The Desktop Security Committee of the I.T. Security Task Force Response to Charge

Report to the Security Task Force
December 30, 2004

Committee Chair

Marc DeBonis	MS Implementation Group

Committee Members

Roger Anderson	University Computing Support
Kevin Davis	University Computing Support
Doug Edmonds	Systems Engineering & Administration
Siegfried Hill	AIS Alumni Development
Ted Leinhardt	Systems Engineering & Administration
Dave Martin	Systems Engineering & Administration
Mike Moyer	Systems Engineering & Administration
Brian Rectanus	Database Management Systems
Tommy Regan	Information and Learning Systems
Judy Watson	University Computing Support

Executive Summary

The committee was assigned three questions regarding securing desktop computer systems.

1. How are we currently securing desktop systems (considering the possibility of users running Windows, Macintosh, or Linux-derivative operating systems)?
2. How is desktop system security being compromised?
3. How can we reduce, eliminate, or remediate these security compromises?

In addition to providing detailed answers to these questions, the committee has developed a position paper which attempts to identify and answer questions critical to computing security.

We have defined 11 remediation factors that capture the critical security issues to which modern desktop systems are vulnerable. Each remediation factor has three priority levels - High, Medium, and Low - with recommended security initiatives that will eliminate or mollify these security risks. Of the 31 initiatives identified, the top five initiatives are:

1. Develop Network Intrusion Detection Systems (NIDS) and Host-based Intrusion Detection Systems (HIDS) internally and externally to Virginia Tech's IP space. Based on metrics garnered from these systems, proactively packet shape or deactivate network portals of systems that are potentially compromised.
2. Expand walk-in support to provide the next level after support cutoff; a clinic to perform recovery, repair, reinstall, and securing of OS. This will be a required "class" during which the person would have to stay in attendance, provide the software, and perform the work with guidance from qualified staff. Create a support tier structure through which students/staff can become "gold" support that will give a person stream-lined support if they are listed as having completed the training.
3. Develop a "recipe" for all VT systems so that administration knows what services, protocols, and ports are required to successfully access them. Require VT system developers and implementers to keep this "recipe" up to date. This will help to correctly firewall workstations based on what systems they need to access.
4. Require by policy that all university-owned systems have a primary administrator who is specifically paid to maintain the system. Do not assume the primary user of the system will also correctly administrate it.
5. Require management to empower the "IT Person" to enforce reasonable security policies including patches/upgrades, password configuration, access rights/privileges, file system permissions, etc. on all users.

To improve desktop systems at VT, a systemic process must provide three elements:

Empowerment - The software, education, and support structure to allow localized management of desktop systems and security

Choice - Centralized infrastructure to provide desktop resources to those who do not have the time, money, or staff to correctly manage their own desktop systems and services

Incentive - Processes in place to proactively identify, restrict, and remediate systems with compromised or inadequate security.

Although computer security is a volatile and evolving area, we understand that any process we recommend will raise questions from some users. The Desktop Security Task Force unanimously agrees that we would rather deal with questions about securing computers than help repair computers that have already experienced security breaches. While this method will not necessarily reduce the number of helpdesk calls, it will provide more straightforward, easier to answer questions and greater customer satisfaction. Despite the requisite investment of time and resources, most support people will agree that the time and resources are better spent in a proactive manner.

Position Paper

Critical questions defined, analyzed and answered

In order to address the issue of desktop computer security at Virginia Tech we must clarify both the concept of desktop **computer security** and **desktop computers** themselves.

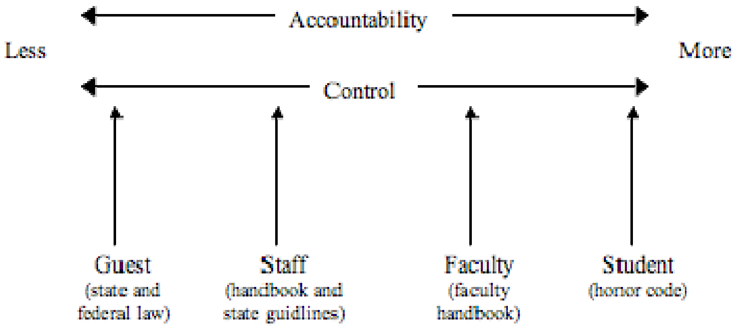
Computer security is frequently defined as “the prevention, detection, and recovery of unauthorized actions by users of a computer system.” Computer security also encompasses confidentiality, availability, and integrity of the system and the data residing on or transferring through that system.

The primary use of a **desktop computer** is accessing and inputting information directly from the console, typically by a single user. Given the versatility of the common “desktop” operating systems, components of a desktop computer may provide “server” services such as file and printer sharing or personal web pages. However, these “server” components are not the primary focus of a desktop computer’s utility. Removing “server” components would not adversely affect the usefulness of the desktop computer. If server-type services are provided and considered crucial to the utility of the machine, it cannot be treated as a desktop computer.

A desktop computer is designed as a tool to use resources rather than a platform to provide resources to others. Nevertheless, the default configuration of many popular “desktop” operating systems enables “server” type resources. Enabling shared resources on a desktop computer should be avoided, but in practice is not the standard. Therefore, a potential “server” component exists for every desktop computer. Desktop computer users need to be aware of any resources they are “serving.”

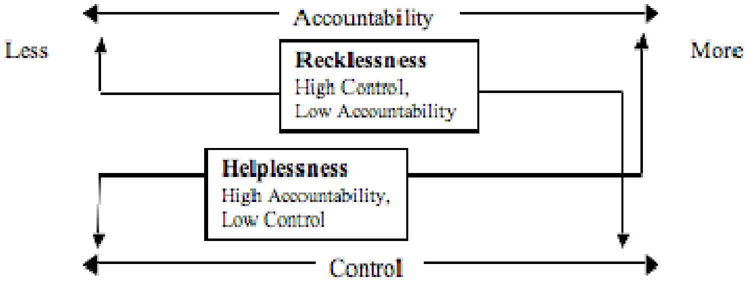
All computer users at Virginia Tech can be categorized by their information technology (IT) consumer role. IT consumer roles can be assigned by establishing individual user accountability – similar to the way the standards for a person’s professional and academic behavior is set through university disciplinary action guidelines. This accountability should be linked directly to the amount of control over a desktop computer. The higher the level of control a user requests, the greater accountability he or she must assume. Accountability (and consequently, control) may be limited by a user’s knowledge level, desire to retain control, and management directives. Failure to manage a desktop computer at the IT consumer’s control level should result in appropriate consequences.

University roles and IT consumer roles should not be confused. A university role of student or faculty does not confer nor release any accountability. Unlike university roles, IT consumer roles are not fixed. IT consumer roles must be assessed every time a person changes their IT resource. A student using her personally owned computer to get her schedule for the day would hold high control/accountability. The same student using a departmental desktop computer in her afternoon work-study job would have medium control/accountability. Lastly, that student doing late-night research with a library kiosk computer would have low control/accountability.



This model highlights a problem with enforcing security on desktop computers. Some IT consumers believe they enjoy “high control” without the concurrent “high accountability.” [redacted]

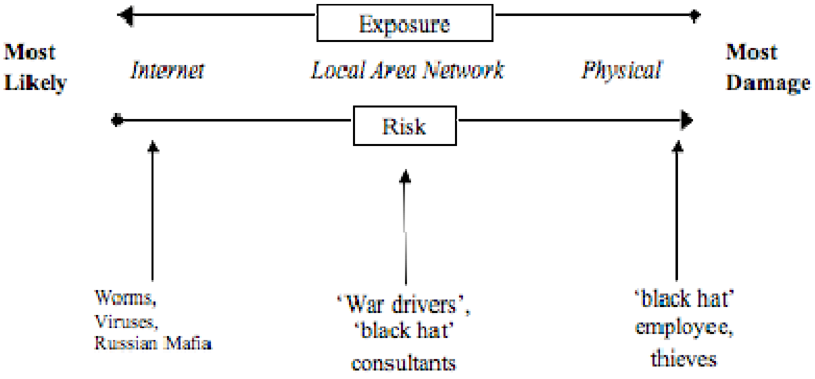
[redacted] The individuals tasked with maintaining those computers are in the opposite situation: “high accountability” and “low control.”



The maintenance person’s “helpless” feeling is due to his lack of control of the computer. These situations may arise from a lack of IT consumer education about their role and the corresponding level of accountability. In addition, past failures to properly maintain a desktop computer may have limited direct consequences, reducing the perceived seriousness of improper or neglected computer maintenance. In recent times the consequences of poor computer maintenance have grown from degraded performance to security breaches as extreme as complicity in the execution of illegal acts.

Poorly managed computers can be exploited in a myriad of ways. Security can be compromised from the Internet, the internal network, or the console. Anyone who can access the machine physically or from the network and who is not trusted by the owner(s) of the computer is a potential attacker. **Trust** is defined as the deliberate granting of permission to an individual to use your resources. By default, anyone you do not know is not someone you can trust. Connecting to the Internet or leaving your computer in an unlocked room exposes the machine to attackers.

The greatest **threat exposures** (for the greatest number of machines at VT) are usually from the Internet, then the local network[1], and then from the console. Conversely, the greatest **threat risk** is an attacker sitting at your computer, then on the local network, and the lowest risk from the Internet. In other words, it is more likely a hacker will attack you from the Netherlands than sitting at your desk, but the odds of them succeeding are lower. Although a black hat hacker enjoying your ego-chair is much less likely, one such attack will very likely succeed.



At the time of this writing the greatest threat is from Internet-based attacks aimed at using machines as relays or zombies. The recent renaissance of automated worms has made the Internet a hostile environment by default. An un-patched Windows 2000/XP/2003 system connected to the Internet will typically get infected

[1] Without firewalls, a local network can be considered the same as the Internet.

within 300 seconds. Spam hosting has increased the market pressure for compromising computers with the pairing of automated spam relays with the worms. With the increased lure of profits, unscrupulous advertisers have joined forces with virus and worm writers to increase the number of zombie systems spewing advertising. "Zero-day" releases of exploit programs for reported flaws in computer systems makes patching and virus scanning a continual game of "one-upmanship." Increased pressure from organizations like the BSA and RIAA are also encouraging illegal software traders to use more "untraceable" zombie systems as "warez" servers. The cracker community also sports a culture that counts the number of zombie systems you have under your control as a measure of your prowess. Unfortunately for us, .EDUs are on the rise over .GOVs as prized zombies. The owners of .EDU machines are less likely to pursue legal recourse and have greater network bandwidth.

We have outlined 11 remediation steps to address these threat areas, including firewalls, antivirus software, user education, secure applications, and administration best practices. Of these steps we believe that the most important is user education. It is the one remediation factor listed for almost every defined threat.

Computer security authorities agree that user education is simultaneously the most important and most difficult task to tackle. The two traditional ways to approach this problem are: 1) provide training to all users on computer security and proper network behavior, or 2) create a managed computer security environment where users aren't responsible for their computers. Many businesses choose the second method by providing secure, restricted workstations that only provide the functionality needed for a user to complete their job tasks. Skilled administrators retain the majority of the control over these desktop computers. Many at Virginia Tech agree this level of restriction would not feasible for every user (i.e. students) as there is no "skilled administrator" for those machines. In addition, many machines function in several roles and have organic security requirements, further moving beyond the scope of our available support environment.

The organic nature of our security environment is rooted in the organic nature of our institutional structure. Since Virginia Tech is primarily an educational and research institution, our constituency is inherently fluid. Every year we see a significant fraction of our constituency matriculate and a similar fraction graduate. A major facet of our organization is to educate the student constituency and produce graduates who will find meaningful roles in society. Another aspect of our organization is facilitating faculty and student research pursuits in a variety of disciplines. A confederation of various entities works to further realize these objectives.

In many ways Virginia Tech is like a city with the confederation of entities acting like businesses operating within a designated boundary. Some of these "businesses" provide the services needed to run the others. Examples of these services are the physical plant, electric service, network and telecommunication infrastructure, and information systems. Except for a hospital and a fire department, we offer every service that you would find in a municipality. Centralized and decentralized services have evolved. Both types have grown out of regulatory or infrastructure limitations. Individual entities are deterred from providing the services in an ad hoc manner due to efficiency costs or limited (or prohibited) authority, creating centralized services. When central entities are not able to efficiently provide the necessary services, decentralized services evolve. In some cases centralized services cannot be authorized to provide the service due to contractual restrictions such as non-disclosure agreements or federal security classifications. Internal "power" issues have also fueled decentralized service proliferation with individual entities finding the concept of relinquishing control and flexibility unpalatable. Central entities' finite resources and interest in maintaining efficiency further promote a culture of "rolling your own" services where possible to avoid delays and potential obstruction.

In addition to our internal constituencies and entities, our overall constituency also includes alumni and financial supporters, the national and international communities that benefit from our outreach programs, various state agencies, state governments, industries, and federal and international agencies. One could state this as "We support and promote education and research, and any ancillary operations that are required to facilitate the community to make those primary operations successful."

Virginia Tech's organizational structure does not lend itself to any single method of securing systems. We have a hybrid of centralized and decentralized governance with mandates, directives, opinions, criticisms, and suggestions coming from varied and differing constituencies. Gaining consensus among these constituencies about how to implement security from the top down could be very difficult, if not impossible. Therefore, we look towards the first method – training all of our users.

Training all of the university’s computer users is admittedly not a simple or easily accomplished task with the constantly changing faculty and student populations. Providing in-depth computer security training would require IT consumers to invest their highly valued time. The training may be viewed as a poor use of time by those IT consumers who only consider the computer as a tool to accomplish their daily tasks. In-depth training would also require Virginia Tech to make a large, recurring investment of time and money; resources which, in the current budget environment, are not likely to be easily available.

A third, non-traditional option is to provide a blend of the two approaches: provide a simple, unmanaged computing environment that provides security and functionality in an easy to use interface. This calls for a process that provides the ability to secure a computer based on the role(s) of that computer and can be run anytime a role change is required. With a limited amount of training a user could use the process to maintain their desktop computer as if a “skilled administrator” managed it. The user would relinquish some of his control (and accountability) to the engineers of the process. We would therefore need to be sure that the accountability issues for the process are well defined in advance.

Although computer security is a volatile and evolving area, we understand that any process we recommend will raise questions from some users. It is the unanimous opinion of the Desktop Security Task Force that we would rather deal with questions about securing computers than help with computers that have already experienced security breaches. This method will not necessarily reduce the number of helpdesk calls, but will provide for more straightforward, easier to answer questions, and greater customer satisfaction. While this method requires an investment of time and resources, most support people will agree that the time and resources are better spent in a proactive manner.

How we secure desktop computers at VT

We first need to determine how desktop systems (as defined by the DSTF position paper) proliferate in the Virginia Tech environment. Students bring desktop systems as part of the VT computing requirement. Faculty can bring their own or are lent desktop systems through the FDI program or local departmental programs. Staff can bring their own or are lent desktop systems either through local department programs or through the Banner desktop initiative. Individual departments also utilize desktop systems for kiosk and lab setups.

The second concern is ownership of the system. Implicit end responsibility for the system is defined at the core by who "owns" the system. Licensing and legal issues are bound to this concern. Based upon this ownership, the onus of having a secure system may shift from the IT administrator to the owner.

The third concern is the whether the end user is also the administrator of the system. Quite often there is no division of administrative responsibility for a system. End users typically have an identified set of requirements that necessitate using a computer. Rarely, if ever, is proper administration of the system explicitly stated and evaluated within a user's set of tasks.

Identifying the three core concerns help us base what type of security can be applied proactively. If the system is privately owned, a process must be developed to allow the owner to follow proscriptive security practices quickly and efficiently, or abdicate this responsibility and authority to a third party (typically VT staff).

To help manage the process of securing a desktop computer, the lifecycle of a computer must be understood. This process follows the system from creation to destruction:

Design → Deploy → Maintain → Surplus

In the **design phase** a system's specifications are identified. Does the system need a large amount of video memory? Does the system require the ability to burn CDs or DVDs? At this early stage, security is typically given little thought. Some questions we could (and should) ask are:

- Does this system need to be physically secure?
    - Solution: Add locking case, cable and alarm.
- Does the system need alternative authentication methods?
    - Solution: Add biometrics, smart card reader, fingerprint reader or camera.
- Does the system's USB and Firewire ports need to be secured?
    - Solution: Maybe add glue or disconnect wiring internally.

In the **deployment phase** a system needs to be built with security foremost in mind. The DSTF has identified the following steps to provide a good security-minded deployment strategy.

1. Power on system (w/o network)
2. Profile current system
3. Wipe system
4. Re-install OS w/latest SP
5. Disable/uninstall unnecessary applications/services
6. Apply critical security hotfixes
7. Harden local security policy
8. Harden local accounts and create accounts w/correct privileges
9. Enable/install and config firewall
10. Install and config A/V
11. Enable and config backup solution
12. Internal audit/baseline
13. Config and enable network
14. External audit/baseline

In the **maintenance phase** appropriate system administration dictates that a subset of the steps we initially followed for deployment are continuously monitored, updated, and re-evaluated. These steps are:

1. Identify any applications or services no longer needed and disable/delete
2. Identify, evaluate, and install any new OS and application fixes
3. Re-evaluate local security policy for possibilities of tightening
4. Verify firewall is up-to-date, working correctly and blocking unnecessary traffic
5. Update antivirus application and signature files
6. Test backup and restore procedures
7. Verify audit baseline matches stated requirements

The desktop in the **surplus phase** is no longer deemed a valuable commodity. Steps are needed to correctly remove the system from production responsibilities and ensure that any data is removed from the system so that that unauthorized recovery is impossible.

In the design phase administrators can make use of peer support via 4help, the VT knowledge base, and email listserv communication. The IT Security Office (ITSO) can also be contacted and queried about the best design practices for desktop systems.

In the deployment phase administrators can utilize many mechanisms for developing a secure strategy. VT websites like *security.vt.edu*, *antivirus.vt.edu*, and *ita.vt.edu* can be reviewed for low cost, free security and antivirus software and proscriptive guidance. Vendor websites and tools like *windowsupdate.microsoft.com* and SUS can be utilized to download and install hotfixes. Free and open-source products like Daisy and Ivy can be bundled into desktop deployment to lower the total cost of the system. VT websites that help owners and administrators identify low cost or no cost firewall solutions (like IPsec) are locatable.

The maintenance phase requires more work on the administrator’s part. Subscription to email lists like techsupport, NTbugtraq, and vendor specific lists (like MS security bulletins) are frequently required to get important update information on operating systems and application fixes. Low cost storage and backup solutions are available from central IT to help reduce the burden of maintaining adequate desktop backups.

In the surplus phase 4help, ITA, and Surplus can help to properly decommission university-owned equipment. For individually-owned systems, free tools like Killdisk can be located and downloaded to insure that hard drive media is properly sanitized before reusing or selling the equipment.

Several mechanisms are available to owners and administrators of university and personally owned computer systems that interact with the VT IT architecture. The three greatest immediate concerns when developing a strategy to secure these systems are:

A. How is the system introduced to the VT computer environment
B. Who “owns” the system
C. Who is responsible for administrating it

Once these questions are adequately addressed, the desktop computer lifecycle can be examined and a process formulated to ensure security is maintained.

How desktop security is compromised

One of the tasks assigned to the Desktop Security Task Force (DSTF) is the identification of mechanisms used to exploit desktop computers at Virginia Tech. The avenues of exploit can be broken down into four categories: **Person**, **Physical**, **Network**, and **Management Override**. This document identifies and describes the subsections of each exploit "zone."

1) Person

a) Post-it note passwords
People find complex passwords difficult to remember. Rather than forget the password or get temporarily locked out from the system due to a bad password, they write down the password and leave it near their computer.

b) Malicious attachments
People are generally curious and assume that other people are well intentioned. Well-worded emails with interesting attachments are shiny, candy-like attractions for people to open.

c) Weblinks (forged/malicious)
HTML email and websites can be constructed in such a way as to mislead users into believing that they are navigating to one place when they are actually being redirected to a malicious site.

d) Spyware/trojans
People who have the permission to install new programs on systems are constantly tempted to install programs or applications which appeal to them. These include applications that have additional, unintended functions.

e) Unrestricted P2P
Some people use peer-to-peer applications to trade data across the Internet. Often these illicit files are trojans or contain viruses.

f) Insecure/obvious passwords
If password complexity, length, and history are not enforced across all authentication mechanism, people have the tendency to choose a simple and easy to remember password. Unfortunately, simple passwords are most often easy to guess or compute. Some common, easy-to-remember passwords include obviously guessable things like the username, dictionary words, relatives' names, or no password at all.

g) Account sharing/sharing passwords
People consider their first and foremost task as getting their work done. Sometimes computer security causes difficulties in this task. Rather than request the proper authorization and incur the delays that may be involved, the user may share their own or ask for another user's userid and password to expedite the process.

h) Out of date security patches
People tend to not maintain their desktop workstation OS and applications at the most current patch level, leaving them vulnerable to exploit.

i) Out of date antivirus software
People tend to not maintain their antivirus definitions at the most current version, leaving them vulnerable to new viruses.

j) User ignorance/lack of education
Users are generally not taught the steps required to maintain a secure system. They don't know what they need to do to ensure their system does not get compromised. In addition, they don't always understand the Internet threat environment and recognize the risks they may be taking.

k) User apathy
Some users consider the computer as simply a tool to be used like a calculator. They do not consider (or do not have written in their job description) computer security as a component of their job.

l) User curiosity
Some users (whose job is not that of IT staff) are generally curious about how computer systems work. They may alter or attempt to subvert security measures to explore the desktop environment.

m) Poor practices

Poorly defined practices allow for generalized or incorrect security settings to be defined. These settings are then insufficiently audited and simply trusted to be working correctly.

n) **Open file/printer shares**
People want to be able to access necessary files or print to printers that are attached to a local computer. Often, the easiest way to share printers or files is to make them available read/write to the world.

o) **"My machine" syndrome**
Some users are very territorial about their desktops. Attempts to provide administrative support may be considered an encroachment on their sovereignty. Territorial boundaries make it difficult for IT staff to ensure uniform deployment of security efforts. An unreceptive user could cut themselves off from structured security efforts that are inefficient or difficult to implement on an individual basis.

p) **Malicious user**
Some users actually wish to cause disruptions and cause damage to systems, services and the network. Having access to a system "internally" can give them a large amount of power to cause problems.

q) **Account types (login using Admin account)**
Some software has difficulty installing or running under an account that does not have "root" or "administrator" rights to the system. It is easier to give all users of a desktop these powerful rights than to attempt to lock down the user's rights.

r) **Saved passwords**
Some applications (like IE and Firefox) allow a user to save passwords when entering them on a website. If the account is shared or compromised, these passwords can be recovered.

s) **Single password, multiple usage**
A user may have one password they use, as a convenience, for all accounts. If the one password is shared or compromised, all accounts are then accessible. This is particularly a problem if the user increases the password exposure by using the same password for internal and external account providers (for example, making PID and Hotmail passwords the same).

2) Physical

a) **No locking screensaver**
Users find it onerous to have to re-enter their password if a screensaver locks the computer. If a system does not have a locking screensaver, physical access to the system is easier for the user but also allows unauthorized users.

b) **Social engineering**
Users may not have a clear understanding of who should have access to their desktop, who they should give sensitive information to or take instruction from. They could be tricked into giving inappropriate access to malicious parties.

c) **Removing components/insecure location**
Desktops in open areas or that are publicly accessible are susceptible to disassembly or being rebooted into other OSes. Malicious devices like hardware key loggers could be installed.

d) **No BIOS password**
Desktops without BIOS passwords can be rebooted and their configurations modified. This would allow access to the boot order, which would allow a malicious user to boot from other devices, thus bypassing security measures.

e) **Evil auto run CDROM**
If unmarked media is used with the desktop and the auto run function isn't disabled, malicious code could be automatically run.

f) **No chain lock for laptop**
If a laptop isn't secured to an immovable object, it can be quickly and easily stolen.

g) **Backup stealing**
Sensitive data resides on backup tapes and CD-ROM. If these records are not secured, they can be restored to a remote machine and attacked with impunity.

h) **Inappropriate hardware de-provisioning**
When storage media is not correctly reformatted or destroyed, it may accidentally be made available to public parties.

i) **Theft of software**

If media is not secured it may be taken and used by unauthorized parties.

j) **Malicious replacement of your software**
If a change revision process is not in place for the desktop, software may be replaced with trojan versions.

k) **Infection vector through system management**
If remote system management services or applications are installed on the desktop, failing to secure the management software server could allow the subversion of all managed desktops.

3) Network

a) **Unsecured wireless**
Inappropriate access may be given to attackers if a laptop or desktop has a wireless network card in peer-to-peer or ad hoc mode and the connection is not secured.

b) **Exploit vulnerable systems/services (buffer overflow, etc)**
Remote network attacks aimed at desktop services may cause corruption or failure of these services and allow inappropriate code execution.

c) **Sniffing**
Compromised desktops may have their network settings altered to listen to all traffic in the subnet and capture information not intended for it.

d) **Denial of Service attacks**
Compromised systems may be used to mount network attacks or fall victim to such attacks that cause services to become very slow or fail.

e) **Unsecured traffic**
Information transmitted from a desktop application over the network may be sent in clear text. The traffic may be sniffed along the way and copies made.

f) **IP spoofing / "Man in the Middle"**
Desktops that send information to another system may be redirected or re-routed through a third party who can copy or alter the information in transit.

g) **Zero day exploits**
Desktops that are connected to the network maybe be attacked by exploits which are previously unknown and for which there is no preventative measure or fix.

h) **Password guessing**
Desktops may receive hundreds or thousands of authentication requests per second as tools attempting brute force guessing of local user accounts and their passwords.

i) **Compromised machines**
Desktops connecting to remote machines may assume the remote system is also secure and trustworthy. A compromised remote machine may use this trust to stage an attack or deliver infected files.

j) **Compromised subnet**
Network subnets where compromised systems are located cannot be considered secure or trustworthy. Information transferred across the subnet may be sniffed and routing information may be suspect.

k) **Purposeful account locking**
If an account lockout policy is known for a desktop, a malicious remote user can make a connection and purposefully submit incorrect passwords for the local accounts, thereby locking them out and preventing legitimate use.

l) **Information disclosure**
Some desktops operating systems expose security-related information to anonymous or public inquiry. This data can be used to profile and identify systems for further probing or custom attack.

m) **Not monitoring network interaction**
Desktop systems may not have their network connection filtered and monitored for appropriate data transmission. Rogue applications or trojans may be allowed to contact third parties without interference.

n) **Wireless**
Desktops set up with wireless networking may subvert intended edge firewalling.

o) **War driving**
Unsecured wireless networks may allow malicious users access to network resources without physical access to the wired network or building.

p) **Device contention**

Different types of wireless devices that are setup without consultation and planning may cause interference or device failure. Intentional interference can be used for denial of service attacks. Man-in-the-middle attacks can be staged by providing a rogue access point that overpowers the signal from a legitimate access point.

4) Management override

a) Convenience

Management may consider security requirements and restriction too burdensome for themselves and their staff. Often they can override policy and procedure because they are in charge of the IT staff.

b) "Nothing important"

Some managers do not consider the effort to secure their desktop cost-effective because they "have nothing of value on them."

c) Desktop is backed up

Some managers do not consider their desktops as needing security because they feel having the systems "backed up" insures them sufficiently against loss.

d) Self sufficiency

Some managers feel that their position entitles/requires that they don't allow IT staff to manage the security of their system. They take it upon themselves to maintain security when they have the time.

Remediation steps for desktop security

The last task assigned to the DSTF (Desktop Security Task Force) is to identify steps useful in the remediation of desktop security issues at Virginia Tech. We have outlined 11 major remediation factors that can address the wide range of previously described exploit "zones." This document details the remediation factors and explains which exploits they mollify. Along with the remediation factor descriptions, we have developed security initiatives and categorized each as a high, medium or low priority.

A **high priority** initiative is of maximum importance. The process or project should (in a best case scenario) have already been initiated. The DSTF feels that all necessary staffing, funding, and political motivation should be brought to bear to achieve these goals.

A **medium priority** initiative is also important, but may be difficult to put into immediate practice due to cost, time, or personnel issues. Medium priority tasks should be implemented during the next possible opportunity (budget cycle, staff hiring, project planning, etc.).

A **low priority** initiative may take a long time to complete or may require a large paradigm shift to accomplish. While low priority tasks are still justified, they may place an unreasonable burden upon the implementers according to the resulting increase in security it would provide.

Multi-factor authentication

Definition:

Multi-factor hardware-based authentication requires a combination of something a person knows, something a person has, and possibly something a person is. The something a person knows could be an easily remembered PIN, the something a person has would be a smartcard, smart USB key, or a smart button, while the something a person is could be their thumbprint for a biometric fingerprint scanner. Two or more would be required in combination.

Mitigates the following risks:

- Sticky Note Passwords (1a)
- Insecure/obvious passwords (1f)
- Account sharing/sharing passwords (1g)
- No locking screensaver (2a)
- Social engineering (2b)
- Removing components/insecure location (2c)
- Password guessing (3h)
- Purposeful account locking (3k)
- Ease of use (4a)

Recommendations:

High priority:

Fast track a pilot program to utilize the VT CA and user certificates to eliminate the requirement for a known password. Utilize smart cards to provide hardened credentials for workstation login and authentication to web sites.

Medium priority:

Offer education on converting from passwords to pass phrases for increase remember-ability and the difficulty of password guessing.

Low priority:

None

Clean Desk policy

Definition:

Security staff does periodic spot-checking of IT worker's desktop and office environment. Special attention is taken for security related issues, i.e., passwords written down in plain sight, documents marked confidential or containing social security numbers left in the open, etc. Identified lapses in security would be noted on staff member's permanent record and influence employee's evaluation.

Mitigates the following risks:

- Sticky Note Passwords (1a)
- Account sharing/sharing passwords (1g)
- No locking screensaver (2a)
- Backup stealing (2g)
- Theft of software (2i)
- Malicious replacement of your software (2j)
- Wireless (3n)
- Device Contention (3p)

Recommendations:

High priority:

1. Implement a policy for managers to do monthly verification that their subordinates are not exposing sensitive data at or around their computers.

2. Proactively utilize Google (via Wikto or other tools) to audit VT's dataspace for publicly available documents that shouldn't be exposed (such as student name/SSN/grade combinations in SAS files) as well as other exposed issues.

Medium priority:

Migrate any systems or service that currently requires SSN identification data to a UID-based system. Remove SSN from timesheets, etc that are exposed as clear-text on the network. Remove requirements for SSN for parking permits, etc.

Low priority:

None

User Education (Awareness)/Accountability

Definition:

Give instruction to those using desktops about the appropriate process and procedure to secure and maintain the security of those resources. User education was repeatedly cited as an important component to improving security, but it was also noted that a lack of enforcement would neutralize most education efforts. Task force members noted that adding information system security into the "universal performance dimensions" for university job descriptions could enforce accountability for lax user security.

Mitigates all risks **except** *the following:*

- Unauthorized P2P (1e)
- User apathy (1k)
- User curiosity (1l)
- "My machine syndrome" (1o)
- Malicious user (1p)
- Removing components/insecure location (2c)
- Infection vector through system management (2k)
- Sniffing (3c)
- Denial of Service attacks (3d)

- Zero day exploits (3g)

Recommendations:

High priority:

1. Implement a one credit required class for all freshmen that educates them on the security issues, rights and responsibilities entailed when utilizing VT network and computing resources.

2. Require that all new faculty and staff take an accelerated version of the course (with a final web-based test) before or immediately after going to personnel training. Require successful completion of the course before their first paycheck is issued.

3. Define an IT security ombudsman that would report at the highest level of the VT organization. Allow for anonymous and secure communications between confidants and this individual. Insure that concerns are addressed and not ignored or swept under the rug.

Medium priority:

1. Based on risk analysis of departments, require that IT administrators are adequately paid, educated, and have appropriate levels of managerial backing. Several key departments on campus do not appropriately value their IT staff and consequently have high turnover in these areas.

2. Require that managers are notified when systems in their departments are exploited, have their network ports deactivated or their systems recovered or reinstalled. Appropriate documentation should be saved for end of year evaluation. This will both encourage staff to care about security (since it affects their salaries) but also will help garner metrics for upper management to see what areas are doing well (or not so well).

Low priority:

Develop a public service announcement (PSA) service that writes, produces, and advertises appropriate computer security practices via local campus TV and radio announcements.

Quarantine process/firewall/detection

Definition:

Discussion of a quarantine process focused on server-side implementation. One option is separating the attachment completely from the message and making it accessible via HTTP (reducing the effectiveness of combined HTML and attachment attacks). Another is delaying delivery of an attachment to allow antivirus definitions time to catch up with virus mutations. Implement a client-side firewall that prohibits unrequited network interaction with other systems.

Mitigates the following risks:

- Malicious attachments (1b)
- Weblinks (forged/malicious) (1c)
- Spyware/trojans (1d)
- Out of date security patches (1h)
- Out of date antivirus software (1i)
- User ignorance/lack of education (1j)
- User apathy (1k)
- User curiosity (1l)
- Poor practices (1m)
- Exploit vulnerable systems\services (buffer overflow, etc.) (3b)
- Sniffing (3c)
- Denial of Service attacks (3d)
- IP spoofing/"Man in the Middle" (3f)
- Zero day exploits (3g)

- Password guessing (3h)
- Compromised machines (3i)
- Compromised subnet (3j)
- Purposeful account locking (3k)
- Information disclosure (3l)
- Not monitoring network interaction (3m)

Recommendations:

High priority:

1. Require all F/S to have AV running and up-to-date on their systems. Refuse technical support unless AV status is verified.

2. Strongly recommend to students that they should have AV running and up-to-date on their systems. Refuse technical support unless AV status is verified.

3. Develop a system to impound attachments from email being sent and received from/to VT email addresses. These attachments would be scanned before the user has access to them.

Medium priority:

1. Require secure authentication to central mail servers when sending email. If users are discovered to be sending spam, notify their superior and block their email access for a period of time. Block the ability for other systems to send/receive email directly on campus.

2. Develop a "tiger team" of security personnel (3-5 FTE, 1-2 GS) which helps identify "owned" systems, take them offline, do a forensics examination, and recover the systems in a timely manner. Once these systems are back in production, they would develop an anonymous public report to help educated admins understand why it was exploited and how to avoid the same thing from occurring in the future.

3. Develop a system to curb the use of email as a file transfer mechanism. Encourage use of an alternative application that provides for secure and encrypted file transfers and that detaches attachments from email into this process.

Low priority:

Develop a system to identify exploited systems. Charge a nominal fee to reactivate the network ports of these systems once they have been cleaned. First time is free, second time (within the semester) costs $15, third time is $50. More than three strikes and the network port won't be reactivated within the semester. Use this money to foster increased safe computing educational seminars, etc.

Consistent password policies

Definition:

Develop a process to enforce synchronized password complexities, rule sets and histories across many VT enterprise systems. This would ostensibly increase security (by having one password of the greatest possible complexity) and reduce usability issues (by reducing the number of passwords a user is required to manage). This process might also include the ability for end users to reset a forgotten password via self-selected password "hints."

Mitigates the following risks:

- Insecure/obvious passwords (1f)
- Poor practices (1m)

Recommendations:

High priority:

Do an audit of all VT systems that require username/password logins. Verify or change functionality of these systems to use the same level of security (HCD – highest common denominator) for password length, complexity, history, and expiration. Do not allow weak systems to continue without an aggressive migration plan.

Medium priority:

None

Low priority:

None

Appropriate administration

Definition:

The administrator of the desktop system has the requisite knowledge and skill set to properly maintain the system during its lifecycle. The administrator of the machine is (ideally) not the primary user of the system. The system is maintained in accordance with the DDMS (Design, Deploy, Maintain, Surplus) lifecycle methodology (as outlined in the document "How do we secure desktop computers at VT?").

Mitigates all risks **except** *the following:*

- Post-it note passwords (1a)
- Account sharing/sharing passwords
- "My machine syndrome" (1o)
- Malicious user (1p)
- Social Engineering (2b)
- Removing components/insecure location (2c)
- Infection vector through system management (2k)
- Sniffing (3c)
- Denial of Service attacks (3d)
- Zero day exploits (3g)

Recommendations:

High priority:

1. Require by policy that all university owned systems have a primary administrator that is specifically paid to maintain the system. Do not assume the primary user of the system will also correctly administrate it.

2. Require management empower the "IT Person" to enforce reasonable security policy including patches/upgrades, password configuration, access rights/privileges, file system permissions, etc. on all users.

Medium priority:

Develop facility-managed infrastructure to alleviate the complex burden of administration for these primary admins. University Services in the Hokies Active Directory is an example.

Low priority:

Pilot a project that replaces IT knowledge worker role systems with inexpensive thin clients. Virtualize (on back end) the desktop OS to enable a few knowledgeable administrators to manage the systems centrally.

100% Anti-Virus scanner

Definition:

Desktop system should have one or preferably more than one antivirus software suites installed. These suites must be automatically updated with the latest possible virus definitions and the core software updated as frequently as possible utilizing more than one vendor's antivirus solution allows for a "broad spectrum antibiotic" instead of a single drug. Identified malware (viruses, trojans, worms, adware, etc.) should be deleted or quarantined. Never attempt to fix the file. A central console mechanism should be available to coordinate attack patterns and determine what users are falling victim to malware for follow-up re-education efforts.

Mitigates the following risks:

- Malicious attachments (1b)
- Weblinks (forged/malicious) (1c)
- Spyware/Trojans (1d)
- Unauthorized P2P (1e)
- Out of date antivirus software (1i)
- User ignorance/lack of education (1j)
- User curiosity (1l)
- Poor practices (1m)
- Open file/printer shares (1n)
- Evil auto run CD-ROM (2e)
- Malicious replacement of your software (2j)
- Infection vector through system management (2k)
- Exploit vulnerable systems/services (buffer overflow, etc) (3b)
- Sniffing (3c)
- IP spoofing/"Man in the Middle" (3f)
- Compromised machines (3i)

Recommendations:

High priority:

1. Buy a site license for more than one vendor's solution for AV and anti-spyware software. Encourage their combined usage on all production systems.

2. Alter ITA's licensing policy for AV software to include all valid users of VT network or computing infrastructure (instead of University owned machines or currently enrolled students only)

Medium priority:

None

Low priority:

None

Patched and secure applications

Definition:

Applications should be maintained at the newest revision available from the manufacturer. Only applications that are required for the proper function of the IT worker should be installed on the desktop workstation. A process must be in place to quickly and verifiably update required applications when hotfixes or service releases come out. If an application that comes with the core operating system is known to be repeatedly vulnerable to exploit, it should be disabled (or uninstalled) and an alternate equivalent application used. Secure applications should not trust the underlying system layers to secure its data files or network traffic.

Mitigates the following risks:

- Malicious attachments (1b)
- Weblinks (forged/malicious) (1c)
- Spyware/Trojans (1d)

- Out of date security patches (1h)
- User ignorance/lack of education (1j)
- User apathy (1k)
- Poor practices (1m)
- Exploit vulnerable systems/services (buffer overflow, etc) (3b)
- Compromised subnet (3j)
- Information disclosure (3l)

Recommendations:

High priority:

1. Develop a policy and procedure so that ITA sells only the most updated and secure software. For Windows operating systems, merge all service packs and hotfixes into a slipstreamed version for distribution. Update software on a monthly basis.

2. Develop a "recipe" for all VT systems so that administration knows what services, protocols and ports are required to successfully access them. Require VT system developers and implementers to keep changes to keep this "recipe" up to date. This will help to correctly firewall workstations based on what systems they need to access.

Medium priority:

Actively discourage the use of highly vulnerable software such as Microsoft Internet Explorer. Require third party vendors and internal developers make their products compatible with open source alternatives such as Mozilla Firefox.

Low priority:

None

Restricted user rights

Definition:

Users of a desktop system should not have full administrative (root) rights to the system. Users should only be allocated the rights necessary to fulfill their daily tasks. If a user is then exploited, the system can only be victimized at the level of control the user has. Administrators should carefully segregate all aspects of a multi-user system so that users cannot intentionally or unintentionally access or modify other user or system settings.

Mitigates the following risks:

- Malicious attachments (1b)
- Weblinks (forged/malicious) (1c)
- Spyware/Trojans (1d)
- Unauthorized P2P (1e)
- Out of date antivirus software (1i)
- User ignorance/lack of education (1j)
- User apathy (1k)
- User curiosity (1l)
- Poor practices (1m)
- Malicious user (1p)
- Account types (login using Admin account) (1q)
- Social engineering (2b)
- Malicious replacement of your software (2j)
- Sniffing (3c)

Recommendations:

High priority:

Develop a policy to disallow end users the rights/requirement to run as root or administrator of systems.

Medium priority:
None

Low priority:
None

Appropriate recovery policy

Definition:

Desktop systems must have their operating system, applications, and data backed up to a local or centralized backup service. These backups should be weekday daily incremental, with full backups done every weekend or in accordance with a risk assessment of the full cost of potential data loss. The administrator of the system should have these backup records centrally monitored to proactively determine if systems are failing or skipping the backup schedule. The backup software should be able to be operated by a user with restricted rights so they can recover data if required, without administrator intervention. Recoverability of data should be scheduled on a weekly or monthly basis with media fitness testing a requirement. Backups should be stored in a secure location and in an encrypted medium to avoid or reduce the risk of theft.

Mitigates the following risks:

- Malicious attachments (1b)
- Spyware/Trojans (1d)
- Out of date security patches (1h)
- Out of date antivirus software (1i)
- User ignorance/lack of education (1j)
- User apathy (1k)
- User curiosity (1l)
- Poor practices (1m)
- Open file/printer shares (1n)
- Malicious user (1p)
- Social engineering (2b)
- Removing components/insecure location (2c)
- Backup stealing (2g)
- Theft of software (2i)
- Malicious replacement of your software (2j)
- Exploit vulnerable systems\services (buffer overflow, etc) (3b)
- Zero day exploits (3g)

Recommendations:

High priority:

1. Actively market centralized backup and network attached storage solutions. Highlight reduced departmental burden, improved security, and lower costs.

2. Expanded walk-in support to provide next level after support cutoff; a clinic to perform recovery, repair, reinstall, and securing of OS. This will be a required "class" during which the person would have to stay in attendance, provide the software, and perform the work with guidance from qualified staff. Create a support tier structure that students/staff can become "gold" support that will give a person stream-lined support if they are listed as having completed the training.

Medium priority:
None

Low priority:

None

Loss of Service/Packet shaping

Definition:

Desktop workstations that exhibit classic antisocial behavior, i.e., attack other workstations on the network, spew DoS style network traffic, MAC cloning, unauthorized DHCP/router service, share copyrighted materials, or any other behavior against the VT AUP and network usage guidelines should be identified, their administrator(s) notified, and its network connection terminated until fixed. If the system is interacting in an unidentified manner, but taking a large amount of network resources, its available bandwidth should be slowly throttled down to a minimal level and the administrator notified. Such "network usage fingerprints" would be valuable to limit the damage which known or unknown worms, trojans, or spambots could potentially cause.

Mitigates the following risks:

- Malicious attachments (1b)
- Spyware/Trojans (1d)
- Unauthorized P2P (1e)
- Out of date security patches (1h)
- Out of date antivirus software (1i)
- User ignorance/lack of education (1j)
- User apathy (1k)
- User curiosity (1l)
- Poor practices (1m)
- Open file/printer shares (1n)
- "My machine syndrome" (1o)
- Malicious user (1p)
- Social engineering (2b)
- Unsecured wireless (3a)
- Exploit vulnerable systems/services (buffer overflow, etc) (3b)
- Sniffing (3c)
- Denial of Service attacks (3d)
- IP spoofing/"Man in the Middle" (3f)
- Zero day exploits (3g)
- Compromised machines (3i)
- Compromised subnet (3j)
- Purposeful account locking (3k)
- Not monitoring network interaction (3m)
- Wireless (3n)
- War driving (3o)

Recommendations:

High priority:

Develop Network Intrusion Detection Systems (NIDS) and Host-based Intrusion Detection Systems (HIDS) internally and externally to VT's IP space. Based on metrics garnered from these systems, proactively packet shape or deactivate network portals of systems that are potentially compromised.

Medium priority:

None

Low priority:

None

Suggested links and additional reading materials

http://www.secunia.com

http://www.securityfocus.com/

A layered approach to security
http://www.broadbandreports.com/faq/8463

Securing Windows XP
http://www.tweakhound.com/xp/security/page_1.htm

Winning the security war requires the means to do the job.
http://www.eweek.com/article2/0,1759,1679514,00.asp

Trends in Web Application Security
http://www.securityfocus.com/infocus/1809

User Education Is Not the Answer to Security Problems?
http://www.useit.com/alertbox/20041025.html

Good report on security of Windows vs Linux
http://www.theregister.co.uk/security/security_report_windows_vs_linux/

Six Secrets of Highly Secure Organizations
http://www.cio.com/archive/091504/security.html

Doing IDS on Windows
http://www.securityfocus.com/infocus/1795
http://www.securityfocus.com/infocus/1801

Examining a Public Exploit, Part 1
http://www.securityfocus.com/infocus/1795

Deploying Network Access Quarantine Control (part 1 of 2)
http://www.securityfocus.com/infocus/1794

http://csrc.nist.gov/publications/nistpubs/

http://www.sans.org/resources/glossary.php

http://www.infosyssec.net/infosyssec/secstan1.htm

http://www.nsa.gov/snac/

The 10 immutable laws of computer security
http://www.microsoft.com/technet/archive/community/columns/security/essays/10imlaws.mspx