SPV: Secure Path Vector Routing for Securing BGP

By Yih-Chun Hu, Adrian Perrig, and Marvin Sirbu

Presented by Sam Small
For the JHU CS Systems Seminar
August 11th, 2004
The Problem

• BGP was designed for a trusted environment and provides relatively minimal security against attackers and misconfigurations

• As such, the potential for severe Internet routing disruption exists

• The network and security research communities have been actively pursuing ways to mitigate these potential disruptions
Properties of a more robust inter-domain routing protocol

- Provides benefits in incremental deployment
- Changes to existing router code should be minimized
- Is interoperable with legacy BGP routers
- Has some form of authentication hierarchy which is computationally efficient
BGP Security Threats

- BGP Updates
- Falsification
- Blackhole
- Grayhole
- Truncation
- Modification
- DoS Attacks
Related Work

- Hop-by-Hop Authentication
- Securing BGP Updates
- Anomaly Detection
Secure Path Vector (SPV)

- The goal is to achieve ASPATH integrity through purely symmetric functions
- attacker cannot shorten ASPATH
- attacker cannot change ASNs in ASPATH
- Removes need for routers to perform computationally complex public-key crypto
SPV Architecture

- Time is divided into epochs in order to prevent replay attacks

- Keys used:
  - Single-ASN public key
  - Epoch public key
  - Multi-epoch public key
  - Prefix public/private key
Cryptographic Mechanisms

• One-way hash chains
• Tree-authenticated values (Merkle hash trees)
• One-time signatures
Figure 1: Tree authenticated values
ASPATH Protector

- Meets both SPV ASPATH goals (from previous slide)
- The intuition is to use a one-time signature scheme to sign each suffix of the ASPATH
  - One-time signatures achieve ASPATH integrity
  - Hash trees enable authentication and verification of one-time signatures
  - One-way hash chains reduce size of the ASPATH protector
Integration with BGP

- Aggregation
- Securing Route Withdrawals
- Expiration
Evaluation

• SPV prevents falsely aggregating or deaggregating and falsely originating a route to a prefix

• Other attack probabilities are extremely low and are discretely fixed to epochs

• SPV provides more flexibility in incremental deployment than S-BGP

• Network overhead is almost 3 times that of S-BGP
Figure 7: CPU Utilization
Summary

- Provides security by limiting the number of options attackers have and using symmetric crypto rather than heavy-weight asymmetric cryptography
- SPV is faster than S-BGP and performs better in periods of high BGP traffic
- SPV can use a shorter epoch period than S-BGP and is more flexible in deployment