New Static Analysis Techniques to Detect Entropy Failure Vulnerabilities

December 12, 2018

Rushi Shah Andrew Russell

1 Introduction

One common misuse of cryptography is the misuse of entropy. Without proper random inputs, many cryptographic algorithms are vulnerable to basic forms of cryptanalysis. Some cryptographic schemes, such as DSA, can even disclose long-term secrets such as the signing key when the random per-message input is low entropy, made public, or nonunique.

We plan to use data dependency tools to determine how entropic inputs in a given program are used by various cryptographic algorithms. That will allow us to identify if and when entropy is too low or is misused. We plan to produce this as a code integration tool for developers to use as part of a compiler toolchain. Our tool will seek to generate an error report from source code using notions of taint analysis.

For this project we consider codebases that maintain version history, in the hopes that we can employ static analysis techniques across program versions to infer more information about how entropy is being used; our primary goal is to identify bugs that are introduced to existing codebases. This may prove to be especially helpful since naive taint analysis can provide mere overapproximations of data dependency for a given program and may generate many false alarms for programmers in a professional development setting.

2 Preliminaries

In this section we describe the background necessary to understand our new approach.

Test reference: [GKW18]

2.1 Taint Analysis

2.2 Predicate Abstraction

2.3 k-safety properties

2.4 Product Programs

3 Our Approach

3.1 Naive Approaches

Before we cover our approach to this problem we will briefly discuss a number of approaches that do not work, but build to our final result.

A first attempt to solve this problem might include running taint analysis on each version P_1 and P_2 of the program. However, since taint analysis merely provides an overapproximation to this problem, this approach is necessarily unsound. Instead, we would like to view this as a 2-safety property:

3.2 Instrumenting Programs for Predicate Abstraction

3.3 Naive Product Program Inference Rules

3.4 Taint-augmented Inference Rules

3.5 Putting it all together

4 Results

5 Conclusion

6 Future Work

7 Considered Approaches

7.1 Taint Analysis

Static code analysis has a history of identifying security vulnerabilities at a source code level. Some examples include SQL injection, cross-site scripting exploits, and buffer overflow attacks. However, there has not been any attempt in the literature to statically analyze source code for cryptographic vulnerabilities stemming from entropy misuse, which we seek to do. We claim that standard static code analysis techniques developed thus far are insufficient for the analysis we would like to perform. The sources of entropy can be tainted standard taint analysis techniques can be used to approximate how the taint propagates. But this approximation may be too coarse to provide useful information to the user. Even with a sufficiently precise taint analysis, it is unclear how to determine the "correct" set of sources a cryptographic value should rely on at any point in the program.

7.2 Differential Taint Analysis

Since we want a stronger notion of taint analysis than a naive approach, we intend to introduce and formalize the concept of "differential taint analysis." Differential taint analysis, in the ideal, will give us more information than simple taint analysis by leveraging the original version of the program as a source of ground truth. This additional information could include reducing programmer annotation work or reduce false positives between versions (since taint analysis overapproximates data flow). By viewing the original version of the program as bug-free, we reduce the number of code audits required: only the original version of the code would need to be audited, and future versions could rely on our tool to automatically detect bugs that were introduced by refactors.

7.3 Product Programs

One technique that we have considered toward the construction of differential taint analysis is the notion of a "product program." In the most general sense, the product $P_1 \times P_2$ of two programs P_1 and P_2 is used to verify relations between the programs, such as equivalence. Product programs have also been used to analyze different runs of the same program. The product program $P_1 \times P_2$ is semantically equivalent to the sequential composition $P_1;P_2$, but such that we can prove useful safety properties of $P_1 \times P_2$ that would be difficult to prove with standard techniques on P_1, P_2, or $P_1;P_2$.

In our setting, we are not so much interested in proving safety properties of a program P but instead wish to prove that cryptographic values rely on sufficiently many bits of entropy when they are used via taint analysis, which is why we cannot simply leverage existing off-the-shelf product program analysis techniques.

7.3.1 Example

Consider the following two programs P_1 and P_2 that are equivalent from a cryptographic point of view, but might have small feature changes.

function P_1
  $s \leftarrow$ entropy
  $\vdots$
  if p **then**
    $c \leftarrow$ AES(s)
  end if
  $\vdots$
end function

function P_2
  $s \leftarrow$ entropy
  $\vdots$
  if p **then**
    $c \leftarrow$ AES(s)
  end if
  $\vdots$
end function

where p is some complex predicate that is difficult to reason about, but does not change between P_1 and P_2 (and no values that p depends on change, either). Then, a safety property about the entropy of the cryptographic values in c would hold in both programs or in neither program.

7.4 Verification Modulo Versions

Verification modulo versions is an idea quite similar to product programs. VMV attempts to identify abstract regressions and relative correctness between two versions of a program. In VMV, the static analyzer is treated as opaque in an effort to cut down the number of alarms by inferring assumptions made by the original program (assumed to be correct). This is especially appealing in the security software development cycle because there are documented cases of entropy bugs being introduced in new versions of programs (for example, OpenSSL and FreeBSD). This would involve under-approximating the taint of one version of the program and over-approximating the taint of another version of the program. Current tooling does not widely support under-approximating taint analysis.

7.5 Relational Verification

Another existing technique is relational verification, in which relational properties between two programs are used to prove k-safety properties. A k-safety property is a safety property of a program that requires reasoning about the relationships between k different runs of a program (or k programs). For example, transitivity is a k-safety property. In our case, we would want to show the equivalence of entropy assignment and the equivalence of the entropy propagation. Relational verification utilitzes product programs; RV constructs a product program between versions of the program that captures the semantics of executing them sequentially, but that lends itself to standard verification techniques.

7.6 Differential Assertion Checking

The last approach that we have considered is differential assertion checking. Differential assertion checking seeks to (statically) prove the relative correctness between two similar programs, with a significantly lower cost than ensuring absolute correctness. That is, DAC allows is to answer if there are conditions under which a program P_1 passes an assertion check but a program P_2 fails. The techniques utilized current DAC work may be of interest, but it seems they rely on an a priori mapping between the two programs, which is something that relational verification work seeks to answer. Thus DAC will be considered further after the idea of product programs is exhausted.

8 Our Approach

Given the two programs in the example, we propose generating a product program similar to the following:

function $P_1 \times P_2$
    $S_1 \leftarrow$ entropy
    $S_2 \leftarrow$ entropy
    $\vdots$
    if f() **then**
        $c_1 \leftarrow$ AES(s_1)
        $c_2 \leftarrow$ AES(s_2)
    end if
    $\vdots$
end function

Note that, during the construction of the product program, we need to be able to merge the if statements in the two programs.

We would like to demonstrate set equality between the taint for s_1, s_2 when they are used in the if statement, which amounts to demonstrating the equivalence of the taint propagation through the program. We would also like to demonstrate that we assign the output of a sufficiently entropic value to a variable in P_1 if and only if we also assign it that sufficiently entropic value in P_2.

Proving these two properties (set-equality and equivalence of assignments) allows us to claim that P_1 has the safety property if and only if P_2 has the safety property.

9 Real World Applications

A verification tool like this could be especially useful for a maintainer of a project that relies on cryptographic values. For example, if she audits her code once to confirm that it uses entropy properly, she can use differential taint analysis on future commits to confirm that the new code does not introduce this class of bugs.

Our tool should be able to detect the infamous Debian OpenSSL entropy bug. We will also test our tool on other libraries that rely on entropy, such as Amazon's signal2noise, LibreSSL, GnuTLS, and GnuPG, which are not known to contain entropy bugs (and likely do not), but we can test on versions in which we introduce our own bugs.

10 Research Hypotheses

These are the principal hypotheses we would like to test:

1. An automated tool can detect entropy bugs in real-world programs.

2. Entropy is insufficiently propagated in programs that rely on cryptography, or entropy propagation follows nontrivial code paths (due to error handling or other control flow).

3. Multiple versions of the same program can make static analysis for this domain more effective by lowering costs (computational and programmer) or providing more fine-grained information.

11 Future Work

As bad data flow can be a source of security bugs other than simply (lack of) entropy propagation (for example, address disclosure and use-after-free bugs in browsers), we believe that our tool could also be applied to these settings to help prevent programmers from introducing security vulnerabilities into their projects.

12 Links

1. Debian/OpenSSL Bug
   (a) `https://www.schneier.com/blog/archives/2008/05/random_number_b.html`
   (b) `https://research.swtch.com/openssl`
   (c) `https://freedom-to-tinker.com/2013/09/20/software-transparency-debian-openssl-bug/`
   (d) `https://www.cs.umd.edu/class/fall2017/cmsc818O/papers/private-keys-public.pdf`
2. Data flow
   (a) `https://en.wikipedia.org/wiki/Data-flow_analysis`
   (b) `https://www.seas.harvard.edu/courses/cs252/2011sp/slides/Lec02-Dataflow.pdf`
3. Static Program Analysis
   (a) `https://cs.au.dk/~amoeller/spa/spa.pdf`
   (b) `https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6859783`
4. Relational Verification:
   (a) `https://dl.acm.org/citation.cfm?id=2021319`
   (b) `https://ac.els-cdn.com/S235222081630044X/1-s2.0-S235222081630044X-main.pdf?_tid=076a0492-9cee-4995-9710-bcb3c64b98e0&acdnat=1539815890_178849b4f14af3751e9acb03b238db4d`
   (c) `https://www.microsoft.com/en-us/research/publication/differential-assertion-checking/`
   (d) `https://www.microsoft.com/en-us/research/wp-content/uploads/2014/06/paper-1.pdf`
   (e) `https://www.cs.utexas.edu/~isil/pldi16-chl.pdf`
5. Projects to analyze
   (a) OpenPGP
   (b) BouncyCastle
   (c) OpenSSL
   (d) GnuPGP
   (e) F# SSL project with proof of correctness
   (f) NQSBTLS
   (g) Amazon's s2n (signal to noise)

References

[GKW18] Rishab Goyal, Venkata Koppula, and Brent Waters. Collusion resistant traitor tracing from learning with errors. 2018.