Juste une imprimante ?

Imprimantes et autres MFD
(Multi Function Devices)

Objectif de cette présentation

- Avertir des menaces
- Identifier les vecteurs d'attaque
- Mettre en avant les contre mesures possibles
- Ouvrir les pistes des futures avancées du domaine

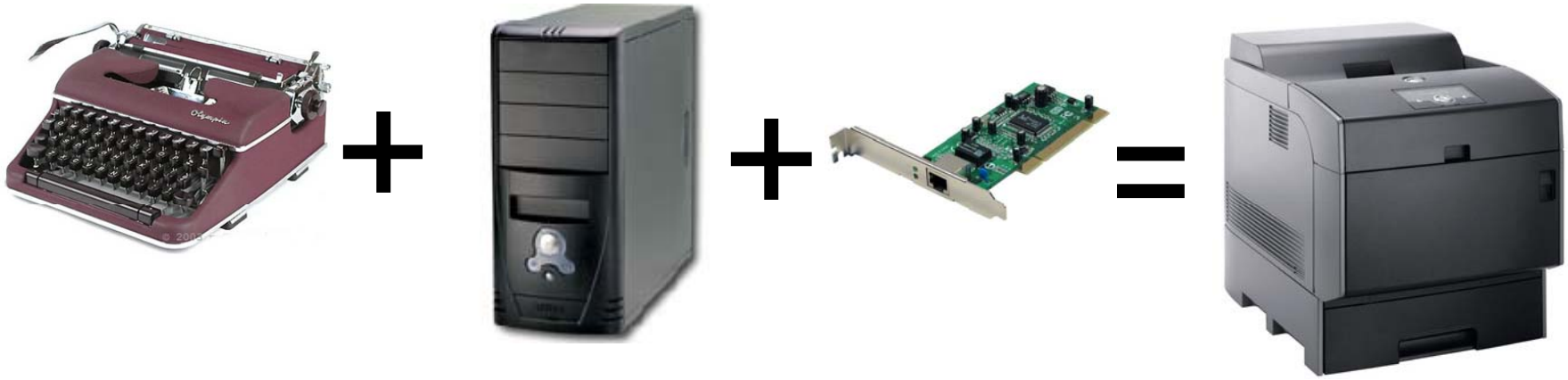
Rapide inventaire de M.F.D

Nous parlerons aujourd'hui de **M**ulti **F**unction **D**evices (MFD, MFP, AIO)

- Imprimantes, Scanners, Photocopieurs, Fax, Caméras IP
- Caméra réseau, PABX, équipements métiers

Tous ces équipements sont devenus pour la plupart de vraies machines, avec une interface réseau.

Coupons court à certaines idées reçues



Rapide état des lieux

Une imprimante réseau est un ordinateur qui imprime mais ne possède pas de clavier, d'écran ou de souris. Le reste est identique donc on retrouve les risques « classiques » de la sécurité informatique :

- Exploitation de vulnérabilités
- Contournement d'authentification
- Ingénierie sociale
- Backdooring, cheval de Troie, etc…

Avec toutefois des différences notables …

Quelques différences notables

- Les MFD disposent de niveaux de sécurité archaïques
- Ceux-ci n'évoluent jamais (qui met à jour le firmware de son imprimante ?)
- Vous connaissez-vous un antivirus pour imprimante ?
- Aucune place n'est faite aux imprimantes dans les PSSI
- Les normes ISO 2700x, SoX et autres n'abordent même pas le sujet
- En cas de compromission du réseau, l'imprimante est au cœur du LAN mais dessus de tout soupçon et pourtant…

Quelques risques spécifiques aux MFD

En plus de tous ces « risques » génériques, certains sont spécifiques aux imprimantes :

- Ces équipements disposent tous d'un serveur HTTP, avec une conception de sécurité anté diluvienne qu'il est possible de contourner et d'exploiter (Drive-by-downloads)
- Un écran LCD d'imprimante est facile à détourner pour duper l'utilisateur en l'incitant à se rendre à une URL ou à appeler un faux support utilisateur
- Une imprimante voit passer tous les fichiers, ce qui centralise la collecte pour un attaquant
- Le tout dans le réseau local, sans filtrage la plupart du temps

Attaques sur les MFD : Dell 1710n

Nous avons maltraité une imprimante de notre réseau, de type « Dell 1710n »

Hardware :

- Cpu : ARM920T at 366MHz
- 16 MB de SDRAM

Système d'exploitation:

- Linux 2.4.0-test6

Signe particulier :

- Il s'agit d'une Lexmark e240n rebrandée

Trois approches pour un même but

- **L'approche Logicielle** : corrompre les services de l'imprimante, overflow, authentification, XSS etc…
- **L'approche Firmware** : patcher le code qui fait fonctionner l'imprimante et s'installer durablement
- **L'approche Matérielle** : dialoguer avec un port série ou ajouter du matériel

Soyons exhaustif, tentons donc les 3 approches !

Sécurité logicielle : 10 min de résistance

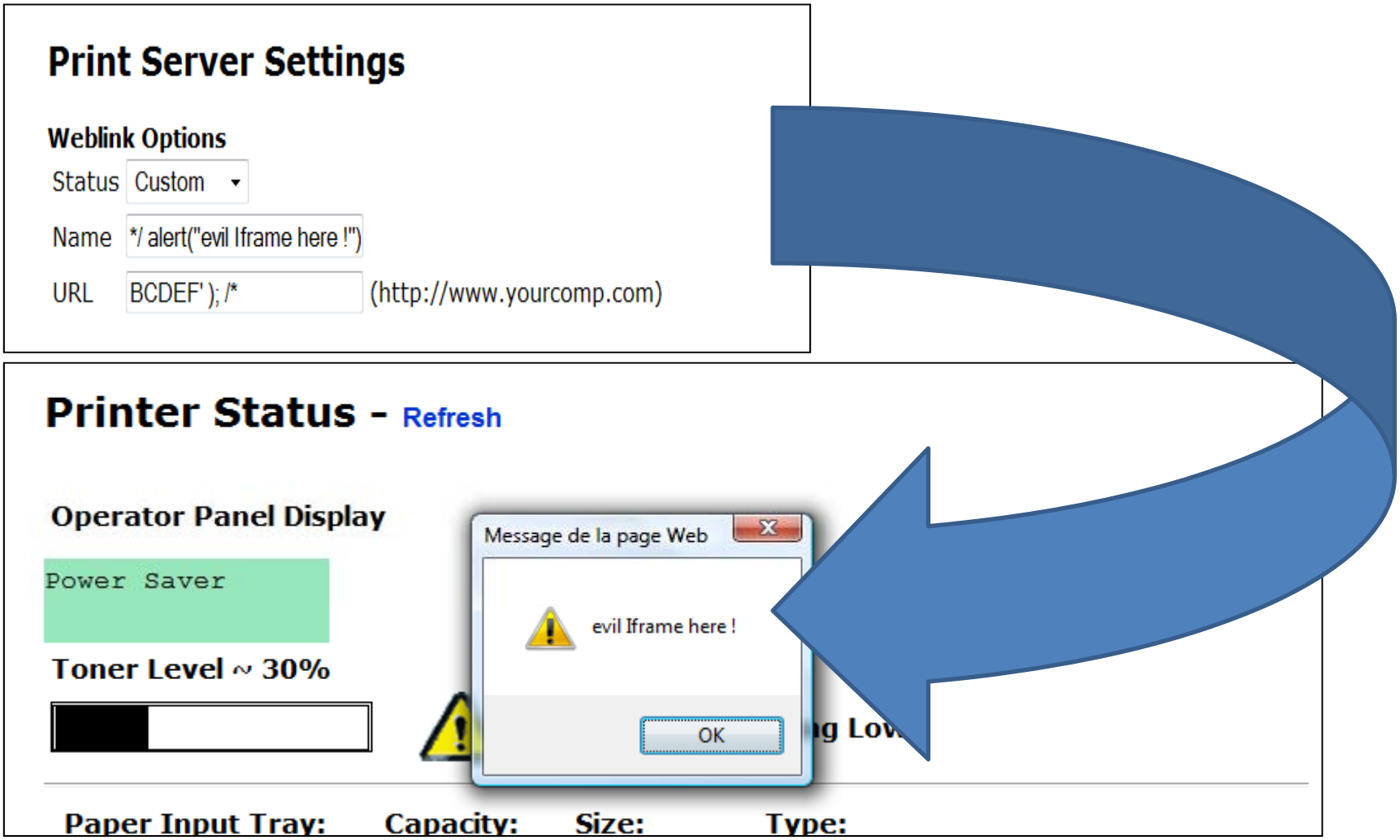
- Il est possible de changer le mot de passe administrateur sans le connaitre par une simple requête HTTP !

```
POST http://$HOST/config/posttest?index=0&page=/security HTTP/1.1
…
GENPASSWORD=$new_pass&GENPASSWORD=$new_pass
```

- Preuve du niveau de sécurité (bug simpliste) et de l'intérêt porté au sujet par tous (non publié, ni par l'éditeur, ni par des chercheurs)
- La page web principale du serveur dispose d'une zone éditable :

Il est possible de d'éditer ce message ->

Des bugs « subtils » comme les XSS



Conclusion de l'approche Logicielle

- Deux bugs triviaux mais graves, découvert en 10 minutes…
- Ouvre la possibilité d'utilisation de webtoolkit, tels que mpack, neosploit, zeus etc.
- Rien qu'avec ces points, il est possible de compromettre durablement la sécurité du LAN (le meilleur reste à venir)
- Les attaques sur les navigateurs sont en « vogue », les serveurs HTTP éditables représentent donc un risque majeur
- Ces vulnérabilités sont légion parmi les MFD, et ce risque est jusqu'à présent tout simplement ignoré !
- En comparaison SCADA, c'est du béton armé renforcé titane…

Le Firmware : Installons nous à vie !

- Pourquoi : car une imprimante reste des années dans un réseau et que son firmware n'est jamais mis à jour
- Quand bien même le serait-il, il est possible de faire croire qu'il a été mis à jour tout en préservant le firmware patché
- Il faut pour cela patcher un firmware et donc en premier lieu l'obtenir puis le décompiler et le comprendre
- Prise de contrôle du panneau LCD de l'imprimante et donc ingénierie sociale ! (appeler le support, aller à telle URL …)
- Une fois ceci fait, il faut modifier un ou deux démons et le noyau linux qu'il contient

En apprendre plus sur la Lexmark e240n

Reverse Engineering :

- Comprendre son fonctionnement
- Rendre exploitables les buffer overflows
- Si possible, backdoorer le firmware !

```
.text:00000054 00 60 A0 E1              MOV     R6, R0          ; Rd = Op2
.text:00000058
.text:00000058              loc_0_58                            ; CODE XREF: .tex
.text:00000058 D0 00 D5 E1              LDRSB   R0, [R5]        ; Load from Memor
.text:0000005C 01 50 85 E2              ADD     R5, R5, #1      ; Rd = Op1 + Op2
.text:00000060 00 3C A0 E1              MOV     R3, R0,LSL#24   ; Rd = Op2
.text:00000064 43 3C A0 E1              MOV     R3, R3,ASR#24   ; Rd = Op2
.text:00000068 03 38 A0 E1              MOV     R3, R3,LSL#16   ; Rd = Op2
.text:0000006C 23 38 A0 E1              MOV     R3, R3,LSR#16   ; Rd = Op2
.text:00000070 00 30 C4 E5              STRB    R3, [R4]        ; Store to Memory
.text:00000074 02 40 84 E2              ADD     R4, R4, #2      ; Rd = Op1 + Op2
.text:00000078 00 30 B0 E1              MOVS    R3, R0          ; Rd = Op2
.text:0000007C F5 FF FF 1A              BNE     loc_0_58        ; Branch
.text:00000080 02 0C A0 E3              MOV     R0, #0x200      ; Rd = Op2
.text:00000084 00 00 8D E0              ADD     R0, SP, R0      ; Rd = Op1 + Op2
.text:00000088 08 00 00 EB              BL      OutputDebugStringW ; Branch with
.text:0000008C 00 00 56 E3              CMP     R6, #0          ; Set cond. codes
.text:00000090 06 00 A0 E1              MOV     R0, R6          ; Rd = Op2
.text:00000094 00 00 A0 D3              MOVLE   R0, #0          ; Rd = Op2
.text:00000098 06 DC 8D E2              ADD     SP, SP, #0x600  ; Rd = Op1 + Op2
.text:0000009C 70 A0 9D E8              LDMFD   SP, {R4-R6,SP,PC} ; Load Block fr
.text:0000009C              ; ---------------------------------------------------------
.text:000000A0 B4 00 00 00 off_0_A0     DCD __imp_vsprintf      ; DATA XREF: DbgP
.text:000000A0              _text       ends
```

Exemple d'overflow sur le service ftpd

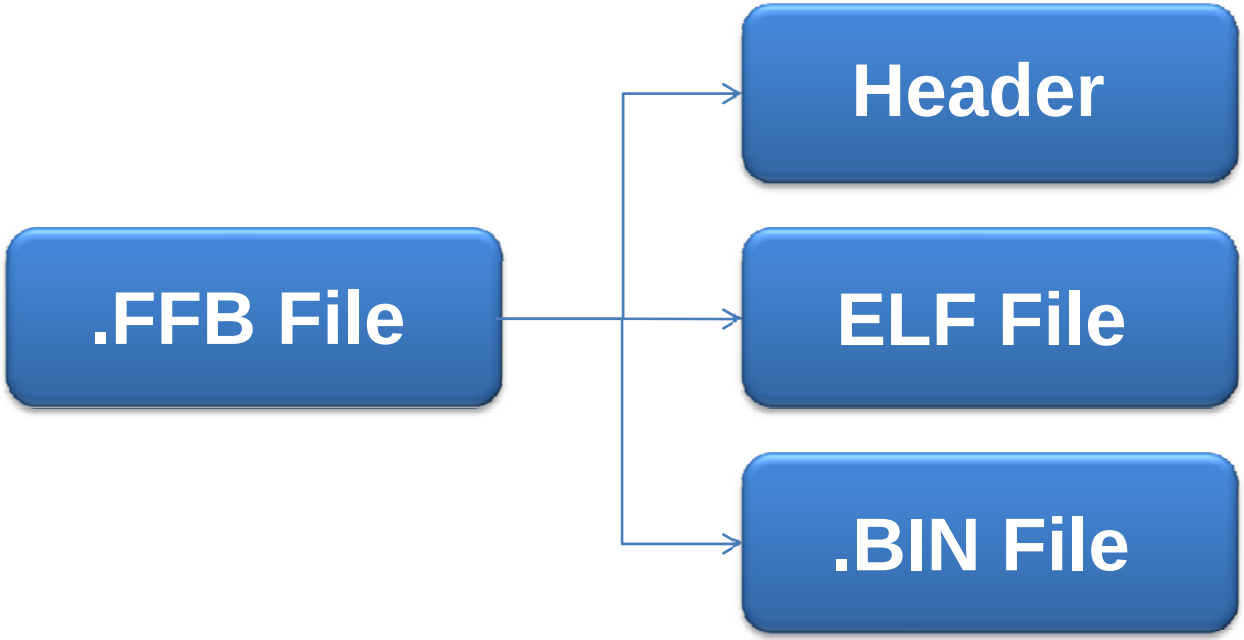
```
Current process: ftpd   pid=236
current=0xc1bfe000 kernelsp=0xfaceface
Current time(jiffies): 86635
Unaligned = u:686 s:0
Last entry  u:4 dabt_usr, s:3 irq_svc

Dumping regs from 0xc1bfec54
r0:00000001 r1:c00240cc r2:a0000013 r3:0000001e
r4:c1bfec94 r5:c00e3e0c r6:0000001e r7:c0103eb0
r8:00000002 r9:00000000 r10:00000000
fp:c001a0f8 ip:c00c7e9c sp:c1bfec94 lr:00000030 pc:c001b420
cpsr:66703a63 orig_r0:00000031

Dumping regs from 0xc1bfefb8
r0:00000000 r1:0054e218 r2:006253d0 r3:4141412f
r4:0054e4ac r5:41414141 r6:00625630 r7:0054e4ac
r8:006253e0 r9:00625630 r10:00000012
fp:00000000 ip:006253e0 sp:affffda4 lr:00503570 pc:005035c0
cpsr:20000010 orig_r0:00503570
```

```
[900 Service     RIP Software    Unable to handle kernel paging request at virt\
ual address 4141414a   cur:ftpd:236
]
Time:    00000362 00050910     Wed Dec 31 19:14:26 1969
UpTime: 866330 mSec
```

Analyse du Firmware

- Base de l'attaque : Le firmware BRQP205.ffb (publique) est composé de 3 parties :
  - Un header
  - Un fichier ELF
  - Un fichier « .bin » (format propriétaire)
- Le firmware comprend une commande PJL de type « LPROGRAMRIP » (instruction PJL propriétaire).
  - Cette commande dispose d'arguments simples, qui correspondent à la version du firmware, et à la taille du fichier ELF + fichier BIN.
  - La commande PJL se termine en fait à la fin du fichier.

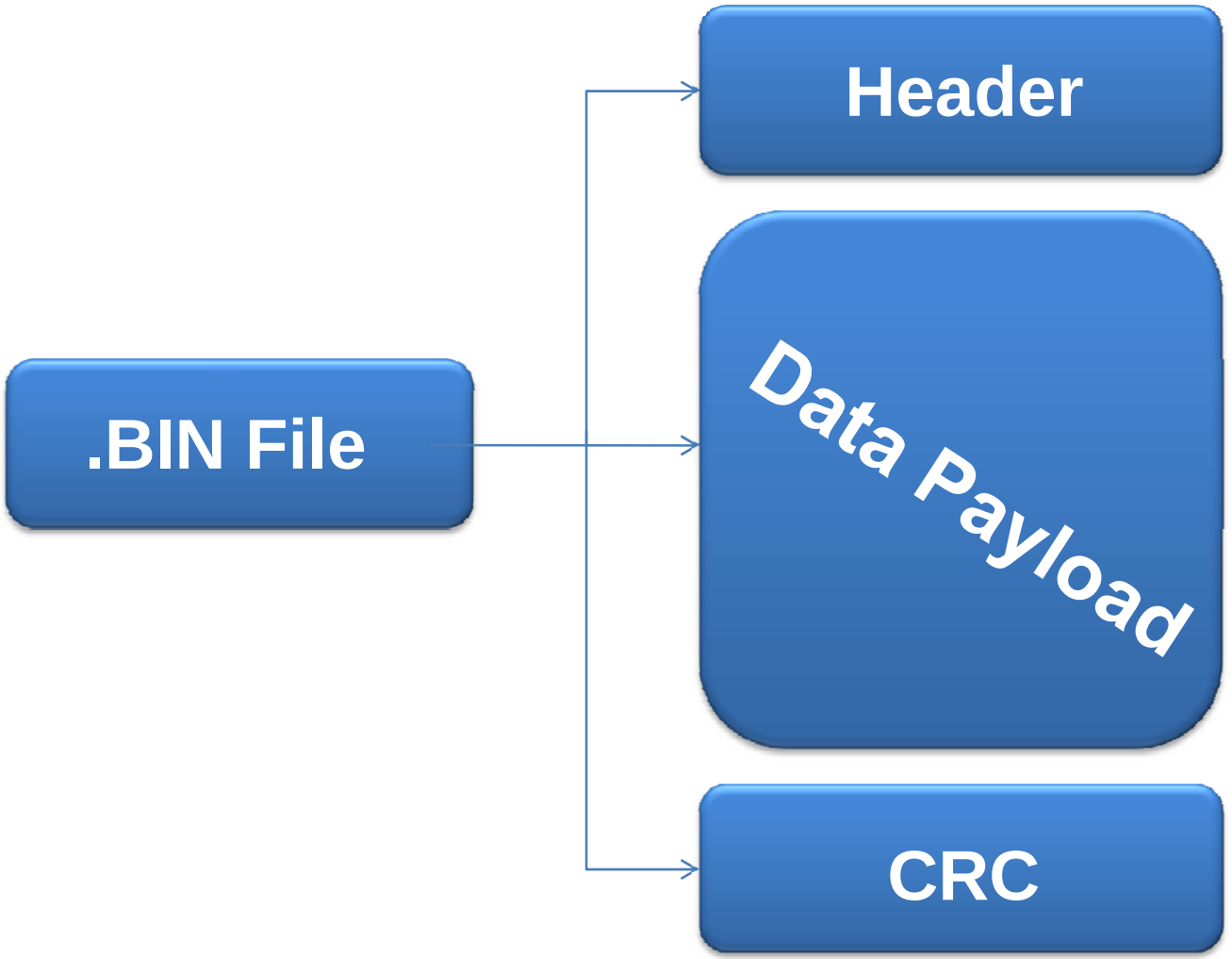
Format du firmware



Patcher le firmware

- Le démon TFTP ou HTTP par lequel est effectué l'update valide la commande PJL, puis passe la main à un autre service « netapps_sa.sa ».
- Le fichier ELF a la charge de l'update. Il se sert du fichier « bin » pour extraire les données et l'écrire dans la flash.
- Le fichier « bin » contient la mise à jour à proprement parler, sous forme de sections, qui contiennent toutes :
  - Un header sur 64 bit
  - La donnée ('|BIN' + la donnée)
  - Un CRC (de contrôle et non de signature) sur 16 bit

Contenu du binaire

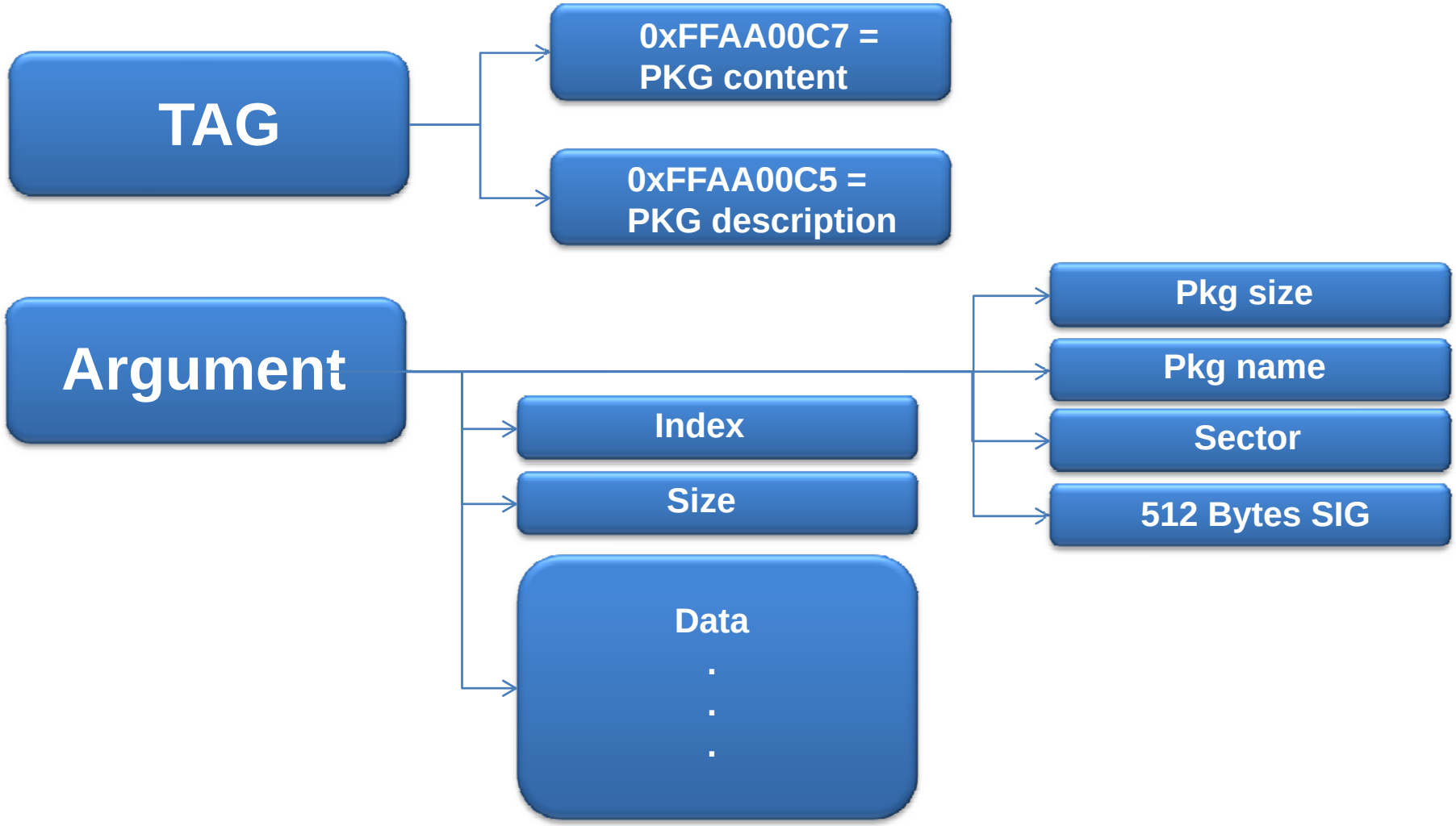


Format du Data payload

- La donnée est formatée sous forme de tags, qui permettent de renseigner l'endroit où placer la donnée, ainsi que sa taille ou encore son type.

- Exemple :
  - Tag « 0xFFAA00C5 » (pkg desc) avec une structure de 256 bytes
  - Tag « 0xFFAA00C7 » (pkg content) contient lui les arguments comme pour un memcpy + la donnée à copier

Format des packages



Structure du firmware

- On peut ainsi retrouver dans le fichier BIN
  - Différents kernels (firmware compatible entre plusieurs versions)
  - Un package Network
- Le package Network est au format CRAMFS
  - Il s'agit d'un CRAMFS modifié (utilisation du mkcramfs de Lexmark)
  - Obtention des binaires réseaux utilisés sur l'imprimante (DHCP, HTTPD, FTPD, RARP, TCP9x00, WINS, PNP, LPD, etc.)

Conclusion sur l'approche Firmware

En dehors de créer une backdoor complète (processus possible mais long), la première analyse permet de :

- Faciliter l'exploitation des vulnérabilités repérées dans les différents services et d'en détecter de nouvelles
- Prouver la faisabilité d'attaques par modification de firmware et donc l'installation (très) durable d'une backdoor dans le LAN
- Trouver de nouvelles vulnérabilités grâce à la possession des binaires et d'en ajouter pour se créer un bastion d'opérations plus complet

Troisième approche : le matériel

Varions les plaisirs et passons à une attaque hardware !

- Insertion d'un petit périphérique interceptant les connexions
- Seules les requêtes d'impression sont vraiment transmises
- Propagation sur le réseau victime
- Impossible à déceler sans démonter l'imprimante
- Facile à insérer grâce au contrôle du panel LCD, en incitant l'utilisateur à appeler la maintenance à un numéro qui nous appartient ! (Voir slide 14)

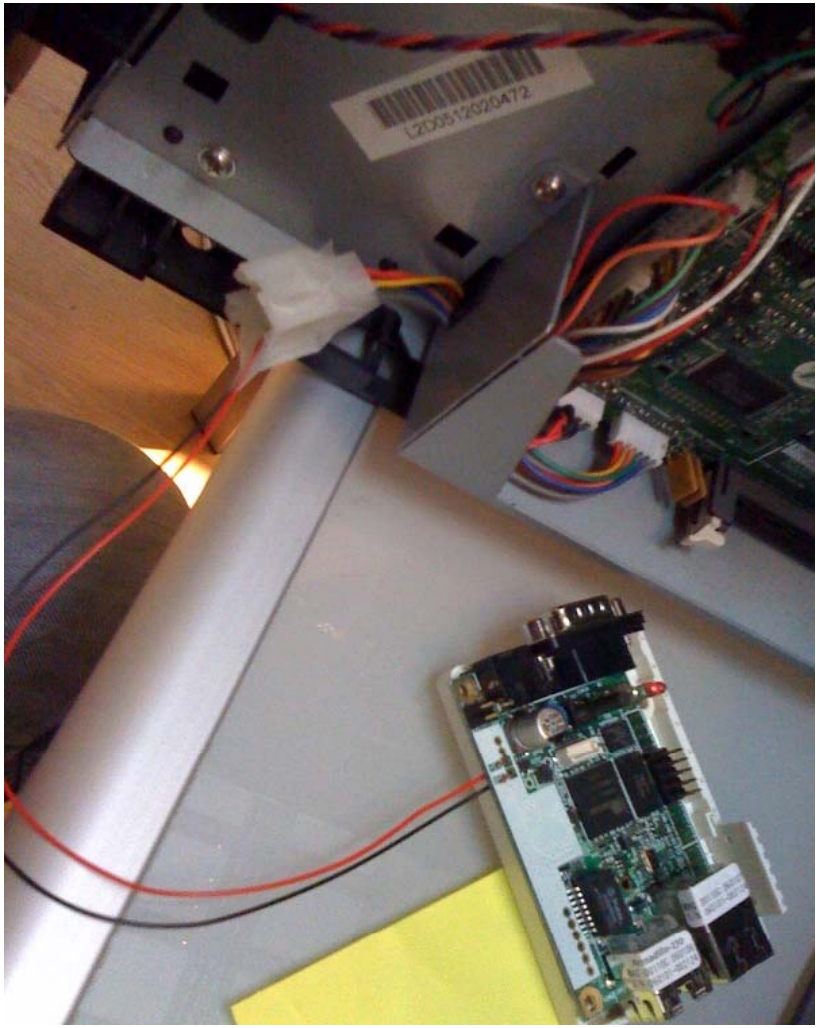
Une discussion très “matérielle”

- Connexion au port UART (Série) de l’imprimante
- Obtention d’un accès en lecture et écriture au système
- Utile pour le débogage !
- La console n’est pas accessible pour le moment car protégée par un mot de passe. (une recherche dans le package du firmware nous le livrera)

La console (Linux) de l'imprimante

```
Linux version 2.4.0-test6 (Lexmark@lexmark) (gcc) #1

Processor: ARM/VLSI Arm920sid(wb) revision 0
Architecture: Lexmark F-ARM controller
On node 0 totalpages: 8192
zone(0): 8192 pages.
zone DMA 32 64 96 rs=8192 sz=8192
zone(1): 0 pages.
zone(2): 0 pages.
Reserving 22612 KB for lxk @ 0xc09eb000
COMMAND: 'porkeys=0 rw hda=autotune hdb=none root=/dev/flasha3
ro PORKEYS=0 i2cpio=0 cachesize=5 SERDBG=0 lbringsize=327
Calibrating delay loop... 325.22 BogoMIPS
Memory: 32MB = 32MB total
Memory: 8568KB available (827K code, 154K data, 40K init)
Dentry-cache hash table entries: 512 (order: 0, 4096 bytes)
...
```

Insertion d'une carte supplémentaire



Conclusion sur l'approche Hardware

Il est possible d'installer facilement une carte dans une imprimante en se faisant passer pour le service de support.

- Un connecteur 5V ou 12V se trouve très facilement dans toutes les imprimantes
- Une carte de la taille d'un demi paquet de cigarette contient un Linux (très) complet et performant de nos jours
- Le dispositif est quasiment impossible à détecter
- Il est (très) durablement installé
- Le coût est ridicule (~100 €)

Bonus sur les hacks d'imprimantes

- L'imprimante peut réaliser un nouveau type de scan : le Fake Idle Scan
  - Les scans simples détectés passeront pour des idle scan
    - Pourquoi ne pas effectuer un fake idle scan ? ☺ On scanne vraiment, mais vu que le scanner est sur l'imprimante, tout le monde croira à un idle scan alors que c'est un vrai scan, d'où le nom de « fake idle scan ».
  - Utilisation des différentes méthodes pour 'maquiller' le scan
  - Une fois une machine piratée, continuer la propagation depuis cette machine sous la forme d'un ver
- Si l'attaque est découverte, le réseau sera désinfecté mais les MFD ne le seront très probablement pas

3 Scénarii d'ingénierie social

- Cas du livreur d'imprimante préalablement piratée

On prépare à la maison une imprimante "patchée" au niveau firmware et on la livre "par erreur" à une personne trop contente de sa bonne fortune pour se méfier.

- Cas de l'ingénierie sociale via l'écran LCD

Il s'agit ici d'inciter l'utilisateur à faire une action comme par exemple convier un réparateur en l'appelant sur son numéro ou même se rendre à une URL contenant un cheval de Troie en Javascript ou la page de commande de toner en HTML de l'imprimante compromise en XSS.

- Cas du réparateur qui modifie l'imprimante

Dans ce cas, le réparateur appelé peut installer une carte dans l'imprimante.

Attaques sur d'autres MFD

Les smartphones, une cible de choix :

- Contiennent de nombreuses données utilisateurs
- Pas de réelle solution de sécurité
- Vont et viennent dans et hors de l'entreprise
- Utilisateurs peu éduqués aux risques
- Des attaques aléatoires très faciles à réaliser

Attaques sur les smartphones

- Chaque application en réseau réduit le niveau de sécurité de l'appareil
- Le chiffrement proposé sur les smartphones n'est parfois pas très résistant
- Les applications ne sont pas vérifiées en profondeur contre les backdoors intentionnées par Apple
- L'interaction des smartphones avec les ordinateurs augmente

Attaques sur les smartphones

- Exemple : de multiples vulnérabilités potentielles sur toutes les applications en ligne
- Le langage objective C utilisé sur beaucoup d'applications Iphone est vulnérable aux attaques classiques (overflows…)

Attaques sur les Caméras IP

Nous avons maltraité une caméra de type « Axis 2100 »

Hardware :

- Cpu : ETRAX 100 (~99 bogomips)
- 8 Mo de RAM, 2 Mo de Flash

Software :

- µLinux

Signes particuliers :

- Nombreuses vulnérabilités de type « Authentication bypass »

Attaques sur les Caméras IP

- Dispose nativement d'un serveur FTP (non chrooté).
- L'initd comporte une ligne intéressante : `#telnetd:3:respawn:/bin/telnetd`
- Le système contient un grand nombre de binaires, tout le nécessaire en fait :

```
# # ls /bin

admin.cgi       dnrd            ifconfig        paramtool.sh    smtpclient
alarm           dotlockfile     image_buffer    parhand         sockclient
audiod          dstd            imgexpand       parhandclient   ssid
basebb          echo            init            pppd            syslogd
boa             editcgi.cgi     iod             pppwrapper      telnetd
bootblocktool   focus           kill            rm              tl_editor
bootpc          ftpwrapper      killscript      route           touch
bufferd         grep            ls              sed             usleep
camd            hwtest          mactool         sftpclient      utask
cat             hwtestio        miscbb          sftpd           vio.cgi
chat            hwtestrtc       mish            sh
cp              hwtestserial    mkdir           shttpclient
dhclient        id_uploader     mv              sleep
# # _
```

Attaques sur les Caméras IP

- Réalisation d'une backdoor en script shell
  - Shell exec via HTTP
  - Scanner WEB
  - Scanner FTP
  - Scanner de ports
- Lancée tout simplement via l'initab, avec les outils déjà présents dans le linux de la caméra !
- Autres pistes

  Il est possible de compiler du code pour ces séries de caméra, Axis a publié une toolchain pour ces machines, même si les processeurs ETRAX 100 ne sont pas directement supportés.

Conclusion : Attaques sur les MFD

- Une attaque facile à réaliser grâce à une ingénierie sociale
  - Très efficace si aucune politique sécurité ne traite des MFDS
- Plus puissant qu'un trojan
  - Assurance d'être administrateur
  - Impossible à effacer (il faut démonter l'imprimante)
  - N'est pas dans un environnement logiciel surveillé

- Seuls des mécanismes réseaux peuvent effectuer la détection du périphérique malveillant

Quelques contre mesures

- Les contres mesures peuvent être d'ordre organisationnelles :
  - Prendre en compte les risques et menaces liés aux MFD lors de l'appréciation des risques
  - L'annexe A de l'ISO 27001 et l'ISO 27002 ne traitent pas des MFD au même titre que les autres systèmes intelligents du SI
  - Prévention quand aux risques d'ingénierie sociale par MFD auprès des utilisateurs
- Mais également technique :
  - L'utilisation de serveurs d'impression permet de ne pas connecter directement au réseau les ports ethernet des imprimantes
  - Isoler les MFD dans un sous réseau et/ou les filtrer
  - Un MFD qui scanne le réseau n'est pas forcément un idle scan

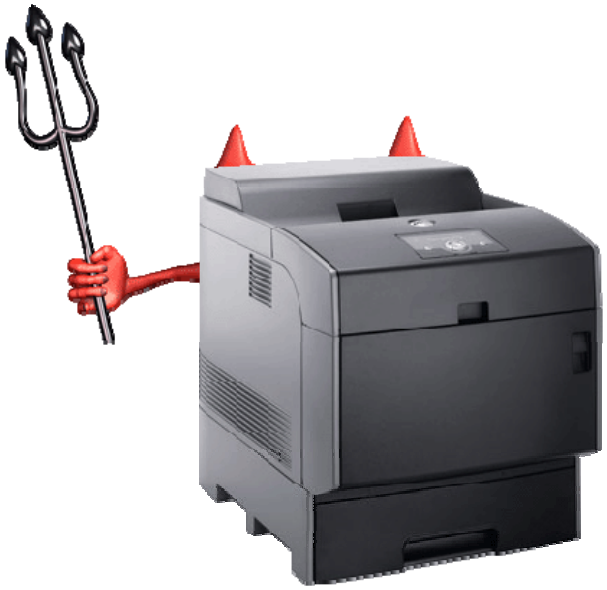
Compromissions possibles sur les MFD

- Overflow : les services sont faillibles
- Authentification bypass, XSS, drive by download, …
- Patch du Firmware
- Patch physique, ajout de carte

Un scénario apocalyptique ?

- Un document qui contient une chaine de caractères qui provoque un overflow dans le service d'impression et lance un shellcode lorsqu'on l'imprime ☺
- Extension de ce scénario ? Si ce shellcode installe un worm, celui-ci peut compromettre les autres imprimantes du LAN, il peut même être multiforme pour s'attaquer à plusieurs modèles / marques d'imprimantes ou de MFD.

Crédits & Bibliographie



Juste une imprimante ?

Auteurs / chercheurs :

- Thibault Koechlin, NBS System
- Jean Baron, NBS System

Remerciements pour leurs contribution à :

- Damien Milleschamps
- Philippe Humeau, NBS System

Autres sources d'informations

- Pour les HP : http://www.phenoelit-us.org/fr/tools.html

Des questions techniques ?

Thibault Koechlin, Responsable Labo Sécurité (tko@nbs-system.com)
Jean Baron, Membre Labo Sécurité (jba@nbs-system.com)

Vous souhaitez que l'on travaille ensemble sur ces points ou d'autres ?

Sylvain Martin, Responsable Commercial (sma@nbs-system.com)

NBS System
140 Boulevard Haussmann
75 008 Paris
Tel : 01.58.56.60.80, Fax : 01.58.56.60.81

http://www.nbs-system.com