



**RESEARCH ARTICLE**

# Signature Free Virus Blocking Method to Detect Software Code Security

*N.Magarani<sup>1</sup>, K.Devipriya<sup>2</sup>, S.Madhan Kumar<sup>3</sup>, T.Viknesh Kumar<sup>4</sup>, K.Kumaresan<sup>5</sup>*

<sup>1</sup>Computer Science and Engineering, K.S.R College of Engineering, Tiruchengode  
kavimaha92@gmail.com

<sup>2</sup>Computer Science and Engineering, K.S.R College of Engineering, Tiruchengode  
priyaksrce@gmail.com

<sup>3</sup>Computer Science and Engineering, K.S.R College of Engineering, Tiruchengode  
madhanks89@gmail.com

<sup>4</sup>Computer Science and Engineering, K.S.R College of Engineering, Tiruchengode  
vickeystormchaser@gmail.com

<sup>5</sup>Assistant Professor, Computer Science and Engineering, K.S.R College of Engineering, Tiruchengode  
mkkumz@gmail.com

---

*Abstract— We propose SigFree, an online signature-free out-of-the-box application-layer method for blocking code-injection buffer overflow attack messages targeting at various Internet services such as web service. Motivated by the observation that buffer overflow attacks typically contain executables whereas legitimate client requests never contain executables in most Internet services, SigFree blocks attacks by detecting the presence of code. Unlike the previous code detection algorithms, SigFree uses a new data-flow analysis technique called code abstraction that is generic, fast, and hard for exploit code to evade. SigFree is signature free, thus it can block new and unknown buffer overflow attacks; SigFree is also immunized from most attack-side code obfuscation methods. Since SigFree is a transparent deployment to the servers being protected, it is good for economical Internet wide deployment with very low deployment and maintenance cost. We implemented and tested SigFree; our experimental study shows that the dependency-degree-based SigFree could block all types of code-injection attack packets (above 750) tested in our experiments with very few false positives. Moreover, SigFree causes very small extra latency to normal client requests when some requests contain exploit code.*

*Key Terms: - Distilling Instruction Sequence Distiller, Instruction Sequencer Analyser, Proxy Based Sigfree, Code Abstraction and SSL Proxy.*

---

Full Text: <http://www.ijcsmc.com/docs/papers/March2013/V2I3201313.pdf>