



# Protecting Privacy & Securing the Gathering of Location Proofs

---

the Secure Location Verification  
Proof Gathering Protocol  
(SLVPGP)





# Structure

---

- ***Introduction***
- System Outline
- The Protocol
- Analysis
- Conclusion



# Introduction

---

- Location verification -> proving a device's current location
- 2 step process
  - Distance bounding to gather proof
  - Proofs sent to Verifier to judge validity of claim
- Protocol protects gathering procedure



# What was there before?

---

- Global Positioning System (GPS)
  - Spoofable
  - Precise Positioning Service (PPS) restricted
- Echo protocol – Sastry, Shankar & Wagner
  - Combines ultrasound and radio frequency
- Proximity Proving protocol – Waters & Felten
  - 802.11 environment
  - Relies on trusted devices
  - No tie between distance bounding replies and involved devices



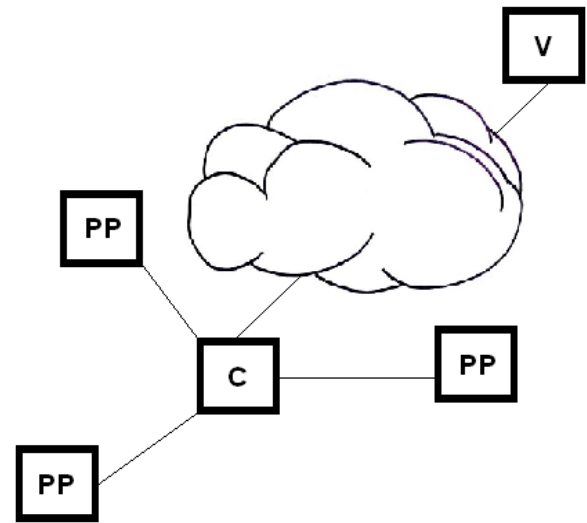
# Up next...

---

- Introduction
- ***System Outline***
- The Protocol
- Analysis
- Conclusion

# System model

- Claimant (C)
- Verifier (V)
- Proof Provider (PP)
- Designed to meet three security properties





# Security properties

---

- Anonymity of *identity*
- Confidentiality of *location*
- Authentication of *information*



# Threat model (1)

---

- Honest nodes
  - Receive all messages broadcast within range
  - Only act on messages intended for them
- Three kinds of malicious node
  - Claimant
  - Proof Provider
  - External to system
- All nodes contain tamper resistant module
- Participation leaks location information



# Threat model (2)

---

- Attacks considered
  - Guessing attack
  - Terrorist fraud (proxy attack)
  - Snooping attack



# And now...

---

- Introduction
- System Outline
- ***The Protocol***
- Analysis
- Conclusion

# The SLVPGP – basic design

1.  $C \rightarrow V: C, X_C$
2.  $V \rightarrow C: B_1, B_2, \dots, B_n$
3.  $C \rightarrow B_i: B_i, N_i, N'_i$
4. Distance Bounding
  - (a)  $B_i \rightarrow C: k, H_{i,k}, N''_i$
  - (b)  $C \rightarrow B_i: H'_{i,k}, N''_i$
5.  $B_i \rightarrow C: T_i, X_i, L_i$
6.  $C \rightarrow V: C, T_C, X_C, \{T_1, X_1, L_1\}, \dots, \{T_n, X_n, L_n\}$

# Extending the protocol – level 1

1.  $C \rightarrow V: \{|C, X_C|\}_{K_C^-}$

2.  $V \rightarrow C: \{|B_1, B_2, \dots, B_n|\}_{K_V^-}$

3.  $C \rightarrow B_i: B_i, \{N_i, N'_i\}_{K_{B_i}^+}$

4. Distance Bounding

(a)  $B_i \rightarrow C: k, H_{i,k}, N''_i$

(b)  $C \rightarrow B_i: H'_{i,k}, \{|N''_i|\}_{K_C^-}$

5.  $B_i \rightarrow C: \{|T_i, X_i, L_i, C|\}_{K_{B_i}^-}$

6.  $C \rightarrow V: \{|T_C, X_C|\}_{K_C^-}, \{|T_1, X_1, L_1, C|\}_{K_{B_1}^-}, \dots, \{|T_n, X_n, L_n, C|\}_{K_{B_n}^-}$

# Extending the protocol – level 2

1.  $C \rightarrow V: \{\{|C, X_C|\}_{K_C^-}\}_{K_V^+}$
2.  $V \rightarrow C: \{\{|B_1, B_2, \dots, B_n|\}_{K_V^-}\}_{K_C^+}$
3.  $C \rightarrow B_i: \{B_i, C, N_i, N_i'\}_{K_{B_i}^+}$
4. Distance Bounding
  - (a)  $B_i \rightarrow C: k, H_{i,k}, N_i''$
  - (b)  $C \rightarrow B_i: H'_{i,k}, \{|N_i''|\}_{K_C^-}$
5.  $B_i \rightarrow C: \{\{|T_i, X_i, L_i, C|\}_{K_{B_i}^-}\}_{K_C^+}$
6.  $C \rightarrow V: \{\{|T_C, X_C|\}_{K_C^-}\}_{K_V^+},$   
 $\{\{|T_1, X_1, L_1, C|\}_{K_{B_1}^-}\}_{K_V^+}, \dots, \{\{|T_n, X_n, L_n, C|\}_{K_{B_n}^-}\}_{K_V^+}$

# Extending the protocol – level 3

1.  $C \rightarrow V: \{ \{ |C, X_C| \}_{K_C^-} \}_{K_V^+}$
2.  $V \rightarrow C: \{ \{ \{ B_1, N_1, N'_1, N''_1 \}_{K_{B_1}^+}, \{ N_1, N'_1, N''_1 \}_{K_C^+}, \dots, \{ B_n, N_n, N'_n, N''_n \}_{K_{B_n}^+}, \{ N_n, N'_n, N''_n \}_{K_C^+} \} \}_{K_V^-}$
3.  $C \rightarrow B_i: \{ B_i, N_i, N'_i, N''_i \}_{K_{B_i}^+}, \{ C \}_{K_V^+}$
4. Distance Bounding
5.  $B_i \rightarrow C: N''_i, \{ \{ |N''_i| \}_{K_C^-}, N''_i \}_{K_{B_i}^-}, \{ \{ |T_i, X_i, L_i, \{ C \}_{K_V^+}| \}_{K_{B_i}^-} \}_{K_V^+}$
6.  $C \rightarrow V: \{ \{ |T_C, X_C| \}_{K_C^-} \}_{K_V^+}, \{ \{ |N''_1| \}_{K_C^-}, N''_1 \}_{K_{B_1}^-}, \{ \{ |T_1, X_1, L_1, \{ C \}_{K_V^+}| \}_{K_{B_1}^-} \}_{K_V^+}, \dots, \{ \{ |N''_n| \}_{K_C^-}, N''_n \}_{K_{B_n}^-}, \{ \{ |T_n, X_n, L_n, \{ C \}_{K_V^+}| \}_{K_{B_n}^-} \}_{K_V^+}$



# Then there's...

---

- Introduction
- System Outline
- The Protocol
- ***Analysis***
- Conclusion



# Cost analysis

---

- Data costs incurred
  - Signatures & encryption
  - Extra nonces & variables
- Time costs incurred
  - Computation of signatures & encryption
  - Additional data transmission
- Extension 2 offers best compromise



# Formal analysis

---

- Confirms security of protocol
- How is it accomplished?
  - Casper model -> CSP script -> FDR check
- One model per extension
- Specifications represent security properties



# And finally...

---

- Introduction
- System Outline
- The Protocol
- Analysis
- ***Conclusion***



# Future work

---

- Effects of malicious/collaborating devices
- Number of Proof Providers required to provide a reliable verdict



# Conclusions

---

- Evidence-based approach to location verification
- Doesn't require trusted agents
- SLVPGP secures gathering of location evidence ("proof")
- Incremental levels of security provided through protocol extensions
- Provable security- model checked