コンピュータ概論 A/B

-- Malware に注意/暗号化 --

数学科 栗野 俊一 (TA: 浜津 翔 [院生 2 年])

伝言

私語は慎むように !!

- 席は自由です (出席パスワード : 20141007)
  - できるだけ前に詰めよう
  - 教室にきたら直ぐにやる事
    - PC の電源 On / ネットワーク接続 / Web を参照する / skype を起動する
- 色々なお知らせについて
  - 栗野の Web Page に注意する事

    http://edu-gw2.math.cst.nihon-u.ac.jp/~kurino
- 今週は「補習」はありません

呼出し

- 履修登録が少ない
  - 4008 石崎さん 23
  - 4018 岡田くん 24
  - 4023 加藤くん 21 (-9)
  - 4038 黒澤さん 24
  - 4041 小嶋くん 21 (-9)

本日(2014/10/07)の予定

- 本日(2014/10/07)の予定
  - マルウェア/セキュリティ/暗号化
    - 暗号化と TrueCrypt
- 実習
  - [演習 1] TaskManager の利用
  - [演習 2] TrueCrtpt のインストール
  - [演習 3] TrueCrtpt の使い方
  - [演習 4] 課題の作成

本日の課題 (2014/10/07)

- 前回 (2014/09/30) の課題
  - 次のファイルを excel で作成して CST Portal に提出してください
    - ファイル名 : 20140930-QQQQ.xlsx (QQQQ は学生番号)
    - 内容 : 自分の成績の偏差値は ?
    - 形式 : xlsx 形式 (sample-20140930.xls を参照)
- 今回 (2014/10/07) の課題 (2 つある)
  - 次の TrueCrypt のボリュームを作成し、CST Portal から提出
    - 表題 : TrueCrypt のボリュームファイルの提出
    - ファイル名 : 20141007-QQQQ.tc (QQQQ は学生番号)
    - 詳しくは、配布した sample-20141007.tc の内容を参照
  - 自分の pgp の key pair を作り、その公開鍵を提出する
    - 表題 : pgp の公開鍵
    - ファイル名 : 20141007-pubkey-QQQQ.asc (QQQQ は学生番号)

PC セキュリティ (復習)

- PC のセキュリティを守ろう
  - 知る事：最新の知識を身に付ける
    - cf. セキュリティホール Memo
  - 危険をさける
    - セキュリティホールをなくす (update する)
    - 対策ソフトを入れる
  - 善後策を練る (怪我をしても血がでなければ良い)
    - 暗号化を行う：情報が流出しない
    - バックアップを行う：情報が消失しない
- 結局は、意識の問題
  - 恒常的な努力が必要
    - 最新情報の入手/適切な判断/効果的な対策の実施

マルウェア

- □ マルウェアとは(What)
  - ○ 悪意のあるソフトウェア
    - ▹ (コンピュータ所有者でなく)作成者の都合で動く(悪さをする)ソフト
    - ▹ 利用者の情報を勝手に送信する/宣伝を表示する/悪い事の踏台になる
  - ○ [反] 通常のソフトは、コンピュータ所有者の都合で、利用される
    - ▹ TeX 文章を Typeset したい → PLaTeX システムをインストール/利用
    - ▹ 数式処理をしたい → Mathematica をインストール/利用
- □ マルウェアもソフトウェアの一種
  - ○ 「動かない」限り「ただのファイル(ディスクの肥やし)」でしかない
    - ▹ 「起動」すると「悪さ」をする事になる
    - ▹ 勝手に起動する / 利用者を騙して、起動するように誘導する事が多い
  - ○ [反] 通常のソフトは、コンピュータ所有者が利益を得るために意識的に起動する
- □ マルウェアの分類
  - ○ コンピュターウィルス : 勝手にインストールされる/他の PC に感染する
  - ○ トロイの木馬 : こちらから何か(Web Acccess)をすると罠に掛けて、マルウェアを起動
  - ○ スパイウェア / キーロガー : 個人情報を勝手に送信してしまう
  - ○ アドウェア : 此方が望んでいない宣伝表示を勝手に行う
  - ○ 他にも色々 : 詳細は調べよう (人の悪意とはいやはや..)

マルウェアをさけるには

- □ 何故マルウェアに感染してしまう (Why)
  - ○ コンピュータの危険対策状態に問題がある
    - ▹ セキュリティホールを放置 (Windows Update / ソフトアプデートをサボる)
    - ▹ ウィルス対策ソフトがない/情報が最新でない (最低限 MSE を..)
  - ○ 利用者が騙されてしまう
    - ▹ 脅迫型 : Web アクセス中に突然「危険だ、対策ソフトを入れろ」といわれ..
    - ▹ 利益誘導型 : このソフトを入れると便利になるよ..
- □ マルウェアをさけるには (How To)
  - ○ ウィルス対策ソフトのシグネチャ(ウィルス手配書)データ更新 / ソフトの更新
  - ○ 安易にソフトウェアをインストールしない
    - ▹ そのソフトが安全かどうかを「確認して」からインストールする
    - ▹ その名前で「ググれば、安全かどうかを判定」する事ができる
- □ マルウェアに「やられているのでは」と思った時は .. (When)
  - ○ 挙動が普段と異る : マルウェア感染を心配してみよう..
    - ▹ 妙に遅い/意図しないサイトのページが表示される/頻繁にエラーが表示される
    - ▹ メールを送ったら、相手から「ウィルス付きのメールが届いた」といわれた
  - ○ 情報を収集しよう
    - ▹ 詳しい人(友達/先輩/親/栗野 !!)に相談 / ググってみよう..

実習 1: TaskManager の利用

- [実習 1-1] TaskManager の利用
  - [Ctrl]+[Alt]+[Delete] でメニューを表示させる事ができる
  - 「タスクマネージャの起動(T)」を選ぶと、タスクマネージャが起動する
  - 「プロセス」タブを選択すると、色々のプログラムが動いている事が解る
    - [注意] より高度(危険)なマルウェアの技術に rootKit を利用したものがあるが、これは、これでは発見できない
- [実習 1-2] プロセスの内容の確認
  - プロセスの一覧で表示されている
  - 適当な名前を選んでググってみる(ファイル名で検索している事に注意)
    - 例 1:「skype.exeとは」で検索 → 当然「スカイプ」のソフトである事が解る
    - 例 2:「dwm.exeとは」で検索 → Desktop Window Manager である事が解る
  - 場合によっては、「マルウェア」である事が判明する事もある
    - [注意] 正常なファイルの名前を、マルウェアが勝手に名乗っている可能性がある

暗号化

- □ 暗号とは
  - ○ コーディングの一種
    - ▷ なんらかの「規則」で、「情報を表現する」方法
    - ▷ その「規則」が解らないとそれが「表現している情報」が得られない
- □ 暗号の用語
  - ○ 文(ファイルの形式)
    - ▷ 平文：調べれば、「それが表現する内容」が得られる
    - ▷ 暗号文：その表現(ファイル)だけでは内容を知るのが大変困難な表現(鍵があれば見れる)
  - ○ 変形(操作)
    - ▷ 暗号化(encode)：「平文」を「暗号文」にすること
    - ▷ 平文化(decode)：「暗号文」を「平文」にすること
  - ○ 鍵(表現の規則を決め、情報を秘密にするための「種」)
    - ▷ 暗号化したり平文化するために、必要な情報(cf. パスフレーズ)
    - ▷ 対称鍵暗号方式：暗号化と平文化で「同じ鍵」を利用する (TrueCrypt)
    - ▷ 公開鍵暗号方式：暗号化と平文化で「異なる鍵」を利用する (gpg)

公開鍵暗号方式

- 対称鍵暗号方式の問題点
  - 暗号の利用目的は？
    - 通信経路が安全でない → 通信の内容を暗号化して秘密に情報交換したい
  - 対称鍵暗号方式の特徴：送信元と送信先が同じ鍵を持つ必要がある
    - 鍵をどうやって通信相手に渡せばよいのか？(通信経路が安全でないのに)
- 公開鍵暗号方式の利点
  - 暗号化と平文化の鍵が異る
    - 送信元に必要な物：暗号化鍵(Public Key) / 誰が知っていても良い(公開鍵)
    - 送信先に必要な物：平文化鍵(Privacy Key) / 自分だけの秘密(秘密鍵)
  - 公開鍵から秘密鍵を知る事ができなければ安全
- 公開鍵暗号方式を用いた暗号通信
  - 準備 (1 度だけやればよい)：自分用の鍵ペア (秘密鍵+公開鍵) を作る
    - 通信相手に自分の「公開鍵」を送る
    - 公開鍵はバレてもよいが、「自分の物」である事は「別に保証する」必要がある
  - 暗号通信
    - 通信相手に、「公開鍵」を利用して、メッセージを暗号化して送ってもらう
    - 自分の「秘密鍵」でメッセージを平文化すれば、メッセージを見る事ができる

TrueCrypt

- TrueCrypt とは
  - ファイルの「暗号化を行う」ためのツール
    - ファイルを暗号化して入れる「箱(暗号化ボリューム)」が作れる
    - 暗号化ボリュームを作る時にパスフレーズを設定する
    - 暗号化ボリュームは暗号化されていてパスフレーズを知らないと見れない
  - 暗号化ドライブを作る事ができる
    - 暗号化ボリュームはマウントできる
    - マウントするには、作成した時に利用したパスフレーズが必要
    - マウントすると、ドライブ(USB メモリみたいなもの)になり、普通にファイルが記録できる
    - 利用しない場合はアンマウトしておく
- 暗号化ボリュームとパスフレーズ
  - 暗号化ボリュームは暗号化されているので、普通に交換してよい
    - メールや skype で送ったり web で公開してもよい
  - 暗号化ボリュームの内容を参照するには、パスフレーズが必要
    - パスフレーズは、本当は「安全な方法」で送る必要がある
    - 今回は、skype を使うが、本当は良くない (skype が覗見される可能性がある)
    - 理想は「手渡し」だが...

Truecrypt の仕組(マウント/アンマウント)

マウントする

→

←

実習 2: TrueCrypt のインストール

- [実習 2.1] TrueCrypt のインストール
  - TrueCrypt のインストールファイルのダウンロード
  - TrueCrypt のインストール
    - 右クリックメニューから、「管理者として実行」すること
  - TrueCrypt の言語ファイルのダウンロード
  - TrueCrypt の言語ファイルのインストール
    - Language.ja.xml を c:\Program Files\TrueCrypt にコピーする
- [実習 2.2] TrueCrypt の動作確認
  - sample-20141007.tc をディスクトップにダウンロード
  - TrueCrypt を起動 (sample-20141007.tc をダブルクリックでもよい)
    - sample-20141007.tc を d: にマウントする
    - パスフレーズは skype で伝達
    - ファイルの中身を確認の事 (課題に関する情報がある)

実習 3: 自分用のボリュームを作る

- [実習 3.1] 新規ボリュームファイルの作成
  - TrueCrypt で、新規ボリュームファイルを作成する
    - サイズ : 1 M byte / ファイル名 : 自由 / パスフレーズ : 自分で決める
- [実習 3.2] 内容の作成
  - TrueCrypt で、新規ボリュームを e: マウントする
  - e: にテキストファイルを作成し、メッセージを入れる
  - TrueCrypt で、新規ボリュームをアンマウント
  - skype で、ボリュームファイルとパスフレーズを友人におくる
- [実習 3.3] 手に入れたファイルの確認
  - 手に入れたファイルをパスフレーズを利用して e: にマウントする
  - 内容を確認する
  - e: をアンマウントする

実習 4: 課題の提出

- [実習 4.1] 新規ボリュームの作成
  - TrueCrypt で、新規ボリュームを作成する
    - サイズ / ファイル名 / パスフレーズ : message.txt を参照
- [実習 4.2] 課題の作成
  - TrueCrypt で、実習 4.1 のボリュームを e: にマウント
  - e: に次の二つのファイルを作成する (message.txt を参照)
    - message.txt
    - password.txt
  - e: をアンマウントする
  - 20141007-QQQQ.tc を CST Portal に提出

実習 5: Kleopatra の利用 (1)

- [実習 5.1] Kleopatra のインストール
  - gpg4win-2.2.2.exe をダウンロードし、実行する
    - Kleopatra がインストールされる
- [実習 5.2] Kleopatra の起動 : [スタート] → [Kleopatra]
- [実習 5.3] 自分の Key Pair の作成
  - [File] → [New Certificate..] → 上をクリックして → [Next]
    - Name : 名前 / Email : NuApps のメール / Comment : 不要(好きにして良い) → [Next]
    - [Create Key] → パスフレーズ(自分で決める)(→それでもこれを使う)→パスフレーズ(先刻決めたもの)
    - [Make a Backup Of Your key Pair] → ASCII armor にチェック →
    - フォルダを指定→[ディスクトップ]→qqqq→[Enter]→[OK]→[OK]→[Finish]

実習 5: Kleopatra の利用 (2)

- [実習 5.4] 自分の公開鍵の取出し
  - [自分の鍵を選択]→[Export Certificates]→[ディスクトップ]→[保存]
    - 出来たファイルを skype 等で、友達に送る / skype で送ってみよう
- [実習 5.5] 他人の公開鍵の取り込み
  - 鍵ファイルを Kleopatora に Drag&Drop する → [Import Certicates] → [OK]
    - 栗野の公開鍵(kurino-pubkey.asc) をダウンロードして取り込む
- [実習 5.6] 他人に暗号ファイルを送る
  - 平文のファイルを作る → D&D → [Encrypt] → [Text output ASCII] → [Next]
    - [送り先を選ぶ] → [Add] → [Encrypt] → [Finish]
    - その人に暗号化したファイルを送る / skype で 栗野に送ってみよう
- [実習 5.7] 自分に届いた暗号ファイルの平文化
  - 暗号ファイルを D&D → [Decrypt] → [Decrypt] → パスフレーズ
- [実習 5.8] 友人同士で、暗号化したファイルを交換してみよう