# Detecting Stack based kernel Information leaks

S. Peiró, M. Muñoz, M. Masmano, and A. Crespo.

*Instituto de Automática e Informática Industrial (AI2)*
*Universitat Politècnica de València, Spain*
*{speiro, mmunoz, mmasmano, acrespo}@ai2.upv.es*

**Abstract.** The Linux kernel has become widely adopted in the mobile devices and cloud services, parallel to this has grown its abuse and misuse by attackers and malicious users. This has increased attention paid to kernel security through the deployment of kernel protection mechanisms. Kernel based attacks require reliability, kernel attack reliability is achieved through the information gathering stage where the attacker is able to gather enough information about the target to succeed. The taxonomy of kernel vulnerabilities includes information leaks, that are a class of vulnerabilities that permit access to the kernel memory layout and contents. Information leaks can improve the attack reliability allowing the attacker to read sensitive kernel data to bypass kernel based protections.
In this work, we aim at the detection of stack based kernel information leaks to secure kernels. We analyse the problem of stack based kernel infoleaks, then we perform a classification of the causes of information disclosure vulnerabilities. Next, we propose an approach for the detection of stack based kernel infoleaks using static analysis techniques, and last we evaluate our approach applying it to the Linux kernel.

```
@incollection{
    title={Detecting Stack Based Kernel Information Leaks},
    author={Peiró, S. and Muñoz, M. and Masmano, M. and Crespo, A.},
    booktitle={International Joint Conference SOCO'14-CISIS'14-ICEUTE'14},
    series={Advances in Intelligent Systems and Computing},
    year={2014},
    volume={299},
    pages={321-331}
    doi={10.1007/978-3-319-07995-0_32},
    url={http://dx.doi.org/10.1007/978-3-319-07995-0_32},
    publisher={Springer International Publishing},
    isbn={978-3-319-07994-3},
}
```