**Abstract**

**Detecting Web Application Vulnerabilities Using Information Flow Analysis**

**Smitha Sundareswaran and Anna Squicciarini**

**The Pennsylvania State University**

Web application vulnerabilities have been commonly exploited to launch a slew of attacks on client systems. These vulnerabilities range from well-known attacks such as SQL injection attacks and cross-site scripting attacks to more recent attacks such as content repurposing attacks like the Gifar and flash-based attacks. In light of this, we recently proposed the DeCore architecture for detecting and preventing content repurposing attacks. The DeCore relies on a control flow graph (CFG) which captures all the possible interactions between the currently browsed web page, the client system and a remote site based on the source code of the web page being loaded on the client machine, and denotes them as possible states that can be reached by the browser. The legitimate states are differentiated from the illegitimate ones based on the user’s input or actions which drive the browser from one state to another. We now show how this architecture can be extended to detect other browser vulnerabilities. Specifically, the extended solution relies on the CFG along with tainting of data to allow the DeCore to detect subtle attacks such as stealing of passwords by allowing it to trace the flow of the client’s information through the browser. We present the performance of this architecture with regards to detecting and preventing content repurposing attacks, and discuss its ability to detect and prevent SQL injection attacks. We also show how the DeCore architecture is a general solution which can be applicable either at the client end or at the server end.