telindus

Belgacom ICT

Broadcasting by Misuse of Satellite ISPs

André Adelsbach
Telindus Luxembourg

Ulrich Greveler
Ruhr-Universität Bochum, Germany

CHANGE THINGS YOUR WAY

October 27, 2006
Unrestricted

Outline

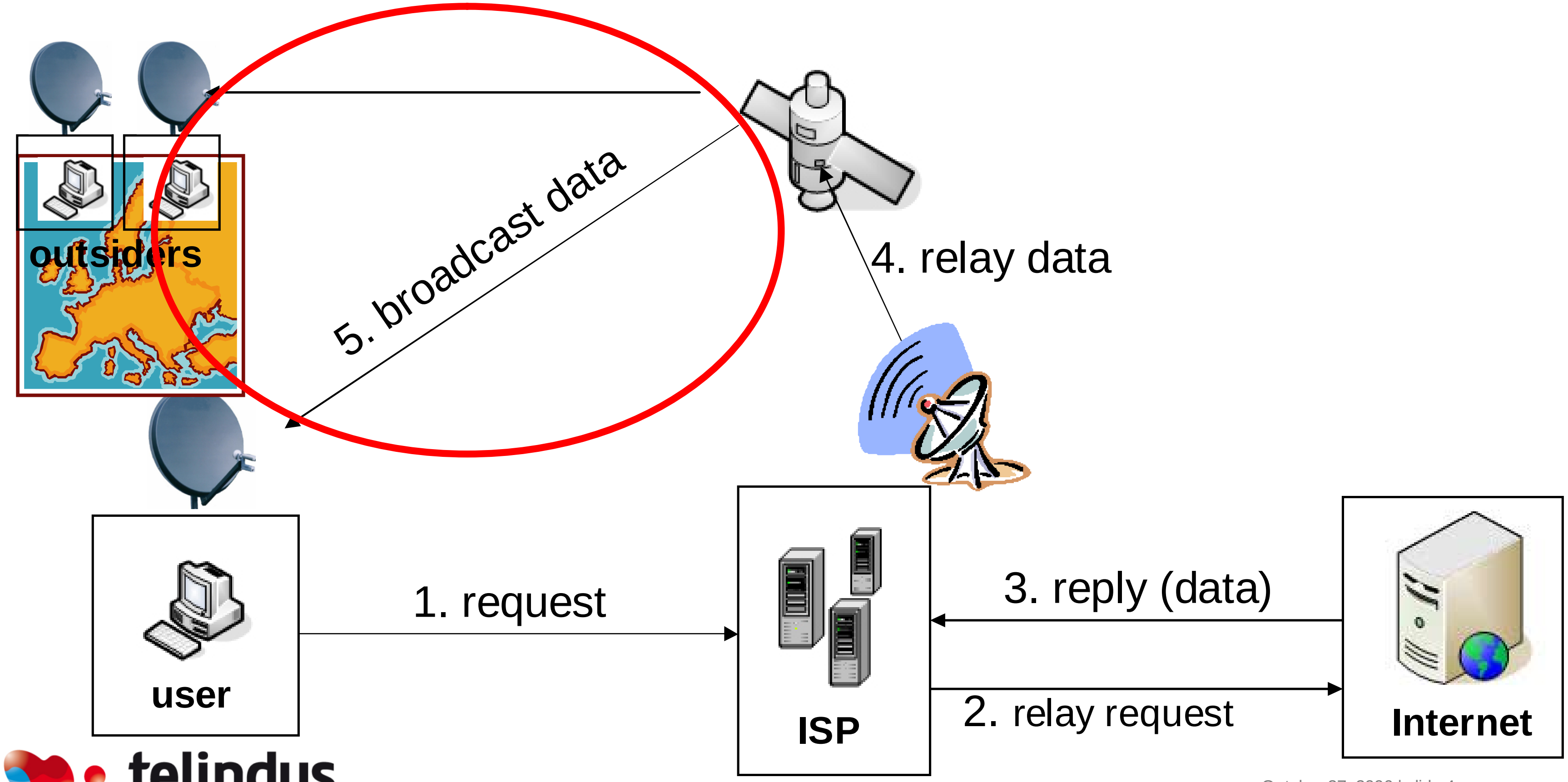
- Introduction: Internet via Satellite
- Some « History » – How we got here
  - Privacy & security issues for users
  - Misuse for Data Broadcasts by
    - outsiders
    - insiders
- Crypto-Enforced Unicast Communication on broadcast/shared channel
  - Abstract Communication Model & Instantiations
  - Insider Attacks: how to misuse ISP for broadcasts despite of encryption
  - Countermeasures against Insider Attacks
- Conclusion

Introduction – Internet via Satellite (I)

- Satellites:
  - Specialized wireless transmitter, placed in Geostationary orbit (36.000 km)
  - 280 ms for ground station ➔ satellite ➔ ground : use of PEPs !
  - Transmit radio, television, …and data (e.g. internet access)
  - Cover low-infrastructure areas (no DSL, or no cable/leased line)
- How Satellite ISPs work
  - « Home-user edition »: mostly asymmetric communication
    - upstream via dial-up; DVB downstream via satellite broadcast
    - TCP/IP packets are encapsulated in DVB frames
  - User’s equipment: PC, satellite dish, DVB card, ISDN card, software proxy

Introduction – Internet via Satellite (II)

- How Satellite ISPs work



telindus
Belgacom ICT

Unrestricted

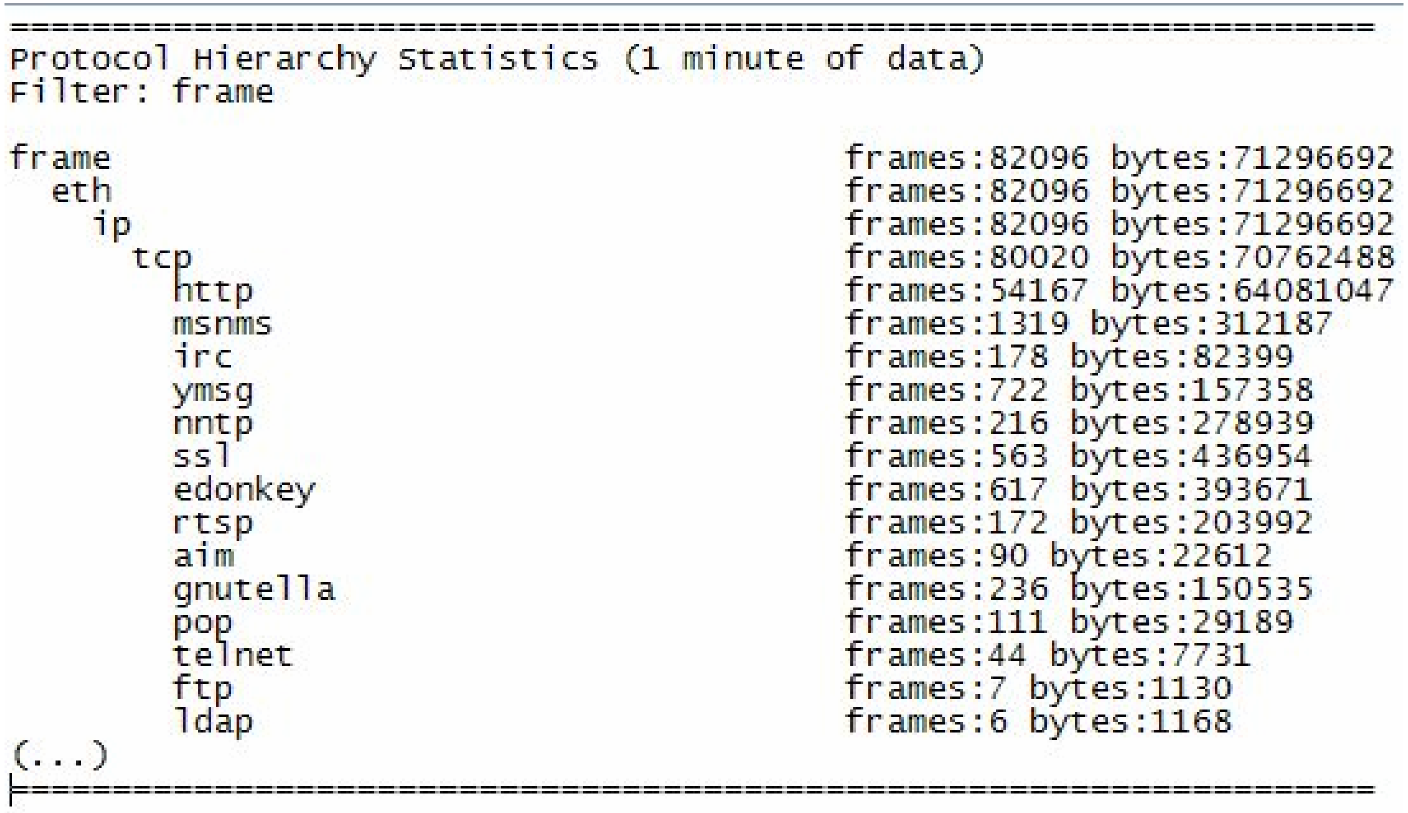
« History » - How we got here (I)

- 2004: study on Satellite ISPs at Ruhr-University of Bochum
  - Findings: (apparently known to hackers before)
    - Some Satellite ISPs do not encrypt satellite downstream
      ➔ can be passively sniffed with standard PC, satellite dish & DVB card

      ➔ Linux DVB driver gives you a network interface that can be sniffed with any standard network sniffer (e.g., Ethereal/Wireshark)
    - sniffing is possible in the whole footprint
    - attackers can do it at home; no way to catch them

« History » - How we got here (I)

- 2004: study on Satellite ISPs at Ruhr-University of Bochum



```
===================================================================
Protocol Hierarchy Statistics (1 minute of data)
Filter: frame

frame                                     frames:82096 bytes:71296692
  eth                                     frames:82096 bytes:71296692
    ip                                    frames:82096 bytes:71296692
      tcp                                 frames:80020 bytes:70762488
        http                              frames:54167 bytes:64081047
        msnms                             frames:1319 bytes:312187
        irc                               frames:178 bytes:82399
        ymsg                              frames:722 bytes:157358
        nntp                              frames:216 bytes:278939
        ssl                               frames:563 bytes:436954
        edonkey                           frames:617 bytes:393671
        rtsp                              frames:172 bytes:203992
        aim                               frames:90 bytes:22612
        gnutella                          frames:236 bytes:150535
        pop                               frames:111 bytes:29189
        telnet                            frames:44 bytes:7731
        ftp                               frames:7 bytes:1130
        ldap                              frames:6 bytes:1168
(...)
===================================================================
```

« History » - How we got here (II)

- 2004: study on Satellite ISPs at Ruhr-University of Bochum
  - attackers can sniff user’s downlink
    - web browsing (HTTP response including cookies)
    - emails, chats
    - some users even try to run VOIP via Satellite ISPs

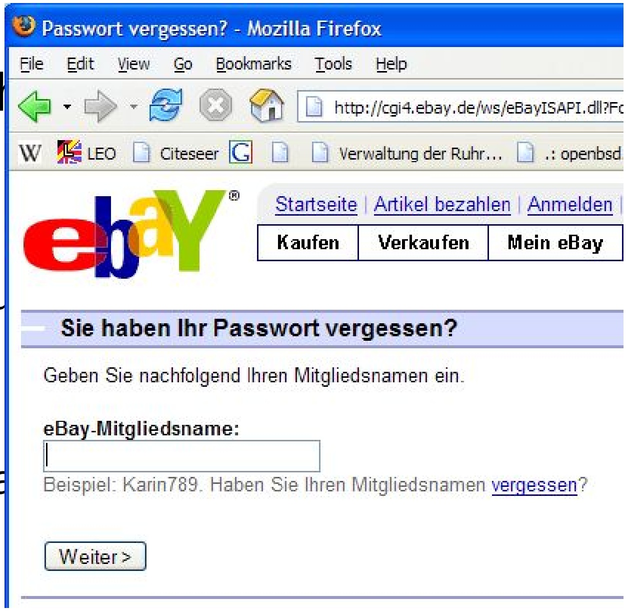
➔ severe security risks for users !
e.g. identity theft (cookies, password recovery via email)

➔ severe privacy risks for users (extensive profiling possible)

➔ **Recommendation:** users should use Satellite ISP that offer encryption or make sure that they use security mechanisms on higher layers (SSL, SSH, ...)

« History » - How we got here (II)

- 2004: study on Satellite ISPs at Ruh
  - attackers can sniff user's downlink
    - web browsing (HTTP response inclu
    - emails, chats
    - some users even try to run VOIP via


Passwort vergessen? - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://cgi4.ebay.de/ws/eBayISAPI.dll?Fo
W LEO Citeseer G Verwaltung der Ruhr... .: openbsd
ebay
Startseite | Artikel bezahlen | Anmelden
Kaufen Verkaufen Mein eBay
Weiter >

Sie haben Ihr Passwort vergessen?

Geben Sie nachfolgend Ihren Mitgliedsnamen ein.

eBay-Mitgliedsname:

Beispiel: Karin789. Haben Sie Ihren Mitgliedsnamen vergessen?

➔ severe security risks for users !
e.g. identity theft (cookies, password recovery via email)

➔ severe privacy risks for users (extensive profiling possible)

➔ **Recommendation:** users should use Satellite ISP that offer encryption or make sure that they use security mechanisms on higher layers (SSL, SSH, ...)

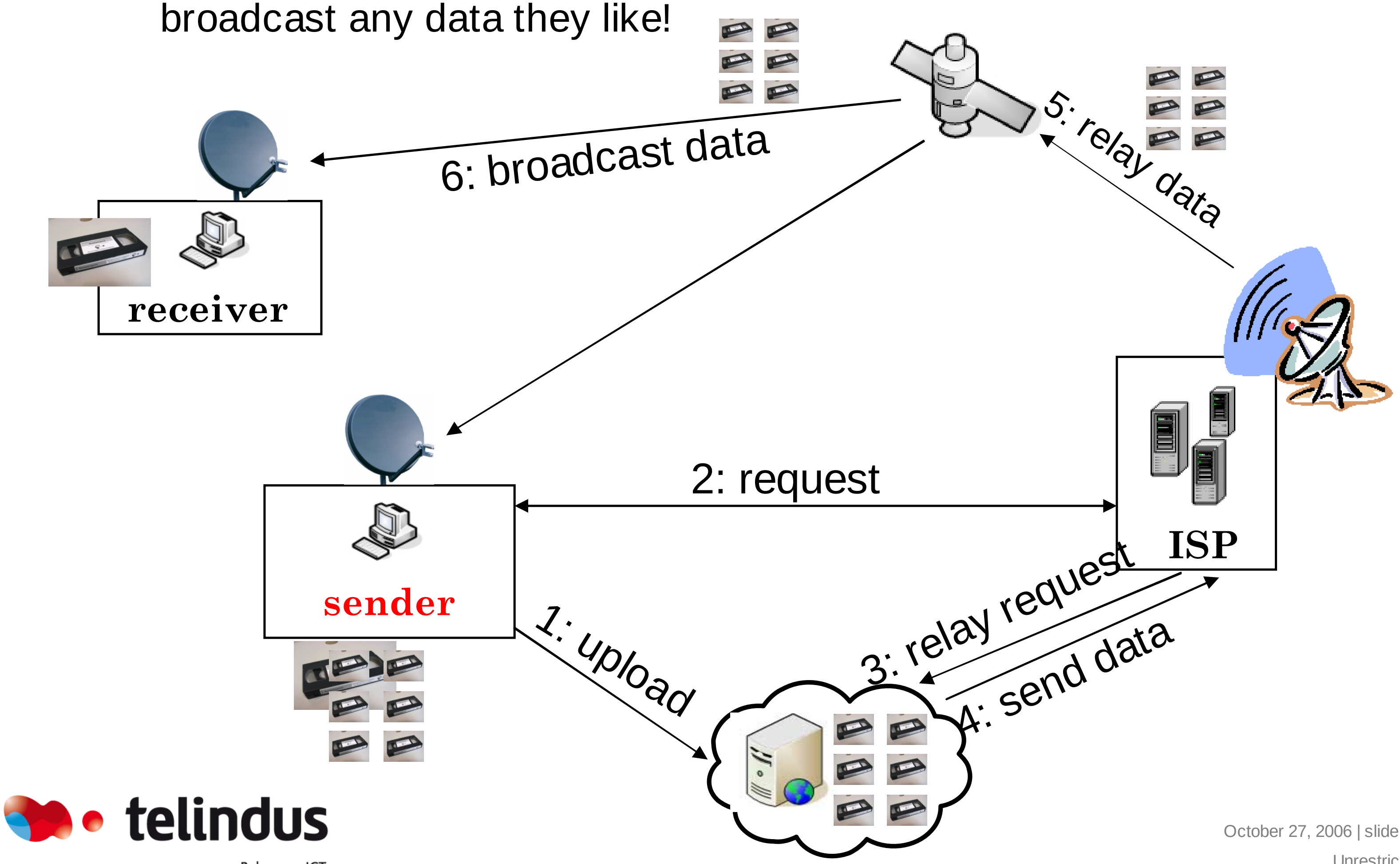
« History » - How we got here (III)

- **Question: Any other security issues due to unencrypted Satellite Downlink?**
- **Outsider attackers** can misuse users of Satellite ISPs to broadcast any data they like!
  - Just send an email with data attached to users
    - when users fetch email from their POP3 account the attackers data will be broadcasted
    - receivers are completely passive and remain perfectly anonymous !
    - attackers may use remailers to stay anonymous as well
    - data can even be encrypted or hidden ➔ perfect for criminals
    - best thing: its for free ☺
  - Countermeasure: Satellite ISPs should offer encrypted downlinks

telindus
Belgacom ICT

« History » - How we got here (IV)

- **Insider attackers** can « misuse » the Satellite ISP themselves to broadcast any data they like!



Why Satellite ISPs should care about such Broadcasts ?

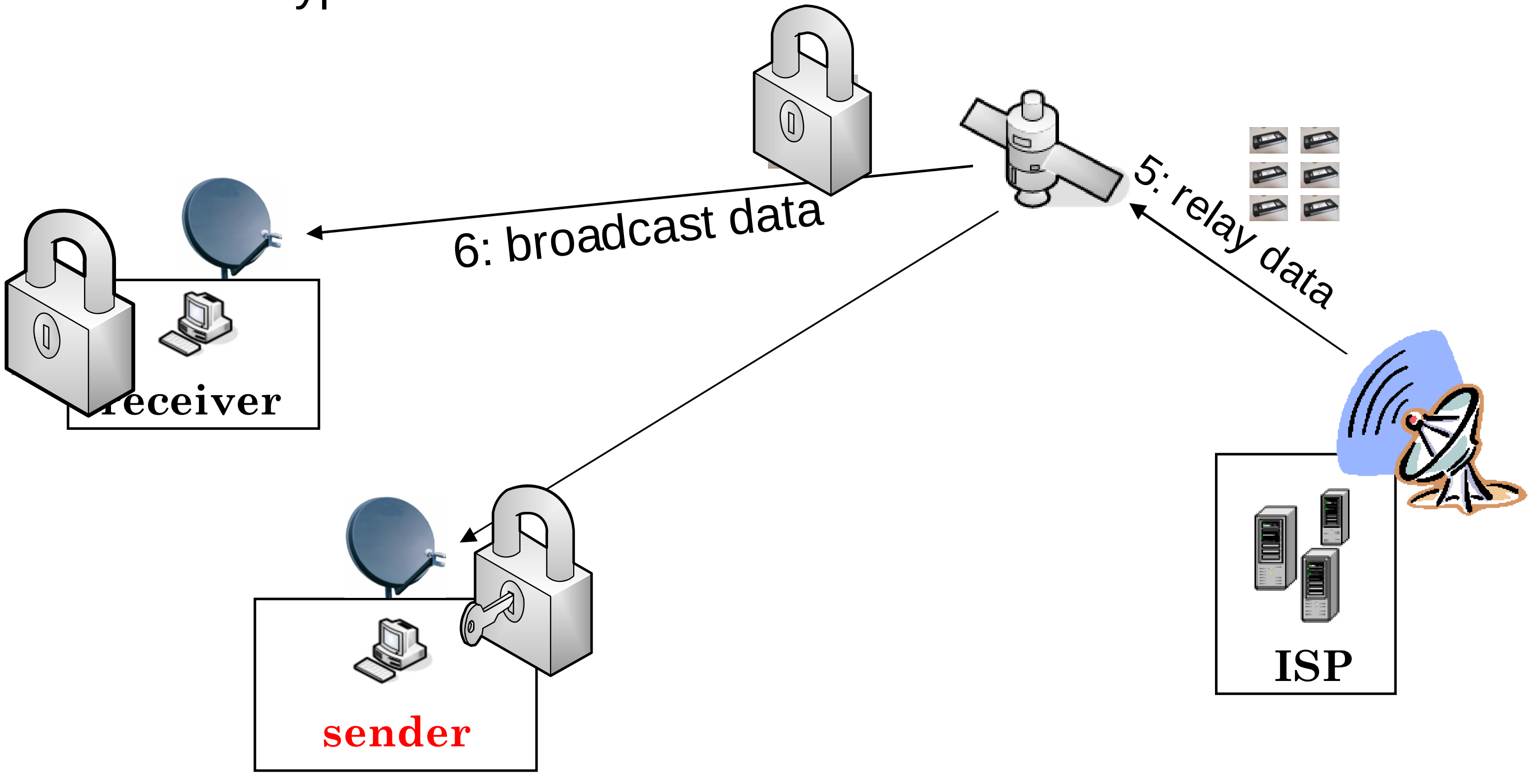
- It may harm the ISP's business model
  - broadcasts are sold at a higher price
- Possible liability and impact on reputation if illegal content is broadcasted
- Attack other services offered by Satellite operator or its customers
  - Card-Sharing attacks: legitimate customers of Pay-TV service distribute their keys to peers
    - mostly unicasts ➔ scales not well to larger groups of peers
  - Next Generation Card-Sharing Attacks on Pay-TV
    - (Mis-)using the Satellite ISP allows to broadcast these keys via the same channel that distributes the encrypted Pay-TV.

      ➔ directly harms the business of Pay-TV provider
      ➔ indirectly harms the business of Satellite carriers

telindus
Belgacom ICT

Effective Countermeasures ?

- What can carriers do to prevent this ?
  - encrypt the satellite downlink !



telindus

Belgacom ICT

Insider Attacks Enabling Data Broadcasts on Crypto-Enforced Unicast Networks

André Adelsbach
Telindus Luxembourg

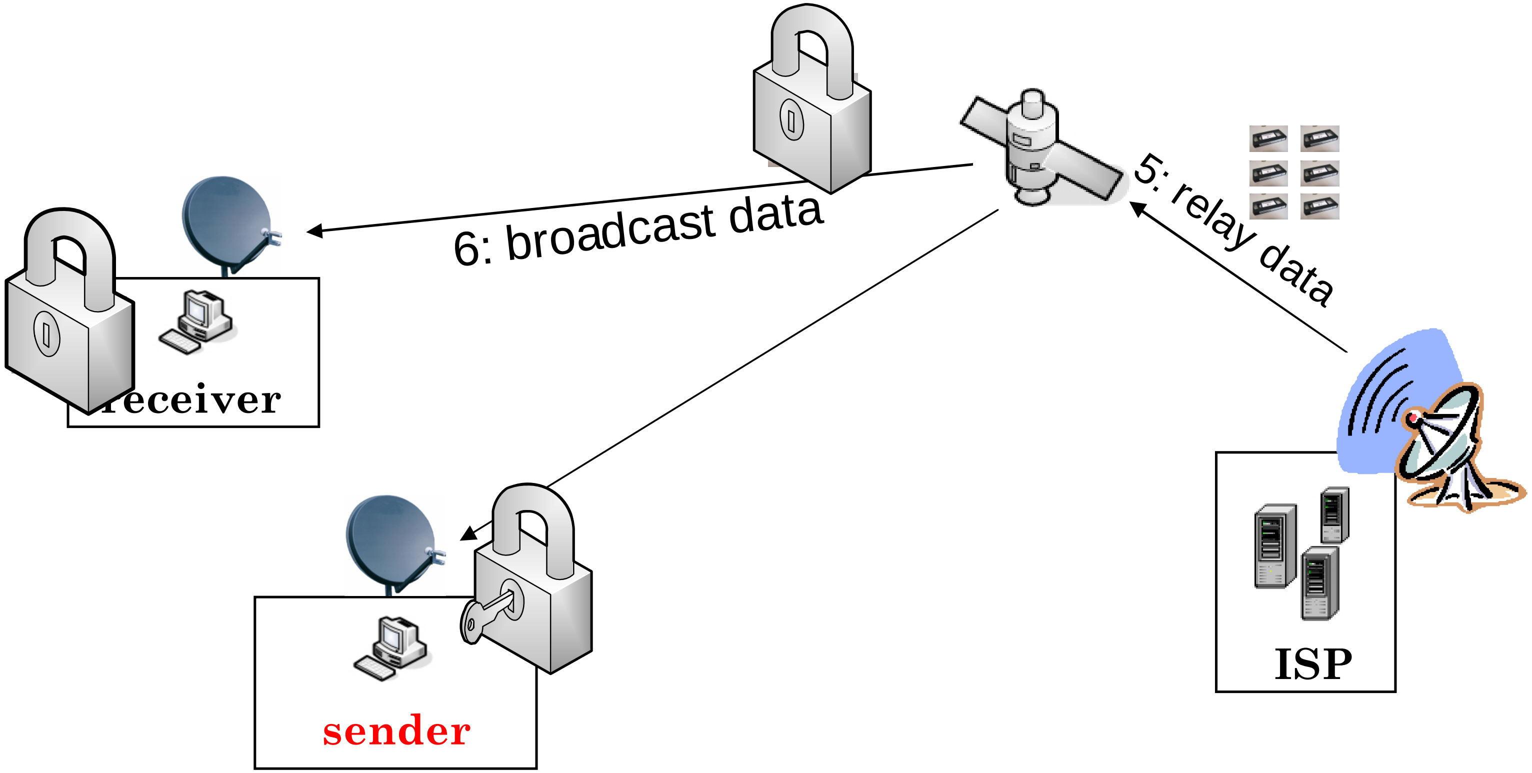
Ulrich Greveler
Ruhr-Universität Bochum, Germany

CHANGE THINGS YOUR WAY

October 27, 2006
Unrestricted

Effective Countermeasures ?

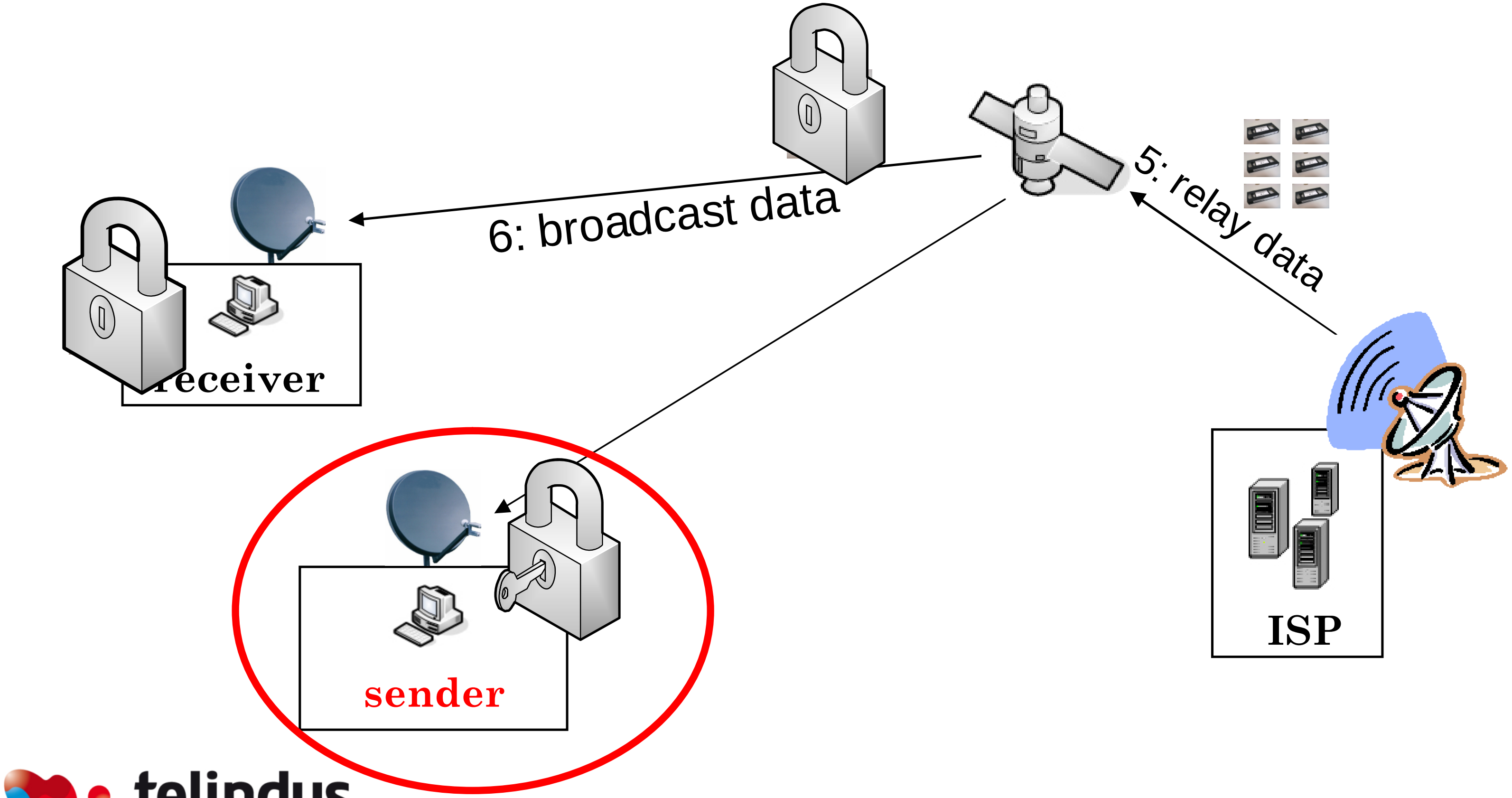
- **Observation:** secure communication protocols aim to prevent outsider attacks



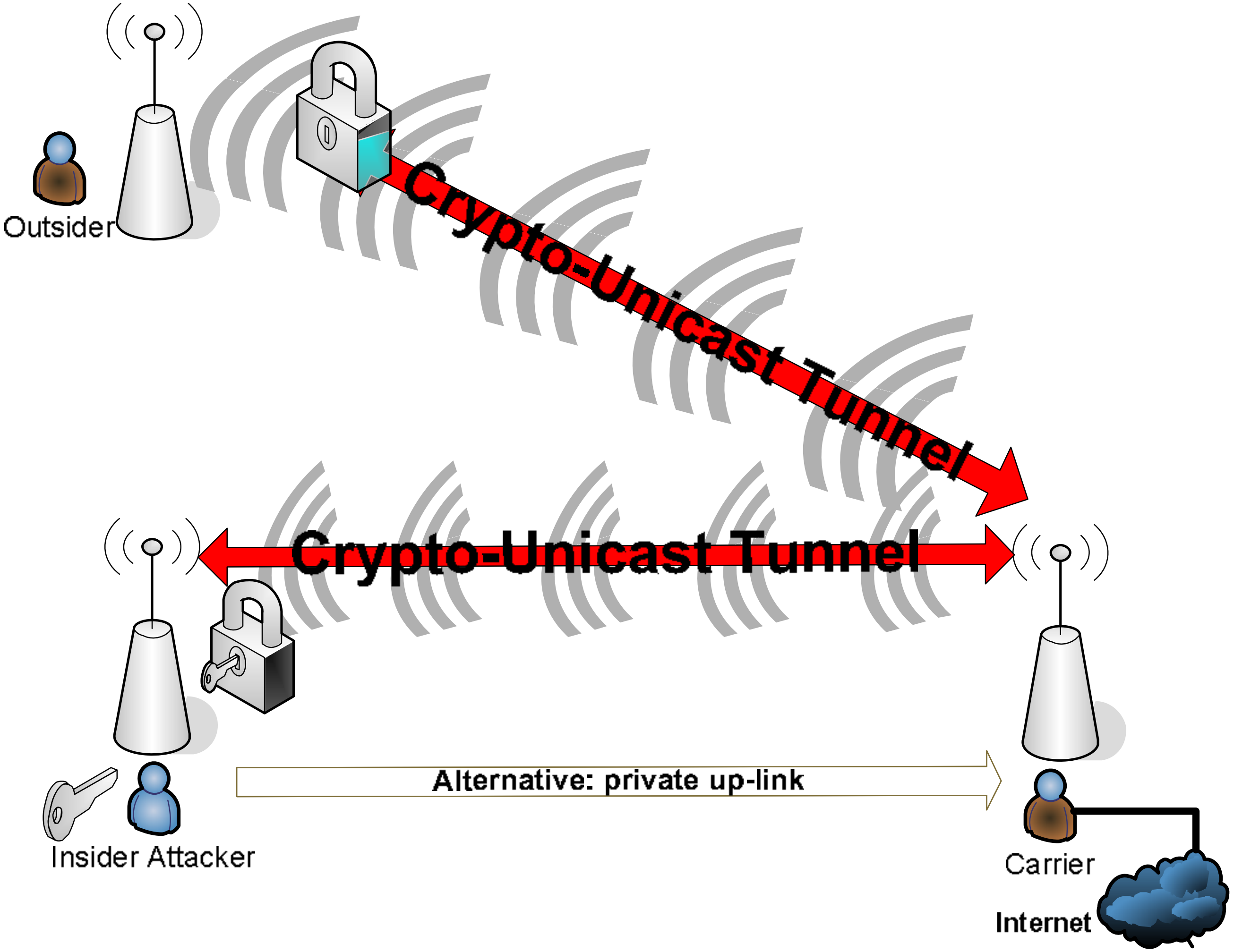
telindus
Belgacom ICT

Effective Countermeasures ?

- But we are dealing with an insider attacker who participates in the protocol and knows the decryption key ...



Generalization to broadcast/shared-medium ISPs

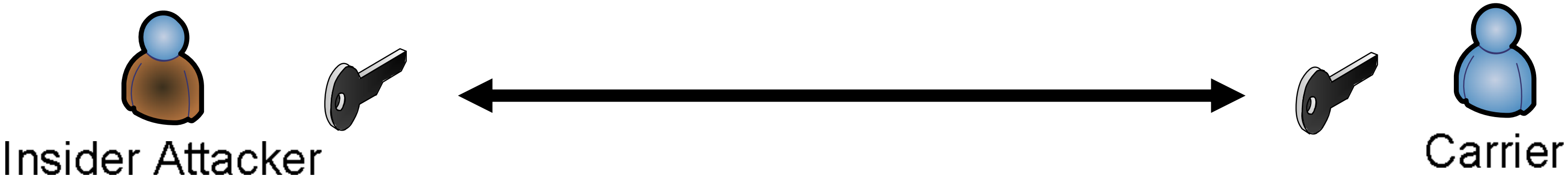


Generalization to broadcast/shared-medium ISPs

- Abstract Communication Model
  - Roles: ISP, user (insider attacker) and outsiders
  - ISP ➔ Users: Broadcast Channel (signals can be received by outsiders)
    - unicast communication enforced by encryption
  - Users ➔ ISP: either Broadcast or private channel
- Instantiations: WIMAX ISPs, WLAN ISPs, Cable ISPs, Satellite ISPs
- But: Satellite ISPs offer the best value for attackers
  - highly asymmetric capabilities in terms of coverage

Insider Attacks

- Crypto-Unicast-Tunnel is established in two phases:
  - Key-Exchange Phase: user and ISP exchange a key



  - Encrypted Transmission Phase: user and ISP communicate encrypted

Crypto-Unicast Tunnel

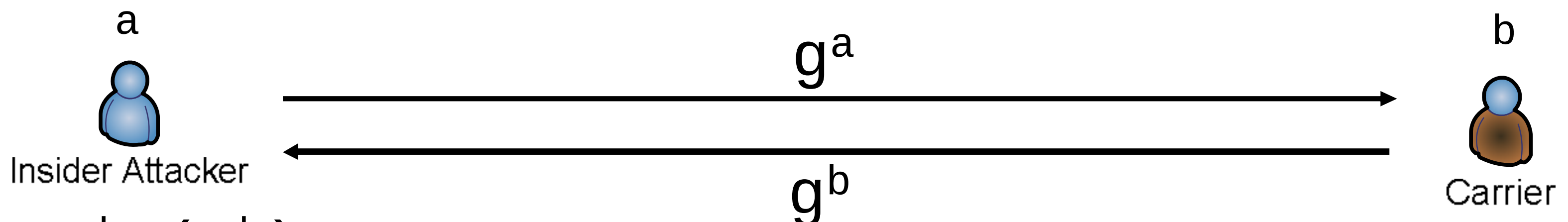
- Insider attacker can try to attack both phases.......

Insider Attacks on Key-Exchange Phase (I)

- Insider Attacks normally not considered in practice
- Insider can always distribute its keys (if he can access it)
  - direct communication, publish in newsgroup, IRC
    ➔ requires additional communication !
  - covert timing channels on broadcast channel
- better ways to attack key-exchange to make sure that outsiders get keys automatically?
  - force key-exchange to yield fixed keys (e.g., 0x00000) a-priori known to outsiders
  - coined «key control» in research

Insider Attacks on Key-Exchange Phase (II)

- Some susceptible examples:
  - Key-Transport (if used from user to ISP) [unusual]
  - Diffie Hellman Key-Agreement: Setup large prime p; generator g



a

Insider Attacker

g^a

g^b

b

Carrier

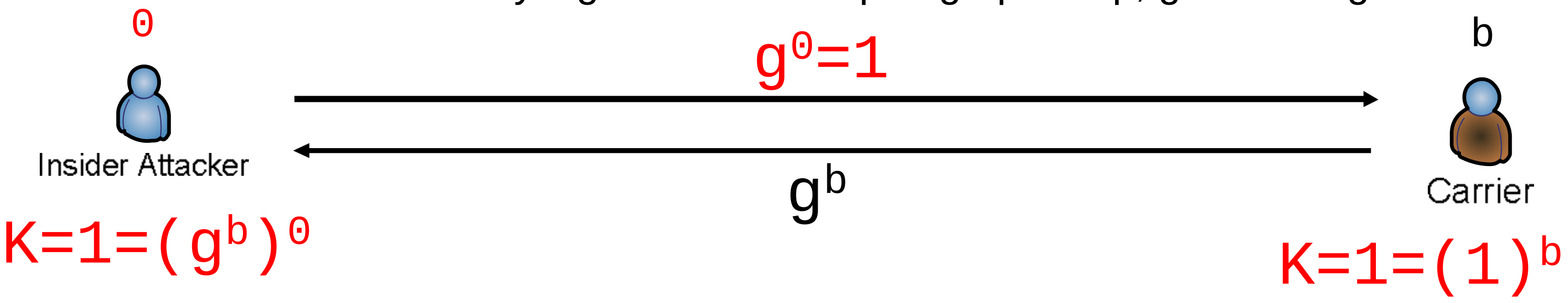
$K=g^{ab}=(g^b)^a$

$K=g^{ab}=(g^a)^b$

- Use Cases:
  - DOCSIS/WIMAX: Key-Transport from ISP to User
    ➔ not susceptible
  - Some Satellite ISPs use DH via dial-up connection
    ➔ may be susceptible

Insider Attacks on Key-Exchange Phase (II)

- Some susceptible examples:
  - Key-Transport (if used from user to ISP) [unusual]
  - Diffie Hellman Key-Agreement: Setup large prime p; generator g



0

b

$g^0=1$

Insider Attacker

g^b

Carrier

$K=1=(g^b)^0$

$K=1=(1)^b$

- Use Cases:
  - DOCSIS/WIMAX: Key-Transport from ISP to User
    ➔ not susceptible
  - Some Satellite ISPs use DH via dial-up connection
    ➔ may be susceptible

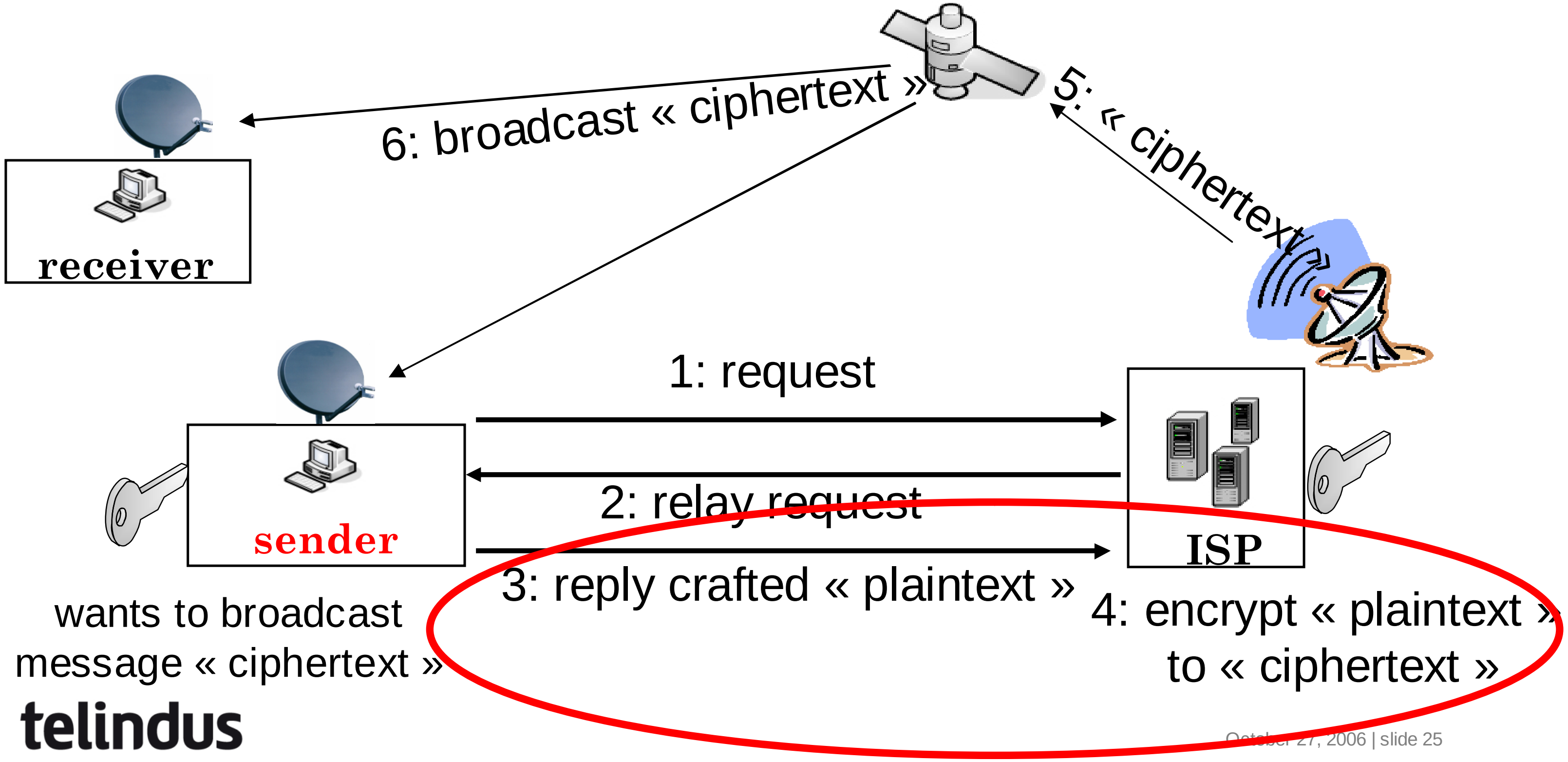
Insider Attacks on Encrypted Transmission Phase (I)

- Idea
  - if insider cannot make the ISP broadcast the message in plaintext...
  - ... the insider may try to make the ISP broadcast « ciphertext » that is exactly the message he wants to broadcast

telindus
Belgacom ICT

Insider Attacks on Encrypted Transmission Phase (I)

- Insider can make the ISP broadcast « ciphertext » that is exactly the message he wants to broadcast
- Illustration:


6: broadcast « ciphertext »
5: « ciphertext »
receiver
1: request
2: relay request
sender
ISP
3: reply crafted « plaintext »
4: encrypt « plaintext » to « ciphertext »
wants to broadcast message « ciphertext »

Insider Attacks on Encrypted Transmission Phase (II)

- Goal: make the ISP broadcast « ciphertext » that is exactly the message the attacker wants to broadcast to outsiders

- Assumption: insider attacker knows the key *k* and he knows encryption scheme *(E, D)* used by ISP

- Setting: attacker requests data *m* from ISP
  ➔ ISP applies encryption *c* = *E(k,* m) and broadcasts *c*

- So, if attacker wants the ISP to broadcast a specific ciphertext *c'*, the attacker computes and replies data m' s.t.

$$c' = E(k, m')$$

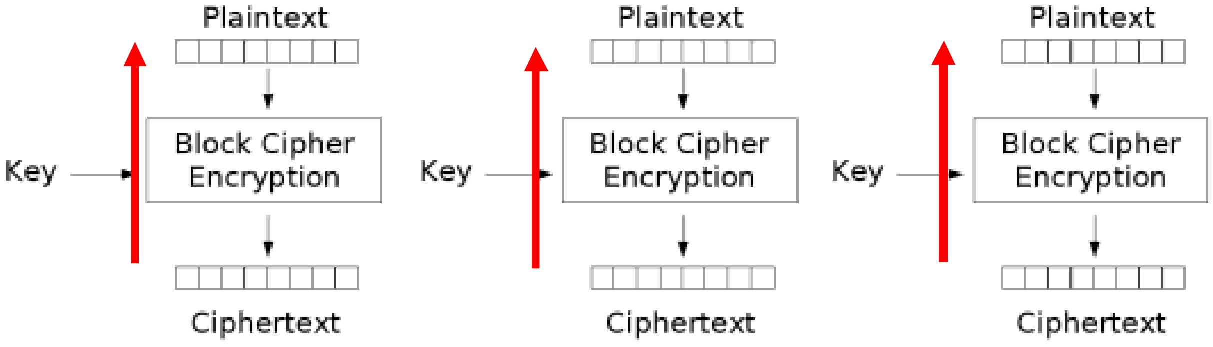
telindus
Belgacom ICT

Insider Attacks on Encrypted Transmission Phase (III)

- So, if attacker wants the ISP to broadcast a specific ciphertext *c'*, the attacker computes and replies data m' s.t.

  $c' = E(k, m')$

- Some examples: Block Cipher in ECB Mode



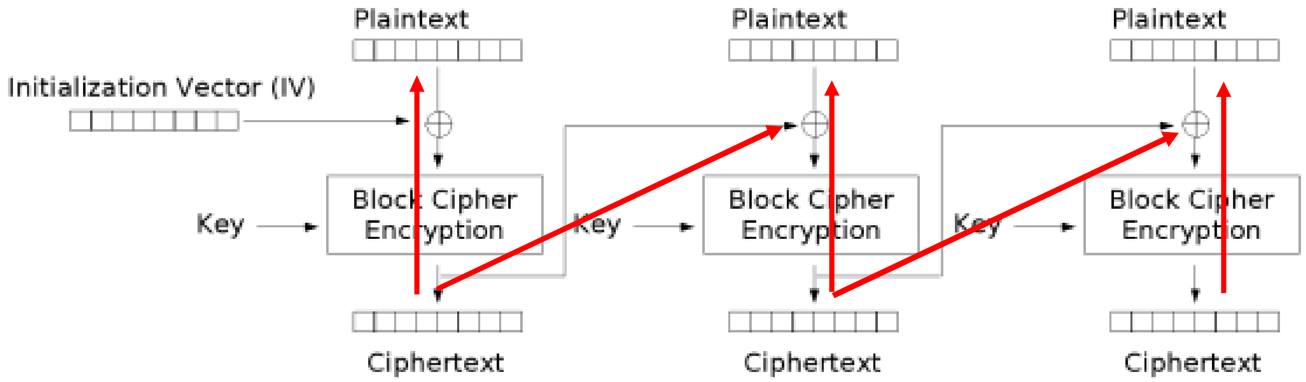
Electronic Codebook (ECB) mode encryption

Insider Attacks on Encrypted Transmission Phase (IV)

- So, if attacker wants the ISP to broadcast a specific ciphertext *c'*, the attacker computes and replies data m' s.t.

$$c' = E(k, m')$$

- Some examples: Block Cipher in CBC Mode (WIMAX/DOCSIS)



Cipher Block Chaining (CBC) mode encryption

Countermeasures

- Key-Exchange Phase
  - use protocol not susceptible to key control attacks
  - frequent key updates requires insider attacker to publish keys at higher rate
  - deter publication of keys by including personal data into keys (credit card number....)
- Encrypted Transmission Phase
  - Randomize the encryption, such that insider attacker cannot craft data that will be encrypted to a specific ciphertext
  - e.g., random prefix to each message block
  - future research.....

Conclusion

- ISPs that operate via broadcast/shared-media should not only offer encryption as an option, but make its use mandatory !
  - leaving users the choice to not use encryption paves the way to
    - broadcast illegal content
    - attack other services of the ISP (e.g., Pay TV)
- Prevention of insider attacks is not trivial
  - many block-cipher modes of operation (OFB,CTR) & stream ciphers are susceptible to the presented insider attack
  - not an «insecurity» of these ciphers, because it was not a design criterion – they are rather applied in the wrong setting
    ➔ can not submit it to FSE 2007 ☹
  - interesting area of future research

telindus
Belgacom ICT

Questions and Answers

Thank you for your attention !

telindus

Belgacom ICT