OWASP AppSec DC 2009 Conference

Jeff Williams, OWASP Board Chair

The OWASP Mission

First I'd like to introduce the OWASP Board (Tom, Dave, Dinis, Seba, and myself)

The board runs the OWASP Foundation, the 501c3 nonprofit which provides support for all the activities that happen at OWASP. Like all the people involved in OWASP, we volunteer our time to make the project a success. I'd like to take this opportunity to thank each of you for all the hard work you do to make OWASP a success.

I'd also like to thank Joe for the thoughtful keynote and for focusing on the entire software supply chain. His focus on malicious intent is right on and I'll be talking about that extensively tomorrow.

If you combine all the materials available through his program and what's available at OWASP, we've got ALL the right stuff out there. But we are still losing ground.

For years, we have watched as the software market fails to produce secure applications.

Increasingly, this situation is worsening and there are two key factors. First, the reliance that we put on our software infrastructure increases every day. Application software controls our finances, healthcare information, legal records, and even our military defenses. Secondly, application software is growing and interconnecting at an unprecedented rate. The sheer size and complexity of our software infrastructure are staggering and present novel security challenges every day.

While we have made some progress in security over the last decade, our efforts have been almost completely eclipsed by these factors. The software market and security experts still struggle to eliminate even simple well-understood problems. Take cross-site scripting (XSS) for example. In the last decade, XSS has grown from a curiousity to a problem to an epidemic. Today, XSS has surpassed the buffer overflow as the most prevalent security vulnerability of all time. It's the same for SQL injection. And CSRF will follow the same pattern too.

These problems, while technically simple, have proven extraordinarily difficult to eradicate. We can no longer afford to tolerate software that contains this kind of easily discovered and exploited vulnerabilities. Read about the RBS WorldPay attack from this week – the level of coordination and sophistication required to pull off this attack are stunning.

In addition to risks like this, we are already seriously limiting innovation in the development of applications that can improve the world.

Why doesn't the software market produce secure software?

It's possible that the risks we focus on are overblown and that the market is actually working to produce an optimal level of security in our applications. But the other possibility is that the software market is broken. Despite what you might hear in economics class, markets are not perfect. They have failures like monopolies, price-fixing, and speculative bubbles.

One classic market problem was detailed in a Nobel Prize winning paper by George Akerlof called “The Market for Lemons.” Basically he showed that when sellers have more information than buyers – like when you’re selling your used car that barely runs – buyers will discount the price they’re willing to pay. That means people with good cars can’t get a fair price and so they won’t sell. And that means you can only buy lemons in the used car market.

Now think about that for software. Buyers really can’t tell the difference between secure software and insecure software. So they’re not willing to pay more for security.

We need radical innovative ideas to fix the software market. We are not going to “hack our way secure” – it’s going to take a culture change.

The automobile industry made the change over at 30 year period after Ralph Nader exposed the industry….and today we have cars that have safety features. The food industry made the change but only after the FDA started the Nutrition Facts program. Even the cigarette industry has been dramatically changed through campaigns like the “Truth…” campaign.

The OWASP mission is to make application security visible. Creating transparency goes directly to the heart of what is wrong with the software market and has the potential to actually change the game.

Why is OWASP the right approach?

OWASP is a worldwide free and open community focused on improving the security of application software. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license.

In many ways, we're like public radio. This allows us to reach a very broad audience and it makes it possible for us to avoid difficult commercial relationships that influence our activities. This freedom from commercial pressures allows us to provide unbiased, practical, cost-effective information about application security.

I believe this objectivity is absolutely critical. For too long, much of the appsec information in the market has come from people selling stuff, and our message has been lost.

What is OWASP doing?

Yesterday, OWASP Leaders from around the world got together to discuss our progress and set our priorities for 2010. Each of our Global Committees reviewed their accomplishments and we discussed the agenda for the future. We just established these committees last year and they are already making huge progress establishing the foundation we need to achieve our mission.

Before I ask Tom to review our 2010 agenda, I'd like to encourage all of you to figure out something you can do to change the culture in your team, company, or industry. In this room are some of the greatest minds in application security. I challenge you to focus your efforts on those things that will actually change the world and allow us to fulfill the potential of what we can achieve with software.