Crypto audit for applications.

Find the high-impact crypto vulnerabilities that other tools miss.
People think that crypto looks like this.
...but it’s really more like this.

16th Century, Citadel of Dinant, Belgium.

Photo © 2016 Ben Heine
Key-management flaws

Problems with random number generation

Interactions between crypto operations

Protocol configuration errors

Weak encryption and signature modes

Weak algorithm and key-length choice

Bad nonce management
Are crypto vulnerabilities a significant threat?
They rank between XSS and SQL Injection on the CVE database...

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1826</td>
<td>XSS</td>
</tr>
<tr>
<td>1755</td>
<td>Cryptographic Issues</td>
</tr>
<tr>
<td>654</td>
<td>SQL Injection</td>
</tr>
</tbody>
</table>

Total High and Medium Vulnerabilities - Mitre CVE database 2013 - 2015
In “Why does Cryptographic Software Fail?” (Lazar et al, 2014), MIT scientists showed that the vast majority of crypto vulnerabilities come from applications misusing cryptography, not from implementation errors in cryptographic libraries.
They are a blind spot for static analysis tools

In the 2013 NIST SATE Evaluation, only 1.7% of flaws in the security features category (which includes cryptography) were detected by any tool.
...and attacks are more and more common.

**FREAK**  
March 2015

**LOGJAM**  
May 2015

**Github SSH keys GCD**  
June 2015

**RC4 NO MORE**  
Aug 2015

**SHA-1 Freestart Collisions**  
Oct 2015

**Invalid Curve Attacks**  
Dec 2015

**SLOTH**  
Jan 2016

**DROWN**  
March 2016

**Sweet32**  
July 2016

**Diffie Hellman Backdoors**  
June 2016

**Diffie Hellman Small Subgroups**  
October 2016

**Weak RSA Keys in Network Devices**  
November 2016
Cryptosense software analyses the security of crypto use in applications at **run-time** to detect and eliminate crypto-related vulnerabilities.
Our tracing methods see all the cryptography used by the application (including dependencies, libraries and framework components).

Our analysis algorithms incorporate the latest applied crypto results and our own in-house vulnerability analysis.
Cryptosense software attaches to a running application while standard integration tests are executed and logs crypto calls.

1. Tracing
Traces are run through our security analysis algorithms derived from the latest academic results and Cryptosense’s own vulnerability research.

1. Tracing

2. Analysis*

* Either on-premise or in the cloud as SAAS
Reports are shown in a web interface with links to stacktraces for fast debugging. Recommendations are given for remediation.

1. Tracing
2. Analysis*
3. Remediation*

* Either on-premise or in the cloud as SAAS
Try it for yourself!

Sign up for a demo account at

testmycrypto.com
Tracer Support

NOW

Q3 2017

Q4 2017

Java
PKCS#11

OpenSSL

.net
Microsoft CNG
Cryptosense Analyzer is available in SaaS mode and on-premise.

The on-premise version is completely self-contained and has no need to access cloud-based servers.

Rule updates are supplied every three months.
Crypto Analysis

Categories
Easily view rules for each category type.

Failed Rules
Click on a rule for more information on risks and to see the instances.

Risks
Each rule has detailed risk assessment information.

Debug View
Links to stacktraces to identify where in the application the weaknesses are.

Instances
Specific cases of failed rules. Can be shared, dismissed, and starred.
Creation of a Custom Profile

**Standards**
Key length rules can be set to ENISA, NIST standards or set to a custom profile using sliders.

**Rules**
Priority and activation of rules can be customized.
Developer View - Remediation

Stack trace
See all the detail for a specific instance in order to fix problems.
Typical POC

SaaS mode

1 application

30 day period

No limit on number of traces uploaded or reports generated

Support from Cryptosense analysts throughout the process, including in-depth advice on remediation of crypto flaws found.
Academic spin-off (2013)

Current clients

» 3 of top 5 European Banks
» 2 SIFIs (Financial Services Infrastructure Providers)
» US and French government agencies

Funding Bodies

Prizes

Graham Steel, PhD
CEO & Founder

Università Cà' Foscari Venezia

IT-Translation

Elaia Partners

UBS
Future of Finance 2015
Global Finalist

prix de l'innovation des assises 2016
Winner
Your Partner for Secure Crypto

https://cryptosense.com

graham@cryptosense.com

+33 (0) 9 72 42 35

@cryptosense