Abstract:

Upgraded software and embedded improvements: Tracking vulnerabilities and bugs on the web
Raviv Murciano-Goroff, Ran Zhuo, and Shane Greenstein

We empirically investigate user propensity to upgrade and patch existing software using the methods developed by Murciano-Goroff, Zhuo, and Greenstein (2021). We document five million months of web server usage at over 150,000 US medium and large firms between 2000 and 2018. We focus on quasi-natural experiments after the appearance of a severe security bug. We find enormous variance in the firm-specific attentiveness to patch software in response to a security vulnerability. A reverse causality occurs due to a correlation between the (low) propensity to upgrade and a (high) prevalence of software containing known security vulnerabilities. We develop hazard model approaches that account for firm-specific proclivities to upgrade and fit a subset of data with a range of explanatory variables. We find a significant propensity to upgrade because a new version has appeared, suggesting many users gain protection against vulnerabilities as a byproduct of routine administrative processes that support maintaining frontier software. Users accelerate upgrading when their webserver supports electronic commerce instead of merely an informational or coordinating role. We also find deceleration when users support an incredibly complex IT operation. These findings are consistent with models of high costs of disrupting operations. In addition, they have counter-intuitive implications for the timing of announcements about vulnerabilities and the release of patches.