www.softwaresecured.com

Proving Adherence to Application Security Best Practices

SoftwareSecured

Develop your software with intelligent security

SoftwareSecured

Software security best practices White Paper

Industry standards and the best practices for developing secure software

Enterprises have become more security conscious when investing in software products, which has put growing pressure on developers to prove that their software is secure. Everybody says they develop secure software, until they get hacked. Now, companies are asking developers to prove that their products are secure, but with no standards across all sectors, proving adherence to best practices remains a challenge. Regardless, customers are demanding improved software products from vendors.

Technology and software applications are changing, but frameworks for developing software continue to lag behind with only the financial industry's Payment Card Industry Data Security Standard (PCI DSS) having a set of requirements with which all developers must be in compliance. The Health Insurance Portability and Accountability Act (HIPPA) was established in 1996, but being in compliance with these regulations provides more flexibility for developers than does PCI. HIPPA doesn't force any developers to do anything, making it easy to work around compliance.

Outside of the financial and health care sectors, there are no mandates by which anyone can actually measure adherence to best practices. Given the lack of standards across sectors of the industry, proving adherence to best practices is subjective at best. While there are certification standards out there, none set forth the security best practices mandated by PCI, not even HIPPA. The market, then, must be self-regulating and governed by the developers in the industry.

Where we are and where we are going

This year's SANS Sate of Application Security Survey, found, "Application security (AppSec) is maturing for most organizations, according to the 475 respondents." This trend in application security continues to narrow the gap between developers and protectors of applications despite the absence of regulations across sectors. There is an increase in both awareness of and concern for application security. Given the growing number of breaches

The 2016 State of Application Security: Skills, Configurations and Components said that despite obstacles from skills to funding and internal communication for many organizations, "The majority [of survey respondents] say their programs are maturing or mature: %38 say their AppSec programs are 'Maturing,' while %22 say their programs are 'Mature'."

In addition, %4 of the survey respondents reported programs that are 'Very Mature', and "The majority (%67) have also partially integrated AppSec into their overall security, risk management and incident response (IR) programs, while another %17 have achieved full integration."

The overall results of the SANS survey, "Reveal that it is critical for an overall enterprise security program to coordinate efforts among developers, architects and system administrators—particularly since many software vulnerabilities are rooted in configuration issues or third-party components, not just in code written by the development team."

According to Jeff Pollard, principal analyst, Forrester Research, "The main challenge in the application development world is one of diversity. Application security could mean Web Application which has the OWASP Top 10 as one set of standards."

Pollard said that web application security is only one type of application development. "Other types of application development could have security guidance based on programming language. For example, CERT and Carnegie Mellon host various secure coding standards by language and platform." Still best practices and who establishes and certifies the adherence to those frameworks remains somewhat ambiguous because the software security problem is only a few years old.

Pollard said that web application security is only one type of application development. "Other types of application development could have security guidance based on programming language. For example, CERT and Carnegie Mellon

host various secure coding standards by language and platform." Still best practices and who establishes and certifies the adherence to those frameworks remains somewhat ambiguous because the software security problem is only a few years old.

A decade ago, no one talked about software security. The focus of the industry was entirely on securing the network. Many still believe that if they secure the network or the perimeter that their security will protect the software as well.

In order for developers to prove their adherence to application security best practices, there must be a greater shift in thinking across the industry. While many organizations are starting to realize that network and perimeter security doesn't protect the software, there is still a lack of awareness of the impact that software attacks can have.

Defining best practices together

A common obstacle in developing secure software has been market pressure. The need to rush a product to market has often trumped the demand for more secure software. Now, though, customers are feeling the impact of this lack of security. Increasingly, customers are demanding that developers prove their adherence to application security best practices, and they are budgeting for continued testing of products.

Sherif Koussa, CEO, Software Secured, said, "The common practice right now is getting a third party assessment. They do a pen test or code review to assess the code. By no means is this ideal because there is no common standard and no common measurement of a standard."

The subjectivity of an adherence score needs to be considered as one third party assessment could score a product at 7 of 10 on the OWASP top 10, but a different assessment might say it's only 5 of 10. "It's all arbitrary," said Koussa. "There is no common way, no common standard which is why companies are wanting to know how they can prove adherence."

The subjectivity of an adherence score needs to be considered as one third party assessment could score a product at 7 of 10 on the OWASP top 10, but a different assessment might say it's only 5 of 10. "It's all arbitrary," said Koussa. "There is no common way, no common standard which is why companies are wanting to know how they can prove adherence."

Even the existing regulations don't translate to a secure product. PCI, which was established back in the late 1990's and has been a driver behind software security has become a mere box on a checklist for developers who don't really care about confidentiality.

Koussa said, "OWASP also has the Application Security Verification Standard Project, which are standards that—although they are not perfect—could be used in the context of guidance or metrics. Although, it is one of the best candidates to fill this gap, few industries (if any) use it as compared to PCI."

When customers ask that developers prove adherence to best practices, they want confirmation that security is a top priority. By customers continuing to demand application security, they will drive a change in culture to the industry. "Software security is more of a culture than a process. The industry needs to focus on agile software development using DevOps methodologies more so than a tool. It's a culture. Everybody in the industry has to get together and improve collectively the state of their application security," Koussa said.

Somebody needs to take the initiative in moving toward this cultural shift, recognizing that within each sector there will be different measures used to evaluate the security of software applications.

255 Centrum Blvd. Ottawa,
Ontario K1E 3W3 Canada

Phone : +1 (800) 611 5741
Fax: +1 (800) 611 5741

info@softwaresecured.com
www.softwaresecured.com