

# SaTC:TTP:Medium:Collaborative: Deployment-quality and Accessible Solutions for Cryptography Code Development

CryptoGuard

**Challenge:** There is a urgent demand for

- High-accuracy deployable solutions for crypto code screening
- Scientific benchmarking and measurement

## Solution:

- Language-specific refinement methods for enhancing precision in static program analysis based crypto code screening
- Systematic benchmarks

Who wouldn't want to write secure code?

False positives

Time

Resources

Budget

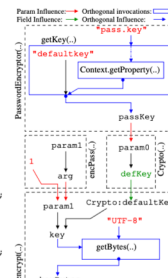


```

1 class PasswordEncryptor {
2
3   Crypto crypto;
4
5   public PasswordEncryptor ()
6     String passKey = PasswordEncryptor
7       .getKey("pass_key");
8
9
10  byte[] encPass(String [] arg) {
11    return crypto.encrypt(arg[0], arg[1]);
12  }
13
14  static String getKey(String src) {
15    String key = Context.getProperty(src);
16    if (key == null) {
17      key = "defaultkey";
18    }
19    return key;
20  }
21  }
    
```

```

22 class Crypto {
23
24   String ALGO = "AES";
25   String ALGO_SPEC = "AES/CBC/NoPadding";
26   String defaultKey;
27   Cipher cipher;
28
29   public Crypto(String defKey) {
30     cipher = Cipher.getInstance(ALGO_SPEC);
31     defaultKey = defKey; // assigning field
32   }
33
34   byte[] encrypt(String txt, String key) {
35     if (key == null) {
36       key = defaultKey;
37     }
38     byte[] keyBytes = key.getBytes("UTF-8");
39     byte[] txtBytes = txt.getBytes();
40     SecretKeySpec keySpec =
41       new SecretKeySpec(keyBytes, ALGO);
42     cipher.init(cipher.ENCRYPT_MODE, keySpec);
43     return cipher.doFinal(txtBytes);
44   }
45 }
    
```



Help developers write secure code with ease

## Scientific Impact:

- Transition secure crypto coding research to practice
- Detect a wide range of crypto API misuses
- High-precision deployable security research is urgently needed

## Broader Impact and Broader Participation:

- **We call for security researchers to understand and help developers**
- Adoption at Oracle Labs
- Integration into Oracle's internal screening framework Parfait
- Multiple 90-minute tutorials to diverse audiences

Award # 1929701. Virginia Tech and University of Wisconsin-Madison. Danfeng (Daphne) Yao (lead PI) . [danfeng@vt.edu](mailto:danfeng@vt.edu) Barton Miller. [bart@cs.wisc.edu](mailto:bart@cs.wisc.edu) Na Meng. [nm8247@vt.edu](mailto:nm8247@vt.edu)