DARTMOUTH

Institute for Security Technology and Society at Dartmouth

DiscX: Should Governments Disclose or Exploit Vulnerabilities?

As more and more vulnerabilities are found in the growing space of connected devices, governments are often confronted with the problem of what to do when their cyber-warfare units discover a new vulnerability. Generally, the two options are either to disclose the vulnerability, which may be ideal if the product containing the vulnerability is manufactured or in wide use in the country, or to hold it in secret and develop an exploit. The decision to disclose or exploit often depends on a number of factors, such as whether an adversary will discover and disclose the vulnerability, what damage an adversary might cause if they choose to exploit, and how disclosure might protect a nation's corporations. In order to better facilitate making the optimal decision, Dartmouth collaborated with military experts from the Netherlands Defense Academy to develop a Repeated Cyber Warfare Game (RCWG) formulation of the problem, as well as a prototype system called DiscX.

DiscX is intended to augment the current decision making procedure for "exploiting vs. disclosing" with a rigorous tool that uses agency experts' inputs to help agencies such as the US Government's Equities Review Board arrive at an optimal solution.

Repeated Cyber Warfare Game (RCWG)

The RCWG framework formulates cyber warfare between two parties by modeling competition over vulnerabilities. The RCWG first considers a one stage game, then extends this one stage game to a repeated stage setting, representing competition over multiple vulnerabilities. In a stage, there are 2 players representing the 2 opposing countries, as well as a joint strategy and a joint payoff function of the two players.

The payoff function depends on several factors, including:

- Development cost
- Exploit payoff
- Disclosure payoff

The one-stage game is formulated as an alternated stochastic optimization problem for computing the best response of a player, is solved using Monte-Carlo sampling.

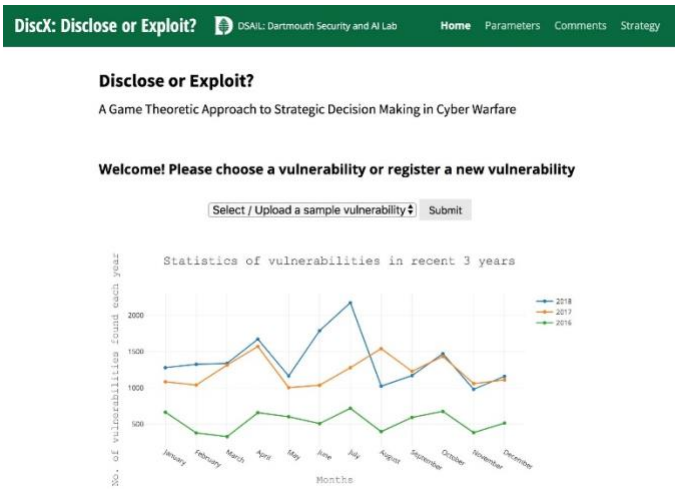
The RCWG experiment setting used in evaluation was created using data from authoritative national security sources, like the Rand Corporation, as actual data from governments is usually classified. Using a dataset of more than 200 zero-day exploits from 2002 to 2016, values for vulnerability related parameters were obtained, such as a mean time of discovery of 200 days and an average cost of developing an exploit based on a zero-day vulnerability at $30,000.

After evaluation, it was found that the RCWG framework yields a much higher payoff than 3 baselines of random, always exploit, or always disclose strategies. Additionally, RCWG converges after 220 iterations, at around 20 seconds on average. It is clear that RCWG efficiently provides the optimal decision in cyber warfare strategy.

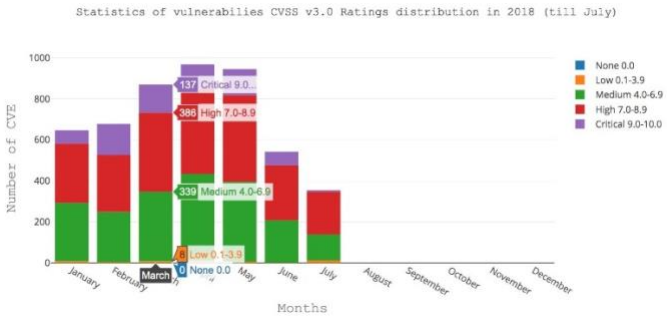
DiscX

Dartmouth has also developed the prototype DiscX system to support government decision making. This system allows for user input of vulnerability information, which runs through RCWG and gives a recommendation on the decision to make based on their knowledge of a

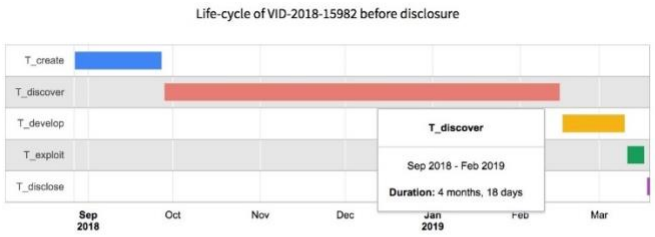
specific situation. Sample screenshots of the DiscX system are provided for display below.



Opening screen of DiscX



Vulnerability statistics after initial selection from opening screen



T_create: The creation time of a vulnerability is the release time of either the hardware/software in which the vulnerability exists.

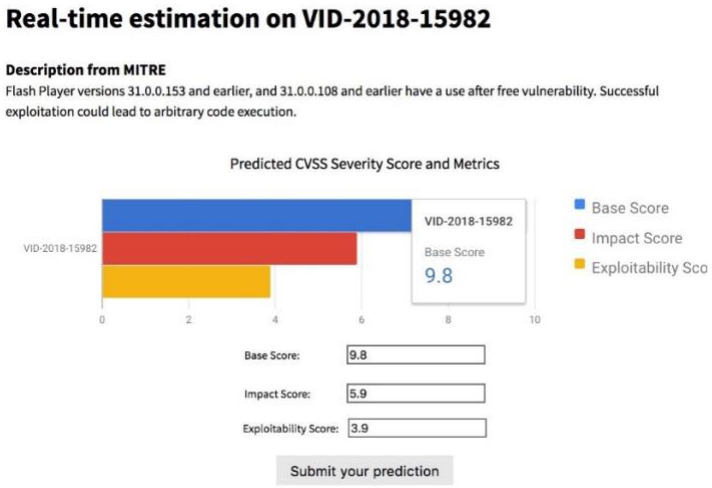
T_discover: This is the amount of time (after T_create) when white/black hat hackers become aware of the vulnerability.

T_develop: This is the amount of time (after T_discover) needed to build an exploit based on this vulnerability.

T_exploit: This is the amount of time (after T_develop) for which the exploit developer operates/uses the exploit.

T_disclose: This is the time when the existence of the vulnerability is publicly disclosed (e.g. through the National Vulnerability Database).

Vulnerability parameter information



Vulnerability score information and user modification

Additional Information

References

1. Haipeng Chen, Qian Han, Sushil Jajodia, Roy Lindelauf, V.S. Subrahmanian, and Yanhai Xiong. "Disclose or Exploit? A Game Theoretic Approach to Strategic Decision Making in Cyber Warfare." Accepted for publication in *IEEE Systems Journal*. https://ieeexplore.ieee.org/document/8967205

Video

https://www.cs.dartmouth.edu/~dsail/projects/discx/discx_demo.mp4

Presentation

https://www.cs.dartmouth.edu/~dsail/projects/game/slides/

PARTICIPANTS

Lead: V.S. Subrahmanian

Haipeng Chen, Qian Han, Sushil Jajodia, Roy Lindelauf, and Yanhai Xiong.

DARTMOUTH

Security and Artificial Intelligence Laboratory