セキュリティを考えたUAC

はなおか じった

おことわり

- 開発者向けではありません
- なぜUACなのかを、知ってください

アジェンダ

- MS-DOSの遺産(legacy)
- NT Technology
- Windows Vista – User Account Control

用語

- ユーザ…Windows を操作する人
- アカウント…Windows にログオンするための識別子
- ユーザ アカウント…ユーザが通常使用するアカウント
- 管理者…Windows の設定を変更する権利を持ったユーザ
- 管理アカウント…Windows の Administrators グループに属するアカウント

DOS, Windows 9x の弱点

- パーソナル（個人の）用途
  - ユーザ＝管理者
  - ひとつのアカウント＝管理アカウント
- デフォルトで出来る
  - 変更しなければセキュリティ ホール
  - 穴がたくさん！！

管理アカウント常用の危険

- ウィルス被害
  - 管理権限で動作する
  - システム領域へもアクセスできる
- 情報漏洩
  - すべてのファイルにアクセスできる
  - アクセス権限を書き換えることも出来る

デフォルトの危険

- 知識の差…「無知」の恐怖
  - 「簡単」が売り
  - 無設定で、「何でも出来る」
  - 難しいから使わない
  - 使わないから設定しない
  - 設定しないから穴となる

識者にとってアタック　ポイント

Microsoft の対応（UAC 以前）

- Windows NT
  - Users グループと、Administrators グループ
  - システム領域へのアクセスを制限
  - ファイル アクセス権を編集可能
  - Administrator のスペル変更
- セキュリティ ガイド
  - http://www.microsoft.com/japan/technet/security/prodtech/windows2000/win2khg/01intro.mspx
  - http://www.microsoft.com/japan/technet/security/prodtech/windowsxp/secwinxp/xpsgch01.mspx
  - http://www.microsoft.com/japan/technet/security/prodtech/windowsserver2003/W2003HG/SGCH00.mspx

Mic 点

- 初 のアカウントが管理アカウ
  - 普通 ザはこれしか使わない
  - Usersクル アカウントの制限が大きい
  - 管理アカウン り換えが困難
  - Administ 手かと思う？
  - デフォルトで「OK」

セキュリティ ガイドが TechNe ろ

- のガイドがない（簡単なもの
- 到達

抜本的対策が必要

Trustworthy Computing

４つの柱

- セキュリティ
- プライバシー
- 信頼性
- 誠実なビジネス

http://www.microsoft.com/japan/presspass/cp/mskk02.aspx

３つの安全原則

- 配置の安全
- 設計の安全
- デフォルトの安全

http://msdn2.microsoft.com/en-us/library/aa480150.aspx

3つの安全原則:配置の安全

- 署名(Code Sign)
  - 64bitバージョン…ドライバは署
  - 一般アプリ…最悪、自己証明書
  - UACメッセージ…色
    - 赤　ブロック
    - 青緑　マイクロソフト製
    - 灰　証明書ストアにあり
    - 黄　証明書ストアにない

将来、管理動作には
署名が必要

UAC チームのブログより
http://blogs.msdn.com/uac/archive/2006/06/19/637181.aspx

3つの安全原則：設計の安全

- 管理特権を求めない

  開発者へのお願い

  – 最小特権の原則

- HKLMハイブ、Program Filesに書き込まない

  – **SHGetFolderPath**を使用し、XML形式で

- 標準ユーザ

  VB.NETならMyクラスから

  – 動作を確認する

3つの安全原則:デフォルトの安全

- 最小機能のみ有効
  - 通常不要な機能はOFF
- 最小限の権限で動作
  - 不用意な昇格を予防
- ユーザに同意を求める
  - ユーザの意図か確認する
- Administratorを無効化
  - 管理アカウントのアカウント名が予測不能

これこそ
UACの目的

開発者の目から

- UACって、どうよ？
  - 面倒くさい
  - いっそOFFにしてやれ！

それ、間違いです！

使用者が関知しない
管理動作を抑制

アプリケーションをUACに対応する

- 新規の場合
  - ユーザ権限で動作する
    - SHGetFolderPath
    - マニフェストで「昇格
  - 管理特権が必要なこ
    - シールド アイコンを

マニフェストを埋め込む

- http://www.atmarkit.co.jp/fdotnet/dotnettips/235embmanifest/embmanifest.html
- http://msdn2.microsoft.com/ja-jp/library/ms235591(VS.80).aspx
- DLL は、Side-by-Side のために埋め込んでおく

り出す

呼び出せない

- C++/CLIで呼び出しルーチンを作る
- 別アプリに分けて呼び出す

ShellExecute(hWnd, "runas", filename, param, directory, nCmdShow);

- プロセスを昇格して再起動する

http://blogs.msdn.com/tsmatsuz/archive/2007/01/25/windows-vista-uac-part-2.aspx

悪しき”習慣”の排除を！

- 互換性の問題
  - XP以前の「こういう動きだった」が、
    - delete したメモリはクリアされる！？
    - グラフィックは黒で初期化される！？
  - 特権が必要な動作がブロックされ
    - 不正なメッセージや DLL Injection の排除
    - ユーザが関知できない昇格動作を禁止
      （管理特権から一般に偽装し、偽装解除は可能）
  - マニフェストの優先順位
    - XP は、外部マニフェストが優先
    - Server 2003 以降は埋め込みマニフェストが優先

もちろん、
単なるバグ

！要注意！
何をするのか
何をしたいのか
吟味すること

Web情報案内

- MVP山崎明子さんによるWebキャスト
  - http://www.microsoft.com/japan/msdn/windowsvista/webcasts.mspx
- UACチー
- Win
- ベ
  - http://msdn.microsoft.com/en-us/library/aa480150.aspx

2007/03/01 現在
β版を元にした情報しかない
4月以降増えてます

課題も残るUAC

- 昇格したプロセスから分岐するプロセス
  - 昇格したまま
  - マルウェアが分岐される可能性
- DLLには昇格情報がつけられない
  - DLLの実行は呼び出し元に依存する
- 証明書の詐称が可能
  - InstallShield Ver.12 によ
    - インストールと見せかけ、マ
  - RunDLL32 や、cmd.exe コマンド
    - マイクロソフトの証明書で昇格許可を求める！！

SxSは埋め込んでおかなければならない

対策片手落ち！！
コマンド プロンプトから runas はブロックされる

UAC 一番の課題

開発者が情報を握っている

- 開発者が「これから昇格します」でいいの？
- システムが、「させていいの？」じゃない？

コード例紹介

- サンプルは、あくまで「見本」
- 何をするコード？
  何をしようとしている？
  考えることが必要！！

- 詳しいことは、
  中さんのセッションを待て！！

おまけ

- MVPになりましょう！！
  - バグかな？
    - まずは掲示板（MSDN
    - バグだと確定したらプロ
  - 製品に対する要望
    - MVPは特別なコネクションがあります
    - まず、MVPを説得してください
  - コミュニティで解決できなかった問題
    - MVPは特別なインシデントがあります
    - MVPに興味を持たせてください

開発製品について、
MVPは強権を持っています！

Microsoft

ready
for a new day

Microsoft Office

Windows Vista

Microsoft Exchange Server 2007