urandom

vol.5

ＣＢＣＴＦ２０１７問題解説

-One of Three Billion-

Ｂｉｔｃｏｉｎによる
公平なＣＴＦ

Computer Security Magazine 2015 - 2017

目次

CBCTF2017 問題解説 - One of Three Billion

1 はじめに

2017 年 11 月 9, 10 日に、セキュリティカンファレンス CODE BLUE 2017 の併設企画として CODE BLUE CTF 2017 が開催されました。この CTF は CTF チームの binja と TokyoWesterns によって企画・運営されたもので、筆者（op）は binja のメンバーとして問題を一問提供しました。提供した問題はスマートカード（Java Card）のメモリダンプを解析するリバースエンジニアリング問題で、題名は One of Three Billion です。本稿ではこの問題について解説します。

2 出題内容

2.1 問題文

問題文は次の通りです。英語の問題文に続いて日本語訳[*1]を示します。

> I got a smart card that works as the client of challenge-response authentication and want to use it for my hacks. However, the card is locked by an unknown PIN and I have ran out the try limit :(Fortunately, (Yes, it's fortunate, at least for me) the card has some security flaws and I could get a partial dump of the internal memory. Could you analyze the dump and get a valid response?
>
> The challenge is 612c4445e078567c. The flag is "CBCTF{(hex response in lowercase)}". If you got response fa9da26c87659999, the flag would be "CBCTF{fa9da26c87659999}".

[*1] 競技中に提供されたのは英文のみで、日本語訳は本稿の為に書き起こしました。

```
0x014a: 11 6d 00    // sspush 0x6d00
0x014d: 8d 08 70    // invokestatic 0x0870
0x0150: 7a          // return
0x0151: 00          // nop
0x0152: 00          // nop
0x0153: 00          // nop
0x0154: 00          // nop
0x0155: 00          // nop
0x0156: 00          // nop
0x0157: 00          // nop
```

sspush命令と invokestatic命令の後ろに続くのはオフセット 0x0150の 0x7aで、これは return命令に対応する値です。return命令は voidを返す (返り値を返さないメソッドから返る) 命令ですから、この箇所は返り値 voidのメソッド内であって、ここで関数から返っていると思われます。return命令の後ろを見るとオフセット 0x0151–0x0157まで全て 0x00で、Java Card VM の命令だと仮定するとこの値は nop命令に対応しますので、もしこれが命令なら 7 バイトの間何も処理をしていないことになります。その上、nop命令が明けたオフセット 0x0158の値は 0xf0ですが、この値には対応する命令がありません。これらの特徴から、オフセット *0x0150*の *return*命令がこのメソッドの終端だと推定できます。

加えて、4.5で書いた通り ISO7816.SW_INS_NOT_SUPPORTED (0x6D00)が使われるのは多くが switch文の defaultケース内です。断定はできませんが、オフセット 0x014a が switch文の defaultケースであると仮定すると、オフセット *0x0000–0x014a*は *switch*文の *case*処理のバイトコードであると言えそう[*17]です。

次に、ISO7816.SW_WRONG_LENGTH (0x6700)と ISO7816.SW_SECURITY_STATUS_NOT_SATISFIED (0x6982)に着目してみましょう。オフセット 0x003b辺りから 0x0049辺りまで、立て続けに長さチェックとセキュリティ状態チェックをしているようです。この前後をバイトコードとして解釈して書き起こすと、次のようになります。

```
0x0036: 1f          // sload_3
0x0037: 10 08       // bspush 0x08
0x0039: 6a 08       // if_scmpeq 0x08
0x003b: 11 67 00    // sspush 0x6700
0x003e: 8d 08 70    // invokestatic 0x0870
0x0041: 7b 28 16    // getstatic_a 0x2816
0x0044: 8b 01 04    // invokevirtual 0x0104
0x0047: 61 08       // ifne 0x08
0x0049: 11 69 82    // sspush 0x6982
```

[*17] 5.2で挙げた 3 つの可能性の内、ここまでバイトコードを読み取った結果として可能性 1 は否定できそうに見えます。仮定が正しければ可能性 3 を否定出るので、可能性 2 を採用できます。

Bitcoinによる公平なCTF

1　はじめに

CTF (Capture The Flag) とはセキュリティに関する技術や知識を争う競技です。本稿では CTF のルールの 1 つである “jeopardy 形式” と呼ばれるものについてを対象に議論を進めます。jeopardy 形式の CTF においては、競技の参加者は暗号やバイナリ解析・フォレンジックといったジャンルごとに脆弱性を攻撃するなどして`FLAG{This_is_a_flag_word}`のようなフラッグワードと呼ばれる文字列を探します。そして、フラッグワードを運営のサーバーへ送信するとそのサーバーがフラッグワードが正しいかどうかを判定し、正しい場合にポイントが得られるという競技です。問題は 10 問程度出題され、24 時間といった制限時間内により多くのポイントを獲得したチームが勝利となります。世界的に有名な CTF では上位チームに賞金が与えられます。たとえば Codegate CTF Finals 2017 では 1 位のチームに 30,000,000 KRW が贈られましたし、また Google CTF 2017（Final）では 1 位のチームに 13,337 USD が贈られました[*1]。

本稿では Bitcoin を利用した新しい CTF の方法について述べます。筆者の提案する CTF にはいくつかの特徴がありますが、まず問題を解いたチームは正しい解答をしたとき直ちに賞金を得られます。従来の CTF は主催する団体の信用によって賞金が後日に受け取れることを保証していましたが、提案する CTF は Bitcoin といった暗号通貨の信頼によって賞金を受け取れることを保証します。またブロックチェーンに問題を解答したという情報を残すため、何もしなくともどのチームがどの問題を解答したかという情報が明らかです。

なお、本稿は Qiita で公開した記事 [1] を大幅に加筆・修正したものです。

[*1] これらの CTF では 2 位、3 位のチームにも賞金が贈られています。

2 本稿の構成

本稿の構成について説明します。まず 3 節にて提案する CTF の特徴を述べます。また 4 節で Bitcoin の構成に必要な暗号技術について詳細に説明し、次に 5 節で Bitcoin の仕組みについて解説します。そして 6 節で提案する CTF を解説します。7 節では不正対策といったより進んだ議論をします。8 節では提案する CTF の課題を紹介し、最後に 9 節でまとめを行います。

3 提案する CTF の特徴

本稿で提案する CTF には次のような特徴があります。

- 賞金が問題に解答した際に直ちに支払われる
- 賞金は Bitcoin で支払われる
- 制限時間が Bitcoin のブロックチェーンの長さに基づく
- 問題を最初に解答したチームのみが賞金を得られる

まず、参加チームが CTF 競技中に正しいフラッグワードを解答したとき、直ちにその問題の難易度と対応する額の Bitcoin を獲得します。従来の CTF では問題を解答してポイントを集め、そのポイントの多さで賞金が決まります。一方で提案する CTF にポイントはありません。したがって、賞金を最も獲得したチームを 1 番として順位を付けます。

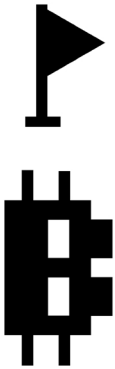
また提案する CTF は Bitcoin を利用する都合で、賞金が日本円などではなく全て Bitcoin で支払われます。ちなみに一般的な CTF は開催する国の通貨が利用されます。

そして、提案する CTF の制限時間は 24 時間といった時刻を利用せず、Bitcoin のブロックチェーンの長さによって決められます。つまりブロックチェーンの長さが n となったときに開始され、m $(m > n)$ となったときに終了するということになります。Bitcoin のブロックが作成されるためには約 10 分必要と言われています。したがって提案する CTF は約 10 分刻みの制限時間を指定できることになります。一般的な CTF はおおむね 24 時間や 48 時間といった時刻単位なので、1 分刻みのような正確な制限時間は必要ないと思われます。

また一般的に jeopardy 形式の CTF はある問題を何番目に正しく解答したかはポイ

urandom vol.5

発行者	urandom
表紙デザイン	秋弦めい
発行日	2017 年 12 月 29 日
バージョン	1.00（2017-12-25 17:57:55+09:00）
連絡先	`https://blog.urandom.team/`
印刷所	株式会社栄光



Happy Hacking