Integrity (I) Codes: Message Integrity Protection and Authentication Over Insecure Channels

Mario Čagalj†
Ramkumar Rengaswamy‡
Mani Srivastava‡

Srdjan Čapkun§
Ilias Tsigkogiannis‡
Jean-Pierre Hubaux†

†EPFL §Technical University of Denmark ‡UCLA

May 23, 2006
Common wisdom

- Any security system is only as secure as its weakest link
- Weakest link commonly the user, given that the considered system is not user-friendly

Folk theorem:

User-unfriendliness $\Rightarrow$ security systems highly insecure
Problem Statement

− “ ” public (insecure) radio channel
− Alice and Bob within each others’ transmission range
− Alice and Bob share neither secrets nor certified public keys
− How to preserve the integrity of the “message”, while minimizing the users’ involvement?
Existing Approaches

- Users share prior context
  - Certified public keys
  - Passwords (Bellovin and Merritt - PAKE)
- No prior context
  - Physical contact (Stajano and Anderson)
  - Location limited infrared channel (Balfanz et al.)
  - Hash visualization (Perrig and Song)
  - Hash functions to readable words (Dohrmann and Ellison)
  - Seeing is believing (McCune, Perrig and Reiter)
  - Short string comparison (Čagalj, Čapkun and Hubaux)
The presence or absence of energy in a given time slot of duration $T_s$ conveys information.
Integrity (I) Codes

Definition

An integrity code is a triple \((S, C, e)\), where the following conditions are satisfied:

1. \(S\) is a finite set of possible source states (plaintext)
2. \(C\) is a finite set of codewords
3. \(e\) is a source encoding rule \(e : S \rightarrow C\), satisfying the following:
   - \(e\) is an injective function
   - it is not possible to convert codeword \(c \in C\) to another codeword \(c' \in C\), such that \(c' \neq c\), without changing at least one bit 1 of \(c\) to bit 0.
I-code Example: Complementary Encoding

- Complementary encoding rule (Manchester) $e$:

\[
\begin{align*}
1 & \rightarrow \ 10 \\
0 & \rightarrow \ 01 \\
\end{align*}
\]

- $S = \{00, 01, 10, 11\} \overset{e}{\rightarrow} C = \{0101, 0110, 1001, 1010\}$

\[
\begin{align*}
0101 & \rightarrow \ 0111 & 0110 & \rightarrow \ 0111 \\
0101 & \rightarrow \ 1101 & 0110 & \rightarrow \ 1111 \\
0101 & \rightarrow \ 1111 & 0110 & \rightarrow \ 1110 \\
\end{align*}
\]
Assumptions

1. Sender and receiver are in synch wrt. the beginning and the end of c
2. Adversary cannot block (annihilate) signal 1 (except with $\varepsilon$)

Theorem

The adversary cannot trick the receiver into accepting the message $\hat{m}$ when $m \neq \hat{m}$ is sent, except with $\varepsilon$ probability.

Proof:

- $\hat{m} \neq m \Rightarrow \hat{c} \neq c$ (I-code)
- $c \rightarrow \hat{c}$ implies at least one bit 1 of $c$ to bit 0 (I-code)
- Adversary has to annihilate some of the emitted signals (with $\varepsilon$ prob.)

q.e.d.
Definition (informal)

Given $C$, $i$-delimiter is a minimum-length bit string such that any valid codeword $c \in C$ received between two consecutive $i$-delimiters is authentic.

Example (complementary encoding)

$S = \{0, 1, 00, 01, \ldots, 11 \ldots 1\}$, $C = \{01, 10, 0101, 0110, \ldots, 1010 \ldots 10\}$

$\ldots 111000 1010011001 111000 1010011001 111000 \ldots$

$i$-delimiter $i$-delimiter $i$-delimiter

Receiver does not have to know the length of the $c$ in advance

“Correct” $c$, received between two subsequent $i$-delimiters is authentic
Synchronization via Incongruous (i) Delimiters

Definition (informal)

Given $C$, i-delimiter is a minimum-length bit string such that any valid codeword $c \in C$ received between two consecutive i-delimiters is authentic.

▶ Example (complementary encoding)

$S = \{ 0, 1, 00, 01, \ldots, 11 \ldots 1 \}$, $C = \{ 01, 10, 0101, 0110, \ldots, 1010 \ldots 10 \}$

$c$

\[
\begin{array}{cccc}
\text{i-delimiter} & 111000 & 1010011001 & 111000 & 1010011001 & 111000 & \ldots \\
\end{array}
\]

▶ Receiver does not have to know the length of the $c$ in advance

▶ “Correct” $c$, received between two subsequent i-delimiters is authentic
Anti-blocking Property of a Radio Channel ($1 \nrightarrow 0$)

\[
\begin{align*}
\hat{r}(t) &= \cos(\omega_0 t) - \cos(\omega_0 t - \theta), \text{ where } \theta \in [0, 2\pi) \\
&= r(t) = \cos(\omega_0 t) - \cos(\omega_0 t - \theta), \\
\text{receiver} & \quad \text{sender} \quad \text{adversary}
\end{align*}
\]

\[
E_r = \int_0^{T_s} r^2(t) dt 
\approx 2 T_s \sin^2 \left( \frac{\theta}{2} \right)
\]

\begin{figure}
\centering
\includegraphics[width=\textwidth]{chart.png}
\end{figure}
Anti-blocking Property of a Radio Channel \( 1 \rightarrow 0 \)

Alice \( \rightarrow \) Mallory \( \rightarrow \) Bob

\( d_{AB} \)

\( d_{MB} \)

\( \Delta d \) (distance shift) [cm]

\( \theta \) (phase shift) [rad]

\( f_0 = 0.5 \text{ GHz} \)

\( f_0 = 1 \text{ GHz} \)

\( f_0 = 2.4 \text{ GHz} \)

\( f_0 = 5 \text{ GHz} \)

ˇCagalj et al. (EPFL, DTU, UCLA)  
IEEE S&P  
May, 2006 11 / 19
Anti-blocking Property of a Radio Channel \((1 \rightarrow 0)\)

\[
R(t) = \cos(\omega_0 t + \Phi) - \cos(\omega_0 t - \Theta), \quad \Phi \in U [0, 2\pi)
\]

- \(\Theta\) a random variable (example, \(\Phi = 0\))
  - Energy content \(E_R = \mathbb{E} \left[ \int_0^T R^2(t) dt \right] \approx T\), for uniform \(\Theta\)
  - Gaussian Distribution of \(\Theta\) with zero mean and variance \(\sigma^2_\theta\)

\[
\sigma^2_\theta = (2\pi f_0/c)^2 \sigma^2_d
\]

\(f_0 = 5\, \text{GHz}\),
\(\sigma_\theta = 1.189\ \text{rad} \Leftrightarrow \sigma_d = 1.14\ \text{cm}\)
Randomization at the Sender

\[ P[K_{\text{attenuated}} \leq K_{\varepsilon}] \geq 1 - \varepsilon, \quad \varepsilon = 10^{-14} \]
Applications of I-codes

- **Authentication through presence (radio channel)**

- **Solving our initial problem**

Alice sends Bob the message $m$ and the I-code $I-code(h(m))$.
Other Applications

- Broadcast Authentication
  - Access Point Authentication
Implementation of I-codes

- Mica2 sensor networking platform (UCLA SOS operating system)
  - Frequency Shift Keying, output power $-20$ to $10$ dBm
- Complementary encoding
  - Every bit 1 transmitted as an 48-bit packet ($T_s = 10$ ms)
  - Every bit 0 transmitted as an absence of signal ($T_s = 10$ ms)

![Graph showing transmission success ratio vs. message size]
Time-invariance

Alice ⇄ Bob

Time-variant solutions

Time-invariant solutions

Symmetric Key Size
Crypto. Hash Function Size in Bits

Years


60 65 70 75 80 85 90 95 100
Optimal Message Transfer (MT) Authenticator

Alice

Given $m$

Pick $N_A \in_U \{0, 1\}^k$

$(c, d) \leftarrow \text{commit}(m\|N_A)$

$s_A \leftarrow N_A \oplus \hat{N}_B$

Bob

Pick $N_B \in_U \{0, 1\}^k$

$c \leftarrow N_B$

$d \leftarrow \text{open}(\hat{c}, \hat{d})$

$s_A \leftarrow N_B \oplus \hat{N}_A$

If $s_A = s_B$, “Accept” $\hat{m}$

- Transmit $s_A$ using I-codes
- Free choice of the size of $s_A$ (e.g., 50 bits)
- Time-invariant solution

---

\(^1\)Čagalj, Čapkun and Hubaux. “Key Agreement in Peer-to-Peer Wireless Networks”. Proceedings of the IEEE (Special Issue on Cryptography and Security), 2006.
Optimal Message Transfer (MT) Authenticator

Alice
Given \( m \)
Pick \( N_A \in \{0,1\}^k \)
\((c, d) \leftarrow \text{commit}(m\|N_A)\)
\( s_A \leftarrow N_A \oplus \hat{N}_B \)

Bob
Pick \( N_B \in \{0,1\}^k \)
\( \hat{m}\|\hat{N}_A \leftarrow \text{open}(\hat{c}, \hat{d}) \)
\( s_B \leftarrow N_B \oplus \hat{N}_A \)

If \( s_A = s_B \), “Accept” \( \hat{m} \)

- Transmit \( s_A \) using I-codes
- Free choice of the size of \( s_A \) (e.g., 50 bits)
- **Time-invariant solution**

---

\(^1\)Ćagalj, Čapkun and Hubaux. “Key Agreement in Peer-to-Peer Wireless Networks”. *Proceedings of the IEEE (Special Issue on Cryptography and Security)*, 2006.
Summary and Future Work

- Integrity and authentication without shared keys/certificates (over insecure radio channels)
  - Anti-blocking property of a radio channel
  - Location awareness

- Applications
  - Walk-in scenarios (AP authentication)
  - Broadcast authentication with low-power devices (Mica2 sensor platform)
  - P2P and group key establishment

- Authentication through presence

Future work: Application of I-codes to a wired channel?