Introduction

Security in Internet routing protocols:
- Border Gateway Protocol (BGP)
- Vulnerable to attacks

Secure variants:
- Secure extensions:
  - E.g. S-BGP, so-BGP
- Clean-slate redesigns:
  - E.g. SCION, ICING

Lack of formal verification:
- Secure guarantees are informally proved
- Existing formal tools (e.g. cryptographic protocol verifier) have difficulty specifying and proving security properties
- Routing protocols run in arbitrary topology
- Recursive security property is hard to specify

Solution

Our solution: A unified formal framework
- Combine the development and verification of new secure Internet protocols
  - Developer of Internet routing protocol writes specification in declarative language.
  - Specification can be used for both formal verification and performance evaluation.

Framework comprising two main components:
- A declarative language, SeNDLog, as specification language
- Integrated compiler translates SeNDLog program into:
  - Imperative code for implementation and evaluation (C++)
  - Proof obligation for verification (Coq)

SeNDLog: Logic programming for routing protocols:
- Tuples: Network configuration & events
- Rules: Derivation of tuples
- User-defined functions:
  - E.g. f_head(p), f_concat(p,q)

Security mechanism:
- Encryption extensions:
  - Symmetric and asymmetric encryption
- Message authentication code (MAC)

SeNDLog program is fed to both code generator and verification condition generator, which in turn produce imperative program for performance evaluation and proof obligation for formal verification respectively.

Case Study

Protocols analyzed:
- Secure-BGP (S-BGP): Secure extension of BGP protocol
- SCION: Clean-slate redesign of routing infrastructure

Encoding is compact:
- S-BGP: 6 SeNDLog rules
  - Route initialization: Advertisement generation and sending
  - Route authentication: Signature generation and verification
- SCION: 28 SeNDLog rules
  - Path construction: Beacon receiving and processing
  - Data forwarding: Packet receiving and forwarding

Property verified:
- Route authenticity: Accepted path does exist
  - S-BGP: GoodPath(p); p = n'nA:n''A:g A link n n'A A link n n''A GoodPath(n'm'->p')
  - SCION: GoodInterface(lf); lf = lf':n'"A:"eeg":m'::eeg::m'
  - A provider n n'A A customer n n''A
  - A GoodInterface(lf':n'm'->"eeg":m')

This work is supported by NSF grants CNS-1117052