Jouons avec des clés USB

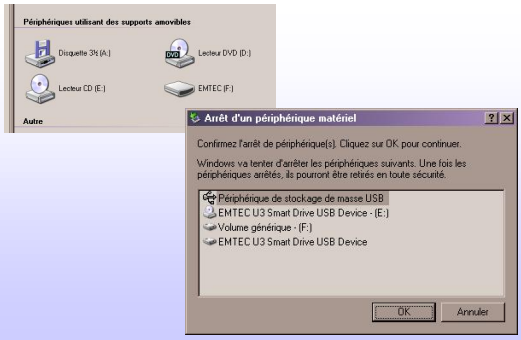
Pierre-Yves Bonnetain
py.bonnetain@ba-cst.com

Les clés USB « U3 »

Organisation de la clé

- Simuler un CD.
- Partition spéciale, lecture seulement, sur la clé (environ 6 Mo).
- Contient des programmes et un autorun.inf.
- Une fois branchée sur un ordinateur
  - un lecteur CD,
  - un disque amovible.

Sur le poste de travail



Sous Linux...

- La partition « CD-ROM » est invisible, sauf si le pilote SCSI est bien configuré :
- `[*] Probe all LUNs on each SCSI device`
- `(CONFIG_SCSI_MULTI_LUN=y)`

```
usb 1-1: Product: U3 Smart Drive
usb 1-1: Manufacturer: EMTEC
usb 1-1: SerialNumber: 07000777112B0C48
usb 1-1: configuration #1 chosen from 1 choice
Initializing USB Mass Storage driver...
scsi0 : SCSI emulation for USB Mass Storage devices
USB Mass Storage support registered.
    Vendor: EMTEC     Model: U3 Smart Drive    Rev: PMAP
    Type:   Direct-Access                      ANSI SCSI revision: 00
    Vendor: EMTEC     Model: U3 Smart Drive    Rev: PMAP
    Type:   CD-ROM                             ANSI SCSI revision: 00
```


La partition CD

Le LaunchPad

- Simule un menu « Démarrer »
- Fonctions de configuration
  - Paramètres
  - Ajout de programmes U3-isés
  - Mot de passe de la partition Flash (à creuser...)

Mise à jour du CD

- En théorie :
  - Ancienne version (LPInstaller.exe)
    - Image cruzer-autorun.iso
    - cherche l'image en local (dans le répertoire où se trouve LPInstaller.exe) ou
    - la télécharge depuis updates.u3.com
  - NOTE : LPInstaller.exe est indisponible sur le site de sandisk.
  - Installation automatique sur la clé
- Possibilité de jouer avec le DNS pour diffuser une image « personnalisée »

Mise à jour

- Le LaunchPad dispose d'une fonction de mise à jour automatique.
- Exécutée au branchement de la clé (à l'initialisation du LaunchPad ?)
- Paramètre UpdatesAutoCheck (flash:/system/apps/lpgdb.xml)
- La clé se met à jour sur le site updates.u3.com
- En pratique :
  - A voir... lors de la prochaine mise à jour.

Protocole de mise à jour

- GET /lpupdate (+ paramètres)
- Les paramètres amusants :
  - unique et instance : identifiants de la clé ?
  - capacity et used : volume total de la clé, volume utilisé effectivement sur la partition flash.
  - apps : nombre d'applications « u3-isées » installées.
- Récupère un fichier XML définissant la mise à jour (ou son absence)

Fichier de mise à jour

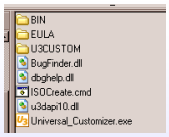
```
<u3updatemanifest>
<LPUpdateAvailable>0</LPUpdateAvailable>
<LPUpdateVersion></LPUpdateVersion>
<LPUpdateProtocolVersion>1.0
</LPUpdateProtocolVersion>
<AddressURL></AddressURL>
<description></description>
<ReleaseWebPageURL />
</u3updatemanifest>
```


Universal Customizer

- www.hak5.org/packages
- Version modifiée de LPInstaller, qui permet
  - De créer une image ISO9660 avec « ce que l'on souhaite dedans »
  - D'écrire une image sur la partition CD d'une clé U3
- ATTENTION :
  - parfois ça marche, parfois moins (clés SanDisk // clés EMTEC ?)
  - risque de perte des données de la partition flash

Organisation et utilisation

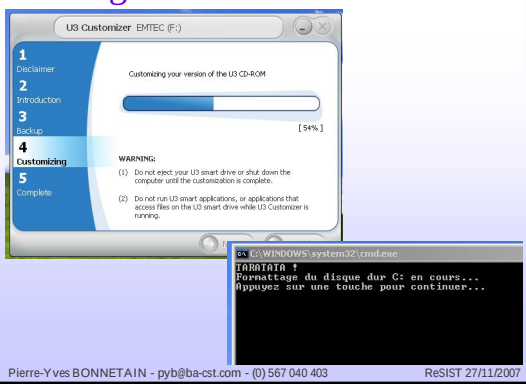
- Procédure complète :
  - Placer les fichiers dans le répertoire u3custom.
  - Exécuter ISOCreate.
  - Puis Universal_Customizer
- Procédure abrégée :
  - Placer une image ISO9660 nommée U3CUSTOM.ISO dans le répertoire BIN
  - Exécuter Universal_Customizer.



Déroulement

- Recherche d'une clé USB U3.
- Sauvegarde des données de la partition flash (fichier ZIP avec mot de passe demandé à l'utilisateur).
- Formattage de la partition CD.
- Ecriture de l'image U3CUSTOM.ISO.
- Restauration des données de la partition flash.
- NOTE : le programme en AUTORUN peut être exécuté durant la procédure !

En images

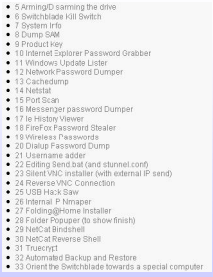


Hacksaw

- wiki.hak5.org/wiki/USB_Hacksaw
- Extraction automatique du contenu de toutes les clés USB connectées au système « infecté ».
- Envoi des documents vers un compte Gmail.
- Propagation possible vers une autre clé U3.
- Utilise USBDumper, Blat, Stunnel (et Gmail).

SwitchBlade

- wiki.hak5.org/wiki/Switchblade_Packages :
  - ensemble de programmes que l'on peut ajouter sur la partition CDFS
  - Avec des fonctionnalités très diverses



Des questions ?

- Le PDF de la présentation est disponible (sur une clé USB…)