

The Rise of Greynets: Unsanctioned End User Applications and Their Impact on Enterprise Security

By **Jonathan Christensen**

Chief Technology Officer and Vice President of Products

FaceTime Communications, Inc.

Table of Contents

| | |
|--|----|
| Introduction | 3 |
| The Growth of Greynets | 4 |
| Instant Messaging | 5 |
| Web Browsing | 6 |
| The Adware and Spyware Epidemic..... | 7 |
| Peer-to-peer File Sharing in Business Networks..... | 8 |
| Legitimate P2P: Is There Such a Thing?..... | 9 |
| Security and Compliance with Greynets | 10 |
| How Even a Benign Greynet Can Wreak Havoc..... | 10 |
| Challenges in Detecting and Managing Greynets | 12 |
| Greynets Are Becoming More Evasive..... | 12 |
| Greynet Management—Requires Defense in Depth..... | 13 |
| Managing PCs (Software Restriction Policies)..... | 13 |
| Blocking at the Perimeter..... | 13 |
| Conclusion | 14 |
| About the Author | 15 |

Introduction

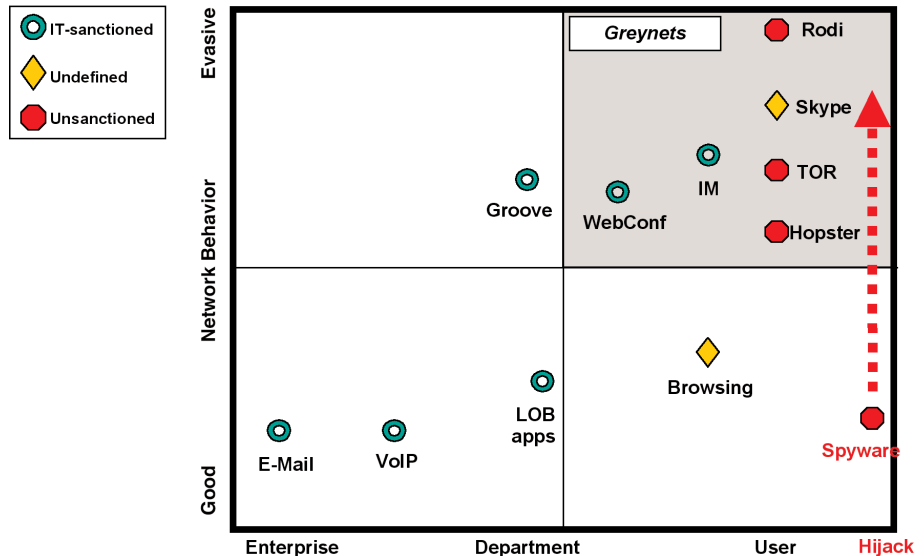
A “greynet” represents a network enabled computer application that is downloaded and installed on an end user’s system without expressed permission from IT administrators.

Enterprise information workers are using corporate PCs, internet connectivity and an emerging class of applications to communicate and conduct business online. Many of these applications are “showing up” on end users’ PCs from external download sites. Many are consumer-oriented applications such as instant messaging (IM) and peer-to-peer (P2P) file sharing. Some have been purpose-built for business use by third party service providers—such as web conferencing services, adware and spyware applications—and can be easily installed without corporate IT consent. FaceTime Communications calls these applications “Greynets.”

A “greynet” represents a network enabled computer application that is downloaded and installed on an end user’s system without expressed permission from IT administrators. Greynets are frequently evasive to existing network security defenses, using techniques like port agility and encryption to avoid being detected and blocked. There are multiple reasons for the evasive behavior, many of which will be discussed in this paper. This paper will also address the growing security threats that accompany the adoption of greynet applications in the enterprise environment.

Greynet examples include public instant messaging (AIM, MSN, Yahoo!), adware “Utilities,” P2P file sharing clients, anonimizers and remote control utilities and web conferencing. (See Figure 1).

Figure 1
Greynet Landscape



When greynets are installed ad hoc on the desktop by employees, this can create numerous security problems for the entire enterprise:

- Security** Greynets expose vulnerabilities and become vectors for malware distribution
- Privacy** Greynets establish undetectable outbound communication connections and allow holes through which sensitive corporate information may leak
- Compliance** Greynets establish invisible and unmanaged communication networks that corporate employees may use (or misuse) for business communications

No matter their origin, greynets all share a few common characteristics: They are adopted directly by end-users who install them in a “download-and-run” manner and once installed, they bypass corporate security and allow users to evade established rules and network use policies. Regardless of IT corporate edicts against unauthorized downloading of software onto PC’s, either for business reasons or to prevent unintended “drive by,” greynet applications are part of the landscape of modern enterprise networks and IT managers need to develop capabilities that allow good greynets and defend against malicious ones.

The Growth of Greynets

Greynets are now virtually everywhere in the corporate business computing environment. More than 90% of enterprises have public instant messaging (IM) use at rates that are approaching 50% desktop penetration (source: Osterman Research). More than 70% of the enterprises surveyed by FaceTime have peer-to-peer (P2P) file sharing applications running on their networks. Adware utilities are infecting desktops at epidemic levels, overburdening help desk functions, threatening information security, and resulting in damaging productivity loss.

It is important to consider the motivations behind greynet use to understand what drives this explosive growth. But keep in mind that, as the following list shows, some greynet applications provide important business value, others are a nuisance and some pose grave security threats.

| | |
|---|---|
| Instant Messaging and Soft Phone (e.g., Skype) | Private communications, collaboration and productivity |
| Web Browsing | Business research and fact gathering |
| Peer-to-Peer file transfer | Multimedia entertainment and efficient data transfer of large files (e.g., software images) |
| Web Conferencing | Sales meetings and collaboration |
| Blogging and Webmail | Private unmonitored online communications |
| Adware/Spyware Utilities | Very few of these provide legitimate business benefits, but nonetheless users are often “tricked” into installing these applications or they are automatically installed without user knowledge |

Instant Messaging

Public instant messaging (IM) is one of the fastest growing greynets today. The rising adoption of IM is fueled by the community effect inherent in IM networks. What started as a way for consumers (mostly kids) to stay in touch online has evolved into a business critical application that link vendors and customers together in revenue generating relationships. Three networks (AOL, MSN, Yahoo!) dominate the IM scene but there are as many as 25 smaller IM networks and clients. Many of these variants aggregate connections to existing IM networks, giving users the ability to log in to multiple networks with a single client application (notable among these are Trillian and the open source application GAIM).

Another IM greynet that has shown unprecedented growth is Skype (www.skype.com). Skype combines IM, voice over IP (VoIP), and file transfer. Skype is built on a proprietary peer-to-peer protocol that is very similar to the popular Kazaa file sharing application.

The Web has become the largest application to embody all the elements of the greynet concept.

Skype is at the vanguard of innovation in internet collaboration. Its differentiators include:

- Excellent and reliable voice quality
- Full featured IM and file transfer
- Built in NAT and firewall traversal
- Private/encrypted communications
- Inexpensive phone calls

Skype is quickly becoming valued as a communications tool for businesses with remote offices, teleworkers, and distributed sales forces. Low cost telephone calls make Skype especially attractive in geographies where flat rate telephony plans are not yet the norm (e.g. AsiaPac and EMEA).

In early 2005, Skype exceeded 100 million downloads and reported more than 20 million registered users. While Skype is a very promising collaboration application, it also presents new risks to IT departments. The Skype infrastructure cannot be integrated with IT control mechanisms. Corporate authentication and identity management are not supported. Bandwidth utilization cannot be managed for Skype users, and virus writers have already begun setting their sites on the Skype client. Even detecting which systems are Skype-enabled is difficult because the underlying network protocol is proprietary and evasive:

- Its P2P underpinnings mean that Skype connections are made to an infinite set of destination IP addresses (they appear to be “random” from the perspective of a network traffic analyzer).
- The Skype data payload for voice, instant messages, and file transfers is encrypted and therefore cannot be examined for policy violations.
- The Skype client does not conform to application policy management frameworks that are included in other enterprise class applications (e.g. Active Directory or other software usage and application policy managers).

In November of 2004, Internet security firm Secunia issued a “Highly Critical” security alert regarding Skype (<http://secunia.com/advisories/13191/>). The flaw exposed malicious Skype users who might want to compromise other users’ systems. This Skype vulnerability was patched quickly and there was no evidence of attack or compromise. All applications pose some risk; however, the issue that compounds the danger of Skype for IT managers vs. other applications is that Skype is not monitored or controlled by the IT infrastructure.

Web Browsing

The Web has become the largest application to embody all the elements of the greynet concept. It is the richest source of information ever assembled and at the same time it contains content depicting the darkest elements (images, viruses, etc) of the human experience. Web browsing in the corporation usually happens in a manageable context.

In most cases, browsers connect to sites over well known ports (eg. port 80) and through approved network elements such as a firewall or proxy server. Many corporations deploy URL filtering tools on these devices to monitor or restrict HTTP access to categories of content that may be deemed inappropriate—such as pornography. These same solutions are sometimes used by foreign governments to restrict and censor access of entire nations (nationalized ISPs). In both cases, the end user is confronted with restricted access. To counter this set of HTTP controls, many software applications have focused on providing tools that circumvent this monitoring (sometimes called “censorware”). As an example: TOR is an application that was written explicitly for this circumvention purpose (<http://tor.eff.org/>). TOR is an “onion router”—a network layer software shim that encrypts and re-routes application traffic in order to disguise it and bypass restrictive policies and monitoring. This means that any web browser coupled with TOR (or any similar tool) becomes an evasive greynet application. It bypasses corporate security controls and exposes the organization to risk.

The Adware and Spyware Epidemic

“Adware” and “Spyware” are relatively new terms that are used almost interchangeably to describe software that uses a deceptive hook or drive-by installation to get installed on a user’s PC and then, based on user activity, presents pop-up ads and/or sends confidential information to a “phone home” server. While some experts are more clinical in their definitions (see www.spywareguide.com for more info), all agree that the majority of infections today are cases of unintended installations. Adware is exactly what its name indicates; it puts unwanted advertisements on the user’s PC screen. The most sophisticated versions of adware collect information about a user’s browsing or shopping habits and use this information to deliver ads in a highly targeted manner. This is why these applications are often referred to as “spies.” If an infected user browses to Blockbuster.com, for example, the adware application might display a competitive promotion pop-up advertisement from Netflix.

To get broad distribution and installation, adware/spyware makers use highly deceptive and unethical methods to get their code onto users’ systems. Adware is often accompanied by an application or utility that the user is tempted to download. Some common examples are:

- Third party internet search bars
- Time synchronization utilities
- Wallets and form filling applications
- Weather trackers
- P2P file sharing applications

The most common adverse effect of adware infection is system performance degradation and the associated loss of end user productivity and help desk costs to remedy the situation.

Once installed, adware can be very difficult to remove. This is because adware makers take pains to have their applications persist on the user's system. There is a strong economic incentive to stay resident on the users' PCs. Each adware installation is being used to promote products as part of a paid advertising campaign. The adware makers are compensated based on the effectiveness of these campaigns.

To gain broader distribution adware is often bundled with other popular applications (e.g., P2P file sharing applications like Grokster). These "Trojan" applications are often freeware and lack sustainable business models. Adware provides a new business model. Perhaps the most annoying thing about these freeware applications is that the bundled adware installs itself without the user's informed permission or knowledge. Adware vendors are notorious for being stealthy, deceptive and unethical.

The risks exposed by adware include:

- Spyware: Rogue applications that allow unmonitored code to run on enterprise systems. A strong case can be made that the identity systems employed by the enterprise community have been defeated by spyware attacks.
- System vulnerabilities that can be exploited by malicious users, much like any other host-based code.
- Collecting and sending private data out of the organization

However, the most common adverse effect of adware infection is system performance degradation and the associated loss of end user productivity and help desk costs to remedy the situation. As part of its greynet research effort, The FaceTime IM and P2P Activity (IMPact™) Team has installed and analyzed hundreds of adware applications on test systems in the IMPact labs. Frequently these test systems show substantially degraded performance after adware is installed; occasionally these infected systems become completely unusable as the adware programs compete for system CPU and memory resources. This is a case where the parasite effectively kills the host.

Peer-to-peer File Sharing in Business Networks

P2P is not just a consumer phenomenon. It is being installed by end users on business PCs and running over corporate networks. A recent survey by AssetMetrix & the RIAA found that 77% of all businesses in North America had P2P file sharing installed and running in their networks. On average they found almost one in ten desktops had P2P applications installed.

Bittorrent is a relative newcomer to the P2P arena, but it has already made a huge impact on the media industry, ISP networks, and software distribution models. Because of its unique properties, Bittorrent is an efficient way to distribute very large files. This has made it the most popular P2P protocol for distributing digital copies of pirated movies.

**Legitimate vs. Malicious
Use of Greynet Applications**

Legitimate P2P: Is There Such a Thing?

At first glance, there does not seem to be any legitimate use case for P2P in corporate networks. However, P2P has advantages that apply to business applications as well. Because P2P file sharing is fully distributed, it does not require an expensive central infrastructure. The new economics of P2P networking mean that it is also used increasingly as an efficient digital distribution channel for legitimate purposes. These applications include:

- Distribution of OS software images (e.g. the DVD image of popular Linux distributions like Fedora Core are too big to transfer over traditional means such as email or disc)
- Broadcast feeds for RSS syndicated content (e.g. Podcasts)

| Application | Business Value | Corporate IT Threat |
|--|--|--|
| Public Instant Messaging (such as AOL or YAHOO) | Real time communications with business partners, customers and colleagues increases productivity, reach, and service levels. | Most rapidly adopted communication tool in history. Viruses and worm infections and other spIM threats to grow to 17.9 billion messages in 2008. |
| P2P File Sharing | Download large files quickly (e.g. OS updates). | P2P file sharing is predominantly used for illegal “swapping” of copyrighted materials. Viruses, spyware and other malware are distributed as trojans in many of these files. |
| Web Conferencing | Real time collaboration with business partners, virtual teams and customers. Increases productivity, reach and service levels. | Most web conferencing use occurs in an unmanaged state. The IT and compliance department do not have access to inspect content nor do they control how users identify themselves to external parties when they are using web conferencing. |
| Web Browsing | At-your-fingertip research and commerce for business efficiency. | Largest vector of spyware infections. |

Again, Skype is another P2P application that provides legitimate use scenarios for business users. While Skype does not conform to typical IT deployment and management norms, it is arguably the most cost effective voice and data collaboration tool in mass distribution today. It is only a matter of time before the P2P architecture is used for low cost web conferencing and other business communications applications.

This means that it is not sustainable for businesses to block all forms of P2P. At first, there will be a few exceptions for “power users” and special business cases. Then legitimate P2P will spread to a broader user base as application scenarios proliferate. Legitimate P2P greynets offer a good example of how the line blurs between bad and good; black and white.

Security and Compliance with Greynets

Greynets are innovative and use an ever-evolving set of unanticipated actions to circumvent the security infrastructure.

Not all greynets are malicious (though at this point many are). However, by their nature, good or bad, greynets try to avoid detection. Greynets are innovative and use an ever-evolving set of unanticipated actions to circumvent the security infrastructure. Legitimate and responsible use of many of these applications is possible but it is important to note a few things that apply:

- Greynets are evolving in “Internet time” while security infrastructure is being adjusted in “fiscal time.” Greynet development is being funded by large, profitable, public companies. The technology base for greynets is expanding rapidly.
- Greynets were not designed for IT and greynet developers are not beholden to IT. Greynets are designed to connect by evading IT security.

It is important to note that all applications have inherent risks—even greynet applications that may have useful business value. Perfect code is nearly impossible to find, so every new application in an environment should be handled with care. Greynets are complex interconnected applications. They introduce new variables into the IT security equation and this additional complexity is the enemy of good security. Greynets introduce new untested and uncontrolled code segments onto hosts and into the LAN environment. These applications are both interconnected internally and externally connected to other instances of the same code and/or to services running even more code. Frequent vulnerabilities have already surfaced in greynet host applications.

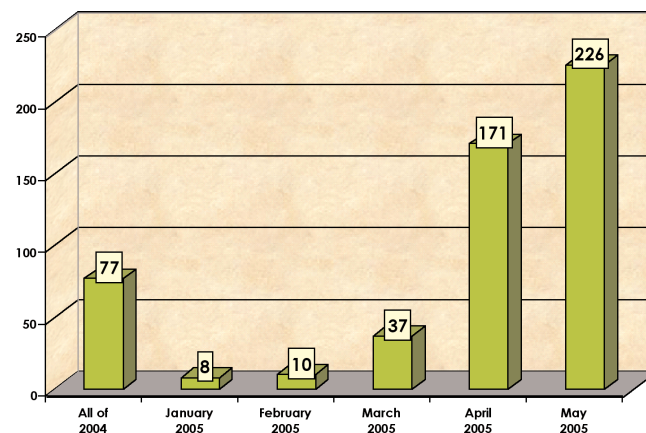
If these greynet host applications can be compromised, their network connectivity can create a spanning vector for the distribution of malicious code. This has been demonstrated with IM worms (e.g. Funner, Kelvir, Bropia). This external connectivity can also be used to leak proprietary information.

How Even a Benign Greynet Can Wreak Havoc

The risks posed by unmonitored adoption of greynets do not depend on bad employees or malicious actions by those employees. Take for example the spread of public IM in a given enterprise. (See Figure 2). Suppose that all of the users in that setting are acting responsibly and according to corporate policies. Everything is going well until a new IM borne worm/virus breaks out. The worm attacks systems with up-to-date virus

signatures, steals and corrupts local data, and transmits sensitive data to the attackers. If this worm were spreading on the corporate email system, it would be possible to isolate it quickly and shut down the vector of transmission. If this worm were spreading over a P2P IM system like Skype, it would be nearly impossible to isolate it and shut down.

Figure 2
Number of IM, P2P
and Related Threats
Reported by FaceTime
IMPact Center



This illustrates that with all that is good about public IM services and new P2P applications from the perspectives of productivity, communication, and collaboration, there is a darker side. The same is true of other greynets. The only possible conclusion is that greynet adoption in the enterprise poses a number of security risks. Here are some examples:

- A 400% increase in viruses, worms and trojans over IM and P2P in last 12 months (Source: SYMC)
- 3 of the top 10 Windows vulnerabilities are IM, P2P or browser-based (Source: SANS)
- Projected 1.5 billion SPIM messages by end of 2004. Growth rate 3x that of SPAM. (Source: Radicati)

Greynet communications in the enterprise environment also pose significant regulatory compliance and policy risks. This exposure spans numerous industry verticals and regulatory environments and includes SEC, NASD, HIPAA, FERC, SOX, and DoD regulated entities:

- 2003-4: \$1.8B in fines and settlements for electronic messaging compliance and audit violations in SEC and NASD regulated companies
- Spyware and phishing at epidemic levels—the top 2005 CIO concern
- P2P file sharing with copyrighted materials liability increasing
- Estimated loss of \$59B in IP & proprietary data between July 2000-June 2001

While new and innovative tools like Skype are providing real benefits to users and IT, it is unfortunate for IT managers that Skype is a closed and proprietary grey network. This means that once adopted by users it cannot be controlled by IT. Users create their own identities and personas in the Skype network. All Skype traffic is encrypted and cannot be monitored or audited. File transfers over Skype cannot be scanned for viruses or checked against corporate policies (e.g. file size, type, extension.).

Challenges in Detecting and Managing Greynets

More than 90% of all enterprise environments tested by FaceTime are vulnerable to greynet infiltration.

More than 90% of all enterprise environments tested by FaceTime are vulnerable to greynet infiltration. These environments lack the tools to detect and apply consistent policies regarding application distribution and use. Even now these include some of the largest and most secure corporate and government network environments in North America.

Readers may wonder how these applications became so prevalent in private networks—or why they are so hard to control. The simple answer is that the tools and infrastructure have fallen behind the innovation curve of greynet developers.

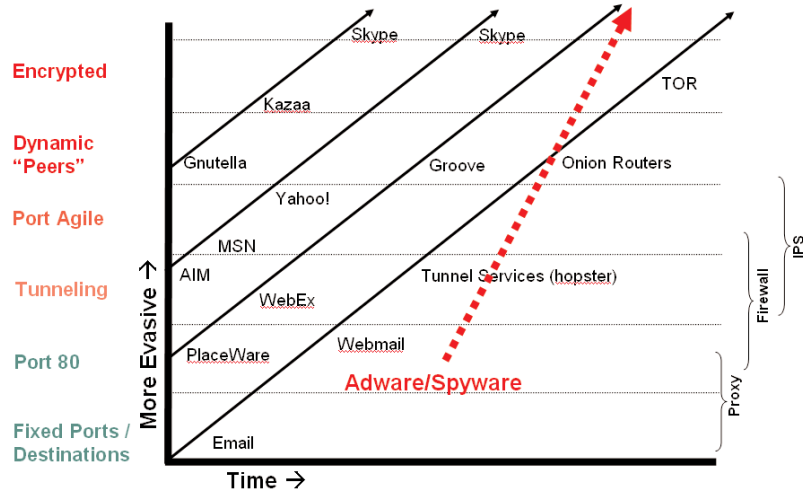
Greynets Are Becoming More Evasive

P2P application developers are leading innovators in the charge to create “private and invisible” network applications. P2P content distribution makes economic sense and represents the current state of the art in greynet development. The evasive nature of P2P is in the user’s interest because anonymity is especially appealing when a user does not want to be seen using the application in question (e.g. illegal file sharing). Experts note that P2P users actively migrate between applications based on the reputation for maintaining the privacy of their users. The emergence of popular P2P technology on the Internet is a significant sea-change that will have ongoing effects on networked applications and this evasive network behavior is being adopted by all of the greynets:

- P2P overlays are here to stay: they will be used by more greynet applications because P2P offers huge cost advantages vs. traditional download distribution models. Take the new techie trend of “podcasting” as an example: podcasting combines independent audio programming with RSS to create internet radio programs that users can subscribe to and listen to anywhere they choose. The podcaster’s RSS syndicated mp3 files are being distributed over P2P via the Bittorrent functionality that is built into podcasting software (www.ipodder.org).
- Greynet traffic will be encrypted because encryption offers privacy and “security” to users.
- All greynet applications will adopt evasive network behavior because it allows the applications to work where IT or ISP administrators are attempting to block or limit them.

Already the evasive trend in P2P networking is taking hold more generally across all greynet applications. As greynets are targeted for control and management by corporate and ISP network administrators they will adopt the evasion techniques of the P2P applications and become increasingly harder to detect at the network level. (See Figure 3.)

Figure 3
Greynet Applications Are
Becoming More Evasive



Greynet Management—Requires Defense in Depth

Effectively managing greynets requires a multi-layered investment in both technology and business practices. IT needs to start by implementing coherent policies and developing education programs for promoting awareness. Then there are the infrastructure investments necessary to provide end-to-end control and security.

Managing PCs (Software Restriction Policies)

Controlling host systems in large environments can be a daunting task. While many organizations have the means to push out and add software to the desktop, few are able to strictly limit what is installed and executed on end user machines. Even where strict policies are enforced, exceptions are made and holes exist. Most of the popular greynet applications do not require administrator access to the host to be downloaded and installed. Others use Java or browser-based access. New techniques are required for managing software proliferation at the desktop.

Blocking at the Perimeter

Most enterprise environments have adopted a “best-of-breed” mix of security infrastructure. Firewalls, application proxies, and the more recent addition of Intrusion Prevention Systems (IPS) may seem to be enough to filter out the undesired greynets. Unfortunately, blocking greynet adoption at the network perimeter is nearly impossible using today’s security products. This is because greynets specifically are designed to exploit known structural gaps in that infrastructure.

▶
Structural Gaps in Existing Solutions

| Network Elements | Intended Purpose | Security Risks |
|------------------|--|--|
| Firewalls | Manage flow by address, port and flow direction | <p>Greynets use any available open port</p> <p>Greynets do not have fixed address destinations</p> <p>Greynets initiate connections from the inside out; firewalls are generally more permissive/porous</p> |
| Proxies | Manage protocol adherence and enforce policies having to do with black-listed or white-listed destination addresses (e.g. no browsing www.playboy.com) | <p>Greynets mimic valid applications at the protocol level</p> <p>Greynets change their network address schemes faster than blacklists can be updated</p> <p>Greynets use P2P connection overlays that utilize an infinite set of destinations to conceal where they are going</p> |
| IPS | Scan packets looking for matches against static signatures e.g. text strings in packet headers or data payloads) | <p>Greynets connect to an infinite, always changing and seemingly random set of destinations making the IP destination information in packet headers useless</p> <p>Greynets conceal their data payloads with proprietary encryption schemes</p> |

Monitoring and managing greynets requires new tools and a new approach. FaceTime has a singular focus on the emerging area of greynet management. Our dedicated research and customer feedback loop has led to significant breakthroughs in delivering a defense-in-depth solution to secure and enable greynets.

Conclusion

Today greynet applications are deeply embedded in the computing structure of corporate networks where they offer new benefits, but at the same time they represent new vectors for threats. Because of their highly evasive nature, greynets have evolved into a parallel application network overlay that IT can't see, can't manage, and can't control. The preponderance of existing security infrastructure provides little more than a comfort blanket. IT success in the era of greynets will be defined by those who understand how these new technologies operate, and deploy defenses that are designed to stop them.

FaceTime (www.facetime.com) is dedicated to researching and developing products that give IT the tools needed to effectively manage and control greynets.

About the Author

Jonathan Christensen is chief technology officer and vice president of products at FaceTime Communications (www.facetime.com), provider of security solutions for the management and control of greynet applications. Jonathan has more than a decade's worth of expertise shaping growth strategies and delivering technology solutions for major corporations such as Microsoft Corporation and Time Warner. He is known as a visionary for his work in Microsoft's Real-Time Communications (RTC) group as overall program manager for global technology partnerships. He was also a founding member of Microsoft's "Greenwich" project for enterprise IM.

Prior to joining Microsoft, Jonathan held management positions at Time Warner, where he pioneered commercial Internet services including access, hosting, and Web design. He was also instrumental in bringing to market the first generation of consumer broadband services.

Jonathan is a regular speaker at numerous security forums including RSA, Vanguard Security Expo and VON.



FaceTime Communications, Inc.

1159 Triton Drive • Foster City, CA 94404

| | |
|---------------------|--|
| Toll Free | 888.349-FACE (3223) |
| Phone | 650.574.1600 |
| Fax | 650.574.2700 |
| General Info | info@facetime.com |
| Sales | sales@facetime.com |