Should people who discover a software vulnerability make the information public?

blogs.lse.ac.uk/businessreview/2016/01/26/should-people-who-discover-a-software-vulnerability-make-the-information-public/

1/26/2016

Despite the best efforts of software developers, we continue to discover mistakes in IT products. Often these mistakes are security vulnerabilities that, unfortunately, attackers can exploit to steal information or to disrupt operations. What should we do when these mistakes are found?

Ideally, we could keep these mistakes secret until they are corrected and all the users have installed the corrections. The window of opportunity for attackers would be closed before they knew the window was even open. Wouldn't it be great to tell the "good" people so that they can correct the problem but not tell the "bad" people so they can't use them for nefarious purposes?

That would be ideal, but ideal isn't possible in this scenario. While it may sound easy, it is far from it for four main reasons. First, the separation between "good" and "bad" isn't black and white; there are many shades of gray. Differentiation between who should and who shouldn't know about a vulnerability depends on context, perspective, timing, etc. Second, even if clear delineation could be made about who to tell, once information is out to anyone, it is difficult to keep secret. Third, it can take considerable time to deploy countermeasures and to diffuse corrections to all affected systems. Attackers won't wait. Finally, some attackers may have already discovered the vulnerability independently and know that the window is open.

As a result, there is an inherent tension in disclosure. When a security problem is discovered in software, what should the discoverer do?

One option is that the discoverer could publicly tell everyone about the vulnerability as quickly as possible. This is termed full or immediate disclosure. The benefit of this approach is that that security professionals and end users know that they need to implement countermeasures and corrections. However, the unfortunate side effect is that potential attackers also learn about the vulnerability (if they didn't already discover it on their own) and can then use the information to attack the affected systems.

Alternatively, the discoverer could tell the software vendor and/or security vendors discretely before widely telling everyone else. This is termed limited or coordinated disclosure. The hope is that corrections and countermeasures get a head start before potential attackers are alerted to the weakness. But without public pressure, this approach may mask the urgency to resolve weaknesses.

Our recent research studies exactly this tension. We use a log of 2.4 billion information security alerts from intrusion detection systems installed at 960 firms to quantify the effects of each disclosure method. We find that full disclosure accelerates the diffusion of attacks and increases the risk and penetration of attacks based on the vulnerability. The aggregate number of attacks is about the same for both disclosure methods; however, attack activity starts sooner when fully disclosed but also ends sooner.

Despite the evidence of accelerated attacks, the result does not necessarily support a conclusion that limited disclosure is preferable. The sooner end of attacks is insightful. Attackers abandon attacks when they are no longer effective and move on to exploit other vulnerabilities. The finding that attackers abandon earlier indicates that full disclosure accelerates the deployment of countermeasures as well. The countermeasures reduce the effectiveness of the attacks, helping bring an end to attacks.

A realistic interpretation of our findings is not that limited disclosure is the best path but instead that our research quantifies the tradeoff in full disclosure, informing security researchers and professionals. Knowing the results of full

disclosure should allow security professionals and users to plan for and manage the inevitable security vulnerabilities as they are found. Additionally, increased emphasis on the Internet of Things will exacerbate these issues.

Beyond our specific security context, the question of disclosure comes up in many other areas. Should a scientist who discovers a way to create a deadly disease or engineer a new weapon publish the results? Should people who realize weaknesses in airport security keep it to themselves? One important consideration in grappling with these questions is the differential effect across society. Weaker, poorer, or less sophisticated parts of the population may bear more of the brunt of these decisions than other parts of the population. Furthermore, timing of disclosure is also an important consideration; at times when people involved in protection are already overburdened, the beneficial defensive effects of disclosure may be diminished relative to the potential detrimental effects on the attackers.

♣♣♣

Notes:

- *This article is based on the authors' paper Information Disclosure and the Diffusion of Information Security Attacks, Information Systems Research journal, Volume 26, Issue 3, September 2015.*
- *This post gives the views of its authors, not the position of LSE Business Review or the London School of Economics.*
- *Featured image credit:* A modern hacker Davide Restivo CC-BY-SA-2.0

Sam Ransbotham is an associate professor of information systems at the Carroll School of Management at Boston College and the MIT Sloan Management Review Guest Editor for the Data and Analytics Big Idea Initiative. He can be reached at sam.ransbotham@bc.edu and on Twitter at @ransbotham.

Sabyasachi Mitra is a full professor of information technology management and the senior associate dean of programs at the Scheller College of Business at the Georgia Institute of Technology. He can be reached at sabyasachi.mitra@scheller.gatech.edu.