

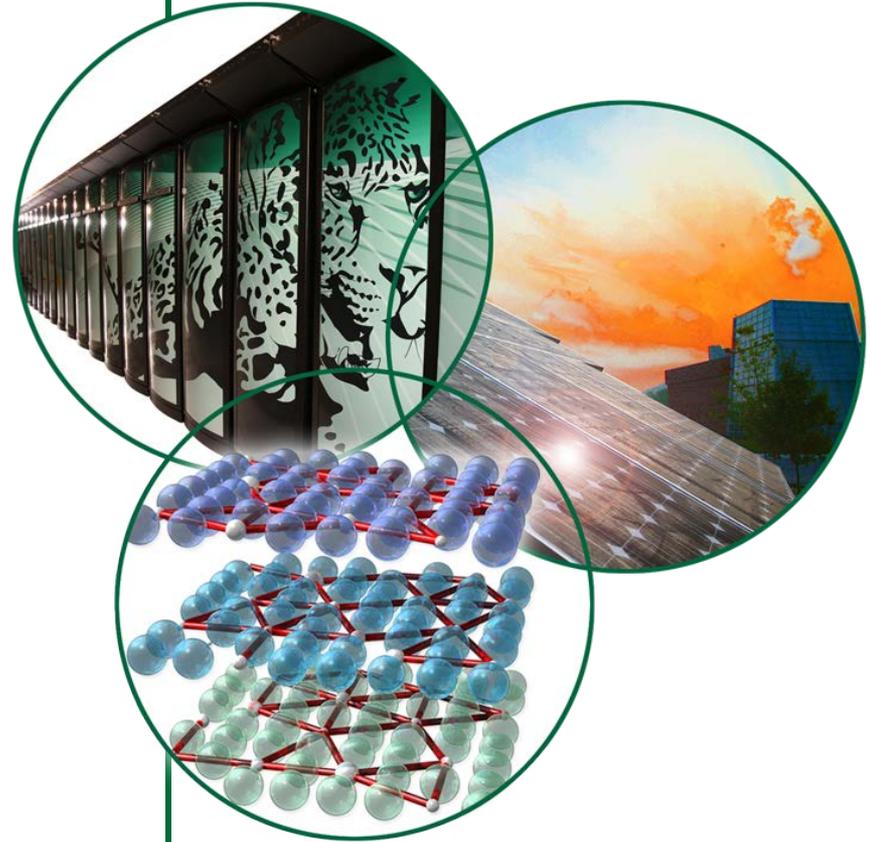
USB-ARM: USB Architecture for Removable Media

Logan Lamb

lamb1m@ornl.gov

Cyberspace Sciences and
Information Intelligence Group

Oak Ridge National Lab



Need

- Persistent cyber-threats
- 2012 Cost of Cyber Crime Study
 - Annual incident costs average \$8.9 million
 - 1.8 successful attacks per company per week
 - Network security improvements have led attackers to explore physical access avenues
 - Stuxnet
 - SillyFDC worm / Afghanistan
- Traditional antiviruses are not sufficient
 - Initial detection rate less than 5%

Need

- Threat addressed via policies hinder productivity
 - Simply placing epoxy in USB ports
 - Required scanning at dedicated location
 - Banning of all removable media
- Actual effectiveness of policy
 - If USB ports are not epoxied, then policy can be easily circumvented
- Physical security warrants specialized software as much as network security

A good setup

- Firewall ✓
- Intrusion Prevention System ✓
- Deep Packet Inspection ✓
- Antivirus up to date ✓



But not good enough

- Firewall ✓
- Intrusion Prevention System ✓
- Deep Packet Inspection ✓
- Antivirus up to date ✓
- Removable media protection ✗



The Takeaway

- USB-ARM is the solution which will allow the use of removable media in any organization

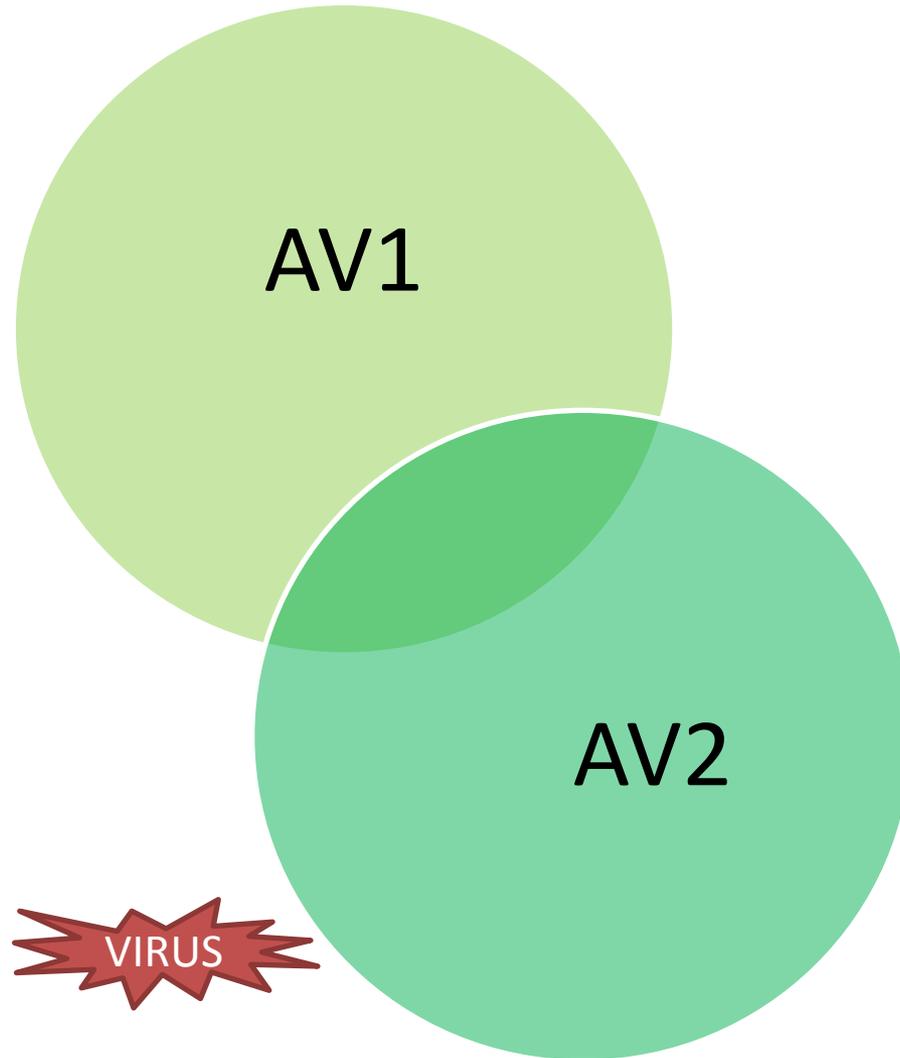
Approach

- Create a Windows driver which intercepts all communication between removable media and operating system
- Executes user-defined 'stages' and either grants or disallows access on a per file basis
- Guarantees no access is allowed until all stages are completed
- Example:
 - Run McAfee anti-virus
 - Run AVG anti-virus
 - Disallow access to Windows executables (PE / PE+)

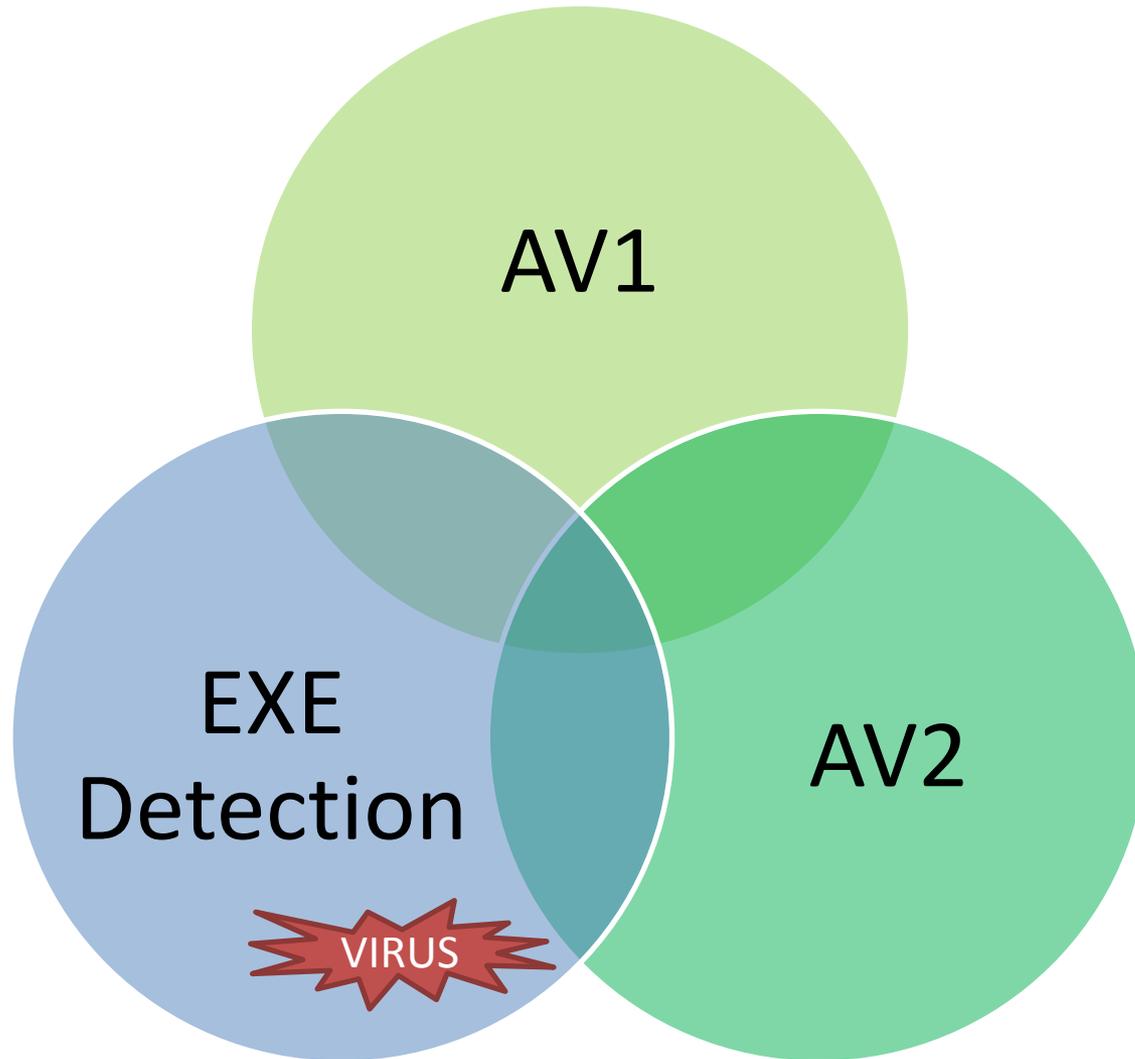
First Stage



Second Stage



Third Stage



Benefit

- No more auto-run!
 - Even if it is still enabled in Windows, USBARM prevents all race conditions
- Guarantees user/organization-defined criteria are met prior to allowing access to the removable media
- Is as effective as the sum of its parts
- Extensible, allows user/organization defined whitelisting and blacklisting

Competition

- Only blocks drives or disables Windows auto-run
 - Windows policy can do that
- Applocker (from Microsoft)
 - Only enables access control of applications
 - Same policy applied across all volumes
 - Only certain versions of Windows
 - Arbitrary rule/feature limits

Risks

- Cost of USB-ARM stages
 - Multiple AV licenses, development of new plugins
- Time to market
 - Straightforward idea and approach, barrier to entry is low

In closing

- User/Organization knows best what policy they need
- Simple, Effective, Supplemental, Extensible