

Realtime
publishers

"Leading the Conversation"

The Shortcut Guide[™] To



Protecting Business Internet Usage

sponsored by


SurfControl[®]

Dan Sullivan

Chapter 4: Trends in Internet Access Protection for Business Integrity and Compliance.....	52
Challenges of Mobile Devices	52
Vulnerabilities of Mobile Devices	53
Wireless Vulnerabilities.....	53
Theft.....	54
Lax Understanding of Mobile Device Security	55
Mobile Device Malware and Other Threats.....	55
Managing Mobile Devices.....	56
The Changing Rules of IT Management.....	56
Semi-Managed Devices: Employee-Owned Hardware	56
Increasingly Complex and Porous Network Perimeters	57
The Crowded Perimeter	58
Intrusion Detection and Prevention	58
Content Filters and Anti-Malware Filters.....	60
VPNs.....	61
Porous Perimeters	62
Loss of Intellectual Property and Industrial Espionage	64
Zero-Day Threats	65
Increasingly Complex Countermeasures	66
The Future of Content Protection	67
Summary	68

Copyright Statement

© 2006 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.

Chapter 4: Trends in Internet Access Protection for Business Integrity and Compliance

The means and the methods for using the Internet for business are constantly expanding—and so are challenges to protecting information assets. Throughout, this guide has examined fundamental issues—both business and technical—entailed in the use of the Internet. This chapter examines several emerging and dynamic areas of concern for Internet security:

- Challenges of mobile devices
- Increasingly porous network perimeter
- Loss of intellectual property through industrial espionage
- Protecting against zero-day threats
- Increasingly complex countermeasures
- Future of content protection

Each of these entails threats to Internet use that can compromise business and organizational activity if not properly addressed. It is the goal of this chapter to provide a starting point for adapting to these emerging threats.

Challenges of Mobile Devices

Smart phones, personal digital assistants (PDAs), and Blackberries are becoming commonplace in today's organizations due to their ability to help increase productivity and enable more effective communications. As with any new technology, the introduction of mobile devices brings both benefits and costs. The cost of mobile devices includes security risks that did not exist in businesses before their introduction. Some of the most important are:

- Vulnerabilities of mobile devices and wireless networks
- Mobile device malware and other threats
- Unique characteristics of managing mobile devices

Mobile devices radically improve accessibility to information and many users would be hard-pressed to live without their mobile email access devices. These tools are here to stay. We simply need to ensure that they can be used in such a way that protects the confidentiality, integrity, and availability of information assets.

Vulnerabilities of Mobile Devices

Emerging technologies tend to leverage and expand on existing technologies, and mobile devices are no different. Although these devices provide fundamentally new types of functionality, they build on existing platforms. For example, mobile versions of Windows operating systems (OSs) are used in mobile devices. However, software designed for mobile devices may not have the same level of security features as its more mature counterparts developed for traditional client devices. Some of the most pronounced vulnerabilities of mobile devices include

- Wireless vulnerabilities
- Theft
- Lax understanding of mobile device security

These vulnerabilities can be countered, but first they must be understood.

Wireless Vulnerabilities

The same threats and vulnerabilities that afflict wired networks often apply to wireless networks. In addition, wireless networks have several of their own to contend with. For example, unencrypted communications on wireless networks can be intercepted without physical connections to a wired network. Unauthorized wireless access points can be introduced, allowing for rogue access to the wired network; some steps that can be taken to reduce these risks include:

- Shut down features such as always-on infrared or Bluetooth connections when not in use
- Use VPNs to access corporate networks from mobile devices
- Use countermeasures originally designed for servers and desktops, such as personal firewalls, anti-malware, and file integrity checking software

As Figure 4.1 shows, rogue wireless devices can gain access to a network as legitimate wireless devices if the access point can be compromised in some way. In addition to preventing such access, systems administrators must address OS vulnerabilities.

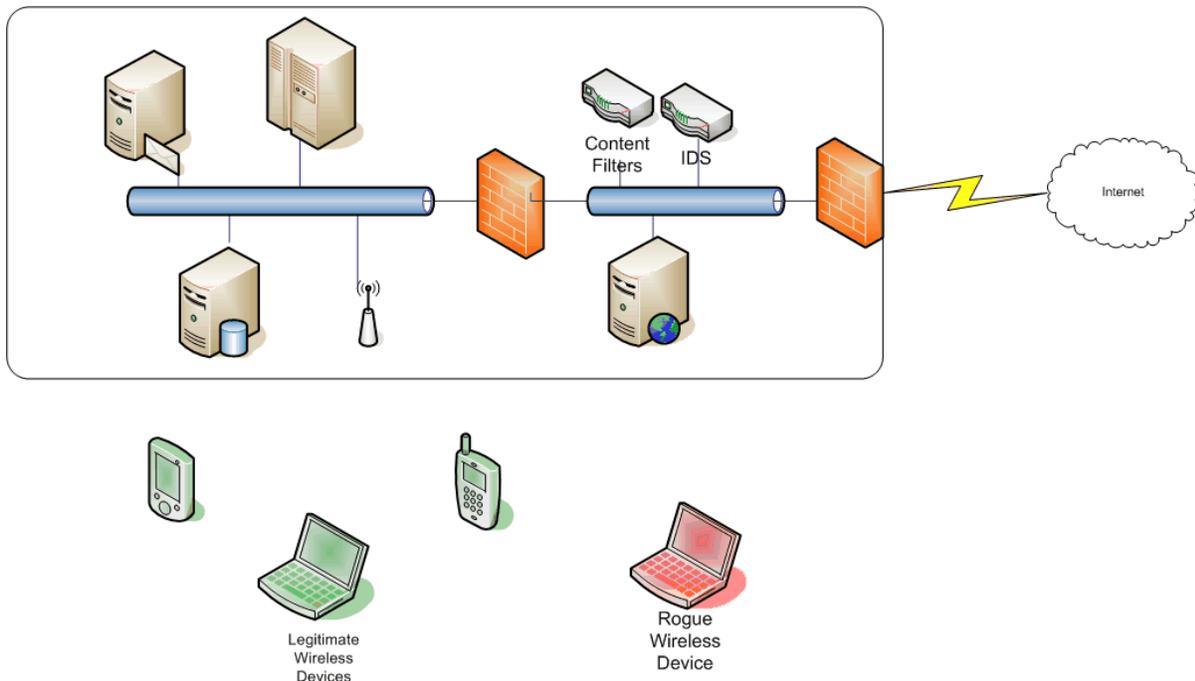


Figure 4.1: Wireless access points create the potential for both legitimate and rogue users if proper countermeasures are not deployed.

Theft

Theft is a key problem for mobile devices. By definition, these devices allow a user to keep the device with him or her and use it as needed. The great convenience has the accompanying downside of making the devices vulnerable to theft. Well-publicized laptop thefts are becoming too common:

- In one case, a laptop used by an employee of the United States Veterans Administration (VA) was stolen from the employees home; it contained the names, Social Security numbers, and other personal information about 26.5 million veterans and their spouses.
- In another case, a Department of Transportation employee's laptop was stolen along with names, addresses, Social Security numbers, and dates of birth of more than 130,000 persons.
- When a laptop used by an employee of an accounting firm was stolen, information about 59,000 Chevron employees was lost.

In addition to improving behaviors of mobile device users, encrypting data on these devices is essential to reducing the risk that a stolen device will yield useful information. Additional security measures, such as the use of security tokens and biometric authentication mechanisms, can further mitigate the risk of data loss due to theft. The problem of mobile device theft makes it clear that more than technical solutions are required to protect information assets.

For more information about laptop and mobile device theft, see Andrew K. Burger, "US Mobile Security Part 1: How Great is the Risk" at <http://www.technewsworld.com/story/wireless/52298.html>. For more examples of laptop thefts and other privacy breaches, see the Privacy Rights Clearinghouse at <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.

Lax Understanding of Mobile Device Security

Too often, security is thought of as a technology problem. If only you can find the right encryption algorithm or patch a buffer overflow vulnerability, you can make your device or application secure. It is true that the technical characteristics matter, a lot, but they are not the only ones. The non-technical, human use factors play critical roles as well.

Consider some disturbing results from several surveys about mobile device use and security:

- 22 percent of survey respondents lost a PDA in the past year; of those, 81 percent did not employ protective measures such as personal identification numbers (PINs) or encryption.
- 37 percent of PDAs have sensitive information on them, including account numbers, corporate data, and passwords.
- Only 40 percent of respondents to one survey reported the mobile device theft to the police.

Some of the challenges in mobile device security should be addressed by technical countermeasures, such as encryption and multi-factor authentication; others need to be addressed by well-defined and enforced policies, such as limiting the types of data that can be downloaded to mobile devices.

 Survey statistics are from “IT Professionals Turn Blind Eye to Mobile Security as Survey Reveals Sloppy Handheld Habits” at <http://www.pointsec.com/news/release.cfm?PressId=108> and “Mobile Security and Responsibility” at http://regmedia.co.uk/2006/01/31/security_responsibility_report.pdf.

Mobile Device Malware and Other Threats

Mobile devices are now, not surprisingly, the target of malware developers. Examples of malware targeting mobile devices include:

- Cabir worm appeared in 2004 as the first mobile device worm. It spreads using Bluetooth connections.
- Lasco is a worm similar but more adaptive than Cabir and spreads via Bluetooth as well as by infecting other files on a device.
- Commwarrior is a worm that spreads using multimedia messaging service (MMS) and by infected memory cards. It infects smartphones that use Symbian.

In addition to spreading via Bluetooth and memory cards, some mobile malware can be deployed from rich clients. The Cardtrp worm can infect mobile devices during synchronization.

 For details about mobile device malware, see the Mobile Antivirus Researchers Association at <http://www.mobileav.org/>.

Clearly, the same level of measures used to protect stationary clients and servers from malware should be deployed to protect mobile devices as well. Although some of the threats to mobile devices are converging with their older counterparts in stationary devices, there some unique characteristics of mobile devices that make them especially challenging to manage.

Managing Mobile Devices

Many IT organizations standardize on a set of applications, OSs, and hardware configurations, either by design or by unintended consequence. Either the management evaluates a set of applications and related platforms and chooses the best option for the organization or their options are limited by resources and skills. Once an IT infrastructure is in place, it tends to stick. Not many organizations will throw out a platform in one radical change and replace it with another. Changes tend to be evolutionary and might require support for multiple platforms simultaneously.

Similar patterns occur with the use and deployment of mobile devices with one significant difference: it is often not the IT professional that introduces mobile devices into an organization—it is professionals from throughout the company or agency who bring their personal devices into the technology mix. This has a number of implications.

The Changing Rules of IT Management

IT no longer dictates the platform used within the IT infrastructure. Some executives may have smartphones that run Symbian; others will have Windows Mobile devices. Many will use Blackberries for remote email access; others will use Palm OS PDAs for on-the-road email access. The grassroots introduction of mobile devices may be slow, but at some point, it may reach a critical mass and become part of the expected level of support.

IT is left with the responsibility for technology it may not have planned on supporting. Consider the problem of legal issues threatening to shutdown the Blackberry network in the United States. Now imagine working for an organization with executives that had become dependent on constant email access and you are expected to formulate a “Plan B” in the event Blackberry email access is not available. That is the kind of support challenge that can creep into an organization; it often starts slowly but then builds momentum. A de facto information service, whether it was planned or not, becomes the responsibility of IT departments.

Semi-Managed Devices: Employee-Owned Hardware

Another issue is that mobile devices are often owned by employees. This raises a number of management, service, and liability questions, such as:

- How much control can an IT department exercise over the use of those devices? For example, if a PDA contains information downloaded from a customer relationship management (CRM) database, would you want the employee’s child playing Tetris on that device?
- Can IT dictate certain levels of protection (for example, encryption) be used for corporate data? What data is allowed on personally owned devices?
- How much support will IT service desks provide for personal devices?
- Will IT maintain a minimum set of requirements, such as application versions and patch levels, for all mobile devices and OSs?

- Are these devices subject to the same compliance standards as company-issued devices? If so, how are policies enforced?
- Can an employer search data on an employee's personally owned mobile device if it contains even the smallest amount of business-related information?
- What are the procedures to ensure personal mobile devices do not contain confidential or proprietary information when the employee leaves the organization?

These are just some of the questions that arise when mixing personal and corporate resources. Regardless of how an organization might answer each of these questions, it is important to document policies governing the use of corporate information on personal devices. At the very least, policies should describe:

- What organizational information may be stored on personal mobile devices
- What devices can data be copied to (for example, uploaded to a home PC when synchronizing a calendar)
- The expectations the organization has to review corporate data on a personal device, especially when an employee leaves
- What security practices the organization expects with regards to data encryption and theft deterrence
- The penalties for failing to comply with the policy

Mobile devices can improve productivity and enable staff to work more effectively in a wide range of circumstances. The benefits of mobility are difficult to deny. At the same time, mobile devices introduce management challenges as well as security vulnerabilities that must be understood and addressed. Organizations should formulate policies governing the use of both corporate and personal devices, train users on basic security principals, and compensate for vulnerabilities by introducing appropriate countermeasures. Mobile devices are also part of a broader trend in fundamental changes to the network perimeter and the effectiveness of perimeter security measures.

Increasingly Complex and Porous Network Perimeters

Network perimeters are the boundaries between internal and external networks. Typically, firewalls and boundary routers are used at perimeters to control the flow of traffic; the intention is to prevent unauthorized traffic from entering while keeping internal traffic safe behind a logical barrier. This simple model was fairly representative of organization networks at one time and with some modifications for multiple layers, as in DMZ configurations. Two trends have emerged at the perimeters that make the perimeter both more complex and more porous than it has been.

The Crowded Perimeter

In some ways, network perimeters have become more complex. In addition to firewalls and boundary routers, other devices are appearing near perimeters, including:

- Intrusion detection and prevention systems
- Proxy servers
- Content filters
- Anti-malware filters
- VPN components

These devices provide additional levels of protection. For example, although firewalls are adept at determining when packets should be blocked and allowed through, they are not designed for other essential perimeter defense operations, such as blocking viruses and spam before it enters trusted zones of the network or email servers. As security threats have changed, so too have the countermeasures deployed at the perimeter.

Intrusion Detection and Prevention

Intrusion detection and intrusion prevention systems monitor networks and hosts in an effort to identify attacks. In the case of intrusion detection, the goal is to identify an attack and notify systems administrators who can then respond to the attack. Intrusion prevention, ideally, detects and stops attacks. Detection methods are based on heuristics, generally applicable rules, statistical profiles, or comparisons with known secure states.

Heuristic Detection

Heuristic detection uses a library of attack patterns to determine whether an attack is underway. For example, if a large number of TCP connection requests are made and confirmations are not received after initiating the connection, a SYN Flood attack may be in progress.

 For more information about SYN Flooding, see <http://www.cert.org/advisories/CA-1996-21.html>.

Heuristic rules have the advantage of targeting known attacks and can be effective against them, but there are limitations. Variations in attacks may be missed and new attacks will go undetected until the base of rules is updated. Statistical approaches can compensate, at least to some degree, for these shortcomings.

Statistical Profiling

Attacks against a host or a network usually represent something out the ordinary for a system. They may manifest themselves as an increase in incoming network traffic, as in a Denial of Service (DoS) attack, or an increase in outgoing traffic (for example, if a database has been compromised and a large amount of data is being stolen). In the case of an attack on a host, an unusually high CPU utilization during off hours may be indicative of a Trojan horse application stealing CPU cycles.

Watching for patterns that are out of the ordinary allows for a more customized approach to intrusion detection than found in heuristic methods. It also, though, has limitations. One of the most difficult challenges with statistical profiling is defining what is the “normal” behavior for a system.

For example, normal behavior for a particular set of servers may not entail large volumes of data being copied from several servers to a single server. This could indicate an attacker stealing data and consolidating it before transferring it out of the network. However, it could also be the nightly load of a data warehouse. If the profile of “normal” behavior included variations over a 24-hour period, the data load may not appear to be anomalous behavior. But what about activities that occur every 2 or 3 days, every week, or every month? What is the appropriate window of time for defining the profile? If the window becomes too large, the range of possible “normal” behaviors becomes so large that attacks can appear normal; if the window is too narrow, normal behavior can trigger the detection of a supposed attack.

Known Good Profiles

Known good profiles are signatures that are used to detect changes in files. These techniques are used for host intrusion detection. The basic idea is that for any known good file, such as an OS file just installed on a cleanly formatted drive, a signature is calculated. These signatures are known as message digests. These message digests are strings that correspond to the contents of a file; if the contents change, so does the message digest. Message digests are like fingerprints; they are unique and correspond to a single entity, such as a person in the case of fingerprints, or files, in the case of message digests.

The calculations used to create message digests have two very important properties. First, it is extremely rare to find two input strings (or files) generating the same output string. Therefore, it is highly unlikely that someone can make a change to a file and get the same message digest as the original. The second property is that given a message digest, it is impossible to determine what input string was used to create the message digest. Thus, one cannot determine the contents of the file from the message digest.

For intrusion detection purposes, the following procedure is used:

- Install known good files, such as is the case with a fresh operating system or application installation.
- Calculate a message digest for each known good file.
- Store the message digests in a secure file, directory, or database.
- On a scheduled or ad hoc basis, recalculate the message digest for each file and compare the result with the original result stored in the secure file, directory, or database.
- If the results are the same, do nothing; the file has not been compromised.
- If the results are not the same, then either a legitimate change has been made to the file, or the file integrity has been compromised.

No single method for intrusion detection and prevention will work well in all circumstances, but combining multiple techniques can help to mitigate the limitations of each method while benefiting from their strengths. Not all threats first manifest themselves by direct attacks on servers or networks. Some threats move as content in and out of networks.

Content Filters and Anti-Malware Filters

Information moving in and out of an organization can present a variety of threats to security and efficiency. Consider, for example:

- Employees wasting time on shopping, entertainment, or gaming Web sites during business hours
- Staff downloading offensive material that could contribute to a hostile work environment and leave the employer liable for the results
- A consultant or contractor with access to proprietary or confidential information copying it to a third-party site without their client's permission
- Trojan horses unintentionally downloaded by employees who think they are just installing a free utility program
- Email servers taxed by unwanted spam and phishing messages

To minimize these threats, content should be filtered at the perimeter as well as at the host. Multiple layers of countermeasures, known as defense in depth, help to ensure some level of protection if one of the countermeasures is compromised or otherwise ineffective.

A challenge of effective content filtering is maintaining up-to-date information about malicious software, phishing attacks, and inappropriate Web sites. Ideally, a content-filtering system will utilize:

- A realtime database of categorized Web sites, including adult-oriented, gambling, shopping, criminal activity, hate speech, and comparable sites.
- Frequently updated database of malware signatures and behavior-based detection methods
- Frequently updated database of spam and phishing signatures
- Ability to block specific programs, such as peer-to-peer file sharing and instant messaging applications

Content filters supplement the work of firewalls by examining traffic at a more aggregated level. They are able to identify threats that packet-level analysis alone cannot detect. The perimeter is also the point at which many VPNs establish an endpoint for incoming connections.

In addition to traditional content filters, authenticated email frameworks, such as the Sender Policy Framework (SPF), can help block emails that contain forged sender addresses. Within the SPF model, a sender can publish information about the servers it uses to send messages. This information is stored along with DNS information. Recipients of messages can use this information to verify that a message originated from one of the servers used by the purported sender. In addition to SPF, another email authentication mechanism is Sender ID, which is supported by Microsoft.

 For more information about SPF, see <http://new.openspf.org/Introduction>. For detail about Sender ID, see <http://www.microsoft.com/mscorp/safety/technologies/senderid/default.aspx>.

VPNs

VPNs logically extend a secured network by providing an encrypted information tunnel. VPNs extend beyond the perimeter to remote locations and allow remote users to access network services as if those users were within the perimeter. These secure tunnels use encryption to protect the confidentiality of information as well as message digests (described earlier) to protect the integrity of messages.

The perimeter of a network is an active area. A VPN is no longer just a single level of defense based on packet-level analysis and simple blocking strategies. Content filtering, encryption, and decryption at VPNs, and monitoring for intrusions are all security services that make the perimeter a much more complicated place than it used to be. Ironically, although additional security measures are making perimeters more secure, the perimeters themselves are becoming more porous.

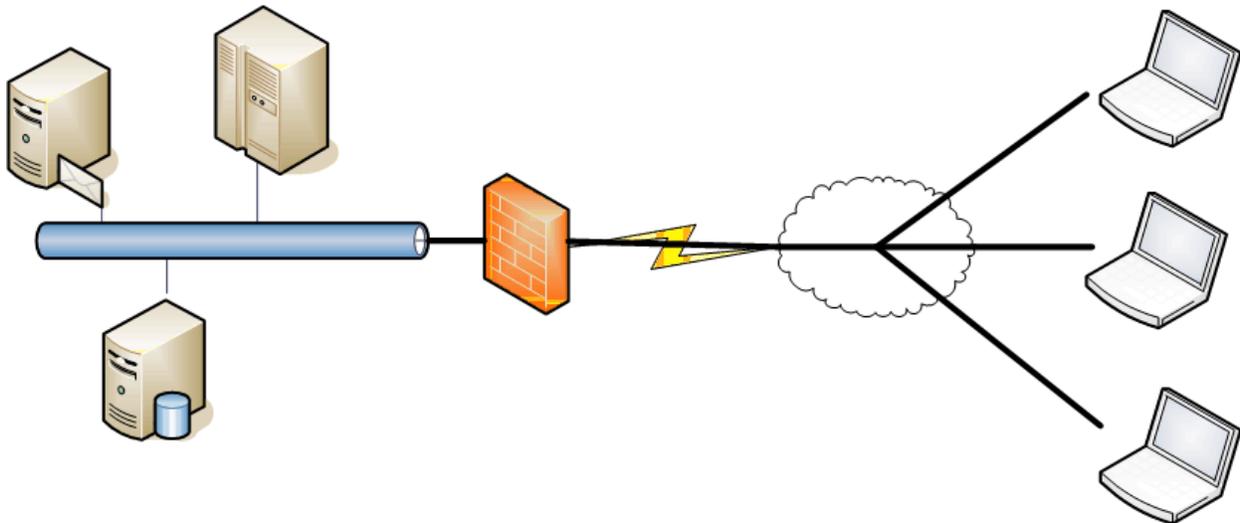


Figure 4.2: VPNs create the equivalent of an encrypted, electronic tunnel (dark lines) through the Internet for confidential communications.

Porous Perimeters

In response to growing demands for access to information resources from a variety of sources, network administrators have carefully begun to open communications channels through the perimeter. A number of methods are commonly used that essentially permeate the perimeter, including:

- VPN access
- Extended access controls
- Application access

Trusted users can access the corporate network through VPNs. This method provides the greatest access to network services but must be used judiciously. Client devices using VPNs, in some important respects, are treated as if they were physically on the network. Once packets reach the terminal VPN point and the packets are decrypted, there may be no additional security checks on the content. This can lead to problems. For example, an employee who connects to the VPN from a home computer may find that a worm that has infected his PC is now working its way into the corporate network.

Another way in which the boundaries of the network are becoming less well defined entails access rights granted to users outside the organization. For example, auditors, consultants, suppliers, and customers may all be granted access to databases, information portals, and other enterprise applications. This introduces challenges around identity management and authorizations. How will you know if an employee of your auditing firm has left the company and their access rights should be revoked? How do you control transmission of data from your managed devices to third-party devices? Extended access controls allow organizations to adapt to the particular needs of business partners and other stakeholders, but the risks should be understood and, as much as possible, mitigated.

Access to specific applications is becoming much more common, especially using Web interfaces. Traveling executives and sales representatives can retrieve email and check calendars from unmanaged devices such as hotel and airport kiosks. Customers can run form-driven database queries to check the status of accounts, orders, and other information. Like the other techniques that make the perimeter more porous, this one has its risks. For example, checking email or downloading documents to an unmanaged device may leave copies of that information in a browser cache accessible to others.

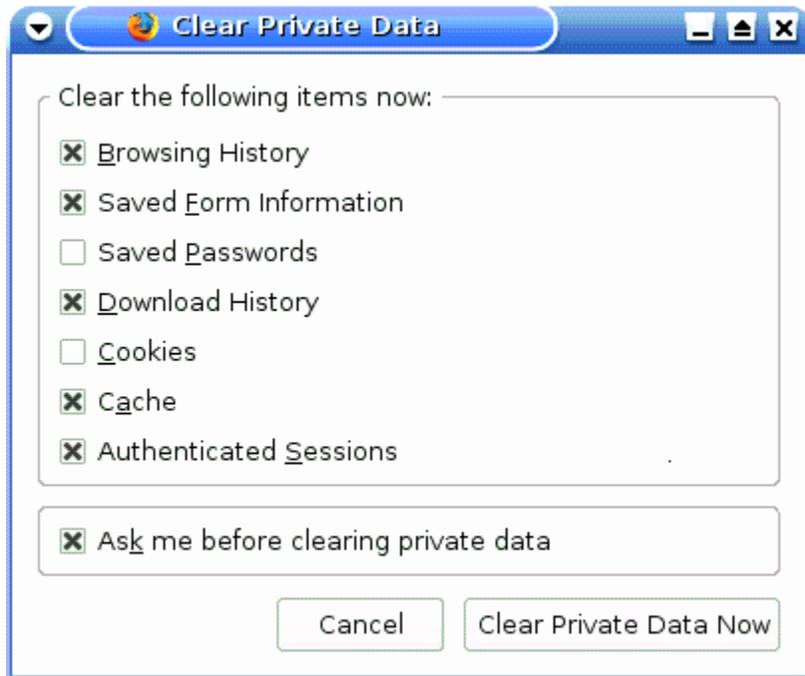


Figure 4.3: Users should be made aware of the need to clear buffer caches to prevent the disclosure of sensitive data. Browsers, such as Mozilla Firefox, allow users to remove several types of cached information.

The network perimeter is becoming more complex. In many ways, it is better protected with the use of intrusion protection and content-filtering devices. At the same time, drivers to improve service, provide more flexible access, and reduce costs are leading to a more porous perimeter. With much attention on protecting information assets from outside threats, it is sometimes easy to forget that threats can emerge from the inside as well.

Loss of Intellectual Property and Industrial Espionage

Businesses have long tried to gather information about their competitors. Often, a great deal can be learned about a business by using publicly available sources, such as government filings, press releases, articles and speeches by corporate executives, and so on. These are all legal and legitimate sources of information. Unfortunately, not everyone plays by the rules and, as the value of intellectual property increases, such data is becoming more of a target for cyber-attackers. To see evidence of the rise of intellectual property theft and economic cybercrime, consider recent changes by the U.S. Department of Justice, which according to Enterprise Government (<http://governmententerprise.com>) include:

- Adding hacking and intellectual property units in 12 cities
- Working to deploy prosecutors to Southeast Asia and Eastern Europe who will work on intellectual property enforcement
- Provided technical assistances to thousands of their foreign counterparts

Intellectual property theft can come in many forms, such as copycat goods; pirated software, music, and videos; and the unauthorized use of patented or trade secret techniques. Whenever intellectual property is embodied in a digital form and stored on devices connected to a network, and even in some cases when devices are physically isolated, it is at risk of theft.

Protecting information assets is not just about keeping the bad guys out; it is also about preventing the loss of confidential and proprietary information. An important point to remember when controlling information loss is that the thieves may come from inside as well as outside the organization. For example:

- A former technology manager for a San Jose, California company was convicted of planting a logic bomb that destroyed information about 50,000 accounts.
- A Charlotte, North Carolina man was convicted of stealing information from the America College of Physicians about 80,000 members of the association, presumably for use in his business, which sells databases to marketers targeting physicians and other professionals.
- The United States Attorney for the Northern District of California indicted a former employee of a network equipment manufacturer who left to work for a competitor. After leaving his former employer, the man allegedly downloaded dozens of files with trade secrets and other proprietary information.

 These and other examples are available at the U.S. Department of Justice Cybercrime Web site at <http://www.usdoj.gov/criminal/cybercrime/cc.html>.

What can organizations do to protect themselves? Following the basic principles of risk management, defense in depth, patch management, and backup and recovery is important. Specifically:

- Develop formal procedures for revoking access to information systems to terminated employees. Employees should not have physical or logical access to systems after they leave.
- Rotate duties and have systems administrators and others in position of authority over information resources take vacations. This will allow others to perform routine tasks, review logs, and possibly detect something out of the ordinary. Also, knowing that duties are rotated may deter malicious activity before it occurs.
- Audit access to critical servers and applications. Also audit significant changes to access control systems, such as the addition of an account with administrator privileges. Whenever possible, have an outside company perform the audit to avoid conflicts of interest or potential “insider jobs.”
- Implement backup and recovery procedures. These can be the key to recovering from malicious code or other actions which destroy online data.
- If custom software is developed in house or by third parties, conduct code reviews before deploying the code. Programmers should not have access to production servers. These measures will help reduce the chances of someone introducing a back door into a custom application.
- Use content-filtering mechanisms to ensure proprietary information does not leave the enterprise network.

Another challenge that systems and network administrators must contend with is the problem of zero-day threats.

Zero-Day Threats

Zero-day threats are attacks that are launched before software vendors and security researchers are aware of the vulnerability exploited by the attackers. By definition, there is no specific patch for the vulnerability and no targeted information about how to minimize the risk from the vulnerability. Zero-day threats are a popular topic in security discussions, perhaps driven in part by the speed with which new attacks are emerging and the seemingly never-ending stream of vulnerabilities disclosed by vendors and researchers.

Countering a zero-day threat is like planning for a natural disaster: you don't know when it will hit, how bad it will be, or what kind it will be—you don't even know whether you will ever experience one. But you can certainly be prepared minimize the effects. Some general principles apply to both situations.

First, take general precautions that can mitigate the risks of a variety of attacks. A basic backup and recovery plan will allow you to restore systems to a previous state of functionality regardless of what caused the loss of data or functionality to begin with.

 There is always the risk that malware or logic bombs that destroy data may also be on all backups as well. If the code that caused a disruption in service can be identified, backups can be checked and the code purged before returning systems to operation.

Second, implement a patch management program. Doing so might not prevent a zero-day attack but may mitigate the consequences. A common attack method is to deploy a blended threat that exploits multiple vulnerabilities. A well-patched system is less likely to be compromised by multiple attack vectors. Also remember that a non-zero day attack can be just as damaging as a zero-day threat if a system is not patched. For example, Microsoft had released a patch for the vulnerability exploited by the SQL Slammer worm months before the attack that shut down large segments of the Internet in 2003. As a result, those customers with effective patch management programs were mostly unaffected by the worm.

In some cases, intrusion detection systems may recognize anomalous behavior associated with a zero-day attack. As attacks become more sophisticated, it is less likely that a single countermeasure will adequately protect an information infrastructure. Coordinating the use of multiple countermeasures will become increasingly important.

Increasingly Complex Countermeasures

A variety of countermeasures are now deployed in enterprises that use defense-in-depth strategies. The basic tools for protecting information assets have come a long way from basic packet-filtering firewalls at the perimeter and antivirus software on the desktop. The fundamental countermeasures are now:

- Anti-malware software on the network and the desktop—this includes systems to detect and block viruses, worms, Trojan horses, keyloggers, root kits, and blended threats that combine multiple threats.
- Content-filtering systems to prevent inappropriate content from entering the network and confidential and propriety information from leaving the network. These systems also reduce the chances that network resources are wasted on non-work related activities such as entertainment and shopping sites.
- Intrusion detection and prevention systems for the network and hosts.
- Access control systems, ranging from basic OS authentication to SSO applications to identity management systems. These provide the means to identify users, authenticate that they truly are who they claim to be, and provide authorizations controlling what the user can do with particular applications and devices.
- Auditing and logging management systems. Ideally, these systems employ triggers and alerts to notify administrators when suspicious or significant events occur.

The countermeasures themselves are growing in complexity. Antivirus software, for example, used to depend on scanning content for signatures of known viruses; after virus developers created techniques to mutate their code as it replicated, antivirus developers had to deploy more elaborate behavior-based detection techniques. Complexity is also increasing because of how the countermeasures are used.

Countermeasures are more likely to be used in combinations to counter attacks, especially when diagnosing unusual events. For example, if an intrusion detection system detects a change in an OS file, the audit logs may contain related events around the same time that can provide further information about the change. That information might also lead to a review of access control audit logs indicating what identity was used to gain access to the system. As the example shows, information from one countermeasure might lead to another countermeasure's log, which, in turn, leads to another, and so on. Coordinating information from multiple countermeasures, especially in real time, is a current challenge for the information security industry.

The Future of Content Protection

Content on corporate and government networks can be categorized by three types:

- The data moving across networks represents a wide range of transactions, personally identifying information, trade secrets, proprietary procedures, strategic plans, and other economically valuable objects.
- Content for direct human consumption, such as a news feed or email message. Within this category, you also have offensive and disruptive material, such as hate speech, which has no place in a work environment.
- Content can also be meaningless packets consuming network resources for no good reason.

Organizations are adapting to the changing nature of content and the requirements of protecting information assets. The future of content protection will entail several factors:

- Improved methods for blocking unwanted content, such as spam, malware, and offensive material. The history of computer viruses has demonstrated that attackers will find a way around a particular detection method eventually, prompting antivirus designers to develop innovative techniques to identify the new threat. This cat-and-mouse game will apply to content protection as well.
- Attackers will continue to take the path of least resistance relative to the payoff. When widespread phishing scams against big name institutions became well publicized, phishers turned to masquerading as smaller businesses and targeting fewer victims. This trend toward “spear phishing” was an attempt to stay under the detection threshold of the countermeasures developed for phishing.

- Compliance and corporate government initiatives will provide strategic direction (and funding) for content protection. The Sarbanes-Oxley Act requires that measures be in place to protect the integrity of business information. As best practices develop, expect to see more emphasis on content protection.
- Disparate countermeasures will become increasingly coordinated. No single countermeasure can block all attacks; nor do they operate in a vacuum. Integrating information from multiple countermeasures is a significant challenge and will improve with time. Do not expect to see the ideal state of real time, fully integrated security management tomorrow but progress will be made to realize the goal.

Summary

This guide has examined the nature of protecting information assets on the Internet. The business case for protecting content-based assets is clear: compliance, human resource and workplace issues, and the threat of service disruption are substantial and immediate challenges facing organizations. The threats faced are evolving, often in response to protective measures. Malware is more complex, spam and phishing messages more stealthy, and the threats from inside the organization are also becoming clear. However, with proper policies and supporting procedures and the deployment of appropriate countermeasures, organizations can mitigate the risks they face every day. Of course, as the attack and disruption methods are constantly changing, organizations must constantly adapt to emerging trends in cyber threats. Fortunately, this can be done, especially as information security practices become more and more a part of normal operating procedures.