CTF的 覚えておくべき暗号・攻撃とその見分け方

@elliptic_shiho

自己紹介

- 緑川 志穂(@elliptic_shiho)
- CTF(vuls, scryptos, Ph//shh/bin)
- Crypto, Pwn辺りをよくやります

CTFにおける暗号

- 暗号解読がメイン
  - 暗号化された文章を読む
  - 暗号化された通信のpcapが渡されたりも
  - 暗号化サービスが与えられて、saltやkeyを答えるような場合も

おしながき

- 古典暗号
- RSA
- ちょっとマイナーな暗号
- 新しい暗号
- エンコード
- ハッシュ関数

おしながき

- 古典暗号
- RSA
- ちょっとマイナーな暗号
- 新しい暗号
- エンコード
- ハッシュ関数

古典暗号

- 意味不明な文字列かつ英数字以外の文字がそれなりに英語の文章っぽいならまず間違いなくシーザー暗号
  - 単語だけ渡されるようなこともあるけどそういう時も大概がシーザー

古典暗号

- 全て意味不明な文字列
  - 特徴で見分ける
  - ADFGVの文字が目立つならADFGV or ADFGVX暗号
    - ADFGV以外にXを含んでいるかどうか
  - ADFGVX?暗号は必ずマトリックスが必要なので、それっぽい文字列が見えたらその時点で確定できるかもしれない

古典暗号

- ただの置換なら換字式暗号ソルバに流せば大体解ける
- 明らかにシーザーっぽくは無いがADFGVX?でもない、換字式暗号ソルバーに流しても不明
  - 大文字だけor小文字だけかつ特定のパターンを繰り返しているように見える?
  - こういうときはVegenere暗号を疑う

古典暗号

- 111523...のように2つの数値がペアになっているように見える数列(偶数長)
  - ポリュビオスの暗号表
  - 隣り合う数値で一意に変換可能なため、アルファベットに変換して換字式ソルバに流す

古典暗号

- 改行で区切られていてそれぞれの行に0-9の数値が書き込まれている
  - ガラケーのキーパッドに割り当てる

古典暗号

- いうて殆どの古典暗号はアフィン暗号なのでそれぞれ表し方を固定できる
  - 数も多いわけではないのである程度は総当りでもいいかもしれない

おしながき

- 古典暗号
- RSA
- ちょっとマイナーな暗号
- 新しい暗号
- エンコード
- ハッシュ関数

RSA

- CTFで出題される中では古典暗号の次に多い?
- 攻撃手法も数多く

RSA

- 素因数分解に帰着できる問題の場合
- そもそもそのRSA moduloは何ビット?
  - print len(bin(N)[2:])
  - 768bitであればweak rsaと呼ばれている素因数分解に成功しているものなので適当に探すだけで解けたりする

RSA

- たまに320bitなんてこともある
  - 素因数分解ゴリ押し問題の例
- msieveという便利なソフトを使いましょう
  - 320bitの素因数分解にi7+32G食わせて1.5h程度

RSA

- 大きい割に素因数分解しか手が無い場合
  - Fermat法かメルセンヌ素数を疑う

RSA

- Nを16進表示した時に、FFFF....00000....のように上位桁にFが、下位桁に0が続いているような形の特徴的な形をしているなら間違いなくメルセンヌ素数を使用した問題
  - 即座に解けます

RSA

- メルセンヌ素数とは
- 詳しくは触れませんが要するに2^m-1の形で表せる素数です
- 総当りの空間が非常に狭くなる

RSA

- Fermat法
- 結構出てくる
- (x+y)(x-y) = x^2-y^2と表せる事を利用し、(x+y)(x-y)をNと変換してN = x^2-y^2とし、yについて最初の式を解くと総当り空間が比較的小さめな式が得られる

RSA

- 素因数分解はこれぐらい?
- 一応例外的な問題もあります
  - ASIS 2015 Quals - cross check
  - Writeupが数式だらけですが面白い問題です
  - 基本的に暗号 = 数学だということを思い出します

RSA

- RSA自体への攻撃
  - 見分けはつきやすいです

RSA

- RSAのパラメータのうちeが異様に大きいもの
  - dが小さいことを疑う
  - Wiener's Attackと言います
- eが65537でないかつ大きいなら大体はこれ
  - 自作のライブラリでは判定条件を65537**2以上にしています

RSA

- 複数のデータセットが与えられている時
  - 中でもeがそれぞれ違うけどもnが全部同じ時、Common Modulus Attackという手法を用いることが出来ます
    - PlaidCTF 2015 Strength
  - また、データセットの中でも全てのeが同じ、かつデータセットの数 = eになるとき、Hastad's Broadcast Attackという手法が使える

RSA

- 去年のHITCONで出題されたrsahaという問題
- enc(m)とenc(m+1)が渡される

  → e, nが同じかつenc(m)とenc(am+b)が与えられている時、Franklin-Reiter Related Message Attackを用いることが出来る

RSA

- 複数のデータセットがある場合は素数を使いまわしている可能性も考慮する

  - p, q, rを用意してp*q, p*rを計算して持っている場合等

  - gcdを取ることでpが出るので素因数分解可能

RSA

- 細かい脆弱性を挙げていくと無数に存在する
  - Short Pad Attack
  - Low Public Exponent Attack
  - Low private Exponent attack
- 挙句の果て
  - Reconstructing RSA Private Keys from Random Key Bits by Nadia Heninger and Hovav Shacham.
  - http://cseweb.ucsd.edu/~hovav/papers/hs09.html
  - PlaidCTF 2014 for450 rsa

RSA

- 発展

  - CTFでは出てきませんが、最近はサイドチャネル攻撃が出てきています

    - CPUの発する電磁波やら電源電圧の変化を利用してオペコードを推測、実行している命令を特定して秘密鍵を盗む

  - RSAの開発者の一人であるA. Shamirによるものです

  - もし理論に興味が有るのであれば調べてみると腰を抜かすかもしれません

RSA

- それなりに研究の進んでる暗号でもあるので、常に目を光らせておくと良さ
  - 素因数分解技術も
    - もしかすると素因数分解技術はRSAと分けて調べたほうが良いかもしれない
- ツールを手になじませることも重要

おしながき

- 古典暗号
- RSA
- ちょっとマイナーな暗号
- 新しい暗号
- エンコード
- ハッシュ関数

ちょっとマイナーな暗号

- なにそれ知らねぇ!っていうタイプの暗号に対する対処
  - ~~英語版WikipediaのCryptosystemの関連項目を回るのが一番早い~~
  - 普段からの情報収集が大事

ちょっとマイナーな暗号

- ASIS 2015 Quals golden medal
  - Goldwasser-Micali暗号という暗号を使った問題
- 完全にわからなかったのでまずはGoogleで調べた
  - golden medal crypto blum等
  - 問題コード中のキーワードから拾えるものを拾った
  - 1時間ぐらい調べてやっと検索10ページ目ぐらいにそれっぽいものを発見

ちょっとマイナーな暗号

- 正直知らなかったら調べるのが早い
  - 解法載ってたりする
- Rabin暗号やElgamal暗号辺りは抑えておくべきだけども...
  - 各種暗号学に関する資料を普段から読み漁ることが大事

ちょっとマイナーな暗号

- VolgaCTF Crypto500 carry
- 謎の乱数生成器を使っていた
  - @_193sと叫びながら解いた
- 終了後に他チームのWriteupを見るとLFSRという単語
  - 線形負帰還シフトレジスタというものだそうです

ちょっとマイナーな暗号

- 乱数生成器の知識だけではダメ?
- どれにせよ図を書いてたら分かった
- ホワイトボードを活用しましょう

ちょっとマイナーな暗号

- マイナーな暗号は大体運営が楽するｔもとい検索力を見ている面が大きいと感じる
  - Recon力を磨く

ちょっとマイナーな暗号

- PlaidCTF 2015 Lazy
  - Merkle-Hellman Knapsack-Cryptosystemを使った問題
  - 結構昔にどのような暗号文でも破ることが可能なことがShamirによって証明されたため、廃れてしまった

ちょっとマイナーな暗号

- 故に、殆ど実装が存在しない
  - 同時にその攻撃手法の実装も存在しない
- 実装力勝負の問題だった
  - 自分も期間中は解けませんでした...

ちょっとマイナーな暗号

- マイナーな暗号だと論文を読んで解読処理実装することが多々ある
  - 普段からsage, python他ツールに慣れておくことが大事
  - 同時にプログラミング力も鍛える

おしながき

- 古典暗号
- RSA
- ちょっとマイナーな暗号
- 新しい暗号
- エンコード
- ハッシュ関数

新しい暗号

- 新しい暗号技術は殆どが楕円曲線を応用しています
  - (実装するのが)難しい・(理解するのが)難しい・(解読するのが)難しいの三拍子
- 数学アレルギーな方は諦めましょう

新しい暗号

- 楕円曲線暗号
  - いつぞやのSECCONで出た
  - あまりCTFでは見ないので今はスルーでもいいかもしれない
    - SSL/TLS系で見かけるかもしれない?

新しい暗号

- IDベース暗号
  - IDを用意してそれを楕円曲線上へ写像して云々
  - ペアリングという概念が必要
    - 楕円曲線のペアから有限体への写像
  - 数学的定義が面倒臭い
    - Laurent級数とか因子とかにﾋﾞﾋﾞｯと来る人なら面白いかも

新しい暗号

- 属性ベース暗号
- 放送型暗号
- 準同型暗号
- まだまだどんどん生まれてます

新しい暗号

- もし出題されたら?
  - それまでにある程度の知見が無いのであれば他の問題解いた方がいいかもしれない
  - 数学力に自信があり、取れるという確信があればどんどんチャレンジしてみてください

新しい暗号

- AES/DESについては専門にする人が一人いればそれだけで心強い
  - 仕組みが結構複雑なので、本腰据えてやらないとつらい
- AES/DESは攻撃というよりも性質を突く問題をよく見かける

新しい暗号

- 31C3 CTF Crypto hwaes
  - 外部ハードウェアにAESを実装したとのこと
  - AESのキーを設定して暗号化ができる
  - キーを見ることができる
  - os.urandom(16)をキーに暗号化されたフラグを見ることができる

新しい暗号

- AESやFeistel構造の暗号等比較的新しいブロック暗号にはラウンドという概念が存在する
  - ラウンドごとにキーを計算する
  - 最初のキーは与えた鍵

新しい暗号

- この問題では、現時点のAESキーを見ることが出来た。
  - 最初に設定したキーを一旦暗号化した後に見ると変更されていた
  - これは各ラウンドのキーの処理でそのキーのバッファを使いまわしていたのでは?

新しい暗号

- つまり、暗号化された後に見えるキーは最終ラウンドの鍵と取れる
  - 逆算できれば強そう
  - 出来ます

新しい暗号

- 攻撃の名前的には選択平文攻撃?
  - '0'の暗号化結果等も見るため
- どれにしてもAESのアルゴリズムを知らないと解けない問題
  - 専門がいると本当に心強い

新しい暗号

- AES/DES初めとした各種ブロック暗号は利用例も多く攻撃手法も出てきている
  - 差分解読法，関連鍵攻撃，選択平文攻撃，線形攻撃、...
  - 詳しくはこちらを。

https://www.jstage.jst.go.jp/article/essfr/7/1/7_14/_pdf

新しい暗号

- 余談: つい最近MISTY1暗号に関してのより効率的な攻撃法が発表されました
  - http://eprint.iacr.org/2015/682.pdf
  - Integral Attackという手法を用いているそうです

新しい暗号

- 日々こうやって増えている攻撃法や暗号を理解できるだけの数学力が欲しい
  - 基礎知識となる周辺技術についても
  - 一朝一夕でなんとかなるものでもない

新しい暗号

- http://eprint.iacr.org/
  - 暗号関連の論文が見れます
    - arXivのようなもの
    - ここ半年の論文の中でRSAに関するものだけでも9件ある
      - 暇な時に目を通す勢い

おしながき

- 古典暗号
- RSA
- ちょっとマイナーな暗号
- 新しい暗号
- エンコード
- ハッシュ関数

エンコード

- 見落とされがちなのでついでに
- base64だけじゃないですよ!

エンコード

- Base64
  - 言わずもがな
- Base32
  - あまり知られていない?
  - 大文字と数値と=しか存在しない

エンコード

- ROT13
  - 13文字ずらしのシーザー暗号
  - エンコードでもある?
- ROT5
  - 数値のシーザー

エンコード

- ROT47
  - 記号も含めたシーザー
- ROT13/47
  - 2バイト文字に対応したもの

エンコード

- uuencode
- ish
  - 両方昔から使われているバイナリ<=>テキストエンコード
  - たまーに出てくる
- mode ??? <data>の文字が見えたらまずuuencode
- ishはそもそも滅多に出るものじゃない

おしながき

- 古典暗号
- RSA
- ちょっとマイナーな暗号
- 新しい暗号
- エンコード
- ハッシュ関数

ハッシュ関数

- ここでは暗号学的なハッシュ関数を見ます
- AdlerﾅﾝﾁｬﾗとかCRCは正直なところ見ない
  - CRCは暗号以外の利用が多いのでそれはそれで知識程度に知っていても良さ

ハッシュ関数

- MD5
  - 衝突耐性がない
  - それなりに逆算サービスも普及している
    - 実務で使うには心許なくなってきた

ハッシュ関数

- SHA-1
  - 衝突耐性は...ある?
  - MD5ほどではないけども、それなりに逆算データベースが存在
  - CRYPTRECの 運用監視リスト入りしてます

ハッシュ関数

- SHA256, SHA512
  - SHA-2と言われる種類のハッシュ
  - 今のところは安全
  - 「ここは解ける場所じゃないよ!」という目印か、Length-Extensionのためのもの

ハッシュ関数

- SHA-3
  - まだ仕様策定とかそんな感じ
  - この先出てくるかもしれない
  - 今のところ脆弱性という脆弱性は見つかっていない?
  - 今後に期待

まとめ

- 覚える量,実践する量が非常に多い
- どうしても数学が必要
- 専門職を一人用意しておくだけで違う
- CTF的な暗号の考え方は微妙に理論寄りの考え方とは違う

参考文献

- クラウドを支えるこれからの暗号技術 光成 滋生著 秀和システム

  ↑レビュワーとして参加してます

- 暗号理論と楕円曲線 辻井 重男,笠原 正雄,有田 正剛,境 隆一,只木 孝太郎,趙 晋輝,松尾 和人 著

- 暗号理論入門 原書第3版 Buchmann,Johannes A 著 林 芳樹 翻訳

参考文献

- どれも高いのでお財布にはご注意を...
- 大体全部3000〜4000円です

ありがとうございました。