Security Ethics and Economics

Yang Gao
yg@eecs.berkeley.edu.cn

Nov. 19th, 2015

1 Crimes related to computer security

1.1 Types of computer crimes

- Damages to computer programs or files
- Theft of hardware, software
- View or manipulate the content that the intruder is not supposed to see.

1.2 Four types of ethical issues [1]

- Privacy: The policy of which information could be required to divulge, be public, or be kept strictly private.
- Accuracy: Misinformation could mislead people's decision and behavior. Thus it's also important to be able to verify that the information is integrate.
- Property: Intellectual rights of information are complex under the current way of information generation. Substantial concerns exist around the ethical and economic aspects of these rights.
- Accessibility: One must have the ability to deal with information, such as read, write and reasoning, have the access to information technology such as the Internet, library, computers and newspaper and have access to the information itself.

1.3 ACM code of conduct [2]

- Contribute to society and human well-being.
- Avoid harm to others.
- Be honest and trustworthy.
- Be fair and take action not to discriminate.
- Honor property rights including copyrights and patent.
- Give proper credit for intellectual property.
- Respect the privacy of others.
- Honor confidentiality.

1.4 Information protection laws

International and federal laws all helps to protect information security of the people, such as International Cybercrime Treaty (ICT), federal-wide laws such as Family Educational Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLB) and Health Insurance Portability and Accountability Act (HIPAA) [3]. An information protection law typically regulates the attributes that need to be protected, the changes that should be made to business patterns and how one should be penalized if it's not obeyed. As a concrete example, HIPAA regulates sensitive information in health insurance domain. It mainly aims to protect the confidentiality of medical data. HIPAA has a set of administrative procedures that require protection such as physical safeguards and technical security services. It also formulates the application scenario, such as when medical data is transmitted.

2 Ethics in security research: which line should not be crossed?[4]

Presented by Christie.

2.1 Four ethical principles

- Should not harm human actively. Tuskegee syphilis experiment [5]: After penicillin has been found to be an effective treatment to cure this disease, the researcher in Tuskegee syphilis experiment intentionally hide this important fact from its subjects. This harms the subjects actively, and by the end of 1972, 128 of 399 subjects died of syphilis or related complications. Other examples includes harming human mentally rather than physically. For example, a man posted fake sex ad. on Craigslist and published the response on his personal blog.

- Should not watch bad things happen. In the Spamalytics research[6], the researchers knew which computers were infected and simply watched without taking actions. This is similar to observing muggers at the backstreet without calling the police. Other examples include the "Your botnet is my botnet" paper [7], which takes over a Torpig botnet for 10 days, observing the users' sensitive information being uploaded without stopping the process.

- Should not perform illegal activities to harm illegal activities. PharmaLeaks [8] is a research work that takes advantage of the leaked transaction data of pharmacy spammers. Although the analysis is based on illegal data, it doesn't automatically provide a self-defense that it's an ethical usage.

- No undercover research. The "Is the Internet for porn?" [9] paper carry out undercover experiments to investigate facts about online adult industry. The experiment sets up a realistic porn website and attracts users to use it, without telling users that it's actually a research project.

2.1.1 Discussion

Some smart pacemaker could be hacked such that it functions abnormally, and thus threaten the life of patients with the device. Researchers at University of South Alabama have successfully hacked the iSan, a wireless patient simulator on the market[10]. The news come out to horrified many patients and lead to a refusal to use pacemaker when they should.

Is it ethical to teach a course of computer security? It is sensible to ask this question, since teaching security also means spreading the techniques of attacking others. We think it's totally acceptable if the content only consist of public knowledge. People could obtain the knowledge even if they're not in the course.

2.1.2 Related courses

- CS195 social implications of computers

- Data science W231. Legal policy and ethical considerations for data scientists.

- Info98. Data and ethics.

3 Economics in cybercrime

Breaking in a system potentially demands lots of time and efforts. Thus an attacker usually break in a system for some reason, either political or economical. Sony Pictures Entertainment is hacked in Nov. 2014 [11]. It's widely believed that North Korean did this to stop *The Interview* from being released, because the movie satirizes the North Korean government. Except political issues, most computer security breaches are economic related.

Security economics is useful to determine whom to fight against, prevent the attack by patching the software and thus make it expensive to be exploited. Also security economics could help to determine which security measure should be used.

China text-message car. Some cars in China equipped with jamming devices illegally block the carriers' mobile signals and send spam texts to mobile phones. They drive through the city to send massive amount of messages, usually 2 million messages a day per car. The costs for the device is around $1600 each and the profit each day is roughly also $1600. This make it a high profit industry. What's more, the spam cars rarely get caught and when they get caught, the fine is only $5000, far less than their expected income. The carriers don't have incentive to stop the spam cars, because most of the time they also earn a lot in the spamming process.

Endgame In February 2011, Endgame was found to sold zero-day vulnerabilities from the emails sent to HB Gary [12]. Most buyers are governments and hack back companies.

Comprised systems are also sold in the underground market. Entire machine, access to specific websites or email accounts all could be sold to a third party.

3.1 The underground economy: priceless [13]

Presented by Grant.

Motivation. They're often motivated by monetary gain. Sophisticated underground business enterprise is setup to facilitate the whole ecosystem. They usually communicate by public IRC channels or underground forums.

Sellers. They responsible for manufacture exploits, infect machines and take control of them.

Buyers. Buyers usually buy the attacked machines from sellers to carry out large scale attacks, or cashing out compromised bank accounts or use it for political aims.

Middle men merchants. Help to connect seller and buyer more smoothly. They're good at salesmanship, playing a role similar to Amazon and supermarkets in normal businesses. Some of them even have online customer services.

Takeaways: The underground cybercrime economy is highly organized, as the usual economy is. They have manufactures (sellers), buyers with various aims, and broker to make the whole process smooth.

To defense against the cybercrime, one could exploit the fragile infrastructure of the underground economy. For example, one could make the attacking not profitable, thus invalidating the incentive of attacking. Or one could impose bottlenecks to disrupt their businesses, such as arrest the brokers, or isolate the banks involved.

3.2 Spamalytics[6]

Presented by Jingcheng.

To understand how much money one could make out of the spams, one has to estimate 3 quantities: the cost of sending a spam, the conversion rate (i.e. how many people are fooled to click on the link and pay

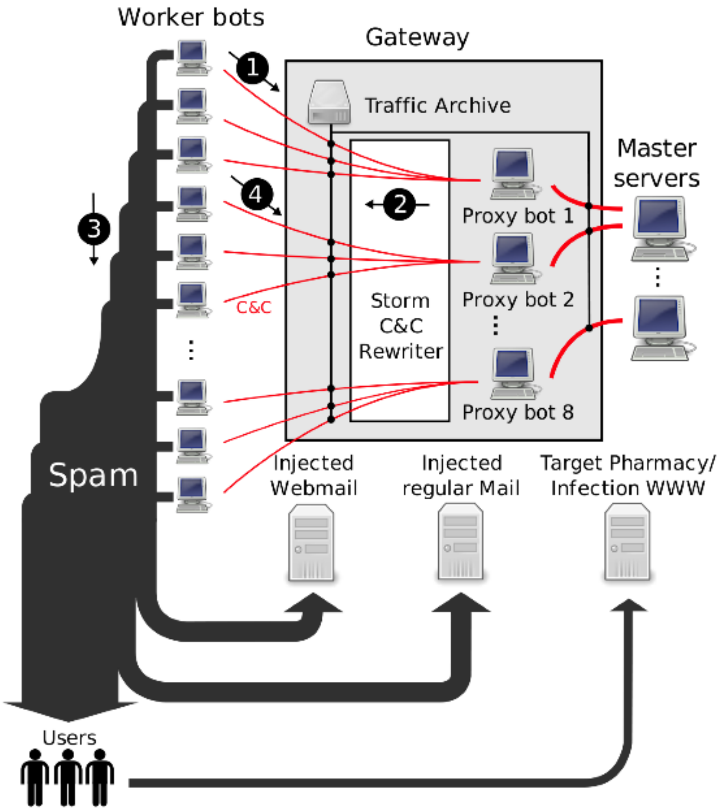

Figure 2: The Storm spam campaign dataflow (Section 3.3) and our measurement and rewriting infrastructure (Section 4). (1) Workers request spam tasks through proxies, (2) proxies forward spam workload responses from master servers, (3) workers send the spam and (4) return delivery reports. Our infrastructure infiltrates the C&C channels between workers and proxies.

for it), and the marginal profit for each sale. The first and the third quantities are easy to estimate, but the second is hard to estimate. Spamalytics aims to estimate the second quantity.

In a typical Storm botnet (Fig. 3.2), there are a few reliable master servers. Each master server controls a few infected proxy servers, which could be reached publicly. The proxy servers directly controls workers, who actually send the spam workload.

In order to analyze the traffic in the botnet, the researchers intentionally infect some of their machines with the malware and let them serve as the proxy. Thus they could precisely see the spam traffic of the worker. And finally they could calculate the conversion rate by measuring how many emails get to the actual users, how many of them clicked through the link and how many finally make a purchase.

They've reached a rather surprising conclusion that the current spam market is quite inefficient: among the 350 million spams sent, only 28 of them get into a buying behavior during a month. On average, each purchase is around $100.

References

[1] Richard O. Mason. Four ethical issues of the information age.

[2] Acm code of ethics and professional conduct.

[3] 104th Congress. Health insurance portability and accountability act of 1996.

[4] Sebastian Schrittwieser, Martin Mulazzani, and Edgar Weippl. Ethics in security research which lines should not be crossed? In *Security and Privacy Workshops (SPW), 2013 IEEE*, pages 1–4. IEEE, 2013.

[5] Tuskegee syphilis experiment.

[6] Chris Kanich, Christian Kreibich, Kirill Levchenko, Brandon Enright, Geoffrey M Voelker, Vern Paxson, and Stefan Savage. Spamalytics: An empirical analysis of spam marketing conversion. In *Proceedings of the 15th ACM conference on Computer and communications security*, pages 3–14. ACM, 2008.

[7] Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna. Your botnet is my botnet: analysis of a botnet takeover. In *Proceedings of the 16th ACM conference on Computer and communications security*, pages 635–647. ACM, 2009.

[8] Damon McCoy, Andreas Pitsillidis, Grant Jordan, Nicholas Weaver, Christian Kreibich, Brian Krebs, Geoffrey M Voelker, Stefan Savage, and Kirill Levchenko. Pharmaleaks: Understanding the business of online pharmaceutical affiliate programs. In *Proceedings of the 21st USENIX conference on Security symposium*, pages 1–1. USENIX Association, 2012.

[9] Gilbert Wondracek, Thorsten Holz, Christian Platzer, Engin Kirda, and Christopher Kruegel. Is the internet for porn? an insight into the online adult industry. In *WEIS*, 2010.

[10] CAE Healthcare. Researchers hack a pacemaker, kill a man(nequin).

[11] Sony pictures entertainment hack.

[12] Haroon Meer. Lessons from anonymous on cyberwar.

[13] Team Cymru. the underground economy: priceless, 2006.