IETF81@Quebec, Canada

Secure Extension of BGP by Decoupling Path Propagation and Adoption

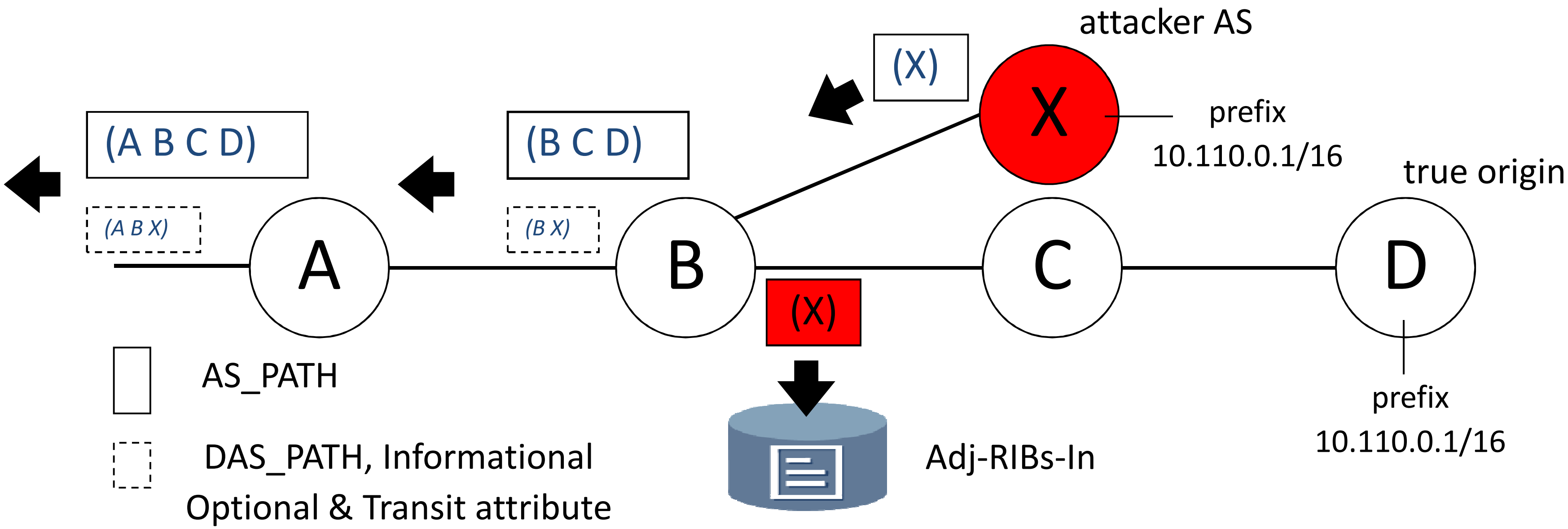
draft-zhang-idr-decoupling-03

Mingui, Bin, Dacheng, Beichuan
zhangmingui@huawei.com

Comments and Answers

- Does DBGP require contiguous deployment?
  - Answer: No.
- If you are going to pass this information across ASes. Wouldn't this become some kind of attacks by intending to manipulate the path.
  - Answer: DAS_PATH is informational. It will never be used for data delivery.
- You are injecting this DAS_PATH thing. But what is really to stop an attacker from injecting a routing? DAS_PATH, like cook for a while and then, you know, at some point, there are attack updates become valid.
  - Answer: Operators do stop the attack. Compared to BGP, DBGP suppresses the attack for a while and creates the opportunity for operators to intervene before attack really take effect.
- Do operators prefer a new path or an old&secure path suggested by DBGP?
  - Answer: It's up to the operators. DBGP is effective even it's partially deployed.

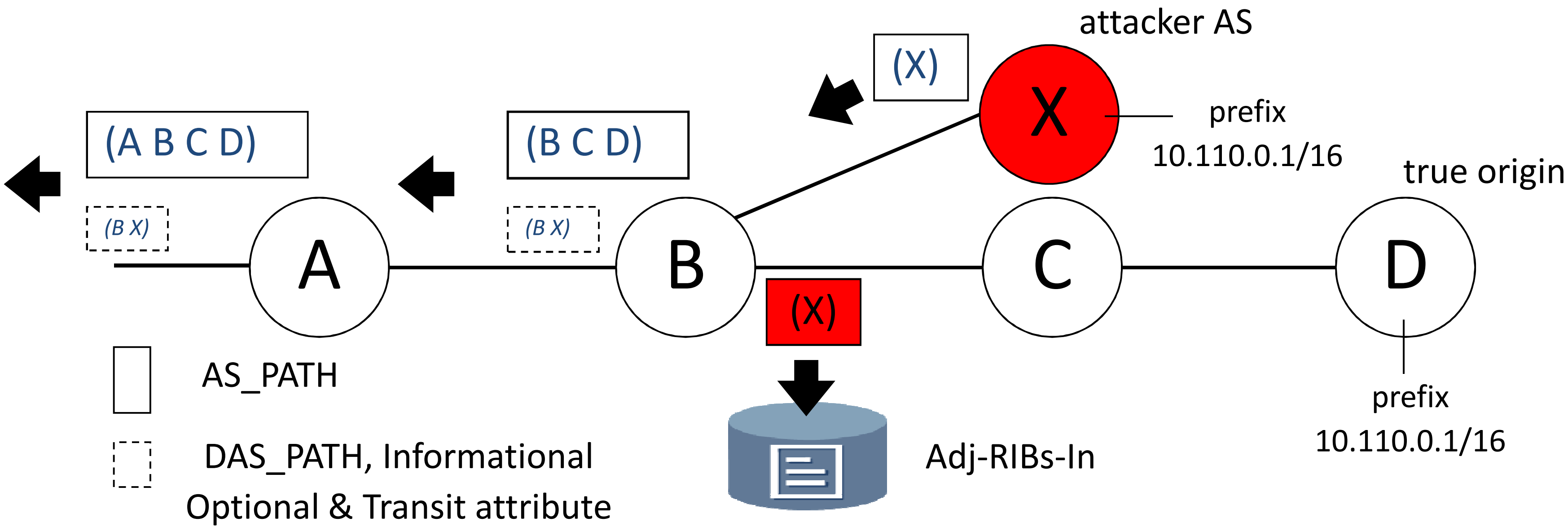
DBGP-A New Mitigation Scheme



DBGP: Decoupling path propagation and adoption in BGP

- (B X) is suspected and propagated in DAS_PATH attribute.
  - A *DAS_PATH will only used for informational purpose rather than real data delivery!*
- If (B X) is actually legitimate, the propagation in fact enable parallel validation.
  - When B propagate it to A as legitimate path later, A MAY have already finished the validation (e.g., checked by operators) in advance and can accept it directly without suspicion.

Discontiguous Deployment of DBGP



DBGP: Decoupling path propagation and adoption in BGP

- If A does not deploy DBGP, it will forward the DAS_PATH without appending itself.
- In the figure, A sends the UPDATE with DAS_PATH *(BX)* intact.
- Remote ASes can still use *(BX)* for the validation purpose in spite that it is incomplete.

Informational

- DAS_PATHs are informational and it is only used for detection/validation purpose.
- DAS_PATHs will never be used for data delivery. It is the job of AS_PATHs.
- Therefore, attackers can not attract traffic via DAS_PATHs.

Suppressed DAS_PATH Becomes Valid

- Think about the **YouTube Hijacking** (Attacked by AS17557 on 24 February 2008). Youtube operators intervene and stop the attack 2 hours later (but the attack already succeeds).
- If DBGP is deployed, the attack will not take effect while the operators can still know that the attack is going on.
- Before the DBGP suppression period ends, the operator should have removed the bogus path.
- DBGP creates the opportunity for operators to intervene and remove the suppressed path before it becomes valid.

Incremental Deployment

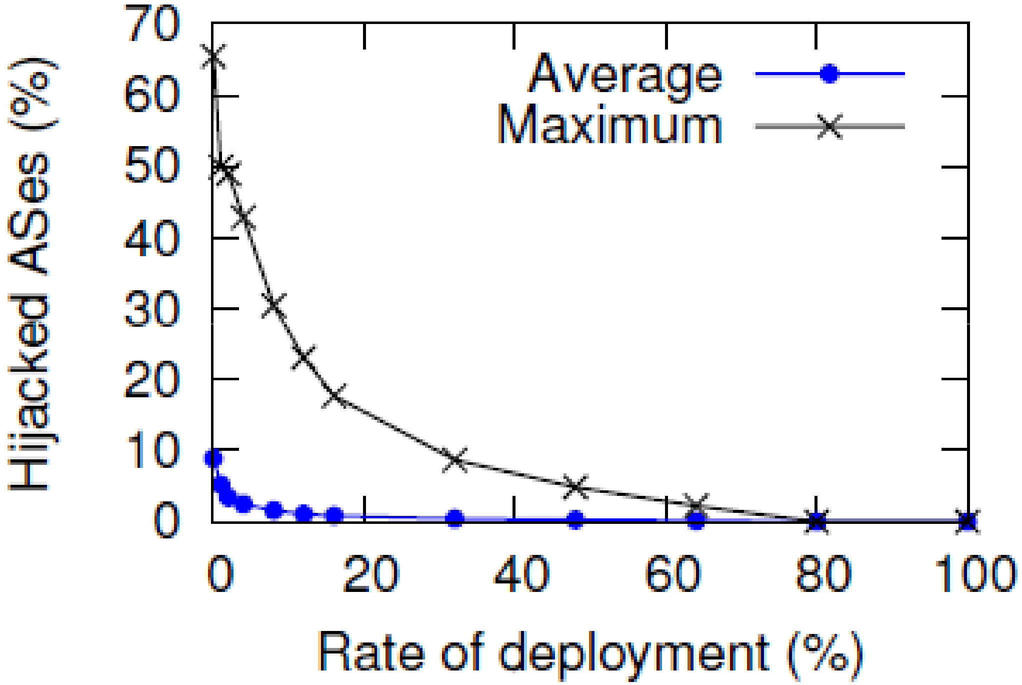
- If an operator chooses the new path rather than the old and secure path recommended by DBGP, that means he does not deploy DBGP.

- Some operators like to deploy DBGP while other operators dislike to deploy it. No matter.

- DBGP is effective even it’s partially deployed.

Incremental Deployment Evaluation

- The simulation is based on an Internet AS topology with 23718 nodes and 94468 links.



Thanks!