@stake℠

Security Briefing

JULY 2003

The Security of Applications, Reloaded

Kevin Soo Hoo
ksoohoo@atstake.com

Andrew Jaquith
ajaquith@atstake.com

Dan Geer
geer@atstake.com

The authors lead @stake's Risk Analytics Center of Excellence, which helps clients quantify the risks and returns of security investment. The Center seeks to define and to promote better information security risk management through the use of measurement and quantitative analysis. The Hoover Project, launched in 2001, is @stake's response to the national call for greater sharing and analysis of information security data.

In early 2002, @stake published a comprehensive study of the state of application security — and found it wanting. As of 2003, applications *are* more secure, but progress appears to be uneven. In this follow-up research brief, we discuss the widening security gap between the best and worst performers.

Fifteen months ago, @stake published the results of its first formal application security study.[1] That effort, part of @stake's Hoover Project, analyzed forty-five e-business applications, profiling the state of security as practiced in 2000 and 2001. We focused on application security because of the growing weight of application vulnerabilities in enterprise security risk profiles. Indeed, that trend has solidified in the past year with incidents such as SQL Slammer demonstrating the importance of application-focused security threats.

In this briefing, we expand upon our original study by looking at security trends over time. As with the previous study, the data is drawn from @stake application security consulting engagements, with the difference being that our time horizon is now extended to 2003. @stake consultants generated all of the observations, using the firm's standardized application assessment methodology. Because the data is derived solely from @stake client engagements, they are consistent but not necessarily representative of any particular population, industry, or group — they may be confirmable, but they are not generalizable. Although we classify some of our results by industry, the data should best be regarded at this time as descriptive rather than statistically significant.

For this update, we analyzed security vulnerability findings from seventy e-business applications across a variety of industries from 2000 to 2003. The data is concentrated most heavily in the financial services and software sectors, which suggest that these two industries are leaders in (or at least early adopters of)

---

[1] See Soo Hoo, Sudbury, Jaquith, "Tangible ROI Through Secure Software Engineering" *Secure Business Quarterly*, Vol. 1, No. 2, Fall 2001, http://www.sbq.com/sbq/rosi/sbq_rosi_software_engineering.pdf.
Also see Andrew Jaquith, *The Security of Applications: Not All Are Created Equal*, Research Report, (Boston, MA: @stake, Inc., February 2002) http://www.atstake.com/research/reports/acrobat/atstake_app_unequal.pdf.

application security. We tracked the number of vulnerabilities per application to generate a rough estimate of software security quality over the last three years.

Financial Services and Software Industries

Generally, application security appears to be improving in the software and financial services industries from 2000 to 2003. *Exhibit A* plots the number of security defects found per application for forty-five (45) applications assessed over twelve quarters from 2000 to 2003. A quartile analysis (see *Exhibit B*) reveals that improvement is evident across the board. However, viewed in the context of relative improvement, the quartile analysis also demonstrates an unevenness in security improvement. A significant gap appears to be opening up between the top and bottom quartiles. The gap is most pronounced between the first and fourth quartiles. In 2003, the average number of defects found in a fourth quartile application was 5.7 times that found in a first quartile application (see *Exhibit C*), representing a gap nearly twice as wide as existed in 2000.

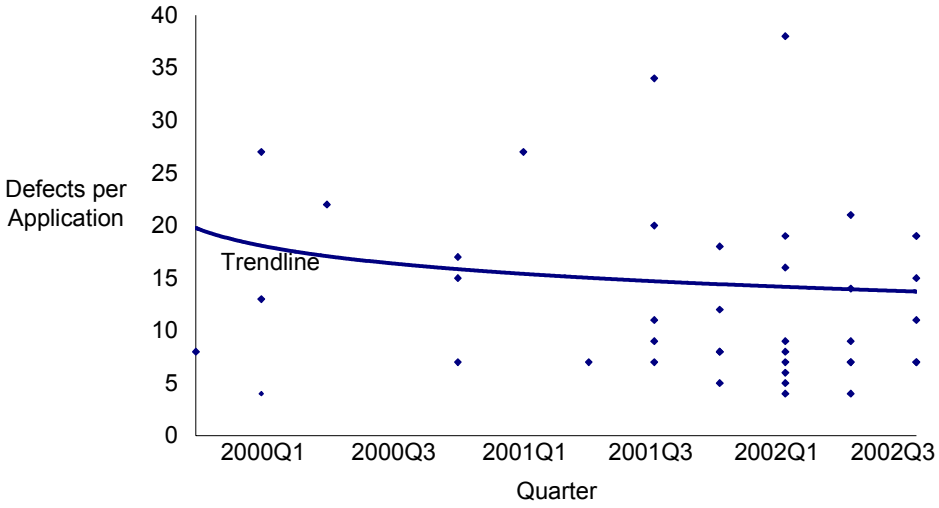


Exhibit A: Application Security Trend in Financial Services & Software Industries

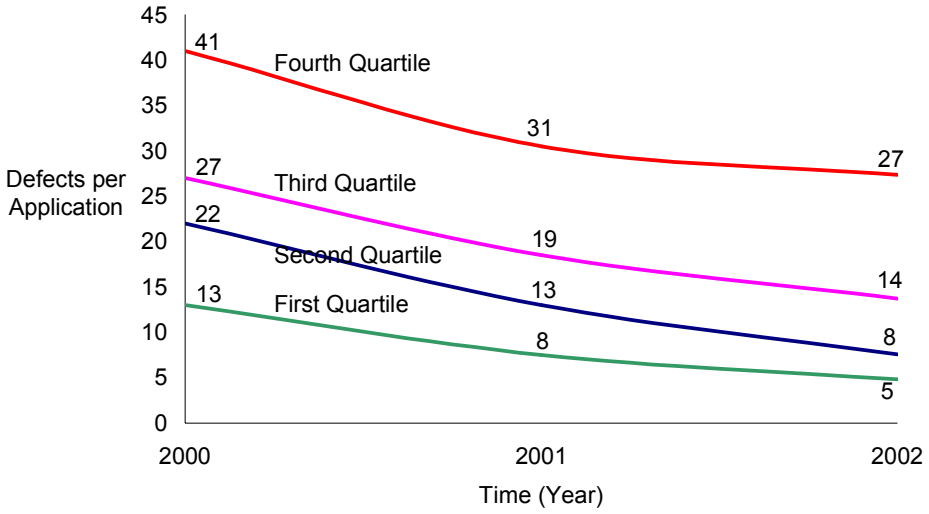
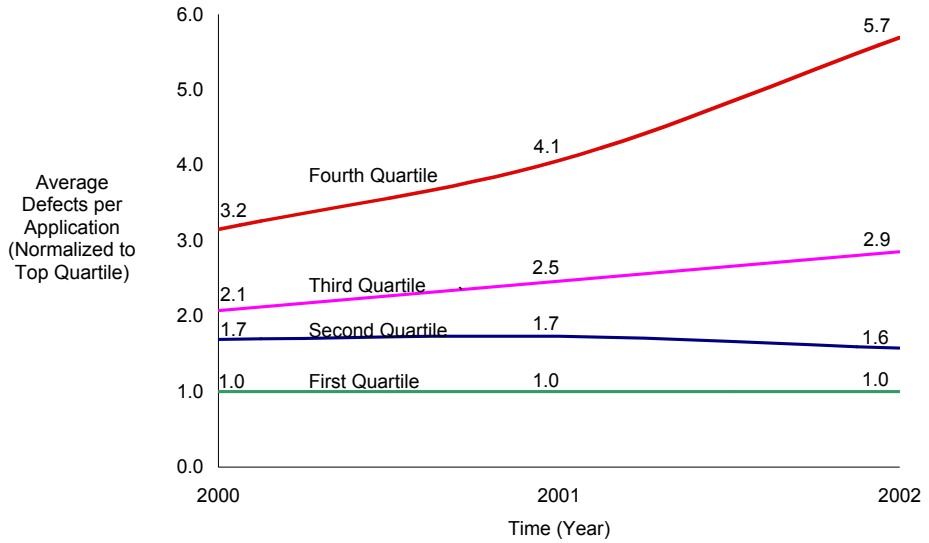


Exhibit B: Application Security Quartiles in Financial Services & Software Industries

For first-quartile firms, this finding strongly implies that counterparty risks are of growing importance. The recent events surrounding MasterCard (not in this study) illustrate this point.[2] In that case, attackers were able to take advantage of a trusted (but much less secure) counterparty to steal millions of credit card numbers. Leading financial services firms in the top quartile are well advised to encourage, or compel, their bottom-quartile business partners to improve their security postures.

Exhibit C: Widening Gap in Financial Services & Software Industries



[2]Fred Katayama, "Hacker Accesses 5.6 Million Credit Cards", *CNNfn*, February 18, 2003, http://www.cnn.com/2003/TECH/02/17/creditcard.hack/.

Other Industries

Data from companies outside of financial services and software (twenty-five applications) present a snap-shot of early-adopter application security quality in the computer, electronics, healthcare, Internet infrastructure, manufacturing, media, utility, and other sectors. The sparse data prevents us from drawing firm conclusions, but we expect that, as first-movers, these companies would have application security comparable to that of early adopters in the financial services and software industries in early 2000 (see *Exhibit D*). The wide dispersion of defects per application in any given quarter appears to support this hypothesis. Since our data set is drawn from companies who proactively seek out professional security advice, we would also expect the data to show better-than-average application security for these firms.

Interpretation

The financial services and software industries continue to lead the way in application security, both in breadth of adoption and in depth of security improvement. The limited representation of other industries in the study is most readily attributable to the present early stage of adoption of application security in non-software and non-financial sectors. The clearest trend in the data suggests that the gap between best- and worst-in-class is widening in financial services and software. The elite are getting better, faster, than the stragglers in application security.

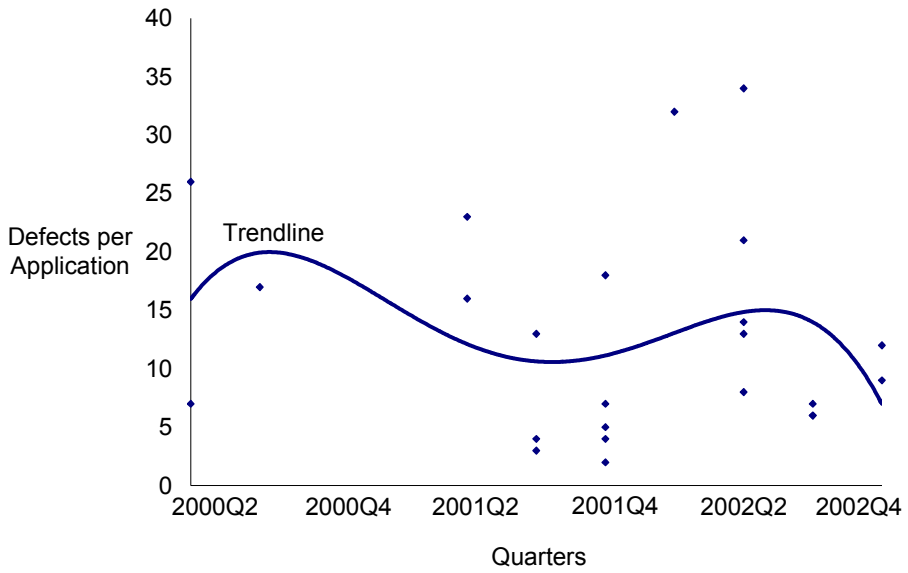


Exhibit D: Application Security Trend in Other Industries

This stratification could have budgetary implications for both leaders and followers. For the leaders, a careful examination of the costs of application security may be warranted if leadership status is purchased at an extraordinary price. Similarly, for the followers, liability concerns may compel them to make the necessary investments to improve their application security. The ambiguity of "industry best practice" and "due

care" is probably sufficient to motivate a move closer to the industry average. And, to repeat, leading firms that are also highly connected are exposed to higher levels of counterparty risk.

A Little More Pooled Data

"Gather a shell from the strewn beach
And listen at its lips."

Dante Gabriel Rossetti, The Sea-Limits.

While the last fifteen months have helped establish application security as the most important emerging information security issue of the day, for many industries it remains a nascent field of endeavor. As with the previous Hoover study, we caution against interpreting our results as statistically representative of any group other than @stake's clients.

Going forward, the trend lines are perhaps the most valuable information we can provide, but to paraphrase Rossetti, we found a seashell, picked it up, and shared what we heard.

About @stake, Inc.

@stake, the premier digital consulting firm, provides security services and award-winning products to assess and manage risk in complex enterprise environments. The company's SmartRisk services cover key aspects of security, including applications, critical infrastructure, wireless and wired networks, storage systems, education, and incident readiness. @stake consultants combine technical expertise with a business focus to create comprehensive security solutions for industry leading companies in financial services, information technology, energy & utilities, healthcare, and telecommunications. As the first company to develop an empirical model that measures Return On Security Investment (ROSI), @stake keeps security investments in line with business requirements. Headquartered in Cambridge, MA, @stake has offices in London, New York, Raleigh, San Francisco, and Seattle. For more information, go to www.atstake.com.