WANG Xing

Specialties: Machine Learning, Android, C/C++, Python, MATLAB, Linux
Ph.D. candidate in Information Security

Education

2010.9~ *PhD in Information Security at Department of Information Security in Beijing Jiaotong University* (Beijing, China).

2014.1~2014.4 *Visit Student*, Machine Intelligence & kNowledge Engineering (MINE), King Abdullah University of Science and Technology, in Thuwal, Saudi Arabia.

2009.9~2010.7 *Master in Computer Science in Beijing Jiaotong University*.

2005.9~2009.7 *B.S. in Computer Science and Technology, Beijing Jiaotong University, China*.

2013.8 *The Fourth International Summer School on Information Security and Protection (ISSISP2013)*, in Northwest University, Xi'an, China.

Publications

[1] **Xing Wang**, Wei Wang, *Characterizing Android Apps Behavior for Effective Detection of Malapps at Large Scale*, Future Generation Computer Systems. (*submitted*)

[2] Wei Wang, **Xing Wang**, Dawei Feng, Jiqiang Liu, Zhan Han, Xiangliang Zhang, *Exploring Permission-induced Risk in Android Applications for Malicious Application Detection*. IEEE Transactions on Information Forensics and Security (**TIFS**), vol. 9, no. 11, pp.1869-1882, 2014

[3] **王星**, 周芳林, 王伟, 韩臻. Android平台的一种安全域隔离方法, 第23届全国信息保密学术会议(IS2013)论文集 ,57-61, 2013.

[4] **Xing Wang**, Zhen Han, and Dawei Zhang, *IDKeeper: A Web Password Manager with Roaming Capability Based on USB Key.* Industrial Control and Electronics Engineering (ICICEE), 2012, International Conference on. IEEE, 2012.

[5] Ruhui Zhang, Ye Du, **Xing Wang**, et al. *An Efficient Episode Matching for Network Security*. Proceeding of the 2nd International Conference on Information, Communication and Education Application. Information Engineering Research Institute Press, Oct. 2011.

Projects

2014.4~2014.9 *大规模条件下 Android 恶意应用行为描述与检测*

负责整体系统的设计和实现。

在应用市场中有效检测恶意应用是 Android 持续发展的关键。本项目从国内6个应用市场（Anzhi，GFan，MyApp等）上抓取了20多万App样本，并从多种渠道获得Android恶意样本18,363个，构成研究所需样本集。基于 Androguard 开发了 Android 应用静态分析工具，从每个样本中提取了权限、组件名、Intent、开发者信息、字符串、API、载荷文件类型等11类特征。将这些特征与多种分类算法进行组合，自动挑选出能够在大规模条件下有效检测 Android 恶意应用的特征。将特征分为平台定义特征和应用特有特征两大类，并将这两大类特征应用在不同时间采集的样本集，分析了两类特征的持久性。所开发的检测系统在误报率为 0.06% 的条件下，检测率达到 96% 。

2013.7~2014.2 *基于权限的 Android 恶意应用检测工具*

负责数据的收集和分析处理，恶意应用检测方法的具体实现。

基于权限的控制方法是 Android 安全机制的核心部分。本项目收集了 Google 官方应用市场上 31 万 应用以及 4868 个真实恶意应用的权限特征。为了理解 Android 的权限模型，本项目从三个层次系统分析了授予权限可能会带来的风险：首先全面分析了单个权限和权限组合的风险，采用基于互信息、相关系数以及T-test的三种特征排序方法，依据权限的风险对其进行排序，并采用序列前向选择和PCA方法识别有风险的权限子集；其次，利用支持向量机、决策树以及随机森林算法评估了利用风险权限检测恶意应用的效果；最后深入分析了检测结果，指出

了基于权限的恶意应用检测方法的有效性和局限性。

2015.8~2015.9 *GUI客户端自动控制软件*

负责客户沟通、项目管理、技术路线研究、软件设计以及具体模块的开发。

自动控制一个运行在 Red Hat 7.1 Linux (2011年发行) 老系统上的图形界面程序，识别该程序的界面状态，接收网络命令后自动按照预定的流程控制鼠标点击，自动控制界面跳转，完成指定控制流程。 项目核心是界面跳转的自动控制，设计了一个非确定性有限自动机来模拟被控客户端界面的变化，受控客户端的每个界面为自动机中的一个状态，鼠标点击等操作是某状态可能接收的事件，设计转移规则控制某个状态接收到事件之后应当执行的动作（如，点击界面上某个按钮），以及动作执行之后要跳转到的状态。项目采用了在C程序中嵌入 Lua 脚本的方案，控制规则易于扩展和并能动态更新。整个工程大约 3000+ 行 C 代码，400 行 Lua 脚本。

2011.3~2011.9 *加密网络应用识别系统*

负责基于节点发现的 BitTorrent 流量识别方法 以及 Episode Matching 算法的代码实现。

通常的网络流量可以采用固定端口、应用层载荷特征等较为直观的方法加以识别，但某些 P2P 应用、恶意软件等采用随机端口，应用层加密、分片、填充等手段规避常用的识别方法，本系统针对此问题设计和实现了：（1）针对基于 BitTorrent 的 P2P 网络应用，设计了一种基于节点发现机制的流量识别方法。该方法从 BitTorrent 协议的协商流量中提取节点信息并用于后续的文件传输流量识别；（2）将 P2P 流量分为长连接、多次短连接和单次短连接三类，重点识别长连接和多次短连接。设计了一种基于扩展的最长公共子序列算法与 K-means 算法结合的自动特征提取系统；（3）针对扩展的最长公共子序列算法提取出的特征，提出了一种时空优化的 Episode Matching 匹配算法，提高了实际应用中的匹配速度。

Specialties

Android	熟悉 Android Framework，App运行机制，App 静态分析与动态分析，熟悉 Android 平台恶意应用运行原理及检测方法。
Machine Learning	能熟练应用 SVM，Random Forest，Logistic Regression 等分类算法；擅长利用 Python，MATLAB 等分析和处理数据。
编程语言和工具	C/C++，Python，Lua, Bash, Makefile, AutoTools, CMake…
GNU/Linux	My daily operating system is Debian

Interests

Sports	Cycling, Ping-pong, Badminton.