Effect of Electronic Evidence Captured by Honeypots

East China University of Political Science and Law
Yi Wang
2012 .9

Outline

- Introduction
- Comparing Honeypot with Entrapment
- Other Legality Challenges
- Evidences Effect Captured by Honeypots
- Conclusion

INTRODUCTION

- **Electronic evidence becomes more and more important in evidence collecting.**
  - Many cases infer e-evidence, in some cases it is the unique evidence.
  - New Code of Criminal Procedure amendment in China regards e-evidence as an independent type of evidence. It will be carried out in 2013.
- **Electronic evidence's attributes**
  - Easy hidden
  - Easy modified
  - Easy erase
  - Time limited

INTRODUCTION-CONTINUE

- **Advantages of active forensic technique**
  - Capture important evidence that afterwards forensic can't be collected.
  - Know more about our adversary

Comparing Honeypot with Entrapment

- **Definition of honeypot**
  - Honeypot is a security resource who's value lies in being probed, attacked or compromised.

- **Definition of entrapment**
  - American legal definition of entrapment is:

--A person is 'entrapped' when he is induced or persuaded by law enforcement officers or their agents to commit a crime that he had no previous intent to commit.

- **Key criteria for judging entrapment**
  - be induced or persuaded by law enforcement officers or their agents.
  - whether it will let common people without criminal intent emerges criminal intent.

- **How about honeypot---not belong to entrapment**
  - honeypot catches those who have already had criminal intent and implemented.
  - Honeypot products are designed as when unauthorized access occurs, the connection is relocated into honeypot.

Other Legality Challenges

- **Privacy**
  - Q: honeypot will catch owners of stored information and intruders' privacy.
  - A: use "Platform for Privacy Preferences"
- **Joint liability**
  - honeypot is attacked by intruders with unknown technique or the flaws. (that don't set deliberately by operators of the honeypot)
    - Victim, like other ordinary intruded machines.
  - honeypot is attacked through the flaws set deliberately by the operators
    - Should take the responsibility of management oversight.

Evidences Effect Captured by Honeypots

- **Precautions to maintain evidence's effect**
  - According to practical requirements select suitable honeypot products.
  - Clear the goal and strategy of your honeypot
  - Don't ignore your honeypot
- **Guidelines for evidence's effectiveness justification**
  - Evidences that qualified witnesses believe are true should be accepted.
  - Proving that a honeypot is normal in critical moment, the honeypot can be deduced that is in normal, evidences recorded by the honeypot should be accepted.

CONCLUDSIONS

- Honeypots technique is very useful in information security.
- It is also an important method to collect valuable information from attackers.
- this technique is still in development, and legal problems are not settled down completely.


Thank you!