Network Security (Continued)
28th September. 2012

Sakshi Jain

October 22, 2012

Broadly, there are two different threat models while approaching network security.

1. Off path/ web attacker

    Eve is not a co-resident on the same local network as A and B

    We assume that the routers on the path are not compromised

    It is generally very difficult to stop the attacker if he is a part of the network

2. On path/ network attacker

    Anything between Alice and Bob is not trusted

    Due to widespread use of open wifi, these models are not as impossible as it might seem

Hopefully the following figures help.

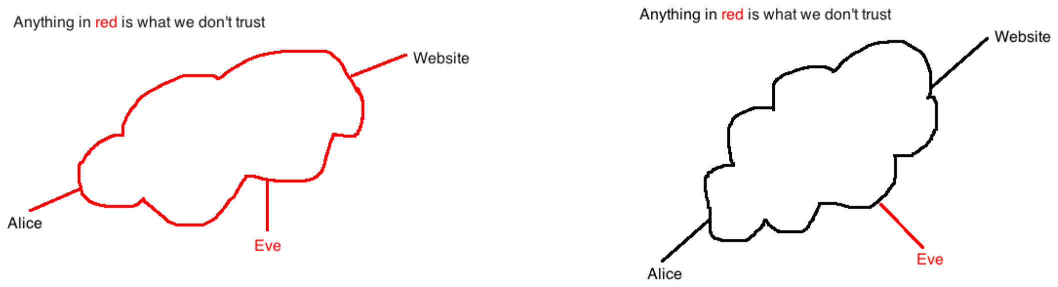
Protocol	Off-path attack	On-path attack
HTTP	yes	no
HTTPS	yes	yes
SSH	yes	yes
IMAP	yes	no
IMAPS	yes	yes
DNS	depends	no
BGP	yes	(if all routers were trustworthy, yes)

1 BGP

Each autonomous system (*examples of autonomous systems: UC, Berkeley, Stanford*) knows only its neighbours in the graph.

AS Path:
Consider the graph shown in the figure. Lets say G is a newly introduced node. F announces to its neighbours {B, E} that it has a one-hop path to G. B, E inturn then annouce it to their neighbours that they have a 2 hop path to G. This goes on, until A announces to B the path [A, C, D, E, F, G]. B does not annouce it further to D since D is already in the AS Path to G and hence a loop is recognized. This prevents cascading of announcements once triggered.

Certain possible attacks:
Example: Youtube-Pakistan: One of the routers say 'R' advertised that they have the shortest


Anything in red is what we don't trust
Website
Alice
Eve
Anything in red is what we don't trust
Website
Alice
Eve

(a) On path/ network attacker

(b) Off path/ web attacker

Figure 1: two different threat models

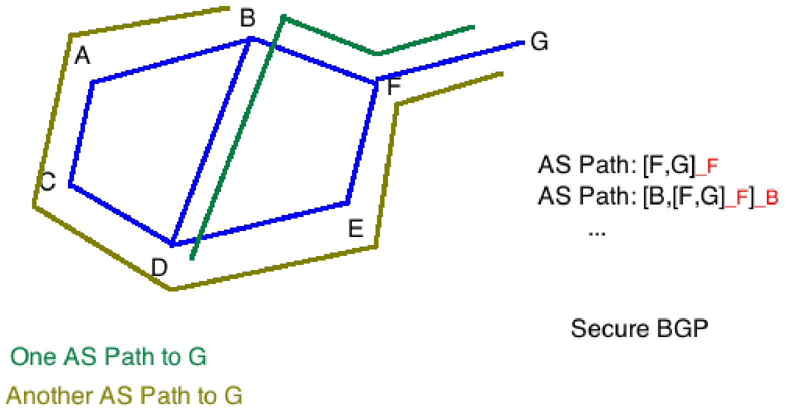


Figure 2: AS Path

route to youtube.com. This trigererd a wave of announcements causing all of the youtube traffic to be directed towards R. The malicious router R would then simply drop the packets thereby creating a black hole. However, this shortest path information got leaked outside Pakistan and hence the attack was detected.

MIT Blackhole:
A router in Florida advertised a very short route to MIT's server. The router got flooded with huge traffic which it was not capable to handling and hence went down and got noticed.

Discussion:
Such black-hole attacks are not as frequent since there is no monetary gain and is easily tracable. Instead, if the attacker is in the path between a user and a destination, he can modify the packets being sent. For example, www.amazon.com uses HTTP protocol for its website except for the payment and check-out section where it uses the HTTPS protocol. When a user checks out, the attacker can redirect the user to a fake HTTP site asking for login password (sent in plaintext) and payment details. The user might not notice the change from HTTPS -¿ HTTP.

Lets say, Berkeley wants to modify Stanford's data being sent to Amazon. Berkeley then announces a fake shortest path to www.amazon.com to its neighbours and thereby Stanford as well. All the traffic from Stanford is then routed through Berkeley. Lets assume Berkeley modifies the data and now wants to send it to Amazon. (It does not want to drop the packets since the black hole would be easily detectable). However, since there is no real short path to Amazon site, Berkeley is stuck with the actual route, say through San Francisco. When San Fancisco receives the packet, it sends it back to Berkeley since Berkeley had advertised for the shortest route which did not really exist. Thus Berkeley is now stuck with huge traffic which it cannot route though any of the routers in the network. One thing what Berkeley can do is to buy a router (Conspirator) close to Amazon, set up a direct cnnection to that router from Berkeley and from that router to Amazon. However, this option is very costly as it involves buying a router with huge bandwidth and setting up direct connections.

The problem with the previous attack was that everyone including members on the real path would send the packets to Berkeley assuming Berkeley has the shortest route. So, here is a modification: The conspirator router could be removed from the attack if there was some way by which we could keep the SanFrancisco's AS Path to Amazon the same despite changing Stanford's. One could use the fact that the announcements for an AS Path are not made if the neighbour exists in the path. Thus, the attacker (us) can create a fake AS Path, send it to Stanford directly mentioning all its neighbours in the path. Thus Stanford will not advertise further and send all its packets to Berkeley. Berkeley could then modify the packets and then route it to Amazon through SF.

However if someone is monitoring the AS Path at Stanford, the attack could be recognized since there does not exist any apparent legitimate reason for an AS Path to conatin all its neighbors. So, one defense could be, if you see more that one neighbor in the AS Path, you do not consider that as a legitimate route. However, there could be benign AS-Paths of such nature due to certain policy implementations of neghboring routers.

2 Secure BGP

Secure BGP uses cryptographic protocols to ensure that every router that appears on the AS Path has signed thereby acknowledging that the particular router can infact route the packets to the destination and that it trusts the AS - path its advertising. The protocol is better explained in the figure above. The previous attack is mitigated using this protocol, since Berkeley cannot send an AS-Path with Stanford's neighbours unless they have signed (which they wont, given that there exists no such path). However this means that every router must have the public key of all the other routers and must check for signatures for everyone on the AS-Path before advertising the path further. This causes is huge performance overhead and hence is not used largely.