Sécurité de l'ADSL en France

Nicolas RUFF

EADS/CCR DCR/STI/C

Introduction

- Le constat
  - Explosion de l'accès ADSL en France
  - La concurrence se joue sur les services
- Les conséquences
  - Développement du "Triple Play"
    - Internet / TV / Téléphonie
- Et au final …
  - Nécessité d'utiliser une "set-top-box" fournie par le FAI
  - Quelle sécurité dans la boite ?

Introduction

- De nombreux offres analysées ces 2 dernières années
  - Derrière une grande diversité de l'offre …
  - … une grande homogénéité des solutions techniques
- Sujet très sensible techniquement et commercialement
  - Ne pouvait être présenté au SSTIC 2005 car les failles n'étaient pas corrigées
  - Aucun opérateur ne sera cité
- Aspects "non techniques" non abordés ici
  - Responsabilité FAI / constructeur / end-user
  - Nécessité d'interception légale sur la VoIP
  - Etc.

Hardware

- Chipsets "tout en un"
  - Principalement du Broadcom
    - Ex. BCM 6345, BCM 6410
  - Processeur à cœur MIPS32
- Forte intégration des cartes mères
  - Très peu de composants accessibles
- Mais les attaques hardware restent possibles
  - Port série
  - Port JTAG
    - Cf. travaux OpenWRT

Système d'exploitation

- 2 familles
  - Système VxWorks
    - Très fermé
    - Difficile à analyser
  - Mais …
    - Système issu du monde industriel pas prévu pour aller sur Internet
      - Ex. Numéros de séquence TCP incrémentaux
    - Peu de fonctionnalités disponibles
      - Ex. Serveur Web avec langage de script minimaliste

Système d'exploitation

- Conséquence : les vérifications se font côté client …

```
…
<SCRIPT LANGUAGE=Javascript>
var old_password = "1234";
function CheckPasswd()
{
if( document.SubmitChPwdUser.OLDPASSWD.value !=
   old_password)
{
…
```

Système d'exploitation

- Système Linux
  - Robuste
  - Riche en fonctionnalités
- Mais …
  - Très facile à analyser
  - Impacté par les bogues publics
    - Ex. ISC DHCP 3.0, libUPnP, etc.

Mise à jour du système

- La mise à jour est une fonction nécessaire
  - Amélioration des services
  - Correction de bogues
- Plusieurs méthodes
  - Manuelle (par l'utilisateur)
    - Problème : rarement effectuée
    - Seule méthode quand le modem est propriété de l'utilisateur
  - Automatique (par le FAI)
    - Problèmes : moment de l'installation non maitrisé, dangereux
    - Pas de signature sur les firmwares
- Techniquement
  - Utilisation du protocole FTP
  - Serveur chez le FAI (pull) ou sur le modem (push)
- N'importe qui peut récupérer le firmware

Interfaces

- Interfaces côté LAN
  - FTP, SSH (parfois), Telnet, Web, UPnP, etc.
- Interfaces côté WAN
  - Parfois un port d'administration
- Comptes
  - Utilisateur (toujours trivial)
  - Support
  - Opérateur
  - Constructeur

Interfaces

- Quelques erreurs graves
  - Absence d'authentification
  - Compte FTP "anonymous"
  - Mots de passe triviaux (ex. 1234, 12345)
  - Mots de passe documentés sur Internet

  - Commandes privilégiées accessibles (ex. debug)
  - Champs "cachés" (ex. mots de passe)

  - Sauvegarde et restauration de la configuration
    - Permet l'accès aux mots de passe en clair
    - Permet l'injection de scripts

WiFi

- Plusieurs écoles
  - Aucune sécurité (ex. PPP over WiFi)
  - WEP
  - WEP+rotation propriétaire des clés
    - Requiert une carte et un driver spécifique
    - Inacceptable pour l'utilisateur
  - WPA (récent)

- Seul WPA présente une sécurité acceptable
  - Sous réserve que (clé WPA != clé WEP)

WiFi

- Remarques
  - Contrôles d'accès basés sur l'adresse MAC
    - Hardware (bouton) ou software
    - Inefficace : une adresse MAC est triviale à usurper
  - Adresse MAC + clé WEP utilisés comme authentifiant sur le site du constructeur
    - Comment le constructeur peut-il valider l'authentification ?
  - Interface d'administration boguée + WiFi non sécurisé = problème ?

Infrastructure

- Réseau basé sur ATM
  - Cellule ATM = en-tête (5 octets) + données (48 octets)
  - Virtual Circuit Identifier (VCI) sur 16 bits
  - Virtual Path Identifier (VPI) sur 8 ou 12 bits
  - Canal ATM = VCI+VPI
- Canaux couramment utilisés
  - Internet = 8/35 ou 8/36 selon les FAI
  - Ensemble des services = VCI 8, VPI entre 35 et 50
  - Certains canaux sont réservés à l'administration …

Infrastructure

- Cibles
  - Serveurs de mise à jour
    - Absence de signature des firmwares => possibilité de compromission massive
  - Serveurs de téléphonie ou TV
    - Fraude
  - Réseau d'administration opérateur

Conclusion

- Conclusion
  - Les modems peuvent être analysés
  - Il existe des failles parfois simples
- Scénarios
  - Réseau de bots installés dans les modems
  - Ecoute/redirection du trafic client
  - Fraude
  - Racket de l'opérateur
    - Ex. déni de service massif