Cryptosense software finds security flaws in the cryptography used by applications and network services.

**ARE CRYPTO FLAWS REALLY A PROBLEM?**

<table>
<thead>
<tr>
<th>High and Medium Vulnerabilities</th>
<th>Mitre CVE database 2013 - 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>1826 XSS</td>
<td>1755 Cryptographic Issues</td>
</tr>
<tr>
<td>654 SQL Injection</td>
<td></td>
</tr>
</tbody>
</table>

83% of crypto vulnerabilities come from **applications misusing cryptography**.

Not from implementation errors in cryptographic libraries

“Why does Cryptographic Software Fail?” - Lazar et al, 2014, MIT.

**CAN I FIND THESE FLAWS WITH THE TOOLS I ALREADY HAVE?**

98.3% of crypto flaws **cannot be detected** by the best performing static analysis tool (2013 NIST SATE Evaluation)

*Only 1.7% of flaws in the security features category (which includes cryptography) were detected by any tool.*

We cover more crypto flaws than existing tools because of our novel analysis methods, and our rulebase which incorporates latest applied crypto results and our own in-house vulnerability analysis.

**HOW DOES CRYPTOSENSE SOFTWARE WORK?**

1. **Tracing**
   
   Our tracer agent records calls from an application to its crypto library. You then upload the trace to our web application Analyzer platform where our powerful analysis algorithms and up-to-date crypto knowledge base are applied to detect flaws and suggest remediations.

2. **Analysis**

3. **Remediation**

For a test on your application contact sales@cryptosense.com or +1 646-893-7657.
Cryptosense Products

**Analyzer**

*Cryptosense Analyzer* finds crypto-related vulnerabilities in applications. It works by tracing the calls from the application to the cryptographic library and then processing the trace with our powerful crypto vulnerability rules to look for key-management issues, crypto misuse, randomness problems, nonce reuse, weak algorithms and key-lengths and more. By testing the running application, the Analyzer can also detect flaws arising from libraries or dependencies, and doesn’t need access to source code.

**Discovery**

*Cryptosense Discovery* finds and analyzes the security of network crypto services like TLS, SSH and STARTTLS (IMAP, SMTP, POP3, LDAP etc). Discovery’s analysis rules are continuously updated to take into account the latest results in applied crypto research, and the tool can also suggest configuration file changes for the most common services. Available hosted in the cloud or as a virtual machine.

**PKCS#11 Toolkit**

*Cryptosense’s PKCS#11 Toolkit* is a complete solution for security audit and monitoring of your PKCS#11-compatible HSM deployment. It includes a special-purpose fuzzing engine for finding vulnerabilities in the HSM implementation and configuration, a tracer agent for analyzing the crypto calls made by the application, and a monitor to test that keys and configurations always stay secure.

Visit [testmycrypto.com](http://testmycrypto.com) to get access to the live demo of Cryptosense Analyzer as well as our other tools.

**Cryptosense Analyzer**

- Easy to use platform
- Leverages existing tests
- Powered by latest results from academia
- Simplify plethora of standards with customizable profiles
- Avoid data breaches related to crypto
- Minimise time-to-market and audit costs with easy bug targeting
- Works without source code so you can test third party products

About Cryptosense

Based in Paris, France, Cryptosense provides its solutions to the financial services industry, government agencies, and software and hardware producers. To arrange a test on your applications, contact sales@cryptosense.com or +1 646-893-7657.