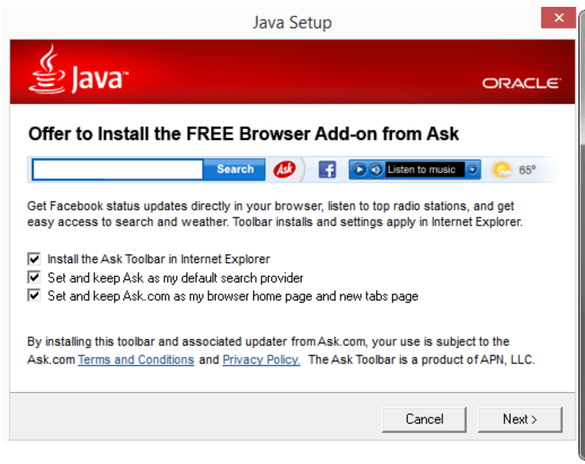
Alberto Geniola, Markku Antikainen, Tuomas Aura

Architecture for Analyzing Potentially Unwanted Programs

Freeware installers are notorious for bundling *potentially unwanted programs* (toolbars etc.) alongside with the applications they are expected to install.

While PUP is not malware (opt-out is usually possible), they may still collect personal information and impair the user experience.

Goal: Large-scale analysis of freeware software installers



Methodology

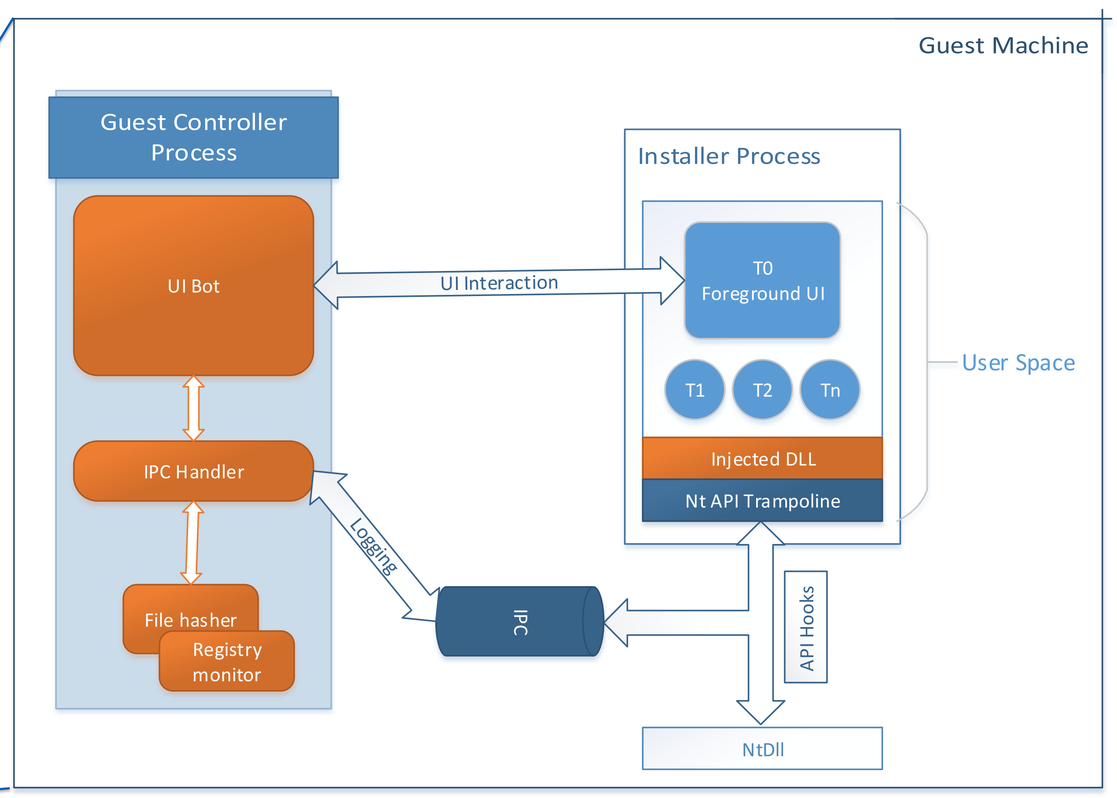
1. Crawl and collect software from download sites
2. Run installers on a (virtual) machine
3. Analyze the collected data

Automate everything

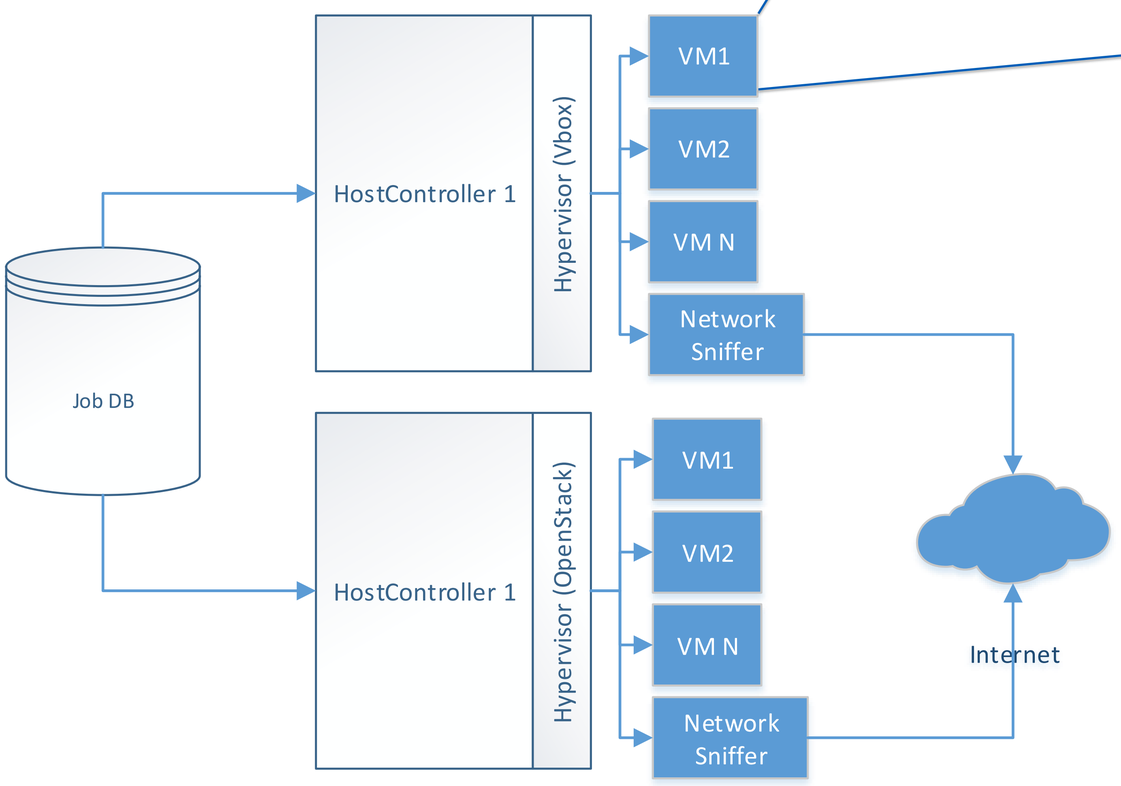
Focus on 32-bit Windows apps

Installation and data gathering

- Click through the installation process
- Automated UI interaction with image recognition and heuristics
- Track and capture the net traffic
- DLL injection and kernel API hooks to log file system and registry accesses



Architecture



Ongoing work and early results

- High throughput thanks to parallel execution = 1.5 minutes per installer
- Single installer average running time 10 min
- Over 70% of installers correctly finished
- Next step: to analyze the data collected from ~900 installers.

Acknowledgment

The work has been done within the scope of the CyberTrust SHOK project funded by DIGILE.

Aalto University

POLITECNICO DI TORINO 1859 1906