Exploitation in the wild: what attackers really do, and what we should(n't) worry about.

Abstract. Vulnerability exploitation is a major threat to software and system security. The current model for the attacker, basically unmodified since the '70s, is well synthetized in Bruce Schneier's famous quote "*security is only as strong as the weakest link*". In other words, if a vulnerability is there the defender needs to fix it because, sooner or later, the *very powerful* attacker will exploit it. From this "vision of security", metrics for vulnerability risk (*CVSS score*) and guidelines and policies for vulnerability remediation (*U.S. Government SCAP Protocol*) emerged. Most research in IT security also relies on these assumptions. However, this model seems in contrast with recent observations of attacks in the wild, according to which automatically generated attacks represent two thirds of the threats for the final user [Google 2011, Symantec 2011]. To better understand this scenario we performed three parallel studies:

1) We analyzed the *Black Markets for vulnerabilities* and extracted information on market properties, traded attack automation tools (namely *Exploit Kits)* and vulnerabilities.
2) We collected and analyzed data on vulnerabilities actually exploited in the wild from Symantec's sensors worldwide.
3) We tested the CVSS score as a "*risk test for exploitation*", as current guidelines (such as the U.S. SCAP protocol) suggest using it.

Our results evidence that current approaches to computer security may be deeply affected and misled by unrealistic assumptions on vulnerabilities and exploits, vulnerability measures and attacker capabilities. As a consequence, current policies and guidelines relying on the worldwide accepted CVSS score could be *widely sub-optimal.* We underline that a new approach to computer security may be needed in order to enhance risk metrics, and therefore to allow for better policies, better investments and a better management of security.

[Google 2011] M. Rajab, L. Ballard, N. Jagpal, P. Mavrommatis, D. Nojiri, N. Provos, and L. Schmidt. Trends in circumventing web-malware detection. Technical report, Google, 2011.
[Symantec 2011] Symantec. *Analysis of Malicious Web Activity bya ttack Toolkits*. Symantec, Available on the web at http://www.symantec.com/threatreport/topic.jsp? id=threat activity trends&aid=analysis of malicious web activity, online edition, 2011. Accessed on June 1012.

Speaker short bio. Luca Allodi received his Master Degree in Information Security from the University of Milan in 2011. Back in 2005, during the last years of high school he was co-founder and CEO of *Area-Software*, a start-up for web development and IT consultancy in Brescia, his hometown. The experience with Area-Software continued for more than six years, until his enrollment as a Ph.D. student at the University of Trento, where Luca is currently located. His interest for research dates back to the time of his bachelor thesis in Milan, where he worked on social network dynamics and information exchange and integrity. This work resulted in two research papers and seeded so far three more Master degree theses at the University of Milan, one of which he co-supervised. During his Ph.D., his research interests moved to the economics of vulnerability exploitation and how these could be used as a proxy for risk measurement and assessment. He is part of the research group UNITN at FP7 European project SECONOMICS.