

Analyse de sécurité des BOX ADSL

Y. Bachy, V. Nicomette, E. Alata, Y. Deswarte,
M. Kaâniche, et JC. Courrege

SSTIC 2014

4 juin 2014

Émergence des équipements grand public connectés



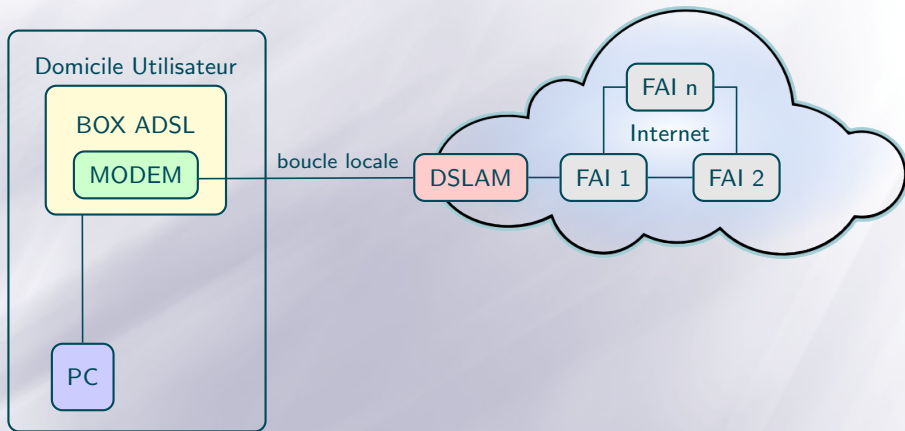
Émergence des équipements grand public connectés



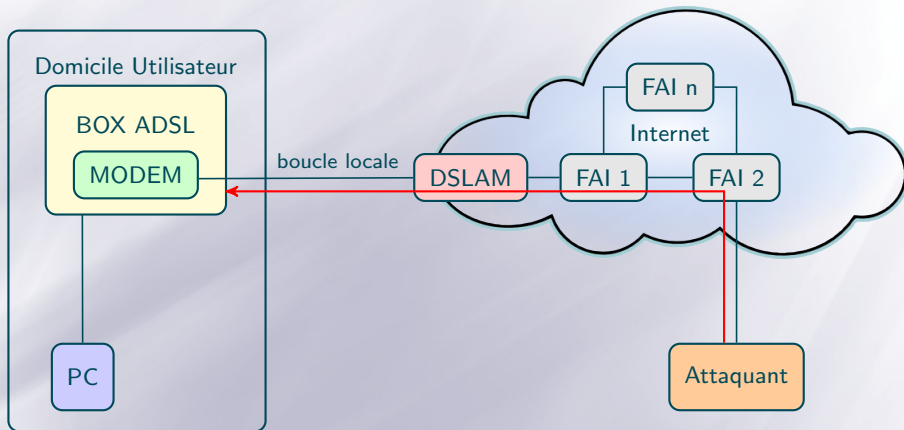
La BOX ADSL

- Introduction à la fin des années 90 d'offres Internet "triple play" proposant trois grands axes de services :
 - Web (NAT, DHCP, ...)
 - Télévision (PVR, Replay, ...)
 - Téléphonie (DECT, répondeur, 3G, ...)
- Développement d'équipements, nommés IAD (*Internet Access Device*) ou BOX ADSL, permettant de profiter de ces services.
- De plus en plus de services rendant les box plus riches → augmentation de la surface d'attaque

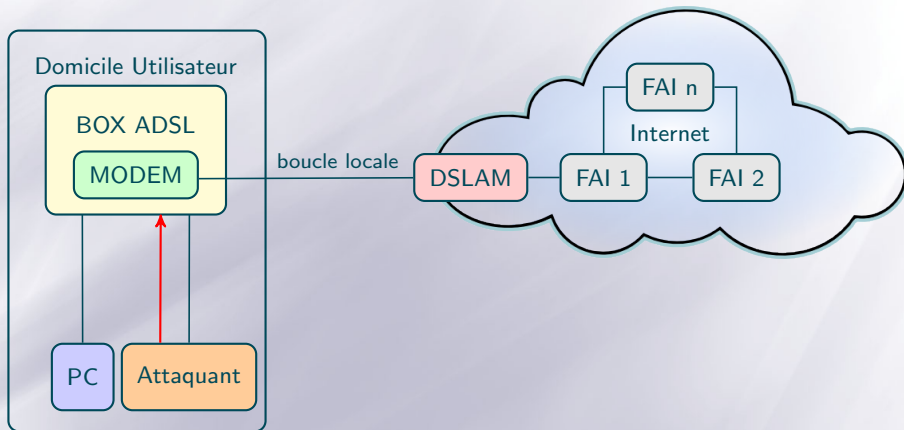
Architecture générale



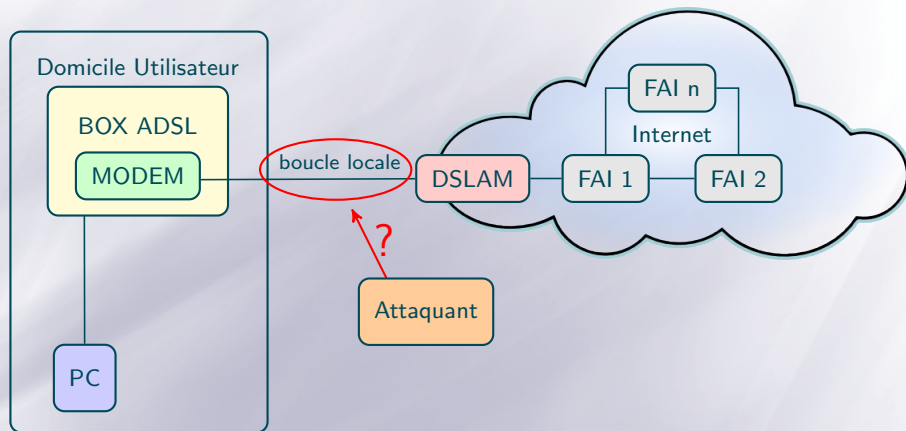
Chemins d'attaque connus (1/2)



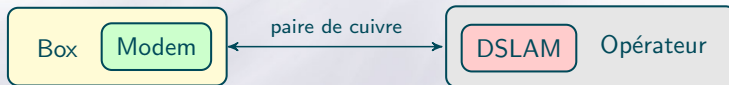
Chemins d'attaque connus (2/2)



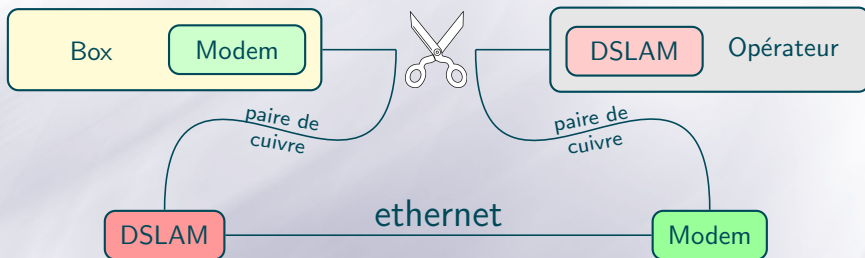
Nouveau chemin d'attaque



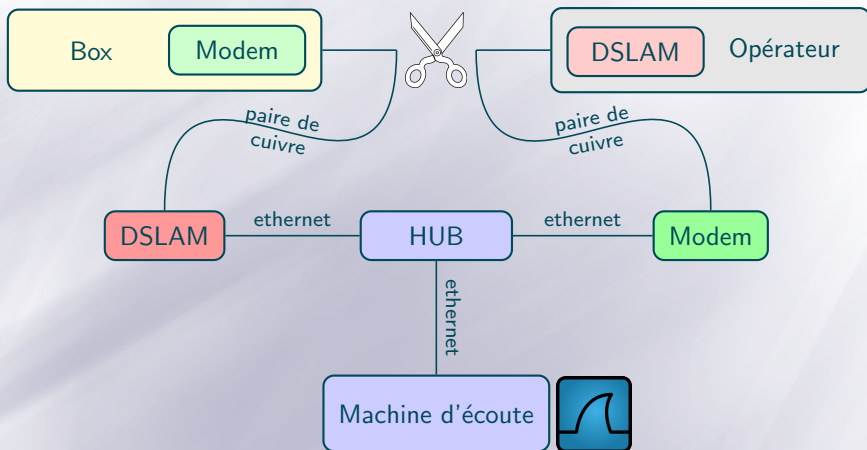
La boucle locale



Observation des communications sur la boucle locale (1/2)



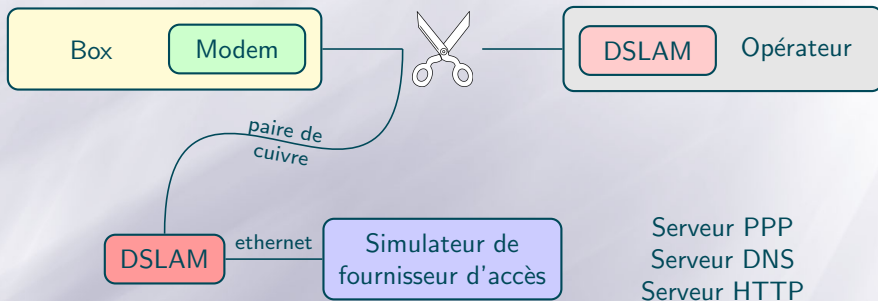
Observation des communications sur la boucle locale (2/2)



Comparaison de plusieurs BOX ADSL

BOX	ATM	PPP	DHCP	SIP	Configuration	Mise à jour
<i>A</i>	8/35/LLC	chap	no	MD5	HTTP, FTP, SSL	-
<i>B</i>	8/35/LLC	chap	yes	MD5	HTTP, SSL	SSL
<i>C</i>	8/36/VC	no	yes	MD5	SSL	-
<i>D</i>	8/35/LLC	chap	yes	MD5	HTTP	HTTP
<i>E</i>	8/35/LLC	chap	yes	MD5	HTTP	HTTP
<i>F</i>	8/35/LLC	chap	no	MD5	SSL	-

Interruption de la boucle locale



Résultats obtenus

Remplacement du firmware

- Désactivation (partielle) du pare-feu
- Ajout d'un compte super-utilisateur
- Désactivation des mises à jour
- Installation de logiciel "soft-phone"

Exploitations réalisés

- Utilisation à distance de la box pour émettre des appels "surtaxés"
- Connexion à distance sur la box (via porte dérobée)

Autres exploitations envisagées

- Réalisation d'un botnet
- Attaques DDos
- Proxy

Conclusion

Principale conclusion

- Mise en évidence d'un nouveau chemin d'attaque des BOX ADSL

Contributions

- Une plateforme d'observation des communications ADSL
- Une plateforme de simulation d'un fournisseur d'accès

Contre-mesures

- Nécessité de généraliser les méthodes cryptographiques pour les communications sensibles → techniquement simple et peu onéreux
- Possibilité d'observer l'atténuation sur la boucle locale

