

# KRACK and the Ethics of Disclosure

Adon Shapiro

December 6, 2017

1. Abstract
2. Introduction
  - (a) Overview of what KRACK is
  - (b) Introduce concept of disclosure, and why it is a difficult question
  - (c) Some specifics about how KRACK was discovered and publicized
3. To the Community
  - (a) KRACK is important to talk about because it is recent and many systems are likely still vulnerable or people unaware
  - (b) Disclosure is important not only because of current relevance (KRACK) but because this question arises every time a vulnerability is discovered and no satisfying conclusion has been reached as to the proper way to disclose a vulnerability
4. Action/Defense (Technical aspects)
  - (a) Technical details of KRACK exploit
  - (b) How KRACK has and has not been fixed since disclosure
5. Non-technical aspects
  - (a) Explain how KRACK was disclosed and how this compares to other similar vulnerabilities
  - (b) Compare KRACK to other well-known vulnerabilities and their disclosure processes
  - (c) explore consequences and implications of above
6. Conclusion
  - (a) Argue for Full Disclosure
  - (b) Use evidence from issues explored with KRACK to back myself up

## References

<https://www.krackattacks.com/>

[https://www.schneier.com/essays/archives/2007/01/schneier\\_full\\_disclo.html](https://www.schneier.com/essays/archives/2007/01/schneier_full_disclo.html)

[https://web.archive.org/web/20060328012516/http://infosecuritymag.techtarget.com/articles/january01/columns\\_curmudgeons\\_corner.shtml](https://web.archive.org/web/20060328012516/http://infosecuritymag.techtarget.com/articles/january01/columns_curmudgeons_corner.shtml)

<https://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00>

<https://www.sans.org/reading-room/whitepapers/threats/define-responsible-disclosure-932>