

Interview with Ivan Arce

Ivan Arce is a co-founder and Chief Technology Officer of Core Security Technologies where he helps to set the technical direction for the company. Arce writes for numerous technical publications, speaks frequently at industry events and is commonly quoted in industry publications. He is a member of the IEEE Computer Society and the Association for Computer Machinery (ACM) he also currently serves as Associate Editor of the IEEE Security & Privacy Magazine.

Prior to co-founding Core in 1996, Arce most recently served as vice president of research and development at VirtualFon, a computer telephony-integration company where he was responsible for the development, testing and deployment of mission-critical computer

telephony applications. Previously, Arce spent 8 years as an information security consultant and software developer for banks, government agencies and financial and telecommunications corporations.

As a user of their Core IMPACT offering, I thought it would be enlightening (shamefully using PenTest Magazine self-servingly as a personal crowbar) to fire a few questions at this very interesting person. He graciously accepted, regardless of the crowbar.

A pioneer of sorts in this space affords the man very unique insights into the industry from the business perspective, as well as the perspective of seeing firsthand the evolution of the threat landscape and how the enterprise could stand to holistically approach it. The IMPACT suite tied in with INSIGHT appear to be able to do just that.

The humble approach of *being a smart guy who admittedly surrounds himself with smarter people* has created a successful process, and for the professional level penetration tester, I feel that you can't go wrong with what Ivan and his group brings to the table.

First some background on how the business came together.

Jay: What came first for you, entrepreneur, or security enthusiast – and did you have a singular moment where you realized you could combine the two?

Ivan: I've been a *technologist* since I was 12 and became a security enthusiast not many years afterwards. I became an *entrepreneur* when I was 19 while attending the year-long pre-college course in Argentina when I founded a company to develop turn-key applications for SMBs with a friend I met at the course.

Disregarding of what came first I've always been more interested in technology generally and in the particular technical aspects of security than in the business and entrepreneurial side of things. Over the years I found out that my interest in both technology and business is

actually secondary to my interest in working with great people. I like working with nice and honest people more than anything else.

There wasn't a singular moment of realization or any such thing, we (me and the other co-founders of Core) simply thought that we liked doing security stuff together and that it would be great if we could actually make a living doing that. That's how Core came about.

Jay: How did you first find the level of competent exploit and UI coders to stock your headcount with?

Ivan: Mostly friends and through our social network (friend of friends, etc).

Jay: Do you contribute code at all these days, or does your involvement take place on a completely different level?

Ivan: No, I do not code at all these days. I haven't done so for years which sometimes I regret. My involvement is similar to that of a retired professional sports player that has moved to a teams general coach role. I could still play a bit but I'd do it very poorly compared to the current players. Also, the game has changed a lot in the past decade and I'd not fare very well as a player today. However, some things did not change much and I think that the contribution more valuable that I can make in my current role is to share the *heuristics* I've acquired over time. Thus, I mostly point at a general strategy and some specific tactics to solve interesting problems or address market needs but people more capable than me actually do the great things that Core comes out with.

Jay: Releasing INSIGHT has allowed enterprise managers to see things for themselves, at their levels of the org chart. Was INSIGHT the result of management teams asking for a less technical interface, or the result of end technicians asking for something gentle for their management?

Ivan: Yes, and none of the above too. INSIGHT is the next natural step from IMPACT. Once penetration testing has been tasted and adopted, scaling up that practice to perform continuous multi-vector testing systematically throughout an organization and using the results to provide meaningful information to support decision-makers is just an evolutionary step from IMPACT, which in turn was the natural evolutionary step needed to improve the low frequency and relatively expensive practice of manual pentesting.

It is not a matter of too technical interfaces or product complexity but rather a need to bring visibility to

information security risk in a way that can be aligned with the business views of an organization.

If that doesn't happen with a certain degree of success the faith of the security posture of an organization (and its security staff) is bleak.

Executives need to understand how security investments fit with the overall business plan of their organizations, if they don't then security is relegated to a tactical matter that is just perceived as a cash drain to appease the paranoids or to put out the fire when half the building is in cinders.

INSIGHT is our attempt at providing that visibility proactively without compromising on the relevance and quality of the data that we generate and aggregate.

Manual pentesting, target based IMPACT-driven and continuous goal-driven security testing using INSIGHT complement each other quite nicely and could provide an entirely new level of quality to the security information needed to make risky business decisions with more confidence.

Jay: Have you sensed a push to move to smaller mobile devices (tablets, netbooks, dare I say an extremely light app for smartphones...) as a launch platform, in a sort of more covertly aggressive posture?

Ivan: As far as I can tell, the market is not really pushing to use mobile devices as launch platform but it is certainly pushing for the ability to actively assess the security of mobile devices that interact with the rest of an organizations network in an uncontrolled manner. The threat landscape points at an obvious short term issue: *mobile devices are* *already targets but soon they will also be pivoting points for* *multistage attacks that go deeper into the target organization*.

In that context, the view of a mobile device as the root node of an attack tree isn't that interesting. To think of it as an intermediate node in one or many paths in an attack graph is more comprehensive. That is why we incorporated mobile device testing to our IMPACT product, so it complements and combines with the other attack vectors.

Jay: Have open source suites influenced you at all regarding UI or framework?

Ivan: Depends. If you are referring to Metasploit the answer is no. It may even be the other way around.

We thought about, developed and released IMPACT long before Metasploit even existed. In fact HD Moore was a beta tester of IMPACT v1.0 in 2002 while he was working for a security consultancy.

So I'd posit that it was the other way around, IMPACT influenced open source pentesting frameworks and

other commercial offerings. For example, in 2002 we demoed IMPACT v1.0 to AtStake's New York office, among the attendees was Dave Aitel who would later found ImmunitySec and develop commercial penetration testing software quite similar to IMPACT v1.0 (also Python-based). So, I wouldn't say that IMPACT inspired the authors of both Metasploit and CANVAS but it is undeniable that it played a role in the process that led to their creation.

On the other hand, open source did influence our choice of a programming language for the IMPACT framework.

We did not want to create yet another ad-hoc proprietary scripting language for our exploits and other modules like other vulnerability management products used to do in the 90s (NASL, FASL, CASL, N-code are just a few examples). We wanted to provide our users with a highly expressive non-proprietary programming language that already had a thriving community supporting it and that did not have a steep learning curve. We evaluated Smalltalk, Python and Perl as candidates and ended up with Python. (BTW, HD Moore was critic of our choice of Python and suggested Perl in his beta-tester's feedback. He wrote Metasploit in Perl only to -unsurprisingly to us- completely rewrite it in Ruby years later).

Jay: Would you like to make a statement about the state of the assessment or infosec industry and how you plan to continue to dominate the commercial space through industry changes?

Ivan: The industry has had a very simplistic and shallow view of the security assessment process for too long, the threat landscape has evolved way past the incumbent industrys perspective. Targeted, multi-vector, multi-staged attacks have always existed (only they call them APT now) but their effects are more visible and dramatic these days.

Current vendor solutions aren't entirely fit to cope with them. If you look at vuln scanning, you'll find that in two decades none of the scanners evolved to conceptualize vulnerabilities and attacks with a level of depth greater than 1. They provide a very flat view of the systems running in an organization. Unless of course, you feed them with legitimate administrative credentials to all systems in which case you end up with a very expensive distributed file checker.

On the other hand, penetration testing provides an in-depth view of an organizations security posture but with a very narrow scope due to its cost. You can't run manual penetration tests against your organization every month or every week unless you are willing

and able to spend lots of cash. To reduce the cost you will need to streamline the process and automate big portions of the practice, that is where software tools come handy. They do not replace the experts but they make things easier for them and help them scale out their practice and share their expertise.

The result of a penetration test is a single data point about your actual security posture against an immense backdrop of uncertainty, we clearly need many more data points but that can only happen if we make penetration testing more efficient and cost effective.

Usually neither vuln scanning nor penetration testing actually provide actionable information in a way that is meaningful to `_business decision makers_`. Thus, at the executive level the situational awareness of an organizations security posture and the idea of what's a commensurate investment in security is created by reactive and purely defensive industry solutions which tend to fail horribly because they entirely miss, underestimate or overly simplify the offensive side of the equation.

We want to change that by providing safe and comprehensive testing and measurement technology that takes into consideration the attackers viewpoint and lets organizations generate lots of data points so they can have a more crisp, accurate and up to date view of their security posture. That's a first step towards a predictive model where business decisions can be made with better understanding about the implied risk.

This may sound too abstract and high-level but its the overall idea.

Interviewed by Jay

JAY

A recovering Unix admin and BOFH, Jay has transitioned full-time into the murky world of Infosec, distressed audit consulting and fatherhood.

View his blog at tactical-intelligence.blogspot.com.