HELP: Helper-Enabled In-Band Device Pairing Resistant Against Signal Cancellation

Nirnimesh Ghose, Loukas Lazos, and Ming Li
Department of Electrical and Computer Engineering,
University of Arizona, Tucson

Presented at the :
26th USENIX Security Symposium, Vancouver
A Pervasive Network-Enabled Ecosystem

- child and elder monitoring
- health monitoring
- fitness tracking
- nutrition tracking
- smart lighting
- home surveillance
- smart cars
- safety and temperature control
- smart appliances

HELP: Helper-Enabled In-Band Device Pairing Resistant Against Signal Cancellation
How to we secure the information flow to protect the plethora of collected sensitive data?

We need some
Achieve **mutual authentication** and **key agreement** in the presence of Mallory

Authenticate the identity of Bob and Alice

Verify the integrity of the communications

Agree on a common secret
In the context of this work, securely pair new devices with a hub

By the end of the device pairing
  - A has verified the authenticity of D
  - D and A share a common key $K_{D,A}$

**Challenge**: Most new devices lack advanced interfaces such as keyboards, monitors, etc.
Goals: (a) pair a rogue device with the hub, (b) force $D$ to join a rogue hub

Means: Perform a MitM attack over wireless
- Aware of the channel between $D$ and $A$, which is predictable and relatively stable
- Aware of the $D$-$M$ and $M$-$A$ channels
- Can synchronize with $D$ (by listening to preambles)
- Can perform overshadowing and/or signal cancellation attacks (worst-case adversary)
Existing Solutions for Trust Establishment

Manually enter a password to the device – requires an advanced interface

Preload password to device – manufacturers often opt for preloading the same password to multiple devices, which leads to massive vulnerabilities (Mirai botnet)

Execute a Diffie-Hellman (DH) key exchange – Vulnerable to MitM

Perform out-of-band verification using light, sound, LEDs, etc. – requires advanced interfaces

Non-cryptographic verification techniques – often require specialized hardware

In-band verification techniques – only require a common RF interface
In-Band Integrity Verification

Manchester coded ON-OFF keyed message

$m_D = 11000$

$m_M = 00011$

Prior works assume signal cancellation is not possible due to the rich scattering environment\(^+\) or it occurs with limited probability\(^*\)


Signal Manipulation Attack

The infeasibility of signal cancellation assumption does not always hold

Pöpper et al.* demonstrated an effective relay signal cancellation attack using a pair of directional antennas

Our Contributions

Constructed an in-band message integrity verification primitive, for devices that do not share any secrets

Proposed HELP, a DH-based authenticated key agreement protocol, which is the first protocol resistant to MitM attacks based on signal cancellation

Analyzed security and showed negligible success probability even if perfect signal cancellation can be achieved

Implemented HELP on the USRP testbed and validated the effectiveness of the primitive in detecting message injections/modifications the adversary’s diminishing success in pairing rogue devices
HELP – Integrity Verification Primitive

$D$  

$H$  

$s$  

$A$  

$M$  

$m_M = 00011$

Cancelled helper’s slots
Device Pairing with HELP

ID_D, (G, q, g)

Pick X_D ∈ U \mathbb{Z}_q
z_D ← g^{X_D} mod q
m_D ← ID_D, z_D

(H active)

ID_A, (G, q, g)

Pick X_A ∈ U \mathbb{Z}_q
z_A ← g^{X_A} mod q
m_A ← ID_A, z_A

(H active)

\[ h(m_D), m_D \] + m_H

AE(s, K)

m_A

K_{D,A} = g^{X_D X_A} mod q

Verify and Extract m_D

K_{D,A} = g^{X_D X_A} mod q
Security Analysis of the Help Primitive

\[ \delta = \left( 1 - \frac{1 - p_I}{4} \right) \]

- Probability of inferring the helper's activity during one slot
- Probability that the hub accepts a message forgery

Graph:
- x-axis: Number of helper's ON slots (|s|)
- y-axis: \( \delta \)
- Three lines for different \( p_I \): 0.50, 0.75, and 0.90
Security Analysis of the Device Pairing Protocol

Given $ID_D$ 
$(G, q, g)$
Pick $X_D \in_U \mathbb{Z}_q$
$z_D \leftarrow g^{X_D} \mod q$
$m_D \leftarrow ID_D, z_D$

$[h(m_D), m_D]$

$[h(m_D), m_D] + m_H$

$(H \text{ active})$

$K_{D,M} = g^{X_D X_M} \mod q$

$K_{D,M} = g^{X_D X_M} \mod q$

$K_{M,A} = g^{X_M X_A} \mod q$

Given $ID_M$ 
$(G, q, g)$
Pick $X_M \in_U \mathbb{Z}_q$
$z_A \leftarrow g^{X_M} \mod q$
$m_M \leftarrow ID_M, z_M$

$[h(m_M), m_M]$

$[h(m_M), m_M]$

$(H \text{ active})$

Pick $X_A \in_U \mathbb{Z}_q$
$z_A \leftarrow g^{X_A} \mod q$
$m_A \leftarrow ID_A, z_A$

$[h(m_M), m_M]$

Extract $m_M$

Fails $s$ verification

$K_{M,A} = g^{X_M X_A} \mod q$
Security Analysis of the Downlink Direction

\[ \delta = \left( p_I' \right)^{|s'|} \]

- \( \delta \): Probability of inferring the helper's activity during one slot.
- \( p_I' \): Probability that the device accepts a message forgery.
- \( |s'| \): Number of helper's ON slots.

Graph shows the relationship between the number of helper's ON slots and the probability \( \delta \) for different values of \( p_I' \) (0.5, 0.75, 0.90).
Probability of Helper Activity Inference ($p_I$)

Adversary’s capability in timely identifying the helper’s ON slot, the adversary could employ several PHY-layer characteristics:

- Frequency offset
- Channel impulse response
- I/Q origin offset
- Transient radio state
- Angle of arrival for incoming signal
- Received signal strength
- Time offset
Fast Helper Detection based on RSS
Probability of Inference with $H$ and $D$ transmit at Fixed Power

$\Prob_{DH}$, $\Prob_D$, $\Prob_H$, $\Prob_{NDH}$

![Graph showing probability of inference with varying windows of samples.](image)

- $\Prob_{DH}$: Red square marker
- $\Prob_{NDH}$: Green triangle marker
- $\Prob_H$: Blue circle marker
Probability of Inference with $H$ and $D$ transmit at Varying Power
Probability of Inference when $H$ and $D$ remain Equidistant
Probability of Inference when $H$ is Moved Towards $M$

$H, D$ powers are fixed

Distance

$P_{DH}$ $P_D$ $P_H$ $P_{NDH}$

Distance (feet)

Probability of Inference

$P_{DH}$ $P_{NDH}$ $P_H$
Probability of Inference when $H$ is Moved Towards $M$

$H,D$ powers are Randomized
Fast Helper Detection Based on Time

Helper Transmission
Device Transmission
Helper Transmission
Adversary Reception

helper is always faster (or slower)
Randomize Slot Starting Times

helper is sometimes faster, sometimes slower
Normalized Number of Slots that Each Device is Faster

![Graph showing normalized number of slots that each device is faster as a function of synchronization offset. The graph compares 'Device Signal' (red squares) and 'Helper Signal' (blue triangles). The x-axis represents synchronization offset in units of $10^{-8}$, and the y-axis represents normalized number of slots faster.]
Protocol Evaluation Setup

Device

Helper

Rx1

Rx2
Protocol Evaluation Results

Graph 1: Length of $h(m_D)$ ($\ell$)

Graph 2: Number of Helper ON Slots ($|s|$)

Legend:
- $p_C = 0.50$
- $p_C = 0.75$
- $p_C = 1.00$

Wednesday, August 16, 2017
Conclusions and Future Work

We proposed a new PHY-layer integrity protection scheme called HELP that is resistant to signal cancellation attacks.

Our protocol is aimed at alleviating the device pairing problem for IoT devices that may not have the appropriate interfaces for entering or pre-loading cryptographic primitives.

We showed that the DH key agreement protocol using HELP can resist MitM attacks without requiring an authenticated channel between device and the hub.

Future Work: Investigate a MitM-resistant in-band pairing technique that does not rely on ON-OFF keying so that it is compatible with COTS devices.