Pretty Secure BGP (psBGP)

Tao Wan
Nortel Networks
P.C. van Oorschot, Evangelos Kranakis
Carleton University

November 10, 2005

Outline

- Goals for BGP Security
- Pretty Secure BGP (psBGP)
- Comparison of S-BGP, soBGP, psBGP
- Concluding Remarks

“Common” BGP Security Goals

- **Data Origin Authentication**
  - BGP Speaker Authentication
  - AS Number (AS#) Authentication
- **Data Integrity (**of control messages**)**
- **Message “Truthfulness”**
  - Prefix Origin Verification
  - AS-PATH Verification

Sample of Related Work

- Perlman 1988 (*Ph.D thesis*)
- Bellovin 1989 (*ACM CCR*), 2004 (ACSAC)
- Kumar 1993 (*ACM SIGSAC Review)*
- Murphy 2001 (*IETF draft)*
- Kent et al. 2000 *(NDSS)* – ***S-BGP***
- White et al. 2003 *(IPJ)* - ***soBGP***
- Goodell et al. 2003 *(NDSS)* – ***IRV***
- Aiello et al. 2003 *(CCS)* – ***OA***
- Hu et al. 2004 *(SIGCOMM)* - ***SPV***

Pretty Secure BGP (psBGP)

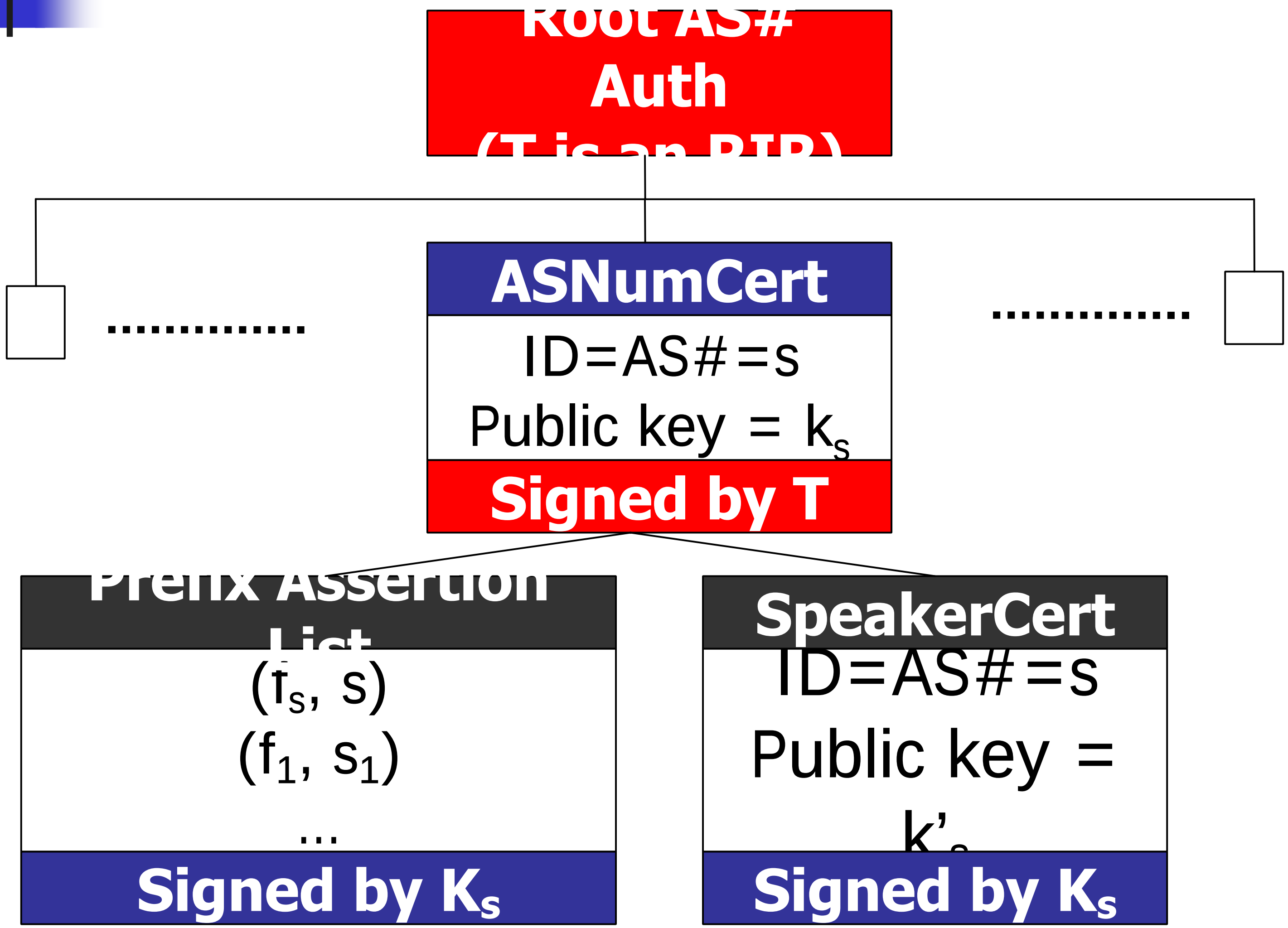
- A Centralized Trust Model for AS# Authentication

- A Decentralized Trust Model for Prefix Origin Verification (by corroboration)

Comparison of S-BGP, soBGP and psBGP

	AS# Authentication	Prefix Origin Verification	AS_PATH Verification
S-BGP	Centralized (multiple levels)	Centralized (multiple levels)	Full integrity
soBGP	Decentralized (with trust transitivity)	Centralized (multiple levels)	Plausibility
psBGP	Centralized (depth=1)	Decentralized (no trust transitivity)	Stepwise integrity

psBGP Certificate Structure



psBGP
AS# Authentication (*analysis*)

- **Reduced trust issue** –
  RIRs are trusted authorities for AS numbers
- **Simplified naming issue** –
  subject IDs are AS#
- **Manageable** # of certificates –
  17,884 ASes as of August 1, 2004 with
  a growth rate on average of 190 per month

psBGP
A Rating Mechanism (1)

- Each AS s_i rates every other AS s_j with a value $r_i(s_j)$ *in* [0,1], indicating s_i's belief in s_j
- Ratings are static and preconfigured
- Belief comb rule ($a_{[1..n]:}$ an assertion by $s_1,..,s_n$)

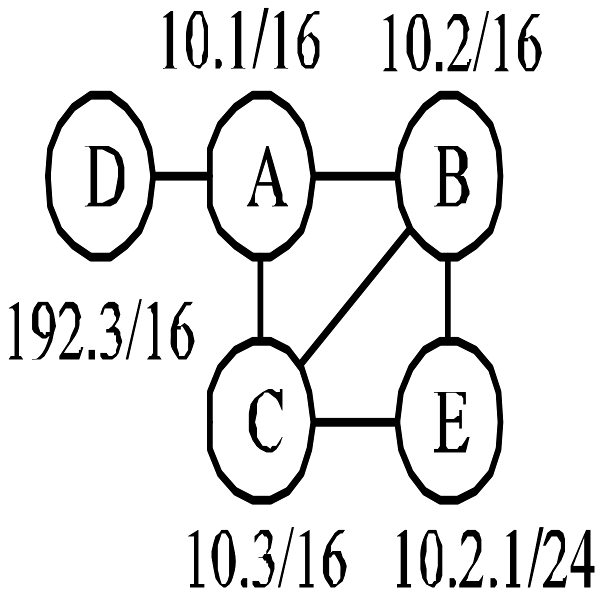
psBGP
A Rating Mechanism (2)

- $r_i(s_1)=0.5,\ r_i(s_2)=0.6 \rightarrow b_i(a_{[1,2]})=0.8$
- $r_i(s_3)=0.4 \rightarrow b_i(a_{[1,2,3]})=0.88$
- Evidence from a fully distrusted AS (rated by 0) does not increase belief
- Evidence from a fully trusted AS (rated by 1) increase belief to maximum, i.e., 1
- Combination rule is commutative and associative

psBGP
Prefix Origin Verification (1)

- Each AS issues a *prefix assertion list (PAL)*, listing *AS#-prefix bindings* for itself + selected neighbors (e.g., customers)
- *PALs* distributed with BGP UPDATE messages
- Each AS builds an *AS-prefix graph* based on its own *PAL* and those received from others
- An *AS-prefix graph* is used for verifying prefix "ownership"

psBGP Example – Prefix Assertion Lists



{(**10.1/16, A**), (10.2/16,B), (0,C), (192.3/16,D)}$_{A}$

{(**10.2/16, B**), (0,A), (10.3/16,C), (10.2.1/246,E)}$_{B}$

{(**10.3/16, C**), (10.1/16,A), (0,B), (10.2.1/24,E)}$_{C}$

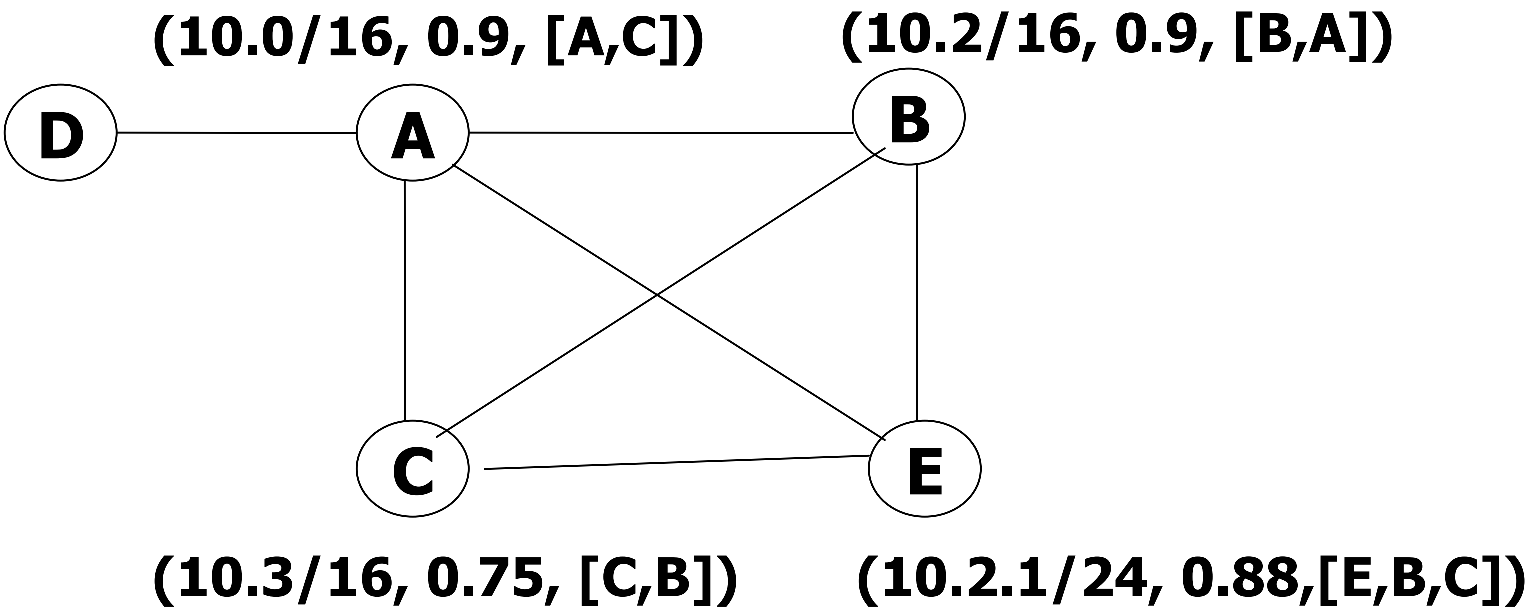
{(**192.3/16, D**), (0,A)}$_{D}$

{(**10.2.1/24, E**), (0,B), (0,C)}$_{E}$

psBGP Example – An AS-Prefix Graph (by D)

R(A)=0.8,   r(B)=r(C)=r(E)=0.5

(prefix, belief, [endorsing ASes])



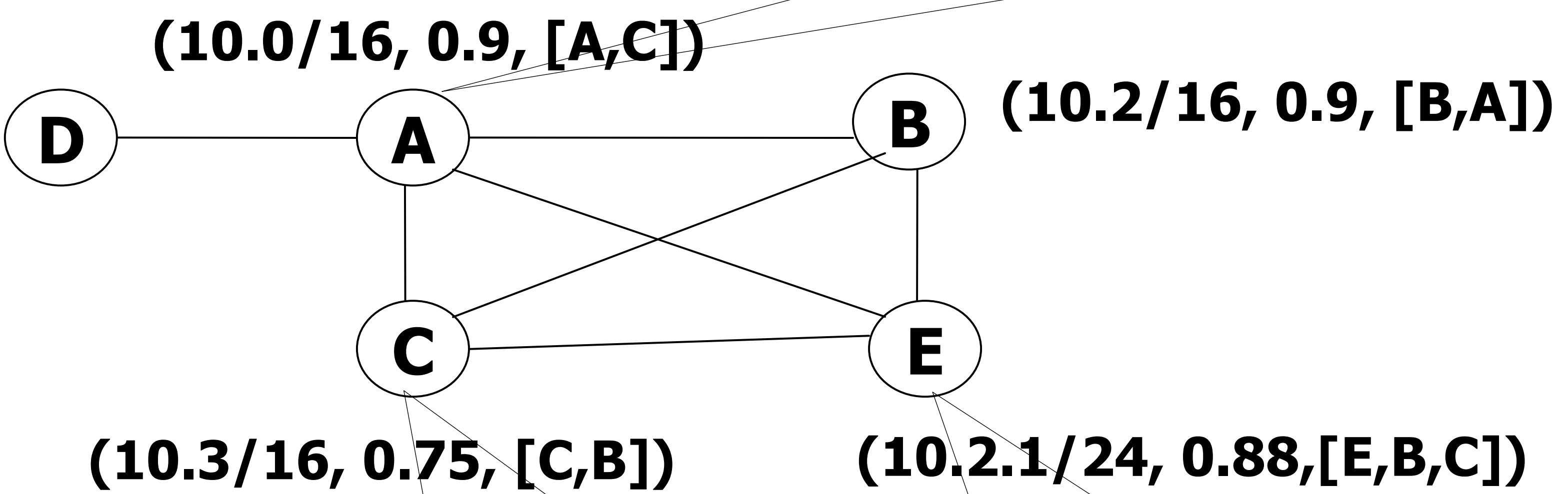
psBGP
Prefix Origin Verification (2)

- Two thresholds used for prefix origin verification
  - **α: *Sufficient confidence***
  - **β: *Sufficient claimants***
- A route (f, [s]) verifies properly by D if
  - D's belief in (f,s) binding >= α; or
  - # of ASes asserting (f,s) >= β

psBGP Example –
Prefix Origin Verification (by D)

$\alpha = 0.9; \beta = 3$

D has sufficient confidence in both A's origin of 10.0/16, and B's origin of 10.2/16.



C's origin of 10.3/16 will fail D's prefix origin verification

Sufficient num of claimants of E's origin of 10.2.1/24

Concluding Remarks

- Resilient to uncoordinated false prefix origin (e.g., attacks or misconfigurations)
- Reasonable deployment effort (e.g., PKI is simple and of manageable size)
- Deployment independent of each other
- Certain incremental benefit

For more information

http://www.scs.carleton.ca/research/tech_reports/2005/download/TR-05-08.pdf