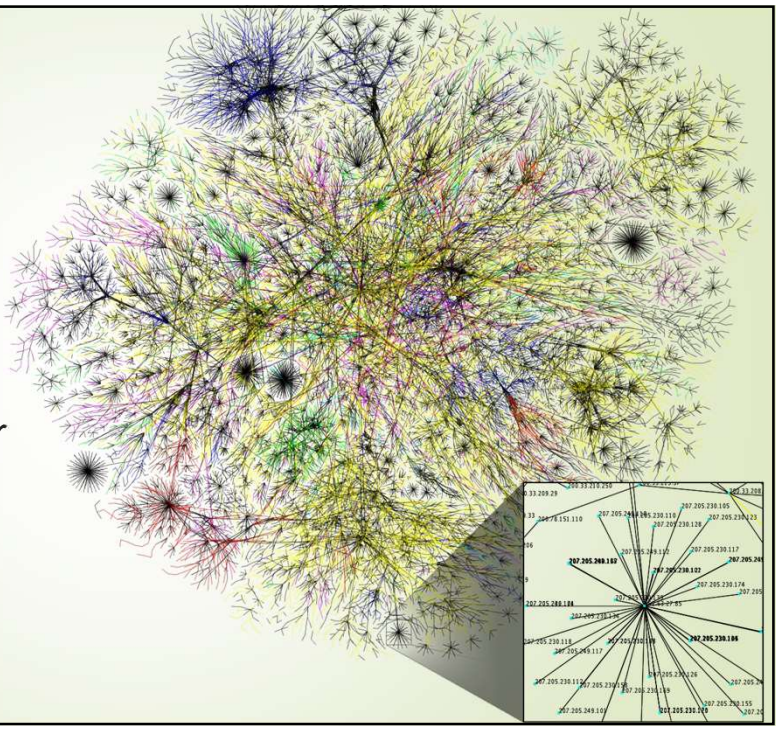
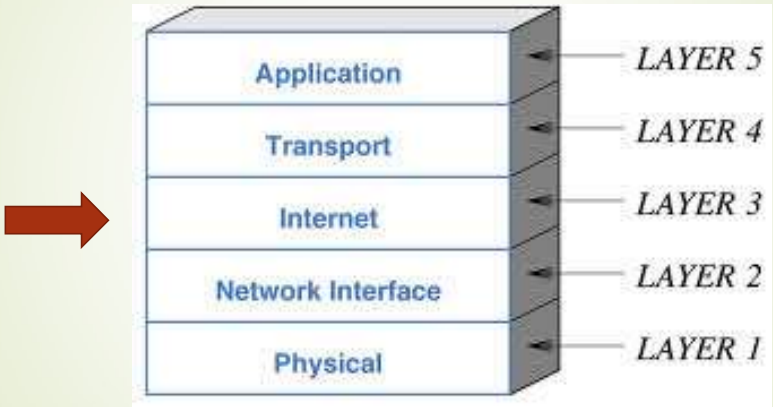


Network Layer Security

Mohammad Sayad
University of Tehran

Extended TCP/IP Protocol Stack



Agenda

- A short review of IPSec
- Routing Security
  - BGP
  - S-BGP
  - …
- Anonymous Routing

Facts حقایق

- Internet Protocol (IP) is not secure
  - It is an old protocol designed in the early ages of the Internet where security was not important
- Security Issues
  - Source Spoofing امکان جعل آدرس فرستنده
  - Replay of Packets امکان ارسال مجدد بسته ها
  - No Data Integrity or Confidentiality عدم وجود مکانیزم تامین محرمانگی و دست نخوردگی

IPSec Facts

- IPSec sits next to (sometimes, on top of) IP layer and is Transparent to upper layers!
- IPsec provides Authentication, Confidentiality, Integrity
- IP security (IPsec) → both IPv4 and IPv6.
- Authentication makes use of HMAC
  - Either on the entire original IP packet (tunnel mode)
  - Or on the packet except for the IP header (transport mode).
- Confidentiality is provided by an encryption format known as encapsulating security payload (ESP).
- IKE (Internet Key Exchange) defines key management techniques.

An IPSec usage scenario

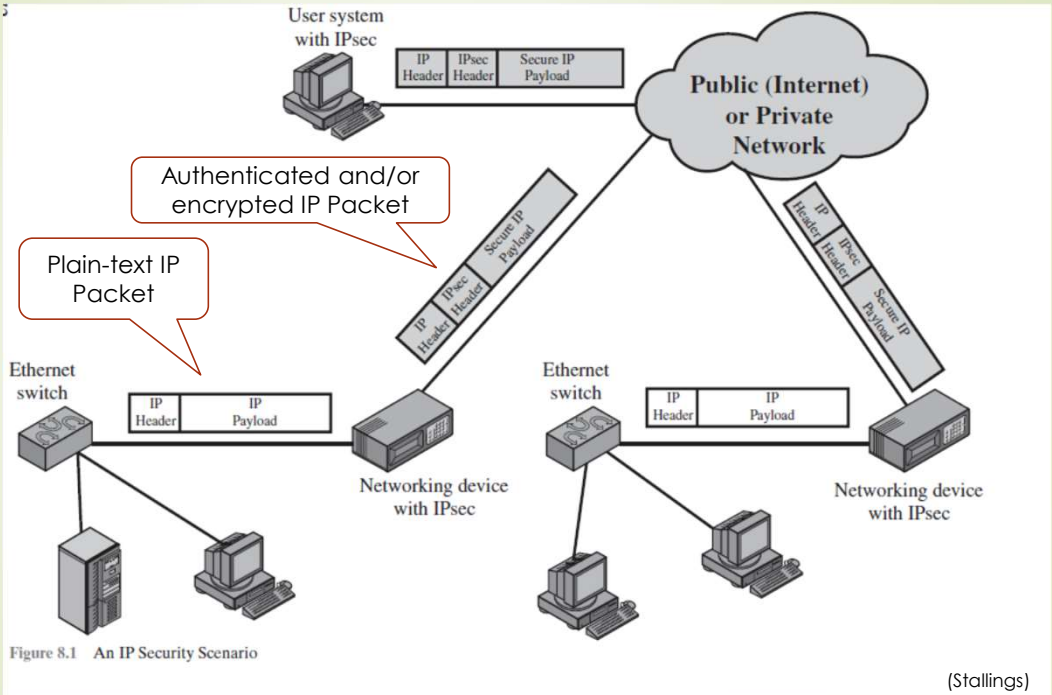


Figure 8.1 An IP Security Scenario

(Stallings)

IPSec Components

- Components of IPSec
  - Security Associations (SA)
    - It's a logical one-way connection providing a security service
    - SA can provide either AH or ESP
  - Authentication Headers (AH)
    - Provides authentication and integrity by adding a MAC.
  - Encapsulating Security Payload (ESP)
    - Provides confidentiality by encryption
  - Internet Key Exchange (IKE) <- ISAKMP/Oakley in IKEv1

IPSec Modes

IPSec can work in 2 modes

1. Transport Mode
   - Doesn't remove the main header. Adds its own header afterwards (in the payload) to provide security services.
     - Good for end-to-end connections

2. Tunnel Mode
   - Makes a new IP packet and puts the old one in the payload after its header.
     - Good for VPN

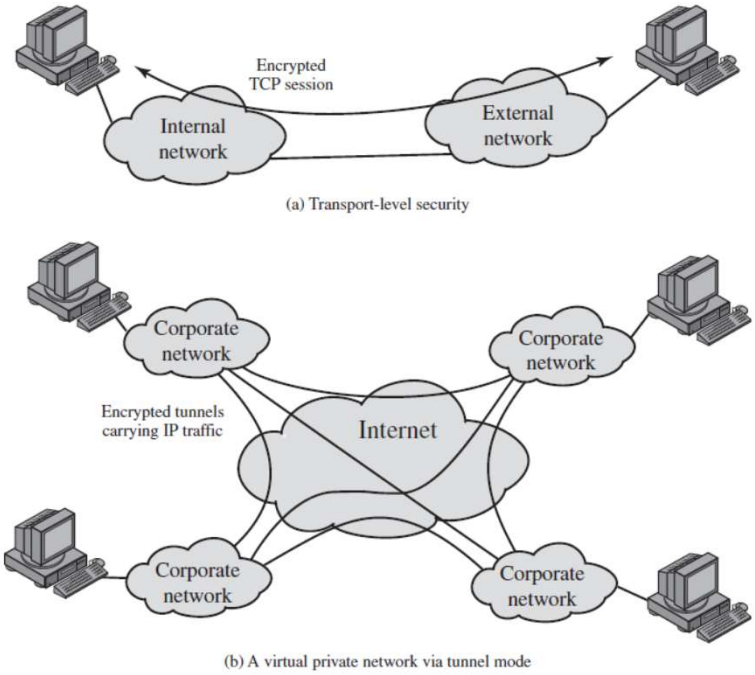
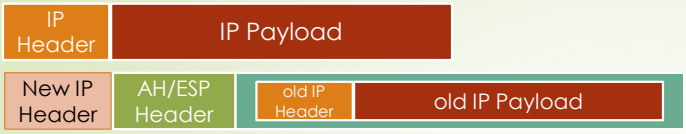


Figure 8.7 Transport-Mode versus Tunnel-Mode Encryption (Stallings)

Tunnel vs Transport

- ESP in Transport Mode: Encrypts the payload. It can optionally authenticate the payload too. But does not protect the IP header.
- AH In Transport Mode: Authenticates both the payload and the header (the parts that do not change).



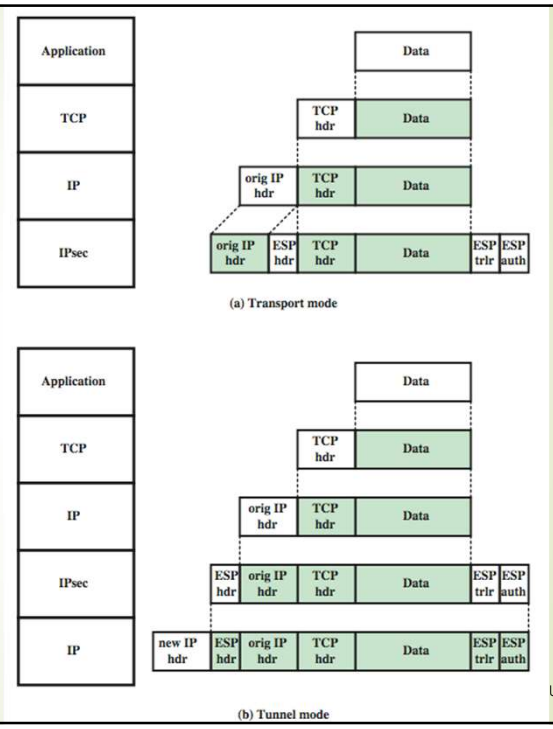
- ESP in Tunnel Mode: Encrypts the whole IP packet (incl. the header). It can optionally authenticate the payload.
- AH in Tunnel Mode: Authenticates the whole original IP packet plus the header of the newly generated packet (except the parts that might change).

Summary

	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers.	Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers.
ESP	Encrypts IP payload and any IPv6 extension headers following the ESP header.	Encrypts entire inner IP packet.
ESP with Authentication	Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header.	Encrypts entire inner IP packet. Authenticates inner IP packet.

Transport & Tunnel Mode

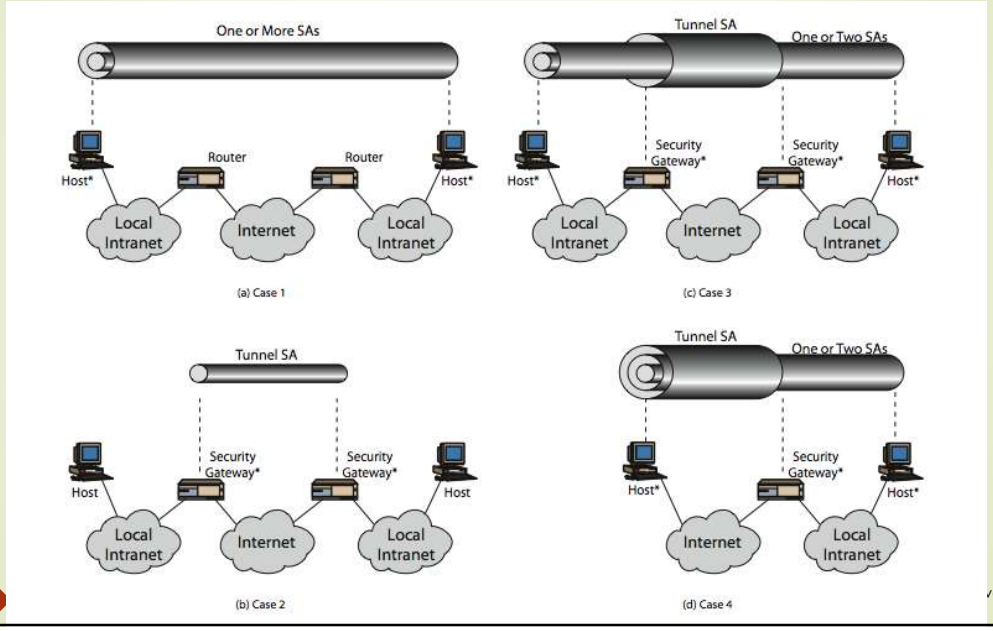
(Protocol Stack View)



ESP or AH? Which one?

- It depends on the service you want.
  - Source/Destination Address Authentication ? → AH
  - Payload Confidentiality? → ESP
- Want both?
  - No worries! You can combine SAs.
    - ESP + AH → confidentiality + integrity + authentication

Examples on how you can combine SAs



IPSec Architecture

Establish keys
E.g. by Oakley (Diffie-Hellman)

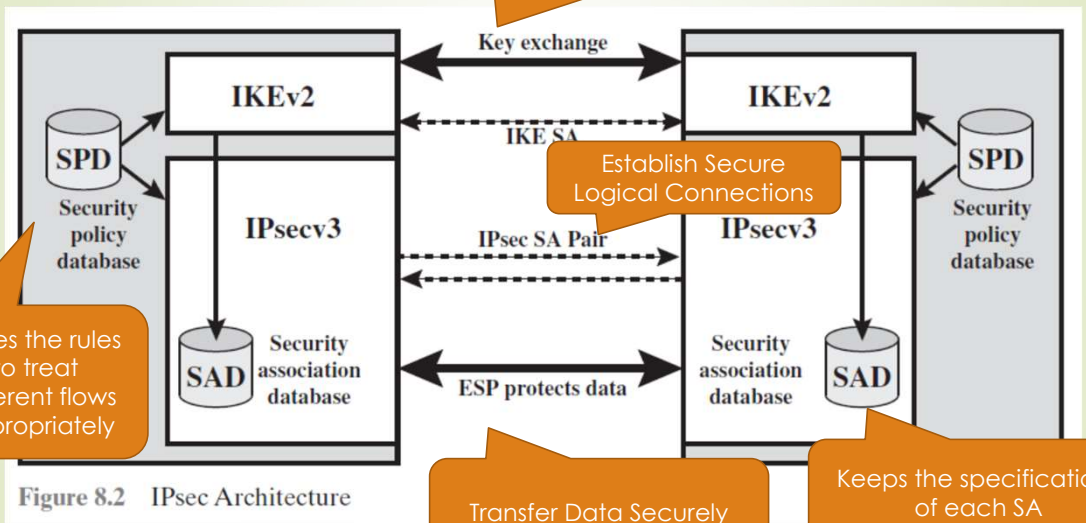


Figure 8.2 IPsec Architecture

Establish Secure Logical Connections

Stores the rules to treat different flows appropriately

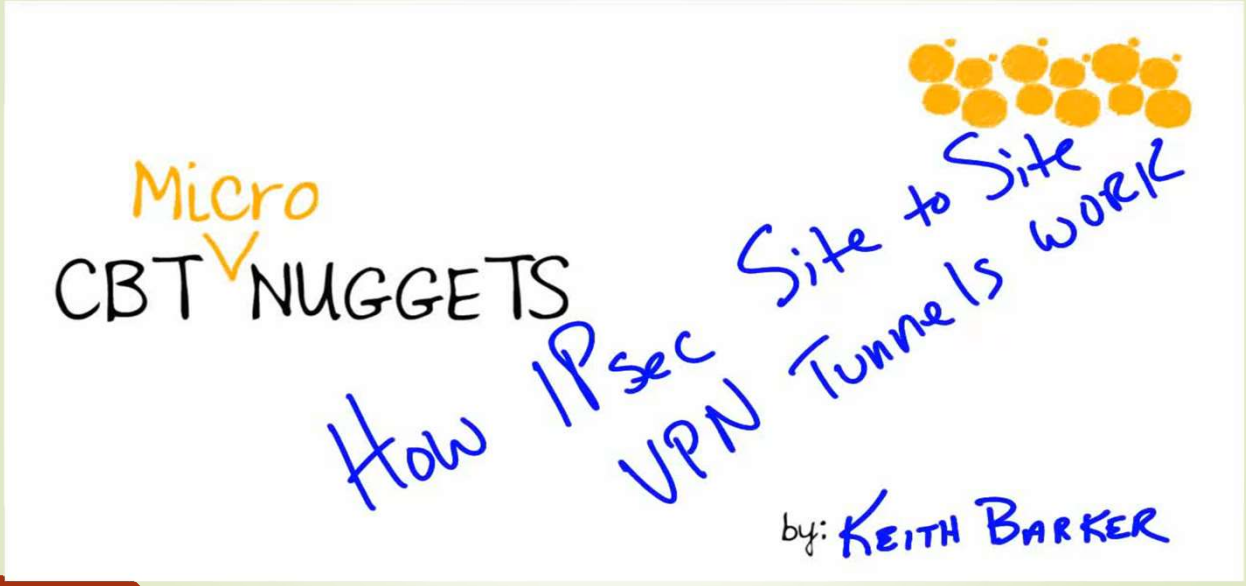
Transfer Data Securely

Keeps the specifications of each SA

VPN Technologies and their operation layer

OSI Layer	VPN Protocol
Application Layer 7	
Transport Layer 4	• Secure Sockets Layer (SSL) / Transport Layer Security (TLS)
Network Layer 3	• IP Security (IPSec)
Data Link Layer 2	• Point-to-Point-Tunneling Protocol (PPTP) • Layer 2 Tunneling Protocol (L2TP) • Multi Protocol Label Switching (MPLS)
Physical Layer 1	

A Practical Setup for an IPSec VPN (ESP in Tunnel Mode)



The end of IPSec

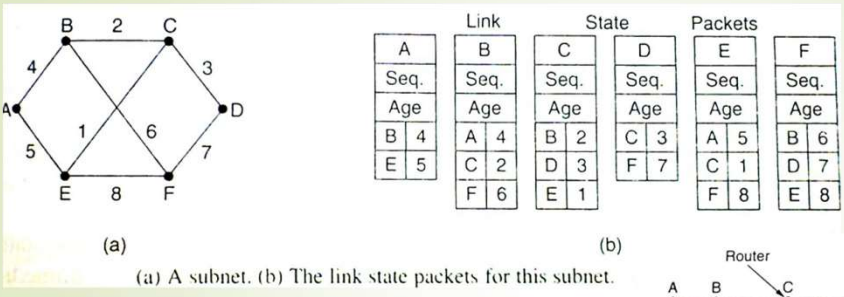
Interested readers are referred to the following reference:

"Network Security Essentials, Applications and Standards", William Stallings

(Secure) Routing

Basics of Routing

- We have different families of routing algorithms:
  1. **Distance Vector**
     - Each node has a routing table to other nodes/zones in the network and updates it once it receives information from tables of the others. → **BGP** (Border Gateway Protocol), **AODV**
  2. **Link-State**
     - Each node sends the cost to its neighbors as a table to everybody in the network. They must find the best route themselves. → **OSPF** (Open Shortest Path First)
  3. Flooding
  4. …

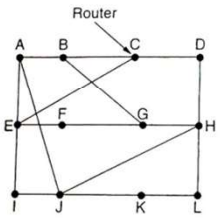


(a) A subnet. (b) The link state packets for this subnet.

You Remember these?

Link State

Distance Vector



To	A	I	H	K	New estimated delay from J	Line
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	–
K	24	22	22	0	6	K
L	29	33	9	9	15	K
	JA delay is 8	JI delay is 10	JH delay is 12	JK delay is 6		New routing table for J

Vectors received from J's four neighbors

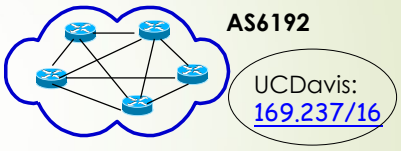
BGP Introduction

- **Border Gateway Protocol** (**BGP**) is a standardized exterior gateway protocol designed to exchange routing information among autonomous systems (AS).
  - BGP makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator and is involved in making core routing decisions.
  - BGP may be used for routing within an AS too. In that case it is referred to as the Interior Border Gateway Protocol (IBGP) in contrast to its normal application as Exterior Border Gateway Protocol (EBGP).

Definitions (AS and Subnet/Prefix)

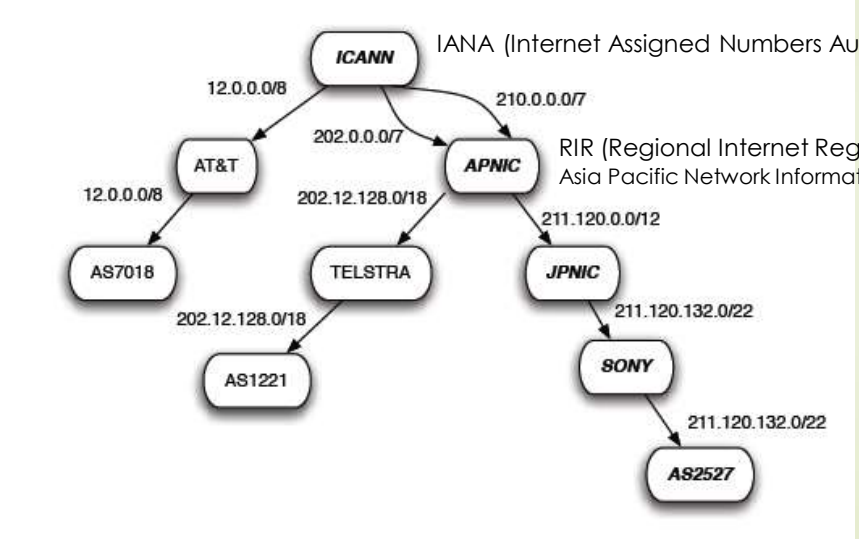
(Felix Wu, UC Davis)

- **Autonomous System (AS):**
  - A set of routers owned by one administrative domain
- Address Prefix:
  - Example:
    - AS6192 consists of routers in UC Davis
    - UC Davis owns 169.237/16



- How do I let the world know about 169.237/16?
  - I announce that I owned 169.237/16
- How does anybody in the Internet know how to send (or route) a IP packet to 169.237/16?

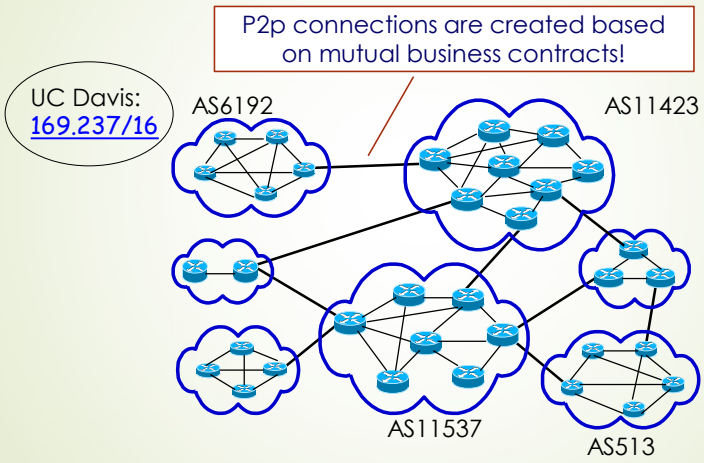
IP Address Delegation



(Kyle Super, 2011)

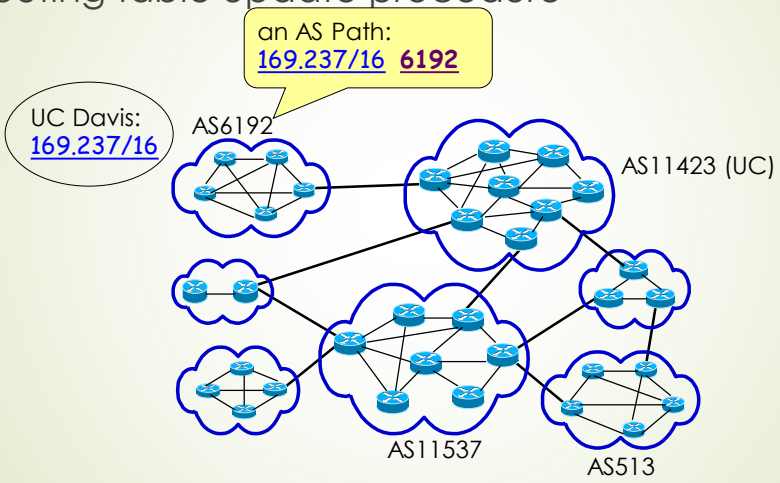
Internet Composition

- Internet is composed of many p2p connected ASs.



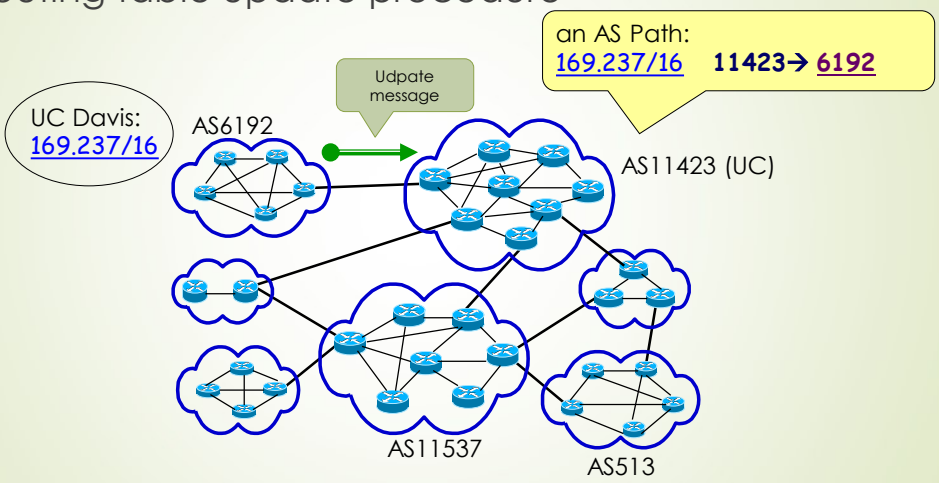
AS Path Advertisement

- BGP routing table update procedure



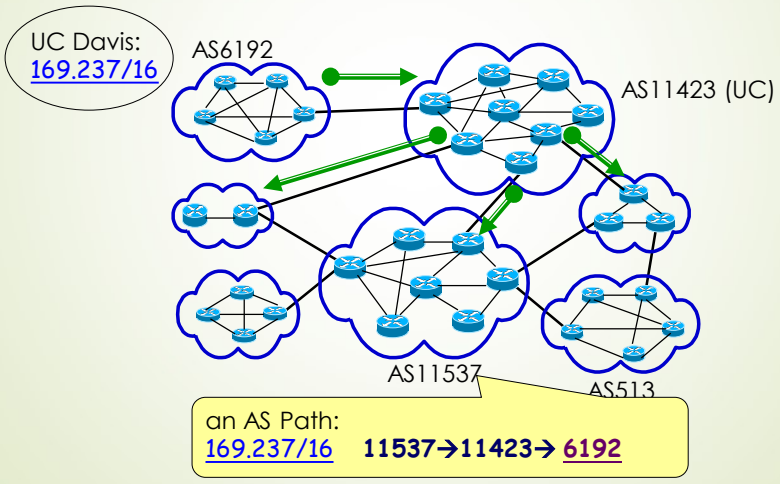
AS Path Advertisement

- BGP routing table update procedure



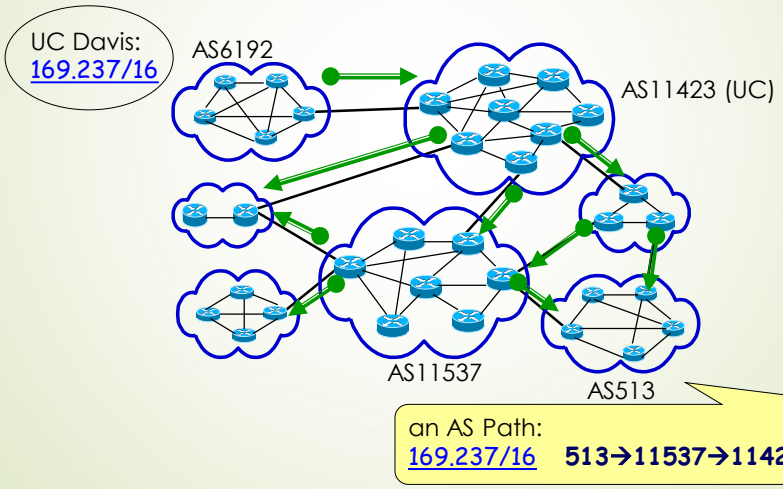
AS Path Advertisement

- BGP routing table update procedure



AS Path Advertisement

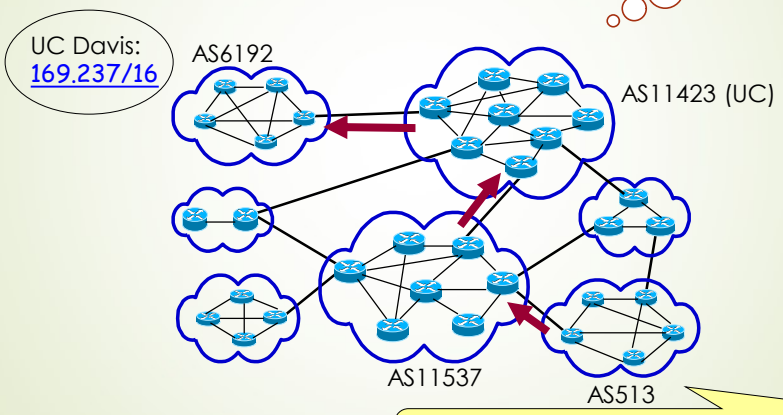
- BGP routing table update procedure



AS Path Advertisement

- Actual Routing / Forwarding

There's no hierarchy or centralized management (No Trusted 3rd party)

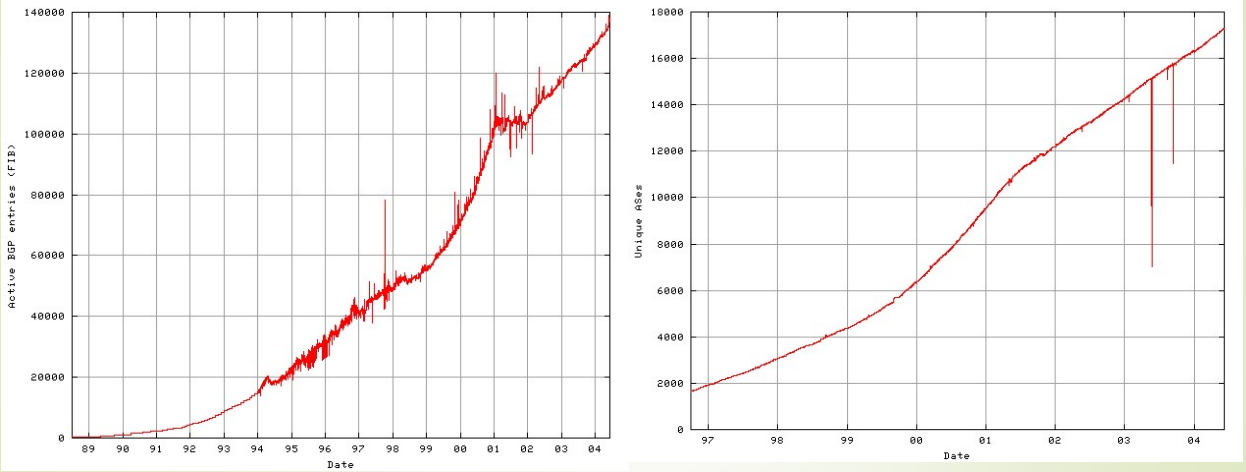


an AS Path:
169.237/16 **513→11537→11423→** 6192

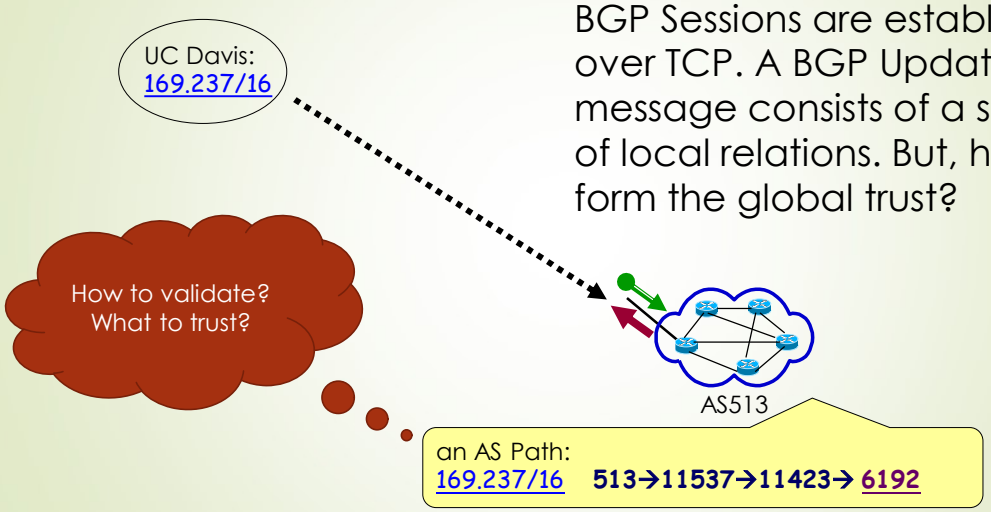
How big was internet in 2006?

- 20464 Autonomous Systems
- 167138 IP Address Prefixes (subnets)
  - Every single prefix, must be propagated to every single AS.
  - Every single AS must maintain the routing table to route the traffic to any one of the 167138 prefixes to the right destination.
- BGP is the protocol to support the exchange of routing information for ALL prefixes in ALL ASs.
  - Note that inside ASs, either iBGP or other routing algorithms (such as OSPF) may be used. EBGP (BGP) is a large-scale routing algorithm.

The "Internet"



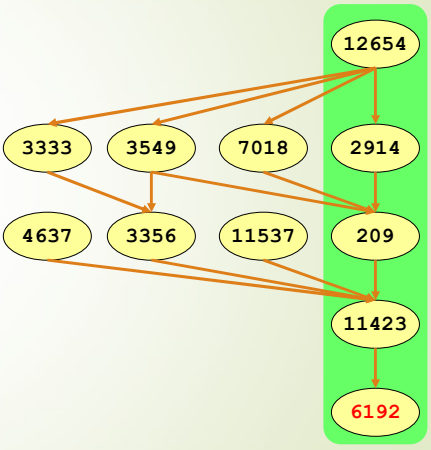
Security and Trust to BGP Updates



BGP Sessions are established over TCP. A BGP Update message consists of a sequence of local relations. But, how to form the global trust?

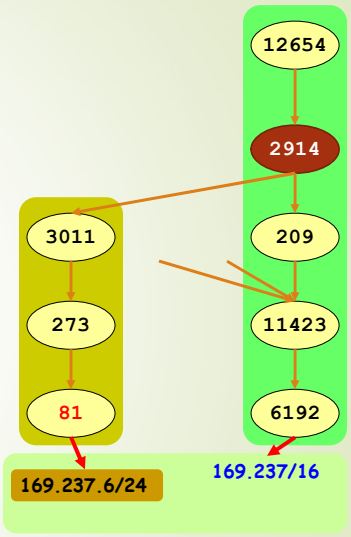
Origin AS in an AS Path

- UCDavis (AS-6192) owns **169.237/16** and AS-6192 is the origin AS
- AS Path: **513→11537→11423→ 6192**
  - 12654 13129 6461 3356 11423 6192
  - 12654 9177 3320 209 11423 6192
  - 12654 4608 1221 4637 11423 6192
  - 12654 777 2497 209 11423 6192
  - 12654 3549 3356 11423 6192
  - 12654 3257 3356 11423 6192
  - 12654 1103 11537 11423 6192
  - 12654 3333 3356 11423 6192
  - 12654 7018 209 11423 6192
  - 12654 2914 209 11423 6192
  - 12654 3549 209 11423 6192



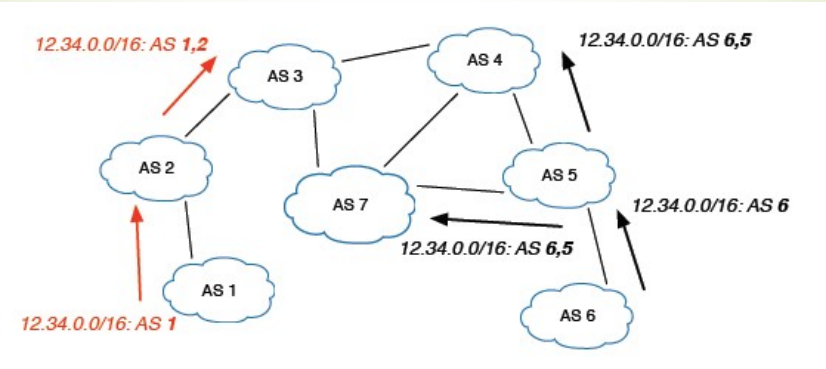
Prefix (Subnet) Hijacking Origin AS Changes (OASC)

- Ownership: UCDavis (AS-6192) owns **169.237/16** and AS-6192 is the origin AS
- **Current**
  - AS Path: **2914→209→11423→ 6192**
  - for prefix: 169.237/16
- **New**
  - AS Path: **2914→3011→273→ 81**
  - even worse: 169.237.6/24
- Which route to use?
- Is this legitimate or abnormal??



Prefix Hijacking – A Different View

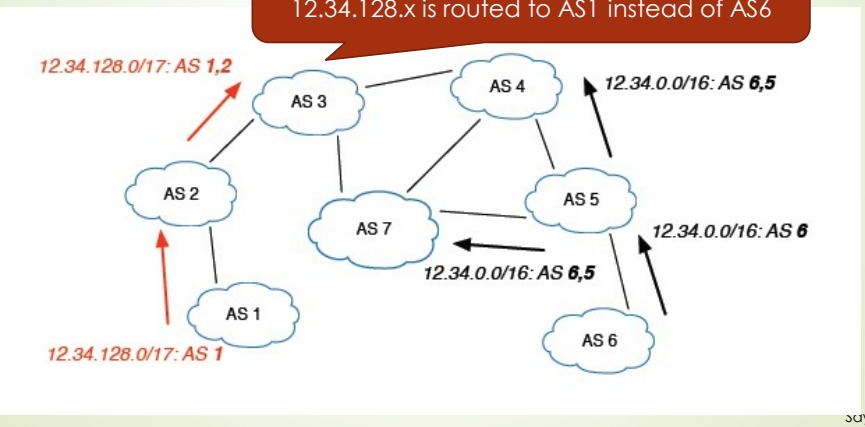
- BGP Does Not Verify AS Number/IP Addresses
  - Prefix Hijack: Black Holes, Interception Attacks



(Kyle Super, 2011)

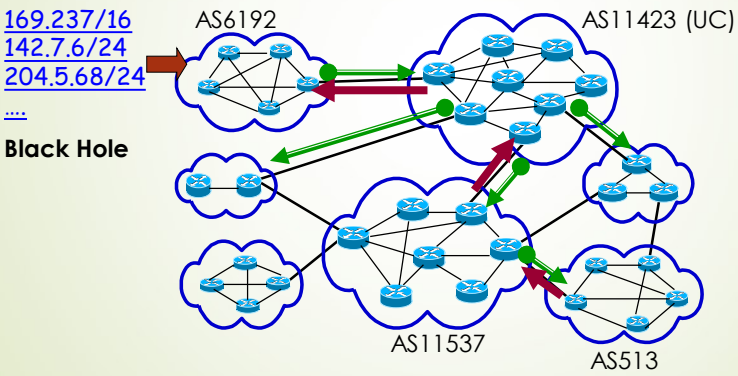
IP Address De-aggregation

- Happens when part of a subnet is said to be somewhere else. Routers select the most specific table entry when there are overlaps in subnets.

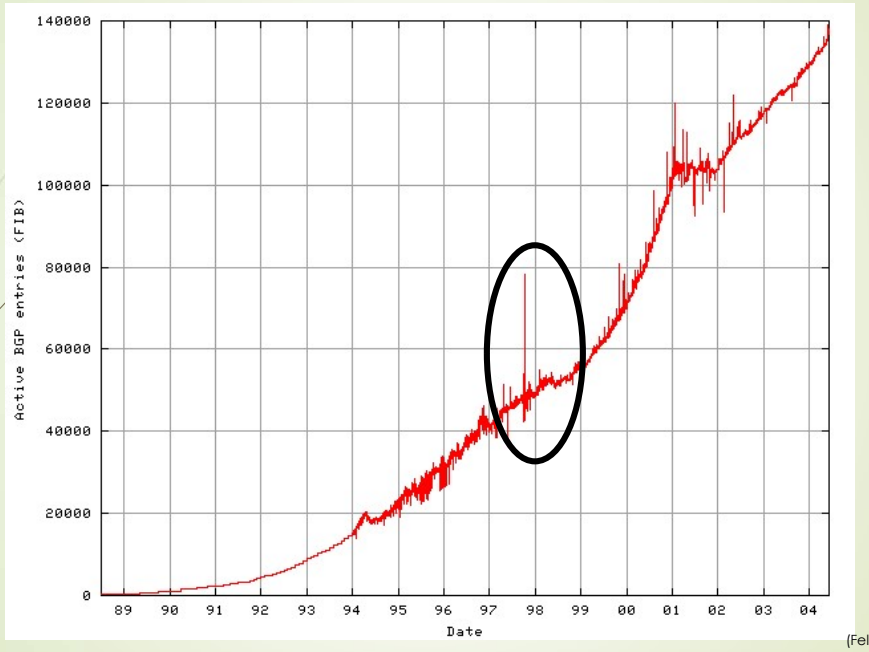


Internet Global Failures

- AS7007 falsely de-aggregated 65000+ network prefixes in 1997 and the US east coast Internet was down for **12 hours.**



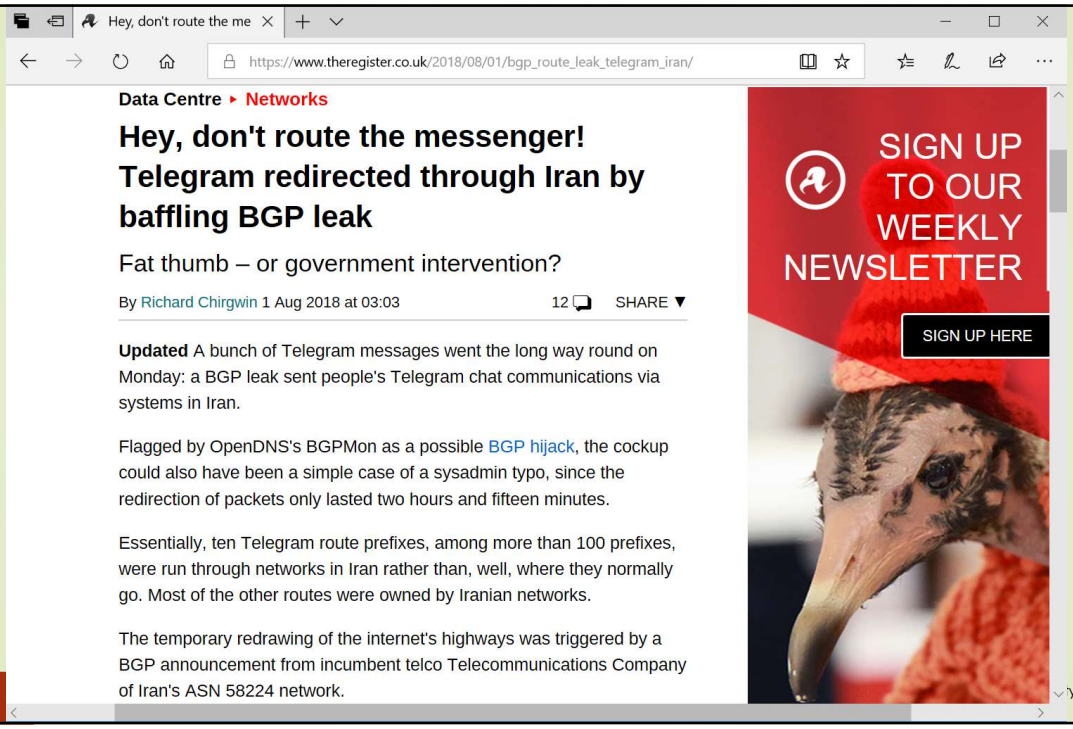
Active BGP Entries



(Felix Wu, UC Davis)

New Prefix Rate-limiting

- **A possible solution for the previous problem:**
  - For any given time window, a BGP peer can only introduce a X number of new IP prefixes.
  - X is limited.
  - But, tier-1 ISPs cannot be rate-limited.
    - There are many updates/changes by them as people sell/buy subnets frequently.
  - Rate limiting works but **It won't help if a specific prefix is hijacked!**



Vulnerabilities in BGP

- No mechanism to verify the authenticity and integrity of advertised routes.
- Routers can send incorrect information to its peers (either intentionally or by misconfiguration)
  - Do you remember the 1997 disaster?

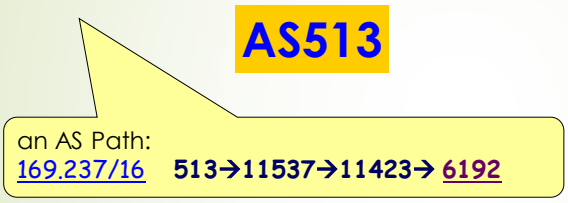
→**Requirement : For every UPDATE received,**

1. **A BGP router should be able to verify that the "owner" of the prefix authorized the first (origin) AS to advertise that prefix and**
2. **that each subsequent AS in the path has been authorized by the preceding AS to advertise a route to that prefix.**

Presentations scheduling

Secure BGP (S-BGP)

- So the best solution is to authenticate/validate BGP update messages.



- PKI (public key infrastructure)
  - Every relationship is certified by related ASs (using some certificates issued by the CA).

Secure BGP (S-BGP) – simple info

- Assumes a Public Key Infrastructure
- Communication over IPsec
- Uses digital signatures to assure the authenticity and integrity of routing information
- Each router signs the proposed path together with the recipient AS
- Signature stored in PATH ATTRIBUTE field of BGP's UPDATE packet

S-BGP Design Overview

- S-BGP makes use of:
  - **IPsec** to secure point-to-point communication of BGP control traffic.
  - **Public Key Infrastructure** to provide an authorization framework representing address space and AS # "ownership".
    - **Attestations** (digitally-signed data) to bind authorization information to UPDATE messages
    - Each router signs the proposed path together with the recipient AS #.
    - Signature stored in PATH ATTRIBUTE field of BGP's UPDATE packet.

A PKI for S-BGP

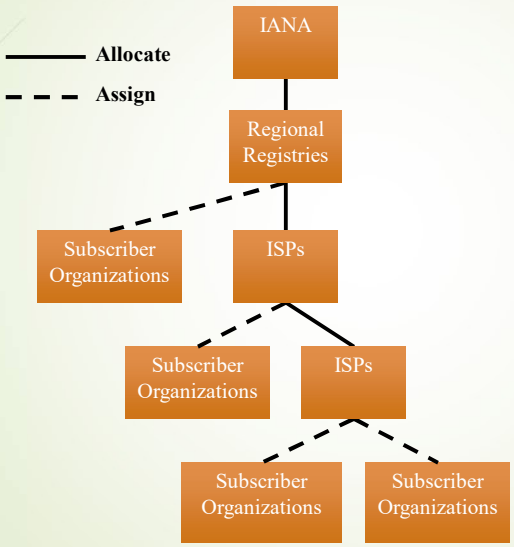
- Public Key (X.509) certificates are issued to ISPs and subscribers to identify "owners" of AS #'s and prefixes.
- Prefix data in certificates is used to verify authorization with regard to address attestations (ownership of prefix).
- Address attestations, AS #'s and public keys from certificates are used as inputs to verification of UPDATE messages.

PKI and Global Trust

- **Is it reasonable to have a global PKI or any weaker form of centralized trust servers?**
  - Chicken and Egg problem:
    - Internet → Trust Service
    - Trust Service → Internet
    - Which infrastructure depends on which?
    - Won't a centralized PKI jeopardize the scalability?

51

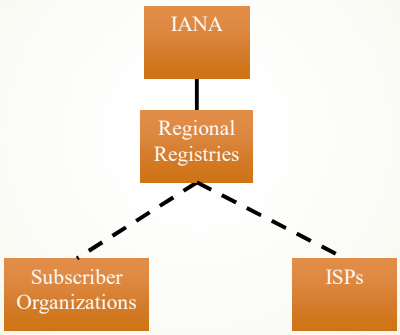
Subnet/Address Allocation Hierarchy



(Kent, BBN)

52

AS # Allocation Hierarchy

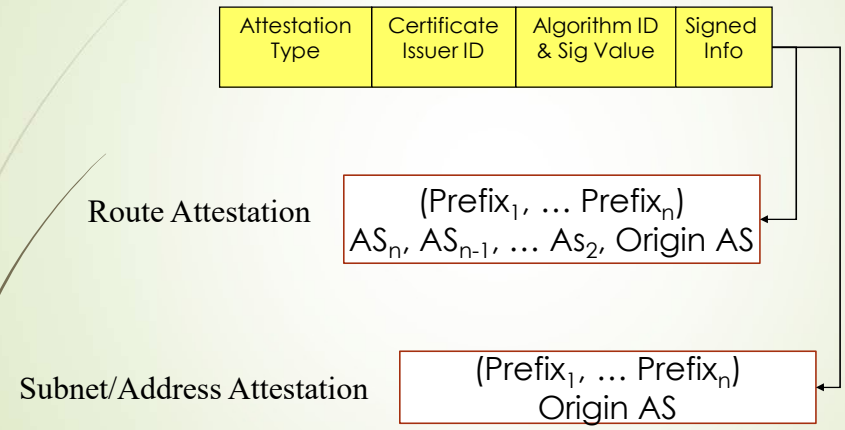


(Kent, BBN)

Two Types of Attestations

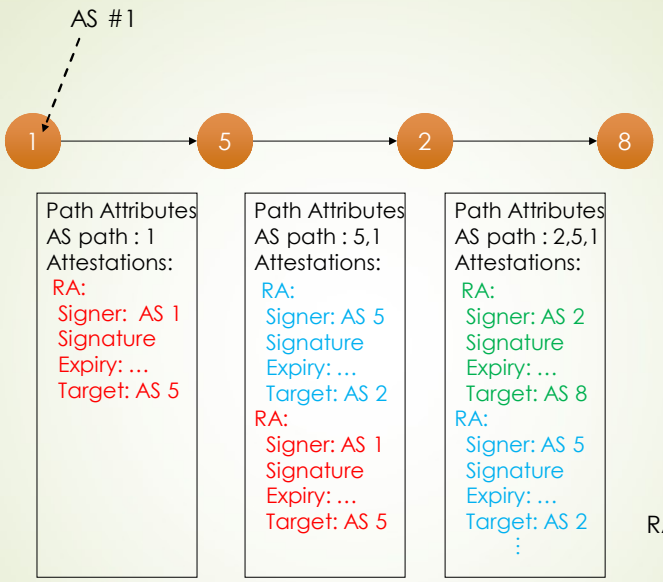
- An **Address Attestation (AA)** is issued by the "owner" of one or more prefixes (a subscriber or an ISP), to identify the first (origin) AS authorized to advertise the prefixes.
  - Simply a certificate signed by an authority showing that for example AS #513 owns 172.160.0.0/24
- A **Route Attestation (RA)** is issued by a router on behalf of an AS (ISP), to authorize neighbor ASs to use the route in the UPDATE containing the RA.

Simplified Attestation Formats



(Kent, BBN)

S-BGP



(Anupam Garg)

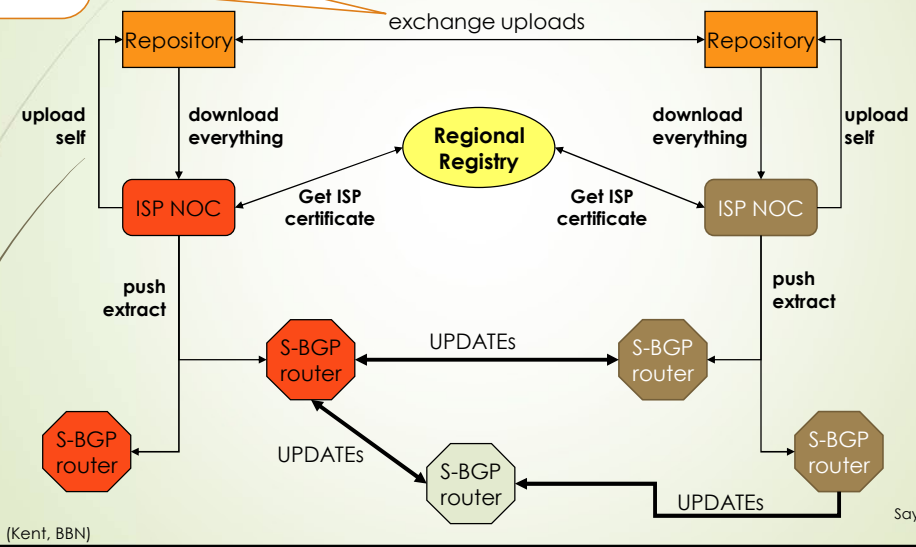
Facts about S-BGP

Why do you think we have Certificate Revocation Lists here?

- Every S-BGP router needs access to all the certificates, CRLs, and address attestations so that it can verify any AAs and RAs.
  - These data items don't come in UPDATE messages.
- S-BGP uses replicated, loosely synchronized repositories to make this data available to ISPs and organizations.
- The repository data is downloaded by ISP/organization Network Operation Centers (NOCs) for processing
  - Each NOC validates retrieved certificates, CRLs, & AAs, then downloads an extracted file with the necessary data to routers
  - Avoids need for routers to perform this computationally intensive processing
  - Permits a NOC to override problems that might arise in distributing certificates and AAs, but without affecting other ISPs.

Note that these are exchanged via the same routers!

S-BGP System Interaction Example



(Kent, BBN)

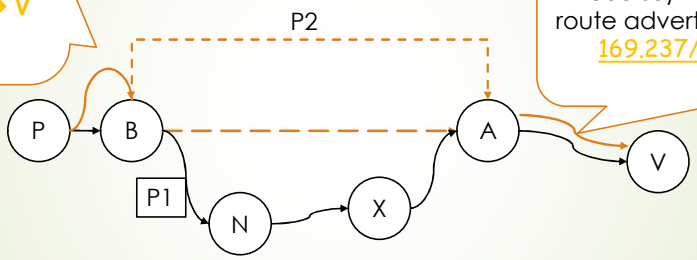
Sayad – University of Tehran

Analysis of S-BGP

Two nodes can forge a direct link between them (wormhole)

Reversely, **B** tells **P** (with signatures of course) that he has got the route advertisement right from **A**.
123.147/16 P→B→A→ V

A tells **V** (with signatures of course) that he has got the route advertisement right from **B**.
169.237/16 V→A→B→ P



Insiders' Wormhole Attack

P1 — Actual Path
Packet signed by B with N as next node in the path

P2 — Advertised Path
Packet signed by B with A as next node in the path

(Anupam Garg)

Sayad – University of Tehran

Analysis of S-BGP

IPSec has an anti-replay subprotocol which uses counters to prevent replay attacks.

- **Replay attacks**
  - Not possible in S-BGP. p2p connections are protected by IPSec. An attacker must compromise IPsec session or the router then.
  - There's an expiry time in every signed message too.
- **Expiry date**
  - When a signature expires the router needs to resend the advertisement
  - Routing information of the whole network has to be refreshed in a certain time period.
  - S-BGP allows the expiration date to be determined locally
    - Many routers refreshing the same day can cause a flood of UPDATEs.

Deploying S-BGP

- S-BGP requires:
  - Router software shall be updated to support S-BGP.
  - Regional registries must act as CAs for address prefixes and AS # assignment/allocation.
  - ISPs and subscribers that execute BGP must upgrade routers, might also act as CAs but must interact with repositories to exchange PKI & AA data.

Analysis of S-BGP

- Interoperability with BGP
  - In the transition phase, BGP packets will be sent encrypted between S-BGP routers and in clear to non S-BGP routers.
    - This gives large amount of known plaintext.
    - Could compromise security of IPSec (known plain-text attack for example , or even chosen plain text one).

Anonymous Routing

1. CROWDS
2. TOR

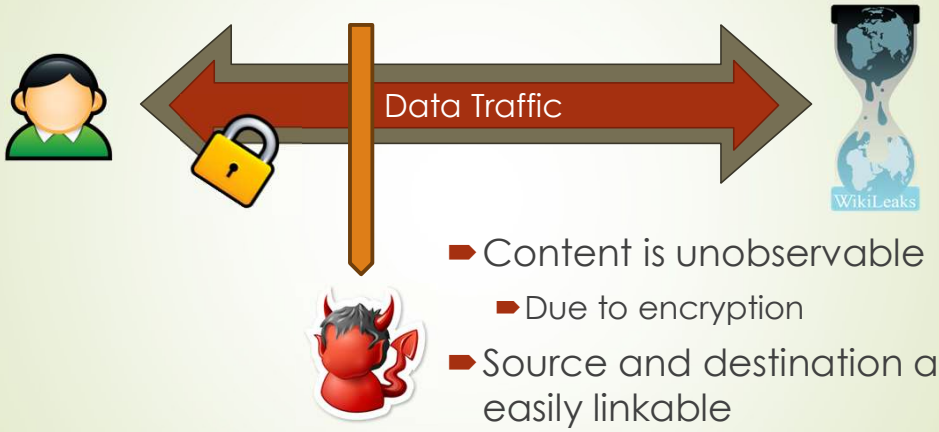
Data To Protect

- Personally Identifiable Information (PII)
  - Name, address, phone number, etc.
- OS and browser information
  - Cookies, etc.
- Language information
- IP address
- Amount of data sent and received
- Traffic timing

Anonymous Routing

- This is a totally different subject.
  - Forget about the BGP stuff for the time being.
- Anonymous routing
  - Source anonymity
  - Destination anonymity
- Anonymity is not the same as security !

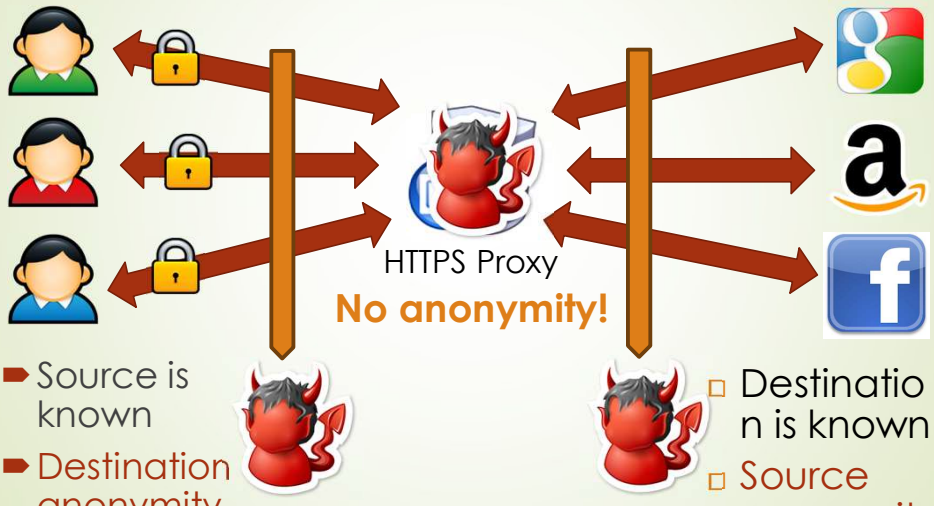
A Typical Way We Use: Crypto (SSL)



- Content is unobservable
  - Due to encryption
- Source and destination are easily linkable
  - Secure. But not anonymous!

(Northeastern University)

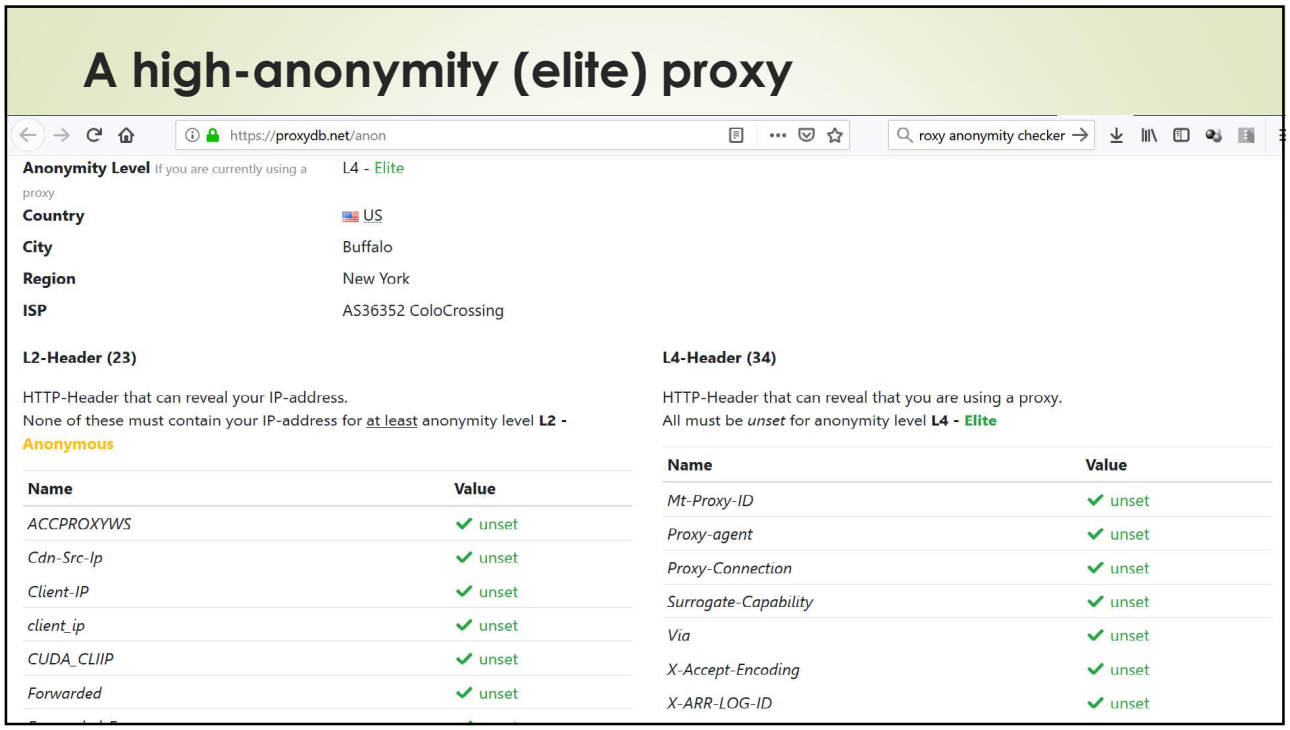
Anonymizing Proxies



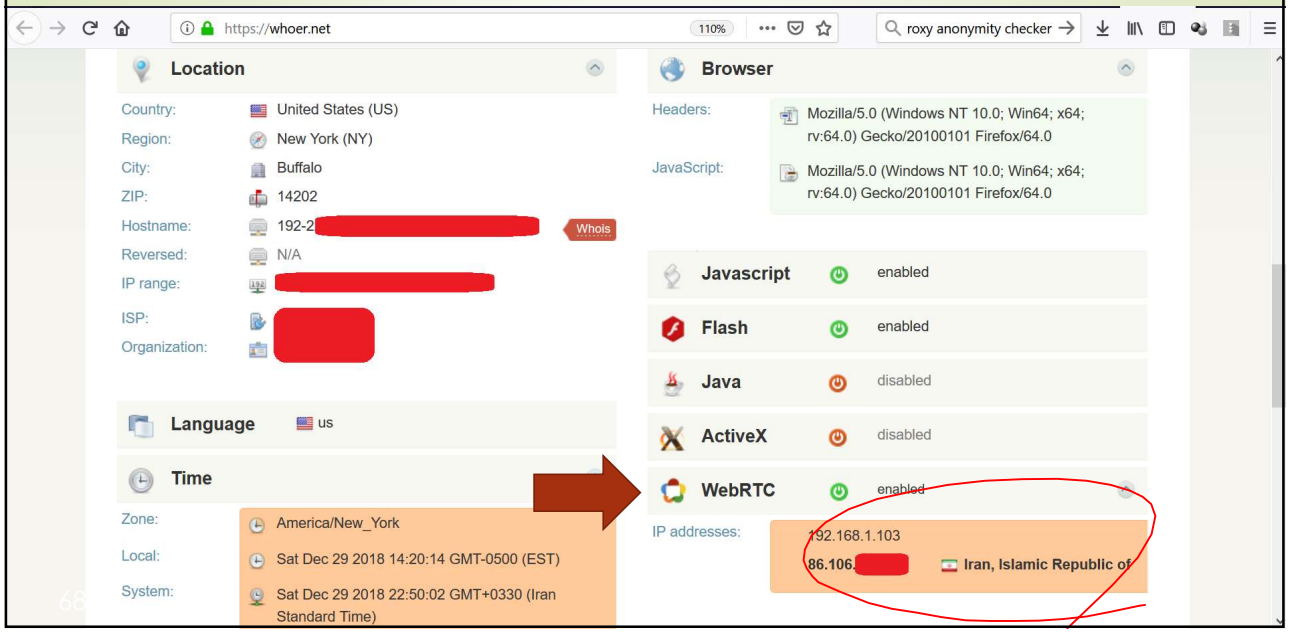
- Source is known
- Destination anonymity

- Destination is known
- Source anonymity

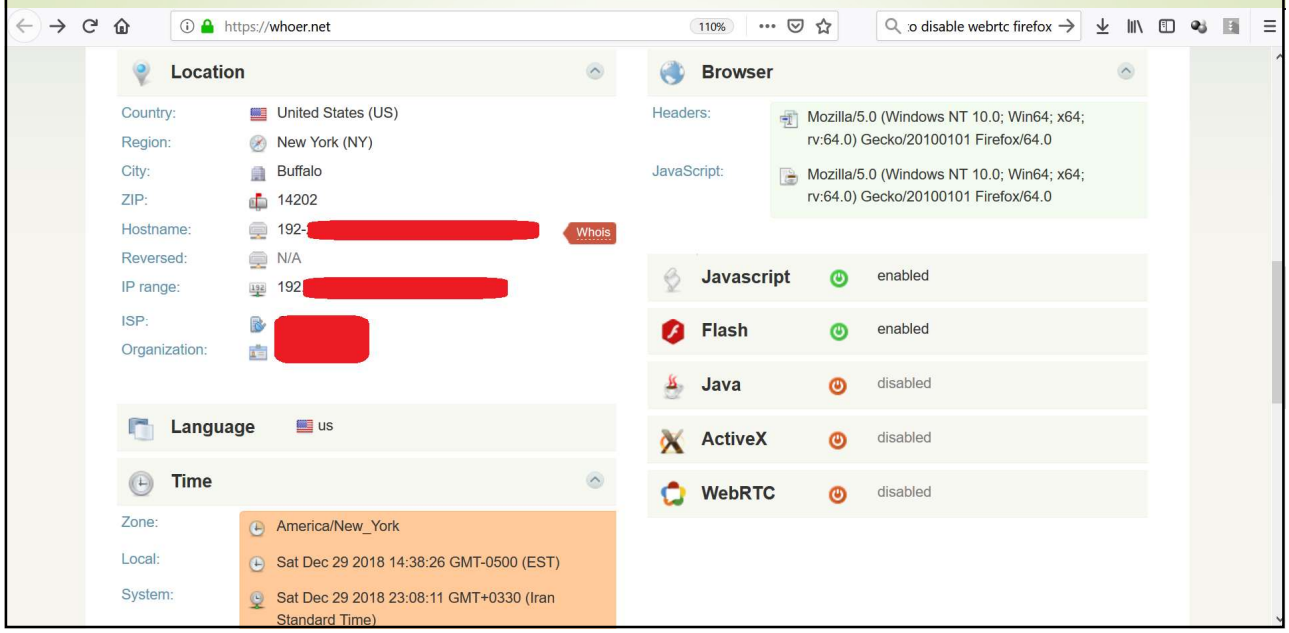
A high-anonymity (elite) proxy



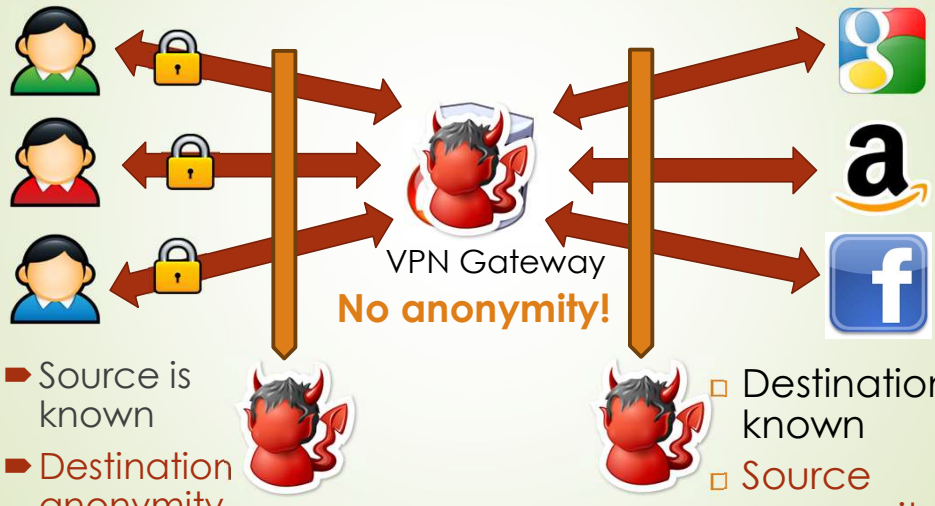
A high-anonymity (elite) proxy



A high-anonymity (elite) proxy



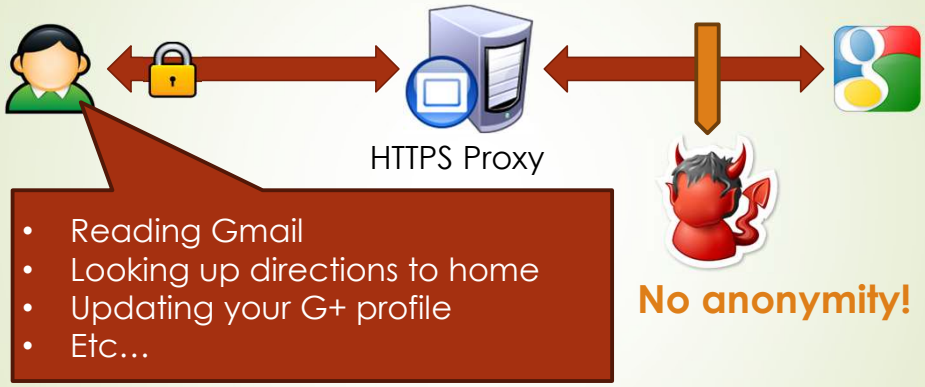
Anonymizing VPNs



- Source is known
- Destination anonymity

- Destination is known
- Source anonymity

Using Content to De-anonymize



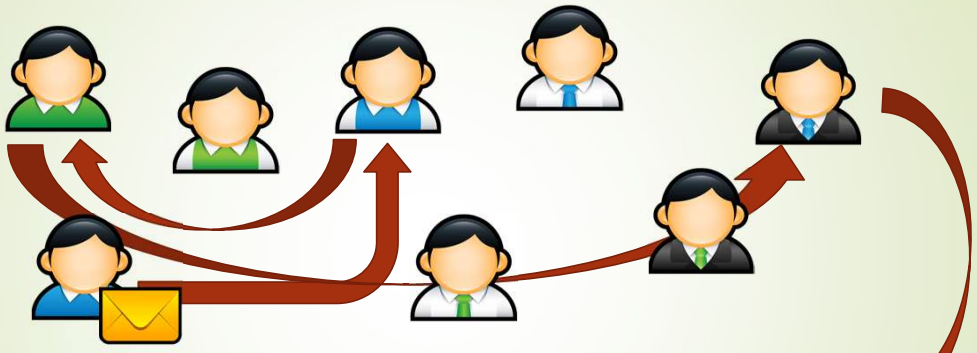
- Reading Gmail
- Looking up directions to home
- Updating your G+ profile
- Etc…

- Fact: the NSA leverages common cookies from ad networks, social networks, etc. to track users

1. Crowds

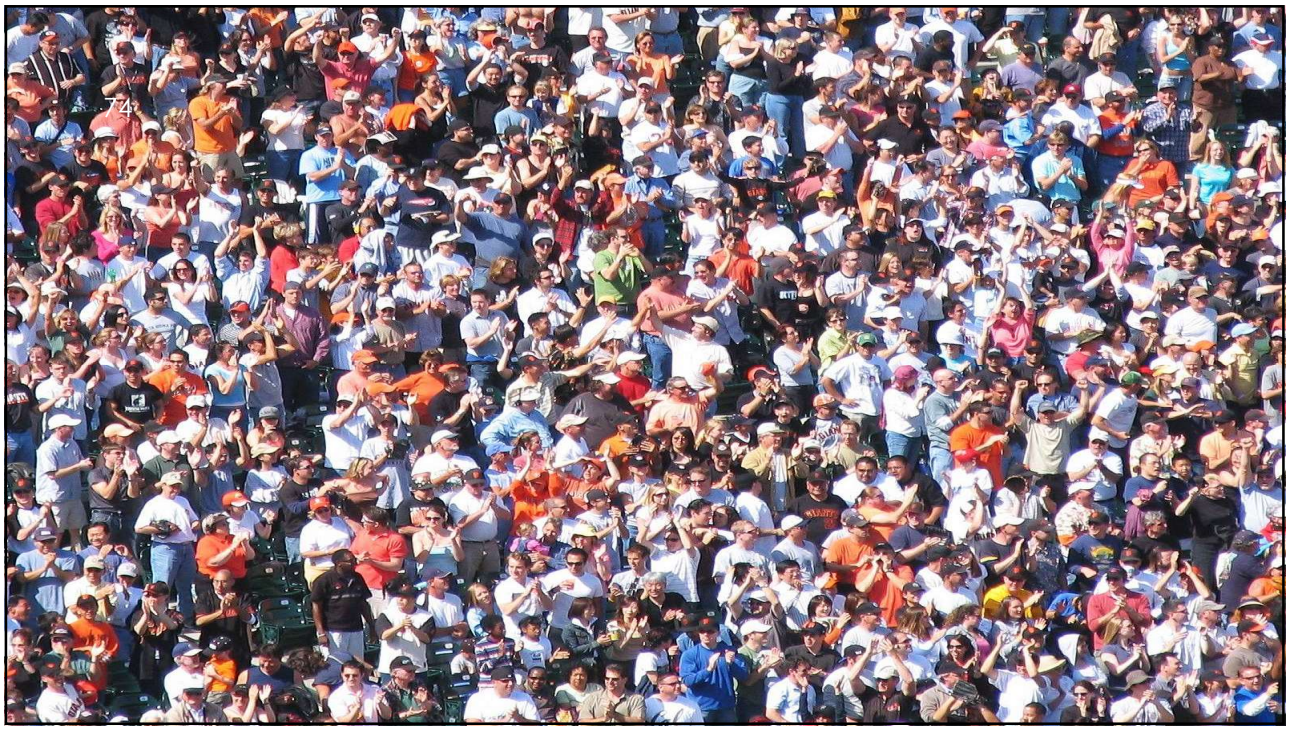
- Key idea
  - Users' traffic blends into a crowd of users
  - Eavesdroppers and end-hosts don't know which user originated what traffic
- High-level implementation
  - Every user runs a proxy on their system
  - Proxy is called a jondo
    - From "John Doe," i.e. an unknown person
  - When a message is received, randomly select $x \in [0, 1]$
    - If $x < p_f$: forward the message to a random jondo
    - Else: deliver the message to the actual receiver

Crowds Example

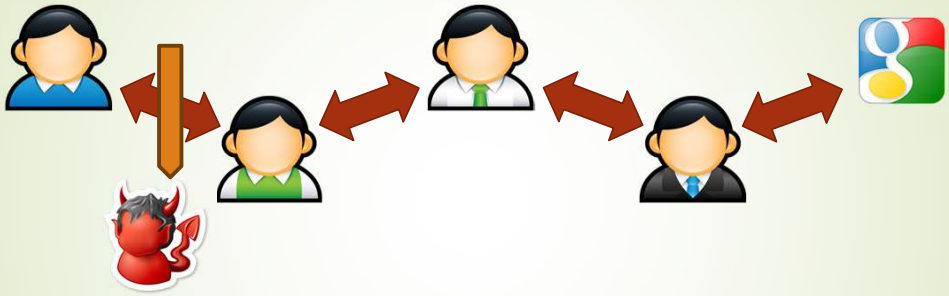


- Links between users use public key crypto
- Users may appear on the path multiple times

Final Destination

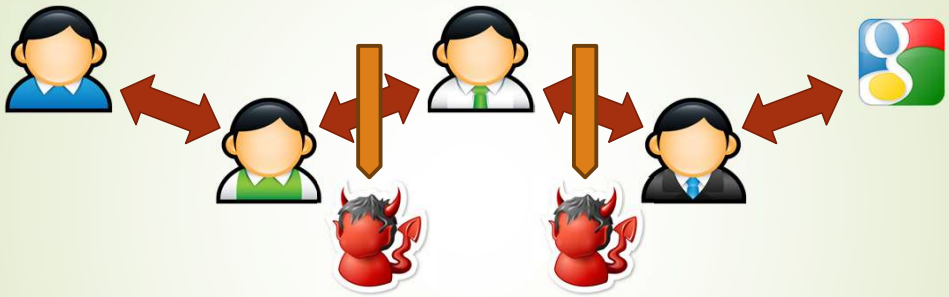


Anonymity in Crowds



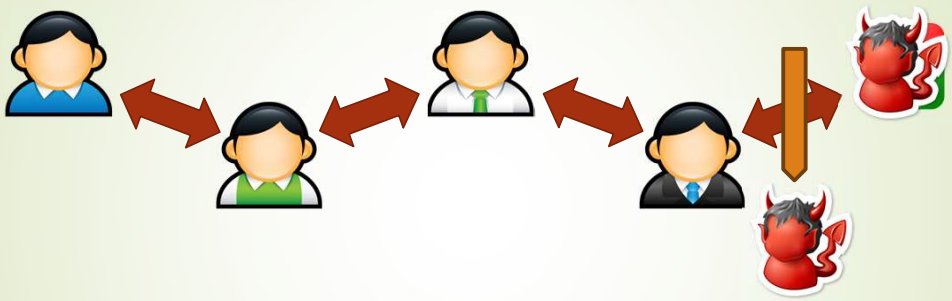
- No source anonymity
  - Source receives *m* incoming messages (*m* may = 0)
  - Source sends *m* + *1* outgoing messages
  - Thus, the source is sending something
- Destination anonymity is maintained
  - If the source isn't sending directly to the receiver

Anonymity in Crowds



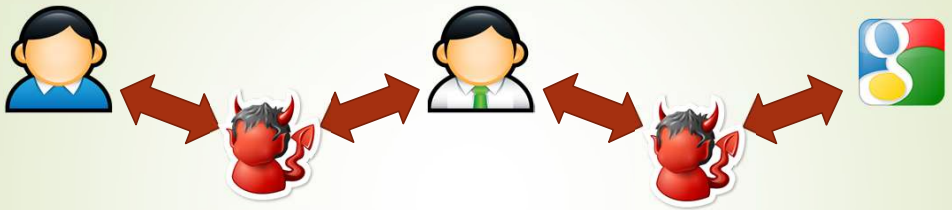
- Source and destination are anonymous
  - Source and destination are jondo proxies
  - Destination is hidden by encryption

Anonymity in Crowds



- Destination is known
  - Obviously No Anonymity
- Source is anonymous
  - O(n) possible sources, where n is the number of jondos

Anonymity in Crowds



- Destination is known
  - MITM jondo is able to decrypt the message
- Source is somewhat anonymous
  - Suppose there are c evil jondos in the system
  - If $p_f > \frac{3}{4}$ then with $n > 3(c + 1)$, the source cannot be inferred with probability > 0.5

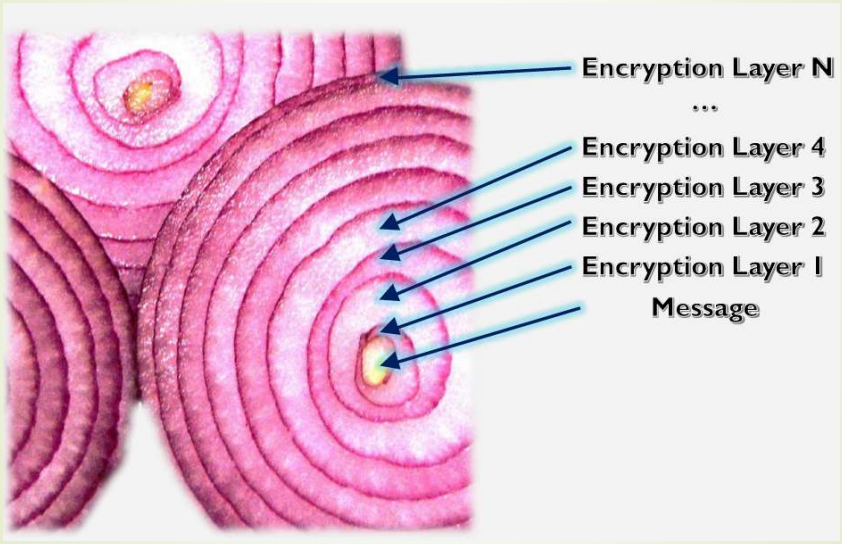
Other Implementation Details

- Crowds requires a central server called a Blender
  - Keep track of who is running jondos
    - Similar to a BitTorrent tracker
  - Broadcasts new jondos to existing jondos
  - Facilitates exchanges of public keys

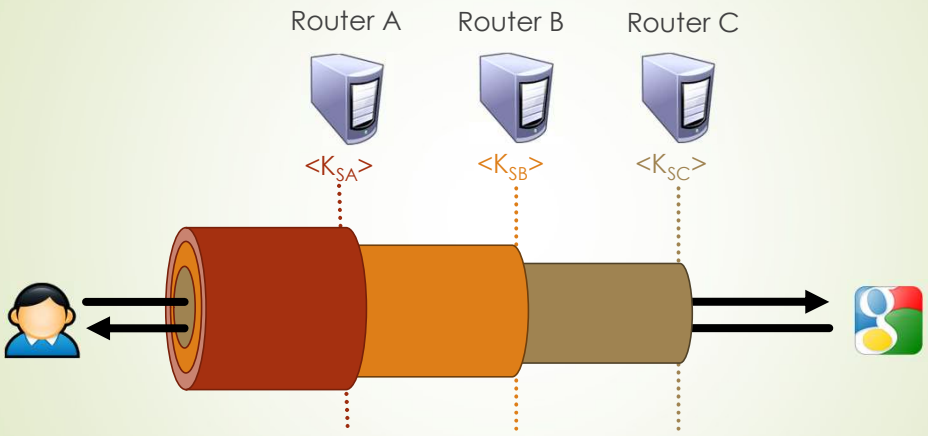
2. Onion Routing (TOR)

- US Navy Labs started the project in 1990s.
- DARPA took over the project in 1997.
- An alpha version was released in 2002.
  - The Onion Routing Project
- The second version was released in USENIX 2004 symposium.
  - open source!

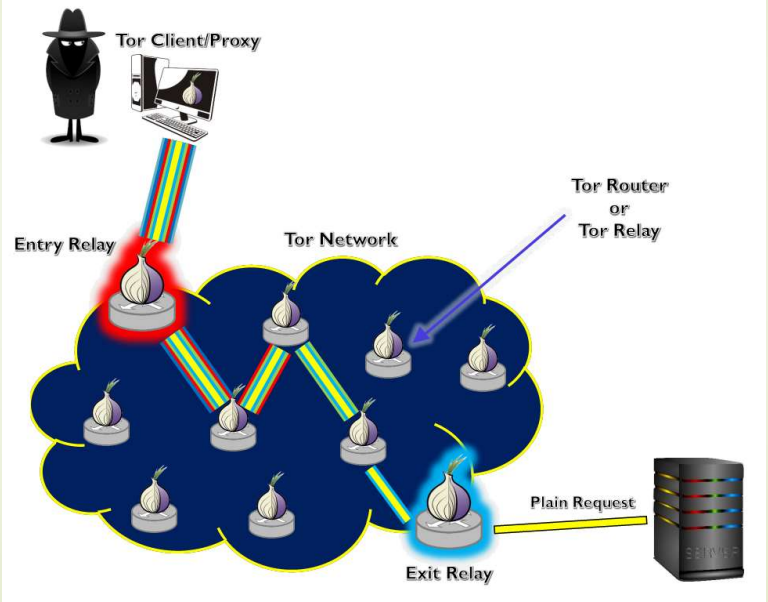
Onion Routing



Onion Routing – the Data Structure



Onion Routing – a big picture



Do You Remember?

Diffie-Hellman Key Agreement

Private key part of user A

Private key part of user B

X_A

X_B

$Y_A = \alpha^{X_A} \bmod q, \quad \{\alpha, q\}$

$Y_B = \alpha^{X_B} \bmod q$

$K = (\alpha^{X_B})^{X_A} \bmod q$
$= \alpha^{X_A X_B} \bmod q$

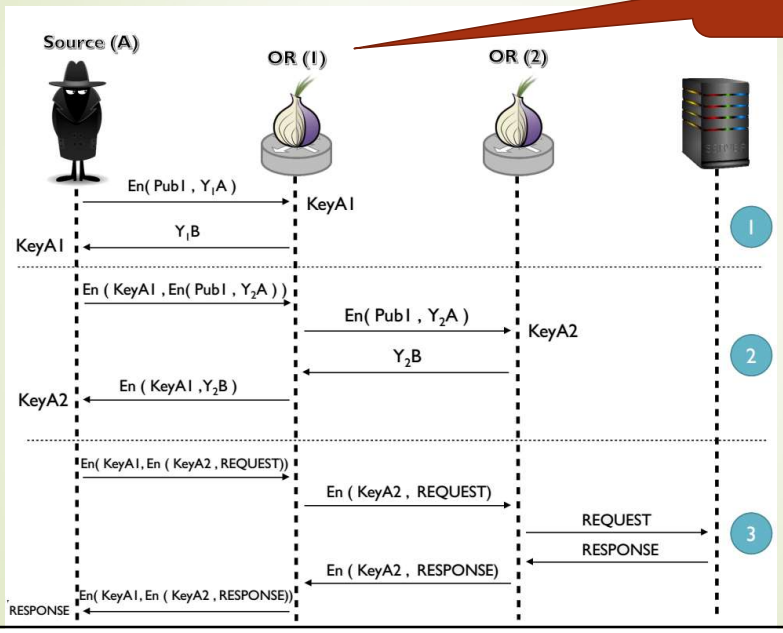
$K = (\alpha^{X_A})^{X_B} \bmod q$
$= \alpha^{X_A X_B} \bmod q$

Secured Channel with the Key K

q & α are both public values and can be used by any adversary

Onion Routing – a detailed picture

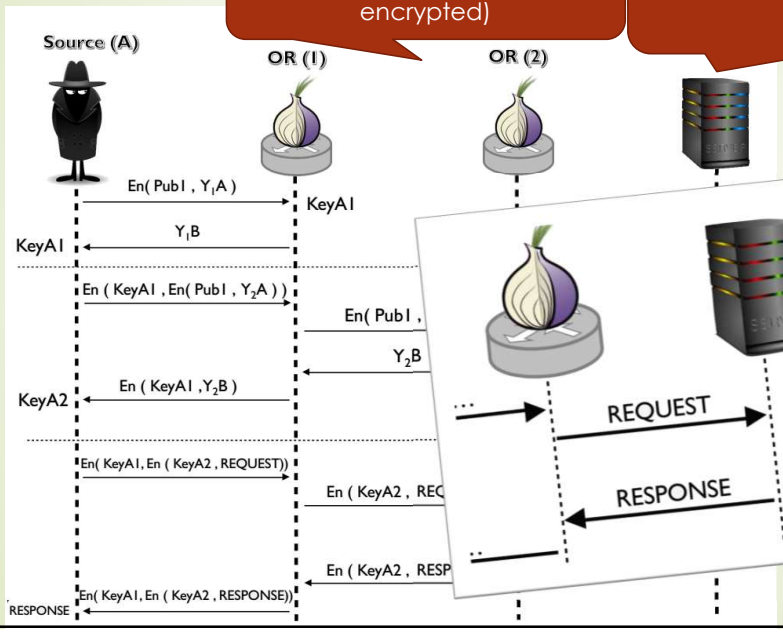
Intermediate routers see the data encrypted. Except the last one.



Onion Routing

The last router (OR2) sees the message in plain text (not encrypted)

From the server's point of view, OR2 is asking for the service, not the source.



Where can I do research?

It's not a very hot topic. It depends on the context. Whenever a new network comes, it becomes hot again.

- Don't worry, there's plenty of room:
  - Inventing new algorithms (e.g. for sensor networks, vehicular networks, …)
  - Key distribution
  - Multi-path routing
  - Fault/attack-tolerant routing
  - Privacy-preserving (anonymous) routing
  - Optimization → e.g. distributed evolutionary algorithms

and many more …

Still You Can Publish!

Nymble: Blocking Misbehaving Users in Anonymizing Networks

Patrick P. Tsang, Apu Kapadia, *Member, IEEE*, Cory Cor

SIR: a secure and intelligent routing protocol for vehicular *ad hoc* network

A PKI Adapted Model for Secure Information Dissemination in Industrial Control and Automation 6LoWPANs

SUDIP MISRA[1], (Senior Member, IEEE), SUMIT GOSWAMI[1], CHAYNIKA TANEJA[2], ANANDARUP MUKHERJEE[1], (Member, IEEE), AND MOHAMMAD S. OBAIDAT[3], (Fellow, IEEE)

A Survey of BGP Security Issues and Solutions

PASER: Secure and Efficient Routing Approach for Airborne Mesh Networks

Improving Security and Performance in the Tor Network through Tunable Path Selection

Rate Allocation for Multipath Routing in Wireless Multihop Networks with Security Constraints Based on Erasure Channel Modeling

Jinho Choi, *Senior Member, IEEE*

Cross-Layer Metrics for Reliable Routing in Wireless Mesh Networks

Stefano Paris, *Member, IEEE*, Cristina Nita-Rotaru, *Senior Member, IEEE, Member, ACM*, Fabio Martignon, *Member, IEEE*, and Antonio Capone, *Senior Member, IEEE*

The End of Secure Routing