Testimony of Professor M. Eric Johnson

Director, Center for Digital Strategies
Tuck School of Business
Dartmouth College

Before the

Committee on Oversight and Government Reform

United States House of Representatives

on

Inadvertent File Sharing Over Peer-to-Peer Networks

July 24, 2007

Introduction

Chairman Waxman, Ranking Member Davis, and members of the committee, it is an honor to testify before you today about this important national security issue.

Peer-to-peer (P2P) software clients have become part of the standard suite of PC applications for many users. With millions of users world-wide sharing music, video, software, and pictures, file movement on these networks represents a significant percentage of internet traffic. Beyond the much discussed copyright infringement issues, P2P networks threaten both corporate and individual security. Our research shows that confidential and potentially damaging documents have made their way onto these networks and continue to do so. The research also shows that criminals trawl P2P networks and opportunistically exploit information that they find.

You might wonder why a business professor is studying P2P security threats? First, let me be clear that I have no financial stake in the P2P security industry nor have I accepted any funding from the recording industry. I became interested in P2P security risks as part of my ongoing research on information security in large corporate enterprises. My research center, the Center for Digital Strategies, at the Tuck School of Business at Dartmouth, is focused on the problems facing Chief Information Officers (CIOs) in global 1000 firms. In 2002, we founded, with Cisco Systems, the Thought Leadership Roundtable on Digital Strategies to bring together CIOs to discuss shared business problems. Over the past five years, security and trust have consistently been at the top of many CIOs agendas. So, as part of the I3P research consortium and through grants from the Department of Homeland Security (DHS), NIST, and the Department of Justice, we have been researching the challenges of information security in large extended enterprises. With the DHS funding, have been conducting workshops for Chief Information Security Officers (CISOs) and driven by the key issues raised in those discussions (Johnson and Goetz 2007), we have focused much of our attention on information leakage and inadvertent disclosures. Today, we examine a common, but widely misunderstood source of inadvertent disclosure: peer-to-peer file sharing networks.

In the next few minutes, I will summarize the results of two of my recent and forthcoming research articles, published in peer-reviewed, scientific publications (Johnson et al 2007, Johnson and Dynes 2007). First, to illustrate the threat of P2P file sharing, we ran a set of "honey-pot" experiments in conjunction with Tiversa, Inc. We posted the text of an email message containing an active VISA (debit) number and an AT&T phone card in a music directory that was shared via Limewire. We observed both the activity of the file on our client and further tracked the file's movement across the P2P network. The file was quickly taken and retaken by a number of different clients. By the end of one week, the VISA card was used and its balance depleted. We observed its use through the account's transactions statement posted by VISA on the web. Not knowing the exact balance of the card, the taker(s) used Paypal and Nochex (both processors of online payments) to drain funds from the card. It appears that two takers of the card were able to obtain funds as the activity was split into two groups and because one taker used Paypal, which is more US-centric, while the other used Nochex, which is UK-centric. Within another week, the calling card was also depleted. Examining the call records of the card, all of the calls were made from outside of the US to two US area codes - 347 (Bronx, NY) and 253 (Tacoma, WA), illustrating the P2P threat both within and outside of the US. Even more interesting, long after we stopped sharing the file, we observed the file continuing to move to new clients as some of the original takers leaked the file to others.

In a second study, we examined bank-related documents we found circulating on P2P networks over a two-month period. Focusing on the Forbes top 30 US banks, we collected and analyzed both user-issued searches and leaked documents. First, we found an astonishing number of searches targeted to uncover sensitive documents and data. For example, user-issued searches for “bank of america database”, “wachovia bank online user id”, or “citi bank balance transfer.” Keep in mind, these were searches issued in music-sharing networks – not the world-wide web. Such directed searches were clearly issued with the intent of finding confidential information. Next we examined thousands of bank-related documents circulating on these networks. Many of these documents were customer-related, leaked by the customers themselves, such as bank statements, dispute letters, and completed loan application forms. Typically these docuements contained enough personal information to facilitate identity theft and fraud. We also found business documents leaking from bank employees and suppliers including performance evaluations, customer lists, spreadsheets with customer information, and clearly marked confidential bank material. For our sample of banks we analyzed tens of thousands of relevant searches and documents. We found a statistically significant link between leakage and firm employment base.

We also found that for many firms, coincidental association with a popular song, brand, or venue represented another problem we call “digital wind.” Millions of searches for that song increase the likelihood of exposing a sensitive bank document. Either by mistake or by curiosity, when these documents are exposed, they are sometimes downloaded to other clients, thus spreading the file and making it more likely to fall into the hands of someone who will try to exploit its information. For example, someone looking for a live performance from the Wachovia center would also likely find documents related to the bank. Likewise, the popular music rapper PNC creates wind for PNC bank. Such "digital wind" increases the P2P security threat for many organizations.

We believe that P2P file sharing networks represent a significant and poorly understood threat to business, government, and individuals. Given the nature of the threat, we would argue that many individuals may be experiencing identity theft and fraud without ever knowing the source of their misfortune. Furthermore, we see many of the current P2P trends increasing the problem. We urge both corporate executives and government officials to educate themselves and their constituencies to the risks these networks represent.

References

Johnson, M. Eric and Eric Goetz (2007), "Embedding Information Security Risk Management into the Extended Enterprise," *IEEE Security and Privacy,* May-June, 16-24.

Johnson, M. Eric and Scott Dynes (2007), "Inadvertent Disclosure: Information Leaks in the Extended Enterprise," *Proceedings of the Sixth Workshop on the Economics of Information Security*, Carnegie Mellon University, June 7-8.

Johnson, M. Eric, McGuire, Dan, and Nicholas D. Willey (2007), "Why File Sharing Networks Are Dangerous," forthcoming in *Communications of the ACM.*