Benjamin Blakely
Ph.D.
Computer Engineering
Major Professor: Doug Jacobson

Cyberprints: Identifying Cyber Attackers by Feature Analysis

Abstract: The problem of attributing cyber attacks is one of increasing importance. Without a solid method of demonstrating the origin of a cyber attack, any attempts to deter would-be cyber attackers are wasted. Existing methods of attribution make unfounded assumptions about the environment in which they will operate: omniscience (the ability to gather, store, and analyze any data relevant to an attack), omnipresence (the ability to place sensors wherever necessary regardless of jurisdiction or ownership), and *a priori* positioning (ignorance of the real costs of placing sensors in speculative locations). The reality is that attribution must be able to occur with only the information available directly to a forensic analyst, gathered within the target network, using budget-conscious placement of sensors and analyzers. These assumptions require a new form of attribution. This work evaluates the use of a number of network-level features as an analog of stylistic markers in literature. We find that principal component analysis is not a useful tool in analyzing these features. We are, however, able to perform Kolmogorov-Smirnov comparisons upon the feature set distributions directly to find a subset of the examined features which hold promise for forming the foundation of a *Cyberprint*. This foundation could be used to examine other potential features for discriminatory power, and to establish a new direction for network forensic analysis.