A Method for Increasing Transmission Rates in Covert Timing Channels

Tim Kelley
kelleyt@indiana.edu

September 8, 2006

Covert channels are useful tools for those that wish to access data on secure systems without being detected. I expand upon the work of Greenwald *et.al.*'s technical report "TFTP UDP Covert Channel Project Phase One[2]," by modifying their UDP covert timing channel to allow it to encode more symbols per tick. Previous literature on covert channels focuses on the binary alphabet, but I demonstrate that, in certain instances, using a larger number of symbols can increase the rate of transmission in a covert channel.

This work is an empirical investigation building on the work of Moskowitz *et.al.*'s work on "The Timed Z-Channel[4]," but placing it into a practical context. Using an UDP covert channel, I propose that using multiple time-slices, one can encode larger alphabets, which in turn will allow a covert channel to increase the mutual information per tick (I_T), which is the information theoretic rate of transmission (rate of transmission that takes into consideration errors in transmission). This hypothesis can be generalized to other channels, but this experimentation is done using UDP.

I have implemented a covert channel in TFTP which can vary its alphabet size; this allows it to send larger fractions of a byte per tick. Within my experiments, I was able to achieve an I_T of 2145 bits per second using this encoding technique; a 36% increase over the timed Z-Channel. Even in the presence of noise, the covert channel I implemented– which I am calling the Saw-Toothed channel due to its graphical representation–performs at least as well as the binary Z-Channel. In lieu of the guidelines defined for high-capacity channels in the NSA's, *A Guide to Understanding Discretionary Access Control in Trusted Systems*, this channel, in the context of my experiments is leaking information at approximately 20,000 times what the NSA views as a dangerous channel[5].

This high transmission rate has profound repercussions on data that a user may wish to keep private. This affects not only governments and corporations, but also citizens and customers. As Lampson defined the confinement problem in "A Note on the Confinement Problem", he viewed it in terms of affecting all customers of information technology, not just those with formal security policies, such as the government or corporations[3]. And, as Baker points out in, "The Evolved Threat Paradigm: Look Who's Wearing the Black Hats!" our threat model should not assume that the people we "trust" to provide services are trustworthy[1]. My work examines the properties of one of the threats we seek to protect against as security professionals.

References

[1] Baker, D. B. The evolved threat paradigm: look who's wearing the black hats! In *NSPW '92-93: Proceedings on the 1992-1993 workshop on New security paradigms* (New York, NY, USA, 1993), ACM Press, pp. 126–130.

[2] Greenwald, S. J., Heydari, M. H., and Kelley, T. TFTP UDP covert channel project phase one. Tech. rep., The Institute for Infrastructure and Information Assurance, 2004.

[3] Lampson, B. W. A note on the confinement problem. *Commun. ACM 16*, 10 (1973), 613–615.

[4] Moskowitz, I. S., Greenwald, S. J., and Kang, M. H. An analysis of the timed z-channel. In *SP '96: Proceedings of the 1996 IEEE Symposium on Security and Privacy* (Washington, DC, USA, 1996), IEEE Computer Society, p. 2.

[5] US Department of Defense. *A Guide to Understanding Discretionary Access Control in Trusted Systems.* Fort George G. Meade, Maryland 20755-6000, September 1987. Also referred to as the "Orange Book." Available at: http://www.fas.org/irp/nsa/rainbow/tg003.htm.