systems in student residence halls, or faculty laptops that go back and forth between home and the office, or any of a variety of other sort of non-centrally managed systems.

Looking For Distributed "Off The Shelf" Solutions To Security Problems Where We Can Find Them

- When we think about security solutions, we're prone to looking for solutions that can be handled in a distributed environment, rather than solutions that require centralized control and campus-wide adoption. Thus, for example, when it comes to secure login, we tend to promote ssh (secure shell) rather than Kerberos-based solutions. Why? We recognize that in many cases you may not be able to dictate a centralized solution – you can only encourage users to do the right thing.
- We also understand that many of you have limited resources (particularly limited staff), so there is often substantial interest in solutions that can be obtained "off the shelf" (ideally as free open source products), simply because large in-house coding projects aren't possible (no staff's available to do them).

Dealing with the User's Workstation

This Part's (Virtually) All About PCs Running Windows

- In this section, you'll notice that we largely focus on PCs running Windows. That's for a couple of reasons:
 - PCs running Windows represent ~94% of the desktop market as of late 2003; see:
<http://content.techweb.com/wire/story/TWB20031008S0013>

Rebut-able hypothesis: hackers crack Windows because that's what's “out there...”

- Alternative/additional hypothesis: hackers crack Windows because it has more unpatched vulnerabilities than some alternative desktop operating systems

What Does Secunia Say About Some Desktop O/S's?

- **Windows XP Pro** (<http://secunia.com/product/22/>):
 - 26 of 118 Secunia advisories listed as "unpatched"
 - with all vendor patches installed and all vendor workarounds applied, is currently affected by one or more Secunia advisories rated **Highly critical** [as of Oct 30, 2005]
- **Apple Mac OS X** (<http://secunia.com/product/96/>):
 - 1 of 48 Secunia advisories listed as "unpatched"
 - with all vendor patches installed and all vendor workarounds applied, is currently affected by one or more Secunia advisories rated **Not critical**
- **Fedora Core 4** (<http://secunia.com/product/5251/>):
 - 0 of 60 Secunia advisories listed as "unpatched"
- **FreeBSD 5.x** (<http://secunia.com/product/1132/>):
 - 0 of 56 Secunia advisories listed as "unpatched"
- We need to get those highly critical patches, Microsoft...

Secunia Advisories

- [Secunia Advisories](#)
- [Historic Advisories](#)
- [Listed By Product](#)
- [Listed By Vendor](#)
- [Statistics](#)
- [About Advisories](#)
- [Secunia Research](#)

Virus Information

- [Virus Information](#)
- [Chronological List](#)
- [Last 10 Virus Alerts](#)
- [About Virus Info](#)

Mailing Lists

- [Secunia Advisories](#)
- [Weekly Summary](#)
- [Secunia Virus Alerts](#)

Info / Contact

- [Secunia Products](#)
- [Customer Area](#)

Microsoft Windows XP Professional

Vendor:
[Microsoft](#)

Product Link:
N/A

Product Affected By:
118 Secunia Advisories

Microsoft Windows XP Professional with all vendor patches installed and all vendor workarounds applied, is currently affected by one or more Secunia advisories rated **Highly critical** 

This is based on the most severe Secunia advisory, which is marked as "Unpatched" in the Secunia database. Go to [Unpatched/Patched list](#) below for details.

Currently, 26 out of 118 Secunia advisories, is marked as "Unpatched" in the Secunia database.

Table of Contents for This Page:

- [Send Feedback to Secunia](#)
- [Statistics Based on Advisories](#)
 - [Advisories Month by Month](#)
 - [Solution Status](#)
 - [Criticality](#)
 - [Where](#)
 - [Impact](#)
- [List of Patched/Unpatched Advisories](#)
 - [2005](#)
 - [2004](#)
 - [2003](#)

Monitor This Product...

...and everything else on your network!

Secunia allows you to easily filter and manage security information.

Alerting you whenever a vulnerability affects any software on your network.

[Secunia Customer Area](#)

Search

Secunia News

2005-06-21

Multiple browsers are vulnerable to the [Dialog Origin Spoofing Vulnerability](#).

2005-04-04

Various Mozilla browsers are vulnerable to the [Mozilla Arbitrary Memory Exposure Vulnerability](#).

2005-03-17

Want a new IT Security job? [Vacant positions at Secunia](#)

Let's Assume You're Stuck With What You've Got

- While it might be nice to hypothetically contemplate a campus desktop environment free of Microsoft Windows, the reality is that you're probably stuck with a substantial number of hosts running Microsoft Windows...
- Assuming that's the case, what should you do?

Supported Version of the Operating System

If Users Are Running An Old Version of Windows They Must Get to a Current Version

- Believe it or not, some of your departments and some of your end users are probably still running older versions of Windows such as Windows 95, Windows 98, Windows 98 SE, Windows ME, Windows NT 4.0, Windows 3.11, etc.

Job number one is to get them onto a current version of Windows (or help them to switch OS if you prefer :-)).

They cannot safely stay on these earlier versions of Windows.

- Note that because of the cost of upgrading ancient hardware to run a current version of the operating system, it may not be cost effective to even try to do so, given that you can get a new low end Dell desktop for right around \$320 (onesie-twosie quantities, Dell Small Business), or a new MiniMac for \$500. 26

System Replacement Lifecycle

- Because operating systems are so tightly coupled to the associated hardware, and because upgrading existing systems is often not cost effective, it is important for you (as an institution) to develop a system replacement lifecycle. For example, you might determine that you'll replace 1/4th of all systems at your university each year, which means that by the end of four years, no system should be older than 4 years.
- As you plan for/execute this sort of strategy, two things to note:
 - yes, it is expensive to replace 1/4th of all systems each year, but system purchase costs are just a small fraction of the total cost of system ownership
 - as you replace systems, you want to get the old systems OUT of the college/university environment; do NOT let them get "pushed down"/linger as machines sold at a discount for home use or machines used in cobbled together labs

Sanitization of Surplus Equipment

- If/when you upgrade, make sure you carefully sanitize the contents of your old hardware before you dispose of it. See:

"Information on Hard Drives in Surplus Hardware: 'Deleted' Does Not Mean 'Gone'"

<http://cc.uoregon.edu/cnews/summer2005/purge.htm>

Interesting Digression... Do You Know When Windows XP Pro Will No Longer Be Available for Direct OEM and Retail Licensing?

- See "Windows Life-Cycle Policy"
<http://www.microsoft.com/windows/lifecycle/default.mspx>
Note the December 31, 2005 date for Windows XP Pro for "Direct OEM and Retail License Availability (end date)"
- On the other hand...
<http://support.microsoft.com/lifecycle/?LN=en-us&x=12&y=15&p1=3223>
mentions dates for Windows XP Professional of:
 - mainstream support retired: 12/31/2006
 - extended support retired: 12/31/2011
- <http://support.microsoft.com/gp/lifepolicy> states
"Microsoft will provide mainstream support* for either 5 years after the date of general availability, or for 2 years after the successor product (N+1) is released, whichever is longer."
- Are you following the testing of Windows Vista?
<http://www.microsoft.com/windowsvista/default.mspx>

The First (of Many) Corner Cases

- As you strive to get everyone onto supported versions of Windows, you'll find that there are some embedded systems running Windows which simply aren't upgradeable. The classic example is a scientific instrumentation controller from a provider who's now out of business, etc.
- When you run into those (and you will, if you're thorough about trying to get people upgraded), you will need to take special care to bi-directionally firewall those systems, protecting them from the Internet, and the Internet from them. Allow only the absolute minimum set of protocols through, and then only to the absolute minimum range of addresses.

Patching the O/S

Microsoft Critical Updates

- Once (most) of your Windows users are running a current version of Windows XP Pro, it is absolutely vital that everyone patch their systems when Microsoft releases Critical Updates... and those updates are now a routine monthly occurrence.
- When critical updates don't get applied, viruses and other malware will infest your systems, compromising confidential data and potentially turning those systems into network sniffers, spam delivery systems, and denial of service attack vectors.

Getting Initially Up To Date

- If you're not currently fully patched up, you'll need to at least get all service packs and critical updates downloaded and installed.

Doing so initially can be difficult for two reasons:

(i) the sheer volume of updates can be onerous for dialup users, and

(ii) unless you're behind a hardware (or software) firewall, you will commonly become infected before you can even finish downloading the required patches. (Yes, it has gotten that bad)

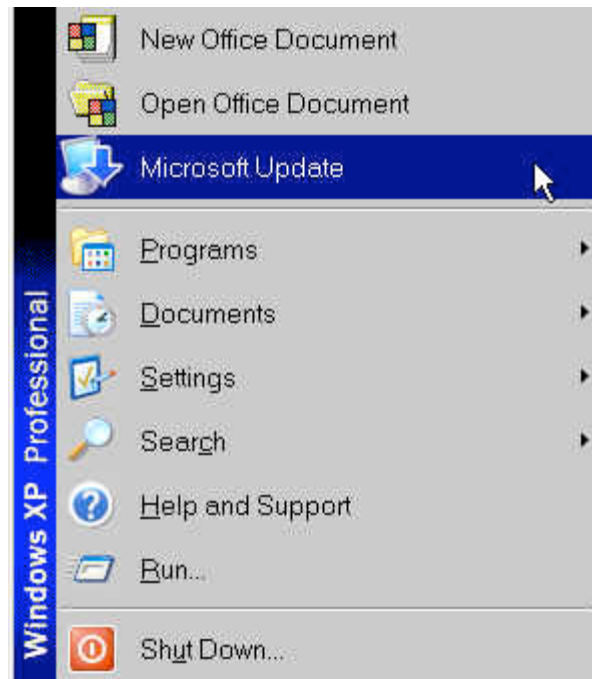
Dealing With the “Chicken and Egg Problem”

- Since you won't have time to download patches before you get infected, how are you to deal with that vulnerability?
- One option is to request a copy of the Microsoft XP SP2 CD by mail (allow 4-6 weeks for delivery; you *may* have enough time to download the patches over a dialup during that time :-)); see:

http://www.microsoft.com/windowsxp/downloads/updates/sp2/cdorder/en_us/default.mspx

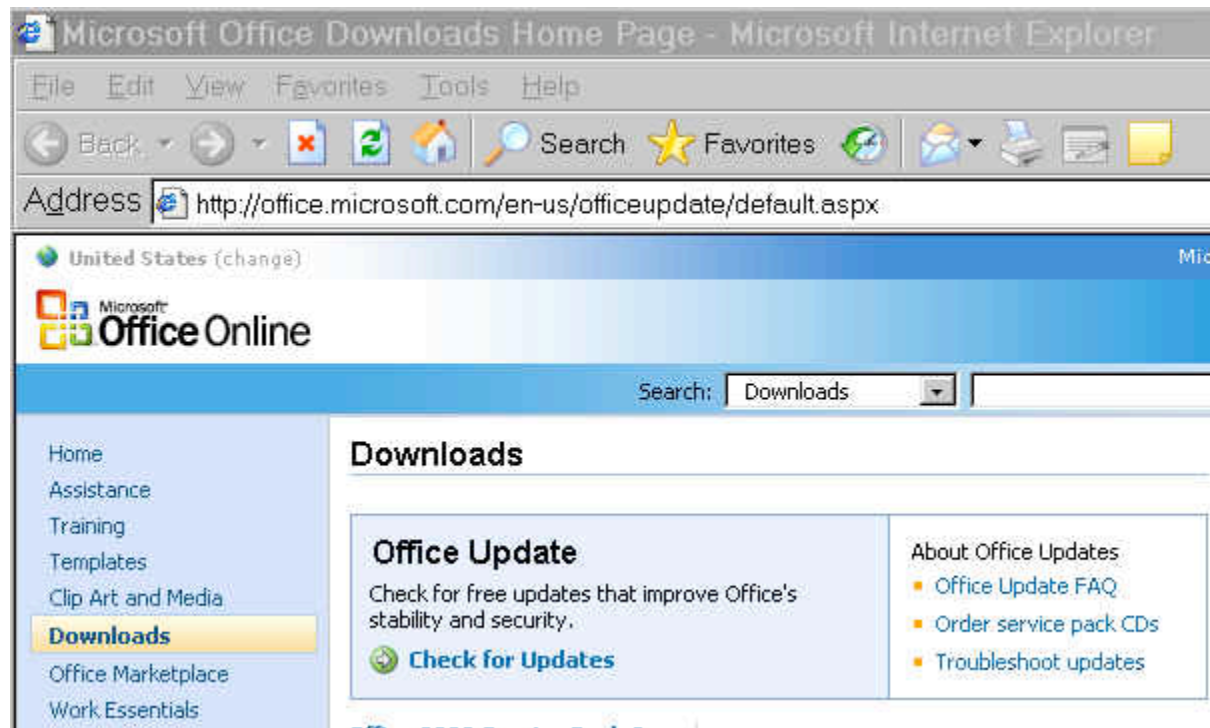
- Alternatively, install a personal hardware firewall or a personal software firewall (such as ZoneAlarm), and ONLY THEN connect the host to the network to get critical updates.

Installing Updates: Microsoft (not Windows) Update



If you or your users don't see this menu item, use Internet Explorer to go to <http://update.microsoft.com/microsoftupdate>

After Updating Windows Itself, Be Sure to Also Check for MS Office Updates



Note: if you're using Microsoft Update (NOT Windows Update) this is only necessary if users are running a version of Office that's pre-Office 2003...

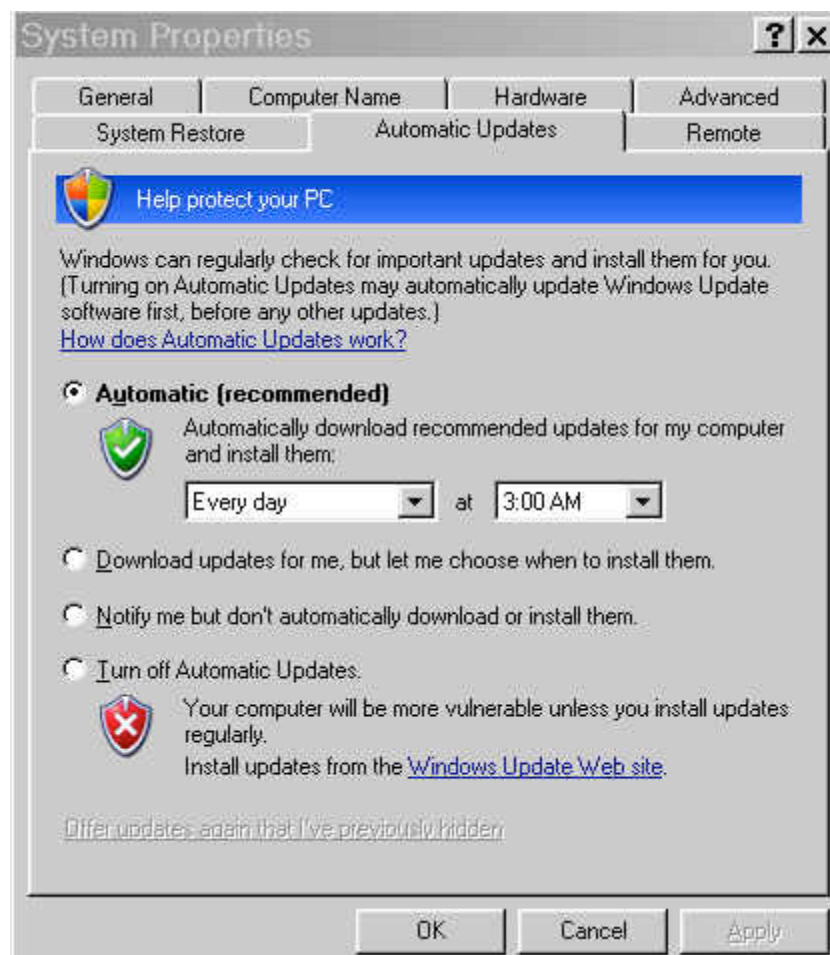
Reboots

- Get in the habit of periodically manually rebooting your system just to make sure that you don't have updates which have been installed, but which have not rolled into place because your system hasn't rebooted for some reason

Enabling Automatic Updates For Future Critical Updates

- Start → Settings → Control Panel → System → Automatic Updates Tab → Automatic
- Specify “Every day” and pick a convenient time when your computer will be powered up and on the network. (multiple machines? Stagger the times)
- Periodically run Microsoft Update manually just to make sure nothing’s “broken”

The Magic Automatic Updates Screen



Note Well: Automatically Applying Patches Is Not Without Its Own Risks

- I've personally had three production W2K servers get blown off the air by a single automatically-applied updates (thankfully all three were subsequently recoverable via SFC /SCANNOW). Trust me when I tell you that automatically patching can be very risky. On the other hand, not patching is definitely even worse.
- I highly recommend you read “Patch and Pray”
<http://www.csoononline.com/read/080103/patch.html> [“It's the dirtiest little secret in the software industry: Patching no longer works. And there's nothing you can do about it. Except maybe patch less. Or possibly patch more.”]

Run Microsoft Baseline Security Advisor 2

- Even better than just manually checking for missing updates by manually running Microsoft Update, try Microsoft Baseline Security Advisor Version 2 available from:

www.microsoft.com/technet/security/tools/mbsa2/default.mspx

Running it will check a wide variety of potential issues, including patch status currency, but also a whole bunch of other issues, too.

- *Note:* to download this free tool, you need to first run the Microsoft Genuine Advantage tool which checks to make sure you're running a legal copy of MS Windows...

Sample MS BSA2 Output (partial)

The screenshot displays the Microsoft Baseline Security Analyzer 2 (BSA2) application window. The title bar reads "Microsoft Baseline Security Analyzer 2". The main header area features the Microsoft logo and the text "Baseline Security Analyzer".

Left Sidebar:

- Microsoft Baseline Security Analyzer**
 - Welcome
 - Pick a computer to scan
 - Pick multiple computers to scan
 - Pick a security report to view
 - View a security report**
- See Also**
 - Microsoft Baseline Security Analyzer Help
 - About Microsoft Baseline Security Analyzer
 - Microsoft Security Web site
- Actions**
 - Print
 - Copy

Main Content Area:

View security report

Sort Order: Score (worst first)

Score	Issue	Result
✓	Office Security Updates	No security updates are missing. What was scanned Result details
✓	Windows Security Updates	No security updates are missing. What was scanned Result details

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
✖	Incomplete Updates	No incomplete software update installations were found. What was scanned How to correct this
i	Windows Firewall	Windows Firewall is disabled and has exceptions configured. Window Firewall is disabled or has exceptions on all network connections. What was scanned Result details How to correct this
✓	Local Account Password Test	No user accounts have simple passwords. What was scanned Result details
✓	Automatic Updates	Updates are automatically downloaded and installed on this computer. What was scanned

Navigation buttons: Previous security report Next security report

© 2002-2005 Microsoft Corporation. All rights reserved.

Trust, But Verify

- You should also consider scanning your own networks to make sure users are patched up to date... Microsoft has tools: <http://www.microsoft.com/technet/security/tools/default.msp> and there are many freely available products (e.g., Nessus)
- Commercial scanning products are also available, and those products may probe more for additional vulnerabilities/issues. One popular commercial product is GFI LANguard (See <http://www.gfi.com/languard/>)
- Notes:
 - scanning needs to be coordinated with/blessed by your legal counsel and by management; do not scan machines you don't administer without proper prior authorization
 - aggressive scanning may cause some systems to tip over
 - as firewall usage becomes more ubiquitous, external scanning is coming to be of diminishing value (good!)

What Do You Mean "It's Good That External Scanning Is Becoming Ineffective?" Are You Crazy?

- Any security tool that you can use, the bad guys can also use. If you can scan for security vulnerabilities, so can they.
- In the ideal world, it won't matter where you scan from, nothing will be visible. Nice onesie-tvosie test of how you look from the point of view of the world is available via GRC's Shield's Up tester: <http://grc.com/>

What About Agent-Based Systems?

- Because of the limitations associated with scanning, agent based solutions have been growing in importance/popularity.
- In this approach, users download and install a small program on their systems. That program, or "agent," can then report on the status of the system, or actually apply specified patches.
- Examples include products from BigFix, Patchlink & Shavlik
- Issues in higher education typically include:
 - cost (the cost of some commercial agent-based patch management products is simply breathtaking)
 - "intrusiveness" (aka "I don't want you to spy on my system")
 - risk (patching someone else's system *could* break it)
 - university folks sometimes use applications which are virtually unknown in traditional corporate markets
 - some patch managements systems don't scale very well
 - some products require central servers running Windows

What About Network Access Control Systems?

- Still another alternative is to check patch status at the time the user attempts to do something (like connect to the Internet). At that time, if the user isn't patched, isn't using an antivirus or antispyware product, or is otherwise deficient, access can be denied (or the deficiency remediated as a condition of proceeding).
- Examples of this sort of product include Cisco Clean Access, Bradford Campus Manager, and Impulse Safe.Connect.

Anti-Virus Software

Site License A Windows Antivirus Product

- Do you have a site license for a Windows antivirus program covering all of your users? You **MUST** do so. This is another absolutely non-optional security measure these days.
- Be sure your people keep their antivirus definitions up to date!
- Be sure they use their AV software both at work **AND** at home!
- Antivirus software with stale definitions, or antivirus software that's used only at some locations, is a recipe for absolute disaster.

Some Antivirus Vendors

- UO currently site licenses McAfee Enterprise 8.0i for antivirus and antispyware (we'd previously used Norton from Symantec, but changed this past summer) however, there are many commercial antivirus programs you should consider/evaluate. Some antivirus product websites you may want to look at include...

<http://www.arcabit.com/>

<http://www.avast.com/>

<http://www.avira.com/>

<http://www.bitdefender.com/>

<http://www.ca.com/>

<http://www.clamwin.com/>

<http://www.drweb.com/>

(continued)

Some Antivirus Vendors (continued)

- <http://www.eset.com/>
<http://www.fortinet.com/>
<http://www.f-prot.com/>
<http://www.grisoft.com/>
<http://www.hbedv.com/en/>
<http://www.kaspersky.com/>
<http://us.mcafee.com/>
<http://www.norman.com/>
<http://www.pandasoftware.com/>
<http://www.quickheal.co.in/>
<http://www.sophos.com/>
<http://www.symantec.com/>
<http://www.trendmicro.com/>

What Factors Should You Consider In Evaluating Antivirus Products?

- Does the product detect, identify and remove the viruses you're seeing? (one strategy for testing is to pick a particularly overrun user system, and then, with the permission of the user, clone that disk; you then try each product, restoring the system from the infested copy of the disk after using each product)
- Does the product block viruses as they're seen in applications (so-called active protection), or does it only deal with viruses found as a result of periodic scans?
- How easy is the product for users to use?
- Are new virus signatures released frequently? Will the A/V product automatically detect, download and install the new virus definitions?
- Does the product do heuristic detection as well as signature-based approaches?

What Factors Should You Consider In Evaluating Antivirus Products? (cont. 2)

- What will the vendor let you do in terms of distribution?
Secure online distribution? Inclusion on your own security CD (assuming you want to do one)? Only distribution via their own copy-protected commercial media? Is activation required?
- Assuming you do work in a managed environment, does the A/V product support central administration?
- Is a bootable version available?
- Is the product used by other colleges/universities similar to us? If so, what do they say about the product when we talk with them about it? If there are no college/university customers using this product, why?
- What versions of Windows (or other operating systems) are supported?
- And of course, what's the direct cost/user? Speaking of cost...⁵²

Some Thoughts on Site Licensing A/V Software

- Be prepared, at least in the case of some vendors, for site licensing to make your head hurt. Sometimes you can't just pay a flat fee or provide an estimate of the size of your school (students plus faculty plus staff) – you may need to separately estimate/track faculty/staff systems vs. student systems, pay a differential amount for Mac vs. PC licenses, separately purchase home use rights (or even license a different product for home use!), etc. This can be a huge pain, and should be avoided. Negotiate a stipulated price to cover all your users.
- Some antivirus vendors may not "get" the unmanaged/consumer-like nature of the typical higher education computing environment, and may try to push you toward an enterprise antivirus product. Enterprise products are often less appropriate for higher-ed's decentralized computing environment than consumer-oriented products.

Some Thoughts on Site Licensing A/V Software (2)

- When negotiating pricing, recognize that some of your users may have more than one computer, some may have one (and only one), while others may have none. Working from a straight "headcount" number may not be appropriate.
- Some vendors may try to push a complete security "suite" rather than just letting you purchase (just) the antivirus product you may actually be interested in. Carefully evaluate whether or not you want a complete bundle including a single vendor's firewall product AND anti-spyware product AND anti-spam product, etc. (some vendors may have an excellent anti-virus product, but a weak firewall product, for example, or vice versa). In other cases, excellent security products may already be part of the operating system, or may be freely available.

"Do I Need A Mac Anti Virus Product?"

- Mac malware, while currently rare, does exist. For example:
securityresponse.symantec.com/avcenter/venc/data/mac0s.mw2004.trojan.html
securityresponse.symantec.com/avcenter/venc/data/sh.renepo.b.html
 - Even if there isn't a pressing threat right now, do you really want to wait until a crisis actually develops before ordering and deploying a solution? Maybe you're faster at ordering and receiving stuff almost just-in-time than we are. :-)
 - If you begin telling folks that they may not need an antivirus product (well, at least not sometimes), you'll be surprised how quickly that generalizes in bad/unexpected ways. You want a nice clean and easy to remember rule: "You must run antivirus."
- On the other hand:
 - Mac viruses are likely a *small* risk (but remember macro viruses)
 - Mac A/V options are rather limited (we use Virex)
- You'll need to make the call on this one...

Antivirus Products for Home Use?

- In some cases, it may be impossible for a college or university to license an antivirus product for home use. When that occurs, a free product available for home use may be another option...
- AntiVir PersonalEdition Classic
<http://www.free-av.com/>
- Avast! 4 Home Edition
http://www.avast.com/eng/down_home.html
- AVG Free Edition
http://www.grisoft.com/us/us_dwnl_free.php
- ClamWin
<http://www.clamwin.com/>
- CA EZ Antivirus (One year free trial, "exclusive offer for Microsoft customers")
<http://www.my-etrust.com/microsoft/>

What About A/V on Email Servers?

- We know that user services folks often do NOT run college/university email servers, but you probably know who does...
- We know that there's sometimes an evil temptation to say "well, since we're dealing with A/V issues on the desktop, I guess we don't need to futz with viruses on our mail servers..." that would be a BIG mistake. Think belt and suspenders, folks! Commercial (and open source) A/V gateway software products for your mail servers are available from the usual suspects.
- If you don't want to run a true antivirus product on your mail servers, and you may not, another option is to strip (or at least defang) potentially dangerous files based on their file extensions. One popular tool used for stripping potentially dangerous executable attachments running Sendmail is the Procmail E-mail Sanitizer. See: <http://public.planetmirror.com/pub/impsec/email-tools/procmail-security.html>

Handling The Viruses That Do Get Detected Properly

- If you do run a gateway antivirus program, or have a program that strips viruses from incoming email, make sure that it is NOT configured to send misdirected “you’ve got a virus!!!” warnings to thousands of forged From: addresses every day
- Bogus virus warnings can be a bigger problem for your users and neighbors than the actual viruses themselves...
- See <http://www.attrition.org/security/rant/av-spammers.html> and <http://www.spamcop.net/fom-serve/cache/329.html>
- In fact, the problems associated with bogus antivirus notifications have become so severe that some sites have begun to automatically block all email coming from sites that have broken antivirus gateways.
- Educate the antivirus software vendors you work with!
Sending bogus virus warnings to forged From: addresses is NOT a feature!

"But, but, but..."

- "If you don't/can't detect viral content while the remote mail server is still actually connected, and you don't want to deliver viral email to random recipients, and you don't want to bounce the mail to a forged purported sender... what should you do with viral email you receive?"
 - you could defang the attachment (e.g., by postpending .txt or by other means), and then deliver it, but users can make a "determined effort" to hurt themselves and "rename the file back" to what it was
 - you could strip the viral (or potentially viral) content, and deliver just what's left (what we call a viral "husk"), but those can quickly become a nuisance in their own right, or
 - you could silently drop the viral content notifying neither apparent sender nor apparent intended receiver (ew, I know)
- We let users choose; see <https://password.uoregon.edu/husks>

What If We Discover New/Undetected Malware?

- Sometimes you'll come across a suspicious file (such as a .scr or a .pif file sent as an attachment) that may not trigger your antivirus product. If that happens, and you're curious what the malware may be, or you'd like to help share potential new virus samples with antivirus vendors so they can quickly update their signatures, you may want to visit:

-- <http://www.virustotal.com/>

-- <http://virusscan.jotti.org/>

- If you'd actually like to see what the executable does if run in a safe environment, you may want to see:

<http://sandbox.norman.no/>

What If I Do Get Infected?

- It would be wrong of me to end this section without touching on a particularly painful point: what should be done if someone does get infected?
- While there's a strong temptation to try just removing the virus using an antivirus product (the cyber equivalent of the patient pleading, "Can't you just give me a pill, doc?"), once a system has been compromised, no matter how good a job someone tries to do cleaning it up, you can never really trust that system again until it has been blown away and rebuilt from scratch.
- Of course, at least for many users, this may be impossible since they've never taken a backup of their files, they've lost the CDs for the software they use, they don't have time, they can't be bothered, etc.
- Consider any infestation to be a teachable moment, and stress life style changes that the user should be making...

Anti-Spyware Software

Some Malware Is Not A "Virus" **(At Least for Vendor Purposes)**

- In addition to viruses, another category of malware that you should know about is “spyware.”
- Spyware, also called “adware,” can hijack your web browser, violate your privacy, and inundate your computer with advertising. Recent estimates are that 80% of users have some form of spyware on their system; see: "Plague carriers: Most users unaware of PC infections,"
http://news.com.com/Plague+carriers+Most+users+unaware+of+PC+infections/2100-1029_3-5423306.html
- While spyware is unquestionable "unwanted stuff I didn't intend to run on my system" it may not be considered a virus for vendors purposes, and as a result, antivirus software will commonly not detect and remove spyware. Vendors are happy to sell you a separate product or products that can tackle this issue, however (for an additional fee).

The Basics of Coping With Spyware

- Make sure your staff and users have and use anti-spyware software – it is fully as important as antivirus software these days. A variety of anti-spyware packages reviews and resources are available at <http://www.firewallguide.com/spyware.htm>
- One particularly popular anti-spyware program at UO is Spybot Search & Destroy from <http://www.safer-networking.org/>
We now also site license McAfee's commercial anti-spyware product...
- Be careful when searching for anti-spyware products in Google or other search engines; some spyware has been known to be distributed by what's touted as anti-spyware products...! See the list of rogue products at http://www.spywarewarrior.com/rogue_anti-spyware.htm

Some Anti-Spyware Tips

- Coverage across products won't be perfect; use multiple products to cover the “corner cases” any single anti-spyware product may miss.
- To help avoid getting spyware, encourage users to avoid P2P applications and instant messaging applications (and the files shared via those channels). Users should also be cautioned to carefully read the fine print of the license/terms of use associated with any product they download (many times they'll actually be told about spyware that's about to be installed, IF they bother to read the license they're agreeing to).
- Speaking of reading licenses carefully, at least one particularly popular anti-spyware program, while free for home use, is NOT free for use by college/university use. Carefully check license terms for all the software you download/use/recommend to your campus community.

Messenger Spam

Ads Popping Up Directly on Your Display?

- Sometimes users think that they're infested with spyware because they're having problems with advertisements popping up directly on their display, yet anti-spyware products find nothing....
- If all you're seeing are ads popping up on your display, be sure Windows Messenger (NOT Windows Instant Messenger) is disabled; see:
 - <http://www.stopmessengerspam.com/> or
 - <http://www.grc.com/stm/shootthemessenger.htm>
- See also:
"Messenger Service window that contains an Internet advertisement appears"
support.microsoft.com/default.aspx?scid=KB;EN-US;Q330904

Regular Spam

Spam and Security

- Yet another security risk your company faces is email spam, or unsolicited commercial email. (Yes, spam **is** a security issue, not just a huge irritation.)
- To understand the relationship between viruses, hackers and spam, see the excellent discussion at “Spammers, Hackers Increasingly Feed Off Each Other,”
<http://www.techweb.com/wire/story/TWB20040212S0009>

What About Legislative Efforts?

- The Federal governments here in the US has made dealing with spam a priority, and has passed “The CAN-SPAM Act;” see <http://www.spamlaws.com/federal/index.shtml>
- 38 states have also passed state-level anti-spam laws... see <http://www.spamlaws.com/state/index.shtml>
- So far, despite all those new laws (and both private and governmental enforcement effort), spam shows no sign of abating.

So Just How Bad Is It? What Should You Do?

- If you're like many sites, ~70 to 80% of all the emails sent to your users are spam (see, for example: <http://www.postini.com/stats/> -- on 4 Nov 2005, they estimated that 69.7% of all emails they scanned were spam)
- For context, this means that for every single real piece of mail, you might see between 2 and 4 pieces of spam (note that if spam gets up to 90%, you'll be seeing 9 pieces of spam for every piece of real mail, ugh).
- Accommodating that excess unwanted traffic means that universities need to build out far more message handling capacity than they'd normally need to handle their legitimate traffic.
- Your college or university **NEEDS** to block spam if it wants to keep its email system affordable and usable.

One Approach to Blocking Spam: DNSBLs

- "DNS blacklists" repurpose the domain name system so that it can act as a database, with mail servers automatically looking hosts that are attempting to transfer email. Listed on a DNSBL that gets checked? Refuse to accept mail from that host. Not listed on any of them? Accept mail from that host.
- DNSBLs can really reduce a mail server's spam load. For example, Spamhaus believes that on average, their SBL+XBL combo list, alone, blocks about 63% of all spam that a site may receive (if anything, I think that's a low estimate).
- Here at Oregon we use (and like) the SBL+XBL (from <http://www.spamhaus.org/>), plus the NJABL open proxy DNSBL (<http://www.njabl.org/>), plus the Trend Micro (formerly MAPS) RBL+ (<http://www.trendmicro.com/en/products/nrs/rbl/>). A detailed description of how we blocked spam circa summer 2004 is available at <http://darkwing.uoregon.edu/~joe/icplspam/>

Advantages of DNSBL-Based Approaches

- Blocking takes place while the remote mail server is still attached; this means that we can reject unwanted SMTP connections and immediately return the reason to the connecting MTA; no problems with address spoofing.
- Everything either gets accepted or rejected. There is no problem with email sometimes getting through and sometimes not get through (depending on content).
- Nothing gets "foldered into oblivion" – mail either gets accepted or rejected, it doesn't get accepted but stuffed into a closet, forgotten potentially forever.
- Spammer content tweaking become irrelevant
- Blocking a single bad connection can translate to avoiding 10K+ pieces of spam; that sort of filtering scales extraordinarily well.

Blocked SMTP Connection Attempts Per Day For Selected Days on Two UO Systems

Date	Gladstone	Darkwing	Total
Sun 14 Jul 2002:	7,405	1,606	9,011
Mon 14 Oct 2002:	16,794	3,452	20,246
Wed 14 Jan 2003:	18,562	5,813	24,375
Mon 14 Apr 2003:	18,714	4,925	23,639
Mon 14 Jul 2003:	15,998	5,116	21,114
Tue 14 Oct 2003:	119,393	9,786	129,179
Thu 15 Jan 2004:	33,289	13,479	46,768
Wed 14 Apr 2004:	59,845	28,339	88,184
Sat 15 May 2004:	59,376	25,401	84,777
Mon 14 Jun 2004:	45,005	49,998	95,003
Wed 14 Jul 2004:	40,728	21,812	62,540
Sat 14 Aug 2004:	45,504	28,584	74,088
Tues 14 Sep 2004:	31,670	20,992	52,662
Thu 14 Oct 2004:	51,318	35,332	86,650
Sun 14 Nov 2004:	44,035	26,106	70,141
Tues 14 Dec 2004:	52,600	40,727	93,327

Blocked SMTP Connection Attempts Per Day For Selected Days on Two UO Systems (cont.)

Date	Gladstone	Darkwing	Total
14 Jan 2005:	47,788	26,722	74,510
14 Feb 2005:	48,579	30,443	79,022
14 Mar 2005:	47,151	37,078	84,229
14 Apr 2005:	60,495	48,315	108,810
14 May 2005:	83,826	58,867	142,693
14 Jun 2005:	85,505	72,514	158,019
14 Jul 2005:	76,288	81,713	158,001
14 Aug 2005:	84,238	111,663	195,901
14 Sep 2005:		154,925	154,925
14 Oct 2005:		187,293	187,293

Note #1: Gladstone is our student server, with 27K accounts; Darkwing is our faculty/staff server with 13.5K accounts (darkwing, gladstone and oregon.uoregon.edu were all aliased/MX'd to uoregon.edu during 2005)

Note #2: These are blocked SMTP CONNECTIONS, not blocked MESSAGES. A single SMTP connection may represent 1, 10, 100 or 1000 (or more) MESSAGES.

Note #3: Blocked connections may include viral traffic as well as spam.

Local Copies of DNSBL Files

- In general, if you use DNSBLs to block spam, you don't need to maintain local copies of them, you can just query the DNSBLs over the network.
- However, if you rely on DNSBLs for large mail servers, try to encourage your DNS administrator to run copies of the zones you rely on locally (it improves performance, immunizes you against any spammer denial of service attacks on the DNSBL name servers, and helps the DNSBL operators scale out to Internet-sized audiences better)

Supplementing DNSBLs

- In addition to DNSBLs, we also use locally maintained filter rulesets (we currently have a little over 6300 rules). Many of those rules are designed to force traffic from hosts with dynamic addresses ("DHCP addresses" or "pool addresses") through the provider's official SMTP server.
- What's the problem with dynamic address hosts? It is impossible to accumulate reputation about those dynamic addresses (one hour the host might be me, running a spam free well secured system; next hour, Uncle Charlie might have his completely 0wn3d host on that same IP address)....
- These days we'd recommend that folks consider using EnemiesList (see <http://enemieslist.com/about/features.html>) rather than building a table of the sort of rules we built manually.

Adding A Second Stage to the Filtering Process

- Spamhaus has recently begun recommending supplementation of that DNSBL filtering process with a second stage, using both traditional DNSBL's *plus* SURBLs (blacklists based on the URLs seen in the body of spams). See:
http://www.spamhaus.org/effective_filtering.html
- If you'd like to read more about SURBLs, please see Jeff Chan's site <http://www.surbl.org/>
- Doing two stage filtering requires that you run a product that can scan the body of the messages you receive. SpamAssassin 3.x is the most common tool for doing this:
<http://www.spamassassin.org/index.html>
- This also provides a nice segue to the other approach to handling spam filtering, content-based methods...

So What About Doing Content-based Spam Filtering?

- The main alternative to using DNSBLs/SURBLs is doing heuristic content-based spam filtering. The most popular server-based solution is probably SpamAssassin (<http://www.spamassassin.org/index.html>).
- A UO CC staff member, Joel Jaeggli, has done a nice job explaining how users could use Spam Assassin to control spam filtering of their email at UO; that guide is available online at:
<http://twin.uoregon.edu/~joelja/taking-email-control.html>
(note that some parts of that guide are specific to UO, including the info on how to opt-out of our default spam filtering, but that guide will at least provide you with a starting point)

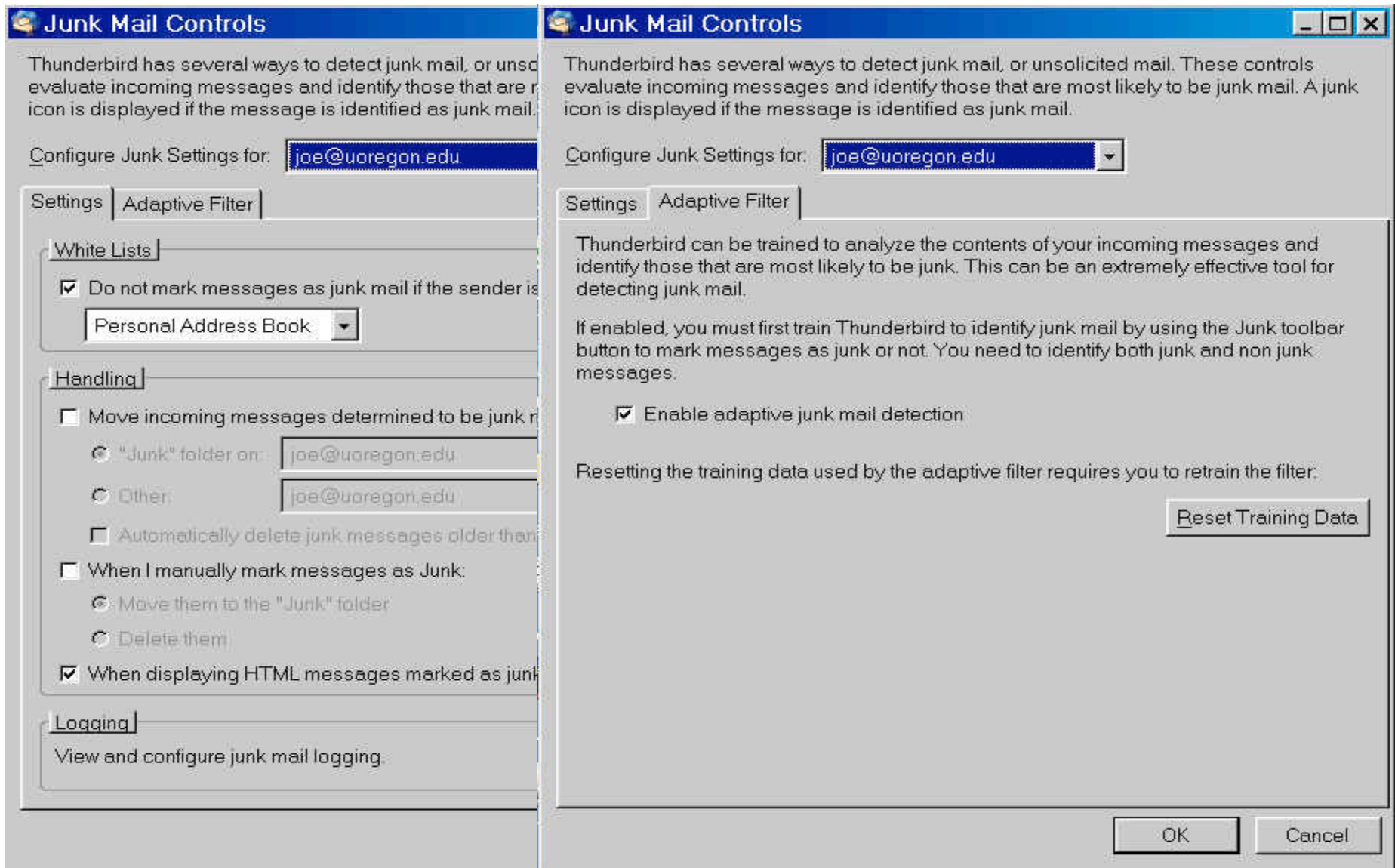
''Opting Out' of Spam Filtering? What Do You Mean?''

- Spam filtering, while now essential, will occasionally block messages that are genuinely wanted (“false positives” or “collateral damage”). In UO's case, filtering is also “on” by default. While users can opt out of the default filtering on UO’s large shared systems, at this point only 280 users out of 45,161 are currently doing so (6/10ths of 1%). We'd love to have a solution that works well for everyone, but if we can “cook” to suit the tastes of 99.4% of our users, we don't feel too bad about that...
- Few may opt out, but having the option available serves as an important “safety valve.”

Client Side Spam Filtering

- While the approaches we've just talked about all stress filtering on the server, users can also do spam filtering on their desktop workstation. Some email clients have integrated spam filtering, or users can always install and use a third party email filtering tool as an alternative.
- A nice review of client side spam filtering options is available at <http://www.pcmag.com/category2/0,1874,4795,00.asp> (sort by editor's ranking to get a reasonable ordering for the products mentioned)

Thunderbird's Built-In Spam Filtering



Firewalls

Do You Have An Institutional Firewall?

- Some of you may have a hardware firewall installed at the border of your network. Some of you may not, and if you don't, you're among friends in higher education circles – many of us do not run with a border firewall. (That's one of the things that just drives some corporate security types absolutely nuts).
- What's the basic problem with a perimeter firewall? It assumes that the stuff that's outside your firewall (e.g., the general Internet) is bad, and the stuff that's inside your firewall (your faculty, students and staff) is good. That's not always true. You may have compromised systems *inside* your firewall, on your campus network, or disgruntled employees, or simply just open network jacks. On the other hand, if there is a firewall in place, it may interfere with legitimate network traffic such as video conferencing, voice over IP traffic, negotiation of max MTUs, etc., unless carefully configured

Subnet Firewalls As An Alternative

- In some cases, rather than a perimeter firewall, or in addition to a perimeter firewall, a site may also run firewalls between key subnets and the rest of campus. An example of this is often the subnet that connects sensitive administrative systems – a firewall in front of those systems correctly recognizes that there's no particular reason why students in university housing, or academic faculty members, say, should be included within the trust perimeter for administrative systems that they may never directly use.
- The problem with subnet firewalls? Each subnet firewall may have different rulesets, and each subnet firewall needs to be maintained and supported. As subnet firewalls proliferate, debugging issues associated with wanted traffic getting blocked also proliferate.

What About Desktop Firewalls?

- You should be looking at per-workstation software firewall products (or inexpensive personal hardware firewalls, such as those from Linksys), in addition to subnet firewalls or your border firewall, much as you should be currently deploying anti-virus software on each desktop.
- Desktop hardware firewalls (also known as "broadband routers") are routine practice on residential broadband networks; the rest of us need to catch up.

Desktop Hardware Firewall Notes

- Hardware firewalls can be potentially be installed “backwards,” in which case they typically act as a rogue DHCP server, handing out RFC1918 addresses to everyone on their subnet. This tends to make support people grumpy.
- Some hardware firewalls may come bundled with wireless access points (which have their own security issues)
- Some hardware firewalls may include a multiport switch on the "inside" side – don't use it. One system should be protected per personal firewall device.
- Some hardware firewalls may end up using uPnP if carelessly configured: <http://cc.uoregon.edu/cnews/spring2003/upnp.html>
Speaking of uPnP, one easy way to disable uPnP is available at <http://www.grc.com/unpnp/unpnp.htm>
- Reviews of desktop hardware firewalls? See: <http://grc.com/lt/hardware.htm>

ICF and Other Software Firewalls

- Windows XP SP2 now ships with Microsoft's integrated Windows Internet Connection Firewall (ICF) "on" by default. This will make a huge difference for your Windows XP users.
- ICF is not without limitations, however, most notably the fact that it does NOT block outgoing traffic sourced by the workstation itself.
- If you'd like a software firewall that DOES block outgoing traffic, you may want to check out Zone Alarm from Zonelabs (<http://www.zonelabs.com/>). Note that while there is a free version of ZoneAlarm available to individuals and non-profit institutions, government and educational institutions need to purchase a license to use this product.
- Nice outward-traffic-oriented review of software firewalls at <http://grc.com/lt/scoreboard.htm>

Some Notes About Software Firewalls

- Novice users can easily become confused when it comes to making decisions for software firewalls about what traffic to accept or to block: "The Frazzleblat TCP/IP Helper Service Would Like to Connect to the Internet. Allow?" If the user makes the wrong choice, and blocks a service that a legitimate application needs, things may break in very hard to diagnose ways; on the other hand, if they "open the door for anyone," there's not much point to giving them the choice to block at least some stuff.
- Some antivirus or antispyware products may include blocking of unexpected or characteristically hostile traffic (e.g., McAfee blocks port 25 traffic from spam zombies, and IRC traffic by default)
- Be sure to include the cost of periodic product updates when thinking about the cost of software firewall products.

An Unexpected Consequence of Deploying Hardware or Software Desktop Firewalls

- There is one unexpected consequence of deploying desktop firewalls that you should be aware of: once you deploy a desktop firewall, particularly if you deploy a software firewall product, you and your users will be amazed by just how often your systems are getting probed. The level of ongoing “background radiation” associated with hacker/crackers activity can be fairly shocking.
- This can be both good and bad: it can raise the level of support for security-related projects, but it can also make users paranoid (potentially, in the worst of cases, leading to the so-called "Goobar With Firewall" hyper-reporting problem).
- If users would like to contribute firewall log data, there are a number of projects that will happily accept that data; see: <http://www.mynetwatchman.com/> and <http://www.dshield.org/>

Passwords

Passwords Are Still The Key to the Realm

- Once you know how often hacker/crackers are “poking” at your systems, the importance of strong system access controls becomes much more understandable, although most universities still rely on conventional/traditional usernames and passwords (rather than hardware crypto tokens or other advanced authentication solutions).
- That's amazing when you realize just how bad passwords are as an authentication method. Passwords are subject to:
 - eavesdropping (sniffing network traffic, videotaping your keystrokes)
 - guessing (many users are stunningly unimaginative)
 - brute force/exhaustive attacks
 - being voluntarily shared with others
 - being forgotten
 - never being changed...

And Regular Passwords Really Aren't “Free”

- Gartner estimates that up to 30% of calls to a typical helpdesk are password related (personally, I think that's probably a low estimate) (<http://www.nwc.com/1317/1317f13.html>)
- Estimates for the cost/call vary widely, but let's hypothetically assume you use comparatively inexpensive student employees, and peg that cost at \$5/call (it is probably far higher when you think about the lost productivity of the employee with the password problem).
- How often do YOUR users forget/need to have their passwords reset?

More Password Issues

- How many do you currently have? Think about your email account, your workstation's password, your ATM card PIN, your long distance authorization code, your username and password for Amazon, eBay, the NY Times, etc., etc., etc.
- Do you make them all the same? If so, if any of those systems get cracked, then people can access all those accounts. (And what do you do when you have to change one of them to something new? Will you change all the others, too?)
- Do you write them all down? I hope no one steals your password crib sheet... and I hope you have that crib sheet with you when you need it.
- Do you pick hard passwords? If not, with modern cracking technology, it's trivially easy to break most passwords, particularly if you never force users to change their passwords.
- What's YOUR password expiration/forced change policy?

More Password Issues (cont.)

- How do you handle initial password distribution?
- How do you handle password resets? A wonderfully strong password policy that is "guarded" by a trivially easy password reset policy is worthless
- What about account creation and removal? WHEN do accounts get created for new students, for example? How do the accounts of faculty members who leave the university for another position get removed? What about faculty, staff or students who die? (Beware rare events – systems often fail to correctly anticipate and handle unusual phenomena)
- What are your policies for administrative disclosure of passwords to supervisors or institutional management?
- You and your university really should be looking at replacing regular passwords with two factor authentication methods.

"What Do You Mean By 'Two Factor' Authentication?"

- Two factor authentication ==> something you have, plus something you know.
- Classic financial industry example: ATM card plus a PIN.
- In the online world, the traditional example is a hardware token (e.g., keychain fob that generates a periodically changing unguessable number) plus a password.
- Generally, you enter your username and password, and then get prompted to enter the magic number that's currently displayed on the hardware token. (Some systems supply a number, you enter the number into the magic calculator-like hardware device you have, it grinds on that number, and then magically returns a corresponding "response" value which you enter via your computer's keyboard)

Even AOL is Doing Two Factor These Days

RSA Security - Press Release - America Online and RSA Security Launch AOL PassCode Premium Service

File Edit View Go Bookmarks Tools Help

http://www.rsasecurity.com/press_release.asp?doc_id=5033&id=1034

SERVICES

PARTNERS

LEADERSHIP

NEWS & EVENTS

- Press Releases
- RSA Security In the News
- Web Seminars
- Events
- Customer Success Stories
- Awards
- Corporate Press Kit

America Online and RSA Security Launch AOL PassCode Premium Service

AOL Is First Online Service to Offer Optional State-of-the-Art Two-Factor Authentication to Consumers

Keychain-Sized Device Provides Second Level of Account Protection Through Automatically-Generated Supplemental Password


Dulles, VA and Bedford, MA, Tuesday, September 21, 2004 —

America Online, Inc., the world's leading interactive services company, and RSA Security Inc. (NASDAQ: RSAS), a leading provider of solutions that secure and manage online identities, today announced the launch of AOL PassCode, a new premium service that offers members a second level of AOL account protection through the use of a keychain-sized device that generates and displays a unique six-digit numeric code every 60 seconds.

Related Solution

By delivering the strongest online consumer security possible, companies can increase customer loyalty.

[Consumer Identity Protection](#)



AOL PassCode is a new premium service for AOL members.

"AOL PassCode is like adding a deadbolt to your AOL account by automatically creating a new secondary password every 60 seconds," said Ned Brody, AOL's Senior Vice President for Premium Services. "Many of our members use their accounts for business purposes, financial transactions or other sensitive activities. AOL Passcode offers a higher standard of protection through the same state-of-the-art two-factor authentication system used by many financial institutions, technology companies, and other major businesses. We're proud to be the first online service to offer this extraordinary supplementary level of security protection to our users."

So Is E*Trade

E*TRADE FINANCIAL - Home - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://us.etrade.com/e/t/microsite/custsecurity?SC=NPNL67G&traxui=F_HV

OPEN AN ACCOUNT

Complete Security Protection, unauthorized access to your account is virtually impossible.

3.

1. Model New Cash Allocations 2. View Results & Suggested Action 3. Complete Security Protection

COMPLETE SECURITY PROTECTION

- We utilize 128-bit encryption, the highest level of web site security available
- Individual RSA SecurID - An optional keychain-sized token which displays a unique 6-digit number that changes every 60 seconds²
- SmartAlerts - configure to inform you of your account activity
- Security specialists monitor your account for unusual activity

Trading
5 star quality
100% satisfaction

Exclusive, Free,¹ Easy & Optional for E*TRADE Customers

Investing
Open your 2004 tax-qualified IRA
No fees, no minimum

Banking
Get higher yields on CDs
Free E*TRADE Bank

Markets

User ID: Password: Start In: Account

Secured by **RSA**

¹ The Digital Security ID will be provided at no cost to Power E*TRADE and Priority E*TRADE customers. A \$25 charge may be imposed for each additional or replacement Digital Security ID. E*TRADE FINANCIAL at its sole discretion may impose a fee for this service in the future or may discontinue the service.

² RSA, RSA logo and SecurID are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. RSA Security Inc. is not affiliated with E*TRADE FINANCIAL Corp. or any of its affiliates and is not a sponsor

A Comparatively Low-Tech Two Factor Approach

Two Factor Authentication - Entrust IdentityGuard for Strong User Authentication

File Edit View Go Bookmarks Tools Help

<http://www.entrust.com/identityguard/index.htm>

With Entrust IdentityGuard, users continue to employ their current user name and password, but are also provided with a second physical form of authentication based on an assortment of characters in a row/column format printed on a card. A user must successfully complete a coordinate challenge to demonstrate that they are in possession of the appropriate card:

Welcome to Any Bank

User Name:

Password:

IdentityGuard: **A2 C4 F3**

ANY BANK **Entrust**

	A	B	C	D	E	F	G	H	I	J
1	7	9	3	5	5	4	9			
2	9	2	3	6	8	4	1	3		
3	4	6	1	4	8	2	8	0	7	
4	5	2	4	8	5	0	1	7	2	
5	6	8	6	8	1	7	4	0	8	0

Serial #1234567

Downsides to Hardware Token Approaches

- Tokens aren't cheap (particularly if you need to issue them to 20,000 students)
- If you forget your token, you won't be logging on until you go home and get it.
- No more convenient (albeit insecure) saved passwords.
- Generally, it is one token per account or service, with no cross-service coordination. If you have ten different accounts secured by hardware tokens, you'll end up with quite a pocketful of little tokens to carry around with you all the time.
- While you may see hardware tokens actually used as key fobs, I don't recommend doing so. The human pocket is an incredibly nasty environment, full of sharp metal objects, with contents subject to sweat and spilled liquids, prone to being bumped and crunched, etc.

What About "Something You Are" -- Biometrics?

- One thing you always "have" with you is "you" – that is, your thumbprint, your iris, your facial features, your voice, etc. Some have proposed using unique biometric features as a way of reducing problems with insecure passwords, while avoiding the cost and inconvenience of multiple crypto tokens.
- Unfortunately, biometric methods face several challenges:
 - when we try biometric methods, we end up substituting the cost of the biometric reader for the cost of the crypto token (you can enter the value from a crypto token from any keyboard, but you can only scan your thumbprint if the system you're using has a thumbprint reader attached)
 - some biometric readers may not always correctly identify legitimate users (frustrating to be locked out!)
 - some biometric readers may falsely permit access by illegitimate users (classic: breathe on reader to raise old print)

Encryption

Protection of Passwords

- Assuming we're stuck with passwords, at least for now, what should we be doing to make the best of a bad business?
- One of the most acute threats to password based authentication is “sniffing” (eavesdropping on passwords while they’re transmitted over your local network or the Internet).
- Has you taken steps to replace plain text services with their encrypted analogs? UO now has, both for interactive logins (“telnet”) and for POP/IMAP email access, and for passwords transmitted via the web. After we changed, the services basically worked the same from the user’s perspective, but now the passwords used in conjunction with those services are resistant to eavesdropping attacks...
- Let's start with the easiest one first: secure web pages.

Secure Web Pages

- If you've purchased anything from an online merchant with a credit card, you've used a secure web site. Secure web sites normally will show https: (instead of http:) in the browser address bar, and a secure padlock icon in the bottom browser bar.
- In the case of college or university web pages, obviously you want any page that collects financially sensitive information (like credit card numbers) to be secure, but you also want to make sure that any page that requires a password to login is secure, including things like web email interfaces, teaching and learning systems, portals, etc.

telnet (and rlogin) ==> ssh

- If you're an old timer, you may be familiar with logging in with telnet (or rlogin) to the % shell prompt on a Unix system, or logging in to OpenVMS's \$ prompt, etc.
- If you're **still** using telnet to do that sort of thing, stop at once, and replace that access with secure shell (ssh).
- Open SSH is available from <http://www.openssh.com/>
- SSH Communication Security (the commercial company) is at <http://www.ssh.com/>

Secure POP and Secure IMAP

- POP and IMAP email access protocols are another example of when plain text passwords may be getting transmitted over the wire, sometimes every couple of minutes (depending on how users configure their systems to check for new mail).
- These days, virtually all email servers and virtually all email clients support secure POP and/or secure IMAP, services which work just like regular POP or regular IMAP, except they're encrypted.
- You can see the POP and IMAP clients which support secure POP or secure IMAP (or at least the ones that we document for our users) at <http://micro.uoregon.edu/email/index.html>

POP Consolidation

- Some users may have email accounts other than the one your schools provides for them. Rather than check multiple accounts separate, many times users will either forward all their accounts to a preferred account, or use "pop consolidation" to pull all the mail from a variety of accounts together into a single preferred account.
- Traditional forwarding has a number of downsides (see the scenario described in "The Impending End of Traditional Dot Forward-Style Forwarding," http://www.campus-technology.com/news_article.asp?id=10313&typeid=153) but POP consolidation is even worse, typically requiring you to save each of your usernames and passwords on the remote system that is consolidating mail from all your various POP accounts (ugh!). Just say no! Don't do it!

Roaming Users and Outbound Email (SMTP) Access

- Another place where usernames and passwords can pop up is in conjunction with outbound email ("SMTP traffic").
- While historically it has been possible to simply hand a mail message to a mail server for delivery with no access control, spammers have abused that permissive model, and as a result most mail servers now only accept outbound message traffic originated by their own customers.
- For local users, that customer relationship is usually inferred from the IP address of the connecting customer host (coming from my network, must be my customer).
- Where things get tricky is when users are roaming, but don't want to change their outgoing mail server, or when providers outsource dialup or wireless access. In those circumstances, username and password auth is usually required. If a password is required make sure that SMTP submit traffic is encrypted! ¹⁰⁸

What About FTP?

- Just as there's an encrypted client that replaces plain text telnet and plain text POP/IMAP, there's also an encrypted file transfer client called scp ("secure cp" or "secure copy").
- ftp and scp differs from some of the other protocols, however, in a couple of ways:
 - scp generally requires ssh version 2; most ssh clients are now ssh version 2, but some may still be version 1
 - ftp is built into a LARGE number of applications such as web page design software; scp support is often missing, and users REALLY like to be able to easily publish their web pages

Secure Versions of Other Network Services

- In addition to ssh, pops and imaps, and scp, virtually any other service can be "tunneled" over ssh
- Tunneling often seems to baffle users, but in a nutshell:
 - the user creates an encrypted session to the remote host using ssh, just as they normally would
 - BUT, at the same time, they indicate that they'd also like to create a companion encrypted tunnel that transports some unencrypted network service from its normal port on the remote host to an port on the local workstation
 - the user then connects to the tunneled port on the local workstation, with the traffic being transparently hauled in encrypted form back to the other end of that tunnel; because the unencrypted contents exchanged over that local connection never touches the network, that traffic's safe.

VPN

- If tunneling as a concept makes your head hurt, you may want to consider using a VPN (virtual private network) connection instead, assuming your college or university offers it.
- In a nutshell, you install VPN software on your laptop, then when you run the VPN software it creates an encrypted tunnel between your workstation, wherever it may be, and the VPN tunnel concentrator (e.g., VPN appliance) back on your campus network.
- Because you login to the VPN with a username and password (or other credentials) and because you'll receive a university IP address, you'll automatically have access to "university community only" resources, including controlled access databases, and things like outgoing mail (SMTP) servers and Usenet News servers, just as if you were working from on campus.

VPN Considerations

- As often configured, all traffic goes back to the campus VPN concentrator. This can be a bummer if you want to talk to local network printers, for example.
- VPNs do not provide end to end encryption; traffic is only encrypted from the user's workstation to the VPN concentrator. (see the illustrations at <http://cc.uoregon.edu/cnews/spring2002/vpn.html>)
- You need to have the VPN software installed on your local system (this can be a pain if you forget to do it before travelling and access to the VPN software is controlled). Browser-based VPNs may minimize this issue.
- Due to encryption and decryption overhead, VPN throughput can be lower than non-VPN'd traffic.
- Some VPNs support PCs only (the Cisco 3000 UO uses also works fine for Macs)

Whole Disk On-The-Fly Encryption (E.G., For Laptops)

- Concern about unauthorized disclosure of personally identifiable information has made whole disk on-the-fly encryption of increasing interest, particularly for laptops. With that sort of encryption, if a laptop is lost, even if the hard drive is pulled from the system and accessed directly, the contents should not be compromised.
- Some operating systems support that sort of thing natively, e.g., Mac OS X offers "FileVault" (see: <http://www.apple.com/macosx/features/filevault/>), but you can also purchase commercial products for Microsoft Windows, see http://www.pgp.com/products/wholediskencryption/pgp_whole_disk_professionals.html
- **Caution:** if you lose your password(s), you'll be SOL, so be careful.

File At A Time Encryption

- If you just need to encrypt or digital sign files one file at a time, check out:

<http://www.gnupg.org/>

and the front end that's available for that product for Thunderbird:

<http://enigmail.mozdev.org/>

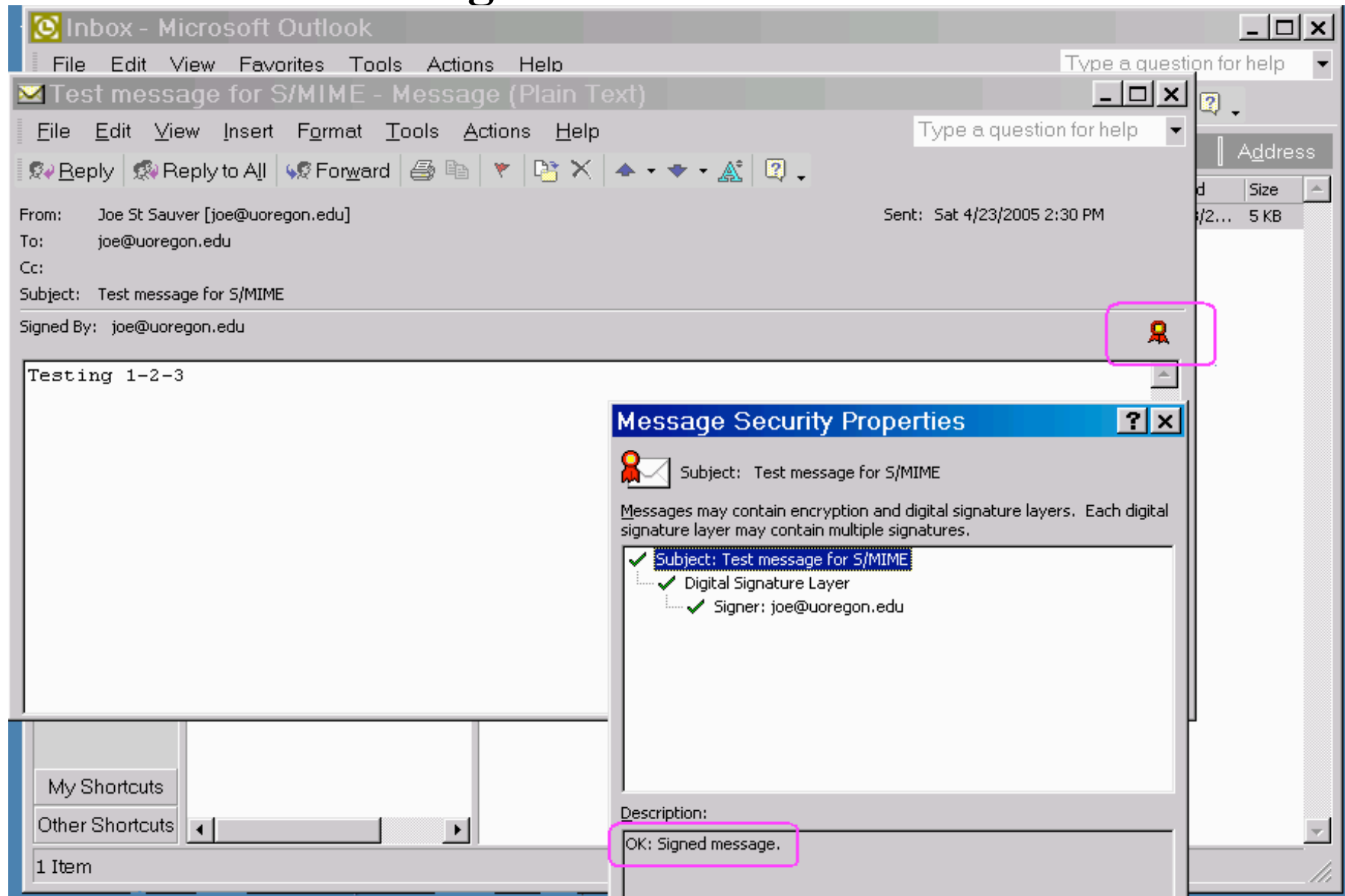
Digital Signing Is NOT Message Encryption

- Sometimes there's confusion about the difference between digitally signed mail and encrypted mail.
- Mail that's been digitally signed can be read by anyone, without doing any sort of cryptography on the message. Yes, there will be additional (literally cryptic!) "stuff" delivered as part of the message (namely, the digital signature), but the underlying message will still be readable by anyone who gets the message whether the signature gets verified or not.
- Mail that's been encrypted, on the other hand, can ONLY be read after it has been decrypted using a secret key.
- The vast majority of "push" communications from a university to its students need NOT need be encrypted, but ALL official university email should be digitally signed.

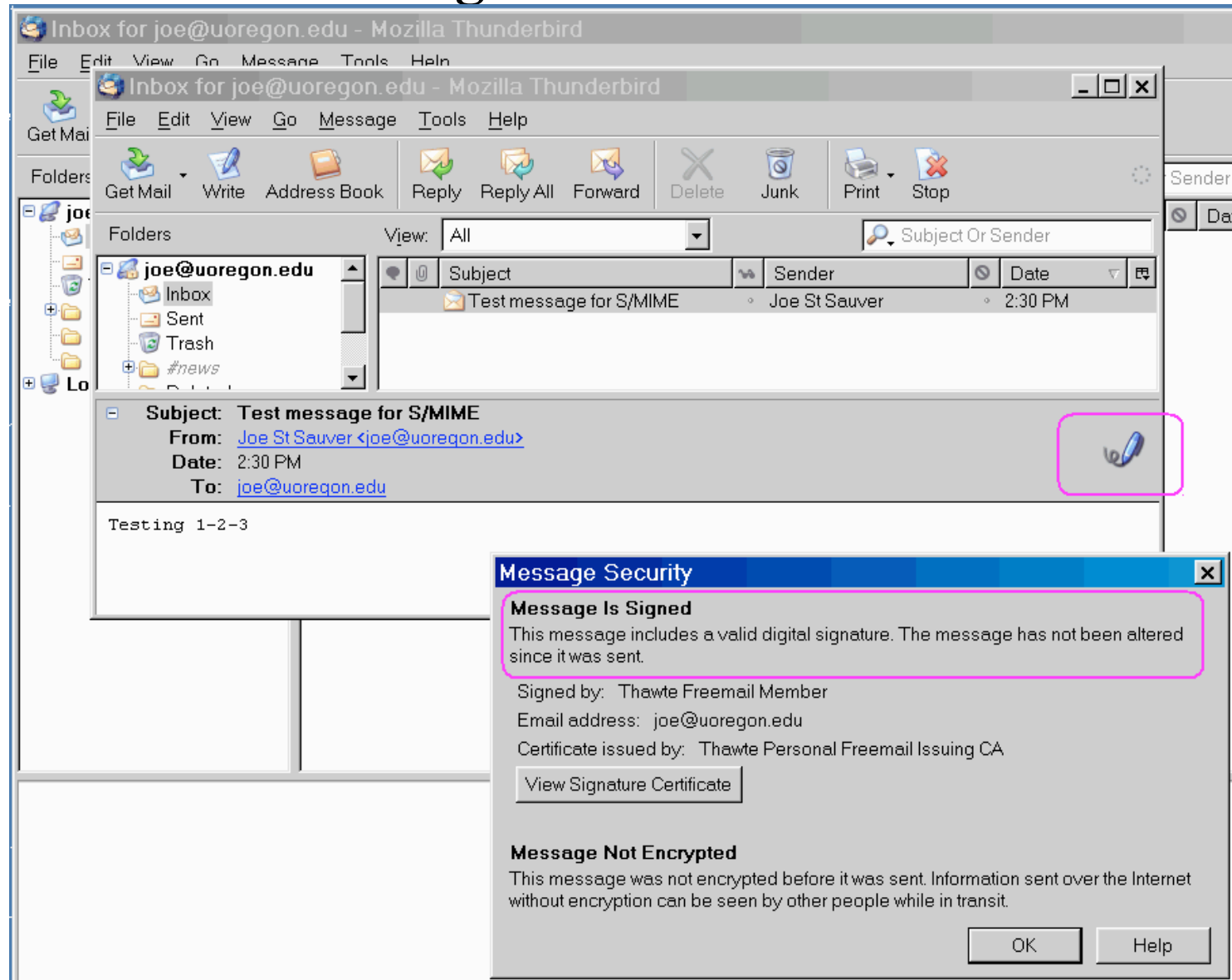
Will Students Even *Know* or CARE What a Digital Signature Is?

- We know/agree that many students won't have the slightest idea what a digitally signed message is (at least right now).
- Over time, however, more users WILL begin to expect to see important messages signed, including messages from their schools, just as consumers now routinely expect to see e-commerce web sites use SSL to secure online purchases.
- Think of digital signatures for email as being the email equivalent of the "little padlock" icon on secure web sites
- For example, if you receive an S/MIME signed email in Outlook or Thunderbird today, it automatically "does the right thing"... here's what that would look like...

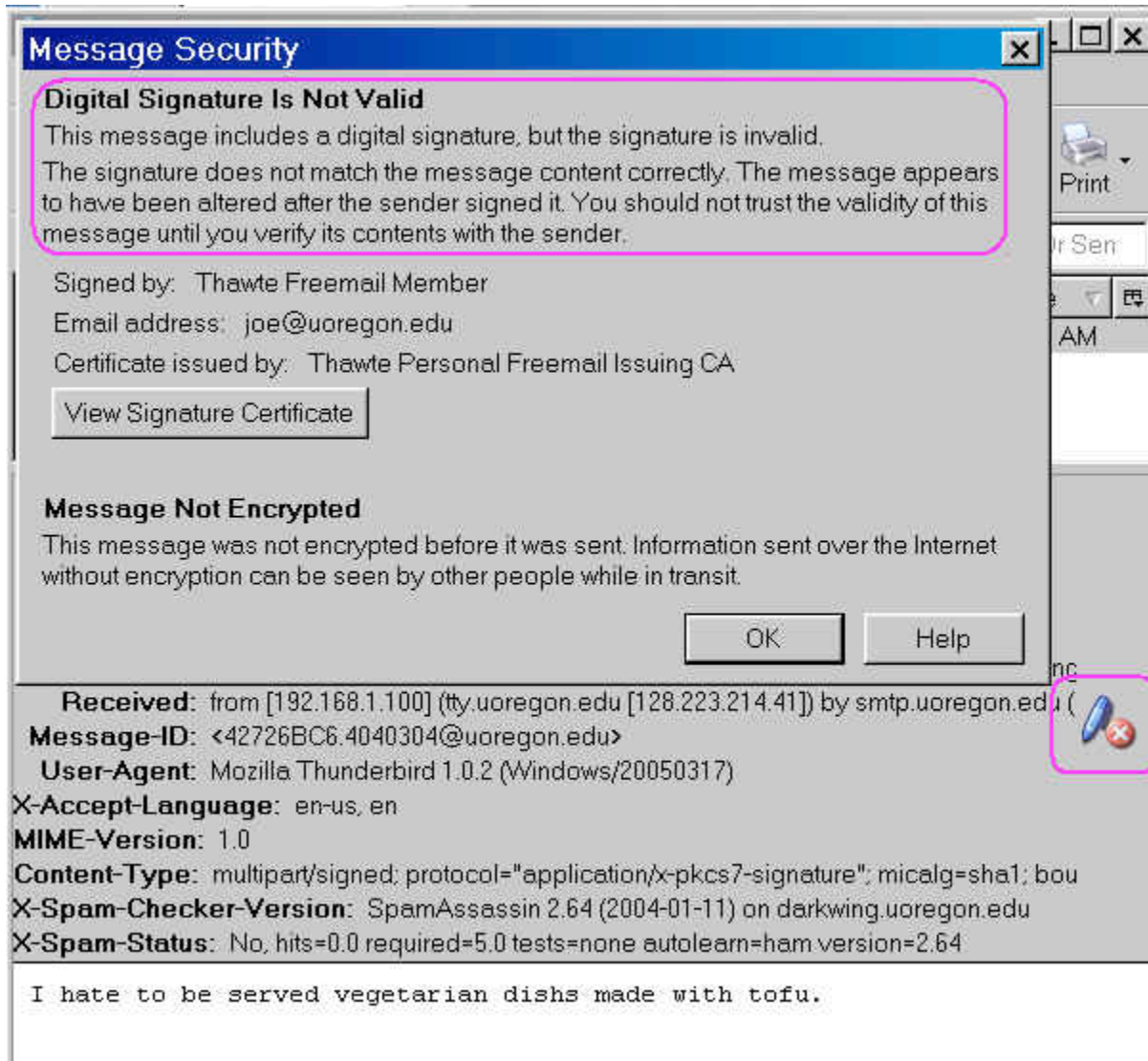
An S/MIME Signed Message in Microsoft Outlook



An S/MIME Digitally Signed Message In Thunderbird



What Do Users See When A Signed Message Has Been Tampered With?



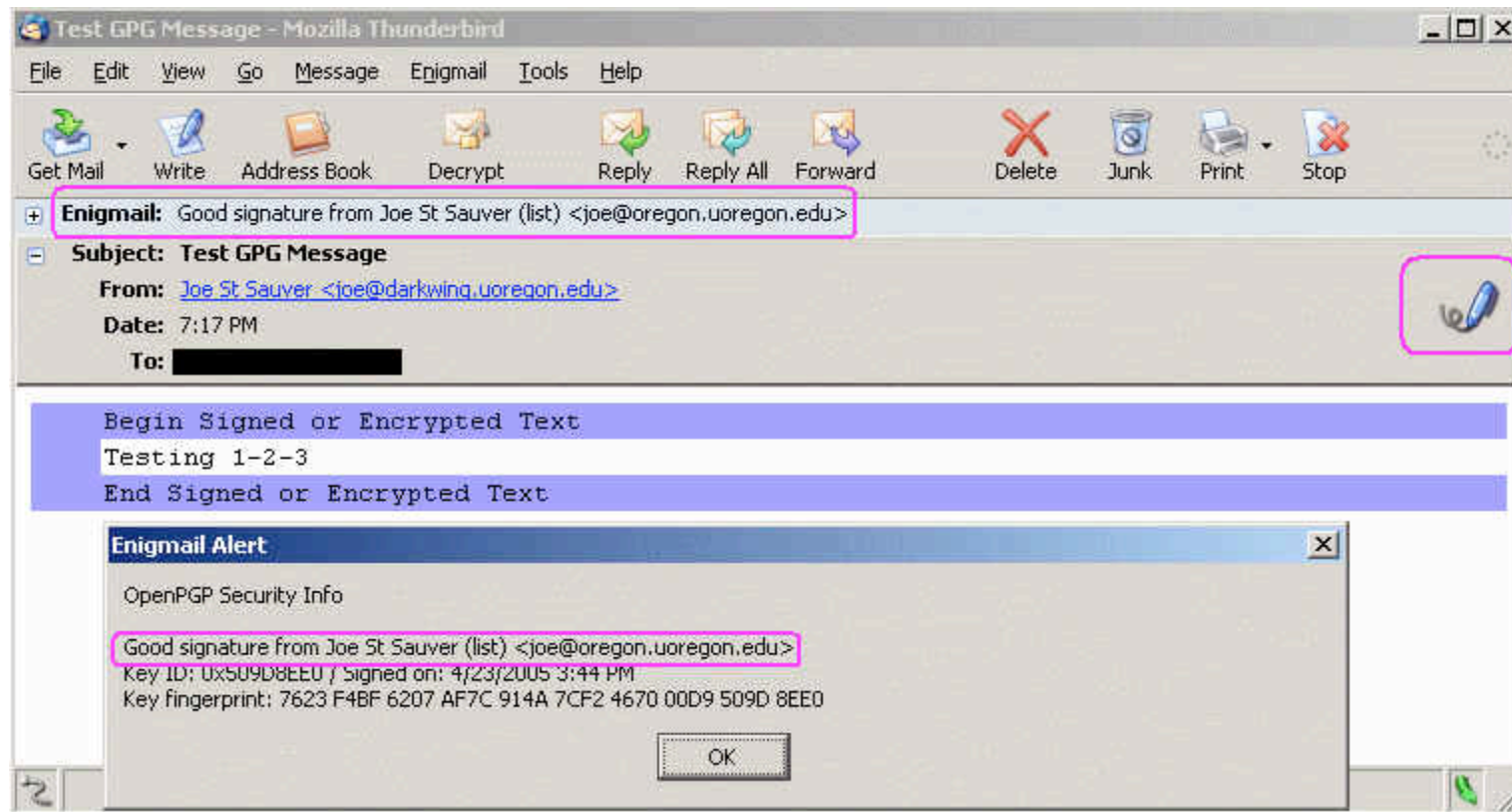
Trying S/MIME Yourself

- If you'd like to experiment with S/MIME signing, you need a certificate. You can obtain a free personal email certificate from:
 - Thawte (Verisign, Mountain View, CA, USA):
<http://www.thawte.com/email/>
 - Comodo (Yorkshire, UK):
<http://www.instantssl.com/ssl-certificate-products/free-email-certificate.html>
 - ipsCA (Madrid, Spain):
<http://certs.ipsca.com/Products/SMIME.asp>

Those Examples Were Using S/MIME, But You Could Also Use PGP

- PGP (and its free analog Gnu Privacy Guard) can also be used to digitally sign emails.
- PGP/GPG is quite popular with technical audiences, and rather than using a hierarchical certificate authority-focused model, PGP/GPG users share their public keys via Internet-connected PGP/GPG key servers.
- The trustworthiness of any freely available individual public key on one of those key servers is recursively a function of the trustworthiness of the keys (if any) that have cryptographically signed the key of interest. This is known as the PGP/GPG "web of trust."
- Alternatively, if you have direct contact with a PGP/GPG user, they may simply confirm the fingerprint of their public key to you person-to-person..

Example of a GPG Signed Message Being Read in Thunderbird with Enigmail



- It may be worth noting that the disconnect between the message "From:" address and the address in the PGP signature of the payload did not cause any alerts/issues.

Choice of Application Clients

Just As Choice of O/S Matters, So Can Your Choice of Network Applications

- Back near the start of this talk, we mentioned the fact that PCs running Windows get targeted a lot more than Macs or other non-Windows workstations.
- I'd be remiss if I failed to mention that similar targeting occurs at the application layer, too.
- You can minimize the risks you face running under Windows through things as simple as the applications you chose to use to surf the web or read your email (and it **is** possible to work from a Windows-based desktop in a virtually completely secure way when it comes to network applications, e.g., see: "Safe Network Computing: Windows Desktop" at <http://www.columbia.edu/kermit/safe.html>)
- But what does Secunia.com tell us about more traditional options?

Web Browser Choice

- See <http://www.sans.org/top20/#w6> and the recommendations in <http://www.kb.cert.org/vuls/id/713878>
- **Microsoft Internet Explorer 6.x:**
(<http://secunia.com/product/11/>) with all vendor patches installed and all vendor workarounds applied: 20 out of 86 Secunia advisories is listed as "unpatched"; one or more vulnerabilities is rated "**Highly critical**"
- **Mozilla Firefox 1.x (<http://secunia.com/product/4227/>):**
with all vendor patches installed and all vendor workarounds applied: 3 out of 25 Secunia advisories is listed as "unpatched;" highest vulnerability rating is "**Less critical**"
- **Opera 8.x (<http://secunia.com/product/4932/>):**
0 of 8 unpatched vulnerabilities
- **Note:** plugins browser helper applications, and browser configuration options also matter (no scripting/Active-X!)

While We're On The Topic of Browsers, What About Anti-Phishing Toolbars?

- While some people really like browser anti-phishing toolbars, others have presented examples of phishing attacks where they haven't worked so hot, e.g., see:
"Phishing Toolbars – The One That Works,"
http://loosewire.typepad.com/blog/2005/04/phishing_toolba.html and the followup day's piece,
"The Antiphishing Toolbars That Didn't,"
http://loosewire.typepad.com/blog/2005/04/the_antiphishin.html
- Some browser anti-phishing toolbars work with IE only
- Some anti-phishing toolbars may include advertising or collect statistics or do other things besides just working to combat phishing (maybe that's a problem for you, maybe not).

Mail Reader Choice

- **Outlook 2003 (<http://secunia.com/product/3292/>):**
with all vendor patches installed and all vendor workarounds applied, 1 of 7 Secunia advisories is marked unpatched,
highest vulnerability: **moderately critical**
- **Outlook Express 6 (<http://secunia.com/product/102/>):**
with all vendor patches installed and all vendor workarounds applied, 6 of 20 Secunia advisories is marked unpatched,
highest vulnerability: **moderately critical**
- **Thunderbird 1.x (<http://secunia.com/product/4652/>):**
with all vendor patches installed and all vendor workarounds applied, 1 of 7 Secunia advisories is marked unpatched,
highest vulnerability: **not critical**
- Don't forget non-graphical mail clients, such as Pine
- We also have a new open source caching web email interface: <http://www.uoregon.edu/~tkay/alphamail.html>

Mail-Related Behaviors

- How you use mail can also have a material impact on your risk exposure. Just to mention a few examples...
- Do you routinely send and receive attachments or formatted mail? Avoid doing so, and just use plain text email instead.
- Do you use third party email accounts, as well as your institutional email account? Do you know the virus filtering practices are of that third party email account provider?
- Do you report all spam? <http://www.spamcop.net> is one easy way
- Do you view mail "from your bank" or "from PayPal" or "from Miriam Abacha" with complete skepticism? You should! Trust NONE of 'em – they're all scammers or phishers. It is trivially easy to forge email to appear as if it is coming from whomever you want it to appear to be from (check the full headers! For info on how to do so, see <http://micro.uoregon.edu/fullheaders>)

Office Productivity Application Suite Choice

- **Microsoft Office 2003 Professional Edition**
(<http://secunia.com/product/2276/>): 2 out of 10 Secunia advisories marked as "unpatched," highest vulnerability is **"highly critical"**
- **OpenOffice 1.1.x** (<http://secunia.com/product/302/>): 0 of 4 Secunia advisories is marked as "unpatched"
- **Note:** I'm not currently seeing Secunia data for WordPerfect from Corel...

Other Security-Relevant Network Applications

- In general, we strongly encourage you to avoid peer to peer file sharing applications; if you'd like access to a wide range of music files, consider the now-legal/commercial Napster, iTunes, or a similar service. (You may be interested in my thoughts on renting vs. buying music online, see: <http://cc.uoregon.edu/cnews/summer2004/buyrent.htm>)
- Other particularly risky applications are IRC and instant messaging applications. If at all possible, we suggest you rely on email instead.
- I tend to be a big fan of Usenet News, at least if you read it using a command line news reader such as trn (if you use a command line client, you will quickly find viral content in Usenet News, particularly in the various binary newsgroups)

Desktop Security Potpourri

System Integrity

- One often overlooked area is verification of system integrity/detection of unauthorized changes to key system files.
- A nice discussion of some “tripwire” type products is available at: <http://cc.uoregon.edu/cnews/fall2003/sysintegrity.html>
- If you find files have been changed w/o authorization, I suspect you will suddenly be interested in...

Backups

- Modern data storage methods (storage area networks/network attached storage (SANs/NAS)) can help improve the survivability of your data by automatically mirroring it across multiple locations, and by giving you access to snapshots (see: <http://cc.uoregon.edu/cnews/summer2005/snapshots.htm>)
- Don't have a SAN or NAS at your disposal (or even if you do)? You still need to take backups.
- Backups, particular failure to backup data on desktop systems remains a major problem at many sites. Most users simply don't bother backing up their desktop systems! Do your users? Are you sure?

Some Backup Suggestions

- “Hard Drives: Bigger, Faster, Cheaper -- and Less Reliable”
<http://cc.uoregon.edu/cnews/winter2004/hdrives.html>
- Be sure backups are actually usable! When you need ‘em is not the time to find out there’s been a systematic problem for “some time!”
- Keep as many versions as you can afford
- Keep at least some backups off site.
- Guard backups the way you would original online media (e.g., watch privacy issues)

Other Topics?

- Assuming we still have time, are there other security topics you might like to talk about? Some possibilities:
 - Wireless security?
 - Botnets?
 - Distributed Denial of Service (DDoS) attacks?
 - VoIP security issues?
 - Physical security?
 - Background checks?
 - DMCA issues?
 - CALEA?
 - Bandwidth managers (such as Packeteer Packetshapers?)
 - IPv6 security?
 - IP multicast security?
 - Security policies?
 - Incident handling?
 - Online security resources?

Conclusion

- Thanks for the chance to talk today!