Cyberlaw: Honeypot Edition

Your guide to the legal issues and honeypots

Jay Radcliffe

My Profile

- Jay Radcliffe
  - jay.radcliffe@gmail.com
  - CISSP, GSEC
  - Six years at ISS with the MSS group
  - Undergrad Pre-Law/Criminal Justice
  - Working on Masters with SANS

Legal Disclaimer

- I am not your lawyer. I am not a lawyer at all. This is not legal advice.

Questions Answered

- What parts/areas of the law should I worry about?
- Is it entrapment if I catch a criminal in my honeypot?
- Can I record/log everything that occurs in my honeypot?
- Can I be sued by a hacker if he gets caught by my honeypot?
- What can I do to reduce my legal exposure?

Honeypot Basics

- A Honeypot is a device that is setup to record the actions as of hackers
- Typically it's setup to look like a "normal" server. Example: File server, web server

Honeypot Resources

- Lance Spitzner's book Honeypots
- Honeynet.org

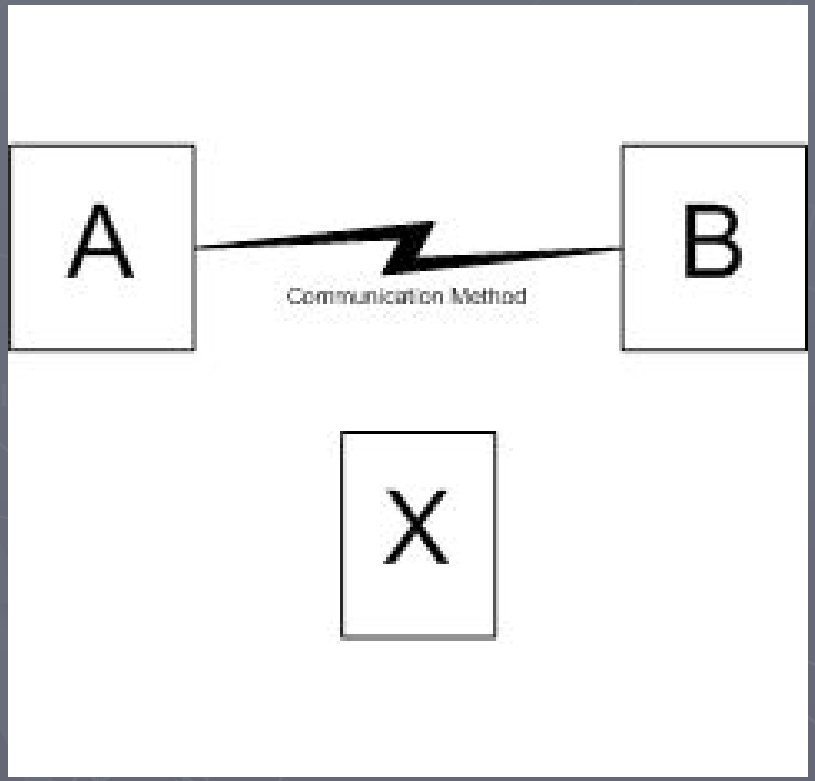
Legal Issue #1: Privacy

- Honeypots record all transactions that occur to and from the device
- US Federal laws limit the ability to perform these recordings
- This is the primary criminal issue in relation to honeypots

EPCA

- The primary law that deals with the privacy issue in relation to computers is 18 USC 2510 (AKA Electronic Communications Privacy Act)
- It started out life just dealing with telephony wiretaps, was extended to include electronic communications

EPCA: Basic Diagram



- "A" is the Honeypot
- "B" is the user communicating with the honeypot,
- X is some 3rd party that is not involved in the communication
- "Method" refers to how the communication takes place

The 1st Rule of EPCA

- If you are operating "A" then you are a party directly involved in the communication
- This gives you the legal authority to record and "intercept" communications.
- This should include if you are not being completely honest with the content on the honeypot

2nd Rule of the EPCA

- If you gain consent from either "A" or "B" then you have the legal authority to record/"intercept" communications
  - This applies to federal law only. There are X states that have laws that require the consent from both "A" and "B"
- This is fairly easy to accomplish:
  - Banners
  - Acceptable Use /Terms of Service

3rd Rule of EPCA

- The Service Provider Exception
  - Let's say you own the network, and you provide service to others (Example: ISP, University)
  - You have a right to intercept traffic to verify that your network is working properly and that others are not going to "damage" your network
  - There are some cases that outline this from a telephony prospective

Wireless and the EPCA

- Let's say your honeypot is off on a wireless network
- The EPCA says that communications that are "Generally accessible to the public" and is not "encrypted or scrambled" then it's potentially LEGAL TO INTERCEPT
- In theory, if you put a wireless network in between "A" and "B" you can legally monitor without consent from either party
- If no WEP or other encryption/scrambling is used

Issue #2: Entrapment

- Very misunderstood legal concept
- Entrapment is only a defense, and can't be used to criminally charge the owner/operator of the honeypot
- Entrapment can only be used by a criminal to "excuse" him of the criminal charges

Entrapment Example #1

- Jake goes to his local 2600 meeting and meets Judy and her friends. Judy is talking about hacking into Acme Inc's webserver and do bad things. Judy offers Jake the opportunity to "prove himself" by hacking the server first. Jake declines the opportunity. Judy calls into question his "skillz" and general masculinity. Jake gives in and hacks into Acme's webserver. Jake is arrested by Judy, who is an undercover officer.

Entrapment Example #2

- Matt goes to a security conference and meets Tom. Tom talks about hacking into Acme Inc's webserver. Tom suggests to Matt the he take a try at getting in. Matt declines. Tom then pulls out a weapon and threatens to harm and potentially kill Matt unless he hacks into Acme's webserver. Matt gives in and hacks into the webserver. Matt is then arrested by Tom, who is an undercover agent.

Entrapment's Position

- The role of presumption is reversed in an entrapment defense
  - The court assumes that the accused WAS NOT entrapped
  - The defendant has to prove that some action that the government took made him commit the crime, and that they would not have committed the crime without that action
  - Exceptionally difficult to prove
  - Also, the defendant has to admit that they committed the crime

Entrapment and Honeypots

- What's all this mean to your ability to deploy a honeypot?
  - Avoid contacting the users on your honeypot.
  - Avoid advertising your honeypots on IRCs, message boards, etc
  - Any communications that are made, need to be very well documented

Entrapment and Research

- What if your honeypot is not to catch criminals, but to study them? Do you need to worry about entrapment?
- YES!
- In some cases you can not control if there is going to be a criminal case
  - Child Pornography

Actions you should take

- Banner all of your bannerable services
  - This action gains consent, one of the key elements in the EPCA
  - There are many examples in SANS course material, and the internet
  - If you have access to legal counsel, have them review the language in your banner

Actions you should take

- Keep the hacker contained
  - While I didn't cover Civil legal issues, there is a concern that the hacker might use the honeypot to launch an attack
  - Limit outbound connectivity
  - Do what you can, and DOCUMENT it.

Actions you should take

- Documentation
  - Have clear build procedures with your banner in them
  - Make a backup of the honeypot
  - There might be a time where you need to prove you had banners in place

Documentation

- Documentation checklist
  - Banners and list of services that are bannered
  - List of actions taken to limit the outbound connectivity from the honeypot
    - Firewall rules, router ACL, etc
  - Permission from managers
    - Be sure to mention reasons for why your putting up a honeypot.
    - "A honeypot is a security tool that we need to assure the services we provide, and enhance our own security"

Documentation

- Network Diagram
  - Needed to prove "method" of communications
  - Especially important for wireless
- Backups
  - Throw the backup tape/CD/DVD in with the documentation folder
- Any communication to the "outside" about the honeypot

Documentation

- Put all of the above into a folder/envelope and put it somewhere safe
- DON’T SKIP THIS
  - An hour of documentation could save your job/company.

Summery

- Cover all three of the EPCA bases
  - Consent (Banners, backups, build docs)
  - Prove you are an agent
  - Provider exception (Purpose Statement, banner)
  - Network Diagram (Wireless loophole)
- Don’t communicate outside about your honeypot
  - If you *must*, document those
- Limit your honeypot from getting out
  - Have to prove “reasonable” security

Questions?

- GSEC Gold Paper should be done this month, much more detailed and includes citations
- E-Mail me and I'll notify when it gets posted on SANS
- Suggestions? Let me know!
  - Other things that need to be addressed
  - Other cyber legal issues you would like to see covered
- jay.radcliffe@gmail.com