Modeling Cyber Crimes and Investigations for Digital Forensics Education

James Palmer, *Cornell University*, Brea Llorens, *DePauw University*, Sarah Kaufman, *Mesa Community College*, Christopher Gibbons, MdGayas Chowdhury, Cindy Chen, and Xinwen Fu, *UMass Lowell*

Abstract: Current network forensics education lacks a systematic view of how real-world cybercrimes are committed and how real-world cases are investigated. In this paper, we fill these gaps. We explicitly define three basic crime strategies as computer assisted strategy, computer focused strategy and non-cyber strategy (traditional crime strategy) and model a real world cyber crime case as a sequence of crimes using these three basic crime strategies. We explicitly define two basic investigation strategies as computerized techniques and traditional operations. These models allow satisfactory explanation of a case that may involve a number of basic types of crimes and investigations. We have also built a real-world case database system for digital forensics education. Our preliminary survey confirms the usefulness of these models and case database system helping students understand cyber crimes and investigations.

1 Introduction

The Internet has become the primary battlefield of the cyber war and the prevalent environment of cybercrimes [Sym15, Sym215]. Digital forensics education meets the urgent need of cyberspace operations professionals. Network forensics is one branch of digital forensics and focuses on evidence collection, analysis and suspect identification in a networked environment. However, the current network forensics education lacks a systematic view of how real-world cybercrimes are committed and how real-world cases are investigated. Individual techniques are taught in class without sufficient real-world case support. In this paper, we fill these gaps by modeling real-world crimes reported by FBI and real-world investigations performed by law enforcement. Such models allow satisfactory explanation of a case which may involve a number of crimes and investigations. We have also built a real-world case repository for digital forensics education.

It is critical to understand strategies and traits of cybercrimes in order to predict and detect, and therefore reduce them. Security terms and jargons are all over the media and textbook, often confusing, ad hoc and not systematic. It is hard to provide a comprehensive view of threats and defense techniques given the chaotic names. An appropriate classification framework will form a common language between victims and law enforcements around the world so that the communication between the collaborating parties is smooth and seamless, given that cybercrimes often involve computers from all over the world [Fur01, GF06, SWL10]. Various classifications have been proposed to this end. For example, classification based on motivation of performing crime helps us understand the foundation of cybercrimes and helps prevent cybercrimes by lessening the need of committing those crimes by criminals [Nga10]. The motivation based classification also has its pedagogical importance.

In this paper, we model cyber-attacks and cyber investigation, and then relate modeling to analyze real-world cases. We design and implement an online cybercrime case database system that can be used in digital forensics education. Our contributions can be summarized as follows.

- We explicitly define three basic crime strategies as computer assisted strategy, computer focused strategy and non-cyber strategy (traditional crime strategy) and model a real world cyber crime case as a sequence of crimes using these three basic crime strategies. Our real-world case study validates this model, which helps understand how cybercrimes are committed in the real world, that is, the cybercrime in a case may be a sequence of crimes using various strategies, not just one crime using one specific strategy.
- We explicitly define two basic investigation strategies as computerized techniques and traditional operations. The goal of a cybercrime investigation is to track and arrest the suspect. Given that a cybercrime is a combination of computer based strategy and non-cyber strategy, a cybercrime investigation also needs actions from both cyber and real worlds. Our real-world case study validates that a real world cybercrime investigation is performed in this fashion.

- Our web based online cybercrime case database system collects case details of both classified cybercrimes and classified cybercrime scene investigations. Currently there is no such system. Our system will advance the understanding of cybercrimes and various attack techniques and works as a valuable resource for digital forensics education.

The rest of this paper is organized as follows. We introduce related work in Section 2. We formally model cybercrime strategies and provide case study in Section 3. In Section 4, we formally model cybercrime investigation strategies and provide case study. Our online cybercrime classification system is introduced in Section 5. We present preliminary survey results of using the models, case study and online database system in classrooms in Section 6. We conclude this paper in Section 7.

2 Related Work

Researchers have been classifying cybercrimes for better understanding their cause and strategies. Furnell [Fur01] and Gordon and Ford [GF06] classify cybercrimes as computer-assisted and computer-focused crimes in terms of the applied strategy. In a computer-assisted crime, a criminal uses a computer to perform the crime, such as cyber stalking. In a computer-focused crime, criminals deploy attacks against computers or networks of computers, such as DDoS (distributed denial of service) attack. Gordon and Ford [GF06] notice the continuum of cybercrimes, some of which may have only "a peripheral cyber element". In this paper, we extend the related work and explicitly classify cybercrimes as a *sequence* and *combination* of three basic crime strategy, computer assisted strategy, computer focused strategy and non-cyber strategy (traditional crime strategy).

The FBI Internet Crime Complaint Center (IC3) has a relatively comprehensive classifications of complaints in its 2009 and 2013 annual Internet crime reports. Please find the description of these categories in the appendix. We can see that FBI performs simple classification and just put those complaints/crimes into ad-hoc groups of similar behaviors of the criminals. This classification uses the traditional definition of crimes [Sie15]: " 'Crime' is a violation of societal rules of behavior as interpreted and expressed by the criminal law, which respects public opinion, traditional values, and the viewpoint of people currently holding social and political power. Individuals who violate these rules are subject to sanctions by state authority, social stigma, and loss of status." Basically, ad-hoc malicious cyber behaviors are grouped and enumerated.

Ngafeeson proposes the motivational model, which borrows from the traditional crime study, and classifies cybercrimes according to five broad classes of needs [Nga10]: 1. Physiological needs; 2. Security or safety needs; 3. Social, belong or membership needs; 4. Esteem needs and 5. Self-actualization or self-fulfillment needs. A need may provoke people committing crime to fulfill the need. An individual may also evaluate the cost and benefit before committing a crime. If the benefit is more than the cost, the individual may pursue the crime. Stabek, Watters and Layton use pattern-recognition analysis to classify scams into seven types [SWL10].

To curb cybercrimes, we have to trace back to the source of the crime, capture criminals and deter similar crimes by punishments. Ciardhuáin proposes a model of cybercrime investigations [Cia04]. It has 13 backtracking components: 1. Awareness: An incident is made aware to the investigators; 2. Authorization: The investigators secure permission for performing the investigation; 3. Planning: The investigators make a plan of where and how to get evidence; 4. Notification: The investigators notify the subject of the investigation if necessary; 5. Search for and identify evidence; 6. Collection of evidence; 7. Transport of evidence appropriately to secured places; 8. Storage of evidence; 9. Examination of evidence; 10. Hypothesis of what happened according to collected evidence; 11. Presentation of hypothesis in court or to appropriate personnel; 12. Proof/defense of hypothesis in case of challenges in court or by appropriate personnel; 13. Dissemination of information with appropriate anonymization and removal of sensitive information. Other cybercrime investigation models are similar to the extended model in [Cia04].

3 Cybercrime Model

In this section, we first introduce our model of cybercrime in a case and then perform real world case study to demonstrate the feasibility and effectiveness of our model. In the case study, we often map a case

based on FBI IC3 category to our model. We can easily see the complication of a real-world case and the usefulness of our model to help understand a real-world case.

3.1 Modeling a cybercrime

We extend the classifications in [GF06] to have three basic crimes using three different strategies: 1. Computer focused crimes where either computers or networks of computers or entities such as data or software in cyber space are the attack target, 2. Computer assisted crimes where computers or networks of computers are used to perform the crimes, while the computers or networks themselves are not targeted; 3. Non-cyber attack (i.e. traditional crime) such as money laundering. Figure 1 illustrates the three basic crime models using the Universal Modeling Language (UML). For Type 2 and Type 3 crimes, on the right, we did not name the role of a person (called actor in UML). This is intended to show that criminals may perform damage to a victim, or a criminal can perform some acts with other criminals. In a Type 3 crime, criminals may damage only physical properties and the crime may not involve people. Therefore, multiplicity of the right actor is set as 0..*.

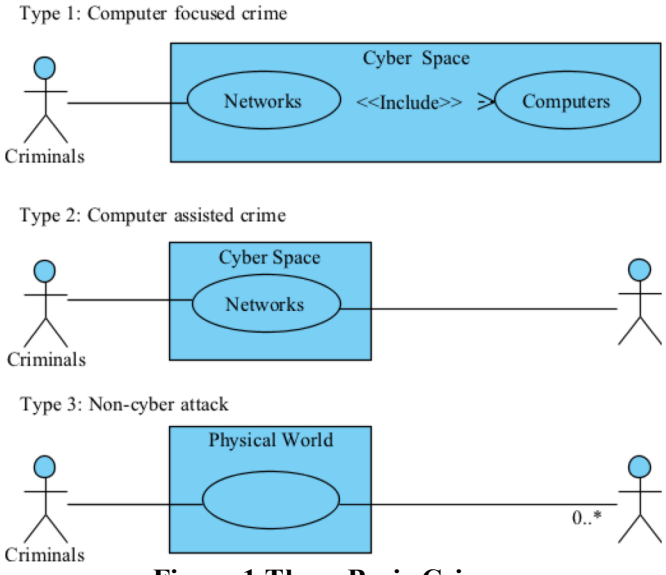

Figure 1 Three Basic Crimes

We further model a real-world cybercrime as the combination of the three basic crimes. How many types of cybercrimes exist under this model? Since a cybercrime is a combination of the three basic crimes, we can count the combinations. Assume a specific crime has n phases and each phase involves a crime. The number of combinations is 3^n. If $n = 5$, there are *243* types of crimes. This number is a rough estimate since we count the type of case where all phases use a non-cyber crime strategy. Actually, each basic crime may use a variety of crime techniques such as buffer overflow and SQL injection. If the number of different techniques corresponding to the three basic strategies is denoted as l, there are l^n types of crimes. In reality, l can be big. This demonstrates the complication of a cyberattack.

3.2 Case Study

To validate our model of cybercrimes presented above, we analyze the cases posted on the FBI website [CC16], and identify the combinations of the three basic crimes in a case. Such analysis helps understand the behavior of cyber criminals and design corresponding investigative strategies. We often use the FBI IC3 categories in the case title to refer to a case. Please find the description of these categories in the appendix. From the case study, it can be observed that a real-world case can be very complicated and consists of a sequence of basic crimes using various strategies.

3.2.1 Computer focused (CF) crime

A case of *stolen property offenses*: In 2010, A Dutch national Joey Vogelaar hacked into a company involved in the production release and stole digital versions of three Hollywood movies: “How Do You Know” by Sony Pictures Entertainment and “Rango” by the Paramount production as well as “Megamind” by Dreamworks [Dut15].

3.2.2 Computer assisted (CA) crime: A case of *illegal business* using Tor

Tor is a low-latency anonymous communication network [Tor16]. It works as follows. Volunteers install the Tor software on their computers and become Tor routers in a virtual network. To start a communication session to a server like a website, the client will pick up three routers across the world, which relay the message from the client to the server. The communication between the client and the first

Tor router and communication between Tor routers is encrypted. The relay path is called a *circuit*. The last Tor router on a circuit is called a Tor exit. The exit router is responsible for sending the client's message to the server. Therefore, in the view of the server, the message comes from the exit, instead of the client. The return message will be relayed through the same circuit back to the client. A special service by Tor is called the hidden server such as a hidden web server with a *.onion* address. The hidden server is constructed in such a way that a browsing client cannot know the IP address of the hidden server.

Ross William Ulbricht created a web site called Silk Road in approximately January 2011 and operated this global dark marketspace for illegal goods and services including controlled substances, hacking software and services [Ulb13, Ulb15]. Silk Road utilized Tor, an anonymous communication system preserving anonymity for the illegal activities, sellers and buyers. Bitcoin was used as the currency of Silk Road. When this online criminal enterprise was busted in October 2013, millions of dollars of Silk Road Bitcoins were seized. "While in operation, Silk Road was used by thousands of drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs and other unlawful goods and services to well over a hundred thousand buyers, and to launder hundreds of millions of dollars deriving from these unlawful transactions." [Ulb13]

3.2.3 Non-cyber (NC) crime: A case of *ATM skimming*

From at least December 2007 through June 2009, Radostin Paralingov and Ulian Parlingov installed skimming devices at branches of Citibank and JPMorgan Chase Bank in the New York City area [Bul10]. A skimming device is installed over an ATM card reader and steals the card information from the magnetic strip. A hidden camera is often installed on or around the ATM machine to steal the PIN number. The two withdrew over $1 million from the victims' accounts.

3.2.4 A case of *Non-Delivery of Merchandise* (*non-auction*)

Romanian fugitive, Nicolae Popescu was the leader running a multi-million dollar cyber fraud scheme and Dumitru Daniel Bosogioiu, another Romanian, was one of the participants [Fra14].

Phase 1 (CA/NC): They employed co-conspirators and emailed victim buyers fraudulent certificates of title and other information in order to lure the victims into buying non-existent cars. They also created phony dealer websites, and pretended to sell cars in the United States. They opened American bank accounts with fake passports.

Phase 2 (CA): After the "sellers" made an agreement with the victim buyers, they emailed the victims fake invoices from Amazon Payments, PayPal, or other online payment services and instructed the victims to transfer the money to their American bank accounts.

Phase 3 (NC): The co-conspirators then withdrew the proceeds from the U.S. bank accounts and sent to the defendants in Europe by wire transfer and other methods.

3.2.5 A case of *Credit/Debit Card Fraud*

The crime has roughly three phases and each phase uses different crime strategies [Bal14].

Phase 1 (using CA): From at least as early as September 2010 through at least June 2012, Olanrewaju Abiola and his conspirators purchased stolen credit card data on the Internet or through other means.

Phase 2 (using NC): They made counterfeit gift cards, credit or debit cards using the data and device-making equipment, such as credit card encoders. Abiola and his co-conspirators then used the counterfeit gift, credit or debit cards and bought gift cards and other merchandise at legitimate merchant locations like Giant, Rite-Aid and Nordstrom in or around the Washington-Baltimore region. Counterfeit driver's licenses were often used during the purchase. They then returned the merchandise they purchased in order to convert the stolen data to cash.

3.2.6 A case of *Extortion*

The crime has roughly two phases and each phase uses different crime strategies [And14]:

Phase 1 (using CF): Cryptolocker is a malware. It showed up about September 2013. A user may accidentally run the malware as an email attachment or when the malware is downloaded from the Internet. It encrypts user data using public key cryptography.

Phase 2 (using NC): The user must pay a ransom to get the decryption key. If the victim does not pay the ransom, it is impossible to recover their files.

4 Cybercrime Investigation Model

Traditionally, to trace the source of an attack, in academia, researchers design strategies fully relying on computer techniques. For example, by analyzing logs from routers and computers, we want to reconstruct the attack scene and find the source. Sentinels can be set up around the Internet and sample network traffic in order to collect necessary information to correlate an attack to specific Internet addresses (IPs).

4.1 Modeling cybercrime investigation in terms of investigative strategies

However, fully computerized techniques cannot be always effectively applied. For example, the model of cybercrime investigations in [Cia04] suggests that appropriate authorizations such as search warrants must be secured before searching for and collecting evidence. The laws and constitution protect user privacy and prohibit arbitrary surveillance on the Internet. Tracing suspects around the Internet is a challenging job without necessary proactive data. Therefore, instead of relying on pure computerized techniques, law enforcement has been using traditional investigative technique such as sting operations in cyber space. For example, law enforcement may impersonate minors to collect evidence against a suspect of child exploitation or by illegal products from dark marketspaces, like Silk Road

Therefore, two broad categories of cybercrime investigative strategies are applied by law enforcement: computerized techniques (CT) and traditional operations (TO). A combination of these two strategies can be utilized in the investigation of a specific case.

4.2 Case Study

We now present case study to demonstrate both computerized techniques (CT) and traditional operations (TO) are used in a real-world investigation.

4.2.1 Traditional Sting Operation: A Case of *Sex Trafficking*

A sting operation is a traditional policing technique. According to U.S. Department of Justice, a sting operation often has the following four elements [Sti07]: "1. an opportunity or enticement to commit a crime, either created or exploited by police. 2. a targeted likely offender or group of offenders for a particular crime type. 3. an undercover or hidden police officer or surrogate, or some form of deception. 4. a 'gotcha' climax when the operation ends with arrests."

Sting operation is often applied for investigating sex trafficking cases [SD14]. Law enforcement agents acted as pimps and approached suspects who were willing to pay for sex with underage girls of 12-15 years old. After the negotiation was sealed for the deal, law enforcements arrested those suspects. Five people were arrested through this sting operation during the 2014 Sturgis Motorcycle Rally.

4.2.2 Computerized Techniques: United States v. Barry Vincent Ardolf, A Case of *Intimidation*

Unexperienced people often leave their household routers open without encryption or with weak encryption. Their neighbors then may use their routers and perform crimes. Then the SWAT team crashed and raided the house for evidence. This type of case has been happening fairly often [Ind14, Tho11, AP11, Kra11]. Because of the scary and damaging raid by a SWAT team, it is called "SWATTING".

The case 11-2602 - United States v. Barry Vincent Ardolf serves the purpose of demonstrating computerized techniques [Kra11, Ard12] by law enforcement. Ardolf was angry at his neighbor reporting his kiss of his neighbor's 4 year old son's lip. He cracked the WEP encryption of his neighbor's router and sent various harassing and threatening emails to different people, including a death threat against Biden, the Vice President of United States on April 1, 2009, under the name of his neighbor. The purpose was to humiliate, terrorize and incriminate his neighbor. The law enforcement traced back to the neighbor's router and found they were innocent. The law enforcement connected a packet capturing device (sniffer) to his neighbor's router and was able to capture the packets when the threat email was sent to Biden. The packets were analyzed. The packet content contained Ardolf's name and his Comcast

IP address. Ardolf was adamant that he did not commit the crimes and was not remorseful. He was sentenced an 18-year prison.

4.2.3 Traditional Operations + Computerized Techniques: United States Of America v. Ross William Ulbricht, A case of *illegal business*

In the case of United States Of America -V- Ross William Ulbricht [Ulb13, Ulb15, Tar14], given the complicated scenario of tracing suspects within Tor, the investigators used a variety of techniques. Traditional sting operations were performed. Individual law enforcement agents registered accounts within Silk Road and purchased over 100 items of controlled substances from Silk Road vendors. The postal markings of the purchased drugs indicate these vendors were distributed across 10 different countries, including United States. U.S Customs and Border Protection (CBP) intercepted counterfeit identity documents from Canada as part of a routine border search on July 10, 2013. The documents carried Ulbricht's photo with different names. Around July 26, 2013, Homeland Security agents visited the residence of the mail address and encountered Ulbricht, who was the person on counterfeit identity documents. The operator of Silk Road expressed the interest of fake identity documents within Silk Road in June and July 2013.

Extensive computerized techniques were employed to identify the operator of Silk Road. *Searching the Internet to find when and how Silk Road was first publicized*: The earliest posting appeared on www.shroomery.org by *altoid* on Jan 27, 2011. Next posting appeared on bitcointalk.org by *altoid* on Jan 29, 2011. Another posting for hiring bitcoin professionals appeared on bitcointalk.org by *altoid* on Oct 11, 2011, which directed interested users to send their response to rossulbricht@gmail.com. Therefore, *altoid* used rossulbricht@gmail.com. Google collaborated with law enforcement and provided the subscriber information for rossulbricht@gmail.com and registered user was called Ross Ulbricht. Ulbricht's Google+ profile refers to Youtube videos from mises.org, where Ross Ulbrcht has an account and profile photo. The same videos were also referred to by the Silk Road administrator DPR (Dread Pirate Roberts) on the Silk Road Forum. *Subpoenaing Google and Comcast to identify the residence of Ross Ulbricht*: Google was subpoenaed to identify the IP address accessing rossulbricht@gmail.com. Comcast was subpoenaed to identify the residence of the IP address, which is in the San Francisco area from January 13 to June 20, 2013. Postings by DPR on the Silk Road forum also referred to the Pacific Time zone. A VPN provider was subpoenaed to identify who was using VPN to access the administrative account of Silk Road. An IP address was embedded in the administrative code of Silk Road. This IP address was the VPN server address. By subpoenaing the VPN provider, the investigators could identify the IP address accessing the VPN belonged to a Cafe, which was less than 500 feet from the identified residence. There are other evidences linking Ross Ulbrcht to DPR of Silk Road. Please refer to [Ulb13] for details. Ross Ulbrcht left various traces on the Internet indicating he created and administrated Silk Road.

The investigators actually identified a few Silk Road servers hosted in other countries than United States [Ulb15]. By inputting invalid login credentials into Silk Road, the investigators were able to obtain error messages that included a Silk Road server IP. They requested the imaging of the server and analyzed the image. By analyzing the image, the investigators also located other Silk Road backup servers. Various evidences were found in these servers, which matched the evidences found on the Internet. By mid-September 2013, Ulbrcht was FBI's lead suspect owning and running Silk Road as DPR. FBI obtained several pen registers to monitor the communication from and out of Ulbrcht's residence. Although no content was captured, the investigators were able to correlate when Ulbrcht was online and when DPR was active within Silk Road. On Oct 1, 2013, the investigators obtained search warrants to search Ulbrcht's residence, laptop, Gmail account and Facebook account.

5 A Web based database system for annotating cases reported by FBI IC3

The FBI Internet Crime Complaint Center (IC3) was established in 2003 and is a good resource for both victims of Internet crime reporting incidents and law enforcement agencies investigating and prosecuting these crimes. However, news reports by IC3 often miss technique details of either the crime or investigation. We have been referring to Public Access to Court Electronic Records (PACER) [PACER16]

and other online court documents including RECAP [REC16] to obtain those details and record them into the online database. We have built a web based database system for classifying and annotating cases reported by FBI at https://casebook.cs.uml.edu/books/FBIbs/service.php. The web system for classified cybercrime cases will be open for public search when this paper is published. We expect the website will generate a great impact on both education and research in academics.

We also found that the cybercrime classification by FBI is useful in practice for law enforcement since it enumerates various cybercrimes corresponding to malicious cyber behaviors. However, the definition of those individual cybercrimes is either missing or not formal. We have been refining the definition of those crime categories. The definitions and other information are stored in the database. Such a database can be used for both research and education. For research, we can refine the classification of these cases based on applied attack and investigative techniques. For education, the database can be searched for particular cases so that students can understand how a specific attack or investigation happens in reality. We will also annotate each case using our cybercrime model.

The database records three types of case data stored in three tables: 1. *cases* that records case description and its category; 2. *crime_category* that records categories by FBI IC3 with their definition; 3. *technique* that records both attack and investigation techniques. The table *case_has_technique* record what techniques are involved in a case. They can be attack techniques or investigative attacks applied by the investigators while dealing with the case. The table *users* is used to control user access to the information stored in the database. We found the FBI news often lacks technique details and will refer to Public Access to Court Electronic Records (PACER) and other online court documents including RECAP [REC16] to fill the gap.

6 Preliminary Survey

We have introduced the cyber crime and investigation models and case studies to two MSIT (Master of Science in Information Technology) classes on digital forensics in Fall 2015 and Spring 2016. The two classes had 48 students in total. They all agreed that the models and case study "Help much understand digital forensics". More rigid survey study will be performed for both undergraduates and graduates as future work.

7 Conclusion

In this paper, we present a comprehensive classification of cybercrime strategies, cybercrime investigation strategies and introduce a web based system documenting and classifying cases listed at the FBI website. We explicitly model a cybercrime in a case as a combination of computer assisted strategy, computer focused strategy and non-cyber strategy. We also model a cybercrime investigation as a combination of computerized strategies and traditional operations. Real-world cases are presented to support these two models, which reflect how cybercrime and investigation are performed in the real world. Our online web based database system provides an easy venue for searching related cases. Technical details of a case will be derived from Public Access to Court Electronic Records (PACER) and other online court documents including RECAP. This online database system populated with real-life examples of cybercrime benefits both research and education for digital forensics.

References

[And14] U.S. Department of Justice, Office of Public Affairs, Conspirators in Two Android Mobile Device App Piracy Groups Plead Guilty, http://www.fbi.gov/atlanta/press-releases/2014/conspirators-in-two-android-mobile-device-app-piracy-groups-plead-guilty, April 15, 2014

[Ard12] 11-2602 - United States v. Barry Vincent Ardolf, http://www.gpo.gov/fdsys/granule/USCOURTS-ca8-11-02602/USCOURTS-ca8-11-02602-0, July 5, 2012

[AP11] The Associated Press, NY men accused of downloading child porn after others use their Wi-Fi,

http://www.syracuse.com/news/index.ssf/2011/04/ny_men_accused_of_downloading.html, April 24, 2011

[Bal14] U.S. Attorney's Office, Eastern District of Virginia, Baltimore Man Pleads Guilty in Identity Theft and Credit Card Fraud Ring, http://www.fbi.gov/washingtondc/press-releases/2014/baltimore-man-pleads-guilty-in-identity-theft-and-credit-card-fraud-ring, August 05, 2014

[Bul10] U.S. Attorney's Office, Southern District of New York, Manhattan U.S. Attorney Charges Bulgarian Man with Using Stolen Bank Account Information to Defraud Banks of Over $1 Million, http://www.fbi.gov/newyork/press-releases/2010/nyfo092310a.htm, September 23, 2010

[CC16] Cyber Crime, http://www.fbi.gov/collections/cyber, 2016

[Cia04] S. O. Ciardhuáin, *An Extended Model of Cybercrime Investigations*, International Journal of Digital Evidence. Summer 2004, Volume 3, Issue1, 2004.

[Dut15] U.S. Attorney's Office, Central District of California, Dutch National Indicted on Computer Hacking and Identity Theft Charges Related to Theft of Digital Versions of Three Hollywood Movies, http://www.fbi.gov/losangeles/press-releases/2015/dutch-national-indicted-on-computer-hacking-and-identity-theft-charges-related-to-theft-of-digital-versions-of-three-hollywood-movies, February 24, 2015

[Ema14] U.S. Attorney's Office, Eastern District of Pennsylvania, Computer Hacker Sentenced for E-Mailing Bomb Threat to Shopping Mall, http://www.fbi.gov/philadelphia/press-releases/2014/computer-hacker-sentenced-for-e-mailing-bomb-threat-to-shopping-mall, October 17, 2014

[IC316] Federal Bureau of Investigation Internet Crime Complaint Center, Annual Reports, http://www.ic3.gov/media/annualreports.aspx, 2016

[Fra14] U.S. Attorney's Office, Eastern District of New York, Reward Money Offered for Information Leading to Arrest of Two Fugitives Charged in Multi-Million-Dollar International Cyber Fraud Scheme, http://www.fbi.gov/newyork/press-releases/2014/reward-money-offered-for-information-leading-to-arrest-of-two-fugitives-charged-in-multi-million-dollar-international-cyber-fraud-scheme, November 18, 2014

[Fur01] S. M. Furnell, The problem of categorising cybercrime and cybercriminals. In *Proceedings of the 2nd Australian Information Warfare and Security Conference*, Sydney, Australia, 2001.

[GF06] Sarah Gordon, Richard Ford, On the definition and classification of cybercrime, Journal in Computer Virology, Volume 2, Issue 1, pp 13-20, August 2006

[Ind14] Indiana grandmother suffers violent SWAT raid after a neighbor uses her wireless internet, http://www.policestateusa.com/2014/louise-milan/, August 16, 2014

[Kra11] David Kravets, Wi-Fi–Hacking Neighbor From Hell Sentenced to 18 Years, http://www.wired.com/2011/07/hacking-neighbor-from-hell/, 07.12.11

[Man13] Mandiant, APT1 Exposing One of China's Cyber Espionage Units, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf, February 18, 2013

[Nga10] Madison Ngafeeson, Cybercrime Classification: A Motivational Model, *Proceedings of Southwest Decision Sciences Institute Conference*, 2010

[PACER16] Public Access to Court Electronic Records (PACER), https://www.pacer.gov/, 2016

[Ulb13] United States Of America -V- Ross William Ulbricht, http://krebsonsecurity.com/wp-content/uploads/2013/10/UlbrichtCriminalComplaint.pdf, 2013

[Ulb15] U.S. Attorney's Office, Southern District of New York, Ross Ulbricht, the Creator and Owner of the Silk Road Website, Found Guilty in Manhattan Federal Court on All Counts, http://www.fbi.gov/newyork/press-releases/2015/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhattan-federal-court-on-all-counts, February 05, 2015

[Ulb16] Runa Sanvick, Feds Reveal Arrest Of Another Silk Road Vendor, Did He Become An Informant?, http://www.forbes.com/sites/runasandvik/2013/11/07/feds-reveal-arrest-of-another-silk-road-vendor-did-he-become-an-informant/

[REC16] RECAP The Law, https://www.recapthelaw.org/, 2016

[SD14] U.S. Attorney's Office, District of South Dakota, Sturgis Sting Operation Nets Five Arrests for Sex Trafficking, http://www.fbi.gov/minneapolis/press-releases/2014/sturgis-sting-operation-nets-five-arrests-for-sex-trafficking, August 14, 2014

[Sie15] Larry J. Siegel, *Criminology: The Core*, Cengage Learning; 5 edition (January 1, 2014)

[Sti07] U.S. Department of Justice, Office of Community Oriented Policing Services, Problem-Oriented Guides for Police, Response Guides Series, No. 6, Sting Operations, October 2007

[SWL10] Amber Stabek, Paul Watters and Robert Layton, The Seven Scam Types: Mapping the Terrain of Cybercrime, in *Proceedings of the 2010 Second Cybercrime and Trustworthy Computing Workshop* (*CTC*), 2010

[Sym15] Symantec, Internet Security Threat Report, https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf, 2015.

[Sym15] Symantec, Internet Security Threat Report Appendices, https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347931_GA-internet-security-threat-report-volume-20-2015-appendices.pdf, 2015.

[Tar14] Declaration of Christopher Tarbell, http://antilop.cc/sr/files/2014_09_05_Declaration_of_Tarbell.pdf, Sep. 5, 2014

[Tor16] Tor, Anonymity Online, https://www.torproject.org/, 2016

[Tho11] Carolyn Thompson, Innocent Man Accused Of Child Pornography After Neighbor Pirates His WiFi, http://www.huffingtonpost.com/2011/04/24/unsecured-wifi-child-pornography-innocent_n_852996.html, 04/24/2011

Appendix

This appendix provides the definition of the list of FBI IC3 complaint/crime categories. The definition comes from FBI IC3 2009 and 2010 reports, Internet and our understanding and summary.

Advance Fee Fraud: A fraudster asks a victim to pay a fee in various forms such as taxes, processing fees, or charges for notarized documents before receiving either money or merchandise. The victim receives nothing after paying the fee.

Auction Fraud: A victim pays for products advertised at an Internet auction site, but receives nothing.

Blackmail/Extortion: A fraudster asks a victim to purchase silence. Otherwise, detrimental information will be released to the public, relatives, or other parties of interest.

Charity Fraud: A fraudster sends emails soliciting compassionate and charitable payment.

Consumer Complaint (non-auction): A complainant complains about a non-auction related incident and notifies the law enforcement of the spam. There is no financial or physical loss in the incident.

Counterfeiting/Forgery: These two terms are associated. The intention of both counterfeiting and forgery is to defraud. Counterfeiting is the fabrication of complete false documents or products. Forgery is a broader concept. It includes counterfeiting and the act of altering genuine documents to defraud.

Credit/Debit Card Fraud: A fraudster uses a credit/debit card to advance money or purchase property without authorization.

Computer Damage (Destruction/Damage/Vandalism of Property): The purpose of the crime is to incur damage to computers. This is the computer focused attack in this paper.

Drug/Narcotic Offenses: The offense involves illegal drug or prescription drug trafficking online.

Business/Employment Fraud: A fraudster offers fake business/employment opportunities online. A victim may be asked to surrender personal information or perform illegal acts such as reshipping goods purchased through counterfeit cards. Business/employment frauds may involve other criminal acts like identity theft, freight forwarding, and counterfeit check schemes.

FBI Scams: A victim is defrauded by a criminal posing as an FBI agent.

Gambling Offenses: Gambling offenses range from operating illegal, unregistered gambling rings, placing illegal wagers, collecting illegal debts, and other illegal activities related to an unregistered place of wager.

ID Theft: In these incidents of ID theft, the identity of a victim is stolen while the physical entities like credit cards may not be stolen. Identity theft often fosters other types of fraud schemes.

Illegal Business: Illegal business involves trafficking in illegal goods such as selling stolen or counterfeit things or other illegal business.

Intimidation: This includes non-terrorist-related threats, forum abuse and cyber-stalking.

Investment Fraud: A fraudster seeks investments or loans with false or fraudulent claims, or provides forged or counterfeit securities for the purchase, use, or trade.

Miscellaneous Fraud: It refers to frauds that are not explicitly listed by FBI IC3. It refers to fraudulent *attempts* such as work-at-home scams, fraudulent sweepstakes and contests, economic stimulus scam and other fraudulent, the purpose of which is to get the victim to send money while nothing is bought or sold.

Non-Delivery of Merchandise (non-auction): In this type of incident, a purchaser did not receive purchased items, or a seller did not receive payment for sold items. These incidents are not related to online auction.

Overpayment Fraud: In this type of fraud, a fraudster sends a victim an invalid monetary instrument and instructs the victim to deposit it in a bank account. However, the victim needs to sends excess funds or a percentage of the deposited money back to the sender.

Pornography/Obscene Material: Pornography/obscene materials involve child pornography, obscenity, making available sexually explicit materials to minors, sexual solicitation/obscene communications with minors, transmitting obscene materials to minors, sexual abuse, sexual harassment, other sexual offenses, luring/traveling.

Prostitution (NIBRS: Prostitution Offenses): Prostitution involves offers (oneself or another) for sexual activity in exchange for money. The National Incident Based Reporting System (NIBRS) offenses include prostitution and assisting or promoting prostitution.

Relationship Fraud: Fraudsters use the online dating and social networking sites as springboards for meeting people and committing what is commonly known as "romance fraud." Fraudsters may also hack a victim, portray to be the victim and send a notice to their contacts.

Rental Fraud: A fraudster posts via classified advertisement websites. The scammer duplicates postings from legitimate real estate websites and reposts these ads, after altering them. The scammers often use the broker's real name to create a fake email, which gives the fraud more legitimacy. Here is an example of the process of rental fraud. When the victim sends an email through the classified advertisement website inquiring about the home, they receive a response from someone claiming to be the owner. The "owner" claims he and his wife are currently on missionary work in a foreign country. Therefore, he needs someone to rent their home while they are away. If the victim is interested in renting the home, they are asked to send money to the owner in the foreign country.

Spam: Spam refers to unsolicited and unwelcome email, usually mass distributed.

Stolen Property Offenses: The crime involves buying, selling, and transporting stolen property. Example crimes include music piracy, software piracy, non-auction sale of stolen goods, and online copyright infringement.

Terrorist Threat: The purpose of terrorism is to cause terror. Example cyber terrorist threats include online terrorist threat (where a criminal declares the intent to commit a crime of violence against a person, building, facility, or public or private habitat), terrorist funding, terrorist information, terrorist recruiting and other terrorist.