Homeland Security / Cyber Security

White Paper Topic

Cyber Criminal Activity

Team

Avichal Singh - UW

Chris Fleizach - UCSD

Pravin Mittal - UW

Hemavathy Alaganandam - UW

Project Description

The rapid growth of the Internet, not just in terms of users, but also in terms of functionality has allowed entire industries to move their operations, and importantly their money, onto the Internet. This has lead naturally towards a prolific growth in criminal activity conducting solely through virtual means. Although cybercrime is not a new phenomenon, computers have always proved to be valuable targets, the essentialness of the Internet has necessitated a change in our understanding of security, risks and threats.

Cybercrime started as an insider job, grew into a threat that came from a determined outsider and has morphed again into an autonomous attack platform aimed at compromising any machine in order to leverage the might of the masses. The story of how targets, defenders, attackers, threats and vulnerabilities have changed is illustrative of the current state of cybercrime.

The present-day climate is a multi-faceted window into nefarious activities that scale from small-time pranksters to nationally funded spies, each with their own goals and targets. The entry of organized crime into the arena has raised concern amongst many, along with the exponential growth of botnets that have the power to inflict great damage against potential victims. Understanding and analyzing these various aspects will allow a better grasp at prevention and protection.

One area that many have proposed may be able to stem the tide of criminal activity are legal measures that can effectively deal with many of the situations that are novel and exist outside current legal definitions. But the threat of punishment is useless without the ability to capture and prosecute such criminals. Currently, it is difficult, if not impossible to track those who perpetrate crimes. Cyberforensics is a developing field which aims to solve these inherent flaws in the Internet and allow cyber criminals to face the same risk model that real-world criminals must contend with.

In this White Paper we will start with the history of CyberCrime, profiling of attackers, targets, defenders, vulnerabilities and goals of attacks. Next we will do a case study of botnets. We will briefly look into links between terrorism and cyber criminals. We will then research on Cyberforensics and current trends. This paper will also cover the existing legal policies on Cybercrime and its effectiveness. We will close the topic with some research on the future direction of Cybercrime and countermeasures.

Work Division

Avichal

Cyberforensics

CyberCrime and Terrorism

Chris

Legal Policies on Cybercrime: effectiveness of laws, examples, etc.

Future Direction of Cybercrime & Countermeasures

Hema

History of Cyber Criminal activity and Current Situation

Profile the evolution of attacker, targets, defenders, vulnerabilities, threats, and goals of attacks.

Pravin

Case Study : Emerging threat of Internet Bots – attacks, vulnerabilities, threats and goals and presenting possible responses to this particular threat.