urandom

Computer Security Magazine

vol.7

目次

SECCON2018 国際大会決勝参戦記

1 はじめに

チーム urandom は、2018 年 10 月に行われた SECCON2018 予選で 9 位となったため、12 月 22, 23 日に秋葉原 UDX で行われた SECCON 国際大会の決勝に参加することとなった。本稿では、urandom が SECCON 国際大会の決勝に参加した記録を時系列で記していく。

2 チームメンバー

- 競技参加者 op, mayth, yuscarlet, yyu
- 参戦記執筆担当 fetastein, favcastle

3 競技・ルール解説

- 競技時間は 12/22 11:00 - 17:00 と 12/23 10:00 - 16:00 の合計 12 時間
- 競技形式は “King of the Hill”
  - 各問題を解くとフラグが得られる（1 つの問題には複数のフラグが存在することもある）。このフラグを解答サーバーに送信するとポイントが得られる。これによって得られる得点を **Attack Point (AP)** という。
  - 各問題毎に設定されている特定のファイルや Web ページに、各チーム毎に設定されている Defense Keyword を書き込むことで 5 分に 1 度、ポイントが得られる。この得点を **Defense Point (DP)** という。1 問あたりの Defense Point は 20pt. であり、複数のチームが同じ問題で Defense Keyword を書き込んでいる場合、20pt. を均等に山分けする（端数切り上げ）。Defense Keyword は 5 分に 1 度更新され、最新のものだけが有効である。したがって、継続的に Defense Keyword の書き込み操作をしなけれ

DEFENSE POINT

DP に関しては、立場が逆転し、oracle で pass してしまうような文字列を検出することが目的になる。oracle に対して行われる「攻撃」を、YARA と呼ばれるマルウェア検知ツールのシグネチャ記法でマッチさせ、その検出数によって DP を獲得できる。ただし、この DP は最多検出数を獲得したチームが総取りする。

4.2 弐

出題内容

紙幣認識のための画像認識システムを模したシミュレータをだますことが目的の問題。`1280x800` の画像をアップロードすると、それに対する結果として、次のような出力が返ってくる。

```
Statistics for each color: 54/11520
Recognition rate = 0.026042%  (1/3840)
```

これらの結果の意味するところは次のようになる（と思われる）。

- `Statistics for each color`（各色の統計）：判定に用いられている 3840 ピクセルのうち、RGB の値のそれぞれが閾値以内だった数。
- `Recognition rate`（認識率）：判定に用いられている 3840 ピクセルのうち、RGB の値のすべてが閾値以内だったピクセル数。

ATTACK POINT

認識率が 50%、60%、70% を超える毎に 500pt ずつの AP が得られる。

DEFENSE POINT

認識率が 45% を超えたチームのうち、最も高い認識率の画像をアップロードしたチームに 5 分毎の DP が 20pt 加点される。しかしながら、2 時間毎に認識率の閾値が更新され、徐々に難易度が上がっていくため、手際よく認識率を上げることができるシステムを構築できるかが鍵となる。

されていた The Finals 2018[*1]に執筆要員が行ってるのではと疑いを掛ける。

- 14 時ごろ四について 5 つある小問のうちの 2 問を解き終え、他の 2 問についても解ける見通しが立つ。残る一つのよく分からない小問に手を付け始める。
- 14:21 問題の趣旨をガン無視して、単色画像を投げまくって#282828 の画像を投げているとなぜか Recognition rate が 78% 程度となり、1500pt 分の Attack Point を獲得。これに対し、チームメンバーから「俺たちは雰囲気で CTF をやっている」の言葉が発せられる。
- 14:31 参戦記担当、会場到着。とりあえずスコアボードを撮る。

[*1] Magic: The Gathering のイベント。執筆要員は MtG フリークである。

展開署名: Folding Signature の進捗

1 はじめに

近年、PC やスマートフォン・コンシューマー機向けのゲームはほとんどに 3DCG が利用されています。ところが、中にはこういったゲームのソフトウェアに含まれる 3DCG のモデルデータをリバースエンジニアリング的な手法によって不正に取り出して利用する者もいます。このような不正にデータを盗む行為を止めるべきではありますが、3D モデルは最終的にグラフィックカードで読み取り可能な形になるため、不正利用を企てる者がグラフィックカードのように振る舞うデバイスまたはソフトウェアを用いた場合、いくらソフトウェア内のモデルデータを複雑に暗号化したとしても盗まれてしまいます。従って、我々ができることは盗まれることを防ぐのではなく、盗まれたことを “検出” することです。ある者が利用しているモデルデータが、その者が作りあげたものであるか、あるいは誰かから盗んだものであるかを判定する必要があります。最もナイーブな方法は、ステガノグラフィーを用いて 3D モデルデータに署名をすることです。3D モデルデータとは三角形の面をつなぎあわせることで作られた多面体であり、実態のデータ構造は三角形の頂点座標と、どの頂点が隣接しているかという情報の集合です。実用上は浮動小数点数で表現される頂点座標が多少ずれたところでほとんど見た目に影響しないため、複数の座標に署名をなんらかのエンコーディングで埋め込み、それを利用して誰が作成したモデルであるかを判定するという方法が使えます。一方で、このような手法は不正利用者が 3D モデルデータの頂点情報に何らかの加工をした場合は無力になります。そこで本稿は、筆者がこのような 3D モデルデータの不正利用を検出する新しい方法についての暫定的なまとめを述べます。

本稿は技術書典 4 にて配布したペーパーで述べた内容を基にしており、一部に重複した内容を含みます。これは記事の自己完結のためにあえて重複させたものです。また当時のペーパーでは「折り畳み署名」と表記していましたが、より適切と思われる「展開署名」と変更しました。

2 3DCG の基礎

本稿の具体的な内容へと進む前に、ここでは基本的な 3DCG に関する用語を整理しておきます。

まず 3D モデルデータとは三角形を繋ぎあわせて作られる**多面体**です。たとえばサイコロのような立方体も 6 つの面を持つ多面体となります。

モデルの表面には**テクスチャ**と呼ばれる 3D モデルの表面の質感や色といった情報をラスタ画像として用意しておきます。このテクスチャは 3D モデルデータの多面体の**展開図**のようなものとなっており、それを 3D モデルデータの表面に貼り付けることで最終的な 3D モデルが得られます。これにより、たとえば岩の凹凸といった複雑な表面を多面体として表現するといった手間を省略することができるほか、ある 1 つの 3D モデルデータに対して複数のテスクチャを用意することで湿った質感と乾いた質感の両方を表現する省略に利用されます。このテクスチャを作るためには 3D モデルデータの展開図のようなものを入手する必要があります。3D モデルの作者はそれに Adobe Photoshop といったドローソフトで色や質感などを書き込み、それを多面体に貼り付けることで表面の質感や色といった情報を持つ最終的な 3D モデルが完成します。

さて、この節ではまず多面体や展開図といった基本的な用語の定義を与えることとします。

定義 1. 多面体とは *3* 次元立体のことで、平坦でかつ全ての内側の角が 180° 未満である多角形の面のあつまりである。

このとき多面体の面と面の境界線のことを**辺**と呼び、辺が他の辺と衝突した点を**頂点**と呼びます。このあたりは日常的に利用する単語ですが、いちおう形式的な議論のため用語の定義をはっきりとさせておきます。

また、多面体はドーナツのように穴を作ることもできますが、穴も凹みもどちらも持たない多面体を特別に**凸多面体**と呼びます。

定義 2. 凸多面体とは、穴も凹みもどちらも持たない多面体である。

実際にゲームなどで利用する 3D モデルにおいては、ドーナツのように穴のある多面体や凹みがある多面体がありえると思います。もちろん本稿では多面体に関する議論をしますが、凸多面体と多面体に関してどちらの話をしているのか明瞭にするため、このようにそれぞれの用語を定義しておきます。

さて、次に展開図について定義します。

urandom vol.7

発行者	urandom
表紙デザイン	秋弦めい
発行日	2018 年 12 月 30 日
バージョン	1.00
コミット ID	934af80
連絡先	https://blog.urandom.team/
印刷所	株式会社栄光