Gone in 360 Seconds: Hijacking with Hitag2

Roel Verdult, Flavio D. Garcia, Josep Balasch
Radboud University Nijmegen, The Netherlands
KU Leuven ESAT/COSIC and IBBT, Belgium

Institute for Computing and Information Sciences
Radboud University Nijmegen, The Netherlands
✉rverdult@cs.ru.nl  🌐www.cs.ru.nl/~rverdult
Contents

• Introduction
  – Vehicle Immobilizers
  – Hitag2 and its Usage

• Hitag2
  – Functionality
  – Cipher and Protocols Weaknesses
  – Attacks and Complexity
  – Practical Experiments
  – Mitigating Measures

• Conclusion
Vehicle Immobilizers

- Passive RFID Tag (125 KHz)
- Introduced in the '90s
- Prevents hot-wiring
- Mandatory
  - Europe (EU Directive 95/56/EC)
  - Australia (AS/NZS 4601:1999)
  - Canada (CAN/ULC S338-98)
- Do not confuse it with remote controls that unlock the car doors (433 MHz)
# Makes & Models

<table>
<thead>
<tr>
<th>Make</th>
<th>Models</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acura</td>
<td>CSX, MDX, RDX, TL, TSX</td>
</tr>
<tr>
<td>Alfa Romeo</td>
<td>156, 159, 166, Brera, Giulietta, Mito, Spider</td>
</tr>
<tr>
<td>Audi</td>
<td>A8</td>
</tr>
<tr>
<td>Bentley</td>
<td>Continental</td>
</tr>
<tr>
<td>BMW</td>
<td><strong>Serie 1</strong>, 5, 6, 7, all bikes</td>
</tr>
<tr>
<td>Buick</td>
<td>Enclave, Lucerne</td>
</tr>
<tr>
<td>Cadillac</td>
<td>BLS, DTS, Escalade, SRX, STS, XLR</td>
</tr>
<tr>
<td>Chevrolet</td>
<td>Avalanche, Caprice, Captiva, Cobalt, Equinox, Express, HHR Impala, Malibu, Monte Carlo, Silverado, Suburban, Tahoe, Trailblazer, Uplander</td>
</tr>
<tr>
<td>Chrysler</td>
<td>300C, Aspen, Grand Voyager, Pacifica, Pt Cruiser, SebringTown Country, Voyager</td>
</tr>
<tr>
<td>Citroen</td>
<td>Berlingo, C-Crosser, C2, C3, C4, C4 Picasso, C5, C6, C8 Nemo, Saxo, Xsara, Xsara Picasso</td>
</tr>
<tr>
<td>Dacia</td>
<td>Duster, Logan, Sandero</td>
</tr>
<tr>
<td>Daewoo</td>
<td>Captiva, Windstorm</td>
</tr>
<tr>
<td>Dodge</td>
<td>Avenger, Caliber, Caravan, Charger, Dakota, DurangoGrand Caravan, Journey, Magnum, Nitro, Ram</td>
</tr>
<tr>
<td>Fiat</td>
<td>500, Bravo, Croma, Daily, Doblo, Fiorino, Grande PuntoPanda, Phedra, Ulysse, Scudo</td>
</tr>
<tr>
<td>GMC</td>
<td>Acadia, Denali, Envoy, Savana, Siera, Terrain, Volt, Yukon</td>
</tr>
<tr>
<td>Honda</td>
<td>Accord, Civic, CR-V, Element, Fit, Insight, Stream, Jazz, Odyssey, Pilot, Ridgeline, most bikes</td>
</tr>
<tr>
<td>Hummer</td>
<td>H2, H3</td>
</tr>
<tr>
<td>Isuzu</td>
<td>D-Max</td>
</tr>
<tr>
<td>Iveco</td>
<td>35C11, Eurostar, New Daily, S-2000</td>
</tr>
<tr>
<td>Jeep</td>
<td>Commander, Compass, Grand Cherokee, Liberty, Patriot Wrangler</td>
</tr>
<tr>
<td>Kia</td>
<td>Carens, Carnival, Ceed, Cerato, Magnetiis, Mentor, OptimaPicanto, Rio, Sephia, Sorento, Spectra, Sportage</td>
</tr>
<tr>
<td>Lancia</td>
<td>Delta, Musa, Phedra</td>
</tr>
<tr>
<td>Mini</td>
<td>Cooper</td>
</tr>
<tr>
<td>Mitsubishi</td>
<td>380, Colt, Eclipse, Endeavor, Galant, Grandis, L200Lancer, Magna, Outlander, Outlander, Pajero, Raider</td>
</tr>
<tr>
<td>Nissan</td>
<td>Almera, <strong>Juke</strong>, <strong>Micra</strong>, Pathfinder, Primera, Qashqai, Interstar Note, Xterra</td>
</tr>
<tr>
<td>Opel</td>
<td>Agila, Antara, Astra, Corsa, Movano, Signum, VectraVivaro, Zafira</td>
</tr>
<tr>
<td>Peugeot</td>
<td><strong>106</strong>, <strong>206</strong>, 207, <strong>307</strong>, 406, 407, 607, 807, 1007, 3008, 5008Beeper, Partner, <strong>Boxer</strong>, <strong>RCZ</strong></td>
</tr>
<tr>
<td>Pontiac</td>
<td>G5, G6, Pursuit, Solstice, Torrent</td>
</tr>
<tr>
<td>Porsche</td>
<td>Cayenne</td>
</tr>
<tr>
<td>Renault</td>
<td>Clio, Duster, <strong>Kangoo</strong>, Laguna II, Logan, MasterMegane, Modus, Sander, <strong>Traffic</strong>, Twingo</td>
</tr>
<tr>
<td>Saturn</td>
<td>Aura, Outlook, Sky, Vue</td>
</tr>
<tr>
<td>Suzuki</td>
<td>Alto, Grand Vitara, Splash, Swift, Vitara, XL-7</td>
</tr>
<tr>
<td>Volkswagen</td>
<td>Touareg, Phaeton</td>
</tr>
</tbody>
</table>
Vehicle Immobilizer

Roel Verdult

Hitag2 transponder
Hitag2 Functionality

• “Quotes” from the datasheet
  – Ideally suited for vehicle immobilization
  – Proximity (20cm) and long range (1m)
  – Effective communication protocol with outstanding data integrity check
  – Secret Key and a random number in order to cipher any communication
  – Mutual authentication function
  – To achieve a main stream security, data may be transmitted enciphered
Unbreakable security levels using mutual authentication, challenge-response and encrypted data communication
# Hitag2 Functionality

<table>
<thead>
<tr>
<th>Block</th>
<th>Contents</th>
<th>Command</th>
<th>Bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>transponder identifier <em>id</em></td>
<td><em>authenticate</em></td>
<td>11000</td>
</tr>
<tr>
<td>1</td>
<td>secret key low <em>k₀...k₃₁</em></td>
<td><em>read</em></td>
<td>11<em>n₀n₁n₂</em>00<em>n₀n₁n₂</em>...</td>
</tr>
<tr>
<td>2</td>
<td>secret key high <em>k₃₂...k₄₇</em> — reserved</td>
<td><em>read</em></td>
<td>01<em>n₀n₁n₂</em>10<em>n₀n₁n₂</em>...</td>
</tr>
<tr>
<td>3</td>
<td>configuration — password</td>
<td><em>write</em></td>
<td>10<em>n₀n₁n₂</em>01<em>n₀n₁n₂</em>...</td>
</tr>
<tr>
<td>4 – 7</td>
<td>user defined memory</td>
<td><em>halt</em></td>
<td>00<em>n₀n₁n₂</em>11<em>n₀n₁n₂</em>...</td>
</tr>
</tbody>
</table>
Authentication Protocol

id = 32-bit identifier
{nR} = Encrypted reader nonce
{aR} = Encrypted reader answer
{aT} = Encrypted tag answer

No tag nonce (nT)
Replay {nR}{aR} results in same keystream
Hitag2 Cipher

• 48 bit internal state (LFSR stream $a_0 a_1 \ldots$)
  
  $a_0 \ldots a_{31} = id_0 \ldots id_{31}$
  
  $a_{32} \ldots a_{47} = k_0 \ldots k_{15}$
  
  $a_{48+i} = k_{16+i} \oplus \{nr\}_i \oplus f(a_i \ldots a_{47+i})_i \quad \forall i \in [0,31]$

  Initialized LFSR = $a_{32} \ldots a_{79}$
Hitag2 Cipher

- Dependencies between sessions
  - Reader nonce (nR) is **only** 32 bits
  - Remember that \( a_{32}…a_{47} = k_0…k_{15} \)
    and initialized \( \text{LFSR} = a_{32}…a_{79} \)
  - We can conclude that \( \text{LFSR}_0…\text{LFSR}_{15} \) are fixed for each session, regardless of \( nR \)
Hitag2 Cipher

- **Non-linear filter function** (20 → 1 bit)
  - Contains sub-functions with fewer inputs
  - Tree function with two layers
  - There are 5 sub-functions with 4-bit input
  - Each function delivers one input bit for second layer function $f_c$
Hitag2 Cipher

- Filter function weakness
  - 4 bits cover 14 bits of the internal state
  - In 8 of the 32 configurations, the output of $f_c$ is **not** influenced by the last bit
  - Probability $\frac{1}{4}$ the output is determined by the first 34 bits of the filter function
Hitag2 Protocol

| read | 11n₀n₁n₂00n₀n₁n₂… |

- After authentication, it uses encrypted instructions of 5 bits which are sent (at least) twice
- The instruction is concatenated with its complement for integrity
- Extra redundancy can be achieved by adding complements multiple times
Hitag2 Protocol

| read          | $11n_0n_1n_200\overline{n_0n_1n_2}\ldots$ |

- Instruction contains a 2-bit command and a 3-bit memory block
- Some examples of (equivalent) read instructions on memory block 3
  - $\text{read } (\text{block3}) = 11011\ 00100$
  - $\text{read } (\text{block3}) = 11011\ 00100\ 11011$
  - $\text{read } (\text{block3}) = 11011\ 00100\ 11011\ 00100$
Hitag2 Protocol

- **Replay** same \{nR\}{aR} and use variable length to get a keystream oracle

  \[
  \text{read (block3)} = 11011 00100 \\
  \text{keystream} = 01010 01101 \oplus \\
  10001 01001
  \]

  **Try all 32 possibilities, only answers when correct**

  \[
  \text{read (block3)} = 11011 00100 11011 \\
  \text{keystream} = 01010 01101 \ldots \oplus \\
  10001 01001 \ldots
  \]
Malleability attack

- Eavesdrop only one authentication attempt \{nR\}{aR} from the car
- Use oracle to recover 42 of keystream bits, enough to read out the memory
- Recover all memory blocks except the secret key (could be read protected)
  - If not configured correctly, the secret key is still readable.
  - In such a case the total attack time is less than one second
Time/memory tradeoff attack

• Once, use a smart trick to build a table with $2^{37}$ cipher states
  – Sort table on 48 produced keystream bits
• Eavesdrop only one authentication attempt $\{nR\}{aR}$ from the car
• Use keystream oracle to recover $2^{11}$ bits
• Apply sliding window on contiguous keystream and find table entry
  • Total attack time is one minute
Cryptanalytic Attack

• Gather only 134 authentication attempts from the car (~1 minute)
• Use first cipher weakness to combine different reader nonces
• Try for every $2^{34}$ cipher state (~5 minutes)
  – Which $\frac{1}{4}$ of the 134 are useful to eliminate
  – If first keystream bit of \{ar\} passes the test
  – Verify handful of candidate keys
• Total attack time is 360 seconds
Comparison and Complexity

<table>
<thead>
<tr>
<th>Attack</th>
<th>Description</th>
<th>Practical</th>
<th>Computation</th>
<th>Traces</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>[45]</td>
<td>brute-force</td>
<td>yes</td>
<td>2,102,400 min</td>
<td>2</td>
<td>4 years</td>
</tr>
<tr>
<td>[14]</td>
<td>sat-solver</td>
<td>yes</td>
<td>2,880 min</td>
<td>4</td>
<td>2 days</td>
</tr>
<tr>
<td>[42]</td>
<td>sat-solver</td>
<td>no¹</td>
<td>386 min</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>[44]</td>
<td>cube</td>
<td>no²</td>
<td>1 min</td>
<td>500</td>
<td>N/A</td>
</tr>
<tr>
<td>Our</td>
<td>cryptanalytic</td>
<td>yes</td>
<td>5 min</td>
<td>136</td>
<td>6 min</td>
</tr>
</tbody>
</table>

¹Soos et al. require 50 bits of contiguous keystream.
²Sun et al. require control over the encrypted reader nonce \(n_R\)
Practical Experiments

- Weak random number generators

<table>
<thead>
<tr>
<th>Origin</th>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAR</td>
<td>18</td>
<td>authenticate</td>
</tr>
<tr>
<td>TAG</td>
<td>39 0F 20 10</td>
<td>id</td>
</tr>
<tr>
<td>CAR</td>
<td>0A 00 00 00 23 71 90 14</td>
<td>{n_R}{a_R} {a_T}</td>
</tr>
<tr>
<td>TAG</td>
<td>27 23 F8 AF</td>
<td></td>
</tr>
<tr>
<td>CAR</td>
<td>18</td>
<td>authenticate</td>
</tr>
<tr>
<td>TAG</td>
<td>39 0F 20 10</td>
<td>id</td>
</tr>
<tr>
<td>CAR</td>
<td>56 00 00 00 85 CA 95 BA</td>
<td>{n_R}{a_R} {a_T}</td>
</tr>
<tr>
<td>TAG</td>
<td>38 07 50 C5</td>
<td></td>
</tr>
</tbody>
</table>
Practical Experiments

- Weak authentication
  - Default password “MIKR”
  - Using key of the form 0xFFFFF* * * * **FF

<table>
<thead>
<tr>
<th>Origin</th>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAR</td>
<td>18</td>
<td>authenticate</td>
</tr>
<tr>
<td>TAG</td>
<td>E4 13 05 1A</td>
<td>id</td>
</tr>
<tr>
<td>CAR</td>
<td>4D 49 4B 52</td>
<td>password = MIKR</td>
</tr>
<tr>
<td>CAR</td>
<td>18</td>
<td>authenticate</td>
</tr>
<tr>
<td>TAG</td>
<td>E4 13 05 1A</td>
<td>id</td>
</tr>
<tr>
<td>CAR</td>
<td>DA 63 3D 24 A7 19 07 12</td>
<td>{n_R}{a_R}</td>
</tr>
<tr>
<td>TAG</td>
<td>EC 2A 4B 58</td>
<td>{a_T}</td>
</tr>
</tbody>
</table>
Practical Experiments

- Tested cars use identifier white-listing
  - Car stores a list of known keys (identifiers)
  - Only authenticates to known identifiers
- First wirelessly pickpocket this identifier
  - Low frequency 125 KHz
    - Few inches
    - Approach victim a few milliseconds
  - High frequency 433 MHz
    - Up to 300 feet
    - Eavesdrop when owner closes the doors
Wirelessly Pickpocketing

Antenna

Proxmark 3
http://www.proxmark.org

http://www.youtube.com/watch?v=UMPs1Zv8tDI
Roel Verdult

• Starting BMW-1 engine
• Look at tachometer
• Without original key
• Using empty key shell and Proxmark to bypass the immobilizer
• Car keeps running after successful authentication

http://www.youtube.com/watch?v=S8z9mgIkqBA

• Start and drive BMW-5
• Car costs $100,000 USD
• Broadcasted on the Dutch national television

http://www.youtube.com/watch?v=QomCiTjqJgo
Attack implications

- Cipher is broken beyond repair
- With tuned antenna larger pickpocket distances can be achieved
- Very serious when the attacker has a few seconds access to the car and key
  - While renting a car
  - Valet parking at hotel
  - Test drive at the dealer
  - Insurance fraud, car owner theft
Conclusion

- Security by obscurity often covers up negligent designs
- Immobilizer based on 3DES or AES cost only a few dollars more
- Notified the manufacturer NXP
  - Responsible disclosure (6 months ahead)
  - Verified and acknowledged our findings
  - Collaborated constructively by discussing mitigating measures