**恶意代码检测**

学习课程：

<http://crypto.stanford.edu/cs155/syllabus.html>

<http://inst.eecs.berkeley.edu/~cs161/sp15/>

<http://courses.cse.tamu.edu/guofei/csce465/>

<http://www.cs.colostate.edu/~massey/pmwiki/pmwiki.php/CS356/Schedule>

特别注意其中malware、botnet、dns等章节

学习BOOK：

[**Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software**](http://anopaia.com/reviews/best-books-to-learn-malware-analysis1.php), by Michael Sikorski and Andrew Honig.

[**The Tao of Network Security Monitoring: Beyond Intrusion Detection**](http://anopaia.com/reviews/best-books-to-learn-malware-analysis2.php), by Richard Bejtlich.

[**Network Forensics: Tracking Hackers through Cyberspace**](http://anopaia.com/reviews/best-books-to-learn-malware-analysis4.php)，by  Sherri Davidoff

研究论文：

1 [Hybrid detection and tracking of fast-flux botnet on domain name system traffic](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6674213)

2

[Peer-to-Peer Botnet Detection Using NetFlow](https://staff.science.uva.nl/c.t.a.m.delaat/rp/2013-2014/p65/report.pdf)

**3**

FIRMA: Malware Clustering and Network Signature Generation with Mixed Network Behaviors  
Connected Colors: Unveiling the Structure of Criminal Networks

研究目标：

设计检测算法和系统，能够达到足够的检测性能。

expert in Malware Analysis & Intrusion Detection

时间节点：

一个月学习和讨论，探索方案，每周二晚前提交论文读后感或课程学习心得到我邮箱。通过QQ群讨论项目思路，每周三会议见面讨论。

10月前完成所有方案，包括撰写论文、申请专利等

期刊：

**ACM Transactions on Information and System Security (TISSEC)**

**IEEE/ACM Transactions on Networking (TON)**

**会议：**

**SRC：**<http://faculty.cs.tamu.edu/guofei/>

|  |  |  |  |
| --- | --- | --- | --- |
|  | Deadline | Notification |  |
| [DIMVA](http://www.dimva.org/)'14 | Feb. 15 | Mar. 26 | 7/10-11, Egham, UK |
| [USENIX Security'14](https://www.usenix.org/conference/usenixsecurity14) | Feb. 27 | May 9 | 8/20-22, San Diego, CA |
| [RAID'14](http://www.raid-symposium.org/) | Apr. 1 | June 1 | 9/24-26,  Gothenburg, Sweden |
| [ESORICS'14](http://homepages.laas.fr/esorics/) | Apr. | June | 9/7-11, Wroclaw, Poland |
| [SecureComm'14](http://www.securecomm.org/) | Apr. 21 | June 30 | 9/24-26, Beijing, China |
| [ACM CCS'14](http://www.acm.org/sigs/sigsac/ccs/) | May 16 | July 22 | 11/3-7, Scottsdale, Arizona |
| [IMC](http://www.sigcomm.org/events/imc-conference)'14 | Apr. 30/May 7 | July 25 | 11/5-7, Vancouver, Canada |
| [ACSAC](http://www.acsac.org/) 2014 | June 8 | Aug. 15 | 12/8-12, New Orleans |
| [NDSS'15](http://www.isoc.org/isoc/conferences/ndss/) | Aug. 1 | Oct. 22 | 2/8-11, San Diego, CA |
| [NSDI'15](https://www.usenix.org/conference/nsdi15) | Sep. 18/25 | Dec. 15 | 5/4-6, Oakland, CA |
| [ICDCS'15](http://icdcs-2015.cse.ohio-state.edu/) | Dec. 5/12 | March 23 | 6/29-7/2, Columbus, OH |
| [IEEE S&P](http://www.ieee-security.org/TC/SP-Index.html) [2015](http://www.ieee-security.org/TC/SP2015/) | Nov. 14 | Feb. 8 | 5/18-20, San Jose, CA |
| [WWW](http://www.wwwconference.org/) [2015](http://www.www2015.it/) | Nov. 3/10 | Jan. 17 | 5/18-22, Florence, Italy |
| [DSN'15](http://dsn.org/) | Nov. 28/Dec. 8 | Feb. 25 | 6/22-25, Rio de Janeiro, Brazil |

**写作风格：**

**Exposure** **: A Passive DNS Analysis Service to Detect and Report Malicious Domains**

**Touring DNS open houses for trends and configurations**

**A Decision Support System for Placement of Intrusion Detection and Prevention Devices in Large-Scale Networks**

**An Anti-Phishing System Employing Diffused Information**

**Detecting algorithmically generated domain-flux attacks with DNStraffic analysis**

google或scholar.google.com或www.lib.sjtu.edu.cn搜索下载论文