EURECOM
Sophia Antipolis

Attaques sur Systèmes de Clefs de Voiture Sans-Fils

Aurélien Francillon

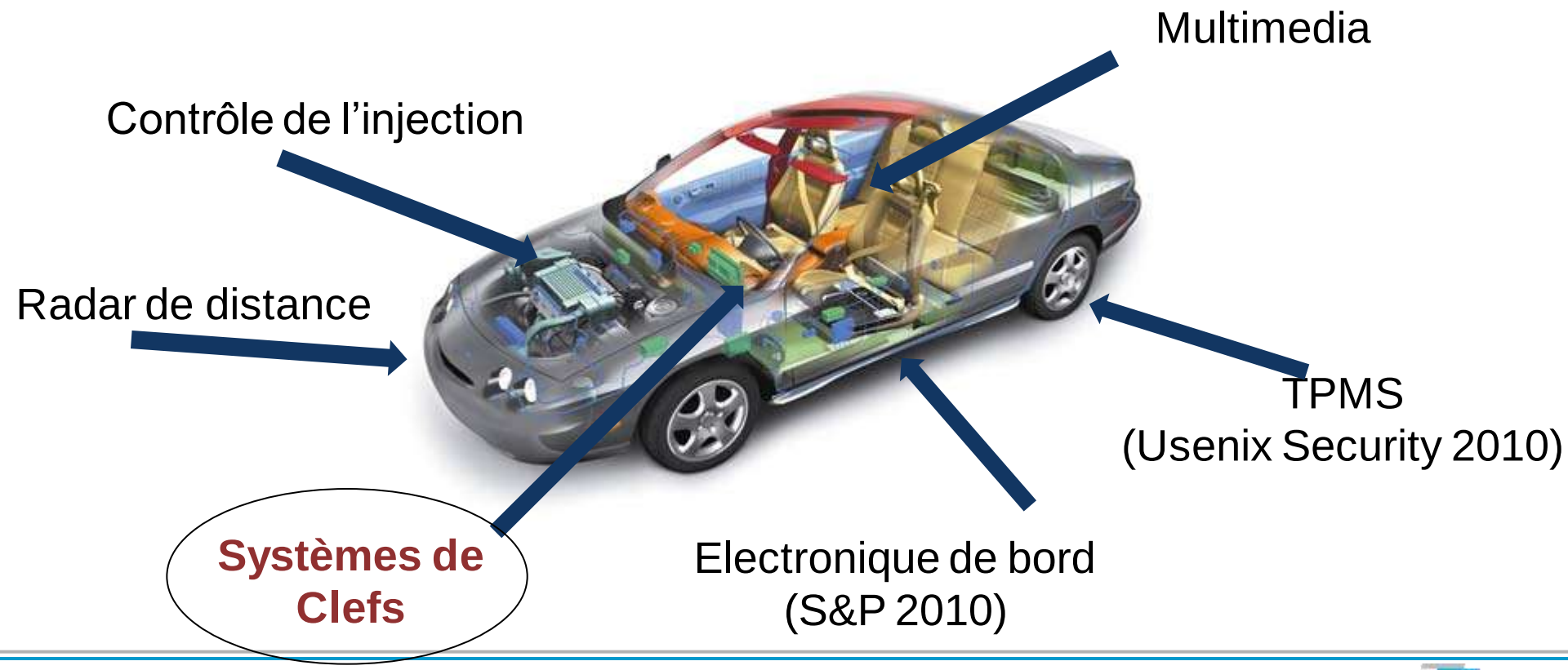
(joint work with Boris Danev, Srdjan Čapkun)

Agenda

1. Les systèmes de clefs de voitures
2. Attaques précédentes en pratique
3. Les clefs dites « Passives » PKES
4. Attaques par relai sur PKES
5. Analyse de 10 modèles de voitures
6. Conclusion

Evolution des Voitures

- **De plus en plus d'électronique**
- **Convenance, sécurité and fiabilité**



4 Catégories de Systèmes de Clefs

- **Clef métallique**
- **Télécommande d'ouverture**
- **Puce d'anti-démarrage**
- **Systèmes d'entrée et démarrage passifs**
  - Passive Keyless Entry and Start: PKES
  - Smart Key
  - Nombreux noms commerciaux

Télécommande d'Ouverture

- **Clefs "Actives":**
  - Presser un bouton pour ouvrir la voiture
  - Clef métallique pour démarrer la voiture
  - Proximité nécessaire (<100m)

- **"Clef cryptographique" partagée entre la clef et la voiture**
- **Attaques précédentes: cryptographie faible**
  - e.g.
    - Keeloq (Eurocrypt 2008, Crypto 2008, Africacrypt 2009)
      - ☞(Microchip systems)

Clefs avec Puces Anti-Démarrage

- **“Immobilizer chips”**
  - RFID Passif
  - Autorise le démarrage du moteur
  - Proximité: centimètres
- **Présents dans la plupart des clefs de véhicules actuels**
  - Avec clefs métalliques
  - Avec télécommande
  - Introduits dans les 90’s suite a pressions des assureurs…
- **Clef cryptographique partagée entre la voiture et la clef**
- **Attaques précédentes: cryptographie faible**
  - e.g. Texas Instruments DST Usenix Security 2005
    - ☞ “Security Analysis of a Cryptographically-Enabled RFID Device”

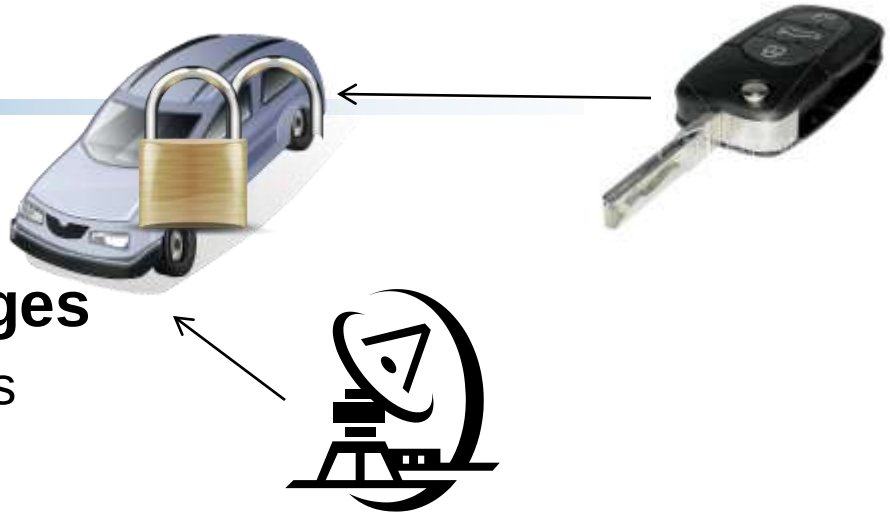
Passive Keyless Entry and Start

- **PKES / Smart Key …**
  - La proximité (<2m) suffit a déverrouiller la voiture
  - Etre dans la voiture pour démarrer le moteur
  - Sans action de l'utilisateur sur la clef
  - A la fois un système RFID Passive et Actif
- **Autorise d'ouvrir et de démarrer la voiture**

Agenda

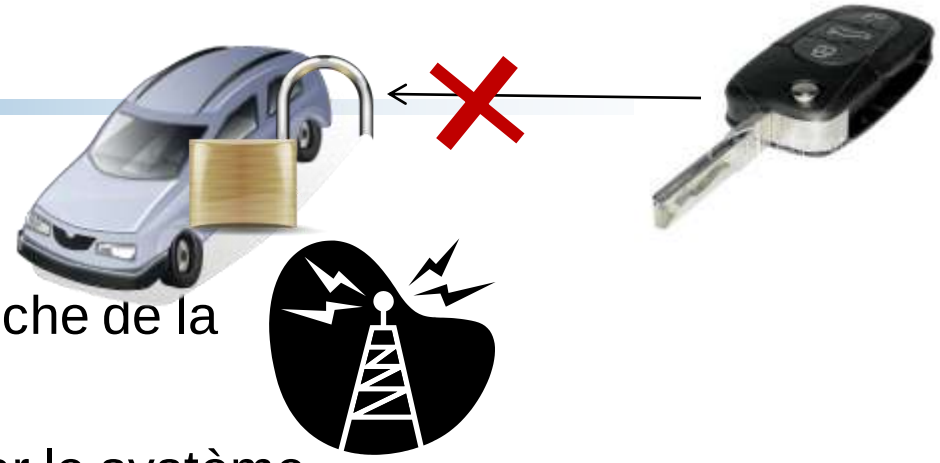
1. Les systèmes de clefs de voitures
2. Attaques précédentes en pratique
3. Les Clefs dites « Passives » PKES
4. Attaques par relai sur PKES
5. Analyse de 10 modèles de voitures
6. Conclusion

Attaques des Protocoles



- **Rejeu ou création de messages**
  - Sur les très systèmes mal conçus
- **Nécessite:**
  - Ecoute/analyse de messages puis rejeu
    - Seulement quelques messages
    - Pas de vérification de nouveauté (Freshness)
  - Peuvent être réalisés sans la présence de la clef
- **Création de fausse clef pour ouvrir/démarrer la voiture**
  - N'existe probablement plus dans le parc actuel de véhicules
  - Nous avons trouvés un model e "after market" vulnérable
    - Acheté sur l'Internet

Attaques par Brouillage



- **Nécessite:**
  - Un équipement radio dédié proche de la voiture
  - Brouille la fréquence utilisée par le système
  - L'équipement doit être présent lors de la fermeture du véhicule
- **Brouille le message de fermeture envoyé par la clef**
- **Empêche la fermeture du véhicule**
  - L'utilisateur peut remarquer que la voiture ne se ferme pas
    - Ou pas ….
  - Ne **permet pas** de démarrer la voiture … ou de l'ouvrir alors qu'elle est fermée

Attaques sur les Algorithmes de Chiffrement

- **Sur les systèmes a télécommande et/ou anti-démarrage**
- **Requièrent soit:**
  - Ecoute des messages échangés
    - Parfois milliers ou millions de messages
  - Accès physique à la clef (attaques par side-channels)
- **Permet d'obtenir la clef cryptographique**
  - Création d'un clone de la clef an utilisant la clef de chiffrement

Agenda

1. Les systèmes de clefs de voitures
2. Attaques précédentes en pratique
3. Les Clefs dites « Passives » PKES
4. Attaques par relai sur PKES
5. Analyse de 10 modèles de voitures
6. Conclusion

PKES Modes de Fonctionnement

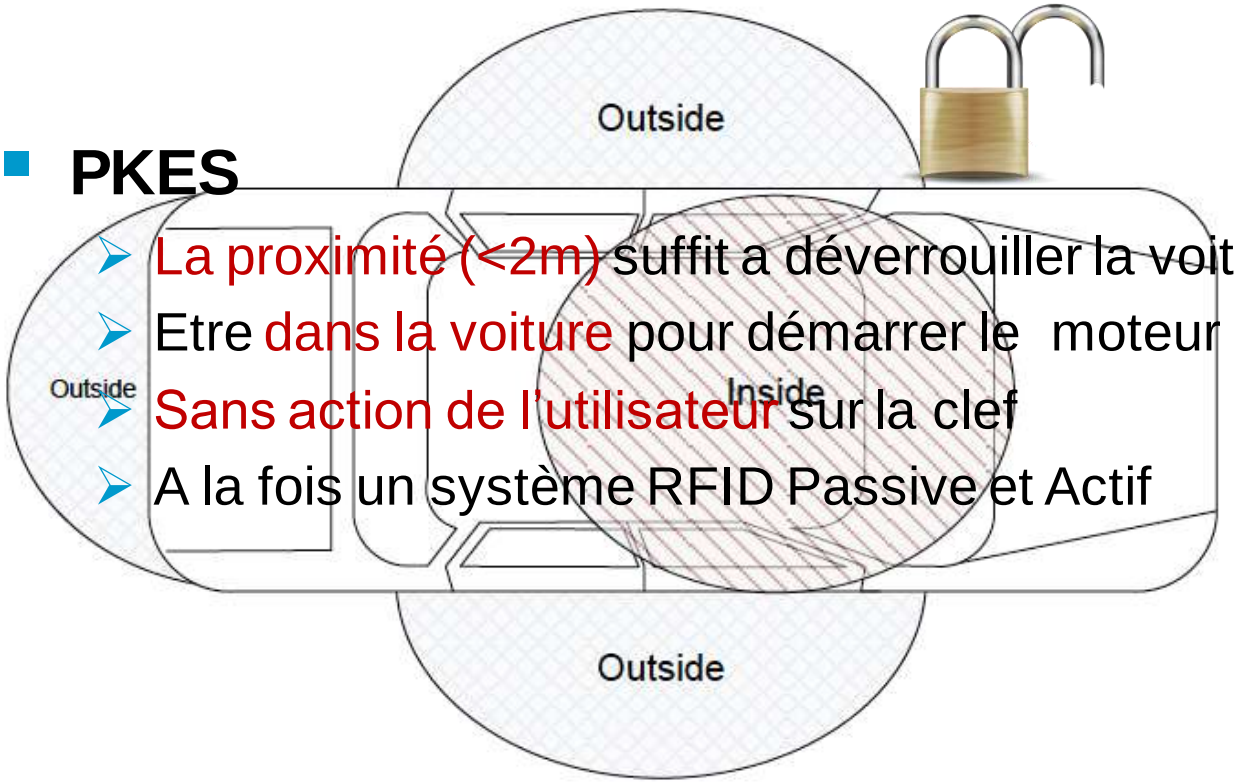
- **Mode Normal:** **Ouverture/démarrage passif**
  - Utilise 2 canaux sans-fils — Clef ⟷ Voiture

- **Ouverture distante « Active »:** **Bouton sur la clef**
  - Messages unidirectionnels — Clef → Voiture
  - Comme les systèmes « a télécommande »

- **Mode batterie épuisée** **Clef métallique de secours**
  - RFID Passif bidirectionnel — Clef ⟷ Voiture
  - Puce d'Anti-démarrage
  - Portée centimètres

Passive Keyless Entry and Start

- **PKES**
  - La proximité (<2m) suffit a déverrouiller la voiture
  - Etre dans la voiture pour démarrer le moteur
  - Sans action de l'utilisateur sur la clef
  - A la fois un système RFID Passive et Actif



Passive Keyless Entry and Start

1. Probe périodique (LF)

2. Confirmation de proximité (UHF)

3. Car ID || Challenge (LF)

4. Réponse de la Clef(UHF)

LF (120 – 135 KHz), (1-2 mètres)

UHF (315 – 433 MHz), (50-100 mètres)

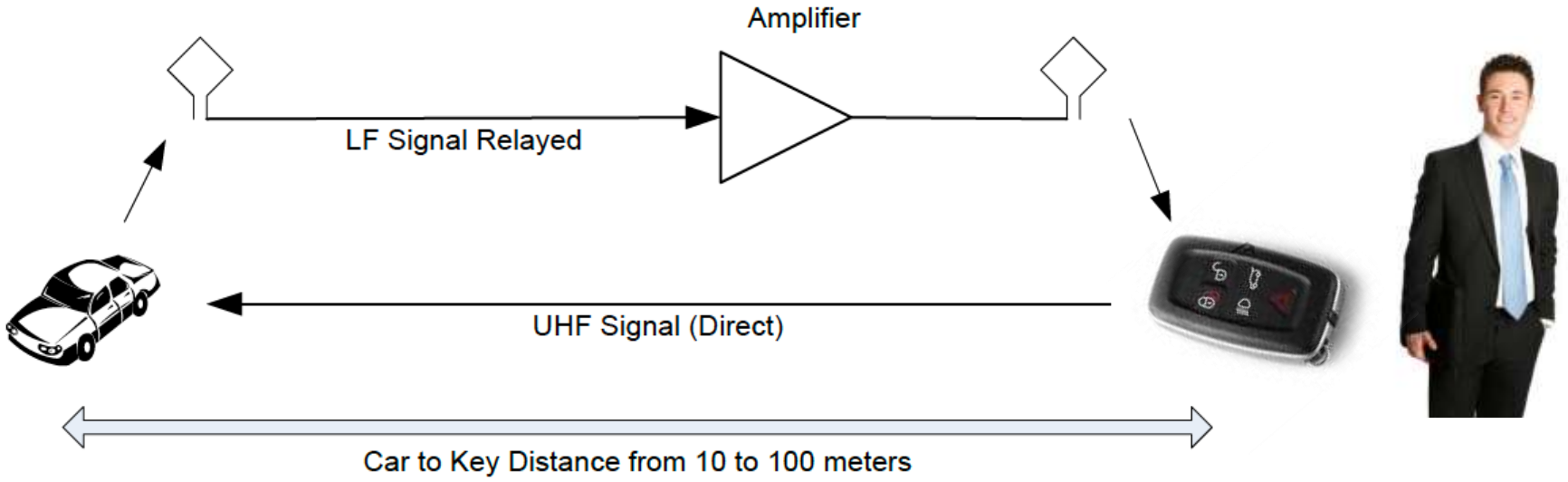
Systèmes PKES : Résumé

- **Authentification avec clef de chiffrement**
  - Protocole “challenge-réponse”
  - Rejeu de vieux signaux impossible
  - Timeout, « freshness »
- **Car to Key: signaux basse fréquence « inductifs »**
  - Puissance du signal décroit en d^{-3} => portée ~2m max
- **Proximité physique**
  - Détectée par la réception des messages
  - Induction dans l’antenne de la clef
- **Le système est vulnérable aux attaques par relai**

Agenda

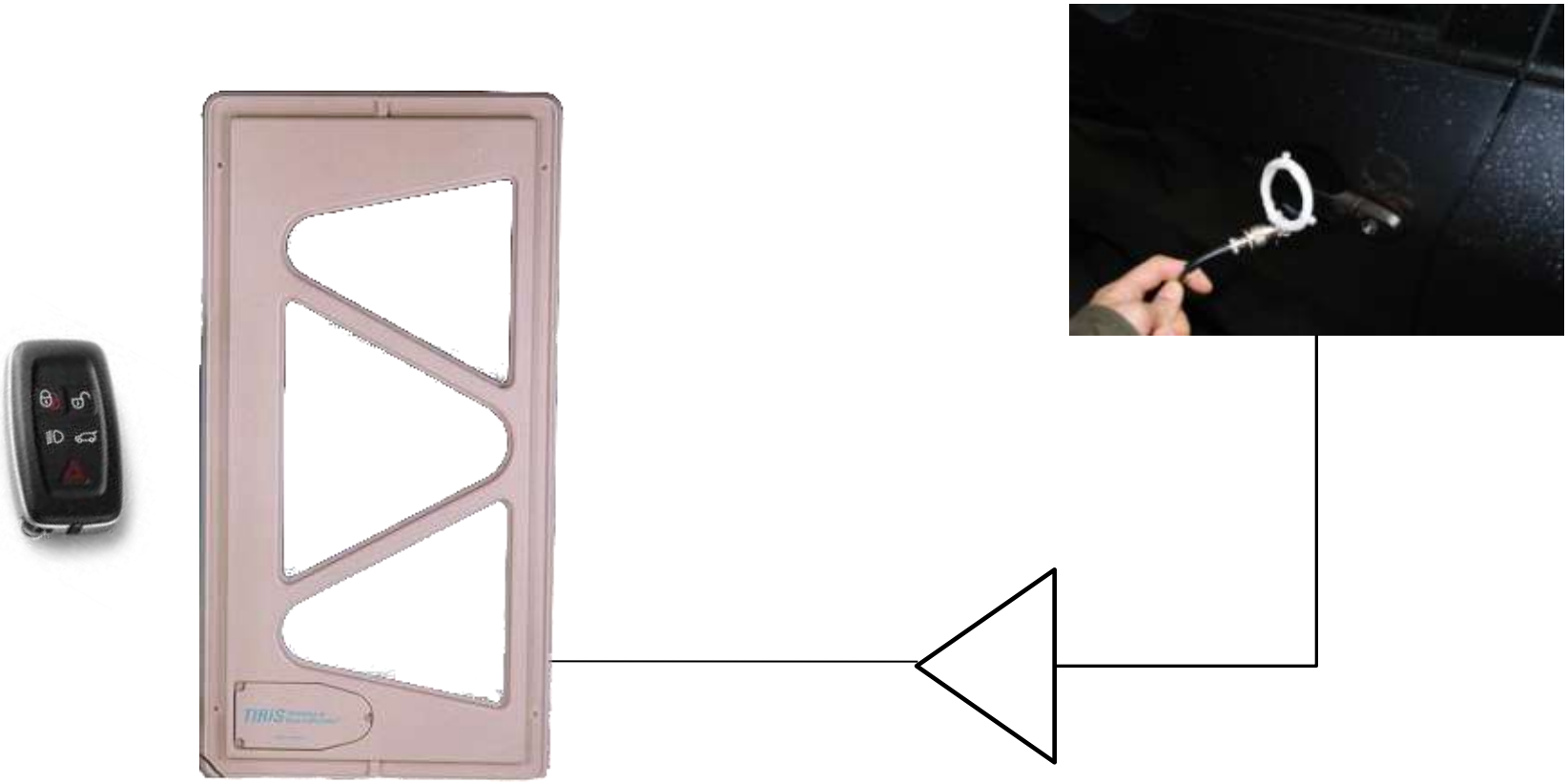
1. Les systèmes de clefs de voitures
2. Attaques précédentes en pratique
3. Les Clefs dites « Passives » PKES
4. Attaques par relai sur PKES
5. Analyse de 10 modèles de voitures
6. Conclusion

Attaque sur PKES par Relai avec un Câble

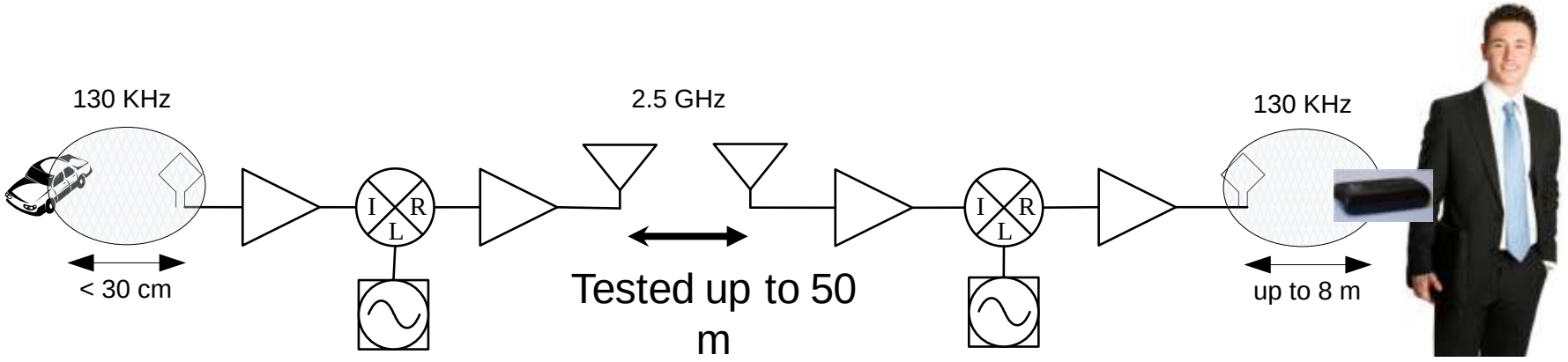


- **Attaque à très bas coût (~50 ou 100€)**
- **Indépendant du modèle / protocole / cryptographie**

Relai Physique, Expérimentations

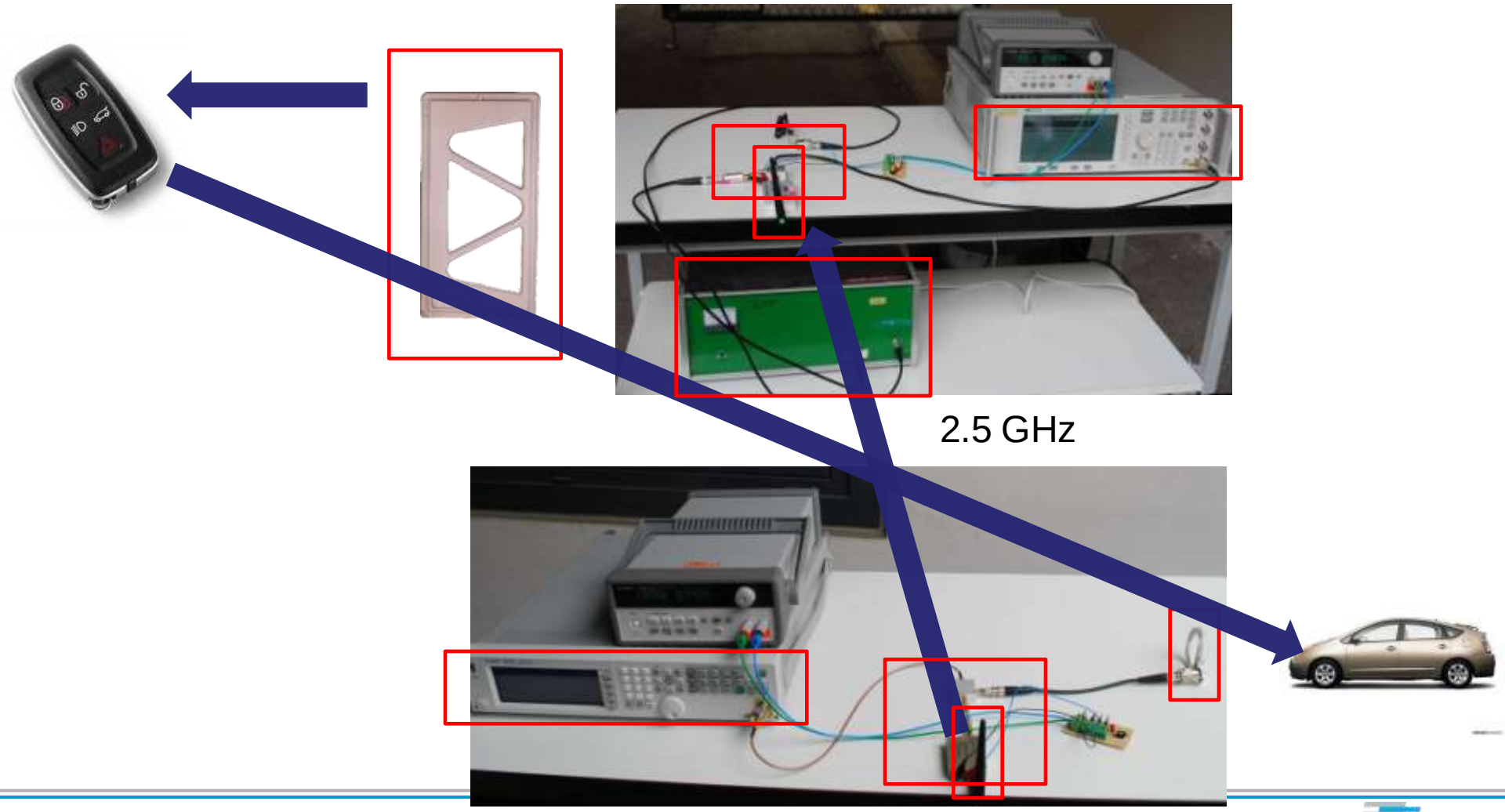


Relai Sans-Fils au Niveau Physique



- **Cout plus élevé, (~1000 EUR)**
- **Faible délai difficile a détecter**
- **Indépendant du modèle / protocole / cryptographie**

Relai Sans-Fils au Niveau Physique, Expérimentations



Agenda

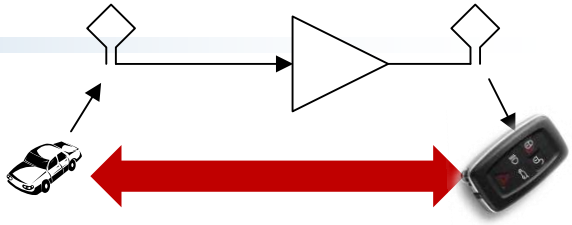
1. Les systèmes de clefs de voitures
2. Attaques précédentes en pratique
3. Les Clefs dites « Passives » PKES
4. Attaques par relai
5. Analyse de 10 modèles de voitures
6. Conclusion

Analyse de 10 Modèles de Voitures

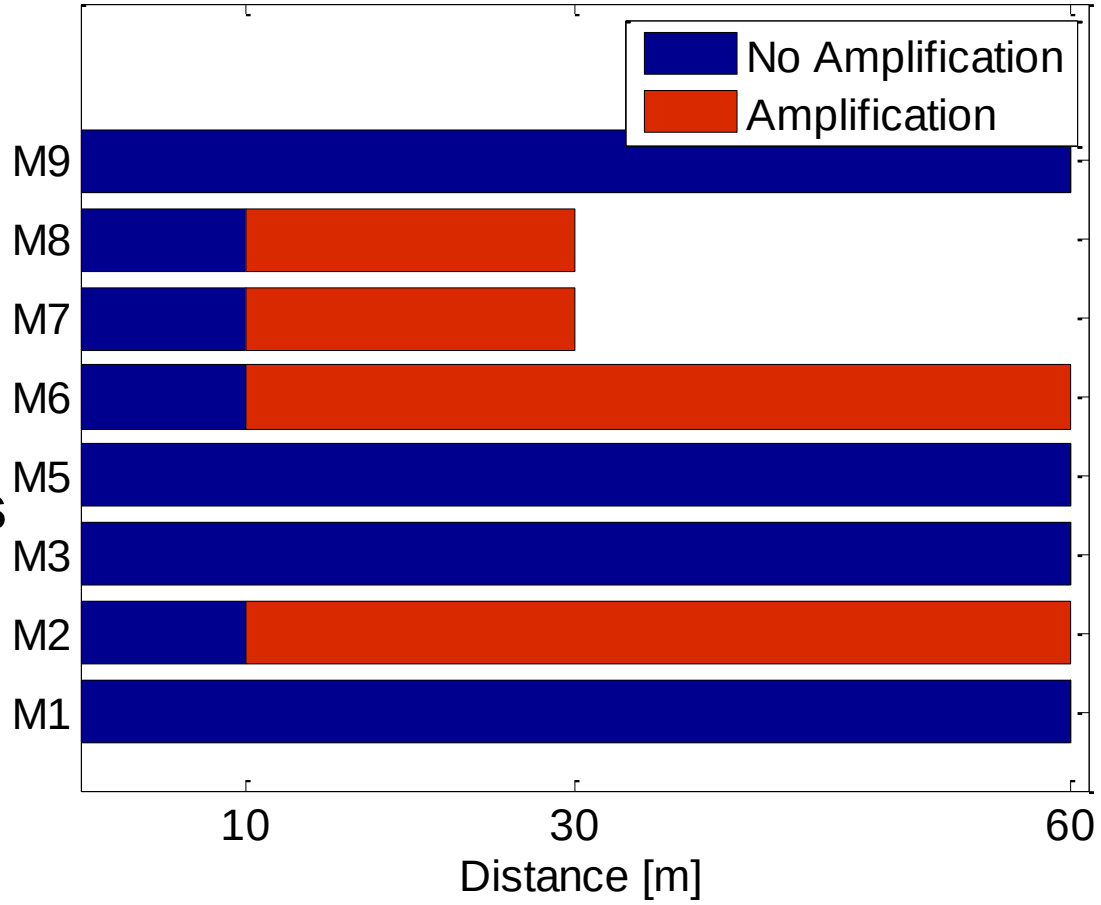
- **Modèles de voitures avec PKES**
  - 10 modèles de 8 constructeurs
  - Tous utilisent la technologie LF/UHF

- **Aucun n'utilise exactement le même protocole**
  - D'après traces d'exécution
- **Certains utilisent des messages assez longs**
  - Crypto forte ?

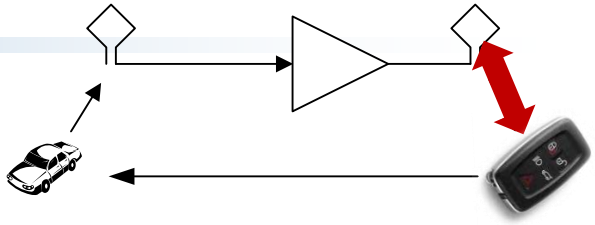
Relai sur Câble vs. Modèle

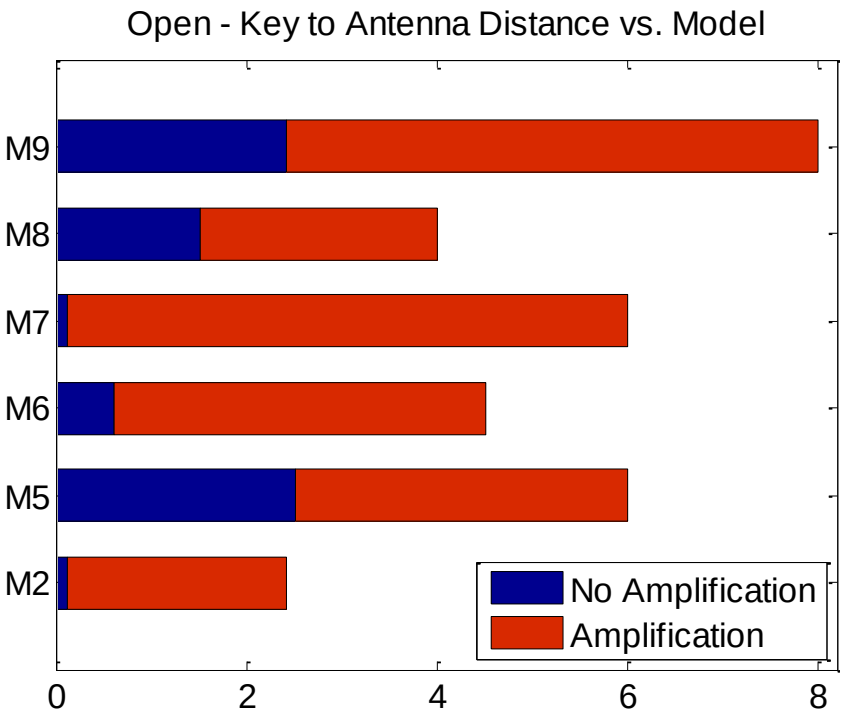


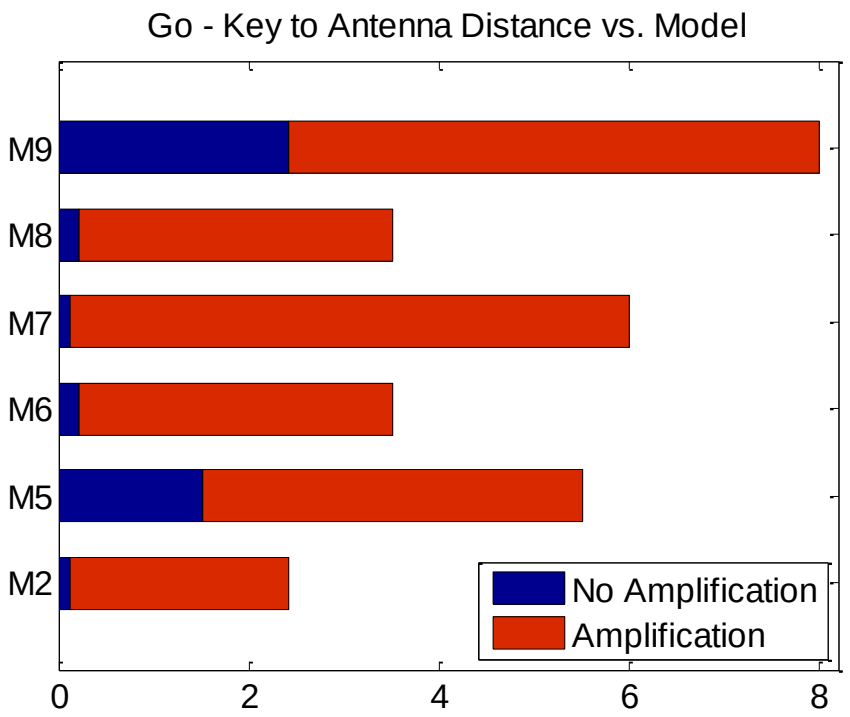
- **Câbles**
  - 10, 30 et 60m
- **Distances plus grandes**
  - Dépend des conditions expérimentales



Distance Clef - Antenne



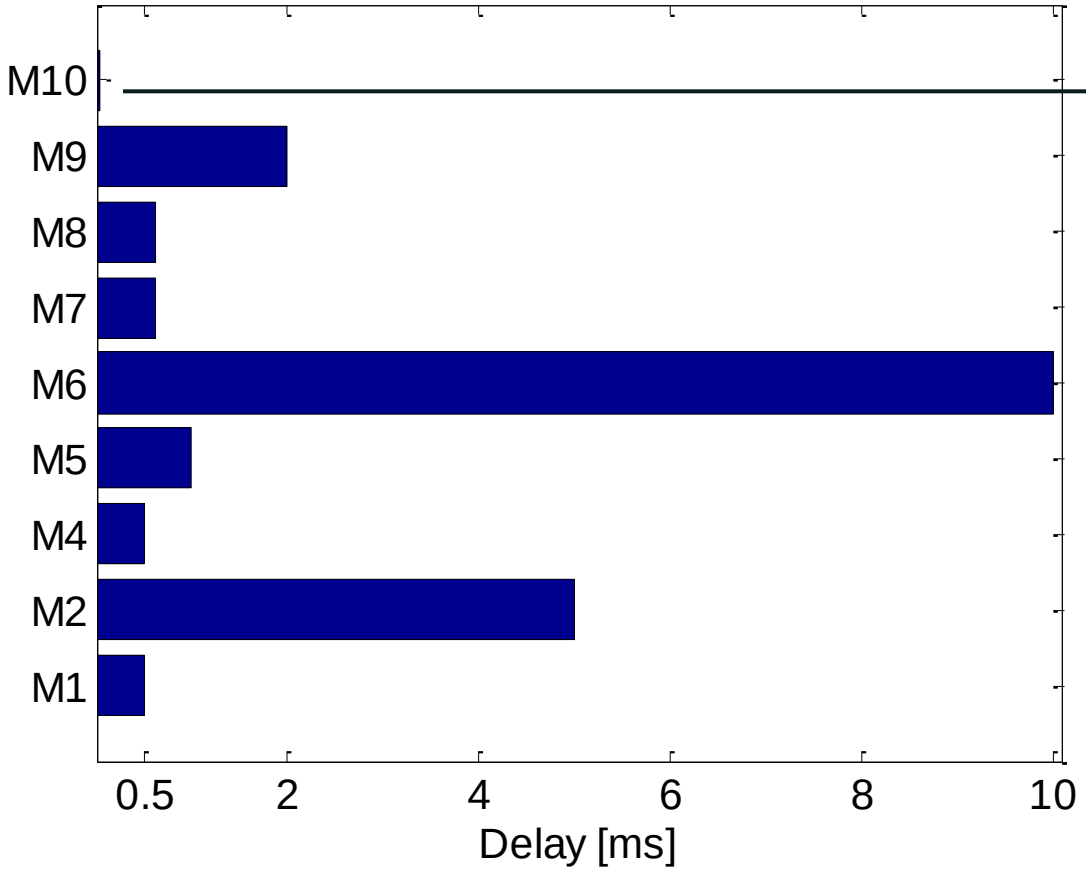




Quel Délai est Toléré par la Voiture?

- **Distance de relai maximale dépend de**
  - Delay max accepté
  - Vitesse des ondes radio (~ Vitesse de la lumière)
- **Possibilité de relai a des niveaux plus élevés?**
  - E.g. relai sur IP ?
- **Pour connaitre la réponse on doit retarder les signaux**
  - Longueurs de câble: Pas pratique
  - Oscilloscope/générateur de signal: Trop lent
  - Software Defined Radios: Toujours trop lent
  - SDR « custom »

Délai Maximum vs. Model



35 µs => 5 Km

10 ms => 1500 Km

Relais autres qu'au niveau physique difficiles

Implications de l'attaque

- **Relai dans un parking**
  - Une antenne prés de l'ascenseur
  - Voleur prés de la voiture quand le propriétaire attend devant l'ascenseur

- **Clef dans la maison, voiture garée en face**
  - E.g. clefs sur la table de la cuisine
  - Voleur met une antenne près de la fenêtre
  - Ouverture et démarrage de la voiture sans entrer dans la maison
  - Testé en pratique

Détails Supplémentaires

- **Une fois la voiture démarrée le relai n'a pas besoin d'être maintenu pour conduire la voiture**
  - Il serait dangereux de stopper le moteur si la clef n'est plus détectée
  - Certains modèles émettent un son, d'autres limitent la vitesse

- **Pas de trace d'effraction, de démarrage forcé, de serrure forcée**
- **Sérieux problèmes légaux, de forensics, de responsabilité, d'assurance…**
- **Beaucoup de travail a faire sur l'analyse des ECU**
  - Electronic Control Unit

Agenda

1. Les systèmes de clefs de voitures
2. Attaques précédentes en pratique
3. Les Clefs dites « Passives » PKES
4. Attaques par relai
5. Analyse de 10 modèles de voitures
6. Conclusion

Moyens de Protection

- **Court Terme : “Blindage” de la clef, Retirer la batterie**
  - Réduit fortement la facilité d’utilisation
  - Qui est le but du système…
  - Interrupteur pour désactiver le système
- **A long terme**
  - Un système de vérification de distance sécurisé
  - N’existe pas actuellement !
    - Ou alors très consommateur d’énergie…
- **Premières étapes: « Realization of RF Distance bounding »**
  - Usenix Security 2010

Conclusion

- **Un concept simple, attaque très efficace**
  - Analyse « forensique » difficile
  - Clef originale utilisée pour ouvrir/démarrer le véhicule
- **Tous les véhicules testés jusque la sont vulnérables**
- **Complètement indépendant**
  - Du protocole, de présence d'authentification ou chiffrements forts
- **Solutions a long terme pas encore disponibles**
- **Contacts fabricants, experts, police, medias…**

Questions ?

Contact : Aurélien Francillon aurelien.francillon@eurecom.fr
Boris Danev bdanev@inf.ethz.ch
Srdjan Capkun capkuns@inf.ethz.ch