A Survey of BGP Security Issues and Solutions

Rohan Tabish, Josh Eckhardt, Joseph Gonzalez

Presentation Outline

- ❖ INTRODUCTION
- ❖ MOTIVATION
- ❖ BORDER GATEWAY PROTOCOL SECURITY PROBLEMS
- ❖ BGP SECURITY TODAY
- ❖ BGP SECURITY SOLUTIONS
- ❖ FUTURE DIRECTIONS IN BGP SECURITY RESEARCH
- ❖ CONCLUSION

Introduction

- **BGP related Security Incidents**
  - A misconfigured router in Florida (1997) became a black hole.
  - Turkey TTNet 2004.
  - Con-Edision 2006.
  - Pakistan Telecom hid YouTube (2008).
- The **Border Gateway Protocol** (BGP) controls much of Internet traffic, but is **vulnerable** to **communications interruptions** and **failures**; finding suitable improved security measures with acceptable costs is difficult.

MOTIVATION

- **Why securing BGP is important?**
  - Many applications such as Online banking, ubiquitous healthcare and stock trading etc depend upon BGP.
  - BGP security is important from homeland security
  - Neighbours cannot always be trusted.

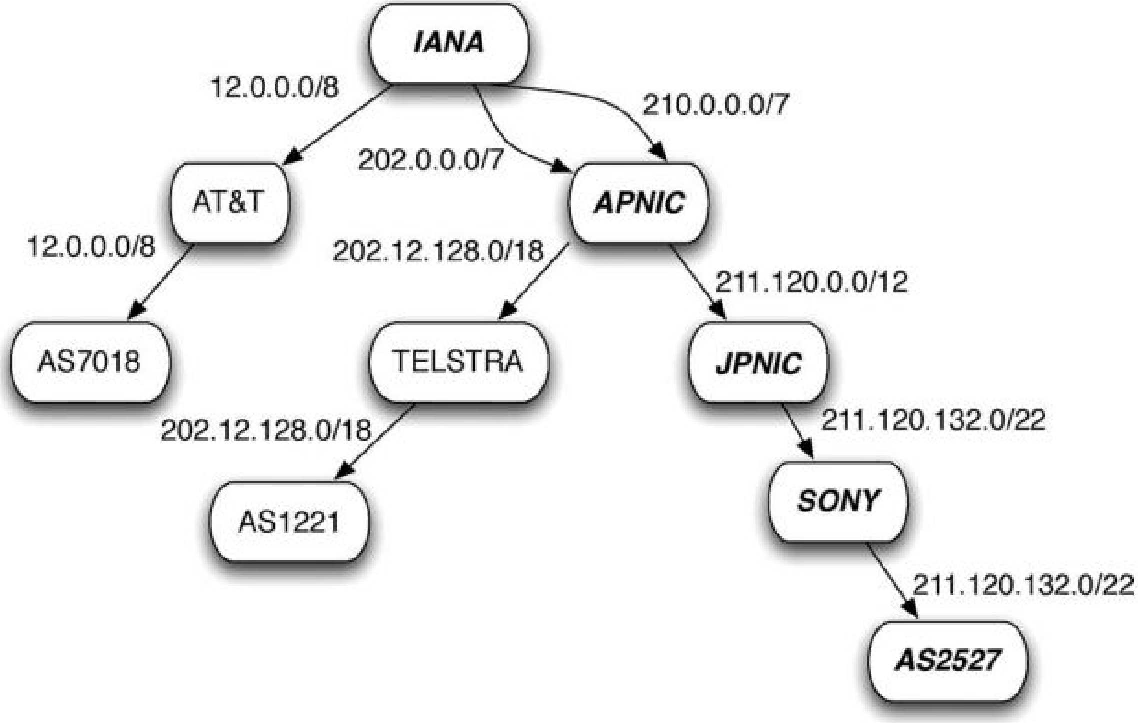
BORDER GATEWAY PROTOCOL Security Problems (BGP SP)

- ➔ IP Prefixes and AS Numbers
- ➔ Using TCP as the Transport Protocol
- ➔ Routing Policy and BGP Route Attributes

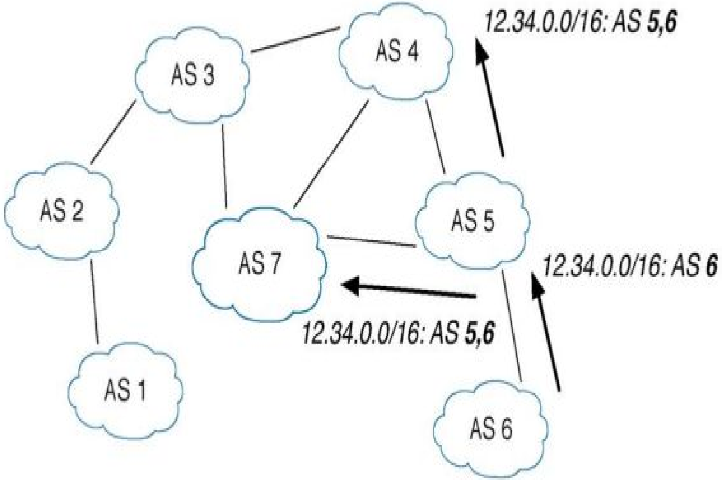
BGP SP - IP Prefixes and AS Numbers

- Addresses are assigned in a hierarchical manner
  - Internet Assigned Numbers Authority (IANA)gets assigned to regional authorities, then national authorities and then ISP’s.
  - Each entity gets address block represented as IP.
  - Autonomous System Numbers (ASN) from IANA.
  - BGP paths are represented in the form of ASNs to the prefix.

BGP SP- IP Prefixes and AS Numbers- IP Address Delegation

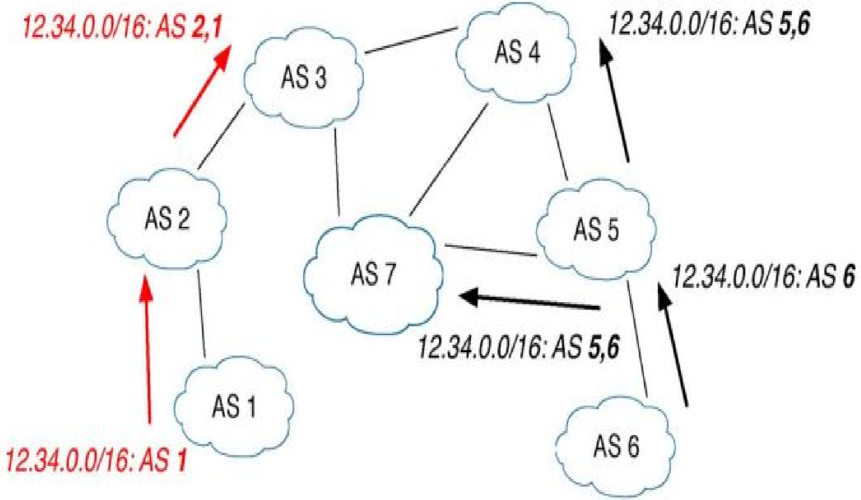


BGP SP - IP Prefixes and AS Numbers- Normal Vs Malicious Organization



(a)

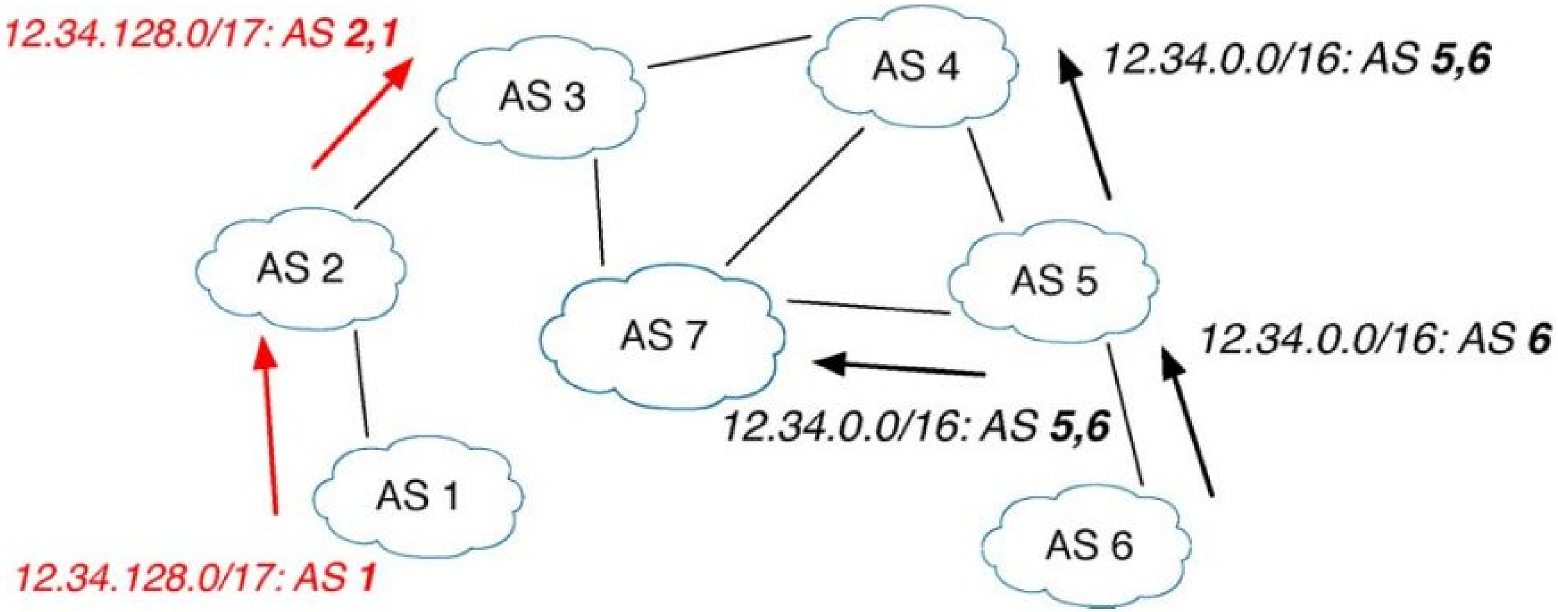
Normal Organization



(b)

Malicious Organization

BGP SP - IP Prefixes and AS Numbers- Deaggregation example



BGP SP - Using TCP as the Transport Protocol

- BGP routers rely on TCP for communication.
- Communication is susceptible to different attacks.
- Attacks against confidentiality
  - Third Parties can eavesdrop BGP communication
- Attacks against message integrity
  - Various man in the middle attacks
  - Replay attacks, Forged and Reset attacks
- Denial-of-service attack
  - Link-Cutting to force use of other paths
  - SYN flooding attack

BGP SP- Routing Policy and BGP Route Attributes

- ❖ Important BGP route attributes include:
  - ➢ Local preference, AS path length, Origin type and Multi-Exit Discriminator (MED).

- ❖ An adversary could manipulate BGP route attribute by:
  - ➢ Shortening or Lengthen the AS path
  - ➢ By changing MED value to influence neighbour decisions

BGP Security Today - Cryptographic Techniques

- Pairwise Keying
  - Complexity of key management is O(n^2)
  - Key replacement is required, if not replaced might lead to cryptanalysis attack
- Cryptographic Hash Functions
  - Uses Hash functions such as MD5 and SHA-1
  - Requires Shared key
- Message Authentication Codes (MAC)
  - MAC generated using HMAC
  - MAC are appended to the message that provides security by guaranteeing integrity of message and authenticity.

BGP SECURITY TODAY - Cryptographic techniques

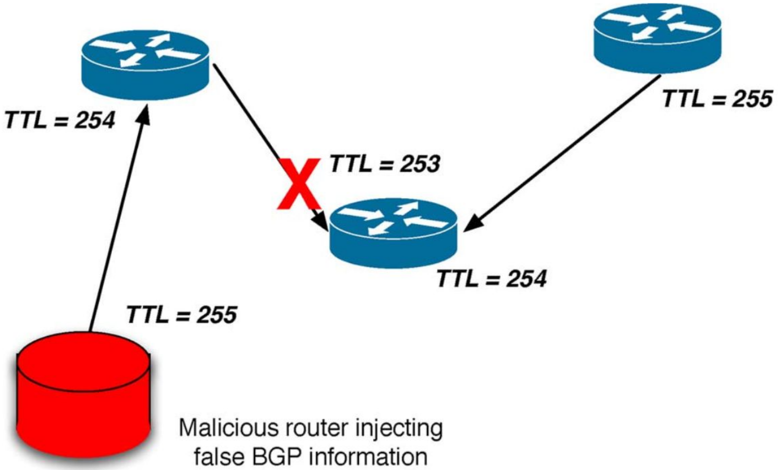
- Diffie-Hellman Key Negotiation
  - Allows anonymous hosts to share secret key.
- Public Key Infrastructure
  - One public/private key pair per AS
  - Public key needs to be distributed
  - Relies on Hierarchical infrastructure
- Public Key Cryptographic Primitives
  - Encryption with public key decryption with private key
- Certificates and Attestations
  - Allows building chain of interests
  - Requires public key infrastructure

BGP SECURITY TODAY - SESSION PROTECTION

- MD5 Integrity
  - Include MD5 keyed digest of the TCP header and BGP data in packets between two routers
- Session and Message Protection Countermeasures
  - Encryption of all BGP data in control messages between peers, digital signing of fields in UPDATE messages, and new fields in UPDATE messages (SEQUENCE# and PREDESSOR)
- Hop Integrity Protocols
  - Sequence numbers and MACs to detect any modification or replay of exchanged information

BGP Security Today - Session Protection

- Generalized TTL Security Mechanism
  - Drop packets with time-to-live (TTL) decremented by more than one - i.e. only accept packets from direct neighbors
  - Drop threshold can be modified for specific cases
  - Easily evaded by sophisticated attackers



BGP Security Today - Session Protection

- IPsec
  - Suite of protocols implementing security at a lower layer
  - Not BGP-specific
  - Long-term key management
  - Encryption, authentication, and integrity checking of headers and payload

BGP Security Today - Session Protection

Summary:

	Integrity	Confidentiality	Replay Prevention	DOS Prevention
MD5 Integrity [28]	yes	no	yes	no
Countermeasures [33]	yes	yes	yes	no
HOP Protocol [34]	yes	no	yes	no
GTSM [35]	no	no	no	no
IPsec (AH) [39]	yes	no	yes	yes
IPsec (ESP) [40]	yes	yes*	yes	yes

BGP Security Today - Filtering

- Currently filter innocuous artifacts
  - Documented Special Use Addresses (DSUAs), like loopback addresses or link-local
  - Bogons/martians, advertisements of address blocks and ASes with no other available data
- Occasionally extended to provide more security
  - Filter/rewrite BGP attributes incorrectly modified by neighbors
  - Enforce single-value origin-type attributes
  - Fundamentally limited by heuristics, and ineffective against subtle/sophisticated attacks

BGP Security Today - Routing Registries

- Shared, global view of “correct” routing information
- Contains prefix ownership, AS-level connectivity, and routing policies
- ASes insert their policy and topological information into registry, which is queried by other ASes
- Registry must be secured in order to be trusted
    - Authentication/authorization model for providing integrity
- Some AS owners consider this information proprietary/sensitive
- Information quality tends to deteriorate over time

BGP Security Today - Router Management

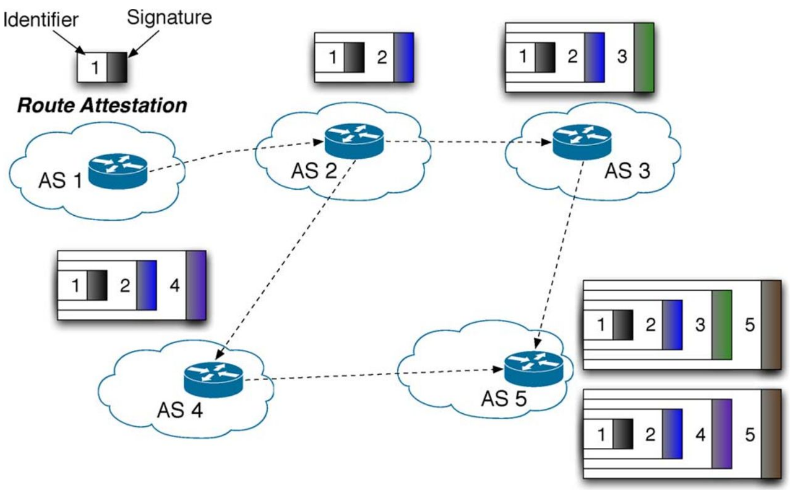
- Because BGP lies atop TCP, which is dependent on lower OSI layers, an attack on lower layers can disrupt BGP
  - Link cutting
  - Flooding links with traffic (DoS)
  - Accessing management interfaces of routers and disabling interfaces, etc.
- Physical security - physical access to devices must be approved and monitored
- Simple Network Management Protocol (SNMP) settings must be secured to prevent rogue remote access
- Robust network infrastructure, e.g. redundancy
- Internal use of protocols preserving message integrity

BGP SECURITY SOLUTIONS - BGP SECURITY ARCHITECTURES

- Secure BGP (S-BGP)
  - First comprehensive routing security solution for BGP
  - Validates path attributes in BGP UPDATE messages with digital signatures and associated public key certificates
  - PKI binds ASes to organizations and organizations to routers via certificates
  - All exchanged information is validated using certificates - this much validation, despite providing definitive authentication, is computationally expensive
  - Provides most comprehensive security guarantees, but high computational requirements are a barrier to widespread adoption

BGP SECURITY SOLUTIONS - BGP SECURITY ARCHITECTURES

- Secure BGP (S-BGP) (continued)
  - Address attestations - digitally signed claims that an AS can originate a prefix; distributed out-of-band
  - Route attestations - nested signatures of path in BGP UPDATEs:

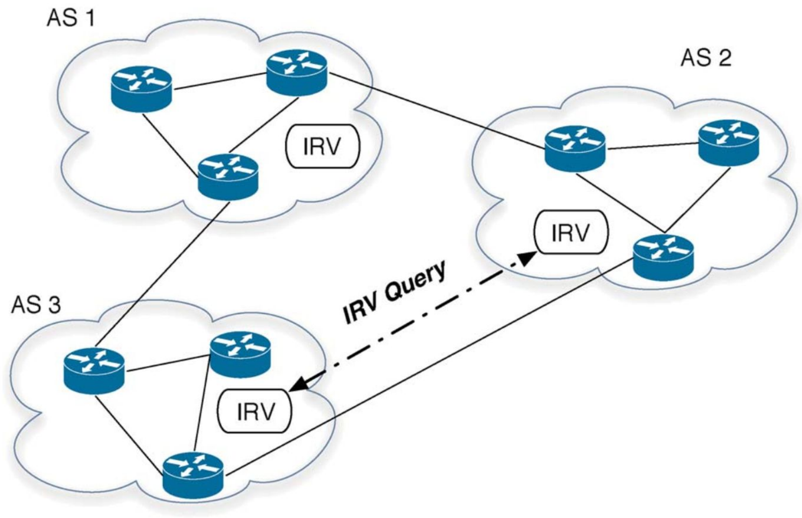


BGP Security Solutions - BGP Security Architectures

- Secure Origin BGP (soBGP)
  - PKI to authenticate/authorized entities and organizations is similar to S-BGP
  - Security information is transmitted in-band via a new SECURITY message type
  - Each AS signs and distributes peers to form a global, distributed database of network topology
  - Routers use topology database to validate routes
  - Topology graph is mostly static, changes rarely (only when new policy certificate is issued)
  - Cannot detect “plausible” forged paths that are consistent with topology graph

BGP SECURITY SOLUTIONS - BGP SECURITY ARCHITECTURES

- Interdomain Route Validation (IRV)
  - Least centralized comprehensive security solution for BGP
  - Each AS contains an IRV server to check UPDATE message data
  - IRV servers verify information by directly querying IRV servers in other ASes
  - IRV queries secured by IPsec or TLS
  - Needs a functioning network to be useful, vulnerable to outages



BGP SECURITY SOLUTIONS - EXPERIMENTAL SYSTEMS

- Reducing Computational Overhead
  - Origin Authentication (OA) can validate address ownership - previously too costly too be feasible. Recently discovered that it can be efficiently implemented using techniques from Merkle hash trees
  - Modification using symmetric key variant (much faster) of asymmetric recursive signatures in S-BGP. Uses MACs instead of digital signatures
  - Secure Path Vector protocol (SPV) uses a single off-line signature to generate many signatures. Signatures forwarded to next hop(s) for validation of one-time signatures. Computationally cheap but expensive in memory

BGP SECURITY SOLUTIONS - EXPERIMENTAL SYSTEMS

- Reducing Computational Overhead (continued)
  - Signature amortization - BGP UPDATE messages require only one signature for the group. Aggregates UPDATE messages in Merkle hash tree for collective signing
  - Alternate method of signature amortization using reference locality - uses other cryptographic constructions for path authentication that make use of the fact that paths are stable and new paths appear slowly
- Alternatives to PKI
  - IRDP protocol - an interdomain routing path vector protocol that is a superset of BGP and EGP. Encrypted checksums sent with routing messages provide authentication. Rendered obsolete by advances in cryptographic efficiency

BGP SECURITY SOLUTIONS - EXPERIMENTAL SYSTEMS

- Alternatives to PKI (continued)
    - Pretty Secure BGP (psBGP) - uses decentralized origin authentication
        - Each AS uses maintains prefix assertion list (PAL) of local ASes and peers, and origin claims are checked by comparing PALs of peers
        - Vulnerable to collusion and requires centralized PKI
        - Path authentication with S-BGP signatures
- Detecting and Mitigating Anomalies
    - MOAS conflict occurs when a prefix is originated by multiple ASes - can happen naturally but frequently seen in attacks

BGP SECURITY SOLUTIONS - EXPERIMENTAL SYSTEMS

- Detecting and Mitigating Anomalies (continued)
  - Proposed BGP enhancement uses community attributes (lists of ASes authorized to announce prefixes) to determine if a MOAS conflict is valid
  - Intrusion detection techniques to identify forged origin announcements - uses historical associations between prefixes and ASes to build a “normal” representation of net. Deviations from this are flagged as malicious; subject to false positives
  - Prefix Hijacking Alert System (PHAS) - centralized server keeps list of prefix owners. Changes to route originators cause a check with prefix owners. Single point of failure, vulnerable to false registrations

BGP SECURITY SOLUTIONS - EXPERIMENTAL SYSTEMS

- Detecting and Mitigating Anomalies (continued)
  - Pretty Good BGP (PGBGP; distinct from psBGP) - distributed state of “normal” routes inferred from historical data. New routes are considered suspicious and are avoided until no more trusted routes are available
  - Build fingerprints of prefixes from various pieces of information. When a conflicting origin AS is advertised, compare collected fingerprints against probes sent to all advertised origins and choose closest match
  - Whisper protocol validate initial source of path information. Random value assigned to each prefix and at each hop that value is repeatedly hashed. Receiving routers compare hash values to see if they came from the same source

BGP SECURITY SOLUTIONS - CHALLENGES OF ADOPTION

- Scalability
  - Additional data in secure protocols
  - Additional computational requirements of secure protocols places greater strain on currently deployed routers. Cost for upgrades may be prohibitive or outright infeasible

FUTURE DIRECTIONS IN BGP SECURITY RESEARCH

- Routing Frameworks and Policies
  - Work towards a routing infrastructure that remains scaleable in spite of additional overhead from security assurances
- Attack Detection
  - Detect attacks or inconsistencies in routings and adapt
- Data Plane Protection
  - Current solutions protect control plane (messages like path announcement/withdrawal)
  - Need efficient solution to protect data plane (detect ASes who forward along paths not on announced on control plane)
- Partial Deployment
  - Deploying secure BGP to all ASes at once is infeasible
  - Need secure BGP solutions that remain effective over incremental deployment

How Secure Are Secure Interdomain Routing Protocols?

(2nd paper) - High level summary

- From weakest to strongest: origin authentication, soBGP, S-BGP, data-plane verification
- S-BGP and data-plane verification only marginally outperform soBGP but have high computational costs
- Defensive filtering of paths from stub ASes is simple yet highly effective
- Most security solutions only solve half the problem - they can restrict the path a manipulator chooses to announce but cannot restrict his export policies

Questions?