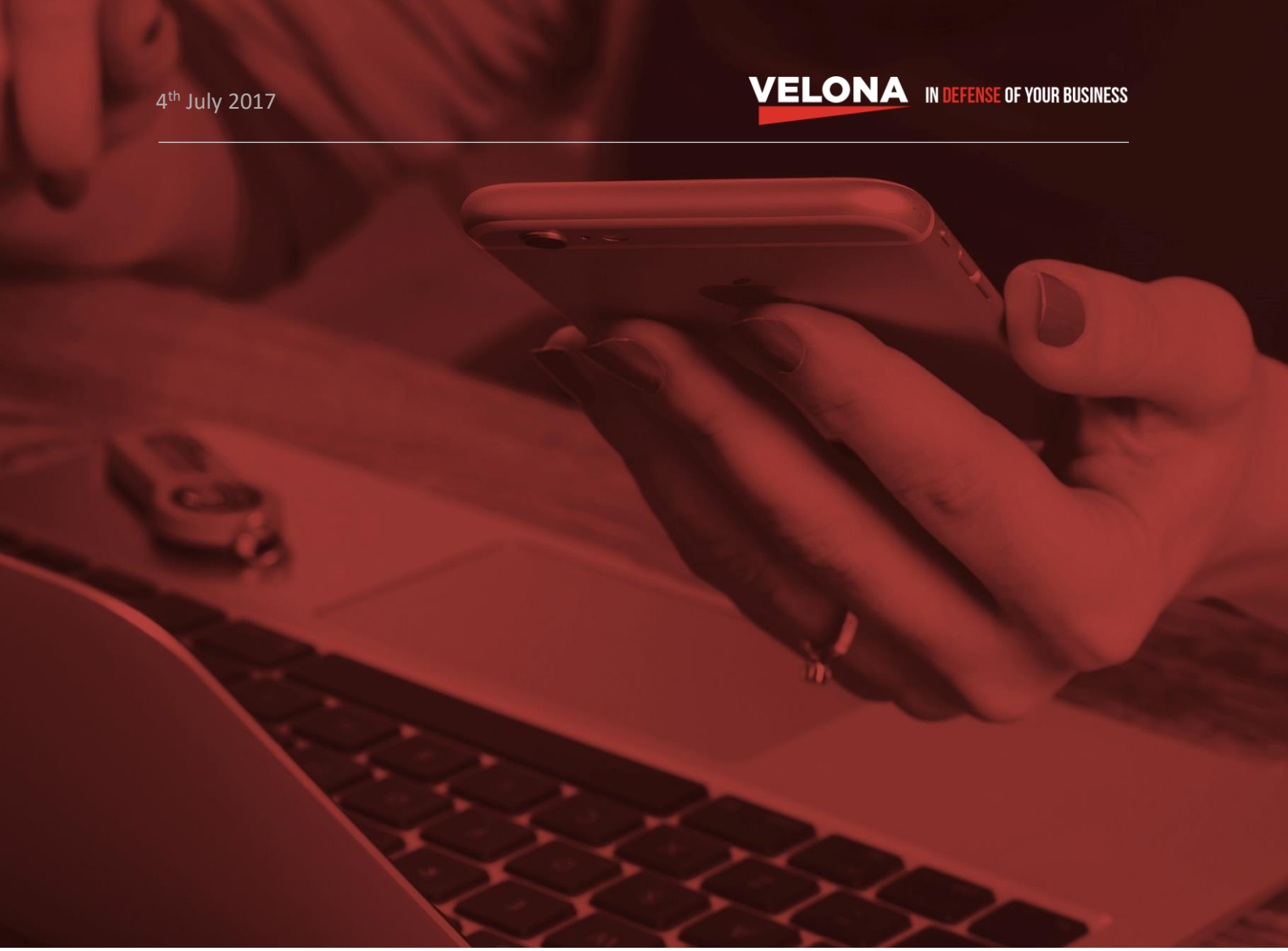
4th July 2017

VELONA IN DEFENSE OF YOUR BUSINESS



Validating Vendor SIP Security

Case study showing how Vodafone used CRACKER to independently assess the SIP security capability of an E-SBC Vendor.

Velona Systems R&D

Validating the true SIP Security capability of an E-SBC

Our client required an independent assessment of the SIP Security capability of a market leading Enterprise Session Border Controller (E-SBC), under consideration for deployment into enterprises as part of an end-to-end hosted voice solution for SMEs. Velona undertook the evaluation of the E-SBC, using the CRACKER to test the ESBC's capability to withstand SIP attacks of various forms.

How we did it

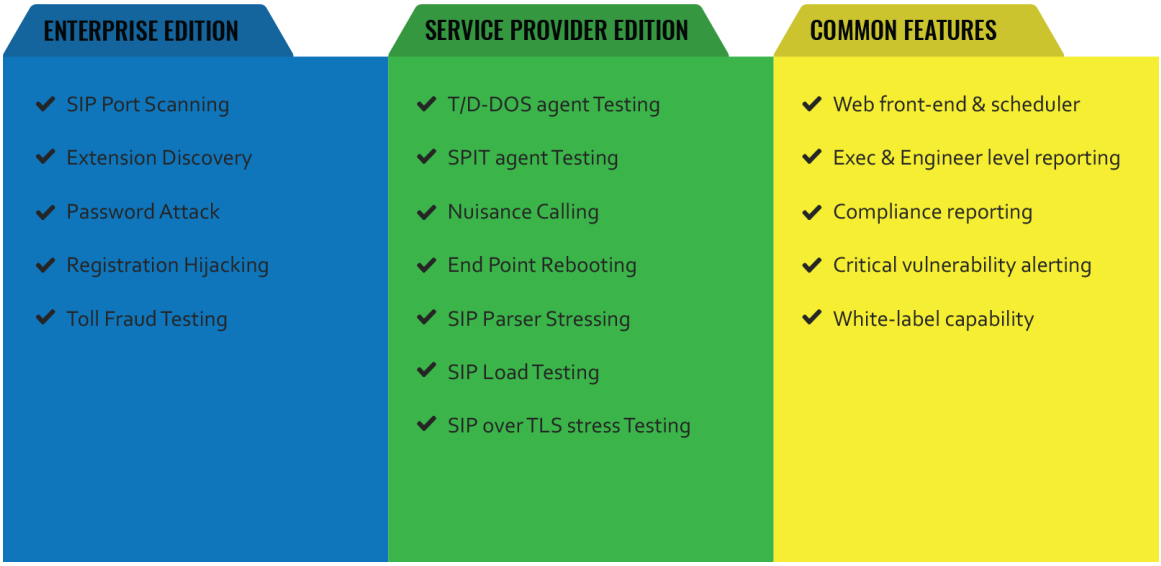
Velona used features from both the Enterprise and Service provider editions of CRACKER, as shown below. Testing focused on 'the outside looking in' as the primary security aim of an E-SBC is to detect and block external threats.

1. Could the E-SBC be caused to crash, freeze, or stop processing some or all SIP signalling or media?
2. Could the E-SBC be used to route SIP signalling in ways that should not allowed, including to signalling which could enable toll fraud?
3. Did the E-SBC pass badly formatted messages?
4. Focus was on tests which are applicable in real environments. Complicated and rare tests are applicable provided they can be executed in a real-world environment.

Key Findings

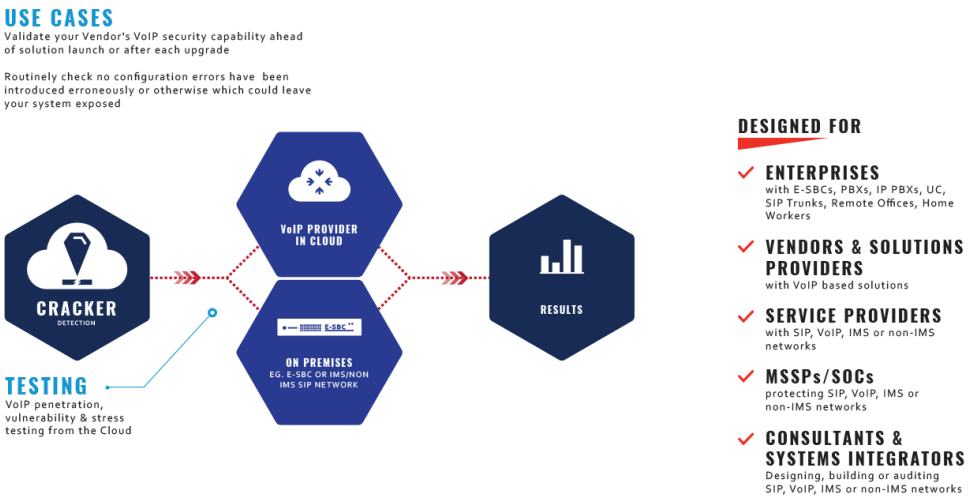
CRACKER found over 50 issues with the E-SBC during a two-week test run, with the main issues summarised as follows:

1. Certain single malformed message attacks caused an outage which lasted for more than fifty minutes.
2. E-SBC could be compromised and used as a DoS relay.
3. Inbound SIP requests could force the E-SBC to send responses to IP addresses or FQDNs that were not authorised in either the inbound or outbound SIP server rules.
4. Source IP address spoofing was not stopped.
5. The rules limiting inbound messages to the listed SIP proxies / SIP servers could be bypassed.
6. UDP and IP layers were not considered when calculating the maximum SIP message size that it would accept.



Velona's Generic approach to SIP Security

Our starting basis is always that SIP DoS attacks using methods more sophisticated than simply mass calling will become more prevalent and that both enterprise and service provider networks must be able to protect against such attacks.



TESTING COMMUNICATIONS SYSTEMS

CRACKER runs a suite of SIP penetration & stress tests against VoIP Network Equipment Manufacturers (NEMs) which makes it easy to proactively assess the robustness of any element on the Enterprise or Core side of a VoIP network. When delivered as a service, our testing methodology consists of:

1. Scope definition and agreement
2. Reconnaissance and verification
3. End-End Test run
4. Vulnerability Analysis
5. Reporting and Debrief

The end deliverable is a comprehensive report identifying vulnerabilities and areas for exploitation, with guidance on remediation, as well as a high-level management report. We calculate a perceived severity of each identified risk using a qualitative approach and a combination of the Business Impact should the risk occur and the Likelihood of the risk occurring.

What is in Velona's Cracker Test Suites

- ✓ Basic SIP parser testing – individual messages
- ✓ Basic SIP parser testing – combinations of messages
- ✓ Advanced SIP parser testing
- ✓ SIP routing testing
- ✓ Load testing including soak testing using one or more of UDP, TCP, TLS
- ✓ Non-SDP message bodies (XML, etc.)
- ✓ Fax

The starting point for Basic SIP parser testing is RFC 4475, with additional Velona Systems tests. We design standard tests for each type of equipment or software (e.g. standard tests for IP Phones, standard tests for softphones, standard test for SBCs, etc.) as well as tests specific to specific manufacturers and models.

INDEPENDENT ASSESSMENT - we continuously update our Test capability to optimize the benefits of your test runs, but always allow you to benchmark on a like-for-like basis.

AVAILABLE FROM THE CLOUD - Your VOIP security test capability is always available and is automatically kept up to date.

DEDICATED TO VoIP - Built by SIP experts to remove 99% of the knowledge complexity requirement of SIP/VoIP. We know the vulnerabilities in voice systems which can quickly impact system capacity.

PROJECT BASED PRICING - Simply use our advanced VoIP security testing as required, and reduce the need for expensive equipment.

VELONA SYSTEMS

OUR MISSION

TO ELIMINATE T-DOS AND TOLL FRAUD FROM VOIP COMMUNICATIONS

Real-time VoIP threat detection & prevention via Cloud SaaS solutions to eliminate risk to key infrastructure, productivity loss, revenue loss, or brand damage

OUR PRODUCTS

CRACKER
VoIP penetration & vulnerability testing from the Cloud

WATCHER
real-time VoIP threat detection & protection

SIP FINGERPRINTER™
C Library via commercial licence

FIND US

ADDRESS
Velona Systems Limited, 2nd floor, 11 Anglesea Street, Cork, Ireland

POSTCODE
T12CYR8

ON THE WEB
www.velonasystems.com