

## **Session E23 – Security Development Lifecycle Applications and Infrastructure**

*By Himanshu Dwivedi, @stake*

### Topic Summary

This session will describe the different authentication protocols Microsoft has included in its operating systems from LanManager to Kerberos, as well as the known theoretical and practical attacks against each. We will explore real-world situations, drawn from the experiences of @stake consultants, where a lack of knowledge regarding the inner workings of Windows authentication can lead to full compromise of an Active Directory based network. We will also demonstrate how many common system administration and security tools, including Microsoft's official security compliance software, can inadvertently expose AD enabled networks to compromise. We will then present a new tool which performs pre-computed dictionary attacks against the NTLM authentication protocol used by Internet Explorer. A live demonstration of this tool, as well as an explanation of different attack scenarios, will emphasize the danger inherent in ignoring the cryptographic details underlying basic authentication technologies. The talk will conclude with mitigation strategies and technical precautions that administrators can take to reduce the risk of using a unified Windows authentication infrastructure.