ΟΙΚΟΝΟΜΙΚΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΑΘΗΝΩΝ

ATHENS UNIVERSITY
OF ECONOMICS
AND BUSINESS

Information-Centric Networks

Section # 4.3: Routing Issues

Instructor: George Xylomenos

Department: Informatics

European Union
European Social Fund

OPERATIONAL PROGRAMME
EDUCATION AND LIFELONG LEARNING
investing in knowledge society
MINISTRY OF EDUCATION, LIFELONG LEARNING AND RELIGIOUS AFFAIRS
MANAGING AUTHORITY
Co- financed by Greece and the European Union

NSRF
2007-2013
programme for development
EUROPEAN SOCIAL FUND

Funding

- These educational materials have been developed as part of the instructors educational tasks.
- The **"Athens University of Economics and Business Open Courses"** project only funded the reformatting of these educational materials.
- The project is being implemented as part of the Operational Program "Instruction and Lifelong Learning" and is co-financed by the European Union (European Social Fund) and national funds.

European Union
European Social Fund

OPERATIONAL PROGRAMME
EDUCATION AND LIFELONG LEARNING
investing in knowledge society
MINISTRY OF EDUCATION, LIFELONG LEARNING AND RELIGIOUS AFFAIRS
MANAGING AUTHORITY

NSRF
2007-2013
programme for development
EUROPEAN SOCIAL FUND

Co- financed by Greece and the European Union

Licencing

Week 4 / Paper 3

- A Survey of BGP Security Issues and Solutions
  - Kevin Butler, Toni Farley, Patrick McDaniel, and Jennifer Rexford
  - Proceedings of the IEEE, 98(1):100--122, January 2010
- Main point
  - BGP is the glue that holds the Internet together
  - It is however highly vulnerable
  - It does not adequately address security
  - Review of proposed improvements

Introduction

- Serious security incidents
  - A misconfigured router in Florida became a black hole
    - It advertised incorrect routes (too good)
    - But nobody validates these routes
  - Pakistan Telecom hid YouTube
    - Attempt to close access to local customers
  - Spammers introduce fake prefixes
    - Avoid spam registries by exploiting unused addresses
  - Snoopers introduce fake routes to snoop on traffic
- Operational and security concerns
  - Interrelated to a high degree
- Survey of current practice and research

IP prefixes and AS numbers

- Addresses are assigned hierarchically
  - IANA to regional authorities, then national authorities, then ISPs
  - Each gets and address block represented as IP/prefix
    - Each block is the allocated further down
    - Longer prefixes indicate smaller address blocks
  - Autonomous System Numbers from IANA
    - Each network has one or more public ASNs
    - Networks with a single upstream provider can have a private ASN
  - BGP paths are expressed in terms of ASNs to a prefix
    - But there is no foolproof way to check the validity of either
    - Announcing prefixes you do not have is prefix hijacking
      - Black holes: data ends up nowhere (maybe just a mistake)
      - Impersonation: the hijacker pretends to offer services
      - Interception: the hijacker inspects traffic

Using TCP as the transport protocol

- BGP routers communicate via TCP
  - No need to deal with error, flow and congestion control
    - But TCP in itself is quite insecure
  - Attacks against confidentiality
    - Eavesdropping on multi hop connections
  - Attacks against message integrity
    - Various types of man in the middle attacks
    - Message replays, forged messages, resets
  - Denial of service attacks
    - More feasible from off path intruders
    - Link cutting to force use of alternative paths

Routing policy & route attributes

- BGP employs route attributes to enforce policy routing
  - Local preference: select routes inside an AS
  - AS path length: prepending an AS number inflates route length
  - Origin type: routes learned from within the AS are preferred
  - Multi-exit discriminator: select one of many connections
  - Route filtering also allows complex policies to be enforced
    - Which routes are propagated and which are not
  - The problem is that advertised routes may be fake!
    - A route may be truncated to become more attractive
    - A route may be extended to seem valid
    - A route may be edited to hide undesirable ASes

Cryptographic techniques for BGP

- Basic security limitation: the system is decentralized
  - Localized solutions are far more practical
- Cryptographic techniques applicable to BGP
  - Pairwise keying: relies on shared secret keys
  - Cryptographic hash functions: to produce digests
  - Message authentication codes: to verify signed digests
  - Diffie-Hellman key negotiation: jointly select secret keys
  - Public key infrastructure: allows public key cryptography
  - Public key cryptography: simplifies authentication
  - Certificates and attestations: allows building chains of trust

Protecting BGP sessions

- Integrity protection: use of MACs for sensitive data
  - MD5 or arbitrary digests and digital signatures
- Session and message protection
  - Encryption and numbering of BGP messages
- Hop integrity protocols
- Generalized TTL security mechanism (GTSM)
  - Drops packets with TTL lower than expected
  - Limited protection for a limited surrounding area
- IPsec: lower level session encryption
  - Extensively used for VPNs, therefore widely available

Defensive filtering

- Filtering rules for suspicious routes
  - Using special address prefixes or private AS numbers
    - These should never exit an AS
  - Using unallocated prefixes
    - Requires a service that knows what is allocated
  - More aggressive filtering for customers
    - You know what to expect from a customer
  - Rewriting rules for malformed routes
  - Good practice but inherently limited
    - Can only catch obvious errors

Routing registries

- A global view of routing would prevent many attacks
  - An accurate routing registry would be invaluable
    - Prefix ownership, AS-level connectivity, routing policies
  - But ASes do not want to expose their policies
  - And the registry is also a target for attacks
- Unfortunately even address registrars are inaccurate
  - Registries allocate addresses to networks
  - But address delegations change and are not updated
- Many approaches also require a PKI
  - Essentially a registry for public keys
  - Also for certificate revocation lists

Securing router management

- The BGP router interface has to resist attacks
  - Gaining access to the CLI allows lots of attacks
  - Physical and network security required
  - Management interfaces need to be secured
  - Only secure management connections should be allowed
  - Physical redundancy to guard against DoS attacks
  - General security hardening is even more important for BGP
    - Bringing down router connections allows more attacks

BGP security solution issues

- Implementing security solutions is a scalability issue
  - 40000 AS numbers have been allocated to regional registries
  - 35000 have been allocated to institutions
  - 32000 are being routed
  - Advertised routing prefixes increase continuously
- Many security solutions exist
  - Some have been implemented, some proposed
  - But they are not widely deployed and accepted
- Routing registries
  - Too much information to keep accurate
- Computational complexity
  - Overload of BGP servers due to cryptography

End of Section # 4.3

Course: Information-Centric Networks, **Section # 4.3: Routing Issues**

Instructor: George Xylomenos, **Department:** Informatics

European Union
European Social Fund

OPERATIONAL PROGRAMME
EDUCATION AND LIFELONG LEARNING
investing in knowledge society
MINISTRY OF EDUCATION, LIFELONG LEARNING AND RELIGIOUS AFFAIRS
MANAGING AUTHORITY

Co- financed by Greece and the European Union

NSRF
2007-2013
programme for development
EUROPEAN SOCIAL FUND