



Home Product Guide Recommend Products People Hot Companies Technology Deployments Awards About This Guide



Info Security Products Guide

PUBLISHED BY SILICON VALLEY COMMUNICATIONS

California, United States of America



Eliminating risk through proactive, pre-emptive quality assurance tools

Codonomicon's objective is to ensure the security and robustness of any application or service implementation. Development and security personnel in a lab or staged environment use Codonomicon DEFENSICS to fortify quality and security assurance – quickly, easily and reliably. The test software offers a systematic blackbox and negative test methodology uniquely capable of revealing un-desired behavior and issues in protocol implementations. Codonomicon teams its patent-pending Protocol Modeling Engine and Attack Simulation Engine with the industry's broadest protocol support covering network, wireless, and digital media. Thousands of pre-built, highly targeted and well-documented test cases allow users to start seeing results as soon as the platform is connected to the target system – accelerating time-to-value. Codonomicon was spun out of the successful PROTOS test tools research of the Oulu University Secure Programming Group. Years later, the world-proven Codonomicon DEFENSICS platform remains unmatched in its ability to quickly find quality, resiliency and security flaws within the broadest array of applications. Thousands of developers and security analysts across telecommunications, networking, manufacturing, financial services and defense industries rely on Codonomicon to reduce costly reputation, quality and compliance risks.

Name: Ari Takanen

Position: CTO

Popularly known as: Fuzzing Evangelist, Road Warrior

Company: Codonomicon

Previous positions: Researcher at PROTOS project, University of Oulu, Finland

Education: Eternal project at completing the Master of Engineering (Computer Engineering) at University of Oulu

Presentations: About once per month, at conferences related to security, quality assurance, wireless, VoIP, and software development (RSA, Eurostar, Techno Security, CSI, VON, and many others)

Books: Securing VoIP Networks (Addison-Wesley)



and Fuzzing for Software Security (Artech House)

In the following interview, Ari Takanen, CTO - Codenomicon discusses 1:1 with Rake Narang, Editor-in-chief of Info Security Products Guide, a better way to expose and find problems in applications and services before they are rolled out to users.

Rake Narang, Chief Editor - Info Security Products Guide: *What are the most common security risks consumers face when using products or services that may have flaws and weaknesses? How do your company's testing tools differ from competitive product and service testing methods and tools?*

Ari Takanen, CTO - Codenomicon: In my opinion, all pieces of software have flaws until the software has been tested and flaws are found. In my numerous studies since 1999, first at as part of the PROTOS project at the University of Oulu, and later at Codenomicon labs, my team and I have seen that 80-90 percent of all tested software fails when tested with Codenomicon's tools. The risk is already there, we are just offering the means of eliminating that risk through proactive, pre-emptive quality assurance tools. We can also see the same security threat through the constant updating processes with any off-the-shelf software. If the available robustness testing and fuzzing tools are not used, hackers will always eventually find the same flaws that you could have caught with your own tests. The result of a third party finding those flaws is a race whether you will be attacked before you will have access to an update that will correct the flaw in software.

The major differentiator between Codenomicon's tools and the competitive solutions is test efficiency. We have been developing these model-based robustness testing techniques since 1999, and have had our commercial products available since 2002. This has given us a head start in the testing domain that is revealed through our test efficiency. Our customers have told us that some of our tools find a factor of ten times more flaws than the competitors' products. This is the main goal of fuzzing: to find the flaws. There are other differentiation factors. Our tools are purely software based, and therefore our software is perfect for anyone from a programmer, tester, or a security consultant to use. Our tools run on high-end multiprocessor hardware with multitude of 10G interfaces, but it also runs on small and mobile tablet PC's. We integrate with any test automation framework and work together with the majority of the standard penetration testing toolkits to make our customers' lives easier wherever they need our tools. But those are just features. People do not buy fuzzing tools based on features, but based on the test efficiency.

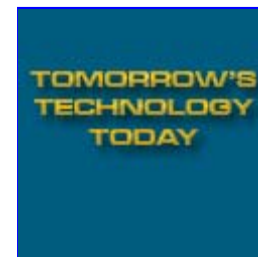
"Products and services already tested to perform their essential functions may still be flawed and a security risk. Codenomicon solutions can test wireless devices, consumer electronics and Web services providing a better way to expose and find problems so that a proactive approach may be taken before such products or services are rolled out."

Rake Narang, Editor-in-chief, Info Security Products Guide

Rake Narang: *How has Codenomicon kept up with the competition and product innovation? What are the latest products and services provided by your company?*

Ari Takanen: Codenomicon looks to our 100+ customers for real customer-driven product enhancements. When our customers start deploying a new communication technology, we support them with timely tests. Today we support about 150 communication interfaces with state-of-the-art tests, which is more than twice as many as our closest competition. There is a constant race for protocol support. If the tool is not ready in time, the customer will look elsewhere.

All tests also need maintenance. Protocols in the IMS domain change constantly. In fact throughout our nearly ten years of experience in VoIP testing (our first VoIP test tool was built in 1998 although it was not ever released) we have seen that protocol development first-hand. Our customers have said that we beat even the most recognized test tool vendors with our timeliness of supporting new specifications in various protocols. Some protocols have less frequent update cycles. For example, IPv4 has had very few changes during the past 10 years, but we still need to keep a close eye on what can be improved in those types of tools as well. There are always new attack patterns emerging and whenever



something new is found, we need to ensure all our tools will catch that and similar flaws in all various protocols that we support.

Finally, there is the actual testing technology to maintain. Our test generation framework was just upgraded to the fifth generation fuzzer technology, through yet another complete re-write of the core engine in the test tools. Many of our competitors are still stuck somewhere between second and third generation technologies, with problems in both upgrading and maintaining new releases of the software on their legacy hardware appliances. Fortunately, we do not have those problems. The features that we have integrated into our current release outperform capabilities of all other tools in this market. That is enabled by our close communication with our customers about their real-life use scenarios. Still, there are numerous challenges in this type of testing left for the future also.

Rake Narang: *Will the security vendors always be playing a catch-up game with hackers and attackers? How do you see the security products evolving 2-3 years from today?*

Ari Takanen: Reactive security vendors, such as AV and IDS product manufacturers, are stuck in this catch-up game. As the number of attacks build, these vendors eventually will give up. It will be impossible to keep up with the number of attacks in real-time networks. The only solution for the future is proactive tools such as ours. There are numerous business opportunities in the proactive security space, and you will probably see some of them during the coming years. Some of those products are already out there, unfortunately still most go unnoticed.

Another huge trend is also in rebuilding the walls to the communication networks. For example, VoIP does not have to connect into Internet. Similarly, there are also other network-based filtering techniques being deployed. This will make security market less and less attractive, as it will become more and more a service provider market rather than a consumer market. I do not see consumers buying firewalls and antivirus products in the future. They will buy a network service that will take care of their security.

Rake Narang: *How is your company focusing on 2008 growth? As an executive leader, what steps have you taken that have had a positive impact on your company?*

Ari Takanen: We have always had 60-100% annual growth since 2001. We plan on maintaining that in the near future also. One of the major steps in maintaining that momentum is our transition into subscription licensing as well as the launch of our services offering. Both of those developments have received extremely positive feedback from the customer base. We have customers with very limited budgets for tests, and hundreds of protocols to test in tens of different locations globally. Our licensing models enable them to do everything immediately as opposed to hindering their product hardening with limited testing equipment. Our most important driver in this market is our customer base. As far as I know, we have never lost a customer to our competition due to this approach. That combined with our licensing strategy will ensure annual growth in the future.

All About Codenomicon

Head Office Address: Oulu, Finland

Founded in: 2001

CEO: Isaac Sundarajan

Public or Private: Private

Investors: Eqvitec and Prime

Number of Employees: 50

Products: DEFENSICS test tools

Company's Goals: To remain the leader in the categories of both robustness testing tools and proactive penetration testing tools

Awards: JOLT Productivity Award 2008, AlwaysOn AO 100 Top Private Companies 2007, Frost and Sullivan 2007 Product Differentiation and Innovation Award, InnoFinland 2007 Award, Red Herring Europe 100 Top Companies 2007

[HOME](#) | [ADVERTISE WITH US](#) | [TELL US ABOUT YOURSELF](#) | [UPDATED PRIVACY POLICY](#) | [CONTACT OUR EDITORS](#) |

Copyright © 2007 Silicon Valley Communications - All rights reserved.