


复旦大学数学科学学院

数学综合报告会

报告题目：**Eliminating the Threat of Drive-By Download Attacks**

报告人：　徐寿怀教授

（美国德州大学圣安东尼奥分校计算机系）

报告时间：2016-07-14　星期四 10:30-11:30

报告地点：光华东主楼 1801

摘要：Drive-by download attacks exploit malicious websites to compromise computers when they visit those malicious websites. Drive-by download attacks have become a big cyber threat. Given that malicious websites are inevitable, we need solutions for detecting malicious websites, while anticipating that drive-by download attacks will become increasingly evasive. In this talk, I will present our research towards eliminating the threat of drive-by download attacks. I will start with a novel cross-layer method for detecting malicious websites, which essentially uses the network-layer "lens" to expose more information about malicious websites. This cross-layer detection method is about 50 times faster than the dynamic approach, while achieving almost the same detection effectiveness as the static approach (in terms of accuracy, false-negative rate, and false-positive rate). I will then illustrate how sophisticated attacks can evade the detection, and show how proactive defense can achieve a significant success against these sophisticated attacks. I will outline future research directions towards the ultimate goal.

Bio:

Shouhuai Xu is a Full Professor in the Department of Computer Science, University of Texas at San Antonio. He is Director of the Laboratory for Cybersecurity Dynamics (http://www.cs.utsa.edu/~shxu/LCD/index.html). His research is primarily in making cyberspace secure and trustworthy. He is especially interested in both theoretical modeling/analysis of cybersecurity and devising practical cyber defense techniques (e.g., provably-secure cryptographic protocols and other advanced cyber defense mechanisms). His research has been funded by AFOSR, ARO, NSF and ONR. He was a Program Committee co-chair of NSS'15 and Inscrypt'13. He co-initiated the ACM Scalable Trusted Computing Workshop (ACM STC). He has served on the Program Committees of numerous international conferences/workshops. He is currently an Associate Editor of IEEE Transactions on Dependable and Secure Computing (IEEE TDSC) and IEEE Transactions on Information Forensics and Security (IEEE T-IFS). He earned his PhD in Computer Science from Fudan University.