



Ethics for Security Practitioners

Enno Rey, erey@ernw.de
[@enno_insinator](https://twitter.com/enno_insinator)

#whoami

- Infosec since 1997, in different roles.
- Some background in security research
 - Amongst others, six talks at Black Hat US/EU (2006–14) plus numerous talks at Troopers
 - Have been involved in a few high-profile vulnerability disclosure cases
- Founder of a security research & assessment company in 2001
 - Established ethics committee in the organization 2012



Agenda / Objectives

- Discussion & critical reflection of ethical dilemmata relevant for our work
- Jointly coming up with some general guidelines for certain situations
- Foster individual ability to develop own (ethical) perspective ;-)



Where Ethics Affect Our Work As Security Practitioners

- Everywhere ;-)

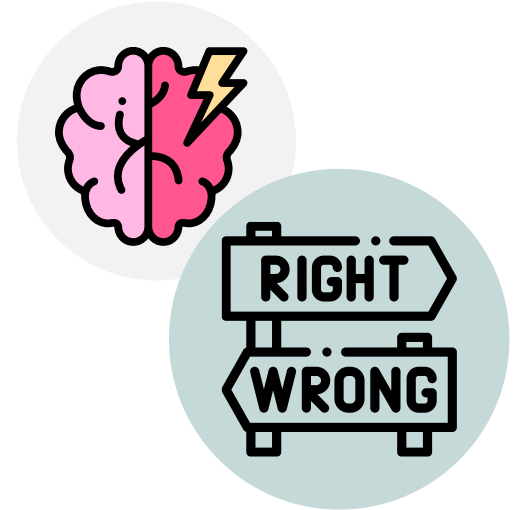
E.g.

- Vulnerability Research & Disclosure
- Most infosec activities that involve humans



Ethics

- The task of practical ethics is to identify moral problems in different target situations
 - clarify what the stakes are in each case,
 - conceptually explore possible courses of actions (considering their most relevant implications)
 - and justify and suggest what the best course of action is likely to be.
- Practical ethics suggests what is the right thing to do by appealing to moral reasons.



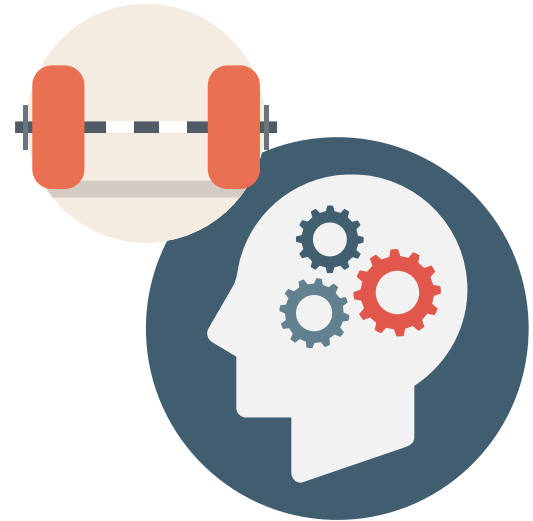
Practical Ethics (2)

- It's all about dilemmata (at least in this talk ;-)
- If it wasn't the effort wouldn't be needed.
 - The whole thing could be codified in some simple rules.
 - That's what, somewhat, is tried when creating laws.



Some Approaches

- Consequentialism
 - Deontology
 - Principlism
-
- All these are mostly discussed “to give you an idea”. See references for further reading.



Consequentialism

- The ends justify the means.
- Can justify actions that people typically consider to be morally wrong.
- Problems / critique
 - difficulty of predicting consequences
 - balancing different categories of consequences



Consequentialism – Critique in a Nutshell



Deontology

- Some choices are morally forbidden irrespective of the good they can create.
- Problems / critique
 - might commit one to duties that can have very bad consequences.



Principlism

- Identify some “global human principles”, look at/apply them and perform weighing where needed. Main principles often being
 - Autonomy
 - Beneficence
 - Non-maleficence
 - Justice
- Main critique/weakness: real-life applicability.



Principlism – Example (fr. Menlo Report)

| | | |
|----------|--|----------|
| C | Application of the Principles | 5 |
| | C.1 Stakeholder Perspectives and Considerations | 6 |
| | C.2 Respect for Persons | 7 |
| | C.2.1 Informed Consent | 7 |
| | C.3 Beneficence | 9 |
| | C.3.1 Identification of Potential Benefits and Harms | 9 |
| | C.3.2 Balancing Risks and Benefits | 9 |
| | C.3.3 Mitigation of Realized Harms | 10 |
| | C.4 Justice: Fairness and Equity | 11 |
| | C.5 Respect for Law and Public Interest | 11 |
| | C.5.1 Compliance | 12 |
| | C.5.2 Transparency and Accountability | 12 |

Typical Approach / Questions to Ask

- Recognize/identify the issue
- Get the facts, stakeholders & values that are affected
- Evaluate alternative actions
 - which option → most good/least harm?
 - to society as a whole?
 - which option (best) respects rights of stakeholders?
 - which leads me to act as the person I want to be?
- Evaluate in hindsight



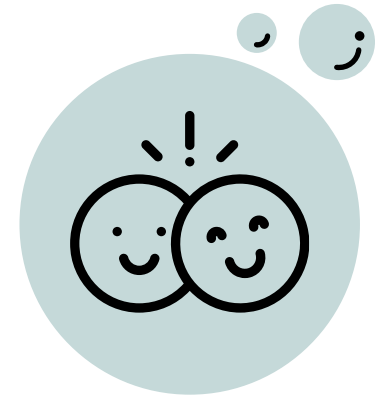
To Consider Also & in General

- Power / knowledge imbalance
- The Internet as a sociotechnical system
 - "technical, highly educated, male, Caucasian, from economically developed countries"
- (Avoid) Setting precedent
- Be careful as for analogies between the physical & digital world.



Also To Keep in Mind/To Consider [II]

- Be honest about incentives & (your) agenda
- Discuss question/dilemma with somebody from different background/society context
 - You'll have to explain it
 - You will be forced to leave your bubble ;-)



Let Me Emphasize

- All this is not an easy task.
- If you reach (or strive for) a conclusion/ decision within five minutes, you're
 - either a strict deontologist (which can be a good thing, I'm not judging here. But then it's a deliberate decision) OR
 - You're doing it wrong.




Case Studies

Vulnerabilities in Alarm Systems

- You find vulnerabilities in an alarm system sold from local electronics stores as an OEM product (so you can't even identify the vendor) and which is widely used in your neighborhood.



Alarm Systems / Performing the Approach

- Facts
 - Easy  (somewhat)
- Values
 - Quick recap of value framework of vuln disclosure here (see also next slide)
 - BUT: very different stakeholders in this case
- Risks, Benefits, Harm
 - Well, that's the crucial part of this one...
- Further reading on this one:
 - https://www.ernw.de/download/ERNW_Newsletter_50_Vulnerability_Disclosure_Reflections_CaseStudy.pdf
 - https://www.ernw.de/download/ACM_SigComm_ENSR_Rey_Vulnerability_Disclosure.pdf



Vuln Disclosure / Assumptions




Simplest Case




- The **finder** who has discovered a vulnerability which she now reports
- to the **vendor** who receives the information,
- in order to provide **remediation**, which in turn benefits all users using the product/software in question.

06/21/15 ACM SigComm2015 - Workshop on Ethics in Networked Systems Research #8 www.ernw.de



Further Assumptions



- At the time of reporting no patch is available.
- The vendor actually takes care of remediation.
- It can be deployed everywhere where needed, without too much delay.
- The people involved/users affected are well-informed, willing to deploy the remediation and capable/enabled to do so.

Let's call them **stakeholders**.

06/21/15 ACM SigComm2015 - Workshop on Ethics in Networked Systems Research #11 www.ernw.de

Alarm Systems / What We Did

- We tried to identify the (“initial”) vendor in order to get in contact with them.
 - We considered going through a kind-of industry body, but, at some point, stopped this due to effort.
- We did not publish the 3rd part of the related blogpost series.
- In a nutshell: we did nothing.
 - As of today: we should have gone through a CERT.
- In hindsight this is highly unsatisfactory. #fail



Case Study (II)

- You find a backdoor in a network device which might be actively used by an intelligence agency of a 5-eyes country.
- Disclaimer: due to the complexity of the case some “elements” were modified.
 - Feel free to speculate which ones ;-)
 - It’s about the reflection & discussion anyway, right?



NW Device with Backdoor / Approach (II)

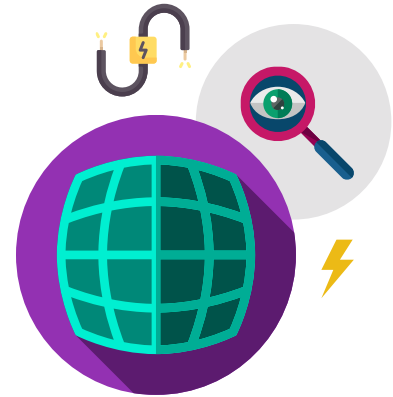
- At first glance might look like a vuln disclosure case.
- But of course it's not: backdoor \neq vulnerability (rly?)
- “One country’s whitelist is another country’s blacklist”
 - This rises the problem of “scope”, see next slide.
- A wholly different context, plus its associated framework of objectives and values, kicks in.
 - This makes it easy for consequentialists ;-)



https://www.ernw.de/download/01_04_vulnerability_assessments.pdf

NW Device with Backdoor / Approach (III)

- Let's take a closer look:
- Who are the affected stakeholders?
 - Internet community vs. one (actually 5) country's inhabitants.
 - This is a classical problem of "scope".
 - There's no easy solution for this one.
 - Main point here: make yourself aware of it!
- Values
 - What about *autonomy*?
- This one serves as a "nice" example where (the inherent broadness of) *principlism* fails.



What We Did

- This was a mere speculative one, for the sake of discussion.
- ;-)



Case Study “Domain Controller Logs”

- You're asked to help with analyzing the logs of a domain controller, with particular focus on one employee, for reasons that remain, say: unclear & dubious to you.



Domain Controller Logs / Approach

- Facts
 - Unclear, which in turn contributes to the overall dilemma.
- Values
 - Autonomy?
 - Might not apply here as corporate context with contracts & rules which by their very nature restrict autonomy.
 - Beneficence
 - To organization? To individual?



Scoping: Organization vs. Individual

- Again, this is a classical one.
- Humans tend to favor humans.
- ... which can be perfectly fine and well:
human. But, then again, one has to be aware
of this.



La casa de papel
© Netflix

More on This Scoping Thing

- Internet scanning has the same dilemma
 - Beneficial to (maybe): “the Internet community” (whoever that is)
 - Harm (to): potentially individual people, namely in the age of IoT
 - (Principle of) *Autonomy* is violated.
 - Often this is further aggravated by an imbalance re: knowledge & benefits.
 - Which in turn can lead to very consequentialist reasoning, with far-fetched arguments as for the (perceived) benefits.



Domain Controller Logs

– What We Did:



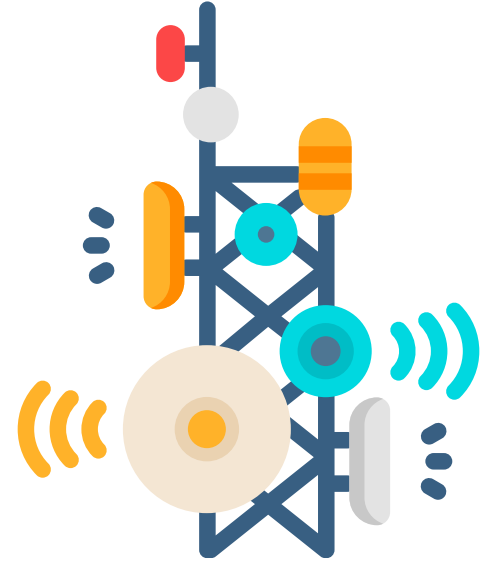
OR



- ERNW Ethics Committee decided against performing the project.

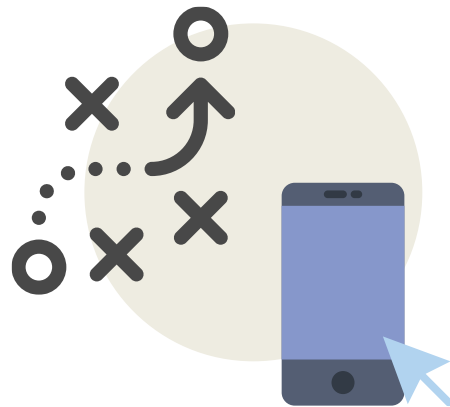
Case Study Telco Training

- You're asked to perform a training on telco technologies and during the setup it turns out that the participants want to perform it with simultaneous translation into Russian and they are solely interested in interception interfaces & surveillance capabilities.



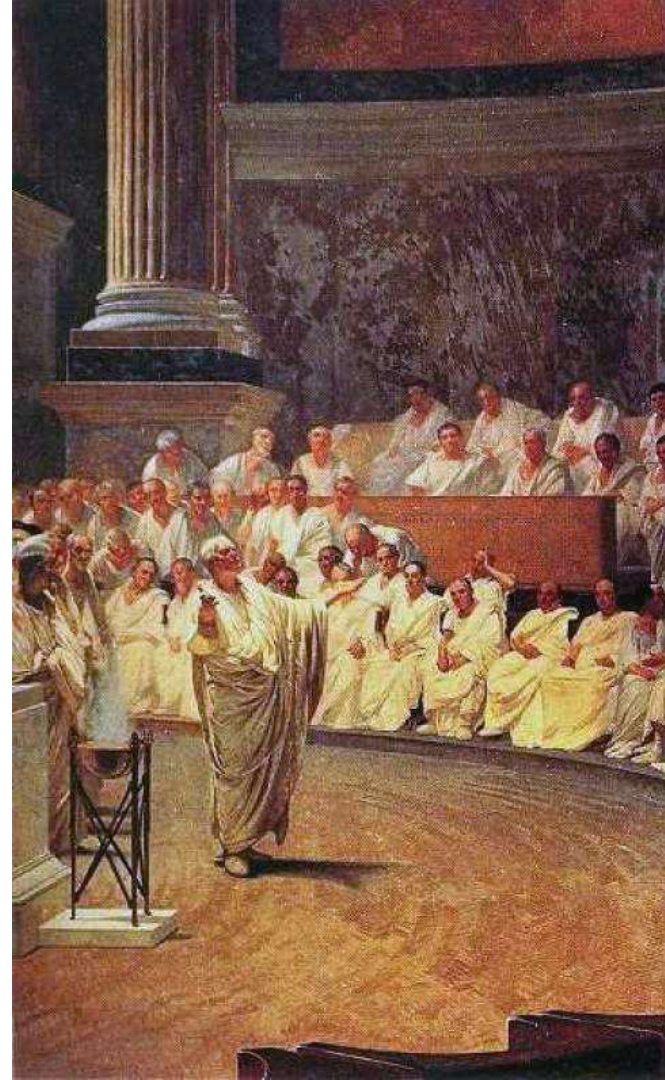
Telco Training / Performing the Approach

- Stakeholders?
 - Scope?
- Values?
 - Autonomy?
 - Benefits?
 - Again we're back with the scoping thing.



Telco Training / What We Did

- We performed the training (as we had already committed this in an early phase. *Pacta sunt servanda...*).
- This case was the trigger to implement the Ethics Committee
 - Not least to relieve individual employees from responsibility of (ethical) *decision taking* in their job.



Case Study: Development of PoC Code

- You haven't had a lucrative engagement for some months and there's this guy asking you to write some PoC code for a vulnerability of a smartphone OS. His business card tells you he's from a state agency in a country which get's "significant coverage" in Amnesty International's Human Rights report.



Development of PoC Code / Some Notes

- This goes to the core the vulnerability/exploit sales discussion.
 - Which is a huge debate on its own.
 - Ftr: we @ERNW have a quite deontological stance (against) it. Evidently, your mileage may vary...
- ***Proof-of-Concept***, by its very definition & terminology, can be considered to be an intellectual exercise without real-life context. In reality, here it might be quite the contrary...
- Exploit code usually can be considered to create a ***power imbalance***...



Development of PoC Code / Approach

- Facts
 - Quite important here but might be difficult to gather.
 - Not least because this is “just PoC”, right?
 - Some parts of this are easy: it’s about money, right?
- Values
 - Autonomy – This one probably heavily violated once PoC leaves PoC state...
 - Benefits & Harms
 - Government vs. individual humans
 - “But I have to feed my family”...



What We Did

- Actually this was a case study merging two different projects.
 - We decided – unanimously, so Ethics Committee wasn't even called – against the PoC thing.
 - We were ready/open to perform a project of a “infrastructure protection” nature for \$CLIENT (but that one didn't happen for other reasons).



Conclusions

- Understand that in the space of Ethics there are different approaches & frameworks out there
 - Consequentialism – which a technical community might have some initial sympathy for – is not a panacea!
- At the same time realize that you can't do without ethics.
- Reflect your own agenda!
- Practical ethics is not about simple rules, but about critical thinking.





Thank You for
Your Attention!



erey@ernw.de

www.ernw.de



@Enno_Insinuator

www.insinator.net



Practical Application

- In research papers
 - “Ethical Considerations” section
 - Example:
<http://mkorczynski.com/IMC16Korczynski.pdf>
- Research projects
 - In advance answer questions from
<http://networkedsystemsethics.net>
 - Write down the answers!
- If in doubt ask ethics committee.



References

- ACM Ethics
 - <https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct>
- FIff (in German)
 - <https://www.fiff.de/about>
- Menlo Report
 - http://www.caida.org/publications/papers/2012/menlo_report_actual_formatted/menlo_report_actual_formatted.pdf

Sources

Image Source:

- Icons made by [Freepik](https://www.freepik.com) from www.flaticon.com

