New cyber-attack model helps hackers time the next Stuxnet

January 13 2014, by Akshat Rathi

Disabling a country’s electricity with the click of a button. Credit: usairforce

Of the many tricks used by the world's greatest military strategists, one usually works well – taking the enemy by surprise. It is an approach that goes back to the horse that brought down Troy. But surprise can only be achieved if you get the timing right. Timing which, researchers at the University of Michigan argue, can be calculated using a mathematical model – at least in the case of cyber-wars.

James Clapper, the director of US National Security, said cybersecurity is "first among threats facing America today," and that's true for other world powers. In many ways, it is even more threatening than conventional weapons, since attacks can take place in the absence of open conflict. And attacks are waged not just to cause damage to the enemy, but often to steal secrets.

Timing is key for these attacks, as the name of a common vulnerability – the zero-day attack – makes apparent. A zero-day attack refers to attacking a vulnerability in a computer systems on the same day that the vulnerability is recognised, when there is preparedness to defend against attack. That is why cyber-attacks are usually carried out as soon as a cyber-weapon is ready and before an opponent has the time to fix its vulnerabilities.

As Robert Axelrod and Rumen Iliev at the University of Michigan write in a paper just published in the *Proceedings of the National Academy of Sciences*, "The question of timing is analogous to the question of when to use a double agent to mislead the enemy, where it may be worth waiting for an important event but waiting too long may mean the double agent has been discovered."

Equations are as good as weapons

Axelrod and Iliev decided the best way to answer the question of timing would be through the use of a simple mathematical model. They built the model using four variables:

1. Cyber-weapons exploit a specific vulnerability.
2. Stealth of the weapon measures the chance that an enemy may find out the use of the weapon and take necessary steps to stop its reuse.
3. Persistence of the weapon measures the chance that a weapon

can still be used in the future, if not used now. Or, put another way, the chance that the enemy finds out their own vulnerability and fixes it, which renders the weapon useless.

4. Threshold which defines the time when the stakes are high enough to risk the use of a weapon. Beyond the threshold you will gain more than you will lose.

Using their model, it is possible to calculate the optimum time of a cyber-attack:

When the persistence of a weapon increases, the optimal threshold increases – that is, the longer a vulnerability exists, the longer one can wait before using it.

When the stealth of a weapon increases, the optimal threshold decreases – the longer a weapon can avoid detection, the better it is to use it quickly.

Based on the stakes of the outcome, weapon must be used soon (if stakes are constant) or later (if the stakes are uneven). In other words, when the gain from an attack is fixed and ramifications are low, it is best to attack as quickly as possible. When the gain is high or low and ramifications are high, it is best to be patient before attacking.

How to plan the next Stuxnet

Axelrod and Iliev's model deserves merit, according to Allan Woodward, a cybersecurity expert at the University of Surrey, because it fits past examples well. Their model perfectly predicts timing of both the Stuxnet attack and Iran's counter to it.

Stuxnet was a worm aimed at interfering with Iran's attempts to enrich uranium to build nuclear weapons. So, from an American perspective,

the stakes were very high. The worm itself remained hidden for nearly 17 months, which means its stealth was high and persistence was low. According to the model, US and Israel should have attacked as soon as Stuxnet was ready. And indeed that is what seems to have happened.

Iran responded to this attack by targeting the workstations of Aramco, an oil company in Saudi Arabia that supplied oil to the US. Although the US called this to be the "most destructive cyber-assault the private sector has seen to date", it achieved little. However, for Iran, the result mattered less than the speed of the response. In a high stakes case, the model predicts immediate use of a cyber-weapon, which is what happened in this case, too.

Although the model has been developed for cyber-attacks, it can be equally effective in modeling cyber-defense. Also, the model need not be limited to cyber-weapons; small changes in the variables can be made so that the model can be used to consider other military actions or economic sanctions.

Just like the atomic bomb

Eerke Boiten, a computer scientist at the University of Kent, said: "These models are a good start, but they are far too simplistic. The Stuxnet worm, for example, attacked four vulnerabilities in Iran's nuclear enrichment facility. Had even one been fixed, the attack would have failed. The model doesn't take that into account."

In their book Cyber War: The Next Threat to National Security and What to Do About It, Richard Clarke and Robert Knake write:

It took a decade and a half after nuclear weapons were first used before a complex strategy for employing them, and better yet, for not using them, was articulated and implemented.

That transition period is what current cyber-weapons are going through. In that light, the simplicity of Axelrod and Iliev's model may be more a strength than a weakness for now.

More information: "Timing of cyber conflict," by Robert Axelrod and Rumen Iliev. PNAS, www.pnas.org/cgi/doi/10.1073/pnas.1322638111

Source: The Conversation