**Homework 12: Exploring Moral and Legal Issues**

Part 1: MD5 Vulnerabilities in Digital Signatures

In reviewing the Alexander Rocco network, I found that MD5 is being used for digital signatures on a Windows Server 2016 CA. This is a concern because MD5 is known to be weak and prone to collision attacks, where two different inputs create the same hash. This flaw could let attackers create fake certificates or impersonate users. Microsoft recommends moving away from MD5 and using more secure algorithms like SHA-256 for better protection​ (NIST Special Publication 800-107).

Part 2: Ethical and Legal Issues of Publishing Algorithm Vulnerabilities

The disclosure of vulnerabilities in algorithms like MD5, SHA-1, and MD4 has unquestionably raised ethical and legal questions regarding the responsibilities of cybersecurity professionals. Here is my take:

1. Should people who are able to break a hashing algorithm be allowed to post their findings on the Internet?

Many security experts favor responsible disclosure, where vulnerabilities are reported securely to give vendors time to address issues before public release. This approach aligns with NIST’s recommendations for responsible vulnerability disclosure to balance transparency with security. However, unrestricted sharing of exploits may help attackers. Responsible disclosure, which requires reporting vulnerabilities to relevant authorities or vendors before public release, helps balance awareness and security.

1. Do you think the reporters of the DVD (DeCSS) crack were exercising their First Amendment rights when including the source code for breaking the DVD encryption key in an article? What about displaying the source code on a T-shirt?

Sharing or even wearing the DeCSS DVD crack code like on a T-shirt, brings up a tricky debate. Some people believe it’s free speech, simply sharing info or making a statement. Displaying the code might be seen as a way to express an opinion. On the other hand, DeCSS breaks DVD encryption, which is protected by laws like the Digital Millennium Copyright Act (DMCA). Sharing this code could be seen as encouraging others to get around copyright protections. The court in *Universal City Studios v. Reimerdes* (2000) found that sharing the DeCSS code violated the DMCA, as it enabled to bypass encryption designed to protect copyrighted material. This ruling suggests that distributing such code, even under the guise of free speech, is not protected when it facilitates illegal activities. The same logic would apply to displaying the code on a T-shirt

1. As a security professional, do you think you have to abide by a higher standard when sharing or disseminating source code that breaks hashing algorithms?

Security professionals are held to higher ethical standards, especially when sharing code that could compromise systems. Expecting them to handle information responsibly. Sharing code that breaks encryption or reveals vulnerabilities isn’t just about transparency, it has real risks. Security professionals need to weigh the impact, like whether it could help attackers if it’s not handled carefully. Responsible handling of security issues means considering potential impacts and following ethical standards to protect individuals and organizations from unintentional harm.

References

* National Institute of Standards and Technology. (2012). NIST Special Publication 800-107: Recommendation for Applications Using Approved Hash Algorithms (Revision 1). <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-107r1.pdf>
* Simpson, M. T., & Antill, N. (2017, 2011). Hands-On Ethical Hacking and Network Defense (Module 12: Cryptography). Cengage Learning.
* **NIST Retires SHA-1 Cryptographic Algorithm**  
  National Institute of Standards and Technology. (2022). <https://www.nist.gov/news-events/news/2022/12/nist-retires-sha-1-cryptographic-algorithm>
* NIST Computer Security Resource Center (CSRC). (n.d.). Hash Functions. National Institute of Standards and Technology. <https://csrc.nist.gov/Projects/hash-functions>
* Joyce, C. (n.d.). *Universal City Studios, Inc. v. Reimerdes*. University of Houston Law Center. Retrieved from <https://www.law.uh.edu/faculty/cjoyce/copyright/release10/universal.html>