



## Secure Wakeup for Car to Home Applications

-

Magic Packets for Wireless

V2VCOM, San Diego, July 21<sup>st</sup>, 2005

---

M. Gerlach, C. Tittel, J. Hünerberg, B. Bochow  
*Fraunhofer FOKUS, Berlin*

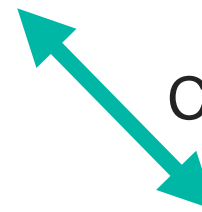
C. Maihöfer  
*DaimlerChrysler AG, Sindelfingen*

---



## Car to Home Applications

- Wireless interface for the Car under development
  - (many) Projects in the U.S. and E.U.
- Market Introduction needs “Deployment Applications”
  - Instant benefit for the user
  - Independent of Deployment progress
- Car to Home Applications
  - Synchronize (Media) Data between Car and Home
  - Vehicle becomes “storage on wheels” and entertainment platform



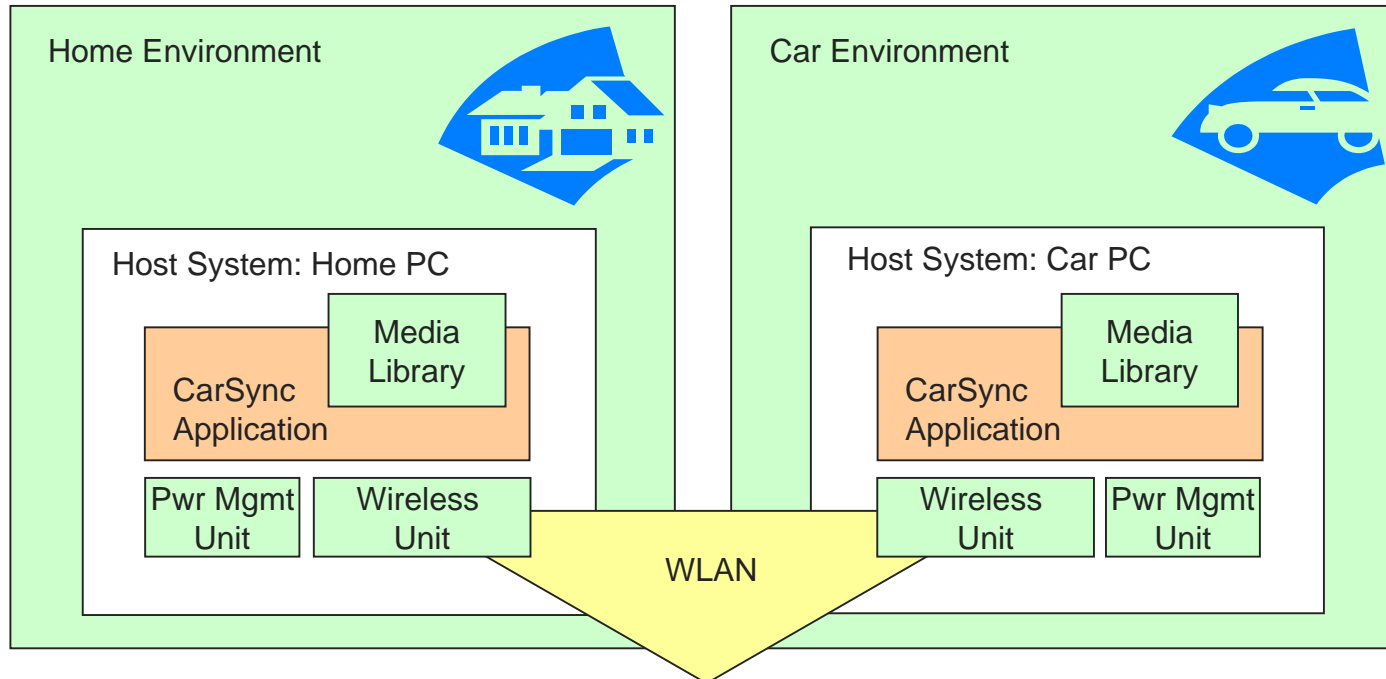
Wireless  
Communications





# The CarSync System

- Client-Server Application
- Media Library automatically updated on Client (CarPC) if in reach.
- Uses Standard Protocols for Data Transfer
- Specified completely in UML





## Wakeup and Duty Cycles

- Why such a fuzz about Wakeup?
  - Need to Save Energy, cannot allow always-on CarPC
  - Would drain Car Battery, render Car unusable!
  - Even the Wireless Interface cannot stay on the whole time.
- Wakeup Mechanism must run on Wireless Hardware only.
- Sleep time of Wireless Interface below 5 seconds to stay in energy budget (calculation in paper).

Modern Laptop:  
20 W  
(~1.6 A @ 12 V)

Car Battery capacity is  
80 Ah @ 12 V

CarPC can run  
 $80 \text{ Ah} : 1.6 \text{ A} = 50\text{h}$

- If not secure, Attacker can drain vehicle battery easily!

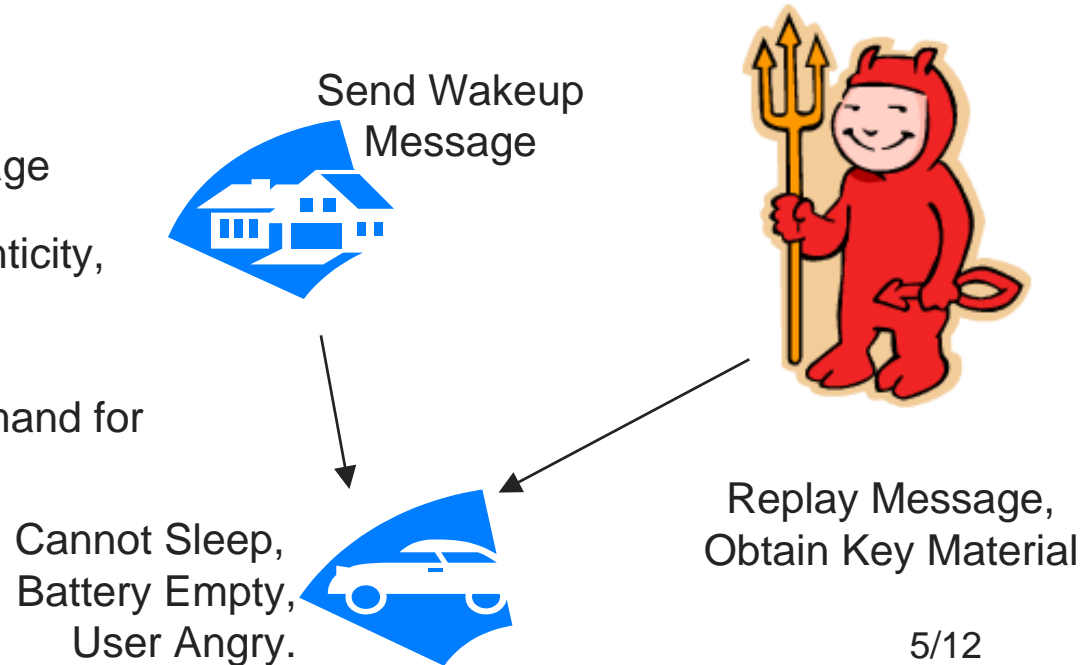


# Security Analysis

- Assumptions:
  - Secure key management using some physical channel (e.g. USB stick)
  - Consider only attacks on sleeping CarPC.

- Desired Protocol
  1. HomePC sends WakeupMessage
  2. WLAN Card HW checks authenticity, freshness (, and integrity)
  3. WLAN Card toggles start command for CarPC

- Attacks
  - Send authenticated Messages
    - obtain key material
  - Replay messages
    - break freshness algorithm

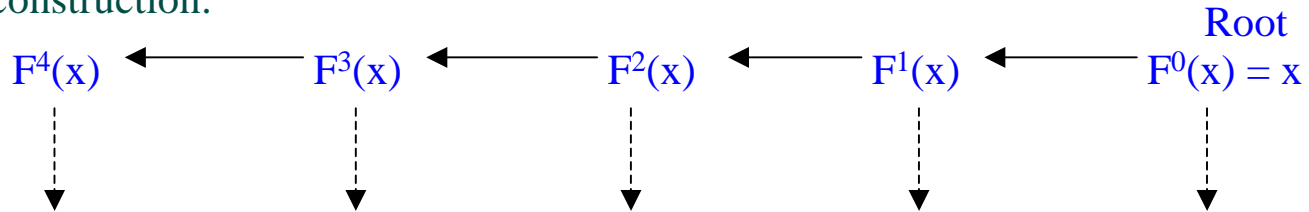




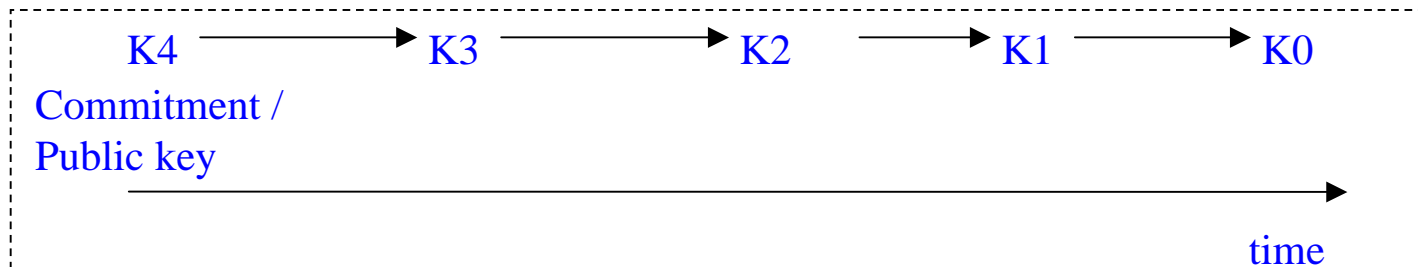
# Hash Chain based Wakeup (1)

- Hash Chains can be used to authenticate a sequence of messages.
- One way-functions (e.g. MD5, SHA) can be implemented and executed on constrained HW (successfully deployed in Sensor Networks)
- HomePC calculates whole chain which is kept secret beforehand.
- Commitment has to be authenticated (USB Stick) and given to CarPC
- Approaches:
  - One-Time Password
  - Time Synchronization Approach

Chain element construction:



Chain element use:





## Hash Chain based Wakeup (2)

- **One-Time Password:**
  - One Hash value for each Wakeup Message
  - Upon successful authentication, current value is marked as used.
- Advantages
  - Simple, straightforward
- Disadvantages
  - Have to ensure that car is there
  - Otherwise: Replay Attack Possible.
- **Time Synchronisation:**
  - Introduce time-slots.
  - One Hash value for each time-slot.
  - CarPC and HomePC synchronized
- Advantages:
  - Need not ensure car is there.
- Disadvantages:
  - Automatic use up of hash chain
  - Nodes need to be synchronized.
  - May take longer to verify authenticity.



**Better Solution!**



# WPA (Wifi Protected Access) based Wakeup

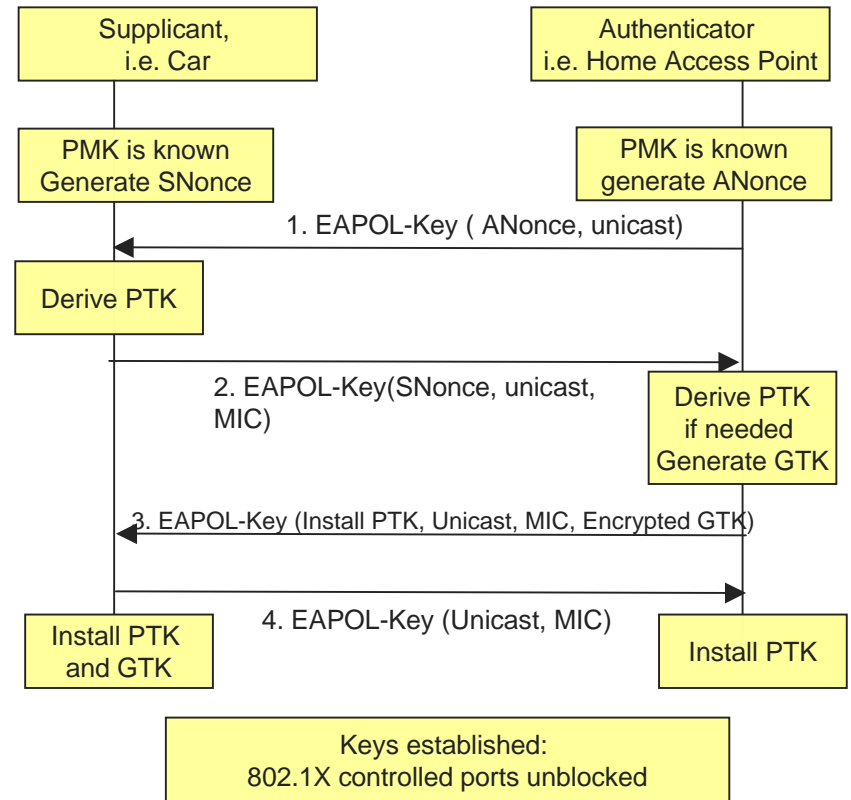
- Assume that WPA and WPA 2 algorithms are executed in Network Interface Cards.
- Solution could be easy !
  - Install WPA keys and you are done!
- Does this really work that simple ???
- Let's have a look at WPA ...





# Wifi Protected Access

- Allows Pre-shared Keys
- Requires 4-Way Handshake to establish shared secret keys (“Temporal Keys”)
  - Authentication
- Primitives support freshness, integrity (and confidentiality)
- Security Associations expire after a certain period, requiring another four-way handshake
  - May render Wakeup mechanism useless
  - Variables may be set accordingly, needs further research.



## WPA's Four-Way Handshake to establish keys



## Comparison (WPA / Hash)

- Need to alter CarPC side firmware of NIC in both approaches.
- Hash Chains
  - Better suited for older Networks (+)
  - More effort to implement (-)
- WPA Based Approach
  - Functionality inherent to recent and future NICs (+)
  - Almost no effort to implement. (+)
  - Incompatible to old hardware (-)
  - Security Association Lifetime could be a problem (-)





## Conclusions

- **Secure Wakeup is necessary**
- Currently deployed technology (old Network Cards and Access Points) do not provide sufficient means.
- Future technology (WPA) provides the basis to implement secure Wakeup easily.
- For now, **hash chain based wakeup** is recommended.





# Thank You!

Do you have  
 any Questions?

