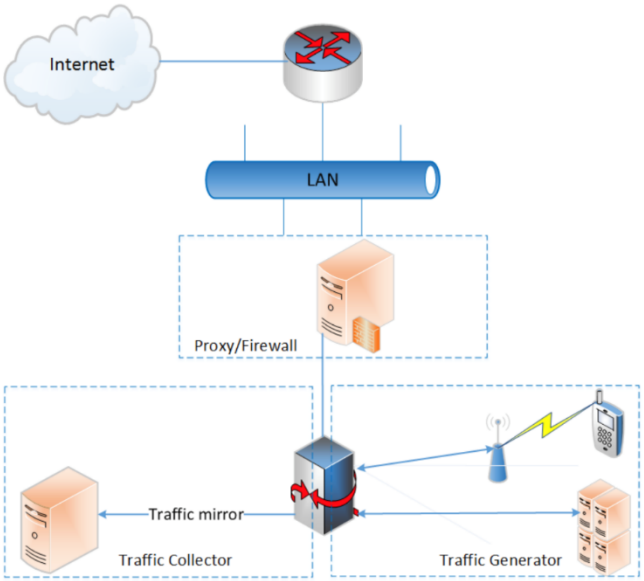
Toward Non-intrusive Detection of Resilient Mobile Malware and Botnet using Application Traffic Measurement

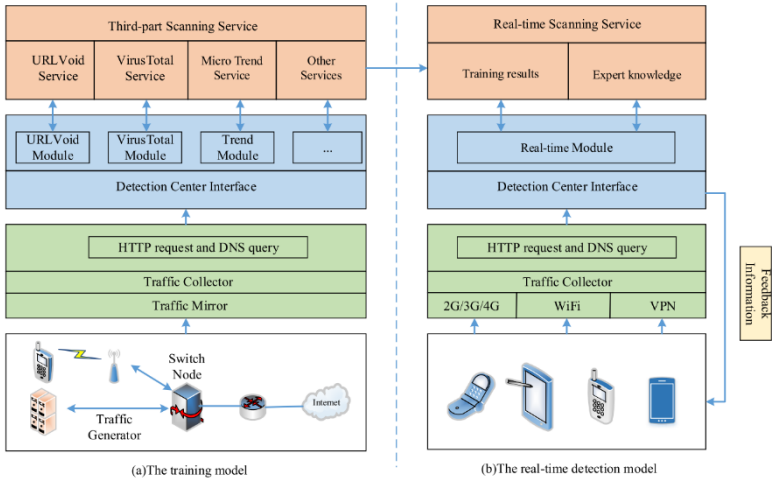
Challenge:

- Mobile malware has become prevalent in app markets
- Mobile botnets become a serious threat to the mobile Internet
- Malware detection based on static and dynamic analysis techniques is too resource-consuming
- How to Identify malware and malicious system activities in **real-time** and in a **non-intrusive** manner?

Solution:

- **Mobile malware traffic collection**: use program analysis to identify network-related APIs, and to develop triggering mechanisms
- **Network-based mobile malware detection**: use data analytics to identify mobile malware in real time using application-layer traffic
- **P2P/HTTP botnet detection and mobile botnet characterization**: evaluate the aggregated network behavior from multiple interactive bots





Scientific Impact:

- Develop a deep understanding of malware network behaviors and to translate this understanding into traffic collection tools that can capture malicious network behaviors
- The research results will offer valuable insights into mobile malware's spreading mechanisms and malicious intents and will inspire novel theoretical and systematic studies in network behavior analysis of mobile apps

Broader Impact:

- The malware traffic dataset will be made available to the research community to inspire mobile malware research
- Industrial partners such as anti-virus security companies, will benefit from the proposed detection and countermeasures
- Incorporate the knowledge developed in this project into both undergraduate and graduate course modules.
- Disseminate research finding to K-12 students in STEM disciplines through Nebraska summer research program and summer camps.

NSF Award #: 1566388
PI: Qiben Yan
Dept. of Computer Science and Engineering
University of Nebraska Lincoln
Lincoln, Nebraska
Email: yan@unl.edu
Phone: 402-472-5075