Modeling the Operations of the Vulnerability Ecosystem

Coordinated Vulnerability Disclosure (CVD) is an emerging capability within DoD. But CVD is known to be difficult and prone to controversy when multiple vendors are involved, as in the case of recent vulnerabilities like Meltdown and Spectre. In this LENS project we modeled the factors affecting cooperation in the multiparty CVD process.

**Calibration Target Ranges for Baseline**

Drivers of CVD Player Behaviors

- **Finder/Reporter Performance**
  - Make Money
  - Establish Reputation
  - Avoid being Sued
  - Clear Conns & Respectful Treatment

- **Vendor Performance**
  - Generate Revenue
  - Generate and Maintain Customer Base

- **Vendor Fix Known**
  - Keep Vendor Costs Low
  - Maintain Vendor Reputation

- **Coordinate Vulnerability Disclosure**
  - Keeping Quiet about Vuls during Embargo before Patching
  - Keeping Quiet about Vuls during Embargo after Patching

**Venity: A Hybrid Modeling Toolset**

Venity is being developed by Ventana Systems, Inc.

- Modeling and simulation environment supporting two types of modeling
- Agent-based modeling
- System dynamics modeling
- Supports modular construction of socio-technical models for scalable development by independent teams

**Used to Model the Multi-Party Coordinated Vulnerability Disclosure (MPCVD) Problem**

- Finders, vendors, and MPCVDs are agents
- Simulation runs many MPCVDs over two years to assess management strategies and policies for the coordinator to try out
- Current model under development has been calibrated along several dimensions

- Adjustable model parameters include the number of finders and vendors, size distribution of the MPCVDs and vendors, embargo duration, likelihood of accidental and purposeful disclosure
- Social cost measure includes likelihood of vul exploitation, maximum amount of damage, hacker vul discovery time, attack rate per deployer, amplification of attack rate after disclosure, user workaround costs over time (adapted from Cavusoglu et al., 2007 [1]).

**Initial Observations from Non-Validated Model**

- The longer after patch development that embargo goes, the greater the chance of reneging
- The more vendors participating in MPCVDs the more early disclosures that occur
- The sooner that patches are distributed the lower the social cost to deployers, whether patch distributed (and vul disclosed) before or after embargo
- Shortening the embargo time leads to lower rates of reneging, but high rates of no patch after embargo
- Assumption: Faster patching is more costly for all vendors.

**Accidental Disclosure Sector**
