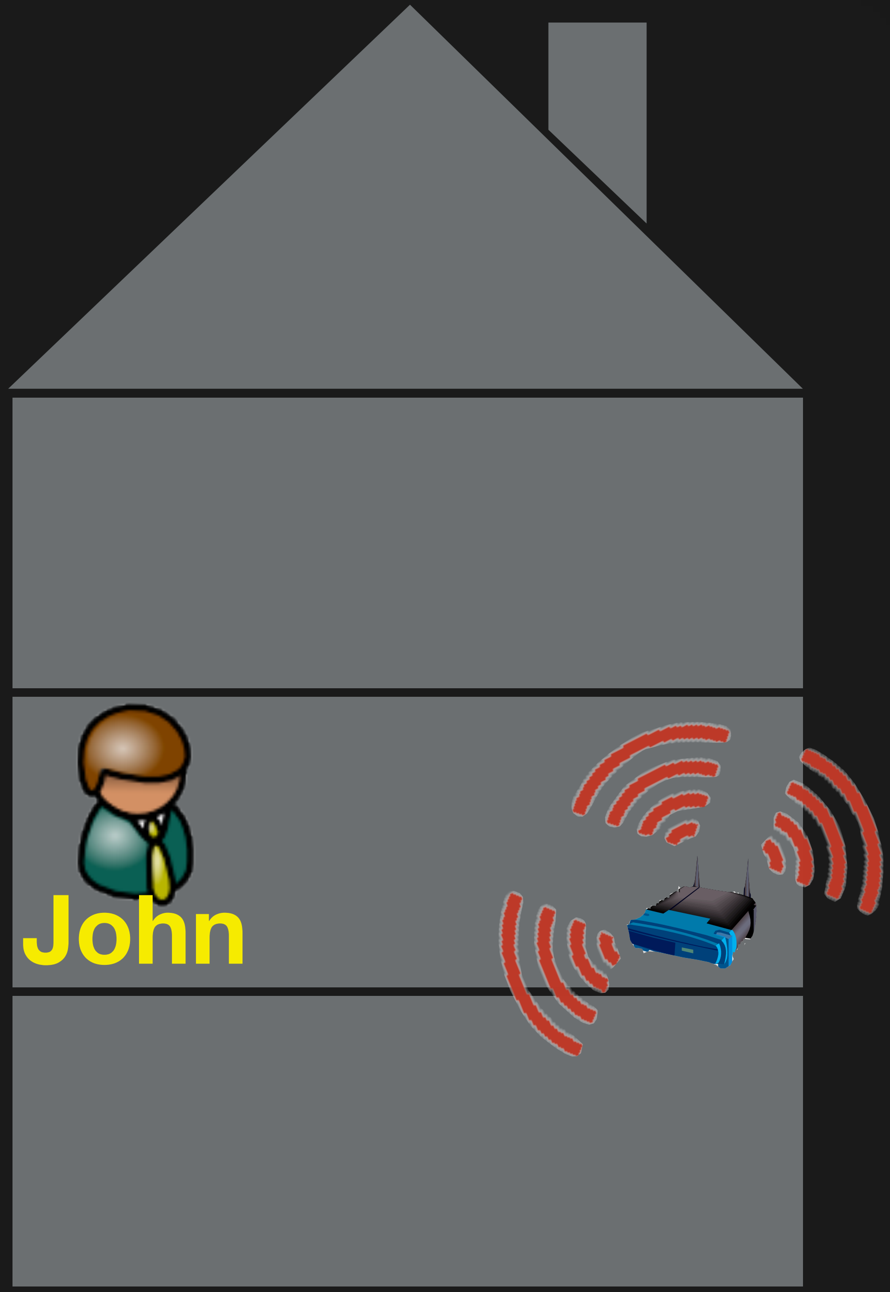
Wireless Roaming using 3-Party Authentication & Tunnels

Damien LEROY[1], Mark MANULIS[2],
Olivier BONAVENTURE[1]

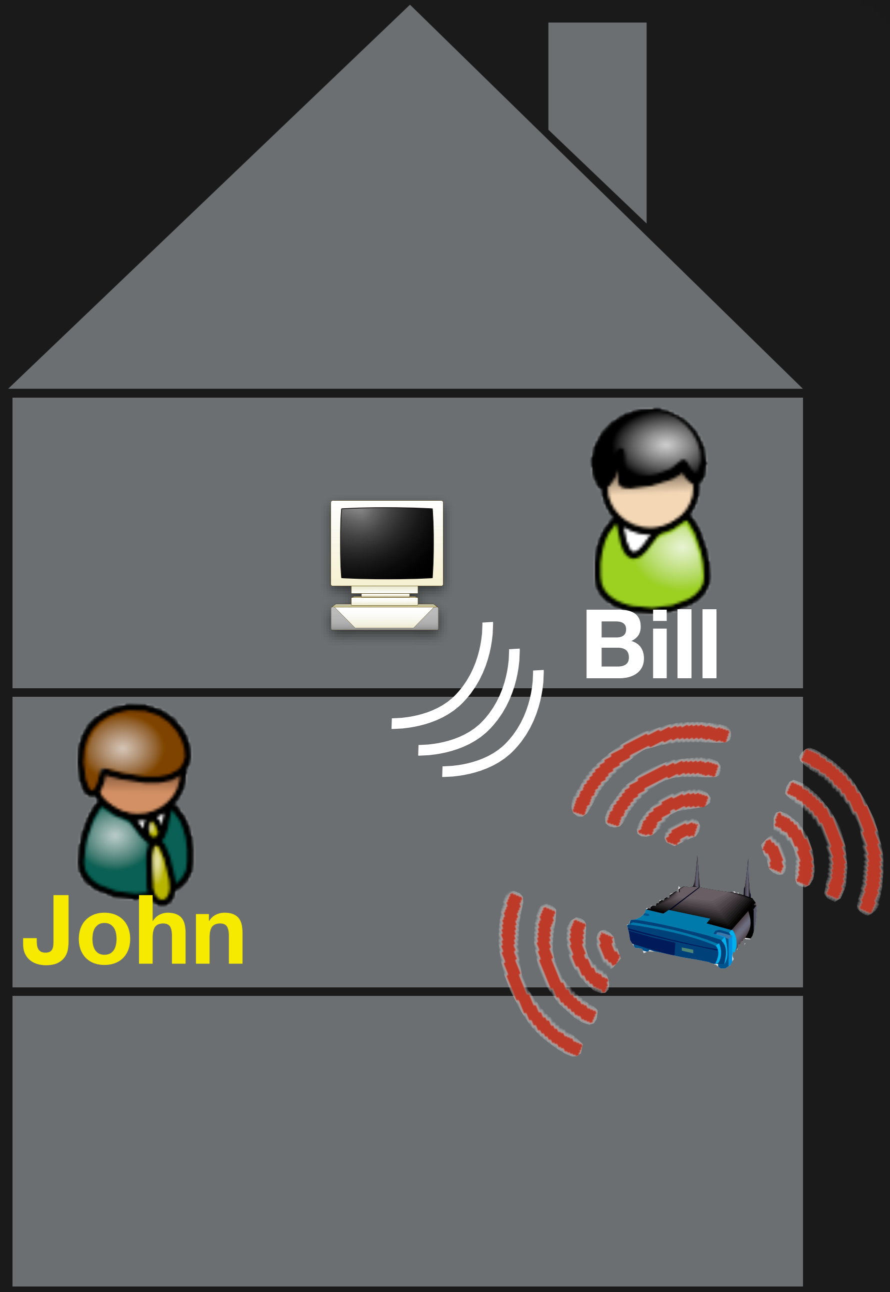
[1]UCLouvain (Be), [2]TU Darmstadt & CASED (De)

U-Net '09 - December 1st, 2009

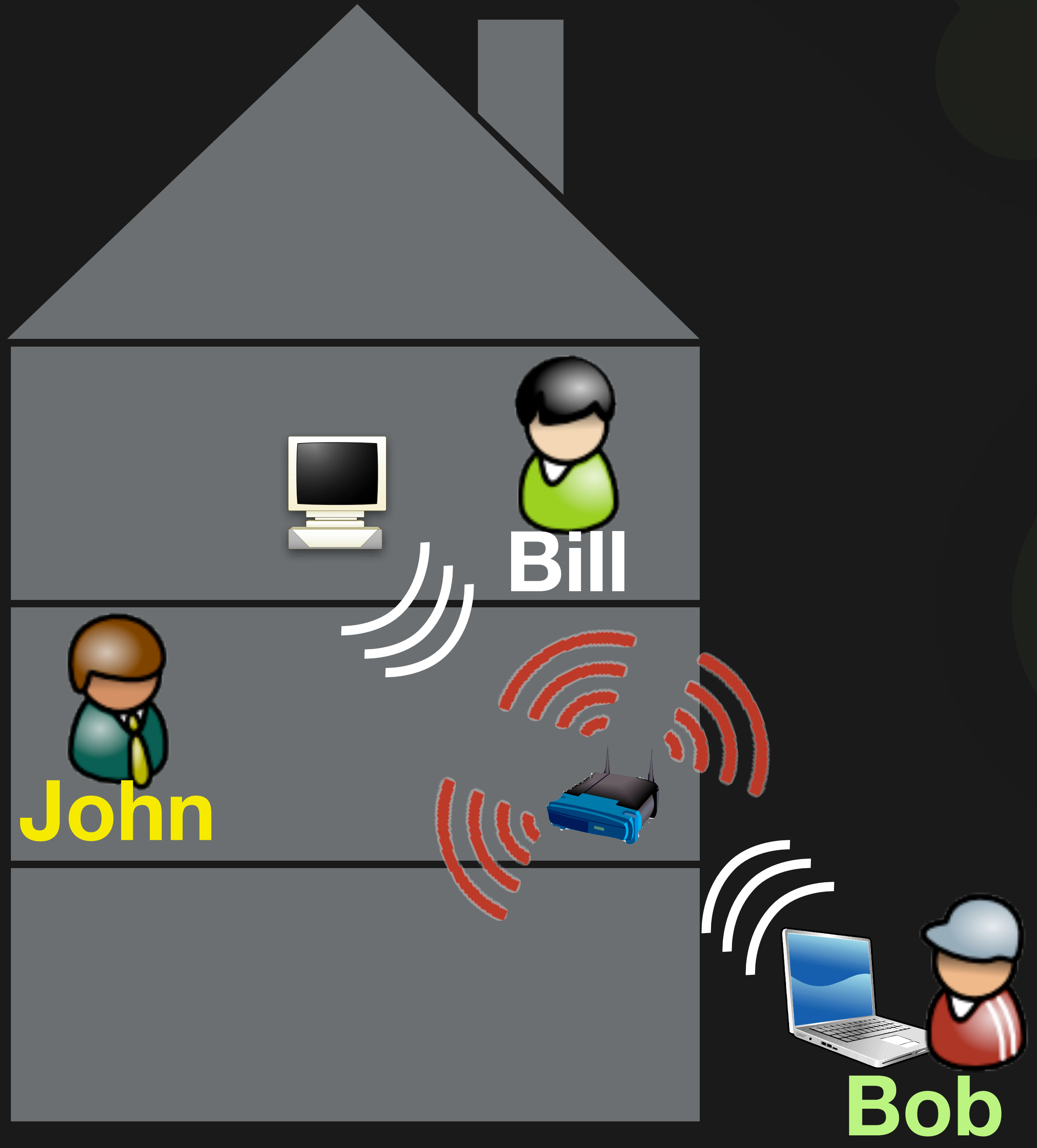
Let’s consider basic WiFi sharing



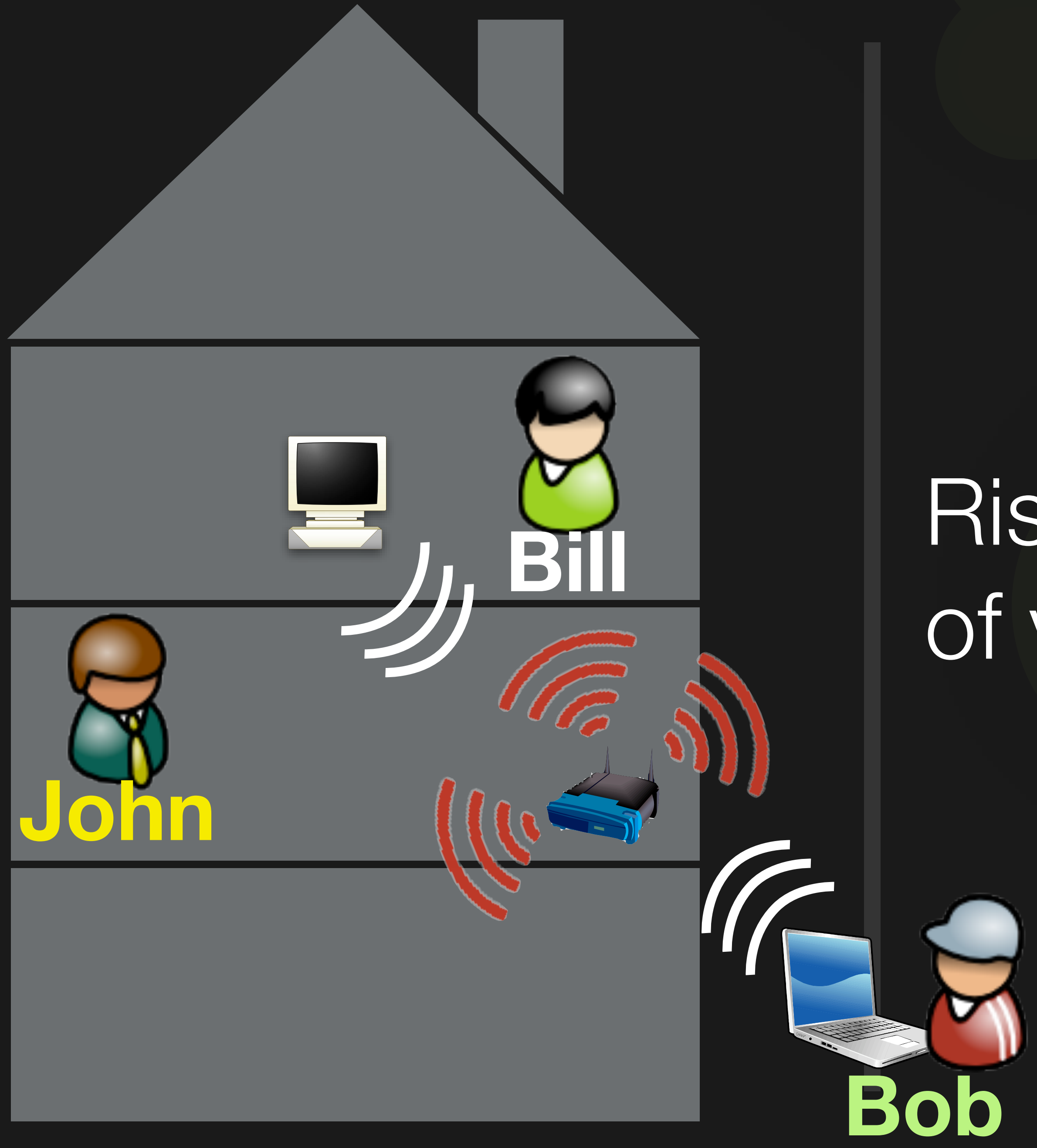
Let’s consider basic WiFi sharing



Let’s consider basic WiFi sharing

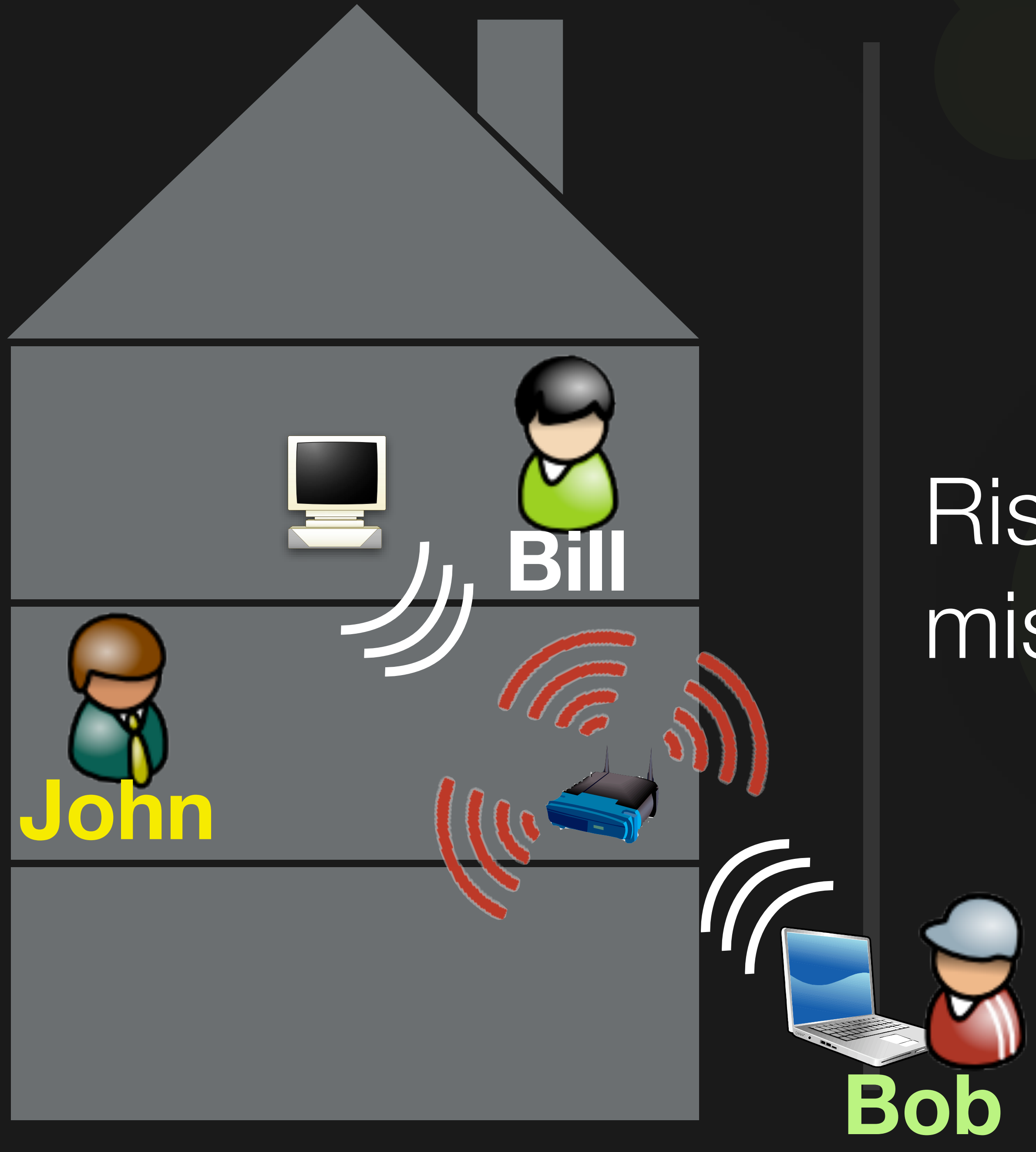


There are lots of risks in sharing one's WiFi connection



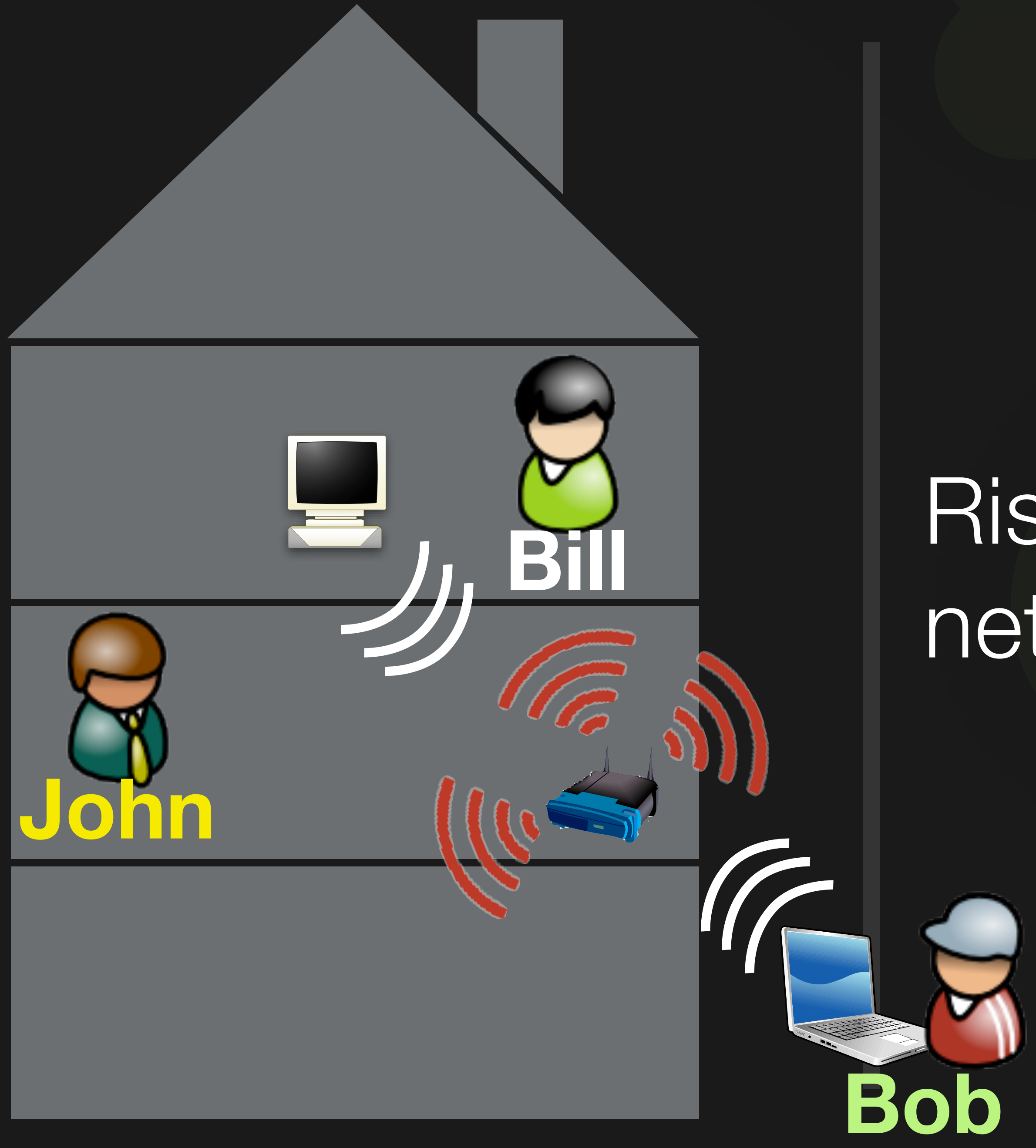
Risk 1: Legal issues because of visitor's behaviors

There are lots of risks in sharing one’s WiFi connection



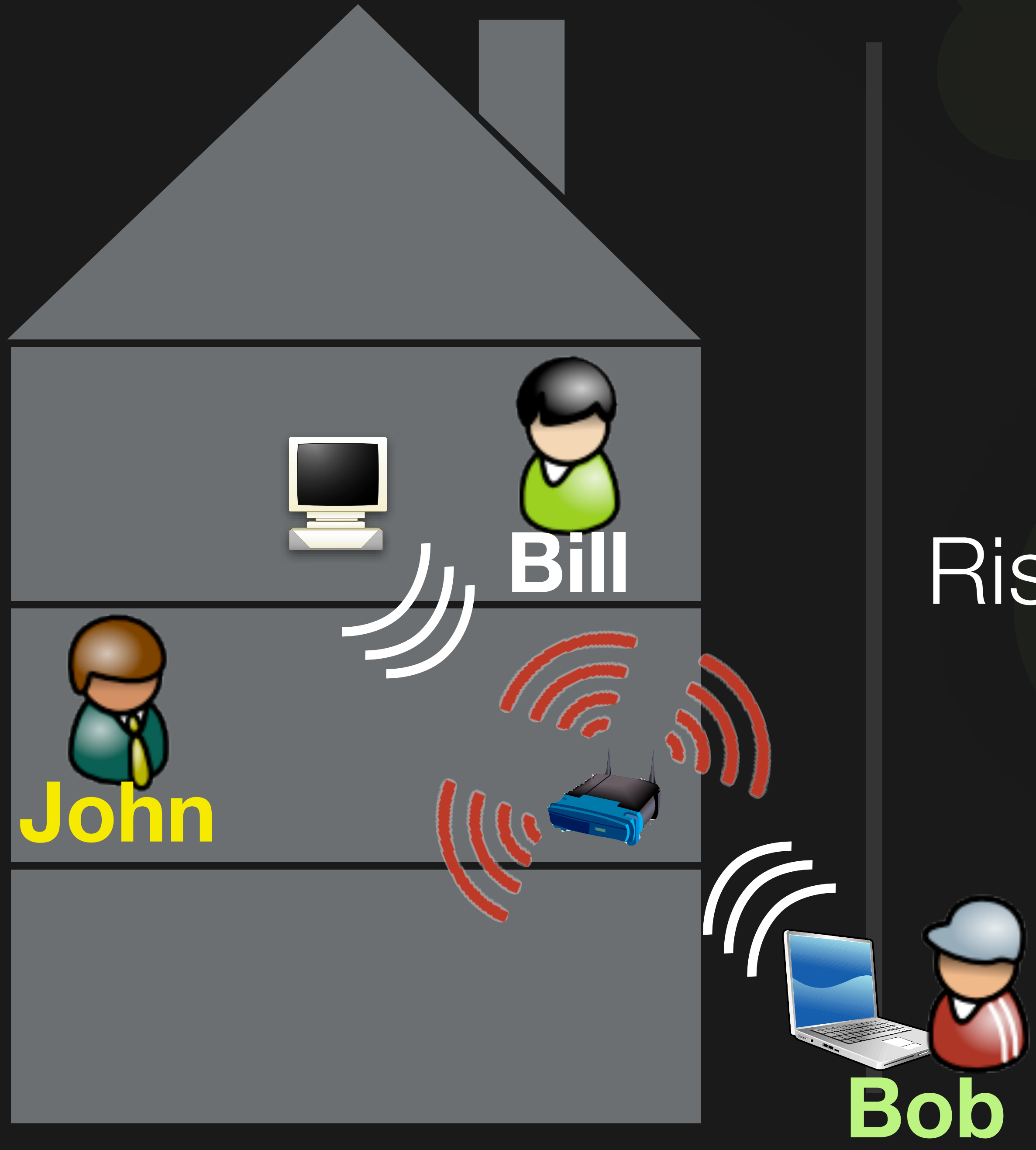
Risk 2: Issues with ISP for misbehavior

There are lots of risks in sharing one's WiFi connection



Risk 3: Attack on John's network

There are lots of risks in sharing one’s WiFi connection



Risk 4: Resource consumption

There are risks in connecting to a shared network

Bill
John
Bob

Risk 5: Man-in-the-Middle attacks

- Sniffing
- Pharming

- Even if AP trusted (AP/SSID spoofing)

The main 5 risks in WiFi sharing

- ✗ legal issues
- ✗ ISP issues
- ✗ attack on visited network
- ✗ resource consumption
- ✗ MITM

Structure of the Presentation

Review of existing solutions

Our proposal

Implementation & Deployment

Software-based WiFi sharing

WEP/WPA keys shared by users on the service website

Specific software must be used

When connecting to a WiFi, the software knows the WEP/WPA key to use wifi.com free yourself!

WHISHER Beta

Software-based WiFi sharing: Issues

Visitors are connected on the same SSID as the AP’s owner

SSID<->key mapping is stored on clients (!!!)

Easy to set up a fake AP to obtain keys

Software-based WiFi sharing: ... risks are still there

- ✗ legal issues
  - but user could be identified
- ✗ ISP issues
- ✗ attack on visited network
- ✓ resource consumption
- ✗ MITM
- ✗ + keys can be known
  - risky if linked to other passwd

Hardware-based WiFi sharing

Have to buy the FON AP

One private SSID (encrypted), One public (open + web-auth)

Access to FON users & paying users

Hardware-based WiFi sharing: issues

Visitors’ traffic can be sniffed

15 free minutes for anybody

Easy to set up a fake AP to stealing FON credentials

Hardware-based WiFi sharing: ... some risks are still there

- ✗ legal issues
- ✗ ISP issues
- ✓ attack on visited network
- ✓ resource consumption
- ✗ MITM

Wisher/Wifi.com & FON are not really satisfying...

Mainly on the following topics:

- liability (against ISP and law)
- possibility of MITM attack from the visited network
- easy to place a fake AP

Structure of the Presentation

Review of existing solutions

Our proposal

Implementation & Deployment

Remaining issues can be solve, but we need another solution

Liability (against ISP and law)

- visitors and users from the visited network must not be mixed on the Internet

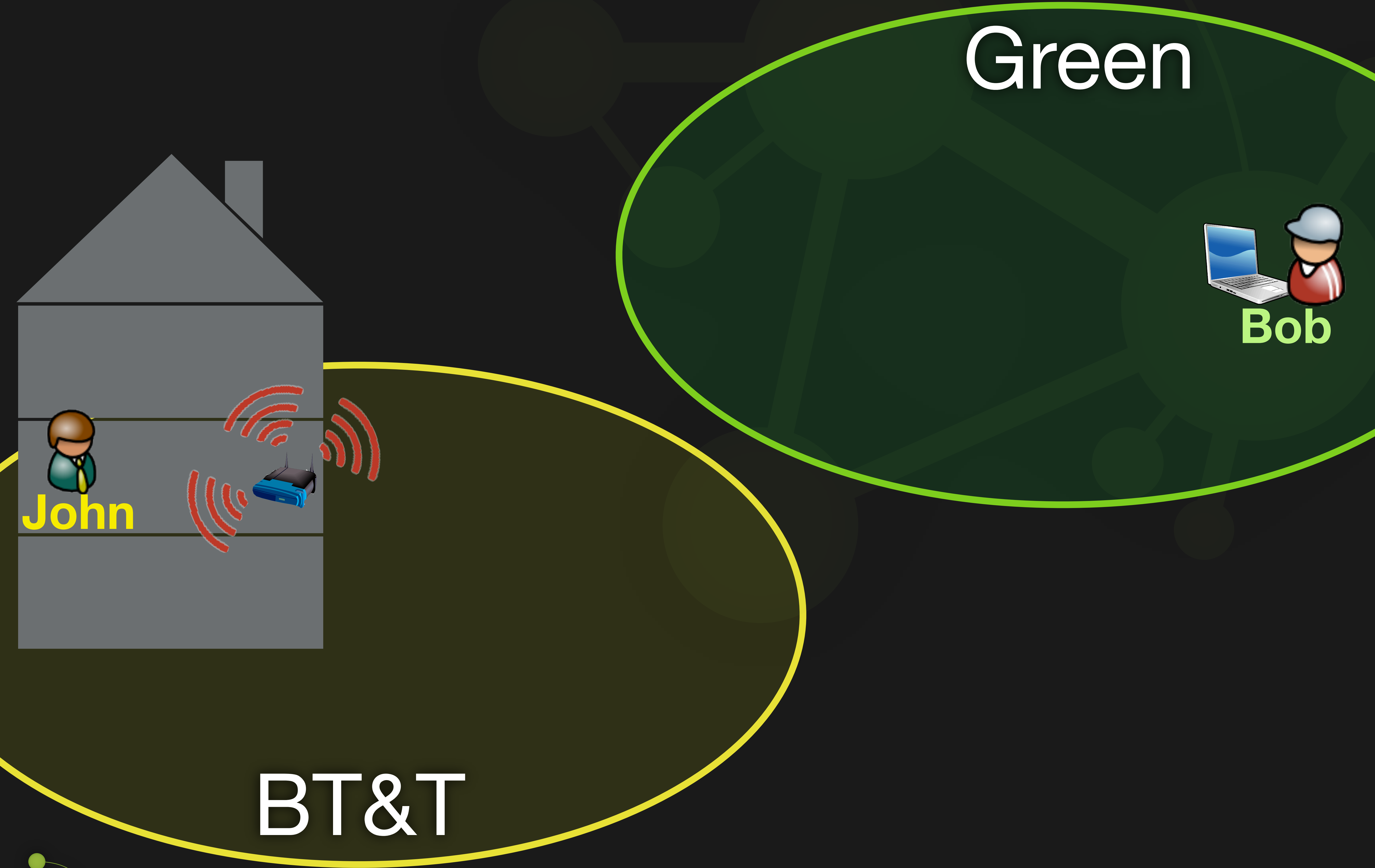
Possibility of MITM attack from the visited network

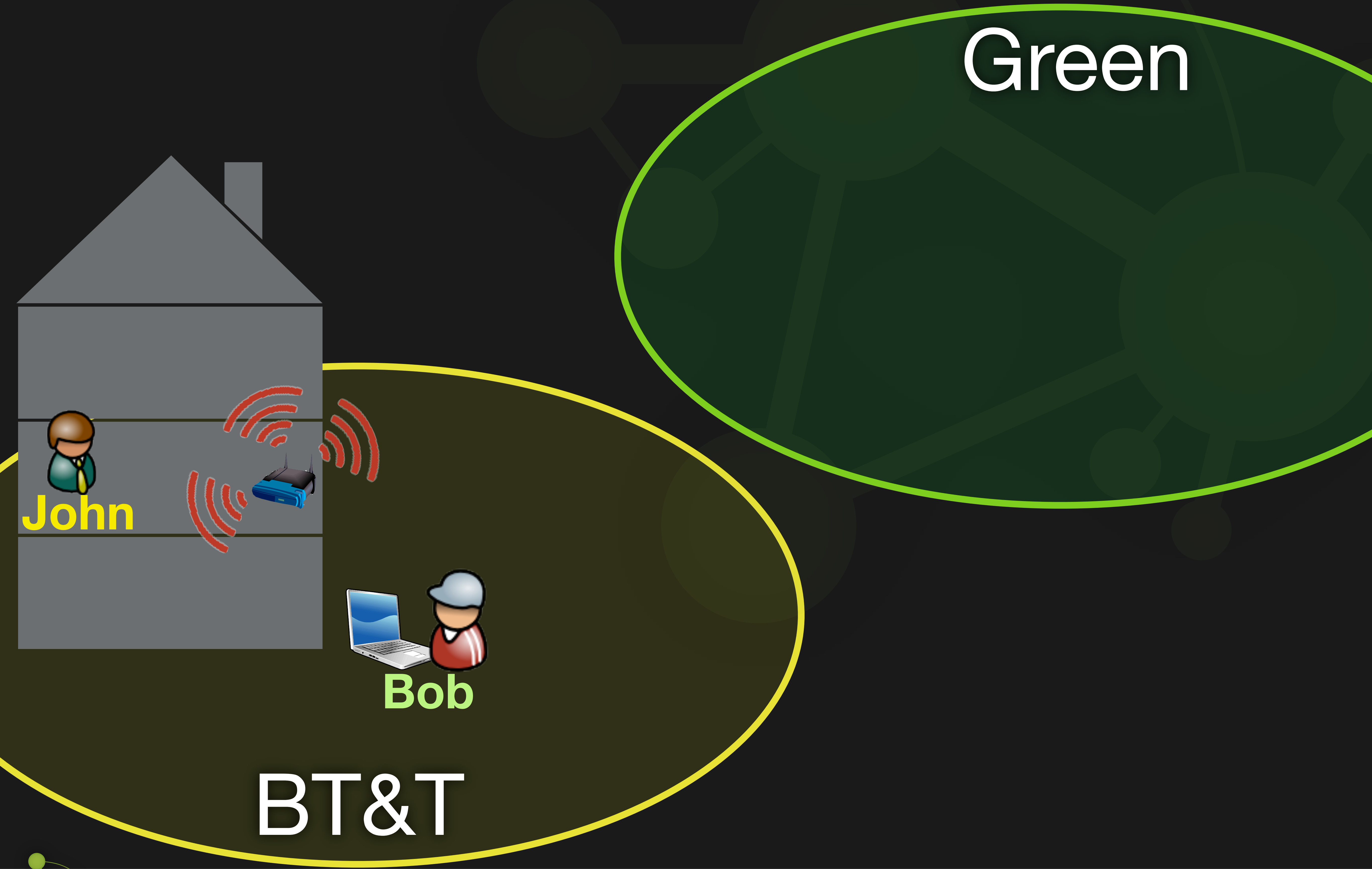
- data sent by the visitors should be encrypted

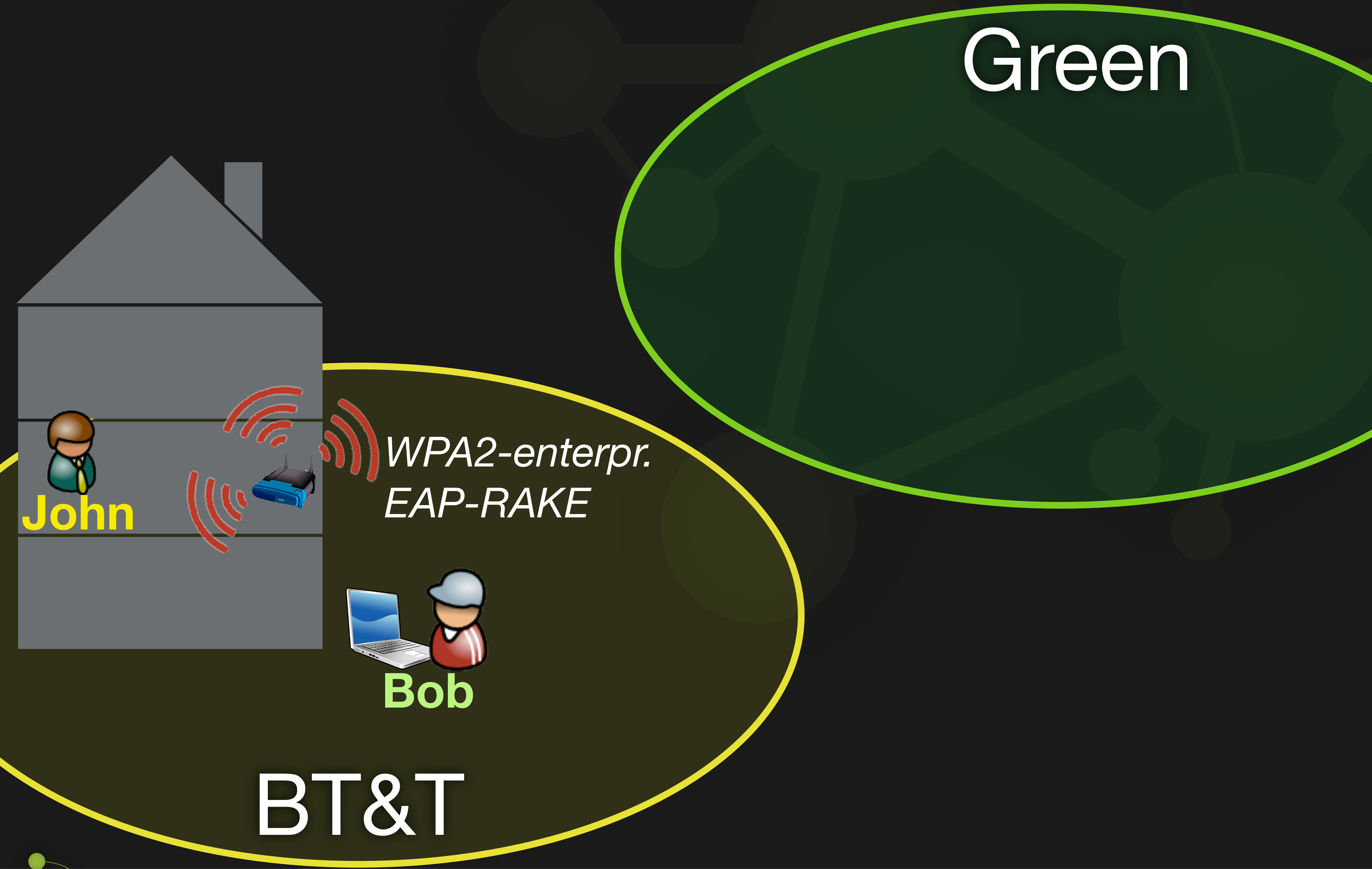
Easy to place a fake AP

- AP should be authenticated

We think we should involve ISPs


Green
Bob
John
BT&T


Green
John
Bob
BT&T



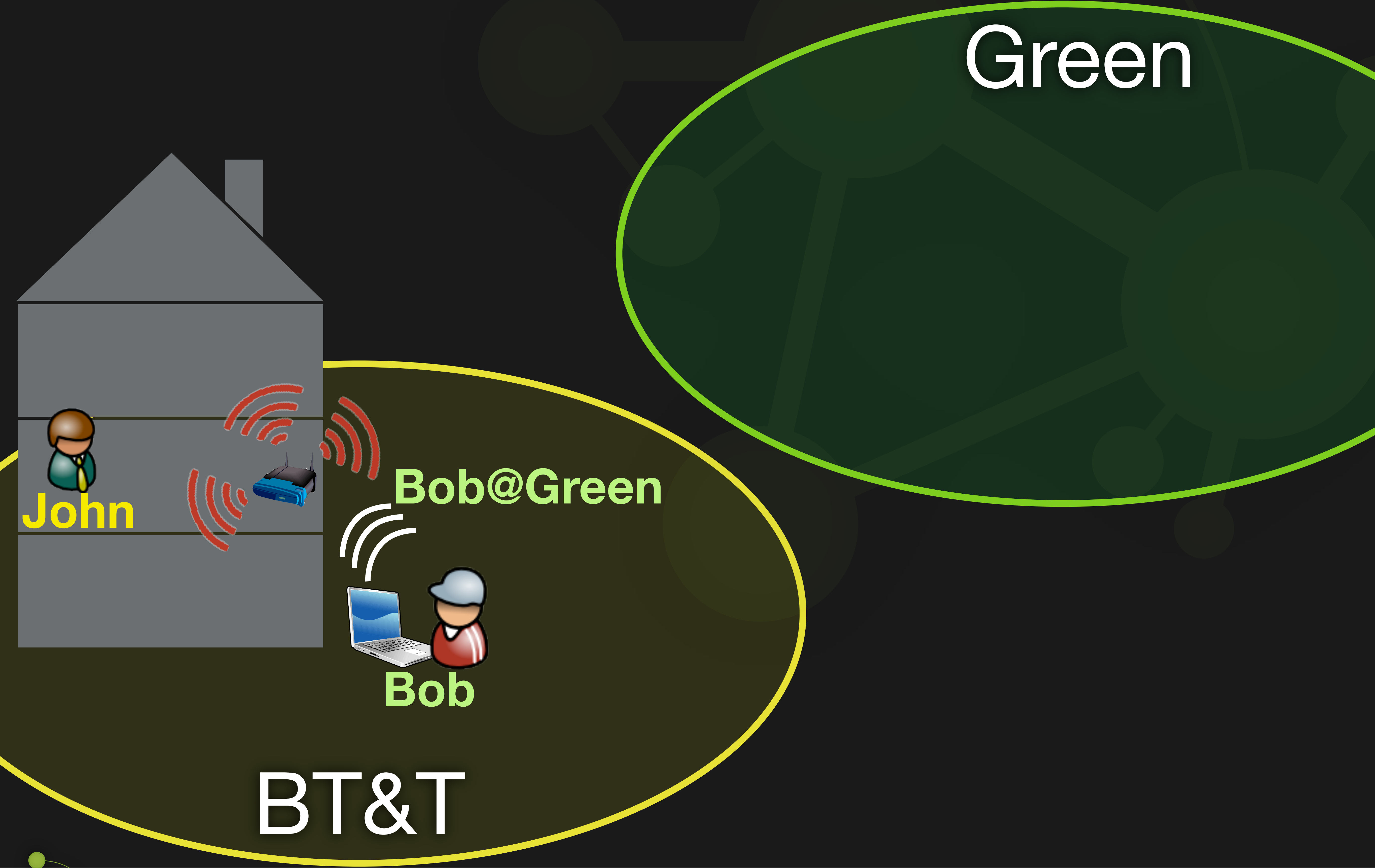
Green

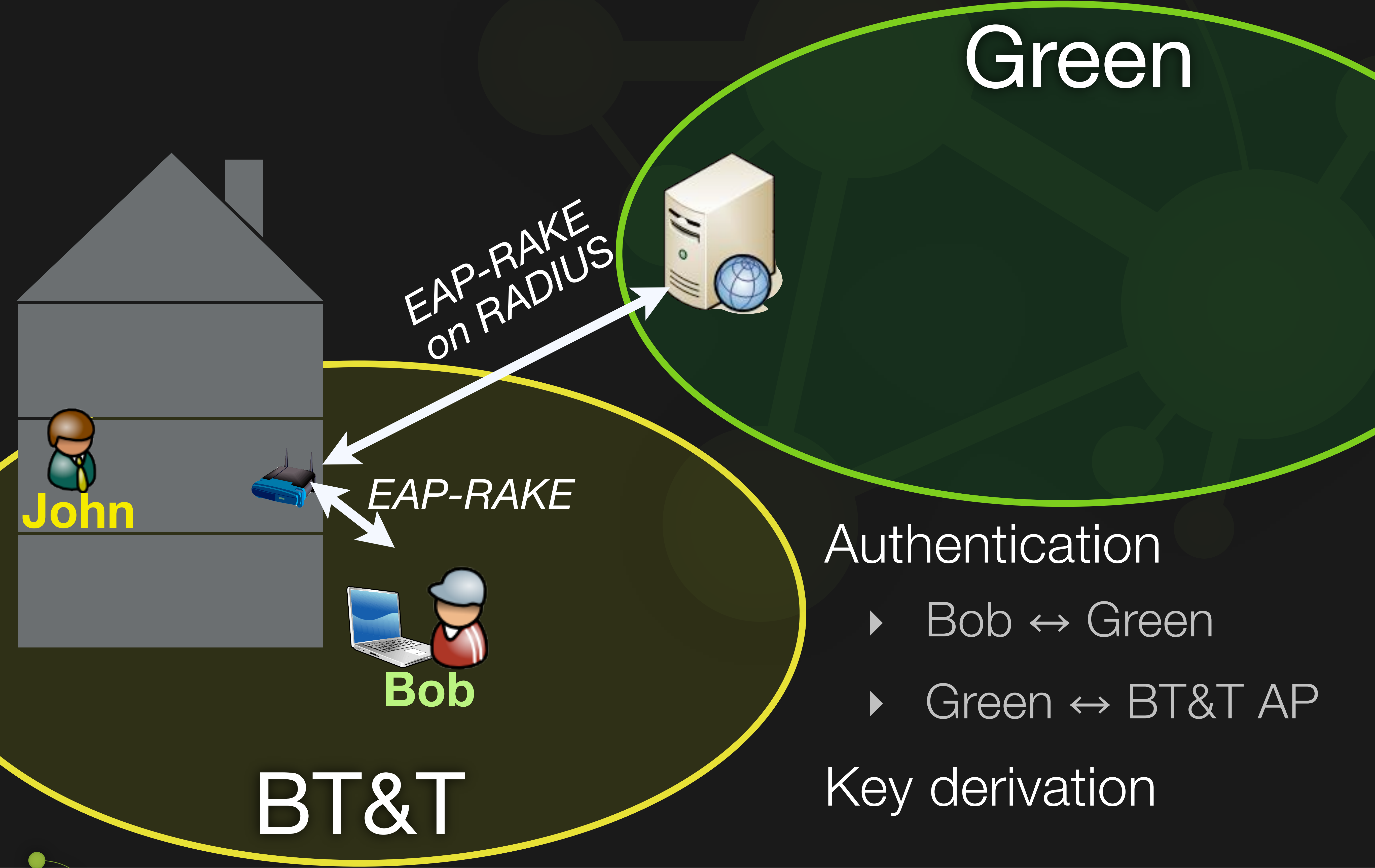
John

WPA2-enterpr.
EAP-RAKE

Bob

BT&T

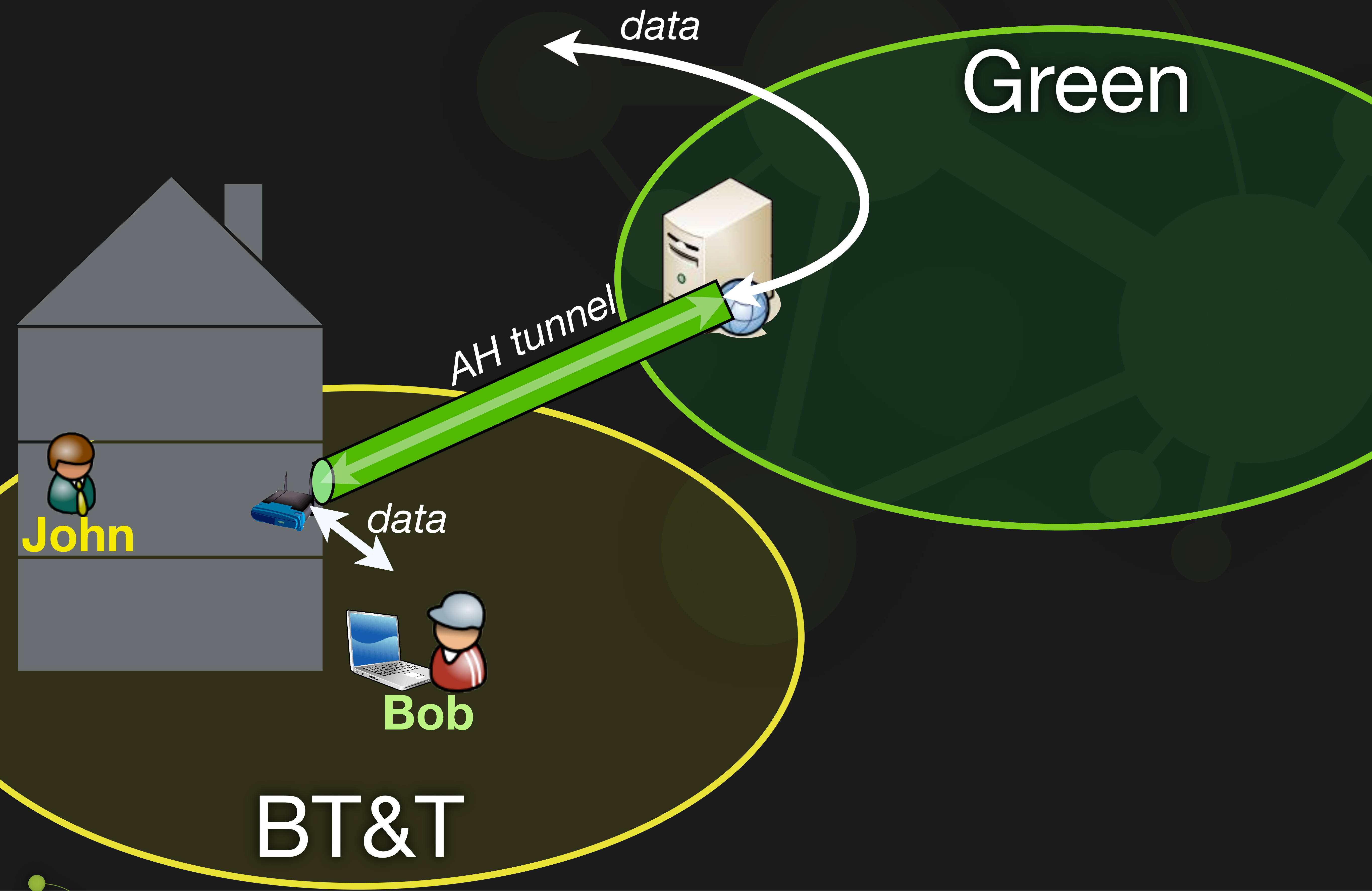

Green
John
Bob@Green
Bob
BT&T

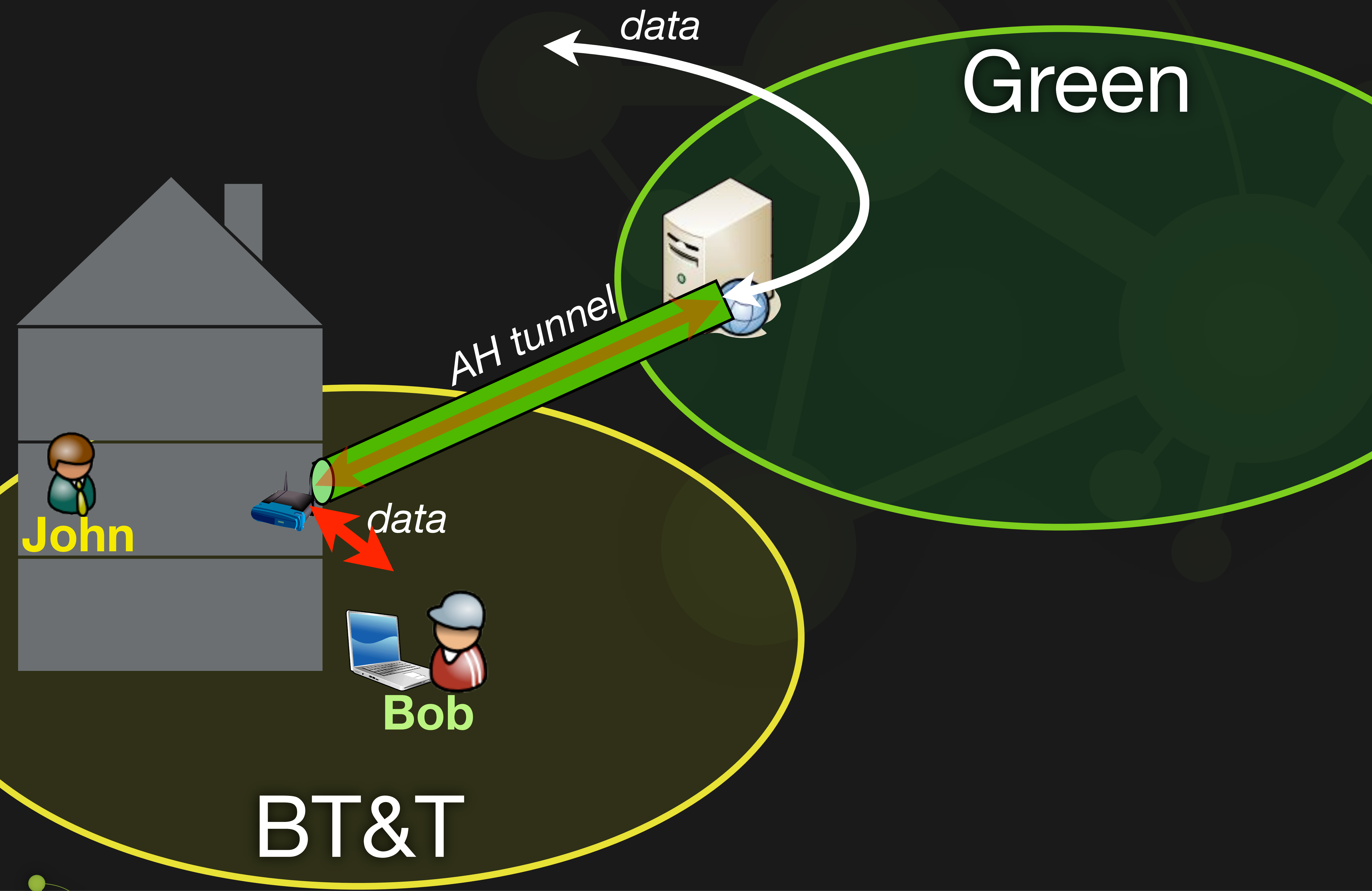


Authentication

- Bob ↔ Green
- Green ↔ BT&T AP

Key derivation

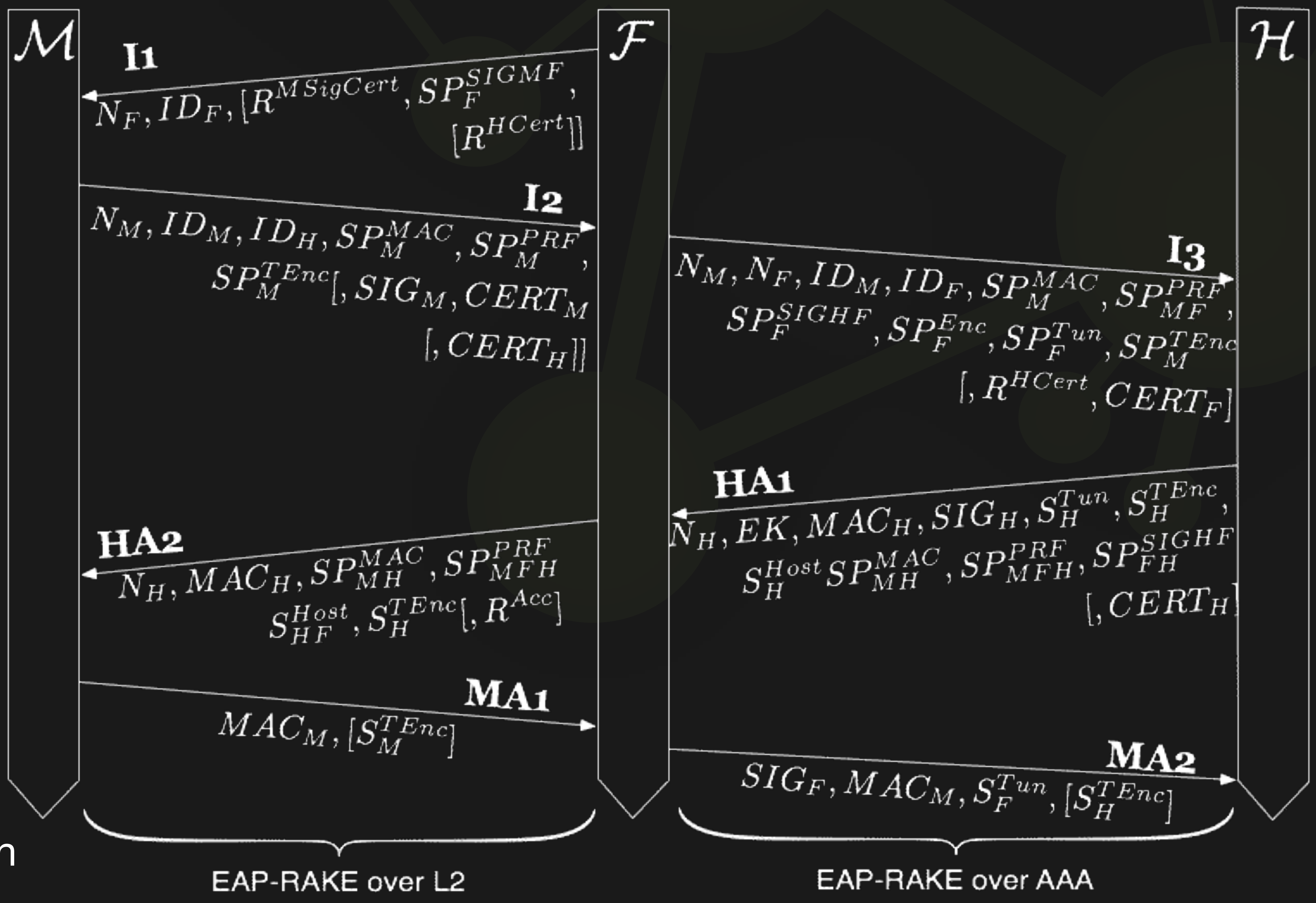

data
Green
AH tunnel
John
data
Bob
BT&T


data
Green
AH tunnel
John
data
Bob
BT&T

EAP-RAKE solves main security issues

- ✓ legal issues
- ✓ ISP issues
- ✓ attack on visited network
- ✓ resource consumption
- ✓ MITM

A look at the authentication protocol: EAP-RAKE


$\mathcal{M}$
$\mathcal{F}$
$\mathcal{H}$
I1
$N_F, ID_F, [R^{MSigCert}, SP_F^{SIGMF}, [R^{HCert}]]$
I2
$N_M, ID_M, ID_H, SP_M^{MAC}, SP_M^{PRF}, SP_M^{TEnc}[, SIG_M, CERT_M [, CERT_H]]$
I3
$N_M, N_F, ID_M, ID_F, SP_M^{MAC}, SP_{MF}^{PRF}, SP_F^{SIGHF}, SP_F^{Enc}, SP_F^{Tun}, SP_M^{TEnc} [, R^{HCert}, CERT_F]$
HA1
$N_H, EK, MAC_H, SIG_H, S_H^{Tun}, S_H^{TEnc}, S_H^{Host} SP_{MH}^{MAC}, SP_{MFH}^{PRF}, SP_{FH}^{SIGHF} [, CERT_H]$
HA2
$N_H, MAC_H, SP_{MH}^{MAC}, SP_{MFH}^{PRF} S_{HF}^{Host}, S_H^{TEnc}[, R^{Acc}]$
MA1
$MAC_M, [S_M^{TEnc}]$
MA2
$SIG_F, MAC_M, S_F^{Tun}, [S_H^{TEnc}]$
EAP-RAKE over L2
EAP-RAKE over AAA

Crypto part has been proved in [Man09]

Tunnels between entities using standards

Tunneling between the AP and the home network

- Using L2TP (or AH tunnel)
- The tunnel is authenticated (e.g., with IPsec/AH)

Encryption

- Kept optional (should be turned off in some cases)

Structure of the Presentation

Review of existing solutions

Our proposal

Implementation & Deployment

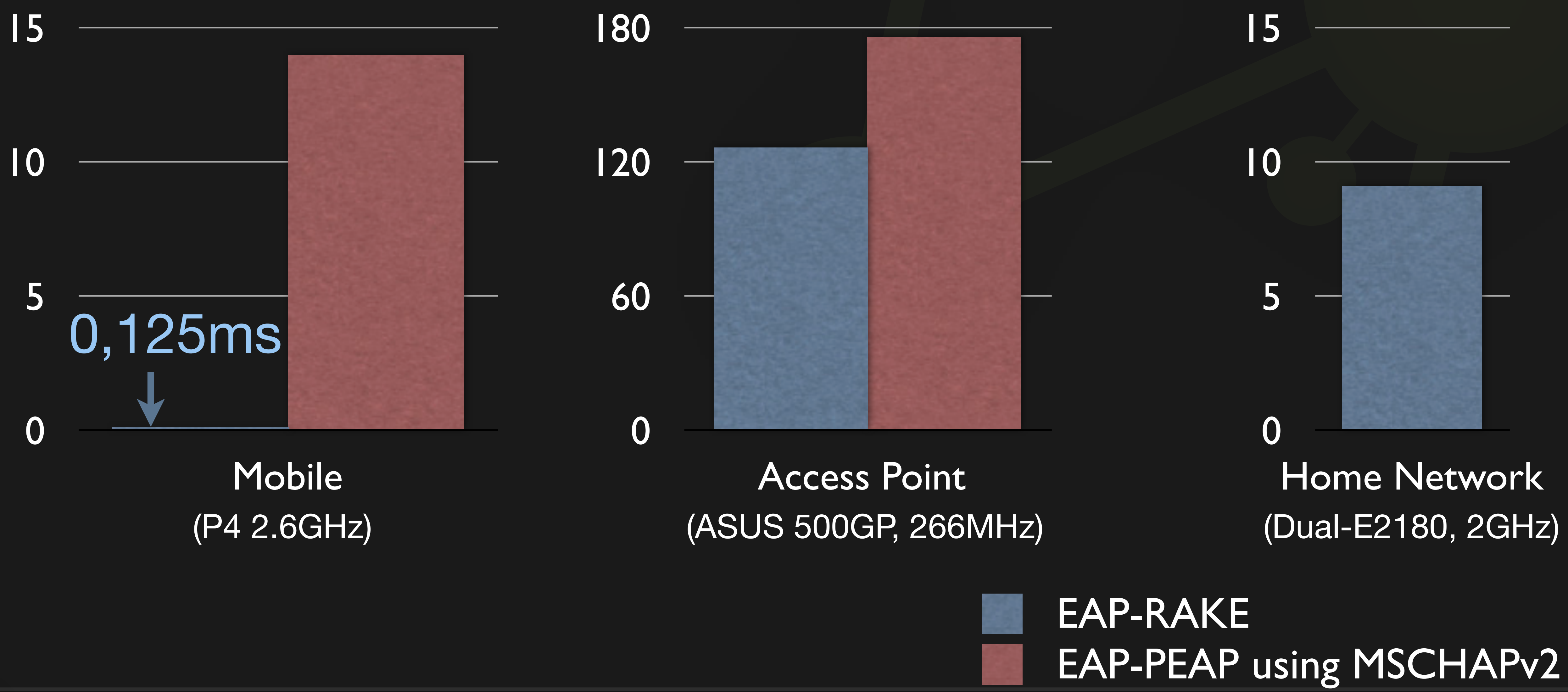
A prototype of the authentication protocol has been implemented

As a new EAP method, in *hostap* implementation

- *hostap* is an open-source project
- (our implementation not yet)
- client (mobile) works on Linux, MacOS, Win (?)
- server (AP) works on Linux (and so on OpenWRT)

Results of first measurements : EAP-RAKE is lighter than PEAP

Processing time for authentication (in msec)



Assembly of tunnels mechanisms has also been made

Using L2TP requires a PPP concentrator (no OpenSource solution existing)

- Using pure IPsec solutions is possible (tunnel mode)

Tunnel encryption/authentication uses AH mechanism (openswan)

It works ! And seems to fit to networks' reality

It was not fair to compare our solution >< FON

Security is stronger in our solution

But (computing) cost is higher in our case

But involving ISPs is a HUGE issue

- even if in our case, ISPs do not increase their security risks (incentive)

What are we willing to do for stronger security ?

Would a more secure mechanism push more people the share their WiFi ?

Lots of people stops sharing their WiFi access after reading / experiencing issues with malicious (or stupid) visitors

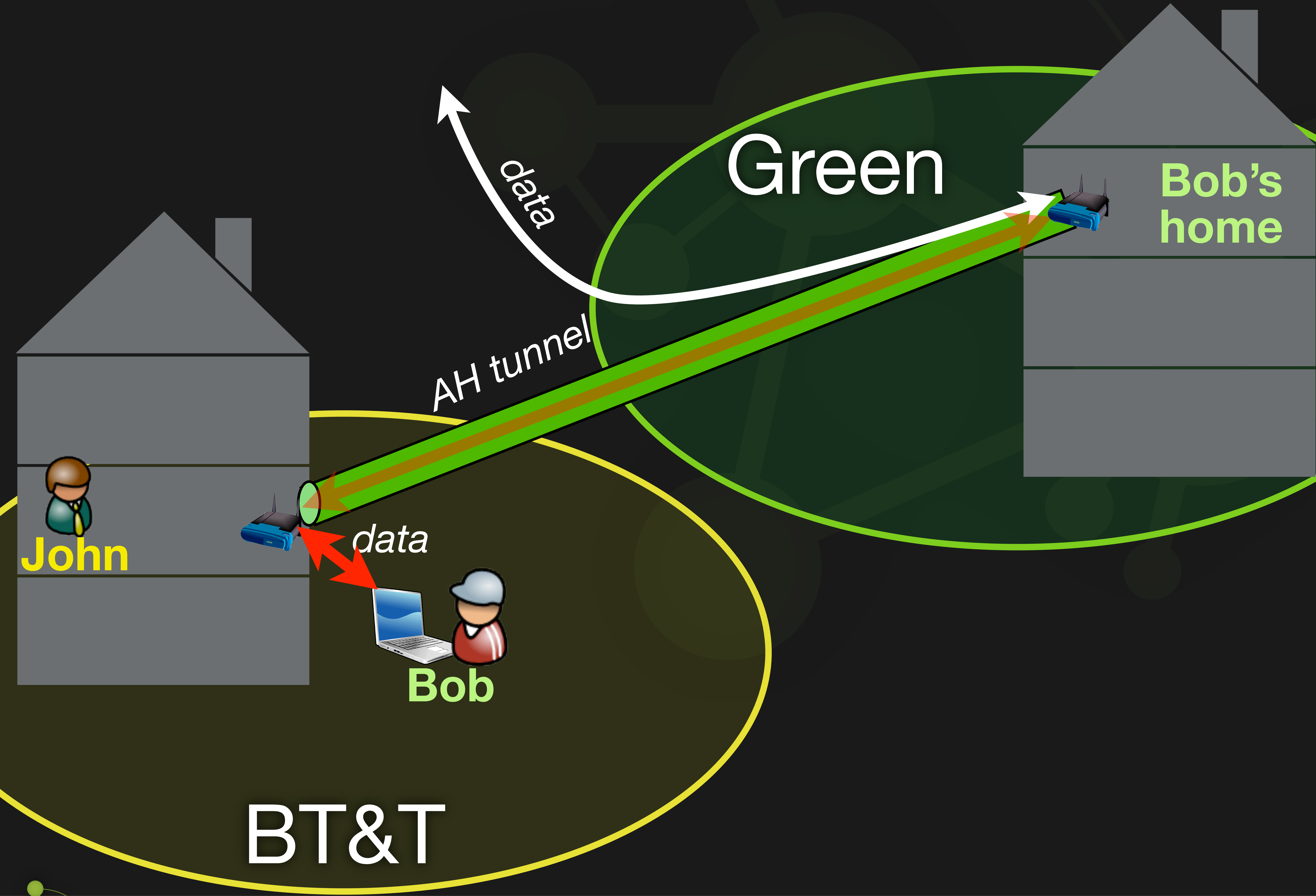
If there was no more risk in sharing, could we observe more sharing ?

QUESTIONS ?

ip networking lab
ucl, louvain-la-neuve, belgium

http://inl.info.ucl.ac.be

Some backup slides


Green
Bob's home
data
AH tunnel
John
data
Bob
BT&T

Our solution requires widespread adoption

Could rely on communities (as FON, Whisher, ...)

ISPs could decide to add EAP-RAKE to set-top boxes (home routers) they control

- but they must be >1 ISP participating

Scalability issues could appear

Cost of the authentication protocol evaluated

Cost of the authenticated tunnel (and encryption) has not been evaluated (yet)

- For home network, should load balance (or distribute servers in data centers around the world)
- For AP,
  - either limiting number of simultaneous clients,
  - or only tunneling (without AH) to a proxy-server that makes the job