Position Paper on Standards and Guidelines to Enhance Software Supply Chain Security

Title: sustainable improvement in software supply chain security must be based on changing market incentives

Authors:
Gregory Rattray (Columbia University Senior Fellow, former CISO JPMorgan, former Director for Cybersecurity National Security Council White House)
Ciaran Martin (Oxford University Professor, NATO Senior Cybersecurity Champion, former CEO UK National Cybersecurity Centre)
Joe Hubback (ISTARI Global Academy MD, former Partner McKinsey & Company, independent researcher)

Position statement areas covered: areas 2-5, but with a special focus on area 2 (standards)

Our position: the cyber security market is broken for supply chain security. In the words of one major CISO we surveyed, at the moment "we buy it, cross our fingers and hope it works". Software supply chain security can be sustainably improved only by changing incentives for buyers and sellers. Our principles, known as "SAFER", set out a framework for delivering this

Why are market incentives the focus of our Position Paper?

In 2020, in a landmark study[i], based on 100+ deep interviews with cybersecurity practitioners, enterprise leaders, technology vendors, assessment organizations, government agencies, regulators and industry associations from across all sectors and geographies, it was revealed that 90% of participants believed cybersecurity in the supply chain is failing because the technology isn't as effective as it needs to be. While issues around lack of talent and poor enterprise processes are already well accepted reasons for failings in cybersecurity, this study also highlighted that the technology is letting us down too, but that better technology is actually achievable if the market incentives are right. The study was very well received, giving us confidence in its findings[ii]. We believe that NIST needs to adopt the learnings from the study to improve cybersecurity throughout the software supply chain.

Better security technology has better efficacy; efficacy of cybersecurity software is defined based on four characteristics, these are the Capability to deliver the security mission (fit-for-purpose), Practicality in operations (fit-for-use), Quality of security build and architecture, and Provenance of the vendor and supply chain.

The root of the efficacy problem is primarily economic rather than technical, characterized by a breakdown in the market relationship between buyers and vendors ('buyers' includes CISOs and the broader enterprise team, not only procurement). The core breakdown is an information asymmetry between the parties that prevents buyers from effectively evaluating technology and incentivizes vendors to bring sub-optimal solutions to the market. This mis-match results in products coming to market that are not as effective as promised and which reduce trust in cybersecurity technology and the efficacy of supply chain security. Broken markets have been studied, and solved, before, as evidenced by Akerlof's 1970 paper 'Market for Lemons: quality, uncertainty and the market mechanism'. The 2020 research builds on Akerlof's work and provides the evidence for the breakdown in the market by looking at the overall system dynamics, stakeholder perspectives, buying practices, technology, and vendor landscape.

As one Chief Information Security Officer (CISO) put it, "we buy it, and then we cross our fingers and hope the technology will work".

Solving the economic problem requires a new model, creating new incentives for vendors and new approaches for customers. Around 2/3 of the research participants proposed independent and transparent efficacy assessment of technology as the way to solve the information asymmetry, and to rebuild customer trust.

Independent and transparent efficacy assessment would give customers better information to make risk-based purchasing decisions and would give vendors stronger incentives to deliver technology with greater efficacy.

Over time, improved technology would clearly reduce the likelihood of successful attacks and would have the additional benefit of reducing dependency on people and process (so potentially also reducing the talent gap in cybersecurity). From a vendor perspective, efficacy transparency could help innovation penetrate the market, reducing the need to spend excessively on marketing and sales to gain traction.

For efficacy assessment to keep up with and support technology innovation, market standards should be set for assessment rather than technology. Assessment, rather than technology, standards already exist in some markets and in parts of security today (eg, GSMA NESAS), however, they are not widely understood or used.

As the largest technology buyer on Earth, the US Government is perfectly positioned to create the required vendor incentives in the software and cybersecurity markets. This will not only benefit the Government's cyber-resilience but will have a massive knock-on effect in the rest of the enterprise software and security markets, creating cyber-resilience for the whole Nation.

What are the SAFER principles?

They are the 5 basic requirements to fix the market issues highlighted previously. We have tested these principles with practitioners in the field and they are gaining strong support. The principles are:

S: symmetry of information between buyer and vendor, addressing the fundamental imbalance at the root of the problem;

A: assessment independence and approach which makes it easier for vendors with effective solutions to navigate markets successfully and for buyers to access independent assurance;

F: freedom of entry and innovation in the market, maintaining, as far as possible, low barriers to new entrants with demonstrably effective solutions;

E: efficacy-based assurance, ensuring that assessors look at the total efficacy of a solution when assuring or reviewing cybersecurity / software solutions;

R: risk-based buying decisions, providing buyers with solution efficacy information to drive a value-based buying decision, trading off likely risk reduction with cost.

How do we propose NIST uses these principles to support the interest areas?

We believe that NIST should use these principles to guide the solutions in areas of interest 2-5, but with a special focus on area 2 (around standards). Per area the SAFER principles can be used:

2: to input into setting the required standards for vendors to serve the secure software market

3: to drive improved risk information supporting selection of security measures for critical software

4: to input into the definition of the minimum requirements for software testing

5: to define the method of assessing requirements for integrity and provenance

We are volunteering to support NIST in using the SAFER principles to implement of the Executive Order.

---

[i] https://www.debatesecurity.com/cybersecurity-technology-efficacy-is-cybersecurity-the-new-market-for-lemons/

[ii] https://www.wsj.com/articles/security-experts-alarmed-by-broken-cyber-market-11603359014, https://www.forbes.com/sites/johndunn/2020/10/22/is-the-cybersecurity-industry-selling-companies-lemons-apparently-lots-of-important-cisos-think-it-is/?ss=cybersecurity&sh=5eda01ef74dc