



CODENOMICON

defensics™

DEFEND. THEN DEPLOY.

Canadian Partner:

NORTAK SOFTWARE LTD.

CRAIG MACKAY
613.234.7212 ext. 276
craig.mackay@nortak.com

MIKE O'NEIL
613.234.7212 ext. 228
mike.oneil@nortak.com

PREEMPTIVE SECURITY AND ROBUSTNESS TESTING SOLUTIONS

"It's what you don't know that makes you vulnerable."

- David Chartier, CEO of Codenomicon Ltd

FUZZING

Fuzzing in a Nutshell

> **ROBUSTNESS TESTING:** Fuzzing is a form of robustness testing, which focuses on communication interfaces and the discovery of security related issues, such as overflows and boundary value conditions.

> **FEEDING INPUTS AND MONITORING OUTPUTS:** Robustness testing is a software testing technique, in which unexpected data is fed to the inputs of a system, and the behavior of the system is then monitored.

> **DISCOVERING PROTOCOL IMPLEMENTATION FLAWS:** If the system under test (SUT) fails, e.g., by crashing or by failing built in code assertions, then there is a bug in the software.

> **BLACK-BOX, GREY-BOX AND WHITE-BOX TESTING:** Fuzz tests can be conducted in a number of ways depending on the tester's needs and the amount of information available on the system being tested.

Fuzzing Benefits

> **REPRESENTING REAL THREATS:** Fuzzing is essentially doing what the attackers do, but before them. Fuzz tests can also be used to simulate system aging or overload situations.

> **FINDING ZERO-DAY VULNERABILITIES:** The main strength of Fuzzing is its unparalleled ability to find unknown vulnerabilities. Fuzzing gives testers more time to create and implement patches.

> **HARDENING SYSTEMS BEFORE COMMERCIAL DEPLOYMENT:** The costs of bad Quality of Service (QoS) and downtime can be considerable to your company reputation and sales. Discover flaws and create patches for them proactively, before problems occur and flaws can be exploited.

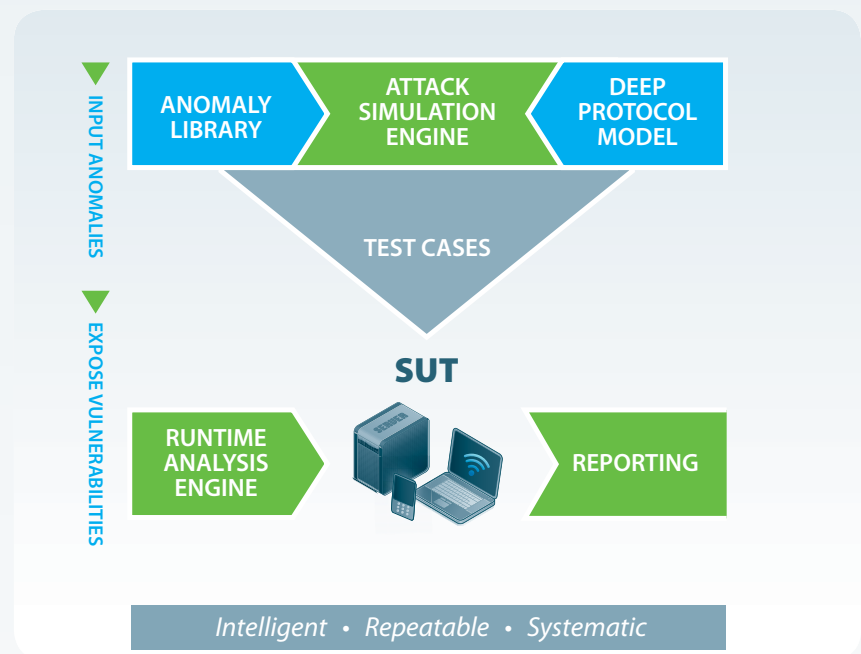
> **BUILDING THE SECURITY INTO YOUR SYSTEM:** Fuzzing improves the quality of your code ensuring the security of your application. Most security systems merely add to the complexity of your system, making it more vulnerable.

The DEFENSICS™ Advantage

Codenomicon DEFENSICS™ testing solutions empower customers to mitigate known and unknown threats in products and services prior to release or deployment. Ensure the Secure Development Lifecycle (SDLC) of your system by building security into it and strengthen it, before exposures or outages occur and zero-day attacks strike.

The fundamental challenges in robustness testing are the infinite number of potential vulnerabilities and the difficulty of reaching the deeper protocol layers.

The DEFENSICS™ Attack Simulation Engine is the industry's first state-aware test case generator. It utilizes deep protocol models to intelligently target protocol areas most susceptible to vulnerabilities even in deeper protocol layers with high accuracy, while maintaining broad coverage through automatic test generation.



How resilient is our service?
Will the next attack take us down?

CHIEF SECURITY OFFICER
CARRIER / OPERATOR

Does our application development process comply
with risk management best practices?

CHIEF INFORMATION OFFICER
FINANCIAL SERVICES ENTERPRISE



“DEFENSICS™ solutions achieve remarkable efficiency in discovering both known and unknown bugs and they are valuable tools for companies seeking to harden their systems before deployment.”

- Srihari Padmanabhan, Research Analyst, Test & Measurement, Frost & Sullivan

Features and Benefits

- > BROADEST TEST COVERAGE:**
DEFENSICS™ provides off-the-shelf testing tools for over 150 protocols and file formats. It can be used to test digital media and wireless infrastructures and network protocols.
- > THOUSANDS OF PREBUILT TEST CASES:**
Built-in expertise and automated test case execution facilitate testing. No manual test case creation effort or testing experience is needed.
- > FAST TEST RUNS:**
DEFENSICS™ utilizes intelligent model-based test cases. By targeting the test cases the amount of test cases needed is significantly reduced making the whole testing process quicker and more cost efficient.
- > EASY TO INTEGRATE:**
As a software-only platform DEFENSICS™ can be easily integrated into your existing software development and testing processes. All the reporting and test case features can be processed with external editors and scripts.
- > PROACTIVE TESTING:**
By integrating DEFENSICS™ into your software development process, you can discover flaws at the earliest possible moment. The earlier the bugs are discovered the cheaper and easier it is to fix them.
- > INTEGRATED ONLINE DOCUMENTATION:**
Share online detailed test case material and results within your organization. The reports have direct links to test cases identifying specific problems making all identified flaws easily repeatable and traceable.
- > MULTIPLE USERS AND LOCATIONS:**
All users can remotely access the same system and reproduce all identified flaws. It is no longer necessary to create identical test environments, because the same test runs can be executed by multiple users in multiple locations.
- > REGRESSION, COMPLIANCE AND AUDITING:**
The off-the-shelf tools combined with powerful test reproduction, documentation and reporting tools make DEFENSICS™ the optimal solution for regression analysis, compliance testing and auditing.



How can we improve the efficiency of security and robustness testing within our organization?

GENERAL MANAGER
NETWORK DEVICE DEVELOPER

Are flaws and patches impacting sales and damaging our brand?

DEVELOPMENT DIRECTOR
CONSUMER DEVICE DEVELOPER

CODENOMICON

Expertise

Codenomicon Ltd. is a spin-off of the widely acclaimed PROTOS project of the Oulu University Secure Programming Group (OUSPG). Codenomicon is recognized in the industry for its innovations in negative black-box testing and its unique targeted approach to fuzz testing networked and mobile applications. The company is actively engaged in the open source community and through its CROSS program, Codenomicon assists open source projects fix critical flaws in their code.

Innovation

First launched in 2001, the DEFENSICS™ testing platform continues to demonstrate a high degree of innovativeness by incorporating the latest research into its intelligent fuzzing techniques. While, traditional security testing has been overwhelmed by the fast adoption rate of new technologies, fuzzing has proven itself as an easily adaptable testing technique. Codenomicon DEFENSICS™ fulfills the changing testing needs of its customers providing not only state-of-the-art tools but also extensive customer support.

Growth

Headquartered in Oulu, Finland with offices in California and Hong Kong, the company markets its test solutions and services directly and through international partners. Codenomicon has over 100 customers including Alcatel-Lucent, AT&T, Cisco Systems, Nordea, Nortel, Microsoft and Nokia Siemens Networks among many others. The company is privately held with investments from Eqvitec Partners and Prime Technology Ventures.



www.codenomicon.com

Test Suites

Core Internet	Net Management	Routing
IPv4 (TCP, UDP, IPv4, ICMP, IGMP, ARP), IPv6 (TCP, UDP, IPv6, ICMPv6), IPsec, DNS (Server, Client, Zone Transfer), NTP (Client, Server), DHCP/BOOTP Client, DHCP/BOOTP Server, HTTP Server, HTTP Client, FTP Server, DHCPv6 Client, DHCPv6 Server, MIPv6 (Client, Server)	HTTP Server, HTTP Client, TLS/SSL Server, TLS/SSL Client, Telnet Server, SSH1 Server, SSH2 Server, SNMPv1/v2 Server, SNMPv3 Server, TFTP Server, UPnP Server, Syslog	IS-IS, DVMRP, GRE, OSPFv2, OSPFv3, PIM-SM/DM, RSVP, VRRP, BGP4, RIP, RIPng, MPLS/LDP, HSRP, NHRP

Remote Access	VPN	VoIP
EAPOL Server, PPPoE, Diameter Server, Diameter Client, LDAPv3 Server, TACACS+ Server, TACACS+ NAS, RADIUS (Server, Client), Kerberos Server	IPSec, SSH1 Server, SSH2 Server, TLS/SSL Server, TLS/SSL Client, ISAKMP/IKEv1 (Client, Server), IKEv2, OCSP (Client, Server)	SCTP, H.248, H.323, RTSP (Client, Server), TLS/SSL Server, TLS/SSL Client, SIP UAS, SIP UAC, SigComp, RTP/RTCP/SRTP, MGCP, UPnP Server, SMPP, x.509

3G / 4G-LTE	Digital Media	Email
SCTP, GRE, IPsec, Diameter Server, Diameter Client, LDAP Server, TLS/SSL Server, TLS/SSL Client, SIP UAS, SIP UAC, GTPv1, GTPv0, RADIUS (Server, Client)	AIFF, AU, AMR, IMY, MP3, VOC, WAV, BMP, GIF, JPEG, MBM, PCX, PNG, PIX, PNM, RAS, TIFF, WBMP, XBM, XPM, WMF, AVI, Quicktime, MPG1, MPG2, MPEG4, ZIP, CAB, JAR, LHA, GZIP, vCalendar, VCard	POP3 Client, POP3 Server, IMAP4 Client, IMAP4 Server, SMTP Client, SMTP Server, MIME

File Systems/Storage	WLAN	Link Management
CIFS/SMB Server, iSCSI Server, SunRPC Server, NFS Server, SMBv2	802.11 Server, 802.11 Client, WPA Server, WPA Client	LACP, STP, MSTP, RSTP, ESTP

Bluetooth	IPTV	PDA/ Smartphone
L2CAP, SDP, RFCOMM, OBEX, OPP, FTP, IrMC Synchron, BIP, BPP, BNEP, HFP, HSP, DUN, PBAP, FAX, AVRCP, A2DP, HCRP, HID, SAP, HFP Client, HSP Client	MPEG4, MPEG2, IPsec, TLS/SSL, RTP/RTCP, RTSP, HTTP, FTP, TFTP, IPv4, PIM-SM/DM, RSVP, IGMP, CWMP (TR-69) ACS, CWMP (TR-69) CPE	IPv4, DHCP/BOOTP, HTTP, TLS/SSL, UPnP, SIP, Audio, Images, Video, Bluetooth, 802.11

Industrial Automation	Archives	Metro Ethernet
(SCADA/DCS) Modbus, IPv4 (TCP, UDP, IPv4, ICMP, IGMP, ARP)	GAB, GZIP, JAR, LHA, ZIP	BFD, CFM, E-LMI, Ethernet, GARP, LLDP, OAM, PBT/PBB-TE, L2TPv2, L2TPv3, STP/RSTP/MSTP/ESTP

General Fuzzer
XML SOAP Traffic Capture Fuzzer

Protocols Supported

802.11	IPv4	RSVP
ARP	IPv6	RTCP
BGP4	IS-IS	RTP
BFD	ISAKMP/IKE	RTSP
BOOTP	iSCSI	SCTP
BT	Kerberos	SigComp
CFM	L2TPv2	SIP
CIFS/SMB	L2TPv3	SIT TT
CWMP (TR-69) ACE	LACP	SMBv2
DHCP	LDAPv3	SMPP
DHCPv6	LLDP	SMTP
Diameter	LPD	SNMPv1
DNS	MGCP	SNMPv2c
DVMRP	MIPv6	SNMPv3
E-LMI	MIME	SRTP
EAP	Modbus	SSH1
ESTP	MPLS/LDP	SSH2
Ethernet	MSTP	STP
Finger	NFS	STUN
GARP	NHRP	SunRPC
FTP	NTP	Syslog
GRE	OAM	TACACS+
GTPv0	OCSP	TCP
GTPv1	OSPFv2	Telnet
H.248	OSPFv3	TFTP
H.323	PBT/PBB-TE	TLS/SSL
HSRP	PIM-DM/SM	TURN
HTTP	POP3	UDP
ICMP	PPPoE	UPnP
ICMPv6	RADIUS	VLACP
IGMP	RIP	WPA1 WPA2
IKEv2	RIPng	VRRP
IMAP4	Rlogin	X.509
IPsec	RSTP	XML

Technical Requirements

Supported Operating Systems

Windows XP SP2 and Linux Fedora Core 5 (or newer)

System Requirements

1 GHz processor (or faster), 1 GB of free disk space, 1024x768 graphics resolution, 256 MB of RAM, CD-ROM or DVD drive, Network card (NIC)

Sun Microsystems Java™ 2 Runtime Environment

Standard Edition 1.5.0_06 or higher.

USB port

USB Bluetooth/WLAN transceivers included with Bluetooth and WLAN tools

CODENOMICON Ltd.
info@codenomicon.com
www.codenomicon.com

Tutkijantie 4E
FIN-90570 OULU
FINLAND
+358 424 7431

10670 North Tantau Avenue
Cupertino, CA 95014
UNITED STATES
+1 408 252 4000

25/F., Queen's Road Centre
152 Queen's Road Central
HONG KONG
+852 3426 22900