



Vendor Corner

The Ethics of Interception

By Simson Garfinkel
CTO, Sandstorm Enterprises, Inc.

“**W**ith great power comes great responsibility” was the theme of last summer’s blockbuster movie Spiderman. But as any IT administrator knows, the reverse also is true. When it comes to computer systems and network management, with great responsibility comes great power.

Since the dawn of timeshare computing, system managers have had the power to read, modify or even delete their users’ documents. When it comes to email, today’s administrators can read or divert email messages, with or without the knowledge of the intended recipient. Unscrupulous managers can even inject fraudulent messages into the data stream that are all but indistinguishable from legitimate ones. Network administrators have more power still: they can intercept email that merely passes through their network, they can create detailed reports of an employee’s web surfing habits, and they can even capture plaintext usernames and passwords that are commonly used on the Internet today.

With today’s heightened attention towards security, much has been said of how these powers can be used to assist law enforcement agencies and help root out terrorists. Surprisingly little has been written of how these same powers can be systematically abused by administrators to satisfy their voyeuristic urges, to harass fellow employees, or even to plan terrorist attacks.

Technologists have traditionally seen encryption as the primary tool to guard against unauthorized snooping. It doesn’t matter if an encrypted e-mail message is intercepted, in theory, if only the authorized recipient can understand the content. Digital signatures can be used to prove the authenticity of an e-mail’s author. Technologies like VPNs and IPsec can hide a person’s browsing patterns. Meanwhile, cryptographic protocols like Secure Shell (SSH) and Secure Sockets Layer (SSL) can protect

passwords, keystrokes, credit card numbers, and even stock quotes.

But unbreakable encryption is a double-edged sword. While SSH certainly protects passwords from an attacker, the cryptographic cloak can also be used as a cover for nefarious activities.

The existence of this double-edged sword was one of the driving motives behind the US Government’s “Clipper Chip” initiatives in the 1990s. Uncle Sam (or at least the FBI and the NSA) wanted all Americans (and indeed, the rest of the world) to base the security of the Internet on a classified 80-bit encryption algorithm called Skipjack. Instead of implementing the algorithm in software, the US government wanted us to use hardware encryption modules manufactured in a classified facility. And most important of all: government officials wanted the encryption system to have a back door, so that the FBI and the NSA could instantly decrypt any encrypted message, as needed.


The Clipper proposal failed, as did all of the government’s follow-up proposals. These proposals were rightly seen as too invasive and too expensive. Even attempts to revive Clipper after 9/11 failed. The Clipper Chip wouldn’t have prevented 9/11 because the alleged attackers weren’t using encryption to thwart court-ordered wiretaps. As near as anybody can tell, there weren’t any wiretaps in place in the weeks leading up to the terrorist attacks.

Yet the need that Clipper addressed is actually more acute today than ever before. That’s because unbreakable encryption is increasingly the rule in today’s enterprise. And when such encryption is in place, there is no effective tool for monitoring and auditing the actions of system and network administrators. It’s widely acknowledged that the mere act of monitoring network users acts as a deterrent to undesirable behavior. But who watches the watchers?

While Clipper is dead, some of the principles that Clipper embodied are just now coming into the marketplace. Sandstorm’s NetIntercept

network monitoring system, for example, has the ability to decrypt and eavesdrop upon encrypted SSH and SSL servers using a “key escrow” system that is somewhat similar to what the US Government proposed in its original Clipper proposal. But unlike Clipper, this system is controlled by the enterprise and can be used for its own purposes - be they securing the network infrastructure, supervising the actions of network administrators, or even debugging cryptographic protocols that don’t seem to be operating properly.

This advances the levels of cryptographic protection to a new level, where companies can have secure communication with their servers, yet still have the access needed to check on the activities of employees with encrypted connections. By creating tiered access levels, and redundant or multiple forms of monitoring, the watchers can be watched, and more importantly senior programmers with root access will be leaving a trail that can be decrypted and open to audit.

In far too many organizations, administrators have been able to wield great power without the corresponding responsibility. Applying the time-tested tools of auditing and accountability to administrative activities will go a long ways towards correcting this imbalance. 

Special Thanks to our
ISSA sponsors:

Gold Sponsors:
Alta Associates
(ISC)²

Silver Sponsors:
Computer Security Institute

Bronze Sponsors:
CyberGuard
CRC Press
PestPatrol, Inc.
Security Awareness, Inc.
Systems Experts Corporation
TruSecure