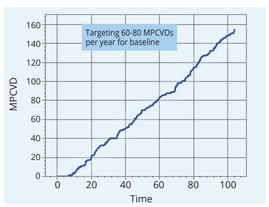
Modeling the Operations of the Vulnerability Ecosystem

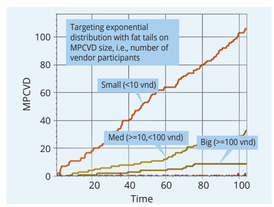
Coordinated Vulnerability Disclosure (CVD) is an emerging capability within DoD. But CVD is known to be difficult and prone to controversy when multiple vendors are involved, as in the case of recent vulnerabilities like Meltdown and Spectre. In this LENS project we modeled the factors affecting cooperation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

Calibration Target Ranges for Baseline

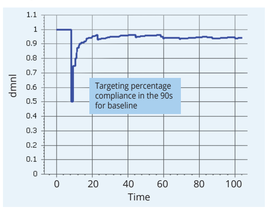
Completed MPCVD Count



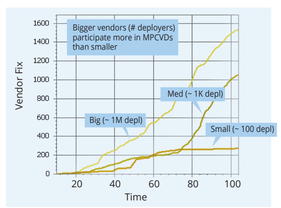
MPCVD Class Count



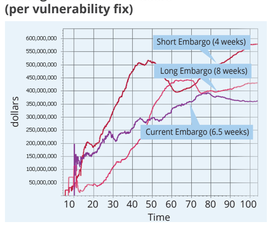
Completed ratio of MPCVDs that held



VendorFix Size Count

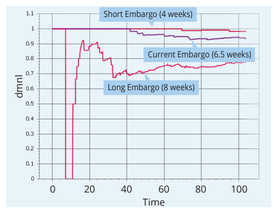


Average social cost to users (per vulnerability fix)



Current embargo (set to about 45 days) to be the lowest cost option per vulnerability fix.

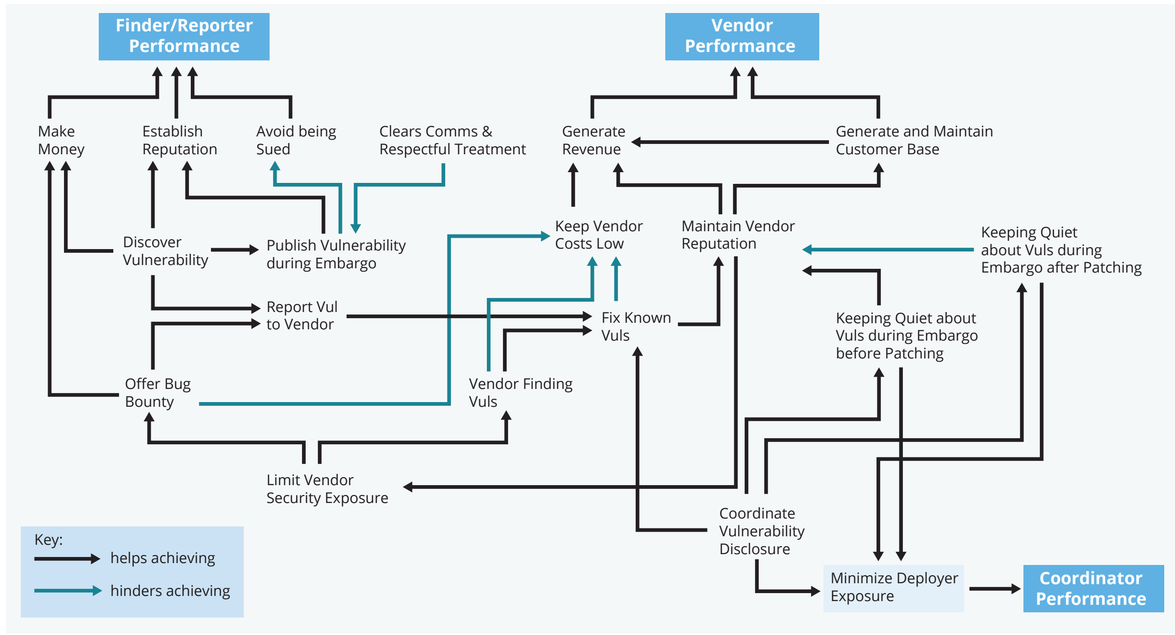
Completed ratio of MPCVDs that held



While the short embargo ensures more MPCVDs hold through the embargo period, as seen in the chart on the left, they are the most costly to users. The current embargo period is a good middle ground to reduce cost to users.

Conclusion: Adjusting the embargo period to increase the likelihood that patches can be developed JUST in time appears to be a good strategy for reducing cost.

Drivers of CVD Player Behaviors



Ventity: A Hybrid Modeling Toolset

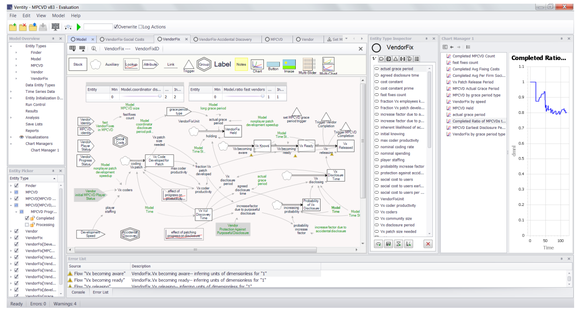
Ventity is being developed by Ventana Systems, Inc.

- 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].

[1] Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2007). Efficiency of vulnerability disclosure mechanisms to disseminate vulnerability knowledge. IEEE Transactions on Software Engineering, 33(3), 171-185.

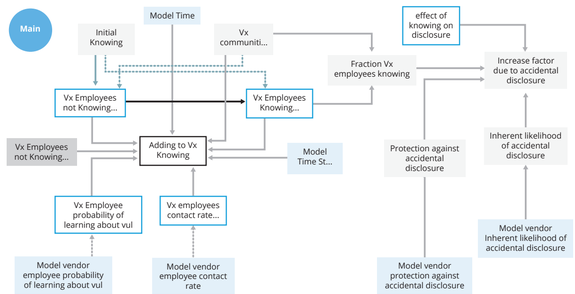


The Ventity Interface

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



Carnegie Mellon University
Software Engineering Institute

Andrew Moore | apm@cert.org
with Dr. Will Casey, Dr. Jeffrey Chrabaszcz, Allen Householder, Dr. Soumyo Moitra