IP Bouncer: An End-User Network Privacy Enhancing Tool

Emergent Research Forum papers

Gregory J. Bott
Mississippi State University
gjb60@msstate.edu

Robert E. Crossler
Mississippi State University
rob.crossler@msstate.edu

Abstract

Internet Protocol (IP) Bouncer is a novel Information Technology (IT) artifact that exposes unexpected and unwanted network communication initiated by trusted "insider" applications. It closely follows design science guidelines illustrated in the five design principles of the artifact. One of the novel aspects of the design is the key-pair approach used for assessing appropriate or inappropriate network communications. By coupling the context-awareness of the user with online aggregators of blacklists, IP Bouncer offers greater individual and organizational security protection and earlier detection of network anomalies.

Keywords (Required)

Design science, information privacy, IT artifact, information security

Introduction

The General Accounting Office and the United States Computer Emergency Readiness Team reported an eleven hundred percent increase in security incidents at federal agencies from 2006 to 2014 (US General Accounting Office 2015). All indicators point to continued increases in the frequency, severity, and impact of computer security attacks. Security resources are focused externally: advanced firewall protection, detection of denial of service attacks, and intrusion detection systems (Crossler et al. 2013).

Although external focus is warranted, trusted "insider" applications also increase vulnerability and must be monitored. However, current technology and processes are not designed to capture the specific key-pair context of application and network destination required to determine potential threats or anomalies. Insider applications are typically assessed once, and either denied access immediately (e.g., malware) or trusted indefinitely. Indefinite trust of insider applications and the ability for those applications to initiate connections to external hosts is an unexplored, and potentially significant, security risk.

Using technology threat avoidance theory (TTAT) (Liang and Xue 2009), protection motivation theory (Rogers 1975, 1983), and two dimensions of computer self-efficacy, a novel network application monitoring artifact is presented. This artifact increases insider application accountability, network communication visibility, and helps identify and report trustworthy, untrustworthy, and suspicious network activity.

Many applications require some form of external network connectivity. Microsoft Office applications utilize cloud services, and various applications such as Intuit's QuickBooks perform regular polling to locate, download and install program updates. Some applications, such as Notepad have no need to connect to the Internet. If a limited use application (e.g., Notepad) is accessing the Internet without an explicit need to do so, it may be compromised.

Privacy risk to computer systems is proportionally related to the number of applications given authorization to access information and to utilize network communications. Although anti-malware software is ubiquitous and provides formidable protection from various external threats, anti-malware software does not protect or monitor network behavior of authorized "insider applications." An "insider application" is much like an insider in an organization. After an application has been granted initial access to the operating system, it is typically free to operate without the oversight of anti-malware software.

Many applications initiate and maintain network connections to external destinations--often without the user's knowledge or desire. What we propose is analogous to a night club bouncer—software that continually monitors behavior of applications already admitted into the system and bounces them for misbehaving. The purpose of IP Bouncer is to increase visibility of unexpected or suspicious network communication. The end user is often the best judge of whether the application in question should be accessing the Internet or not. Linking application context and network connection information is a unique contribution of IP Bouncer.

Literature Review

The purpose of this research is to answer the call for privacy action research (Baskerville and Myers 2004; Bélanger and Crossler 2011) following design science principles (Gregor and Hevner 2013; Hevner et al. 2004; Kuechler and Vaishnavi 2012) to produce a privacy-enhancing artifact called IP Bouncer.

A design premise is the assumption that information technology users desire to avoid technology threats. TTAT differentiates acceptance theories from avoidance theory and provides a greater understanding of users' IT threat avoidance behavior (Liang and Xue 2009). In Liang and Xue's (2009) variance theory view of TTAT, they present three processes: threat appraisal, coping appraisal and coping. Together these three processes form a positive feedback loop that explains IT users' avoidance behavior (Carver and Scheier 1982; Carver 2006). Central to the overall design principles of IP Bouncer is the general desire of the user to avoid threats to network security and privacy.

To motivate IT users to avoid a specific threat, users must first perceive a threat. For protection motivation to occur, an appropriately scoped fear appeal message must be communicated and understood by the user. Only after users both perceive a threat, and believe they are susceptible to it, will they begin a threat appraisal. The associated design principle, therefore, is to communicate to the user that a threat to their system exists and that they have the ability to combat the threat. To maintain credibility with the user, the specified threat level, or absence of a threat level, must be communicated to the user.

Design Principle 1: Clearly communicate potential threats and threat severity (including Unknown severity) to the user.

In addition to the threat appraisal cognitive process, (Rogers 1975) also theorized that individuals simultaneously engage in a coping appraisal cognitive process. Components of this process include response efficacy and self-efficacy. Response efficacy is the user's belief that the recommended response (e.g., blocking a connection) will mitigate or eliminate the threat, and that the user is capable of doing so, which leads to our second design principle.

Design Principle 2: Provide clear options for mitigating or eliminating the threat and maximize ease of use.

Computer self-efficacy is a user's belief in his or her ability to accomplish a specific task using a computer (Thatcher et al. 2008) identified two dimensions computer self-efficacy: internal and external. Internal self-efficacy is how individuals perceive their ability to use a computer *without* help, while external self-efficacy is how individuals perceive their ability to use a computer *with* assistance, whether human or external. IP Bouncer's design accommodates users with varying levels of both dimensions of computer self-efficacy by making the program easy to use without assistance (internal dimension, design principle 2) and providing external assistance by identifying trustworthy and untrustworthy network destinations (external dimension, design principle 3).

Design Principle 3: Users must clearly understand how to utilize external resources both for assistance assessing and reporting network threats.

Ease of use is a well-founded principle for information system acceptance and adoption (Davis 1989; Taylor and Todd 1995; Venkatesh and Davis 2000; Venkatesh, V., Morris, M., Davis, G., & Davis 2003). Adoption and use of IP Bouncer will be predicated, at least in part, by how easy it is to use. Ease of use for security software is different than ease of use for productivity applications. End users do not want to use security software in the same manner in which they would use a word processor. Users don't want to use

security software at all; they simply want the benefit from it. The hallmark of excellent security software is invisibility until needed, and when needed, clearly understood methods of interaction, which is captured in design principle 4.

Design Principle 4: User interaction should be minimized and only visible when a threat is detected. Threat response options are clearly understood and easy to select.

Motivation to protect against Information Systems (IS) threats assumes internalization of a personal message and recognition of a personal threat, however, individuals often also act for the public good (Anderson and Agarwal 2010). Practicing proper antivirus procedures protects not only the individual, but the organization or social context in which that individual lives. Individuals are more likely to act in concert with their perception of what others are doing to promote the public good. Individuals also share knowledge, not only for narrow self-interest, but also out of moral obligation and community interest (McLure Wasko and Faraj 2000). This inclination to act individually, and for the public good, drives the design of a central repository of known and reported IP threats. Repositories for IP addresses linked to spam and unwanted web advertisers have existed for a long time. However, a real-time data collection from users' experience with unwanted or unknown IP connections is a novel contribution and constitutes design principle 5.

Design Principle 5: Users are able to report malicious or suspicious network connections and receive feedback from external sources.

Existing Network Security Tools

Several network connection security tools already exist. They contain much of the base functionality provided by IP Bouncer. However, they are typically intended for the network administrator, system administrator, or security professional and not the end user. No software package was found that utilized the key-pair context design of IP Bouncer.

Firewalls also provide some of the functionality of IP bouncer. However, they lack the ongoing monitoring of communication connected to specific applications in user context. Instead, firewalls examine protocols and packets without regard to the intended purpose or appropriateness of communication in the context of the application that initiated it. Software firewalls employ a once-for-all method of authorization for applications. After an application has been granted public or private access (or both), the destinations sought by the application are not monitored. Many anti-malware applications are capable of identifying phishing sites and matching Universal Resource Locators (URLs) with blacklists, but they lack the application context provided by IP Bouncer, Enterprise-level firewalls do not consider the end user application context.

Artifact Description

User Interface

To accurately identify potential threats and report useful information to the user, the following items should be monitored: local and remote IP addresses, local and remote ports, type of connection Transmission Control Protocol (TCP), User Datagram Protocol (UDP) (Postel 2003), destination country (determined by IP block), the status of connection (ESTABLISHED, WAIT, CLOSED), and the originating application (process).

Connection information collected on the user's workstation is matched with a centralized cloud-based threat repository. Information contained in the repository originates from trusted external blacklist compilers (e.g., Symantec Corporation, EasyList, Sucuri, ESET, MacAfee, Kaspersky). The moment an application makes an unexpected connection, an unnecessary network connection, or a connection to an untrusted destination, the user is immediately notified and presented with options to act. Those options include: gathering more information, reporting a suspicious connection, blocking a connection, and

blocking and reporting the connection (design principle 5). Whitelisted and expected connections to trusted destinations do not interrupt the user (design principle 4).

Centralized Cloud-based Threat Repository

The online threat repository (see Figure 1) forms the external dimension of computer self-efficacy (Thatcher et al. 2008). It enables users to obtain external assistance from other users and organizations to help identify and block potential network threats. Even an expert user would have difficulty determining which web hosts posed security risks. Consequently, users require ongoing assistance to make those determinations. Users can participate in the aggregation of potential threats by indicating questionable network connections—even if those connections are ultimately legitimate and desired.

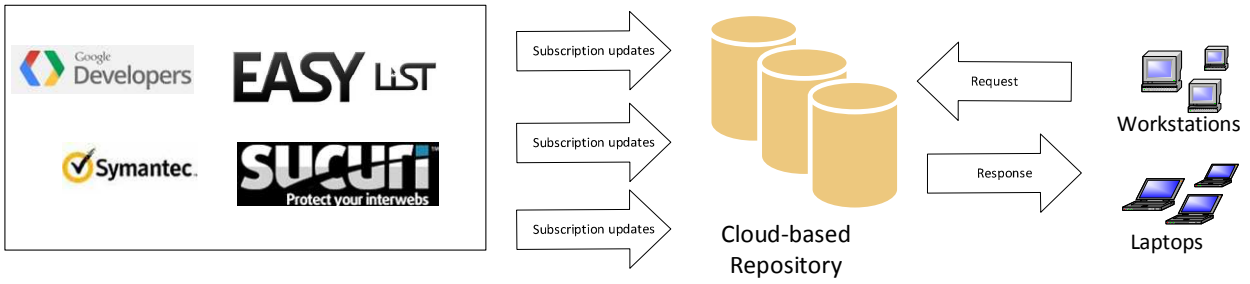

Figure 1- Centralized Cloud-based Threat Repository logical architecture

Millions of websites are categorized by aggregators and useful to end users for identifying unwanted connections (design principle 3). For example, users that never visit gambling sites may request IP Bouncer to trigger an alert when an application connects to a host categorized as gambling. Conversely, a gardening enthusiast may choose to whitelist all sites categorized as gardening, as shown in Figure 2.

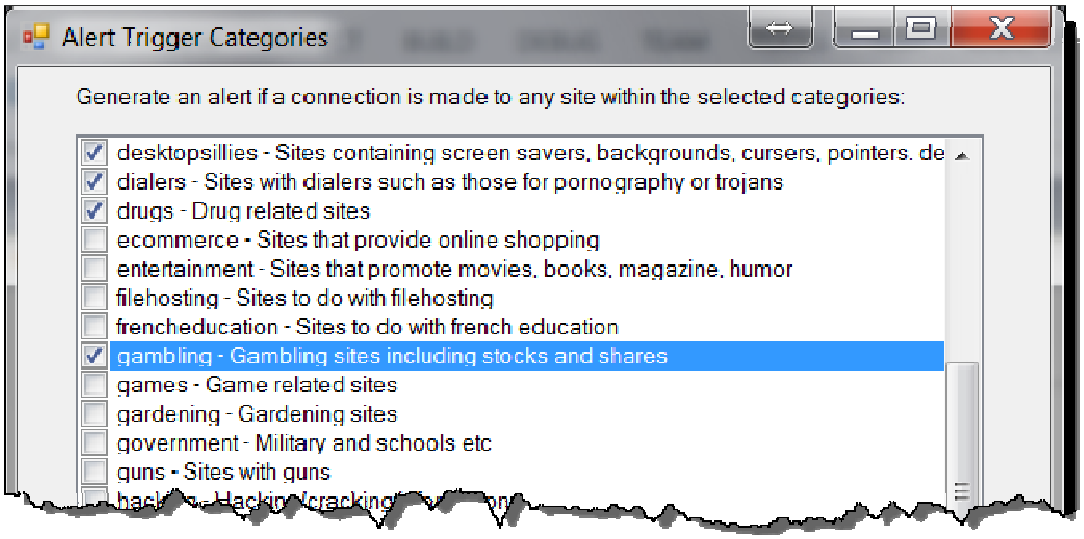

Figure 2 – Configure Alert by Category

To clearly communicate potential threats to the user (design principle 1), we utilize a familiar Microsoft Windows communication mechanism—the system balloon. When the user initiates an outbound connection, both the hostname (if provided) and the IP address are matched to a list of known hostnames and IP's contained in the online repository. If a match occurs, IP Bouncer communicates the threat using a system alert balloon as shown in Figure 3.

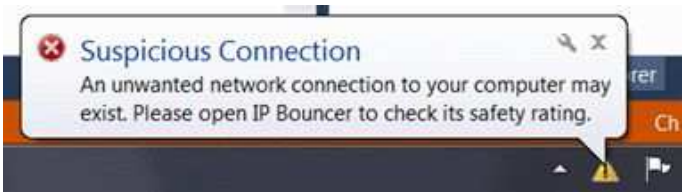

Figure 3 – Suspicious Activity Alert Balloon

After notification, the user has four options. First, if the destination is trusted, the user can whitelist it (design principle 2). Second, if it is untrusted, the user can Block or Block and Report (design principle 2). Third, the user can use IP Bouncer to retrieve additional information about the threat via the online threat repository to aid in making a determination whether or not to block the connection. Fourth, if a connection is unknown to the user and the repository, the user can Mark Suspicious.

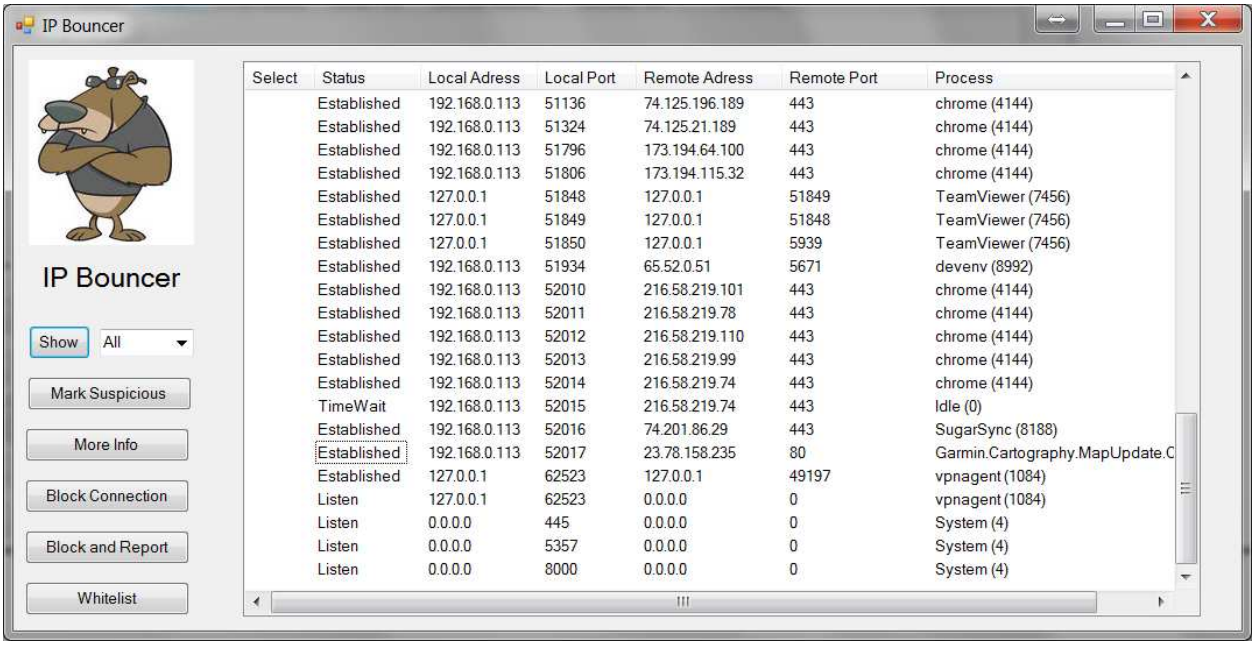

Figure 4 – IP Bouncer User Interface

The user interface, as shown in Figure 4, is simple to understand and provides discrete button choices that clearly indicate choices for threat response, and access external information and reporting (design principle 3).

The application itself runs in the background and is only viewed when a threat or suspicious connection is identified. If the user chooses to defer action, the yellow hazard triangle will persist in the system tray until the user has cleared the issue.

Discussion

IP Bouncer is a prototype designed to expose unexpected and unwanted network communication initiated by trusted "insider" applications. One of the novel aspects of this design is the key pair approach used for assessing appropriate or inappropriate network communications. The key pair consists of the destination coupled with the requesting process (spawned by the application). Firewalls and other network appliances filter traffic based on protocol or destinations, however, a legitimate destination for one application may be inappropriate for another. Firewalls are not able to make this distinction. Some applications have no reason ever to initiate network communications—even to legitimate destinations. Only by coupling the application (process) and the network destination can contextual legitimacy be determined. Ad-supported

applications such as games and other "free" software are expected to draw advertising content from the Internet, but other applications (e.g., a calculator, Portable Document Format [PDF] reader, compression program) are not.

Another benefit of the system is the potential to alert the user to the use of data drops. Hackers, such as those perpetrating the breach of Target Corporation in 2013, used data drops to legitimate servers (Krebs 2014) that did not trigger an exception on the firewall. However, IP Bouncer triggers an unknown connection alert, which the user may mark as suspicious and potentially identify the breach.

Evaluation

As this research in progress moves forward, it will be necessary to evaluate how well IP Bouncer meets the design principles that guided its development. To evaluate IP Bouncer, we plan on implementing IP Bouncer in a controlled environment and recruiting approximately 100 users to use it. We will then ask them a series of survey questions and short answer questions to determine how well IP Bouncer meets its design principles. We anticipate challenges for users to discern whether a given connection is desirable or undesirable, so several questions will center on the decision process employed by the user and how that process can be improved.

Conclusions

User's privacy and security are under attack like never before in history. No longer are malware attacks immediately discernable and automatically neutralizable. More sophisticated tools that leverage expert, real-time data, and the collective experiences of human intelligence are required. Using applications like IP Bouncer increases visibility and raises accountability for insider applications' use of network communications. Applications should be accountable for the increased attack surface they create by maintaining network connections not requested, needed, or desired by the user. This research provides contributions for the end user, the IT professional, and the privacy researcher. Previously hidden network communication is brought to light for even the novice to examine and question. IT professionals tasked with guarding user privacy and network security have a tool to enlist the eyes and minds of users in an "If you see something, say something" manner. This research introduces the concept of the insider application and raises the awareness of security risks inherent in a trust once, trust always application environment.

REFERENCES

Anderson, C. L., and Agarwal, R. 2010. "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly* (34:3), pp. 613–643.

Baskerville, R. L., and Myers, M. D. 2004. "Special Issue on Action Research in Information Systems: Making IS Research Relevant to Practice--Foreword," *MIS Quarterly* (28:3), pp. 329–335.

Bélanger, F., and Crossler, R. E. 2011. "Privacy in the digital age: a review of information privacy research in information systems," *MIS Quarterly* (35:4), pp. 1017–1041.

Carver, C. S. 2006. "Approach, Avoidance, and the Self-Regulation of Affect and Action," *Motivation and Emotion* (30:2), pp. 105–110 (doi: 10.1007/s11031-006-9044-7).

Carver, C. S., and Scheier, M. F. 1982. "Control Theory: A Useful Conceptual Framework for Personality-Social, Clinical, and Health Psychology," *Psychological Bulletin* (92:1), pp. 111–135.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future directions for behavioral information security research," *Computers & Security* (32), Elsevier Ltd, pp. 90–101 (doi: 10.1016/j.cose.2012.09.010).

Davis, F. D. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly* (September).

Gregor, S., and Hevner, A. R. 2013. "Positioning and Presenting Design Science Research for Maximum Impact," *MIS Quarterly* (37:2), pp. 337–355.

Hevner, A. R., March, S. T., Park, J., and Ram, S. 2004. "Design Science in Information Systems Research," *MIS Quarterly* (28:1), pp. 75–105.

Krebs, B. 2014. "Target Hackers Broke in Via HVAC Company — Krebs on Security," *Krebs On Security*.

Kuechler, W., and Vaishnavi, V. 2012. "A Framework for Theory Development in Design Science Research: Multiple Perspectives.," *Journal of the Association for Information Systems* (13:6), pp. 395–423.

Liang, H., and Xue, Y. 2009. "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS quarterly* (33:1), pp. 71–90.

McLure Wasko, M., and Faraj, S. 2000. "'It is what one does': why people participate and help others in electronic communities of practice," *The Journal of Strategic Information Systems* (9:2-3), pp. 155–173 (doi: 10.1016/S0963-8687(00)00045-7).

Postel, J. 2003. "RFC 793: Transmission control protocol, September 1981," *Status: Standard* (88).

Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *The Journal of Psychology* (91), pp. 93–114.

Rogers, R. W. 1983. "Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation," in *Social Psychophysiology*J. Cacioppo and R. Petty (eds.), New York: Guilford, pp. 153–176.

Taylor, S., and Todd, P. 1995. "Understanding information technology usage: A test of competing models," *Information systems research* (6:2), pp. 144–176.

Thatcher, J. B., Zimmer, J. C., Gundlach, M. J., and McKnight, D. H. 2008. "Internal and External Dimensions of Computer Self-Efficacy: An Empirical Examination.," *IEEE Transactions on Engineering Management* (55:4), pp. 628–644 (available at 10.1109/TEM.2008.927825).

US General Accounting Office. 2015. "High Risk Series: An Update GAO-15-290," Washington, D.C.: US General Accounting Office.

Venkatesh, V., and Davis, F. 2000. "A theoretical extension of the technology acceptance model: four longitudinal field studies," *Management science* (46:2), pp. 186–204.

Venkatesh, V., Morris, M., Davis, G., & Davis, F. 2003. "User acceptance of information technology: Toward a unified view," pp. 425–478.