Don’t shoot the messenger!

A criminological and computer science perspective on coordinated vulnerability disclosure

Marleen Weulen Kranenbarg
Thomas J. Holt
Jeroen van der Ham


M.WeulenKranenbarg@VU.nl
@CyCriminologist

Download my dissertation at: http://dare.ubvu.vu.nl/handle/1871/55530
Cyber-offenders versus traditional offenders

• Cyber-dependent offenders
• Compared to traditional offenders

• Four domains in criminology:
  1. Offending over the life-course
  2. Personal & situational correlates of offending & victimization
  3. Similarity in deviance of social network members
  4. Clustering of offending & motives for offending
Coordinated Vulnerability Disclosure

- Coordinated Vulnerability Disclosure (CVD)
- Responsible Disclosure (RD)
- Bug bounties

4 options when finding a vulnerability (usually in daily use of IT-systems):
1. Report to organization => CVD
2. Report publicly
3. Keep private to use for attack => offending
4. Do nothing

Current CVD practice
- Focused on white-hat community
- Generally no prosecution when rules are followed
- Rise in bug bounties but majority offers small non-financial rewards
Coordinated Vulnerability Disclosure

• Current CVD practice: problems
  – Organization’s response: capacity, knowledge, slow, communication
  – Unclear/unjust rules: no guarantee prosecution, deadlines, culture may discourage
  – Public disclosure: information shared limited, governments do not disclose
  – Knowledge about CVD among potential offenders: rules must be known
Coordinated Vulnerability Disclosure

• Current CVD practice: problems
  – Organization’s response: capacity, knowledge, slow, communication
  – Unclear/unjust rules: no guarantee prosecution, deadlines, culture may discourage
  – Public disclosure: information shared limited, governments do not disclose
  – Knowledge about CVD among potential offenders: rules must be known

• Motives using CVD:
  – Increase cyber-security
  – Gain status in white-hat community
  – Frustration about lack of security
  – Bug bounties: money
Coordinated Vulnerability Disclosure

• Motives using CVD:
  – Increase cyber-security
  – Gain status in white-hat community
  – Frustration about lack of security
  – Bug bounties: money

• Motives criminal hacking:
  – Intrinsic: limit to finding vulnerabilities? Or also curious about data stored on system?
  – Extrinsic: status in criminal hacking community
  – Financial: underground markets
Coordinated Vulnerability Disclosure

Rational choice, costs/benefits

• Costs:
  – Risk of legal action when using CVD, while costs of offending are low
  – Time consuming / too many rules
  – Negative effect status in criminal hacking community

• Benefits:
Coordinated Vulnerability Disclosure

Rational choice, costs/benefits

• Costs:
  – Risk of legal action when using CVD, while costs of offending are low
  – Time consuming / too many rules
  – Negative effect status in criminal hacking community

• Benefits:
  – Curiosity/social rewards motives
    • Additional social rewards like helping with testing
    • White-hate role models
  – Financial motives: underground markets more profitable
Coordinated Vulnerability Disclosure

Conclusion:

• **Improve current CVD policies:**
  – Increase awareness / eye-catching CVD information on websites
  – Positive peer recognition: media attention for successful CVD’s
  – Lower threshold: response organization
  – Organize hackathons etc.
  – If desires: invite discloser for additional (paid) help
    • More recognition
    • Recruitment tool
Coordinated Vulnerability Disclosure

Future research:

• Situational factors that influence the decision (awareness/visibility CVD policy/bounty)
• Personal factors (self-control, social control)
• Life-course of IT-specialists (IT-employees, bug bounty programs, CVD users)
• Influence/information online communication (cultures)
• Knowledge/use youth
Don’t shoot the messenger!

Questions/remarks?

Marleen Weulen Kranenbarg
Thomas J. Holt
Jeroen van der Ham

https://doi.org/10.1186/s40163-018-0090-8