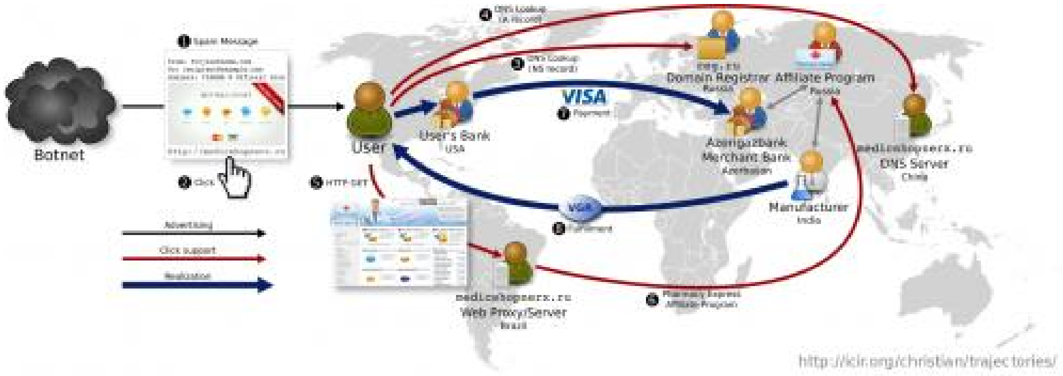
PHYS.ORG

Grant to help computer scientists understand the world of cybercrime

September 25 2012



This diagram describes all the steps involved in monetizing a particular spam message the researchers received. Credit: Jacobs School of Engineering at UC San Diego

Computer scientists at the University of California, San Diego, the International Computer Science Institute at Berkeley and George Mason University have received a $10 million, five-year grant from the National Science Foundation to map out the illicit activities taking place in the cybersecurity underworld and to understand how the mind of a cybercriminal works.

"Fighting cyber threats requires more than just understanding technologies and the risks they're associated with; it requires understanding human nature," said Stefan Savage, a professor of computer science at the Jacobs School of Engineering at UC San Diego, and one of the lead researchers on the grant. "At its heart, cyber security is a human issue. It's about conflict, and computers are merely the medium where this conflict takes place."

Among their goals, the researchers will investigate how criminals make money, their economic and social relationships, and the various ways they interact with victims and defenders to achieve their goals. The researchers hope that by better understanding these dynamics, they will be able to identify the best opportunities for interventions and defenses against cybercrime.

Economics come to the forefront in understanding how the world of modern cybercrime works, including the motives behind the vast majority of Internet attacks, and the elaborate marketplaces that support them. Social interactions are key to understanding how venues such as Facebook and Twitter present new opportunities for attacks and manipulation, and to understanding the relationships among cybercriminals, who heavily rely upon one another for services and know-how.

Savage will work with six other UC San Diego researchers, including social scientist James Fowler, best known for his work on social contagion. The basic idea for this project is that technological security depends on the human factor, Fowler said. "I love that engineers and computer scientists are acknowledging that security depends as much on human behavior as it does on technology," he said. "I look forward to working with them to help tackle these problems."

The UC San Diego team is joining forces with a team of eight researchers at the UC Berkeley-affiliated International Computer Science Institute, led by Vern Paxson, a professor of computer science, and with Damon McCoy, an alumnus of the UC San Diego group and now a faculty member at George Mason University.

This effort is an extension of an ongoing collaboration in cybersecurity that the Berkeley and San Diego teams have built by working together for over a decade. In just the last year, Paxson and Savage's team made headlines for a study that charted the complete "value chain" for email spam – the technical and economic relationships involved in making spam profitable. Researchers also identified which links in the value chain were the most vulnerable. By carefully tracking payment information across an array of test purchases, they showed that just three banks handled payments for 95 percent of spam-advertised products. This finding, what the researchers call a "choke point," suggested that targeting the economics of spam could ultimately be more effective than only addressing its technical symptoms. Today, this approach is being tested through collaborations between financial institutions, brand holders and government agencies.

The NSF grant will fund this kind of interdisciplinary work, but with greater breadth and scale. Researchers will focus on four key areas:

- The economics of E-crime: Researchers will try to get a better grasp of how cybercriminals make money in different scams. They will examine both advertising schemes, such as spam and search engine abuse, as well as theft of user data, such as financial account credentials. They will also get a better understanding of the infrastructure that cybercriminals rely on, including phishing kits, malware distribution and botnets.
- The role of online social networks: Facebook and Twitter have become a new battleground in cybersecurity, where criminals exploit users' trust to various ends. Researchers will map out the ecosystem of attackers that prey in social networks and the ways in which social manipulation is crucial to their activities. They will then try to understand the extent to which unsafe online behavior is learned and transmitted through online social

networks and how these findings might be harnessed to improve online safety.

- Underground social networks: Researchers will study the nature of "trust among thieves" and map out how relationships among criminals are established, maintained and evolve. Scientists will attempt to understand how cybercriminals go from being new to the field to becoming criminal masterminds. They will also try to understand how ideas are generated in the cybercrime underground; how new scams spread; and how trust is managed in building criminal relationships.
- Efficacy of intervention: Finally, the researchers hope to measure the relationship between security practices and security "outcomes," including understanding how different defenses, interventions and educational strategies actually impact the success of cyber attacks. The other researchers from the Jacobs School of Engineering involved on the grant are computer science professors Geoffrey Voelker, Lawrence Saul and Alex Snoeren from the Department of Computer Science and Engineering, as well as research scientists Kirill Levchenko and Erin Kenneally, a cyberforensics specialist at the Center for Advanced Computational Science Engineering.

Provided by University of California - San Diego

Citation: Grant to help computer scientists understand the world of cybercrime (2012, September 25) retrieved 25 April 2024 from https://phys.org/news/2012-09-grant-scientists-world-cybercrime.html