UCI Cybersecurity Policy & Research Institute

Bryan Cunningham
303-349-4870 (m) · 949-824-2720 (o)
E-mail: b.cunningham@uci.edu
www.cpri.uci.edu

CPRI Technical, Legal & Policy Research Initiative

Towards a More Holistic Attribution Model

As demonstrated starkly by the ongoing investigations into, and robust public discussions of Russia's attempts to influence our elections, and the resulting U.S. expulsion of Russian diplomats and imposition of sanctions in response, the ability to accurately and persuasively identify cyber attackers is of vital national interest. This is true whether the challenge is our government dealing with Russian or North Korean cyber aggression; prosecutors helping protect U.S. intellectual property against economic espionage; businesses determining how to recover stolen intellectual property through criminal or civil law and to conduct "defensive measures" under new legal authorities; and even schools battling cyber bullies.

Attribution is difficult and has been at best an uncertain science, with purely technical forensic approaches, such as comparing malware code with prior attacks, often inconclusive at best. Assertions of responsibility are frequently attacked for lack of sufficient "proof" and there is little agreement on the appropriate evidentiary standards for attribution in any context. As has been widely recognized, a cornerstone of future deterrence of cyber aggression, and of relief and justice for victims, will be more accurate and provable attribution of attacks.

Leveraging its unique multidisciplinary approach to solving challenging cybersecurity problems, CPRI's attribution research will examine the feasibility of a holistic, all-sciences approach to attribution, to determine whether such an approach can enhance the current state-of-the art for attribution and make future assertions of responsibility more credible. Such an effort will review publicly available case studies and acquire, under appropriate privacy protections and confidentiality agreements, large datasets of no-longer-sensitive information from prior attacks, and create an interdisciplinary team to review the data, "compare notes" on their conclusions, and develop an integrated view of responsibility.

Contributing experts would include, in addition to computer science and security experts:

- Psychologists to identify behavioral patterns of individual hackers;
- Cultural anthropologists to determine unique organizational and communications patterns, leadership hierarchies, and methods of operations of hacking groups; and
- Linguists and cryptographers to identify hackers' patterns of communications and data security.

This research would result in one or more reports on the feasibility of a multidisciplinary, holistic model of attribution and would include recommendations on how best to protect potential individual privacy and civil liberties under such an approach.

CPRI's Legal Subcommittee, made up of prominent private cybersecurity attorneys, has undertaken the first phase of this multidisciplinary effort: a comprehensive review of potential standards of proof for each level of cyber threat at which attribution is important: international law for nation-state and sub-national group/individual conduct; U.S. federal and state criminal law for prosecutions; and applicable U.S. federal and state statutory and common law for corporate and individual victims seeking civil redress. The group is working to determine the extent, if at all, to which current law is clear, and will propose model laws and standards of proof in each category.