Secure Navigation and Authentication

Sherman Lo
November 2008
Outline

• Motivating Authentication
• Proposed techniques for authentication
  – Source authentication
  – Cross checking
• My research
GNSS: Position, Navigation & Time
How do I know it is right?

Pizza? I’m hungry!
Authentication: What is it & Why?

• GPS (and GNSS) being increasingly used for vital applications
  – Safety: aviation
  – Infrastructure: timing for cellular, power grid
  – Asset tracking & location

• Creates strong incentives to spoof
  – Reasons: Financial, Terrorism
  – Transport of valuable, dangerous material
  – Emergency response, geo fencing
  – Road tolls, taxi fare, & other financial transactions using navigation information

• Current civil signal easy to generate
• Authentication is the ability to verify the navigation signal’s source or content
Need for Location Assurance

Location Assurance is important in many applications
- Valuable Goods/Asset Tracking
- Emergency Response
- Road Tolling
- Any app with significant € or $ tied to location
Incentive for Self Spoofing
GNSS (and Navigation) as a security tool

Position as Security
- Cargo access
- Route auditing
- Content Control
- Marine Fishery Management

Security of Position
- First responders
- Auto tolling
- Cargo delivery
- Route auditing
Spoofing civil GPS signals is quite feasible

Humphreys, ION GNSS 2008
Future Signals have Encryption for Restricted Users
Some Techniques

1. Data Authentication
   - Message contains “unforgeable” hash of information that verifies it has not been changed
   - Encryption key used to verify source
2. Public spreading code
   - Relies on GNSS signal below noise & difficult to extract
   - Delayed release of spreading code means not spoofable a priori/immediately
3. Private spreading code
   - Uses secret key that is never revealed
   - Requires secure receiver
4. Consistency checks of location related information
   - Verify source generated the info & that it has not been altered
   - Limit possible potential delay (hence spoofing)
Classifying Proposed Techniques

- Hidden info revealed later
  - TESLA (symmetric key authentication)
  - Public Spreading Code
  - Requires some time synchronization

- Hidden info revealed never
  - Digital signatures (asymmetric key authentication)
  - Military service: W code, M code Galileo PRS
  - Private Spreading Code
  - Info hidden info for each sat cannot be extracted, no time sync is needed

- Position dependent properties
  - Different properties are observed at different locations (can determine this a priori)
  - May be possible but difficult
1. Data Authentication Techniques

- Digitally signed hash
  - Asymmetric key based
  - Private key signs hash
  - Validated by public key & msg hash

- MAC
  - Tag generated using msg and key
  - Difficult for attacker to generate valid msg, tag pair without key
  - Symmetric key is more efficient (data, computation)
Signed Hash

Signed Hash

\[ [A_1 \ldots A_m] = \text{SIG}_K(\text{HASH}([M_1 \ldots M_n])) \]

Time

- Authentication accomplished by checking that the signed (with private key K) of hash of messages is correct
  - User has public key (requires key distribution)
  - With signature, data cannot be easily spoofed
- Delay is incurred
  - Must wait n+m messages to verify message \( M_1 \)
- Elliptic Curve allows for greater data & computational efficiency
Basic TESLA

\[ \text{tag}_m = \text{MAC} ( \text{data}_m, \text{key}_m ) \]

- TESLA uses time (delayed key disclosure) to achieve the asymmetry property required for secure broadcast authentication.
- Kuhn (2004), Wullems, et. al. (2005) proposed its use.
  - Developed for networks.
- Send data & hash, later reveal key to check that the data.
  - Creates time window where spoofer cannot generate valid msg.
- Key checked with based key using one way hash functions.
  - If \( n \) hashes of \( \text{key}_n = \text{base key} \), then key is from valid source.
• Pre-compute a sequence of key values using one-way hash functions or pseudo-random functions. $K_{i-1} = F(K_i)$, $\ldots$, $K_1 = F(K_2)$

• Use another hash function to compute $K'$. $K'_i = F'(K_i)$

• Generate MAC using $K'$ and Message $M$

• Send packet $P$. $P_i = <M_i, K_{i-d}, MAC_i>$

• Distribute key $K_0$ via secure means (check $K_i$ are from same source)
Authentication Strength and MAC Length

- Strength of authentication depends on choice of hash functions and bits used

<table>
<thead>
<tr>
<th>Hash Function</th>
<th>Hash Length (bits)</th>
<th>Effective Strength (bits)</th>
<th>Time to break*</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD4</td>
<td>128</td>
<td>20</td>
<td>&lt;1 sec</td>
</tr>
<tr>
<td>MD5</td>
<td>128</td>
<td>32</td>
<td>1 sec</td>
</tr>
<tr>
<td>SHA1</td>
<td>160</td>
<td>69</td>
<td>34 years</td>
</tr>
<tr>
<td>SHA256</td>
<td>256</td>
<td>128</td>
<td>$10^{19}$ years</td>
</tr>
</tbody>
</table>

* $100K$ Hardware brute-force attack

SHA 1 now 63 bits
Strength of MAC

<table>
<thead>
<tr>
<th>Time from today (years)</th>
<th>Time to break SHA1</th>
<th>Time to break SHA256</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>34 years</td>
<td>$10^{19}$ years</td>
</tr>
<tr>
<td>12</td>
<td>1.6 months</td>
<td>$4 \times 10^{16}$ years</td>
</tr>
<tr>
<td>18</td>
<td>3 days</td>
<td>$2.4 \times 10^{15}$ years</td>
</tr>
<tr>
<td>24</td>
<td>4.5 hrs</td>
<td>$1.5 \times 10^{14}$ years</td>
</tr>
</tbody>
</table>

- Table of strength vs. time to crack above (give year) + Projection in 12 years (Moore’s law $2^8$)
- Strength is limited by the length of the authentication data
2. Public Spreading Code

- Spreading code segments stored until code revealed
  - Segments are transmitted at same time from each SV (overlap)
- Not spoofable until spreading code info is revealed
  - Time window dictates how synchronized the clock must be
3. Private Spreading Code

- Similar to Military codes
- Implementation above is based on Scott (2003)
  - Limits some vulnerabilities of public spreading code but also retains some
  - Other ways to implement

Diagram:

- Known PRN code
- Unknown PRN code

Data₁ → SC₁ → PSC₁ → ... → Dataₙ → SCₙ → PSCₙ → SC Info → Dig Sig → ...

Time

Verify that signal/info is there & consistent

Secure Module
4. Authentication through Information Consistency

- Doppler and other location measures
  - Difficult to spoof wide area & replicate
- Loran and other ground based nav systems have many other measures
- Multisystem measurements: GNSS, ground transmitters (DTV, Loran), INS, etc.
Consistency Checks Example: Doppler

Aircraft can check Doppler with expected value since tx and user location is known.

However, spoofer can add doppler to affect.
Current Civilian Authentication

• Constrain transmission
  – CAT II/III Requirements Development: Modifications to GBAS for VDB Authentication
    • Presented July 2008 by Tim Murphy

• Cross check measurements or info content
  – RAIM, AIME & other navigation related information
  – Checking consistency of measurements not spoofing

• Data authentication is still not common
Example: VDB Authentication Proposal

Figure 2  Approach Selection Scheme with the Proposed Authentication Protocols Added
VDB Authentication Goals

- Pilot identifies RPI (ref path id) – first char identifies 1 to 8 (SSID of gnd station) using Type 4 message matches approach plate
- Type 2 message give slot group def (SGP) which identifies slot of msg of the GS
  - Broadcast in the slot indicated by SSID

- Prevents spoofing to open slots
- Does not prevent overpowering GS or turning off GS and spoofing
  - If Type 4 or Type 2 msg hijacked, then spoofer can operate without interference
<table>
<thead>
<tr>
<th></th>
<th>GPS</th>
<th>Loran</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-stationary satellites</td>
<td>Stationary transmitters</td>
<td></td>
</tr>
<tr>
<td>High absolute accuracy</td>
<td>Low absolute accuracy</td>
<td></td>
</tr>
<tr>
<td>High repeatable accuracy</td>
<td>High Repeatable accuracy</td>
<td></td>
</tr>
<tr>
<td>Global coverage</td>
<td>Northern hemisphere</td>
<td></td>
</tr>
<tr>
<td>Low SNR</td>
<td>High SNR</td>
<td></td>
</tr>
<tr>
<td>Easy to jam and spoof</td>
<td>Hard to jam and spoof</td>
<td></td>
</tr>
<tr>
<td>Indoor NOT capable</td>
<td>Indoor capable</td>
<td></td>
</tr>
<tr>
<td>Data channel</td>
<td>Data channel (e-Loran)</td>
<td></td>
</tr>
</tbody>
</table>
Thoughts

• Secure navigation info & authentication will become increasingly important
  – Navigation and GNSS becomes more important in economy and people’s lives

• Techniques do exist for authentication
  – Difficult to build into satellite
    • Must work easily within current infrastructure
  – Solution not requiring sat changes more likely/rapid
    • Receiver/ground based processing
    • Very possible to provide strong authentication

• With secure navigation, can use location to enable or strengthen various applications discussed
  – Valuable asset management, road tolling, emergency response, many others