Video Scripts Week 2

### Question 1

Prompt: Identify and describe one research question that was not answered in the Hurley et al. paper on p2p trafficking. In other words, tell me about a potential direction for future work. You should describe how this research question might be answered using the existing data sets. Alternatively, you may describe what new data needs to be collected to answer this question. Importantly, you should explain why this question is useful to answer, e.g., the implications such an answer might have on law enforcement investigations.

In the Hurley research paper on peer 2 peer CP trafficking, an open question was left as to whether network-observable behaviors, like an interest in certain types of imagery, would correlate with off-line behaviors that would be of interest to law enforcement, such as child molestation.

As cited in the Hurley paper, a previous study found that 16% of all investigations of CP possession ended with discovering contact offenders. So to help answer this question of an online/offline correlation, we need an interdisciplinary study between computer and behavioral science researchers, along with the aid of law enforcement.

For this future study, the techniques described and data collected in this paper could be used again to identify CP traffickers. Thos include probing p2p networks for unique IPs sharing files of interest with known Globally unique identifiers in the system as CP. However, this is not enough.

This is where the behavioral science researchers would contribute by interviewing criminals with informed consent to find out whether the actions performed offline were influenced in any way by observing imagery online first.

If found to be the case, it would aid law enforcement because it would give greater incentive for funding to try find new ways to stop p2p sharing of CP. If we can stop a person from acting offline due to influence from online imagery, it is one less terrible act done to child.

### Question 2

Prompt: Describe the intellectual nugget of the Silhouette paper. Warning: I am throwing you into the deep end with this one. You won't have the required background to understand everything, so focus only on understanding the key intellectual contribution. Hint: some of the concepts described in the paper (e.g., shadow stacks) have been around for a while and, as such, are not the key contribution of this paper.

The intellectual nugget of the research paper is that they created a new software defense system that guarantees that a return instruction will always return to its dynamic legal destination. Thy accomplish this by introducing a new intra-address memory space isolation technique dubbed store hardening, which protects memory regions from corruption. Along with store hardening, they built a compiler and runtime system called “Silhouette” that leverages their new memory isolation scheme to provide embedded applications protection from control flow hijacking attacks, with what they called a “protected shadow stack.”

Their new Silhouette compiler and run time system creates this protected shadow stack by transforming application code with four new compiler passes placed after native code but before the hardware abstraction layer. The four new compiler passes include:

A shadow stack transformation, which modifies the native code to save return values on a shadow stack and to use the return value stored there in return instructions.

Store hardening, which modifies all store instructions, except those used in the shadow stack

Control flow integrity transformation which indirect function calls ensure that a program execution follows a pre-computed control flow graph.

And last privileged code scanner which analyzes the native code prior to emitting the final executable.

Though the research was focused on the ARMv7-M architecture, the new technique they developed are applicable to a wide range of ARM architectures.