Criminal Law Perspectives of Contemporary Issues in Computer Security

Sergio Caltagirone
University of Idaho
scaltagi@acm.org

Abstract

In this paper, an analysis of some contemporary computer security issues will be discussed with regard to the criminal law. The paper takes a close look at hacking, active defense, vulnerability publishing, and the hacker community. For each issue, the relevant legal issues and concepts are presented, and then the elements are discussed to determine the potential outcome of each element. The purpose of which is to allow the reader to explore computer security issues from the legal perspective rather than from the technical.

1. Introduction[1]

Computer crime has recently become a popular subject. With the rise of virus publication and hacker activity, most of the population is now aware of security vulnerabilities and searching for answers. Obviously, our societies will turn to the proven methods that have kept us safe for centuries – the criminal law. The question that many of us face is: how does the criminal law apply to contemporary computer crime? This question stems from a misunderstanding and misinterpretation of the crime statutes and how they have been applied in the past. This paper attempts to rectify the problem by allowing the reader to explore computer crime from the legal perspective rather than the technical.

In this paper, an analysis of some contemporary computer security issues will be discussed with regard to the criminal law. A realistic hypothetical case will be posed, which presents some of the challenges of computer security; we will then analyze the elements of the case with regard to criminal statutes to determine where criminal liability and challenges for legal interpretation exist. To do this, a simple format will be utilized. First, the case will be presented, including all relevant details. Second, each element of the case will be discussed in an order (reverse chronological) that lends itself most to legal analysis. To make it easier for the reader, preceding each element discussion will be a section that details the relevant statutes and legal analysis that apply to the element to be discussed.

[1] No analysis, opinion, or statement within this work is, or shall be construed as, legal advice and should not be relied upon in any setting as fact.

2. Hypothetical Case

This is a description of a hypothetical case that contains elements of actual events; however, the order, names and details of the elements have been manipulated and altered for the purposes of this paper, any references to actual people, companies, or products is purely coincidental. Some elements of the case presented are left ambiguous as to allow for greater discussion, especially with regard to actors' mens rea.

Zulu Software is a new company that has just released its first product, SecureServe. SecureServe is a middleware application developed for organizations that conduct a high volume of secure transactions via the Internet. As middleware, SecureServe sits between databases and user applications to provide seamless communication. The software has been marketed as extensively tested and highly secure.

Winning Enterprises, an information portal service based in the United States, offers its customers the ability to conduct secure transactions via the Internet (HTTP and web pages). Customers contract with Winning to host their databases and support the user applications used in their organizations. Winning is interested in investing in a new middleware package to handle the increased number of transactions from its recent expansion serving financial institutions. After much research, Winning has decided to deploy SecureServe from Zulu Software on its servers. These servers will now handle approximately 1,000,000 financial transactions and 7,000,000 medical transactions a day.

Mercy Medical is one of Winning's customers and has contracted with Winning to host their medical databases in a secure environment, and to support the applications that hospitals and clinics use to access patient information. In addition to Mercy, Goal Financial also uses Winning to host their financial databases and conduct credit card transactions as well as allowing customers to access information via the Internet.

Paul is an independent security researcher. Paul's bank, Omega Bank, contracts with Winning Enterprises to provide online customer service for customers like Paul. On April 14, Paul was watching the network traffic

between Omega and Paul's computer when he was checking his bank balance online. Paul noticed that there was a strange pattern in the data and decided to investigate. Paul discovered that if a certain number of network data packets were sent at the right time with the right data, Paul could then access the bank's server as an administrator. As administrator, Paul would then have near unlimited access to the server (and potentially what it was connected to).

To test his theory, Paul wrote a quick computer program (script) to send the correct network packets in the right order, and at the right time to gain administrator access. It worked; however, Paul did nothing more than gain administrator access, he accessed no file or data – he only wanted to prove that the vulnerability actually existed as he theorized.

Paul quickly contacted Omega Bank about the problem. However, their customer service did not know what to do with the report Paul sent, or even if it could be trusted – they did nothing with it. About a week later, and after repeated contacts with Omega Bank customer service, Paul decided that Omega was not interested in fixing the problem.

At this point, Paul wanted to alert his bank and other organizations that the software is flawed, and force them to fix their software so that their systems cannot be easily exploited and Paul's information will be safe. Paul decided that since he could not get any reaction from them through the regular channels of customer service, he would publish his 'proof-of-concept' script so that they would take him warning seriously.

Elsewhere, two 'hackers,' Jim and Terry met in an Internet chatroom. Both had spoken before of their previous criminal activity – and knew each other. Terry, the more experienced hacker, informed Jim that he found a script on the Internet, one which could potentially be used to gain 'root' access to a server, so that he exploit a financial service. At that point, Jim asked Terry where to find the script; Terry explained that he has a copy and sent it to Jim via email. Terry wished Jim good luck and happy hunting – the two then parted.

Jim then searched for a server to exploit with his new script. He quickly found the servers of Winning Enterprises, and ran the script to find that it worked as advertised and Jim was able to access the server as an administrator. After initial access, Jim was able to create a new user for him to use to further exploit the server. Jim then logged into the new user and started searching for other servers connected to the exploited machine and came upon the medical and financial databases of Mercy Medical and Goal Financial.

While Jim was exploring Winning's databases, Winning's network security system, comprised of a network level intrusion detection system (IDS), and a host based IDS on the database servers detected a potential attack. The security system immediately alerted the security staff, which identified the problem and confirmed that there was an unauthorized user exploring sensitive material in their databases. Winning had already developed an Active Defense policy for mitigating threats such as this. Since Winning cannot allow an unauthorized user access to their databases, and shutting down service is not an option (medical and financial services require their databases), their only option is shut down the attacker.

Winning's security system rapidly created a computer virus to attack the attacker's computer and shut down the attacker's network access for a short period of time (24 hours) so that they had an opportunity to contact law enforcement. The security staff got the go-ahead from the Chief Security Officer (CSO), and the virus was launched against the attacker.

The virus was sent against Jim's computer, which exploited security vulnerabilities in Jim's operating system to install itself within his system. Jim lost all network connectivity and the attack was discontinued. Jim no longer attacks servers using the script he received from Terry.

3. Background Legal Concepts

To understand the following discussion, it is necessary to present to the reader a short introduction of a few legal concepts.

First of all, it is important to note that the discussion will use concepts primarily from the Model Penal Code (MPC). The Model Penal Code was developed by The American Law Institute in 1962 in an effort to assist legislators reconcile the criminal statue with contemporary legal understanding. [1] Since its inception, the MPC has been a strong influence in the redevelopment of both federal and state statutes; in fact, many statutes simply mirror the text of the MPC. Therefore, for our purposes, the MPC will serve as our penal code; but when serious inconsistencies exist (or a particular statue does not exist), federal and particular state statutes will be examined as well.

An offense is made up of three parts (which can contain zero or more elements), the actus reus, the attendant circumstances, and the result. Additionally, mens rea is attributed to each element of the offense. The actus reus is the voluntary action (or omission) of a person, which causes a result. An attendant circumstance is simply a

fact surrounding an event. The result of an offense is simply that, result of conduct of an actor.

More abstract than the actual elements of the offense, is the concept of mens rea. Mens rea is the actor's mental state with respect to each element. Important in the concept of mens rea is that each element of the offense may have a different level of mens rea; and therefore each element's mens rea requirement must be inspected. The MPC makes it clear that for an actor to be guilt of an offense, they must have acted either purposefully, knowingly, recklessly, or negligently, with respect to each element of the offense. Where the MPC defines these as,

Purposefully (MPC 2.02(2)(a)): A person acts purposefully with respect to each to each element of the offense when…(i) it is his conscious object to engage in conduct of that nature or to cause such a result; and (ii) if the element involves the attendant circumstances, he is aware of the existence of such circumstances or he believes or hopes that they exist. [1]

Knowingly (MPC 2.02(3)(b)): A person acts knowingly with respect to a material element of an offense when…(i) he is aware that his conduct is of the nature that such circumstances exist; and (ii) he is aware that it is practically certain that his conduct will cause such a result. [1]

Recklessly (MPC 2.02(3)(c)): A person acts recklessly with respect to a material element of an offense when he consciously disregards a substantial and unjustifiable risk that the material element exists or will result from his conduct. [1]

Negligently (MPC 2.02(3)(d)): A person acts negligently with respect to a material element of an offense when he should be aware of a substantial and unjustifiable risk that the material element exists or will result from his conduct. [1]

Additionally, the mens rea definitions have an explicit hierarchy, such that Purpose > Knowledge > Reckless > Negligent; and so if negligent is the requirement, then it is sufficient if recklessness, knowledge, or purpose can be shown, and if knowledge is required, then purpose or knowledge suffices, etc.

4. Underlying Offense (Hacking)

We will begin our discussion with what seems the last element of the case, Jim's use of the script to enter Winning's systems. This may seem as working backwards, but, as we'll see, every other offense and element of the case stems from the underlying offense; it then makes it logical to start with the underlying offense. Furthermore, other offenses and concepts, such as conspiracy, aiding and abetting, and causation are dependent on the underlying offense.

4.1. Legal Background

4.1.1. The Computer Fraud and Misuse Act (18 USC 1030)

In 1986, federal legislators realized the need to formally criminalize computer misuse. Prior to 1986, any computer misuse was prosecuted, if at all, under theft and fraud offenses. However, the theft and fraud statutes were not designed to prosecute offenders that not stealing data or entering systems fraudulently – although some argued otherwise. To remedy the situation, the US congress formalized a statute that would make computer misuse its own crime: The Computer Fraud and Abuse Act (18 USC 1030). It has gone through several revisions since its inception in 1986, and its current form was adopted in 1999.

For our purposes, the important parts of the code are:
(a) Whoever…(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(a)(5)

(A)(i) Knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused) –

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical

examination, diagnosis, treatment, or care of 1 or more individuals;

(e)(2) A "protected computer" means a computer (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(e)(4) A "financial institution" means
(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(e)(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

(e)(8) The term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;

As can be seen, 18 USC 1030 is very limited in its effect on computer crime. It limits itself to primarily government and financial systems (with some protection of medical records). Because of this, most State and Federal prosecutors have used the Wire Fraud statutes; however, these become questionable when the hacker acquires property of little financial value – or simply enters a system without damage.

4.1.2. Significant Case Law Regarding 18 USC 1030

United States v. Sullivan, 40 Fed. Appx. 740 (2002): In (e)(8), damage need not be "actual destruction of a computer system." [2]

United States v. Czubinski, 106 F.3d 1069 (1997): Simply browsing taxpayer's information without intent to commit fraud (nothing "more than to satisfy curiosity") is not criminal under 18 USC 1030. [3]

United States v. Middleton, 231 F.3d 1207 (2000): The court found that the word "person" (5)(B)(i) refers to corporations as well as individuals. Also, the court found that the $5000 damage threshold necessary to find criminal liability, can be met using "any loss that you find was a natural or foreseeable result of any damage that occurred," including costs "to restore the data, program, system, or information that you find was damaged or what measures were reasonably necessary to re-secure the data, program, system, or information from further damage." [4]

United States v. Morris, 928 F.2d 504 (1991): Intention is only necessary with regard to unauthorized access and not damages caused, pursuant to (a)(5)(A). [5]

United States v. Sablan, 92 F.3d 865 (1996): Upheld the Morris decision in that the mens rea requirement of intention is only applied to unauthorized access, which meets constitutional standards for the statute. [6]

Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 199 F.Supp.2d 1121, 1128 (W.D. Wash. 2000): The court greatly expanded the understanding of "protected computers" to mean any computer connected to the Internet; and also broadens the meaning of "exceeding authorized access" to using pre-existing authorization to "obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." [7]

4.1.3. Computer Trespass

As the reader can see, the current federal law does not protect systems that are not governmental, financial or medical. As the court in *Shurgard* noted, Congress purposefully limited itself to computers where "there is compelling Federal interest," and left the states to enact their own laws. [7] As such, several states have created separate computer crime laws that are much more generally applicable to most computer hacking. These state statutes make it a crime to intentionally access a computer in an unauthorized manner. A few of the state statutes are given here for comparison.

Rhode Island §11-52-3: Whoever, intentionally and without authorization, directly or indirectly, accesses, alters, damages, or destroys any computer, computer system, computer network, computer software, computer program, or data contained in a computer, computer system, computer program, or computer network shall be guilty of a felony…

Virginia Computer Crime Act §18.2-152.5: A person is guilty of the CRIME of COMPUTER invasion of privacy when he uses a COMPUTER or COMPUTER network and intentionally examines without authority any employment, salary, credit or any other financial or personal information relating to any other person. "Examination" under this section requires the offender to review the information relating to any other person after the time at which the offender knows or should know that he is without authority to view the information displayed.

The University of Dayton School of Law has drafted a Model State Computer Crimes Code for the purpose of assisting state legislators with the design of their own computer crime statutes. [8]

Model State Computer Crime Code §4.01.1: (A) No person shall purposely, knowingly or recklessly gain access to or cause access to be gained to any computer, computer system, computer network, computer program, computer data base, or computer material without the express or implied authorization of the owner or an agent of the owner empowered to authorize access to the computer, computer system, computer network, computer program, computer data base, or computer material. Any person who violates this section is guilty of the crime of computer trespass.

4.2. Analysis

The first step in our analysis is to determine whether the actus reus was voluntary, and without justification (duress, self-defense, necessity, etc). Clearly, Jim's actions constitute an overt act: he searched for computers that could be compromised, executed the script, and then entered the computers. Following which, he created a new user, logged into that user, and then began exploring financial and medical databases. Since he was not under duress, or threat, nor was he exploiting the server to protect another or himself, there is no justification available to Jim.

Now let us look at Jim's first acts: scanning exposed computers, executing the script, and then entering the computer. At this point, Jim would only be guilty of a crime if he had committed these acts in a state with computer crime statutes. Let us assume he had. If we take the Model State Computer Crime Code of the University of Dayton, then to be guilty, Jim must (1) access to or cause access to be gained to (2) any computer system, computer network, computer program, computer database, or computer material (3) without the express or implied authorization of the owner… Obviously Jim has completed act 1 by using the script and gaining access; and we know from the facts of the case that he was indeed in a computer system and network, satisfying act 2.

Additionally, nothing suggests that Jim had authorization, explicit or implied to access the system. However, an argument can be made that since users are allowed to access the web server, and Jim was also accessing the web server (albeit in a different way), that he had obtained implicit authorization. The *Morris* court answered this question when they held that a computer user, with authorized access to a computer and its programs, was without authorization when he used the programs in an unauthorized way. Therefore, upon the findings in *Morris* and *Shurgard*, although a user has been given some privileges, those do not extend to others not explicitly granted.

As for the mens rea requirements, most state (and federal) statutes require intentional unauthorized access – we then have to show intent. Since, Jim knew that the script gained a user administrator access (from the chatroom discussion with Terry), and Jim also knew that he did not have authorized permission to access the system as an administrator, it is clear that the only reason Jim would have used the script would be if his intent was to gain administrator access to the box –and is then guilty under some computer trespass statutes. Moreover, if the statute requires that damage be done, Jim would also be guilty because creating a new user would have put the system into an unauthorized state, and an administrator would have to expend resources to restore the system (as per *Middleton*).

Let us now examine Jim's second act: accessing Winning's financial and medical databases. According to the findings in *Czubinski*, simply browsing records does not amount to a crime under 18 USC 1030. However, if Jim had recorded any information, such as account numbers, social security numbers, names or addresses, then he would have obtained financial data, and been guilty under 18 USC 1030 (a)(2)(A).

5. Winning's Active Defense Response

Active defense is a security concept where an organization takes steps to mitigate threats to their assets during an attack. These active defense responses can take the form of shutting down communication to the server, or even go as far as attacking the attacker. It is currently a debated topic on whether Active Defense is legal or ethical. One potential scenario is presented here, and analysis given as to the legality of such action.

5.1. Legal Background

5.1.1. Necessity Defense

It is obvious that at times, and in certain circumstances there is no alternative to breaking the law. The law anticipates these circumstances, and so devised the necessity defense: when faced with a number of horrible choices, a person may choose the best one regardless of legality. However, the necessity defense does not remove the legal liability of the actor, they are still guilty of the offense; but rather, the law has decided that it serves no purpose to punish in these cases.

The Model Penal Code developed the Choice of Evils justification for the purpose of providing a justification in a case of necessity.

§3.02

(1) *Conduct which the actor believes to be necessary to avoid a harm or evil to himself of another is justifiable, provided that:*
    a. *The harm or evil sought to be avoided by such conduct is greater than that sought to be prevented by the law defining the offense charged; and*
    b. *Neither the Code nor other law defining the offense provides exceptions or defenses dealing with the specific situation involved; and*
    c. *A legislative purpose to exclude the justification does not otherwise plainly appear.*
(2) *When the actor was reckless or negligent in brining about the situation requiring a choice of harms or evils or in appraising the necessity for his conduct, the justification afforded by this section is unavailable in a prosecution for any offense for which recklessness or negligence, as the case may be, suffices to establish culpability. [1]*

There are a couple of interesting points in the statute provided by the American Law Institute. First, there must be a quantifiable benefit to breaking the law (1)(a). Upon prosecution, it must be quantifiably proven that the choice was the best one. Second, the actor cannot have been reckless or negligent in bringing about the situation – they cannot be the instigators (2); and also the justification is not available to offenses where recklessness or negligent is the mens rea requirement. These specifications are provided to guarantee that the necessity defense will only be utilized in situations where society does not wish to punish a person for their choice.

There are two approaches to a necessity defense statute. The first is that of the Model Penal Code, the second is illustrated by New York. The New York statute requires that the conduct must be such that it qualifies as "an emergency measure to avoid an imminent…injury." This requirement forces the defendant to prove the imminence of the harm to be avoided, and removes the defense from those who act to stop great future harms.

5.1.2. Significant Case Law Regarding the Necessity Defense

United States v. Schoon, 971 F.2d 193 (1992): To invoke the defense, the defendant must show that: (1) they were faced with a choice of evils and chose the lesser evil; (2) they acted to prevent imminent harm; (3) they reasonably anticipated a direct causal relationship between their conduct and the harm to be averted; and (4) they had no legal alternatives to violating the law. [9]

5.2. Analysis

First, lets enumerate Winning's actions. The company, in order to protect their customer's sensitive data, as well as a potentially danger situation if an unauthorized individual was to change medical records, decided to take steps against the hacker rather than stopping their service. To do this, Winning tracked the hacker down to Jim's IP address (a unique address that identifies a specific computer). The company then wrote a virus, designed to only attack the IP address they had tracked. The company then sent the virus out, which searched for Jim's IP address and installed itself on Jim's computer using a well-known operating system exploit. The virus then shut down Jim's network access, with a special rule that it was to disable itself after 24 hours.

Within 18 USC 1030, the computer fraud and misuse act, Winning's actions are obviously illegal. They obtained unauthorized access to Jim's computer (through the use of the virus and exploit) (a)(2), and then transmitted code that caused damage to a protected computer (a)(5)(A)(i). Pursuant to *Shurgard v. Safeguard*, Jim's computer was considered a 'protected computer' under 18 USC 1030 because it was connected to the Internet. The mens rea of the company was clearly and unambiguously intentional, they created the virus specifically to attack Jim's computer and disable his network access.

Although the company is criminally liable for their actions, they may be able to assert the necessity defense as a justification of their actions. To accomplish this justification, Winning must satisfy each of the requirements provided by *Schoon*.

First, Winning was faced with a number of choices: do nothing, alert law enforcement, shut down service, or attack Jim. Obviously, since medical services rely on Winning's databases as a repository of patient history and other life-critical information, shutting down the service may cost lives. Additionally, doing nothing and allowing the attack to continue may have caused the same outcome as shutting down the service (attacker could change patient data or shut down service themselves). Alerting law enforcement, while important, would not have prevented the attacker from shutting down the service at any time. Therefore, since shutting down the service, either by Winning, or the attacker, is not an option, then they must shut down the attacker – hence the action taken by Winning.

Second, Winning did act to prevent imminent harm since at any second, service could have been lost, which would have cost lives. Third, releasing a limited virus was a direct causal relationship to their action and harm being prevented; because shutting down the attacker's network access would have prevented further harm to the system. Fourth, although Winning contacted law enforcement,

there was no other legal action available to them at the time. As provided by *Schoon*, this analysis shows that Winning chose the correct action to prevent any loss of life.

Moreover, as pertaining to the MPC statute, Winning was not negligent in bringing about the harm since they had no knowledge (or could not have known) about the exploit which was recently released. Also, 18 USC 1030 provides an intent requirement with regard to the offense, allowing Winning to assert this defense.

6. Terry and Jim in Chatroom

The scenario of Terry and Jim in the chatroom is very common in the real world when it comes to the hacker community. Most hackers get exploit scripts and other information from other hackers in Internet Relay Chat (IRC). This can be analogized from other criminal activity: two men get together and one tells the other one how to rob a bank. The question is: how does the criminal law address this situation? The answer lies in both conspiracy and aiding and abetting statutes.

6.1. Legal Background

6.1.1. Conspiracy

The MPC defines conspiracy as

§5.03

(1) A person is guilty of conspiracy with another person or persons to commit a crime if with the purpose of promoting or facilitating its commission he:
- *a. Agrees with such other person or persons that they or one or more of them will engage in conduct with constitutes such crime or an attempt or solicitation or commit such crime; or*
- *b. Agrees to aid such other person or persons in the planning or commission of such crime or of an attempt or solicitation to commit such crime.*

(2) No person may be convicted of conspiracy to commit a crime…unless an overt act in pursuance of such conspiracy is alleged and proved to have been done by him or by a person with whom he conspired.

Generally, conspiracy is the agreement of two or more persons to commit a crime, which is followed by an act to actually commit the crime. Additionally, the agreement may be spoken or unspoken.

6.1.2. Significant Case Law Regarding Conspiracy

Pinkerton v. United States, 328 U.S. 640 (1946): The result of the conspiracy must be foreseeable to the co-conspirators. [10]

6.1.3. Aiding and Abetting

The aiding and abetting statutes were designed to deter people from helping others commit crimes. What is misunderstood is that aiding and abetting is not actually a crime. Aiding and abetting is a method of making one person liable for another's illegal actions. Therefore, aiding and abetting cannot occur if an illegal act did not occur, there is no concept of attempted aiding and abetting.

The MPC defines aiding and abetting as

§2.06

(3) A person is an accomplice of another person in the commission in the offense if:
- *a. With the purpose of promoting or facilitating the commission of the offense, he*
  - *i. Solicits such other person to commit it; or*
  - *ii. Aids or agrees or attempts to aid such other person in planning or committing it; or…*

Simply stated, aiding and abetting is any conduct that encourages or facilitates the offense.

6.1.4. Significant Case Law Regarding Aiding and Abetting

United States v. Peoni, 100 F.2d 401 (1938): in order to aid and abet another to commit a crime, it is necessary that a defendant in some sort associate himself with the venture, that he participate in it as in something that he wishes to bring about, that he seek by his action to make it succeed.

People v. Luparello, 187 Cal. App. 3d 410 (1987): If you aid and abet one unlawful act, but another occurs, you had to only be negligent with respect to the other.

6.2. Analysis

In this analysis, we will focus on whether Terry committed a crime during his described interaction with Jim. While not disregarding previous analyses, we will assume that Jim is guilty of computer trespass.

The facts: Terry knew of Jim's previous illegal computer activity, Terry informed Jim of a new exploit and script he had found, Terry informed Jim of the purpose of the script, Terry gave Jim a copy of the script to use, Jim used the script obtained from Terry to compromise Winning's servers.

First, let us discuss Terry's liability with respect to aiding and abetting Jim's computer trespass. Clearly, Terry provided material support to Jim for the commission of a crime. However, the important question is whether, by providing the script, it was Terry's purpose for Jim to commit the crime. For purpose, it must be shown that Terry wished or hoped that the result would occur given his action. If it was his purpose to give Jim the script to exploit systems, then Terry had acted "with the purpose of …facilitating the commission of the offense" (3)(a) and would have been guilty. If it was not his purpose, then Terry does not meet the mens rea requirement of the statute and is not liable for Jim's actions.

The fact is that an exploit has no other purpose than to enable computer trespass. Some argue that exploit scripts are proof-of-concept devices, which enable security researchers to test the exploit. However, security researchers do not need exploit script so prove that a flaw exists. Therefore, handing out the exploit script would have no other purpose than to encourage and facilitate computer trespass using the script – and would satisfy the requirement of a "it is his conscious object to engage in conduct of that nature or to cause such a result" §2.02(2)(a). [1] Using this argument, Terry is liable for Jim's act under aiding and abetting statutes.

Furthermore, since we have already determined that it was Terry's purpose to facilitate the commission of Jim's computer trespass during the aiding and abetting discussion, then the same argument is applied to conspiracy. This would satisfy §5.03 (1)(b). Additionally, there must be an overt act committed in furtherance of the crime. The overt act requirement in (2) is easily satisfied by Jim's use of the script and exploration of Winning's databases. In fact it is uncommon for an aiding and abetting charge not to be associated with a conspiracy charge.

7. Paul's Script

One of the largest debates in computer security is whether it is ethical or legal to release exploits to the public. Advocates of the practice argue that organizations that produce products disregard security warnings by users and researchers, and therefore the only way to protect the public is to actually release the exploit, which will then force the organization to fix their product. In this situation, that is exactly Paul's position.

7.1. Legal Background

All necessary legal concepts have already been discussed in previous sections.

7.2. Analysis

Sometimes security researchers are placed in difficult positions, they know that vulnerabilities exist in a system, but can do nothing about it; only hoping that hackers do not find out before the software is fixed. In this case, Paul was not so patient. He decided that in order for the company to fix their software, he must release the exploit script. Therefore, it was his purpose to release the exploit script to force the organization to acknowledge the vulnerability and fix the software. However, before the fix could be implemented and released, Jim already had access to Winning's financial and medical databases – engaging in computer trespass.

Obviously, if a security vulnerability is released to the public, the researcher is putting pressure on the company to fix their software because they both know that hackers will use that information to exploit their systems. If this weren't the case, there would be no purpose to publishing the vulnerabilities – because it would not pressure the company any more than simply informing them privately. Therefore, it can be concluded that when releasing an exploit to the public, it is purposefully providing a tool to hackers to exploit systems.

If our conclusion is correct, and we can assume that Paul's purpose was to provide a tool for hackers to exploit systems – then he aided and abetted any criminal activity using his script, including Jim's computer trespass. *Peoni* also supports our conclusion because Paul wished to bring about a fix in the software by releasing the exploit script, and by his action sought to succeed. However, if it was not Paul's purpose that the exploit script be used to commit computer trespass, and since he did not commit a crime by releasing the script, then he would not be liable for Jim's criminal activity.

8. Conclusion

The purpose of this paper was to present computer security researchers with an accessible introduction to the legal issues in computer security. To do this we developed a hypothetical case to analyze. The case involved hacking, active defense, and vulnerability publishing; these are contemporary computer security issues that are important to discuss. However, most do not understand the legal concepts that apply to these issues, or how these concepts are applied.

In this paper, I have attempted to discusses these important security topics and make them as relevant to the reader as possible; discussing the necessity defense, the Computer Fraud and Misuse Act, conspiracy and aiding and abetting. Hopefully, the reader will be able to take this knowledge and apply legal concepts to future security issues.

9. References

[1] American Law Institute., *Model penal code : official draft and explanatory notes : complete text of model penal code as adopted at the 1962 annual meeting of the American Law Institute at Washington, D.C., May 24, 1962*. Philadelphia, Pa.: American Law Institute, 1985.

[2] "United States v. John Michael Sullivan," in *Fed. Appx.*, vol. 40: United States Court of Appeals for the Fourth Circuit, 2002, pp. 740.

[3] "United States v. Richard W. Czubinski," in *Federal Reporter*, vol. 106: United States Court of Appeals for the First Circuit, 1997, pp. 1069.

[4] "United States v. Nicholas Middleton," in *Federal Reporter*, vol. 231: United States Court of Appeals for Ninth Circuit, 2000, pp. 1207.

[5] "United States v. Robert Morris," in *Federal Reporter*, vol. 928: United States Court of Appeals for the Second Circuit, 1991, pp. 504.

[6] "United States v. Bernadette Sablan," in *Federal Reporter*, vol. 92: United States Court of Appeals for the Ninth Circuit, 1996, pp. 865.

[7] "Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.," in *Federal Supplement*, vol. 199: United States District Court for the Western District of Washington, Seattle Division, 2000, pp. 1121.

[8] S. Brenner, "Model State Computer Crimes Code," vol. 2004: http://cybercrimes.net/99MSCCC/99MSCCCMain.html, 2001.

[9] "United States v. Schoon," in *Federal Reporter*, vol. 971: United States Court of Appeals for the 9th Circuit, 1992, pp. 193.

[10] "Pinkerton v. United States," in *Supreme Court Reporter*, vol. 328: Supreme Court of the United States, 1946, pp. 640.