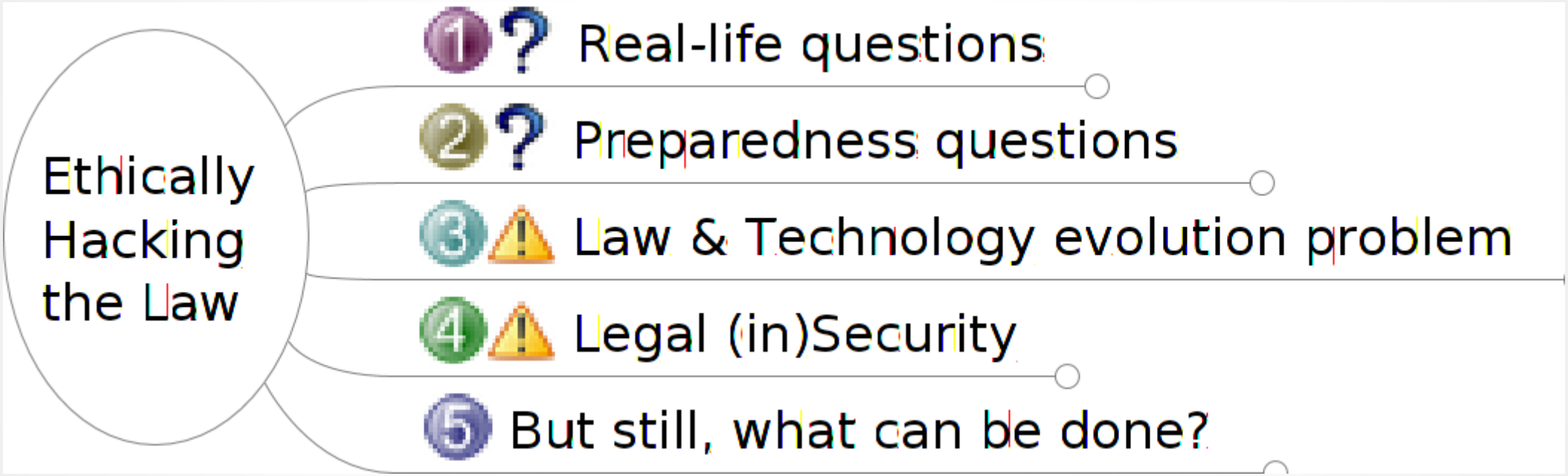
– Knock knock!
– Who's there?
– The Law! Open up!

Ethically Hacking the Law
(Boring Legal Department presentation before lunch)

Cristian Driga – lawyer, executive director
Cybercrime Research Centre Assoc, Romania

Summary


Ethically Hacking the Law
1 Real-life questions
2 Preparedness questions
3 Law & Technology evolution problem
4 Legal (in)Security
5 But still, what can be done?

Real life questions

- Does poor protection of a computer system or data deserve to be exposed regardless of consequences?
- If a company does not respond, do you publish the vulnerability no matter what?
- When you get hacked, do you feel you should be allowed to hack back?

Preparedness questions

- How many of you have read the Criminal Law Code provisions on cybercrime?
- What is the length of the “Legal Aspects” chapter in the Ethical Hacking Manuals?
- ~~Trouble with the Police lately, related to hacking charges?~~
- Do you feel you have enough legal protection for Ethical Hacking activities?

Law & Technology evolution problem

2000

Mostly desktops, laptops (bulky single systems) containing data

Networks and the Internet

2016

IoT

Cloud computing

Information systems are everywhere & vital

Vulnerabilities actively exploited

Irresponsible or abusive companies and vendors

- **Basic Law is the same – Convention on cybercrime**
  - Defines the information system in the legal sense
  - Defines illegal access to information systems and other offenses

2016 – Problems have multiplied

- Finding vulnerabilies without 3rd pary help not possible anymore (professional ethical hackers & pentesters, bug bounty programs, good citizens willing to help)
- Judicial system is still learning the language and logic of IT
- Laws remained the same
  - Growing need to redefine at least the illegal access

Legal (in)Security for Ethical Hackers

- Too many laws to take into account
  - Criminal law
  - Criminal procedural law
  - Copyright laws
  - Dataprotection
  - Other property rights
- Predictibility - similar decisions in similar cases
- Common missunderstandings
- Technical knowledge needed in IT cases

What can be done? Shall I go home?

*If you want "**not to do** something"*
...ask a lawyer!

But still, what can be done?

- WHAT
  - Paperwork & Evidence
  - If you are an employee
  - If you get hacked
  - Hack the basic legalese lang & logic
  - Help judicial system evolve.
    Get involved in policing.
    Have your say.
  - Get public recognition.

Paperwork & Evidence

- **Bullet proof pentesting contracts**
  - Assess all the systems accessed (Real owner, Type)
  - Specify the exact tools and methods used
  - Make sure the client understands the implications
    - Not enough to simply write that client takes full responsibility
    - Go in detail regarding what are those responsibilities
    - Put definitions of terms in the contract
  - Any employee or partner of the client can sue you
  - Provision regarding sincerity of client
- **Actual testing**
  - Do not give into temptation: STOP once proven the 1st vulnerability
  - **Document every step taken in any way you can**
- **Disclose Responsibly** - Publishing - still has risks

Hack the basic legalese lang & logic

- **RTFCP: Read the [...] Criminal Law Provisions**
  Example:
  - Access = entering the whole or a part of a computer system (or network) no matter the method
  - Unlawful = without Authorisation or Right –> get authorisation from the real owner or legal user
  - Intention and motive is analyzed – you need proofs
  - Immediate result of the offense – minimize damage
  - Attempts are punishable

Possible ways out of criminal charges

Art 318 Criminal Procedure Code - Dropping charges

- (1) For offenses punishable with a fine or a penalty of imprisonment of no more **than 7 years**, the prosecutor can drop charges when, considering the contents of the offense, the modus operandi and the instruments used, the goal of the offense and the concrete circumstances of its commission, the consequences that occurred or could have occurred, they find that a public interest is not served in prosecuting. […]

YOU READ THE REST...

- (3) When the offender is identified, weighing the public interest aspect also involves **the person of the suspect or defendant, their conduct previous to the offense** and the efforts they made in removing or minimizing the consequences of the offense.

GET PUBLIC RECOGNITION. SPEAK@DEF.CAMP

Other aspects

- **If you are an employee**
  - Do only what fits the job description
  - And demand (written/email) confirmation for any verbal request outside the job description
- **If you get hacked**
  - Do not hack back
  - Preserve evidence
  - Document the case
  - File criminal charges

Help the system evolve. Get involved in policing.

- **Demand ammending the laws**
  - Illegal access offense exceptions
- **Help the judicial system**
  - Help reaching common definitions in the laws
- **Document and share best practices**
  - among yourselves
  - with the authorities
- **Demand Coordinated Vulnerability Disclosure Policies** - from client companies & From lawmakers
    - https://www.thegfce.com/initiatives/r/responsible-disclosure-initiative-ethical-hacking

Thank you!

Cristian Driga – lawyer, executive director

Cybercrime Research Centre Asoc.

contact@cybercrime.org.ro

www.cybercrime.org.ro