

Build Security into Every Product, Coders Advised

Tom Jowitt, Techworld.com

A panel of security experts agreed that security needs to be thought of a lot earlier in the software development lifecycle, and that the IT industry needs to start shipping "hardened" products, especially [with the advent of the cloud](#) and visualisation making the location of sensitive data even more difficult to locate.

Speaking at [Alcatel-Lucent's Dynamic Enterprise forum](#) in Paris last week, a panel of experts including Wyatt Starnes, the founder and CEO of verification provider [SignaCert](#), discussed how there are now thousands of applications out there, and that the [traditional model of securing them](#) via third party or add-on security packages, is now outdated.

Starnes was previously the founder and CEO of Tripwire, and is a [cofounder of RAINS](#) (Regional Alliances for Infrastructure and Network Security). Also speaking on the panel was [Carlos Solari](#), previously a senior executive at the Federal Bureau of Investigation (FBI), as well Chief Information Officer for the Executive Office of the President (the White House). He is now VP of Security Solution and Strategy at Alcatel-Lucent.

"Clearly, the current approaches are not scalable to Web 2.0," said Solari. "With virtualisation, where does your data reside? We need to rethink the problem. After market, or bolt-on security technology is a failed model, as things are increasingly residing in the cloud now. A new approach is needed."

SignaCert's Starnes agreed. "How we buy technology has to change," he said. He drew the analogy of how we purchased cars nowadays, and the fact that in the old days, cars did not ship with seat belts or airbags. "You wouldn't buy a car now, and then go and buy airbags from another vendor, so why do it with software?" he asked. "Security has to be 'baked in'. Software has to come in a hardened form."

The experts rejected arguments that software vendors cannot possibly know the type of threats their software applications will be facing in the future. "We can harden products because we already know most of the threats the software will be facing in the future," said Solari. "It could be a criminal act, botnets, root kits, but all of these issues have existed before, and they have just mutated into a new form."

"We have gone from individual hackers, to a professional body of hackers, with a lot of tools and resources at their disposal," said Starnes. "The security problem is definitely upstream, where the product is made. It is not a user problem, as cars are now made safe thanks to airbags and seat belts built in by the manufacturers themselves. The same will happen in the software industry," he predicted.