CS 5410 - Computer and Network Security: Localization

Professor Patrick Traynor
Fall 2017
Announcements

• Everything* has been turned in, and is in the process of being graded.

• What should you be doing now?
  • Implementing the methodology you noted in your abstracts
  • Running experiments
  • Making graphs
  • Getting. It. Done.
Who Names These Things Anyway?

SwiftOnSecurity @SwiftOnSecurity · 15h
That worked out

Today In Infosec @todayininfosec
2001: The author of the Nimda worm released a new variant to add a comment that it should be referred to as Concept Virus, not Nimda.
Story Time
Location Matters

• Location can serve as a critical input to many real-world processes.
  • Not strongly knowing location can end up costing you money, or worse…
  • How do we build systems and protocols that allow us to reason about our location?
  • What “proof” do we have?
Global Positioning System

- System consists of 31 satellites flying ~12,550 miles above the earth.
- Begin by calculating distance from individual satellites:
  - Each satellite transmits its own code, which the receiver also generates.
  - Upon reception, the receiver determines the difference.
  - Each message is also timestamped
  - This class of ranging is known as Time-Difference of Arrival (TDOA).
GPS - Trilateration

- Given the distance from three (or more points), the receiver can easily calculate their current location.
- “Worst Case” accuracy is 7.8 meters.
GPS Problems

• Performance assumes clear line-of-sight of the sky.
• So it is not going to work in cities, and likely not well indoors.

• Adversarial model?
• Let’s dig in a bit more here…
GPS Adversaries

• US Government?
  • Criticism: They could shut it off at any time!
  • Reality: Even on 9/11, this did not happen.
  • Response: The EU’s Galileo and Russia’s Glonass

• Active Adversaries?
  • Everyone knows the signal, so anyone (?) can force errors into location calculations.
Defining Adversaries

- **Distance Fraud**
  - A malicious prover is trying to falsify distance

- **Mafia Fraud**
  - A malicious third party is trying to tamper with an honest interaction

- **Terrorist Fraud**
  - A malicious third party and prover work together
Related Schemes

• Indoor Localization

• Instead of satellites, rely on indoor transmitters and their Received Signal Strength Indication (RSSI).

• A wide range of experimental systems were built for this context, relying on largely on 802.11 (and a few on Bluetooth).

• Do RSSI schemes fare well against our adversaries?
Secure Distance Bounding

- Combines random challenges with RTT measurements to determine distance
- Message speed limited by the speed of light
- Ensures an adversary can’t fake their response
Brands-Chaum Protocol

\[ m_i \in \mathcal{R} \{0, 1\} \]

commit(m₁, ..., mₖ)

\[ \alpha_i \in \mathcal{R} \{0, 1\} \]

Rapid bit exchange

\[ \beta_i \leftarrow \alpha_i \oplus m_i \]

\[ c \leftarrow \alpha_1|\beta_1|\cdots|\alpha_k|\beta_k \]

(open commit), sign(c)

Verify commit

\[ c \leftarrow \alpha_1|\beta_1|\cdots|\alpha_k|\beta_k \]

verify sign(c)
Theoretically speaking...

• Existing work considers protocol operations
• Critical assumption: computation time is negligible
  • Which is faster, light or computing anything?
• What about laptops? Credit cards? Phones?
• Few implementations have been built to show this
Tippenhauer et al.

- End-to-end implementation of distance bounding
- Uses customized hardware to send, receive, and compute the rapid bit exchange (RBE) messages
- First demonstration that distance bounding is truly feasible
Signal: modulation

- Determines how bits are represented using analog waves
- Requires time at transceiver to convert between digital and analog
- Must account for noise on the channel
Signal: pulse length

- Depending on radio technology and modulation, bit representations vary in length
- Redundant information (error correcting codes, multiplexing) can increase this length
Early detect/late commit

- Early Detect: Attacker tries to predict the bit before receiving all the signal samples
- Late Commit: Leverages the ability of a receiver to decode the bit even though all the samples are not correct
Detection interval

- Signal is reflected and received multiple times (multipath propagation)
- Combining multiple signals allows for better accuracy
- Listening for multiple signals takes time
Processing: digital or analog

- Converting signal to digital, loading to computer, processing results (and the reverse) takes time

- Confine as much processing to the transceiver itself (in analog)

- Accomplished via custom hardware (FPGAs) and signal reflection
Results

- Distance estimation
  - mean error: 10.9 cm
- Bit error rate (BER)
  - Average BER: 2.7%
- Distance/Mafia fraud distance advantage
  - 15.6 m/1.2 m
- Operating distance: 2.5 m
- Is this good enough?
- Our recent work uses distance-bounding inspired techniques to detect SS7 redirection attacks.
Take-Aways

- Location matters
  - It can help us protect critical resources and life itself.
  - It can also enable a range of new systems!
- Secure localization is critical
  - We rely on these systems daily, but they are vulnerable.
  - New techniques are available that can dramatically reduce an adversary’s advantage.