A Security Analysis of French ADSL boxes

Yann Bachy, Vincent Nicomette, Eric Alata, Yves Deswarte, Mohamed Kaâniche, J.C. Courrège

LAAS-CNRS THALES

Home networks

ADSL box
Internet Access Device

Internet

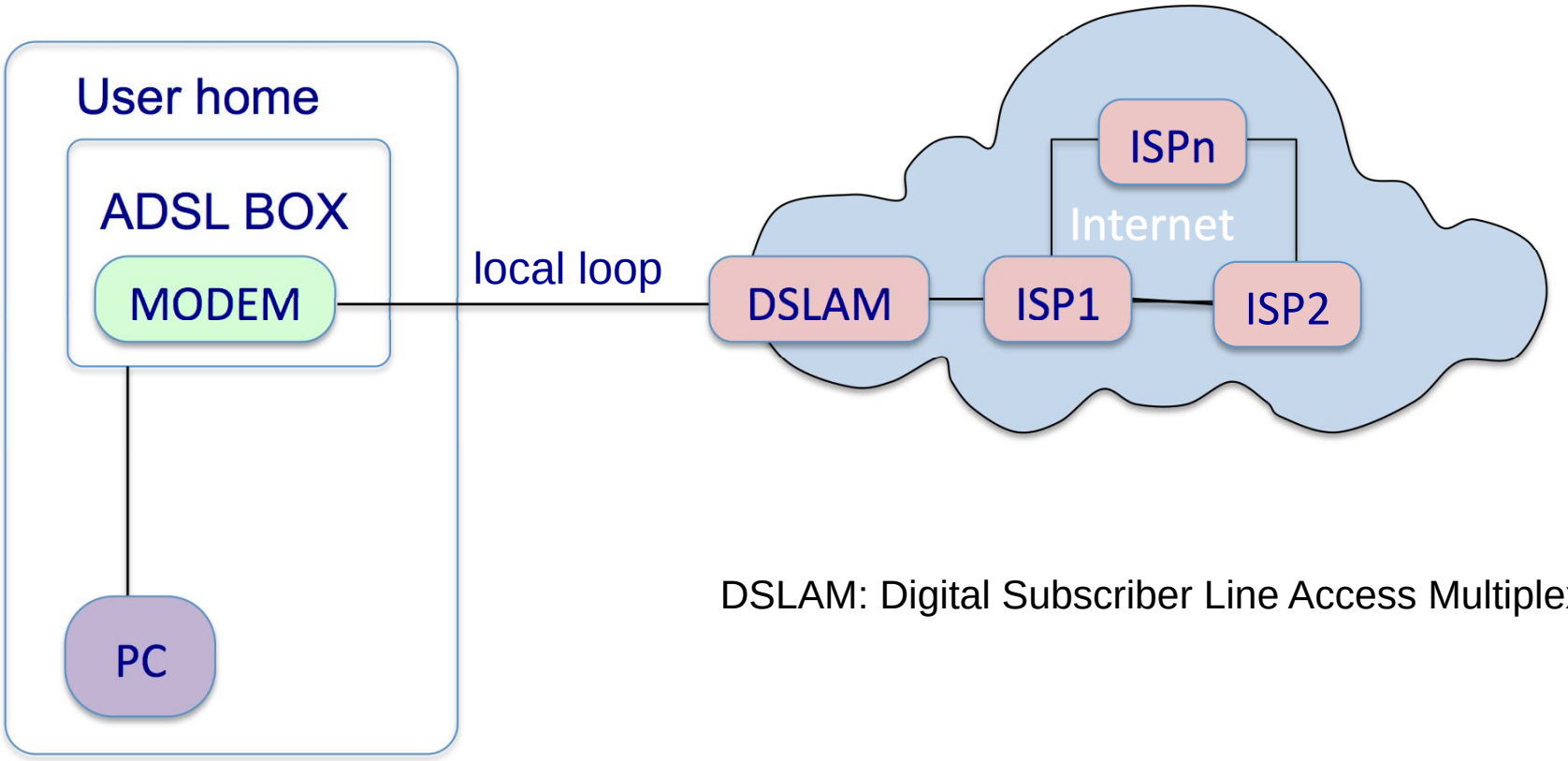
Triple play offers: convergence of voice, data and video

Home networks

Goal

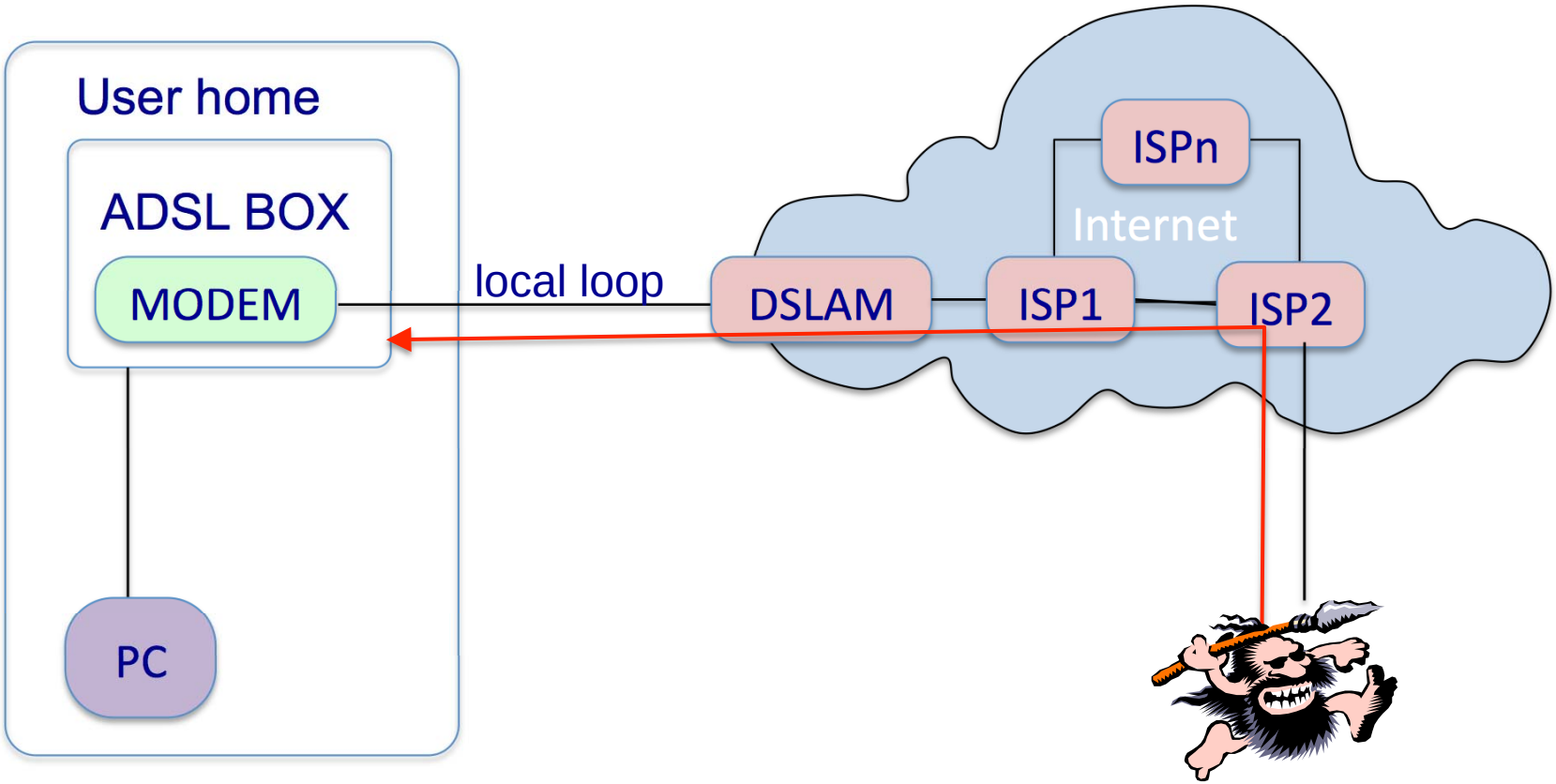
- Analyse the security of ADSL boxes from different providers
  - Identify weaknesses
  - Develop a platform to illustrate possible exploitations
  - Investigate countermeasures
- Black box approach

General Architecture

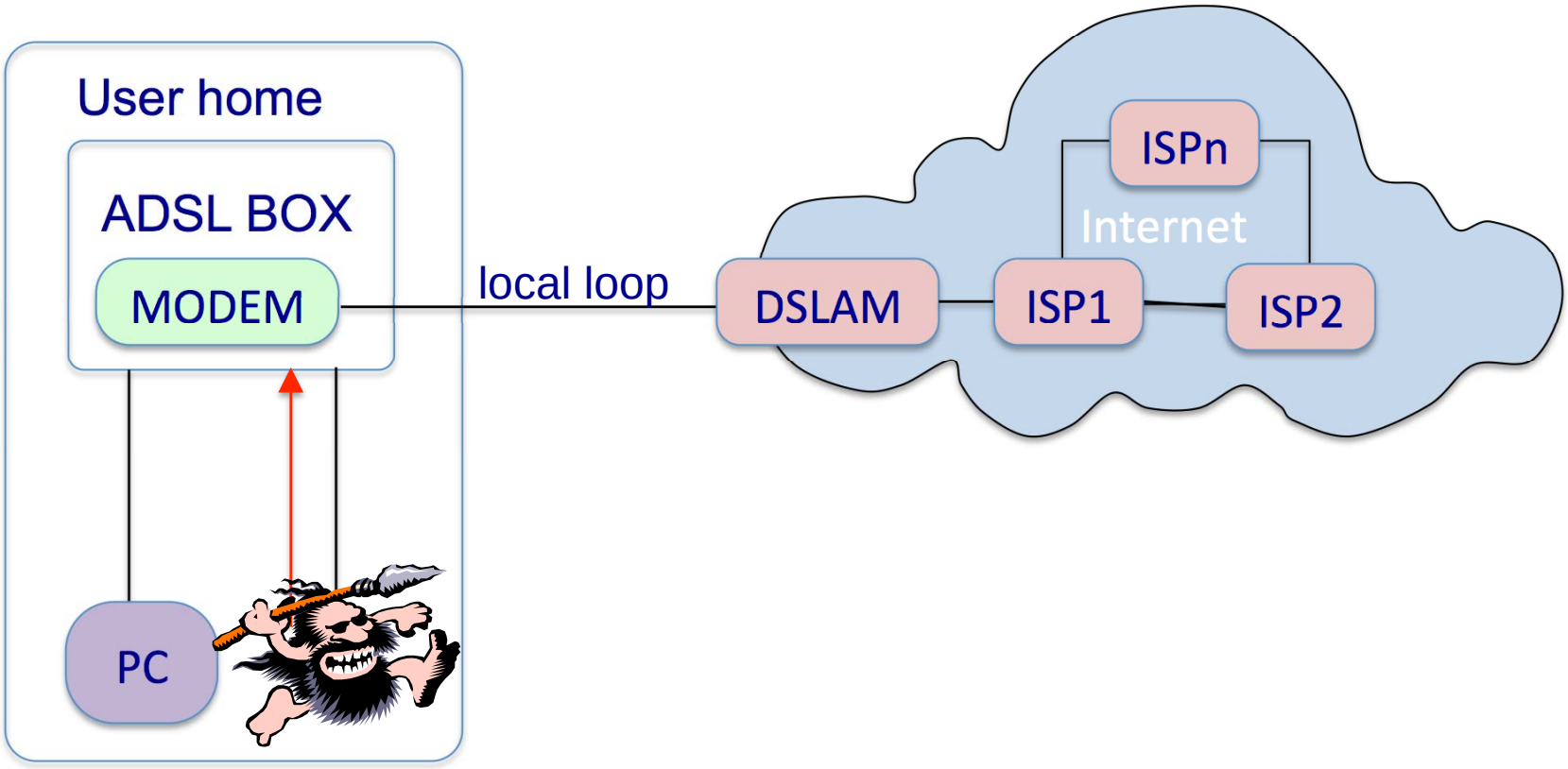


DSLAM: Digital Subscriber Line Access Multiplexer

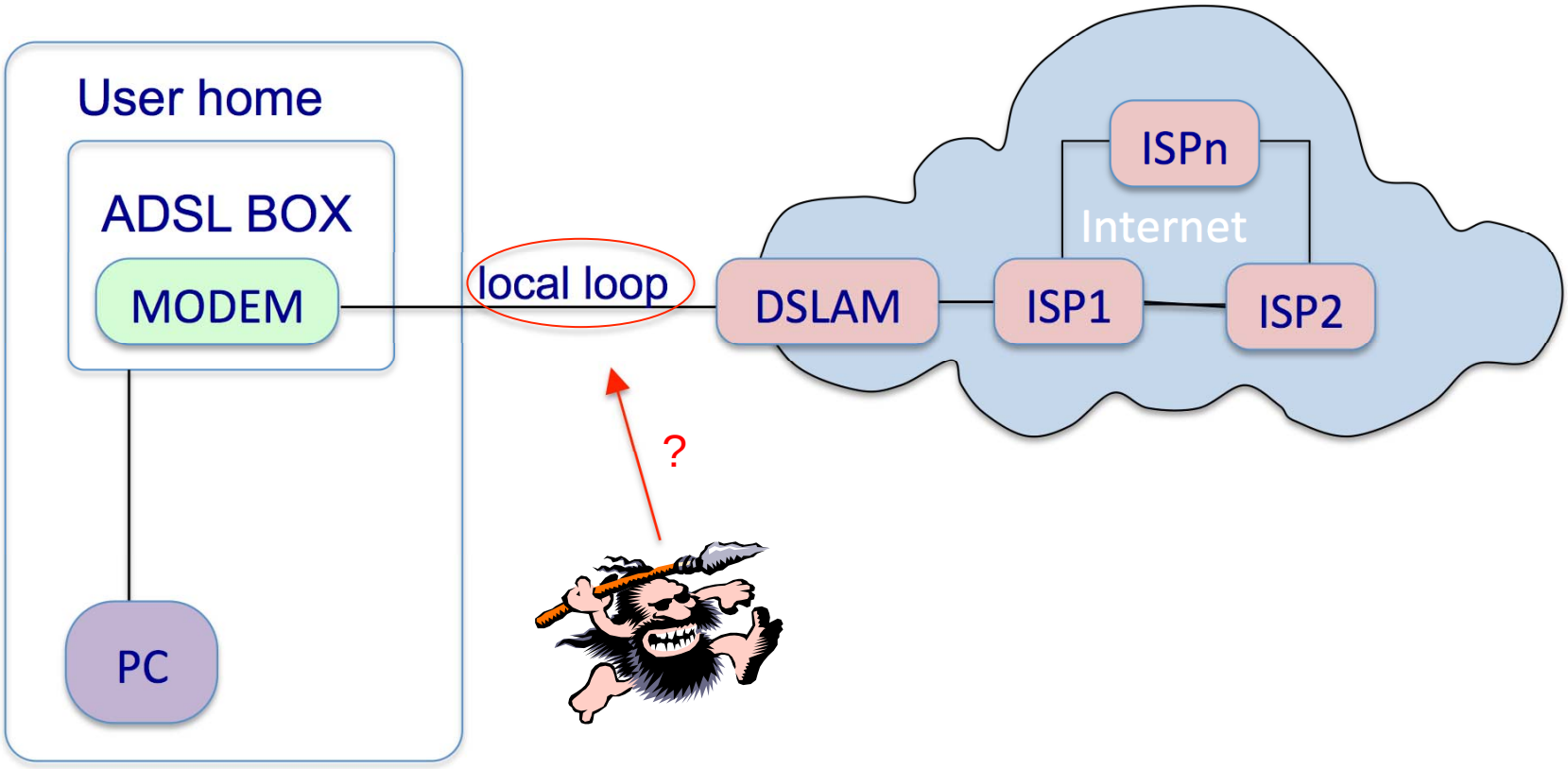
Attack scenarios (1)



Attack scenarios (2)



Attack scenarios (3)

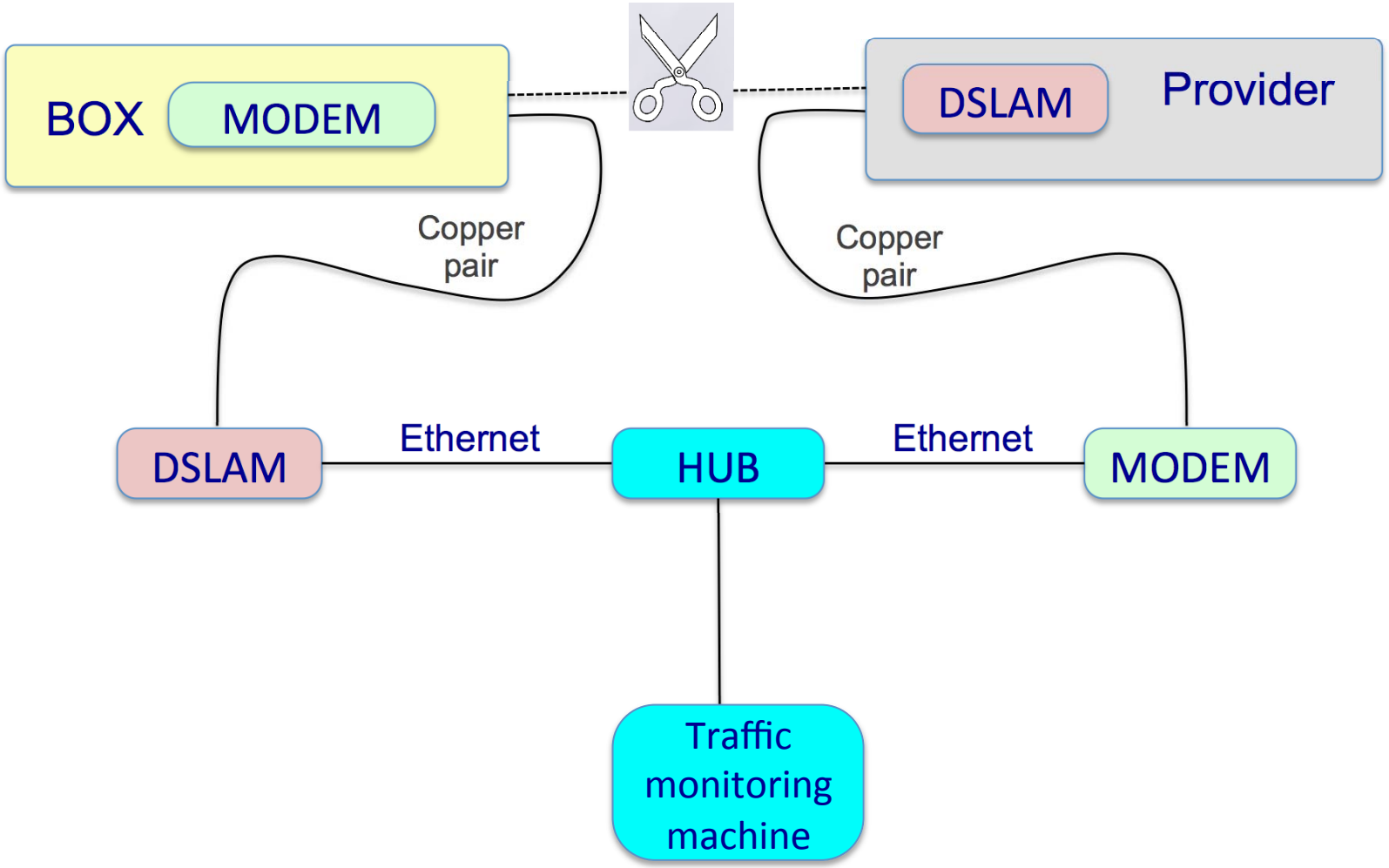


Research objectives

- Design of an experimental platform to analyze the communications between ADSL boxes and the Internet, by monitoring traffic on the local loop
  - Boot up and configuration set up phase
- Compare the different protocols used and identify potential weaknesses
- Illustrate the feasibility of some attack scenarios exploiting such weaknesses and identify countermeasures

Local loop

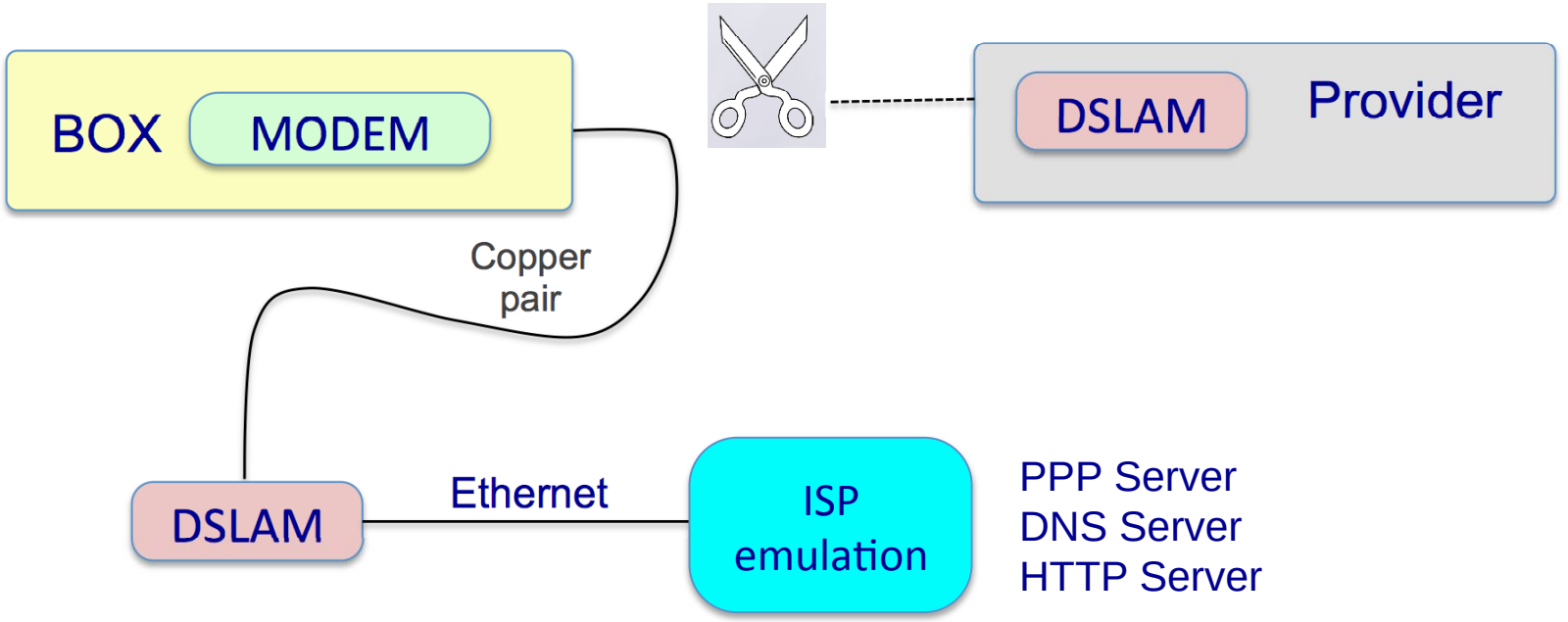
Observing traffic on local loop



Comparative analysis of different boxes

BOX	ATM	PPP	DHCP	SIP	Configuration	Firmware update
A	8/35/LLC	chap	no	MD5	HTTP, FTP, SSL	-
B	8/35/LLC	chap	yes	MD5	HTTP, SSL	SSL
C	8/36/VC	no	yes	MD5	SSL	-
D	8/35/LLC	chap	yes	MD5	HTTP	HTTP
E	8/35/LLC	chap	yes	MD5	HTTP	HTTP
F	8/35/LLC	chap	no	MD5	SSL	-

ISP service emulation



Results

- Installation of a personalized firmware
  - Partial deactivation of the firewall
  - Addition of a super-user account
  - Disabling of firmware updates
  - Installation of a rogue software
- Successful exploitations
  - Remote connection to the ADSL box
  - Initiation of premium rate phone calls
- Other possible attacks
  - DOS
  - Botnet
  - etc.

Conclusion and other ongoing work

- ADSL boxes are vulnerable
- Countermeasures
  - Generalization of encryption techniques during critical exchanges
  - Measuring variation of signal attenuation on the ADSL line
    - It should drastically change when one inserts our platform on the local loop
- Other ongoing studies
  - Vulnerability assessment of smart digital TVs
    - Track illegitimate information flow and privacy violations