Ethics in Vulnerability Assessment
Facts(?) regarding ethics of disclosure

Actions of good-guys never cause harm to other good-guys
Most citizens (all of this class) are good-guys
Actions of bad-guys may cause harm to other people
Facts(?) regarding ethics of disclosure

Actions of good-guys never cause harm to other good-guys
Most citizens (all of this class) are good-guys
Actions of bad-guys may cause harm to other people

White Hat Researchers:
are good-guys ; want to make a living
Facts(?) regarding ethics of disclosure

Actions of good-guys never cause harm to other good-guys
Most citizens (all of this class) are good-guys
Actions of bad-guys may cause harm to other people

White Hat Researchers:
  are good-guys ; want to make a living

Black Hat Coders:
  are bad-guys ; want to find/know about vulnerabilities
Facts(?) regarding ethics of disclosure

Actions of good-guys never cause harm to other good-guys
Most citizens (all of this class) are good-guys
Actions of bad-guys may cause harm to other people

White Hat Researchers:
  are good-guys ; want to make a living

Black Hat Coders:
  are bad-guys ; want to find/know about vulnerabilities

NSA Personnel:
  are good-guys ; want to find/know about vulnerabilities
  want to have command-and-control on all devices
  are bound by law not to “spy” on Americans
  can “spy” on and track lone-wolf terrorists
Facts(?) regarding ethics of disclosure

Actions of good-guys never cause harm to other good-guys
Most citizens (all of this class) are good-guys
Actions of bad-guys may cause harm to other people

White Hat Researchers:
are good-guys; want to make a living

Black Hat Coders:
are bad-guys; want to find/know about vulnerabilities

NSA Personnel:
are good-guys; want to find/know about vulnerabilities
want to have command-and-control on all devices
are bound by law not to “spy” on Americans
can “spy” on and track lone-wolf terrorists

Vendors:
are neither good-guys nor bad-guys
act to maximize profits – may not fix a vulnerability
Facts(?) regarding ethics of disclosure

Actions of good-guys never cause harm to other good-guys
Most citizens (all of this class) are good-guys
Actions of bad-guys may cause harm to other people

White Hat Researchers:
    are good-guys ; want to make a living
Black Hat Coders:
    are bad-guys ; want to find/know about vulnerabilities

NSA Personnel:
    are good-guys ; want to find/know about vulnerabilities
    want to have command-and-control on all devices
    are bound by law not to “spy” on Americans
    can “spy” on and track lone-wolf terrorists

Vendors:
    are neither good-guys nor bad-guys
    act to maximize profits – may not fix a vulnerability

Surveillance by good-guys is healthy for other good-guys
Surveillance by bad-buys may be bad (is reconnaissance)
Non-disclosure doesn't stop others from finding vulnerabilities
Types of disclosure

Full disclosure
All details are made public immediately including PoC

Limited disclosure
All details given to the vendor but no details are made public

Responsible Full Disclosure
All details given to the vendor
Just enough detail given publicly to mitigate the risk
Time is given to fix the vulnerability
After patching, release all details publicly
Partial public release of details if vendor does nothing

Non-disclosure
No details are revealed to anyone
Can disclosure cause legal problems?
(Nearly) true story:
Student in security class finds vulnerability in Physics website
Student tells security professor
Professor tells Physics people and provides a fix
Everyone is happy, student gets an A
Can disclosure cause legal problems?
(Nearly) true story:
Student in security class finds vulnerability in Physics website
Student tells security professor
Professor tells Physics people and provides a fix
Everyone is happy, student gets an A

Two months later:
Physics website is hacked badly – grades are changed!
FBI is called in
Physics people tell FBI that a vulnerability had existed but was found by a student of security professor and fixed
FBI asks security professor for name of student
Security professor refuses to give the name
FBI threatens security professor with court orders and several felony counts!
Can disclosure cause legal problems?

(Nearly) true story:
Student in security class finds vulnerability in Physics website
Student tells security professor
Professor tells Physics people and provides a fix
Everyone is happy, student gets an A

Two months later:
Physics website is hacked badly – grades are changed!
FBI is called in
Physics people tell FBI that a vulnerability had existed but
was found by a student of security professor and fixed
FBI asks security professor for name of student
Security professor refuses to give the name
FBI threatens security professor with court orders and
several felony counts!

Conclusion:
Student came forward voluntarily and was cleared
Professor changed class policy to don't-ask-don't-tell
The Economics of Software Development
Why don't vendors make higher quality software?

In a free market, all other things being equal, higher quality should win out
The Economics of Software Development

Why don't vendors make higher quality software?

In a free market, all other things being equal, higher quality should win out.

At the moment it is expensive and time consuming to make and sell high quality software.

So, software with vulnerabilities abound, even though massive repair efforts may be required as vulnerabilities are discovered.
The Economics of Software Development

Why don't vendors make higher quality software?
   In a free market, all other things being equal, higher quality should win out

At the moment it is expensive and time consuming to make and sell high quality software
   So, software with vulnerabilities abound, even though massive repair efforts may be required as vulnerabilities are discovered

But doesn't that mean lifetime cost is higher?
   Nope – it is more efficient to let the market find the bugs for the vendor! Let the consumers become an ad-hoc quality-control department for the vendor! Anyway, most vulnerabilities will likely not be found and many others will likely be minor.
The Economics of Software Development

Why don't vendors make higher quality software?

In a free market, all other things being equal, higher quality should win out.

At the moment it is expensive and time consuming to make and sell high quality software.

So, software with vulnerabilities abound, even though massive repair efforts may be required as vulnerabilities are discovered.

But doesn't that mean lifetime cost is higher?

Nope – it is more efficient to let the market find the bugs for the vendor! Let the consumers become an ad-hoc quality-control department for the vendor! Anyway, most vulnerabilities will likely not be found and many others will likely be minor.

But now the consumer is burdened with the task of updating immediately when a patch is published.

Too bad.
No Binding Disclosure Policy and Low-Quality Software May Result in Nefarious Behavior that Does Not Benefit the Good-Guys

Mercenaries look for flaws then extort money from vendors to keep the flaws quiet

White hat researchers may report very minor bugs that really do not affect security adversely but sound scary enough to affect the vendor's reputation (and profits)

Good-guys are threatened with legal action or lawsuits for doing something that has great benefit for good guys
But Sometimes This Is Not So Clear

The case of Michael Lynn vs. Cisco

Cisco routers had a bug known to Cisco and some security companies, particularly Intelligent Software Solutions (ISS)

Michael Lynn worked for ISS and discovered that this (buffer overflow) bug could be exploited to bring down the internet

Lynn wrote a paper which was accepted at Black Hat.

ISS told Lynn to remove sections of the paper

Lynn refused, left ISS, gave the talk

Cisco:
  Demanded the paper be stricken from the proceedings
  Demanded that 2000 CDs containing it be destroyed
  Sued Lynn

Settlement:
  Lynn agreed never to say anything about this publicly
  Lynn gave up all material related to his findings
  Black Hat & Lynn gave up recordings of his talk
But Sometimes This Is Not So Clear
The case of Michael Lynn vs. Cisco

Aftermath:

Lynn's presentation went online but was removed due to a cease-and-desist order

Cisco's public relations department downplayed the flaw
“It is important to note that the information Lynn presented was not a disclosure of a new vulnerability or a flaw with Cisco IOS software. Lynn's research explores possible ways to expand exploitations of known security vulnerabilities impacting routers."

"Cisco believes that the information Lynn presented at the Blackhat conference today contained proprietary information and was illegally obtained."

Cisco also said Lynn 'unziped' a Cisco image to do his work and this is a violation of Cisco's user agreement

Lynn got a job at Juniper
But Sometimes This Is Not So Clear
The case of Michael Lynn vs. Cisco

How to look at this case:
Is Cisco acting in the best interest of its customers?
But Sometimes This Is Not So Clear
The case of Michael Lynn vs. Cisco

How to look at this case:

Is Cisco acting in the best interest of its customers?
Disclosing the flaw could make their systems vulnerable
But customers are furious at not being told of the flaw
But Sometimes This Is Not So Clear
The case of Michael Lynn vs. Cisco

How to look at this case:

Is Cisco acting in the best interest of its customers?
Disclosing the flaw could make their systems vulnerable
But customers are furious at not being told of the flaw

Is Cisco violating the first amendment of the Constitution?
Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances
But Sometimes This Is Not So Clear
The case of Michael Lynn vs. Cisco

How to look at this case:

Is Cisco acting in the best interest of its customers?  
Disclosing the flaw could make their systems vulnerable  
But customers are furious at not being told of the flaw

Is Cisco violating the first amendment of the Constitution?  
**Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances**

But legally, instructions are not speech if part of a criminal act such as bringing down Cisco routers
But Sometimes This Is Not So Clear
The case of MBTA vs. three MIT undergrads & MIT

What is claimed by the MBTA:
Students circumvented security features of the MBTA computerized CharlieTicket and CharlieCard fare media systems
Students publicly offered "free subway rides for life" over the Internet
Students plan to allow others to duplicate their claimed "breaking" of the Fare Media's security systems by presenting a paper, releasing software tools, and giving demonstrations at the next DEFCON hackers convention
MIT is unwilling to set limits on the students' activities despite MBTA requests
Students have declined to inform MBTA of the details of their supposed hack
Students did not allow MBTA to fix flaws before going public
But Sometimes This Is Not So Clear
The case of MBTA vs. three MIT undergrads & MIT

What happened:
MBTA got a temporary restraining order to prevent the students from presenting at DEFCON

MBTA argued that students were giving instructions to people to defraud the MBTA

Students argued that submitting research for review by a government agency before publication is unconstitutional pre-publication censorship (censorship of expression by the government before the expression takes place)

Students did not have to go to DEFCON – their results were posted in district court's public website as exhibits

In a moment the result of this case
But Sometimes This Is Not So Clear
The case of MBTA vs. three MIT undergrads & MIT

What happened:
MBTA got a temporary restraining order to prevent the students from presenting at DEFCON
MBTA argued that students were giving instructions to people to defraud the MBTA
Students argued that submitting research for review by a government agency before publication is unconstitutional pre-publication censorship (censorship of expression by the government before the expression takes place)
Students did not have to go to DEFCON – their results were posted in district court's public website as exhibits

In a moment the result of this case
The students win!
This is considered academic research
Future academic research could be suppressed “transmission” in the Computer Fraud and Abuse Act cannot be construed to mean any form of communication
But Sometimes This Is Not So Clear
The case of MBTA vs. three MIT undergrads & MIT

Companies will only design security as good as their customers know to ask for - Schneier
The Web Complicates Disclosure

Consider:

Is a front door to a house considered a vulnerability?
The Web Complicates Disclosure
Consider:
Is a front door to a house considered a vulnerability? Not really, unless it is unlocked or left open.
The Web Complicates Disclosure
Consider:
Is a front door to a house considered a vulnerability? Not really, unless it is unlocked or left open
Is a webpage injecting malicious code into a browser a vulnerability?
The Web Complicates Disclosure

Consider:

Is a front door to a house considered a vulnerability?
Not really, unless it is unlocked or left open

Is a webpage injecting malicious code into a browser a vulnerability?
Not really, it's the user who is the vulnerable one
I.e., if the user does not open the “door,” there is no problem
The Web Complicates Disclosure

Consider:

Is a front door to a house considered a vulnerability? Not really, unless it is unlocked or left open.

Is a webpage injecting malicious code into a browser a vulnerability? Not really, it's the user who is the vulnerable one. I.e., if the user does not open the “door,” there is no problem.

Check this javascript out – looks perfectly benign, right?:

```javascript
print "<html>"
print "<h1>Most recent comment</h1>"
print database.latestComment
print "</html>"
```
The Web Complicates Disclosure
Consider:
Is a front door to a house considered a vulnerability?
Not really, unless it is unlocked or left open

Is a webpage injecting malicious code into a browser a vulnerability?
Not really, it's the user who is the vulnerable one
I.e., if the user does not open the “door,” there is no problem

Check this javascript out – looks perfectly benign, right?:

```
print "<html>
print "<h1>Most recent comment</h1>"
print database.latestComment
print "</html>"
```

Attacker submits comment
```
<script>doSomethingEvil();</script>
```
The Web Complicates Disclosure

Consider:

Is a front door to a house considered a vulnerability? Not really, unless it is unlocked or left open.

Is a webpage injecting malicious code into a browser a vulnerability? Not really, it's the user who is the vulnerable one. I.e., if the user does not open the “door,” there is no problem.

Check this javascript out – looks perfectly benign, right?:

```
print "<html>
print "<h1>Most recent comment</h1>"
print database.latestComment
print "</html>"
```

Attacker submits comment

```
<script>doSomethingEvil();</script>
```

User gets (Zowie!!):

```
<html>
<h1>Most recent comment</h1>
<script>doSomethingEvil();</script>
</html>
```
The Web Complicates Disclosure

The previous is an example of cross-site scripting (XSS)

Consider:

It is estimated that 70% of websites are susceptible to XSS
That's nearly 100 million sites!! How to disclose?
Broadcast on NBC news without even checking?
The Web Complicates Disclosure
The previous is an example of cross-site scripting (XSS)

Consider:
It is estimated that 70% of websites are susceptible to XSS
That's nearly 100 million sites!! How to disclose?
Broadcast on NBC news without even checking?

Answer (maybe not a good one – not responsible):
A discussion board was started – people can add XSS susceptible sites with benign proof of concept (say, dialog opens with !)

Examples: USA Today, NY Times, Boston Globe, ABC, CBS, Warner Bros., Nike, and many more

Some sites have been fixed, but many are not
The Web Complicates Disclosure
The previous is an example of cross-site scripting (XSS)

Consider:
It is estimated that 70% of websites are susceptible to XSS
That's nearly 100 million sites!!  How to disclose?
Broadcast on NBC news without even even checking?

Answer (maybe not a good one – not responsible):
A discussion board was started – people can add XSS susceptible
sites with benign proof of concept (say, dialog opens with !)

Examples: USA Today, NY Times, Boston Globe, ABC, CBS,
Warner Bros., Nike, and many more

Some sites have been fixed, but many are not

But I am pretty sure none of mine are (assuming I have
not been so hacked) –
I stay away from javascript!  And I do not allow students to
change anything on my site from a browser
The Web Complicates Disclosure
Possible dark future for disclosing Internet vulnerabilities

Consider:
Person X applied to USC but was denied
Person X hacked the USC website and pulled sensitive data
The data were sent to a third party who notified USC
Person X was charged and pled guilty to unauthorized access
The Web Complicates Disclosure
Possible dark future for disclosing Internet vulnerabilities

Consider:
Person X applied to USC but was denied
Person X hacked the USC website and pulled sensitive data
The data were sent to a third party who notified USC
Person X was charged and pled guilty to unauthorized access

What the Law says:
Unauthorized access of computers is illegal
But how can you say that access of a public website is unauthorized
Isn't it implied that everyone has permission to access websites?
The Web Complicates Disclosure
Possible dark future for disclosing Internet vulnerabilities

Consider:
Person X applied to USC but was denied
Person X hacked the USC website and pulled sensitive data
The data were sent to a third party who notified USC
Person X was charged and pled guilty to unauthorized access

What the Law says:
Unauthorized access of computers is illegal
But how can you say that access of a public website is unauthorized
Isn't it implied that everyone has permission to access websites?

Future Law?
Exploring all ways a website works is prohibited!!
Yikes – then vulnerability testing becomes illegal!!
Digital Rights Management (DRM), Fair Use, and Digital Millennium Copyright Act (DMCA)

**DRM (applied to software):**
Technological restrictions on what a user can do with software

*Example:* a DVD does not play on a player sold for region 1

**DMCA:**
It is illegal to circumvent DRM – or distribute tools to do so

**Fair Use (in U.S. copyright law):**
Brief exceptions of a work may be used without permission in certain circumstances

*Examples:*
- whistling a tune while walking down the street (public performance)
- cutting out a New Yorker cartoon and posting it on your office door
- photocopying a newspaper article for your files (reproduction)
- quoting a line from The Simpsons in an email to a coworker
- reverse engineering of computer code (reproduction)
- "time-shifting" a radio or television program (reproduction)

**Note:** Fair Use invoked so as not to ask permission to use the above
Digital Rights Management (DRM), Fair Use, and Digital Millenium Copyright Act (DMCA)

Questions:
Do disclosures facilitate circumvention?
Does prohibition of circumvention tools limit Fair Use?
Digital Rights Management (DRM), Fair Use, and Digital Millenium Copyright Act (DMCA)

Cases:
HP threatens SnoSoft (2002)

A novel legal argument – HP claimed SnoSoft violated the DMCA when one of its researchers released an exploit that could give remote hackers control of systems running HP's Tru64 Unix Operating System.

HP warned SnoSoft the incident exposed SnoSoft to potential imprisonment and half a million dollars in fines.

Carly Fiorina was CEO at the time

Enormous outrage resulted.
Digital Rights Management (DRM), Fair Use, and Digital Millenium Copyright Act (DMCA)

Cases:
HP threatens SnoSoft (2002)

A novel legal argument – HP claimed SnoSoft violated the DMCA when one of its researchers released an exploit that could give remote hackers control of systems running HP's Tru64 Unix Operating System.

HP warned SnoSoft the incident exposed SnoSoft to potential imprisonment and half a million dollars in fines.

Carly Fiorina was CEO at the time

Enormous outrage resulted.

HP backed down because its upper management was not aware of what a hot button DMCA is and because they did not want to be a poster child for DMCA abuse.
Digital Rights Management (DRM), Fair Use, and Digital Millenium Copyright Act (DMCA)

Cases:
Felton and USENIX vs. RIAA (2001)

Recording Industry Association of America (RIAA) and Secure Digital Music Initiative (SDMI) threatened to use DMCA to prevent a scientific team, including Princeton and Rice University professors, from discussing their findings that the music industry's new “security” technology is not very secure.

Felton filed suit asking federal court to declare that it is not a violation of DMCA to disseminate their results and that they have protection to do so under the 1st amendment.
Digital Rights Management (DRM), Fair Use, and Digital Millenium Copyright Act (DMCA)

Cases:
Felton and USENIX vs. RIAA (2001)

Recording Industry Association of America (RIAA) and Secure Digital Music Initiative (SDMI) threatened to use DMCA to prevent a scientific team, including Princeton and Rice University professors, from discussing their findings that the music industry's new “security” technology is not very secure.

Felton filed suit asking federal court to declare that it is not a violation of DMCA to disseminate their results and that they have protection to do so under the 1st amendment.

Case dismissed – lack of standing (did not demonstrate to the court sufficient connection to and harm from the law or action challenged to support that party's participation in the case).
Digital Rights Management (DRM), Fair Use, and Digital Millenium Copyright Act (DMCA)

Cases:
Universal Studios vs. Reimerdes/Corley (2000)

Eight movie studios claimed that three defendants violated DMCA by making DeCSS (DVD decryption software) available (trafficking in circumvention devices)
Digital Rights Management (DRM), Fair Use, and Digital Millenium Copyright Act (DMCA)

Cases:
Universal Studios vs. Reimerdes/Corley (2000)

Eight movie studios claimed that three defendants violated DMCA by making DeCSS (DVD decryption software) available (trafficking in circumvention devices)

Movie studios win. Here is what the judge said:

Plaintiffs have invested huge sums over the years in producing motion pictures in reliance upon a legal framework that, through the law of copyright, has ensured that they will have the exclusive right to copy and distribute those motion pictures for economic gain. They contend that the advent of new technology should not alter this long established structure. Defendants, on the other hand, are adherents of a movement that believes that information should be available without charge to anyone clever enough to break into the computer systems or data storage media in which it is located.
Digital Rights Management (DRM), Fair Use, and Digital Millennium Copyright Act (DMCA)

Cases:
Lexmark International Inc. vs. Static Control Components Inc

Lexmark designed an authentication system using a Microcontroller so that only authorized toner cartridges could be used in their printers.

SCC developed a chip that duplicates the 'handshake' used by the Lexmark chip, and includes a verbatim copy of the Toner Loading Program, which was necessary to allow the printer to function. A Lexmark cartridge could successfully be refilled if Lexmark's chip was replaced with the SCC chip. SCC sold its “Smartek” chips to toner cartridge rechargers.
Cases:
Lexmark International Inc. vs. Static Control Components Inc

Result:
Unlike patents, copyright protection cannot be applied to ideas, but only to particular, creative expressions of ideas.

Lock out codes that must be performed in a certain way in order to bypass a security system are generally considered functional rather than creative, and thus are unprotectable.

Lexmark's authentication sequence did not “control access” to the printer engine program. Rather, the purchase of the printer itself allowed access to the program just by dumping the code so SCC did not circumvent access control.

The idea of interoperability was supported

A defeat for companies battling with third party sellers
Digital Rights Management (DRM), Fair Use, and Digital Millenium Copyright Act (DMCA)

Exceptions:

Security Testing:

Information derived is used solely to promote the security of the owner or operator of the tested system.

Information obtained is shared directly with the developer of the system.

Information obtained is not distributed in a way that might enable copyright infringement or other legal violations.

http://digital-law-online.info/lpdi1.0/treatise51.html
Digital Rights Management (DRM), Fair Use, and Digital Millenium Copyright Act (DMCA)

Exceptions:

Encryption Research:

The Senate Judiciary Committee felt strongly that the provisions of the DMCA should not be used to stifle the very encryption research that led to the technological measures the DMCA would now protect.

Using generally available tools is not illegal.

Testing of an encryption algorithm or program that has multiple uses, including a use as a technical protection measure for copyrighted works, is OK if that testing is in a form not implemented as a technical protection measure.

Encryption testing with consent of the copyright holder is OK.

It is OK to publish results if they do not include step-by-step instructions for circumvention.

http://digital-law-online.info/lpdi1.0/treatise49.html
Digital Rights Management (DRM), Fair Use, and Digital Millenium Copyright Act (DMCA)

Exceptions:

Reverse Engineering:

Reverse engineering to support interoperability is considered Fair Use

See http://www.eff.org/issues/coders/reverse-engineering-faq