

Cybersecurity 2020

What will be the future of software design?

March 2014

How will cybersecurity impact software design in the year 2020? To answer this question, let's consider an example from the past. In 2011, iOS 4.3.3 was running on iPhone devices. Then, if you just opened a malicious PDF file, someone would take complete control of your phone, and potentially spy on you, send messages, or track your location. Today we hope this is no longer the case.

Why just hope? Why do we not have any guarantee on the quality of the software? Software experts will tell you it is because software is complicated. It is intricate to design,

Back in 2011, just open a malicious PDF file and someone would take complete control of your phone.

costly to validate, and it is not getting any better. If we look back at trends over the past 10 years, we will see that this is because the size of software is

increasing exponentially.

At TrustInSoft we believe the time has come to change software validation. TrustInSoft Founders have created tools and methods used for mission-critical systems such as airplanes. Now TrustInSoft

TrustInSoft brings high-quality software methods and tools from mission-critical systems to the IT world.

brings high-quality software methods and tools from mission-critical systems to the IT world.

We provide guarantees on software to make sure it is immune to the most common security flaws.

For instance, TrustInSoft has completely secured an open-source implementation of an SSL/TLS communication stack (the protocol used in HTTPS). We are able to guarantee that if you use the stack in a proper manner, the most common

errors cannot occur. This includes buffer overflow or any other memory error. So what will change from now on? Now you have the technological power to be immune to the common security flaw. You now have the power to make it exceedingly difficult for hackers to penetrate your systems.

Will this suppress anti-virus software? No, because phishing attacks or wrong manipulation such as installing a bad executable program will continue to occur.

So in 2020, anti-virus will per-

Applicative and system level software will be immune to attacks used today by hackers.

form a smart monitoring of behaviors to make sure no "wrong manipulation" will damage your system and both applicative and system level software will be immune to most attacks used today by hackers thanks to TrustInSoft. ■

