1. Motivation

- Compare tool’s accuracy and security guarantee.
- Decide which tool is suitable for developers to use.
- Educate cryptographically secure and insecure codes.

2. Threat Models

We consider sixteen cryptographic vulnerabilities from five attack types:

- Predictable Secret
- Chosen Ciphertext Attack (CPA)
- SSL/TLS in MitM
- Brute-force Attack on Cipher
- Predictability in PRNG

3. Design of CryptoAPI-Bench

- Total 171 test cases.
- Contains 135 vulnerable and 36 non-vulnerable cases.
- Contains 40 basic and 131 advanced cases.

4. Evaluation

<table>
<thead>
<tr>
<th>Three Tools Selection Criteria:</th>
<th>Tools</th>
<th>Basic Cases</th>
<th>Advanced Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Open-sourced tool</td>
<td>SpotBugs</td>
<td>Precision (%) 100.00 Recall (%) 92.86</td>
<td>Precision (%) 0.00 Recall (%) 0.00</td>
</tr>
<tr>
<td>- Static analysis tool</td>
<td>CryptoGuard</td>
<td>Precision (%) 100.00 Recall (%) 92.86</td>
<td>Precision (%) 83.33 Recall (%) 95.59</td>
</tr>
<tr>
<td>- Free analysis tool</td>
<td>CrySL</td>
<td>Precision (%) 62.50 Recall (%) 71.43</td>
<td>Precision (%) 55.56 Recall (%) 58.82</td>
</tr>
<tr>
<td></td>
<td>Coverity</td>
<td>Precision (%) 100.00 Recall (%) 92.86</td>
<td>Precision (%) 52.00 Recall (%) 19.12</td>
</tr>
</tbody>
</table>

5. Conclusion

- CryptoAPI-Bench contributes to improvements in the science of security.
- CrySL and CryptoGuard improve their tools using CryptoAPI-Bench that incur real world impact.

6. References

[1] https://github.com/CryptoAPI-Bench/CryptoAPI-Bench
[2] Welcome to the SWAMP. https://continuousassurance.org, 2018

This work is supported by Office of Naval Research under grant ONR-N00014-17-1-2498.

Yao Group on Cyber Security
http://people.cs.vt.edu/danfeng/