Faking It: Calculating Loss in Computer Crime Sentencing

By Jennifer S. Granick*

DRAFT. NOT FOR CITATION.

INTRODUCTION

Thoroughly and consistently calculating losses from computer intrusions is a difficult endeavor because security incidents are characterized by intangible harms like interference with system availability and interference with the integrity of data. These harms can be difficult to translate into monetary terms. More easily measured are labor and hardware costs associated with repairing and restoring compromised systems, if there is a methodology in place for tracking these expenditures of time and money. The area of computer crime sentencing should be one where an accurate method for assessing the cost of attacks develops, since the most important factor in computer crime sentencing under the Federal Sentencing Guidelines is the harm caused by the intruder. Hundreds of computer crime cases are adjudicated in the courts every year, and in each one loss valuation factors into the disposition of the case.

However, criminal law has failed to develop a useful methodology for the accurate and consistent valuation of intrusion losses across incidents and across victims. The statute clearly contemplates that intrusions cause intangible harm by interfering with system and data integrity, but requires courts to define that damage in monetary terms without giving any guidance for how to accomplish that task. Since the labor costs for investigation and remediation are more readily measured, and specifically mentioned by statute, prosecutors and courts rely on these expenses to prove a federal crime and to sentence. Still, courts must look closely at labor costs, and not take victim assessments at face value. The legal definition of investigation and remediation expenses excludes the forensic activities first responders are taught to take following a computer intrusion. Since the burden of proof for sentencing only requires courts to decide whether the preponderance of evidence shows that the victim has made a reasonable assessment of damages, courts are not motivated to look seriously and critically at victim loss assertions. For these and other reasons, computer crime adjudications are highly irregular in damage assessment and in offender sentencing. The statute fails to discriminate well between harmful and trivial attacks. This undermines the goals of sentencing, specifically that courts should impose fair, just sentences that reflect the seriousness of the offense and treat like offenders equally. There are several legal approaches we could adopt to mitigate this problem. However, the question of how to remedy intrusions will

---

* Jennifer Stisa Granick joined the faculty of Stanford Law School in January 2001, teaching the Cyberlaw Clinic and acting as Executive Director of the Center for Internet and Society (CIS). She teaches, speaks and writes on the full spectrum of Internet law issues including computer crime and security, national security, constitutional rights, and electronic surveillance, areas in which her expertise is recognized nationally.

remain so long as there is no social consensus on the nature of the rights and property interests implicated by computer attacks.

COMPUTER INTRUSIONS CAUSE DAMAGE THAT IS NOT CONSISTENTLY OR READILY QUANTIFIABLE IN ECONOMIC TERMS

Computer attacks harm system owners and computer users in a variety of ways, some of which are easier to put a price tag on than others. Following a security breach, owners incur labor costs for investigating the incident, excluding the intruder and fixing the vulnerability that allowed unauthorized access. Owners may also incur labor and hardware costs for upgrading or improving security measures like firewalls and intrusion detection systems. In theory, these expenditures should be relatively easy to classify and quantify if the owner documents the activities responders take and the hardware they use.

While victims can readily quantify economic loss due to investigation or remediation, different victims, even faced with identical security incidents, will have different losses. Security incident investigation is something of an art, and investigations performed by different technicians will not necessarily take anywhere near the same amount of time or resources. In 2001, the Honeynet Project hosted a forensic challenge, publishing an image reproduction of a compromised system, and challenging contestants to analyze the attack and communicate what they found. The contestants were told to keep track of their time, and were given the federal statutory definition of loss as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service". Participants were instructed to assume that their salary was $70,000/year.

The challenge received 13 entries. The consensus was that the analysis of this single compromised system took quite a bit of time. Contestants finished when the contest time ran out, not when they were done. The average time spent per investigation was 48 hours. The most time spent was 104 hours. The least was 10. The winning entry took 37 hours and was submitted by a single investigator with 8 years of experience. At the $70,000 salary, the average cost per investigation was approximately $2000.

What these contest results show is that the cost of fixing a system after an attack has more to do with what actions the victim takes than with what the intruder did. Basic goals of criminal sentencing are to provide just punishment that reflects the seriousness of the offense and to treat like offenders similarly. Damage from an offense is a function of the idiosyncrasies of incident investigation, including the skills, experience, hourly rate, and remediation choices of the victim, not necessarily by the offender. As a result, similar offenders committing similar offenses will be treated differently, because victims will inevitably react differently to intrusions.

Victims' investigation and remediation choices increase when the victim feels the attack has caused or could a loss of reputation. This is true even though loss of reputation

is not and should not be remediable under the law. If harm to reputation stems from the public realization that the system was not, in fact, secure, or from public revelation of information that makes a company look bad, we may not want to remedy or punish this specific injury. Generally, U.S. law does not compensate harm to reputation resulting from the publication of true facts. Where victims clearly claim harm to reputation from either the revelation of security vulnerabilities or from the disclosure of damaging facts, the law can state that defendants will neither have to compensate nor be sentenced based on this harm. But, harm to reputation also affects victim's loss estimates as a factor in determining how much time and money a victim will spend on remediation. For example, in United States v. Jerome Heckenkamp[1], Internet auction site eBay stated that it hired several expensive consulting firms to investigate its website intrusion in order to build customer confidence. Potential harm to reputation caused the company to spend a lot more on remediation and upgrades than it otherwise would have done to reassure customers and the public. Courts that defer to victim loss assessments will have trouble factoring out harm to reputation when it takes this form.

Of course, harm from computer intrusions goes beyond the price of remedial labor and system improvements. Loss of privacy, access to confidential data, system unavailability or downgrade in system performance and sometimes the revelation of previously unknown information all harm victims. Generally, these harms are more difficult to value monetarily than labor costs. The harm can be non-economic and may not require the victim to make any financial expenditure.

It is difficult to put a price tag on the harm caused when once private data is no longer secret. I am adversely affected by knowing that an intruder, whether a stranger or someone I know, read my email without my permission. Information I wanted to keep private no longer is. There is a chance that the intruder will use the information against me in some way. Or that it will be embarrassing. Some victims of privacy invasion describe a psychological sense of violation. Yet there is no amount of money that would repair this harm. Money cannot make the victim whole.

Even where information is commercially valuable, unlike the email in the above example, there may be no readily measurable economic loss when an outsider merely accesses it. Customer lists, trade secret information or software programs under development may have no readily ascertainable market value. And it is unclear whether that value diminishes if the owner of the information retains the full ability to exploit it following unlawful access, for example when an intruder learns of company trade secrets, but does not disseminate them further. In the case of United States v. Mitnick, for example, the defendant accessed proprietary data stored on Sun Microsystems computers. Sun claimed that Mitnick caused US$80M in damages by copying the source code for its Solaris operating system. This number represented the entire research and development costs for Solaris. Yet, Mitnick did not disseminate the source code, and Sun was able to retain complete control of the product, later deciding to give the OS to customers for free.

[1] U.S. v. Heckenkamp, Northern District of California, Judge James Ware.

Did Mitnick cause Sun no damage, because he simply copied something that they were giving away for free, or did he cause US$80M in damage? Clearly, a trade secret does not necessarily lose all value to the owner simply because it is no longer secret from the attacker. Equally clear is that the victim suffers some harm from even this level of loss of secrecy. The owner does not know how far the secret was disseminated and experiences some amount of uncertainty as to the continuing viability of the secret nature of the information. But that uncertainty is not a kind of harm that is readily expressed monetarily.

These difficult questions simply illustrate that the damages characteristically caused by computer intrusions are not readily expressed in economic terms.

Given the theoretical problems with converting intangible harm to economic losses, its not surprising that individuals, businesses and government have trouble calculating the cost of computer intrusions or computer viruses. When asked to measure harm from computer intrusions, victims are not given any guidelines or methodologies with which to do so. The Computer Security Institute (CSI) and the Federal Bureau of Investigation survey CSI members every year about a host of security issues including number of security incidents and their cost. This report is the only one of its kind and is widely cited by media and industry. There are statistical and methodological problems with the survey that others have identified. But for the purposes of this paper, one of the most interesting findings is that survey respondents have trouble figuring out how to quantify loss. The 2004 survey, as in other years, showed almost half of organizations unable or unwilling to quantify financial losses.[2] Nonetheless, the media seems to trade in undocumented assessments of economic loss which to even the least critical reader are suspiciously high. For example, news outlets widely reported the mi2g consultancy firm's estimate that January 2004's "mydoom" virus cost businesses US$38.5 billion.[3] In comparison, the National Climatic Data Center estimates that 2003's hurricane Isabel, which killed over 40 people and took out power for a million, cost on US$4 billion.[4]

THE DEFINITION AND IMPORTANCE OF LOSS IN COMPUTER CRIME CASES

Computer crime sentencing requires courts to value the damage caused by a computer intrusion. By definition, damage is fundamental in the adjudication of federal computer crime cases. The Computer Fraud and Abuse Act (CFAA), codified at 18 U.S.C. 1030, prohibits unauthorized access to computer systems.[5] Damage, expressed in terms of monetary loss, is important in computer crime cases in three ways; it is an

---

[2] CSI/FBI Annual Survey (2004), p. 11. Of 494 respondents, only 269 provided loss estimates. The survey is available at no cost from http://www.csi.org.

[3] http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/press/010204.php

[4] See, http://lwf.ncdc.noaa.gov/img/reports/billion/disasters-since-1980.jpg.

[5] 18 U.S.C. 1030.

element of the crime, it is a major determinative factor in sentencing, and it is fundamental to restitution. While the statute clearly contemplates intangible harms from unauthorized access to data and systems, it requires fact finders to express those harms in economic terms.

Prior to 2001, section 1030 focused almost exclusively on economic harm from damage to computers and computer systems. Subsections (a)(1)-(4) have not been amended. Subsection (a) of the statute addresses unauthorized access to classified information. Subsection (a)(2) criminalizes unauthorized access and obtaining any information from a protected computer, but is a misdemeanor. Subsection (a)(3) criminalizes access that interferes with the ability to use a computer exclusively for government use. Subsection (a)(4) criminalizes access with the intent to defraud if the intruder obtains anything of value. Prior to the amendment, subsection (a)(5) criminalized transmissions or access that caused damage, where damage was defined as any impairment to the integrity or availability of data, a program, a system, or information that causes loss aggregating to at least $5000 to one or more person during any one year period as an element of the offense.[6] Without sufficient loss, there was no offense under (a)(5). For access to private systems, the statute required a showing of economic harm, or else the offense was a misdemeanor.

Amendments to the statute in 2001 added some special kinds of non-economic harm that could substitute for showing US$5000 in loss. The non-economic harms are "the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; access that causes physical injury to any person; a threat to public health or safety; or damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security."[7]

None of the new definitions for damage require courts to place a monetary value on intangible losses, nor do they suggest to courts how this economic calculation should be done. Rather, the statute generally defines damage as including interference with the integrity of the system and then gives specific examples of more tangible losses, including "the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[8]

Loss is not only important to defining whether a crime has occurred, but also to sentencing and to restitution. Prior to 2005, the United States Sentencing Guidelines regulated all federal criminal sentencing. The Guidelines were promulgated by the U.S. Sentencing Commission at the behest of Congress to limit judicial discretion and impose

[6] 18 U.S.C. §1030(a)(5)(B)(i).
[7] 18 U.S.C. 1030 (a)(5)(B)(ii)-(v).
[8] 18 U.S.C. 1030(e)(11).

order on federal sentencing across districts. The guidelines establish a base offense level (BOL) for various crimes, and then list various factors that increase or decrease the sentence. Once the sentencing court determines the total offense level taking all the mitigating and aggravating factors into consideration, and considers the defendant's prior criminal history, the Guidelines prescribe a period of incarceration. In the absence of extraordinary circumstances, the sentencing court must choose a sentence within the small range of months of incarceration the Guidelines prescribe.

Economic loss is a major factor in computer crime sentencing under the guidelines. For the purposes of sentencing, loss is defined in the same economic terms as under the statute. That monetary value is then heavily weighted in sentencing. Section 2B1.1 of the United State Sentencing Guidelines applies to CFAA violations. Section 2B1.1 has a BOL of 6 and dictates a 2 to 30 level upward adjustment for loss. If lost is $30,000, the loss adjustment is 6 levels. Thus, at $30,000 loss or more, over half the defendant's sentence may be determined by loss alone.[9]

Finally, the amount of economic loss directly affects restitution orders. Under non-mandatory restitution provisions, the court is to consider the amount of the loss sustained by each victim as a result of the offense.[10] In the case of an offense that damages or causes loss to property, the statute requiring mandatory restitution requires defendants to pay:

> (i) the greater of--
> (I) the value of the property on the date of the damage, loss, or destruction; or
> (II) the value of the property on the date of sentencing, less
> (ii) the value (as of the date the property is returned) of any part of the property that is returned.

Defendants also must "reimburse the victim for lost income and necessary child care, transportation, and other expenses incurred during participation in the investigation or prosecution of the offense or attendance at proceedings related to the offense."[11] The federal code establishes a procedure whereby the U.S. Probation Department collects evidence from victims, prosecution and defense about the appropriate amount of restitution.[12] Whatever restitution scheme applies, sentencing courts are obligated to put a

---

[9]The BOL for violations of 18 U.S.C. 1030 that do not involve state secrets is six (6). U.S.S.G. 2B1.1(a)(2). The guidelines add an additional six (6) levels for loss greater than $30,000, and continue increasing up to an additional 30 levels.
[10]18 U.S.C. 3663.
[11]18 U.S.C. 3663A(4). At least one court has held that restitution following conviction of 18 U.S.C. 1030 is mandatory under section 18 USC 3663A. See United States v. Harris (2nd Cir. 2001) 302 F.3d 72, 75. See also 18 U.S.C. 3663A(c)(1).
[12]18 U.S.C. 3664.

monetary value on the harm from the offense and to receive input, either directly or indirectly through the probation department from both the government and the defendant.

Statutory and guideline definitions require economically expressible losses for prosecution and punishment of computer intrusions. As courts look to the cost of investigation and remediation as a measure of a defendant's guilt, cases involving intangible harms, but no economic ones, are unlikely to be pursued. Thus, invasions of victim privacy, for example, will not be prosecuted unless the victim can come up with additional economic harms. Section 1030 provides a civil remedy for victims, and in several cases victims have failed to obtain redress because harm to their privacy interests were not economically calculated to exceed US$5000.[13]

The focus on economically expressible losses makes sense if we want computer crime offenses to be proportionate, fair and regular. The process is far more certain and less susceptible to victim manipulation of the sort seen in the Mitnick case if courts use concrete provable damages rather than theoretical or speculative ones.

The risk is that the statute under-protects people from harms to privacy and other intangible interests. Most interestingly, the statute also overprotects victims who chose a lengthy and expensive investigation and remediation response, regardless of the sensitivity of their systems or the extent of the offender's unauthorized access. Victim loss assessments often include the cost of improving their system and helping law enforcement or planning for a civil case. Defendants do more time as a function of forensic costs, system improvements, and decisions to pursue investigation over restoring the system to working order.

REMEDIATION DOESN'T FIT THE LEGAL DEFINITION OF LOSS

Courts have good cause to look more closely at victim loss estimates because they tend to include losses that are excluded by law. Despite the importance of "loss" in computer crime cases, the factor is defined in a way that does not accord with the real-world effects of computer crime. The CFAA defines loss as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[14] Loss does not include any costs incurred improving

[13] For example, plaintiffs have filed class action suits against companies that place "cookies" on the computers of website visitors for purpose of collecting private data for marketers. While the courts have found that cookies are an unauthorized access to computers in violation of the actus reus provisions of section 1030, the invasion did not cause US$5000 in loss and thus dismissed the suit. In re Intuit Privacy Litig., 138 F Supp 2d 1272, ___ (C.D.Cal 2001) [Plaintiffs failed to show that privacy invasion was economic loss in the amount of US$5000 or non-economic damage of the type listed in 18 USC 1030(e)(8)(B)-(D).]

[14] 18 U.S.C. 1030(e)(11).

the system, nor does it include costs for forensic investigation.[15] The comments to guideline 2B1.1 expressly exclude forensic costs, i.e. "costs to the government of, and costs incurred by victims primarily to aid the government in, the prosecution and criminal investigation of an offense."[16]

First, no victim wants to put the system back into its original condition. Everyone wants to improve. Incident handlers do not restore a compromised system to its "condition prior to the attack" as contemplated by the definition. Prior to the attack, the system was vulnerable. The administrator is going to improve the security of the system so that the same attack will not be successful the next time. Responders "harden" systems, install patches, and tighten network perimeter security.[17]

Second, victims invariably include forensic costs as part of labor in response to an intrusion. First responders are taught to do a forensic investigation if at all possible, even though the legal definition of loss excludes forensic costs. Private and public organizations have developed standards and training programs for these first responders. For example, the U.S. Department of Commerce, National Institute of Standards and Technology (NIST) publishes the "Computer Security Incident Handling Guide", which explores policies and practices public agencies and private sector businesses should take following an attack. The federally funded CERT Coordination Center (CERT/CC) also publishes resources for private organizations to build their own computer security incident response teams and to train incident handlers. Their publication, State of the Practice of Computer Security Incident Response Teams (CSIRTs), published in October 2003, is a review and digest of the top incident handling resources.[18] It covers CSIRT services, projects, processes, structures, and literature, as well as training, legal, and operational issues.

The training manuals stress the importance of investigating incidents so that the information can be used in a subsequent civil or criminal case. Obviously, the DOJ guide is intended for law enforcement and for first responders to computer crime scenes. The entirely of the manual advises following appropriate forensic procedures with the intention of preserving evidence for criminal prosecution.

The NIST guide, however, is targeted to all first responders, not only law enforcement and crime scene responders.[19] It is characteristic of the training that first

---

[15] U.S. v. Middleton, 231 F.3d 1207, 1213 (9th Cir. 2000). (The finder of fact could consider only those costs that were a "natural and foreseeable result" of the defendant's conduct, that were "reasonably necessary", and that would "resecure" the computer.

[16] U.S.S.G. §2B1.1 note 3(D).

[17] If the intruder obtained passwords, changing passwords might be required to resecure the system as a result of the incident.

[18] State of the Practice of Computer Security Incident Response Teams (CSIRTs), October 2003.

[19] Section 1.3, p. 1-1. "This document has been created for computer security incident response teams (CSIRTs), system and network administrators, security staff, technical

responders receive in the public and private sectors.[20] First responders are told to collect evidence in a way that will hold up in court.

> Although the primary reason for gathering evidence during an incident is to resolve the incident, it may also be needed for legal proceedings. In such cases, it is important to clearly document how all evidence, including compromised systems, has been preserved. Evidence should be collected according to procedures that meet all applicable laws and regulations, developed from previous discussions with legal staff and appropriate law enforcement agencies, so that it should be admissible in court. In addition, evidence should be accounted for at all times; whenever evidence is transferred from person to person, chain of custody forms should detail the transfer and include each party's signature. A detailed log should be kept for all evidence…[21]

The NIST guide also recommends that the incident handler have forensic training so that she is familiar with legal rules and proceedings.[22] The guide advises recovery actions, including "restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rulesets, boundary router access control lists)."[23] It also advises investigative actions, including validating the attacker's IP address, scanning the attacker's systems, performing web research on attacker handles or email addresses, searching incident databases, and monitoring the attacker's electronic communications.[24]

Thus, system administrators are trained to contemplate either a criminal or civil action at the outset of the investigation. The guides recommend time-consuming system review and evidence preservation activities, which are useful only for legal cases. Procedures for documenting how evidence has been preserved, collecting evidence in accordance with laws and regulations, keeping chain of custody forms, communicating with legal counsel, interviewing witnesses, all are part of building a legal case, not merely investigating what happened.

Forensic activities and training increase both the time spent by and the hourly cost of the incident handler, despite the legal exclusion of such costs.

---

support staff, chief information officers (CIOs), and computer security program managers who are responsible for preparing for, or responding to, security incidents."

[20] The NIST document was based on the advice of security experts at NIST, consulting firm Booz Allen Hamilton, NASA, Indiana University, CERIAS, Purdue University, the Department of Veterans Affairs, Wells Fargo Bank, the University of Tulsa, CERT®/C, MITRE, Ohio State University, Lawrence Berkeley National Laboratory, and FedCIRC.

[21] NIST 3-18.
[22] NIST 3-19.
[23] NIST 3.3.4 at 3-21
[24] Id. at ___.

This would not be a problem if courts scrutinized victim loss estimates. However, courts have proven highly deferential to victims. A review of the Department of Justice's selected computer crime cases published at http://www.cybercrime.gov shows 13 cases sentenced in the past two years. The information provided for four of the 13 cases includes both the government's statement of loss and the court ordered restitution. In three of the four cases, the restitution order equaled or exceeded the government statement of loss, indicating that the court adopted the government's loss estimate. In the fourth case, the government's stated loss was US$100K and the court ordered US$88K in restitution.[25]

Courts could be less deferential if they had the documentation necessary to parse through the time spent or the hourly rate to try to excise extra costs motivated by forensic purposes. Unfortunately, investigating FBI agents do not ask victims to keep track of their time with the legal definitions of loss in mind. As a result, victims usually submit to courts undifferentiated loss estimates with few sub categorizations that would aid a court in distinguishing between permissible and impermissible loss inclusions. Victims simply are not given the information necessary to avoid excessive loss calculations.

There is little or no incentive or format in which the victim can estimate damages in a legally useful way. For example, in *United States v. Butler*, the Air Force OSI investigated the intrusions into Air Force computers. That investigation led to the identification of Butler as the perpetrator. The SA in charge provided the FBI with a flat number of investigative hours the AFOSI devoted to case. He provided no supporting documentation, list of type of work done or records of when the work was performed. For sentencing, the government obtained another document from AFOSI detailing the work. The total number of hours on the worksheet was different from the number initially reported. Again, it contained no indication of what work was done. There was, therefore, no way to tell whether the calculation included time spent on activities explicitly excluded from the loss calculation. The court nonetheless sentenced Mr. Butler based on this information because it was a "reasonable" calculation.[26]

A pattern of deference makes sense. Judges do not have the expertise to second-guess a victim's assessment of what was required to investigate and fix his system. As the Honeynet data suggests, experts in the field can differ widely over the proper course of an investigation. Judges have little competency to question those decisions. However, the parties could bring in experts to support and attack the loss estimate and courts could make judgments based on testimony, as they do in other areas of the law. But the burden of proof at sentencing and standard of review on appeal is so low that trial courts feel confident that any reasonable decision will be upheld.

BURDEN OF PROOF AT SENTENCING IS TOO LOW TO INCENTIVIZE JUDGES TO TAKE A SERIOUS LOOK AT LOSS ESTIMATES BY VICTIMS

---

[25] http://www.cybercrime.gov. A more in depth analysis of the data on computer crime sentencing is needed to confirm that this assertion that courts are extremely deferential is true.

[26] U.S. v. Butler, Northern District of California, Judge James Ware.

Judges have little incentive to take a closer look at victim loss estimates because the burden of proof at sentencing is so low. Between 1986 and 2004, federal courts were required to sentence defendants under the United States Sentencing Guidelines. Recent U.S. Supreme Court decisions have declared mandatory adherence to the guidelines unconstitutional, but have allow courts to use the guidelines as a non-mandatory framework for appropriate sentencing. Under either scheme, sentencing courts are not encouraged to exercise meaningful review of victim or government loss estimates because the standard and burden of proof for these critical matters is extremely low and sentencing courts are not going to get overturned on appeal.

The guidelines do not limit loss in computer crime cases to foreseeable damages. While the definition of loss for other white collar fraud crimes punished under the same guideline includes only reasonably foreseeable monetary harm,[27] a special rule for computer crime cases requires the court to include *any reasonable cost to any victim*, "including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages incurred because of interruption of service", regardless of whether the harm was reasonably foreseeable or not.

Also, the guidelines establish a lower burden of proof for loss calculations in sentencing. Generally, sentencing is by a preponderance of the evidence.[28] However, the guidelines only require the judge to make a "reasonable estimate" of the loss.[29] In other words, the government only needs to show by a preponderance of the evidence that the sentencing court made a reasonable estimate of loss, and that estimate is a factual finding entitled to great deference. [30]

Last terms' Supreme Court decisions in United States v. Booker and United States v. FanFan have changed the way federal courts will use the guidelines in sentencing. The decisions stem from prior case law holding that a defendant has a right to trial by jury for any factor that increases the defendant's sentence. Booker and FanFan then held that the sentencing guidelines, to the extent that they are mandatory, violate the constitution when the total offense level upon which the trial court sentences include aggravating factors not found to be true beyond a reasonable doubt by a jury. A different majority of the court then held that the guidelines are acceptable so long as they are not mandatory. Courts are free to be guided by the guidelines, but need not sentence in accordance with them, and sentencing decisions will be reviewed for "reasonableness." In the future, we can expect that loss will continue to be a critical factor in sentencing decisions, but that courts will still be under little or no pressure to scrutinize loss estimates, since the overall sentence only needs to be reasonable.

---

[27] U.S.S.G. §2B1.1, comment 3.

[28] See e.g. U.S. v. Hull, 160 F.2d 903 (5th Cir. 1992); U.S. v. Collins, 109 F.3d 1413 (9th Cir. 1997).

[29] U.S.S.G. §2B1.1, comment 3 (C) Estimation of Loss.

[30] See 18 U.S.C. 3742(e) and (f).

DEFINING DAMAGE IN TERMS OF THE VICTIM'S INVESTIGATION AND REMEDIATION COSTS DOES NOT PROMOTE PROSECUTION OF THE MORE DISRUPTIVE ATTACKS

As I argue above, the computer crime statute doesn't adequately address intangible damage from intrusions. The core of my argument is that the statute also fails to discriminate well between harmful and trivial attacks. The problem is that the amount of damages depends on the victim's choices, not on the nature of the attack. Since economic loss depends on the victim rather than the offender, victims who mitigate economic losses may not be able to prosecute either civilly or criminally. As a result, attacks on the most economically sensitive systems that immediately have to be restored to functioning may be the ones least likely to be prosecuted.

The victims of computer attacks often have conflicting goals. It may want to perform a thorough analysis of the incident, to determine what happened and to learn from the problem. It may want to perform a thorough analysis of the incident for use in a legal case against the perpetrator. Or most pressingly, it may want to get the computer systems back up and running as quickly as possible to avoid business losses. Doing a full-scale analysis for any purpose may interfere with restoring services. The expense of identifying a perpetrator, versus putting the services back on line, can be immense.[31]

A system owner that decides to investigate will rack up more losses in the form of labor costs than a system owner that decides the computers are mission critical and have to be put back on line immediately. As a result, the first incident will be punished more harshly than the latter, though arguably the intrusion into the mission critical system was more disruptive the attack on a system where the owner had the luxury of time to investigate.

The victim's choice about how to respond to a security incident is the difference between innocence and prison. When different victims treat the identical attack differently, vastly disparate loss calculations result, and thus sentences vary as well. Since loss matters both to guilt and to sentencing, these different calculations mean the difference between "not guilty" and five years of prison, despite the fact that the unauthorized access was exactly the same.

The intrusions that took place in United States v. Butler[32] illustrate exactly this point. In that case, I represented a man who created an automated tool that used a known vulnerability to compromise systems and install new code that both patched the known

---

[31] NIST §3.3.3: "Identifying the attacker can be a time-consuming and futile process that can prevent a team from achieving its primary goal—minimizing the business impact."
[32] U.S. v. Butler, Northern District of California, Judge James Ware.

vulnerability and installed an unknown back door, or trojan, program. Every system accessed by his tool was accessed in exactly the same way, since the tool used the identical automated process on each machine. Some system administrators restored their machines from backup and reported a single hour of work. At government pay rates, this was far less than the requisite $5000 of loss. Other system adminstrators reported spending over 30 hours examining the compromised machines, as well as examining other machines that were not compromised, to investigate the attack. Here, the costs were well above the $5000 threshold. The loss Butler caused could be aggregated across machines as part of a similar course of conduct. However, if Defendant A had compromised the first system and Defendant B the second in identical ways, but unrelated incidents, Defendant A would not be prosecuted and Defendant B would go to prison.

Moreover, trivial attacks may be prosecuted more severely than destructive ones. Assume the defendant accessed a webserver through a known vulnerability and changed the webpage in Incident A. In Incident B, the defendant gained unauthorized access to a University computer and deleted all the data stored on the system. In Incident A, the webserver owner could put the system back simply by restoring the proper name to the file containing the website images. However, it also chooses to hire expensive outside consultants to review the all the computers on the system and make sure there are no other intruders or changes, taking a week's worth of work at a high hourly rate. In Incident B, the researchers restore the data from backup, taking just a couple of hours of graduate student time. In Incident A, the attacker could go to prison. In Incident B, despite the attacker's destructive intent and effect, the offense most likely would not be prosecuted at all.

BASING SENTENCE ON COST OF CLEANUP UNDERMINES SENTENCING GOALS

Since cost of cleanup can vastly different for the same offense conduct, punishment levels do not reflect the seriousness of the offense.[33] Cost of cleanup doesn't even necessarily reflect the sensitivity of the victim to intrusions, since the most loss adverse victims will probably spend the less time investigating in favor of restoring service to users. Since different defendants can receive different sentences for the same conduct, the sentencing scheme does not treat similarly situated people similarly.

The goals of sentencing in the United States federal criminal justice system are (1) to provide punishment levels that reflect the seriousness of the offense[34]; (2) to provide fairness in meeting the purposes of sentencing[35]; (3) to provide defendants with needed educational or vocational training, medical care, or other correctional treatment in

[33] 18 U.S.C. 3553(a)(2)(A).
[34] 18 U.S.C. 3553(a)(2)(A).
[35] 28 U.S.C. 991(b)(1)(B).

the most effective manner where rehabilitation is appropriate [36]; (4) to afford adequate deterrence to criminal conduct[37]; (5) to provide just punishment[38]; (6) to maintain sufficient flexibility to permit individualized sentences when warranted by mitigating or aggravating factors not taken into account in the establishment of general sentencing practices[39]; (7) to protect the public from further crimes of the defendant[40]; (8) to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct[41]; and (9) to provide certainty in meeting the purposes of sentencing[42]. Goals numbered 1, 2, 5, 8 and 9 are not met by the current practice in computer crime sentencing.

CONCLUSION: SENTENCING IN THE FUTURE

My argument illuminates several ways in which the current computer crime statute and sentencing scheme should change. First, we need to find a way to address computer intrusions that invade privacy or cause other non-economic damages. I do not think that the answer will come from a methodology for pricing intangible harms. The endeavor is too speculative, and could lead to victim manipulation or increased risk of excessive sentences. The statute could prohibit unauthorized access to private information, define that information as it is defined in the stored communications act, and hinge the sentence on the number of people effected or some other non-monetary measure.

Second, the sentencing process needs to exclude both system improvements and forensic costs. Training FBI agents and victims to provide courts with accurate and complete documentation will help. Encouraging courts to require such documentation will help as well. We could require a higher burden of proof at sentencing or pass a statute that requires trial courts to make certain findings of fact before imposing sentences.

Third, we need a sentencing scheme that is based on the offense conduct, not the victim response. We need a scheme that does not penalize victims for quick remediation or reward victims of excessive investigation, including investigation or remediation to repair harm to reputation. This is harder to achieve. The security industry does not agree what harm any particular intrusion causes, and leaving it to the victim's discretion does not work. With other crimes, we can look to the effect of the offense conduct on the victim and see that he is $10,000 poorer, has a broken arm or even has sleepless nights. With computer crime remediation, neither the defendant nor an outside observer knows exactly what effect the intrusion will or should have on the victim. And to some extent, the victim can choose whether to spend money, break his arm, or stay awake all night.

---

[36] 18 U.S.C. 3553(a)(2)(B).
[37] 18 U.S.C. 3553(a)(2)(B).
[38] 18 U.S.C. 3553(a)(2)(B).
[39] 28 U.S.C. 991(b)(1)(B).
[40] 18 U.S.C. 3553(a)(2)(C).
[41] 18 U.S.C. 3553(a)(6), 28 U.S.C. § 991(b)(1)(B).
[42] 28 U.S.C. 991(b)(1)(B).

Without an general consensus as to the seriousness of a particular intrusion or the appropriateness of a particular response, we remain highly dependant on victim reporting.