

# RPKI Panel: ROAs and Manifests

Matt Lepinski  
BBN Technologies

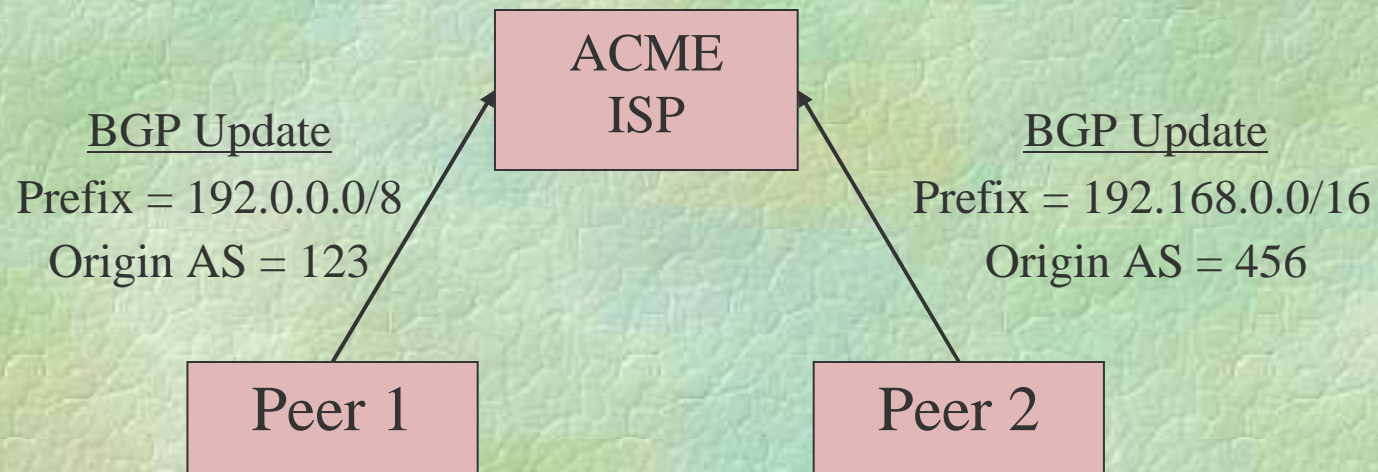
# RPKI Certificates: What are they good for?

---

- ❑ Resource Certificates provide a binding between a block of IP Addresses and a public key
- ❑ If you a signature on an object is verifiable using the public key of a valid RPKI certificate ...
- ❑ ... then the object must have been created by the legitimate holder of the addresses in the certificate
  
- ❑ What kind of signed objects?
  - Route Origination Authorizations
  - RPKI Manifests

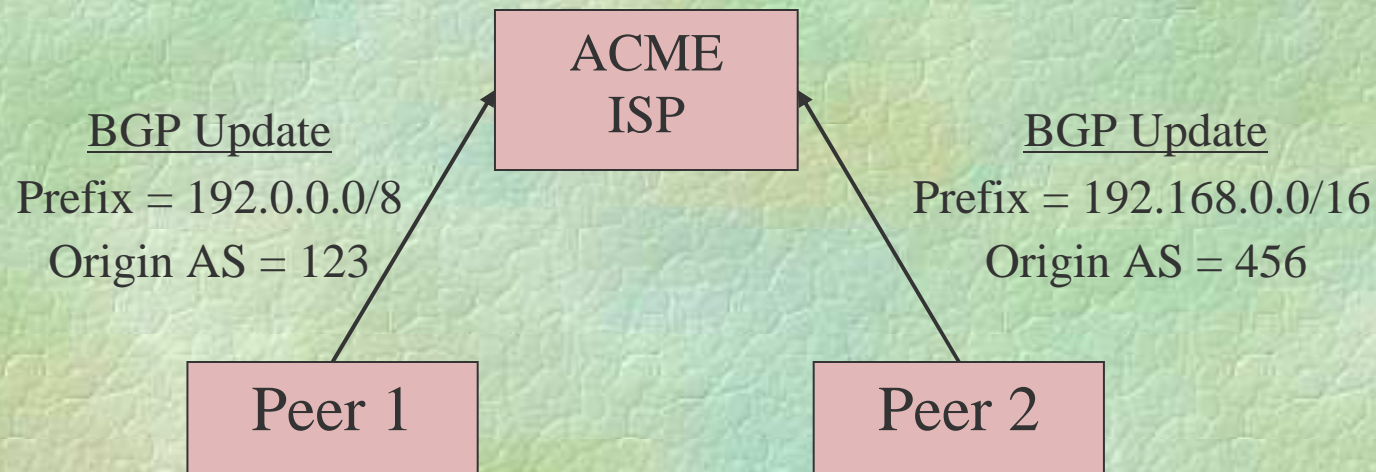
# ROAs: The Problem to be Solved

---



- ❑ ACME ISP receives two route advertisements that cover 4.10.0.0/16
- ❑ The BGP path selection algorithm prefers the advertisement for the more specific prefix
- ❑ In the absence of additional out-of-band information, ACME ISP would forward traffic to Peer 2

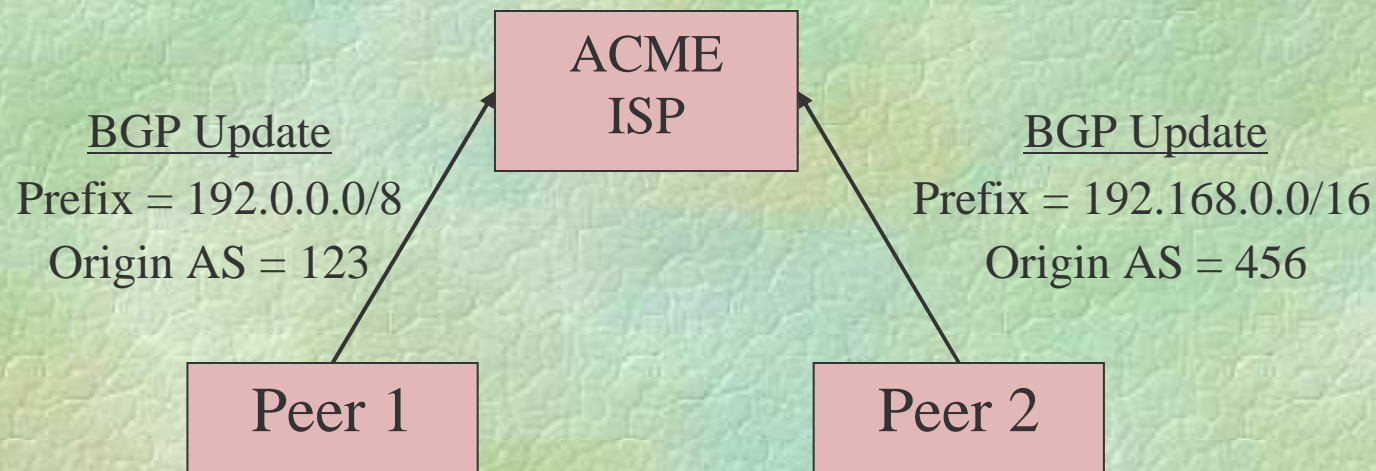
# ROAs: The Problem to be Solved



- ❑ Consider the case where:
  - 192.168.0.0/16 serves [www.youtube.com](http://www.youtube.com)
  - AS 123 is Google  
(the legitimate originator of this address space)
  - AS 456 is Pakistan Telecom  
(who emitted this advertisement due to accidental misconfiguration)
- ❑ Then ACME ISP will send its customer's YouTube traffic to Pakistan Telecom!

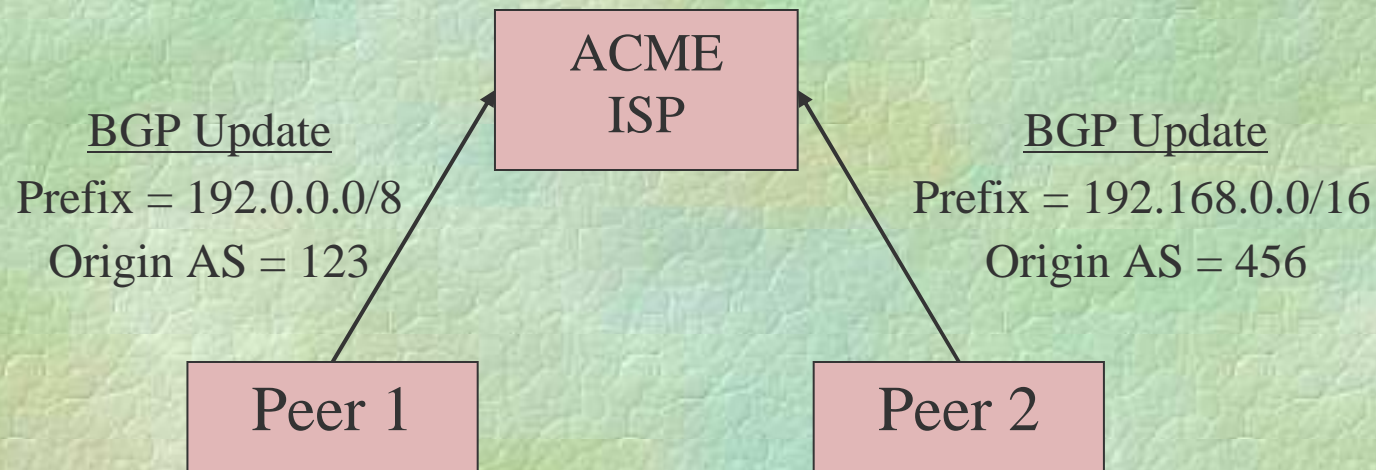
# ROAs: Overview of a Solution

---



- ❑ A ROA enables the legitimate holder of IP address space to state which AS(es) are authorized to originate routes to that address space
- ❑ Since a ROA is signed using an RPKI certificate, the recipient is assured that the statement was made by the legitimate holder of the address space in question

# ROAs: Overview of a Solution



- ❑ In this example, the legitimate holder of 192.0.0.0/8 would issue a ROA stating that AS 123 is authorized to originate routes to 192.0.0.0/8
- ❑ Upon validating the ROA, ACME ISP could, for example, choose to filter advertisements for 192.0.0.0/8 (or any subset thereof) originated by an AS other than 123.

# ROAs: What exactly is a ROA?

---

- ❑ A ROA uses Cryptographic Message Syntax (RFC 5652) to encapsulate the following data:
  - A set of IP address prefixes
  - An AS number
  - Digest and signature algorithms  
(ROAs currently use SHA-256 with RSA signatures)
  - A digital signature
  - An RPKI end-entity certificate

# ROAs: Issuing a ROA

---

- ❑ FooBar, a legitimate holder of IP address space has an RPKI CA certificate corresponding to its address space holdings
- ❑ To authorize AS 123 to originate routes to x.y.0.0/16, FooBar first issues an end-entity certificate (under its CA cert) such that:
  - The validity period matches the intended validity period of the ROA
  - The IP address extension matches the prefix to be originated
- ❑ FooBar then creates a ROA containing the prefix x.y.0.0/16, the AS number 123 and the new EE cert
- ❑ FooBar signs this ROA using the private key corresponding to the EE cert
- ❑ FooBar publishes the ROA in the RPKI repository system

# ROAs: Validating a ROA

---

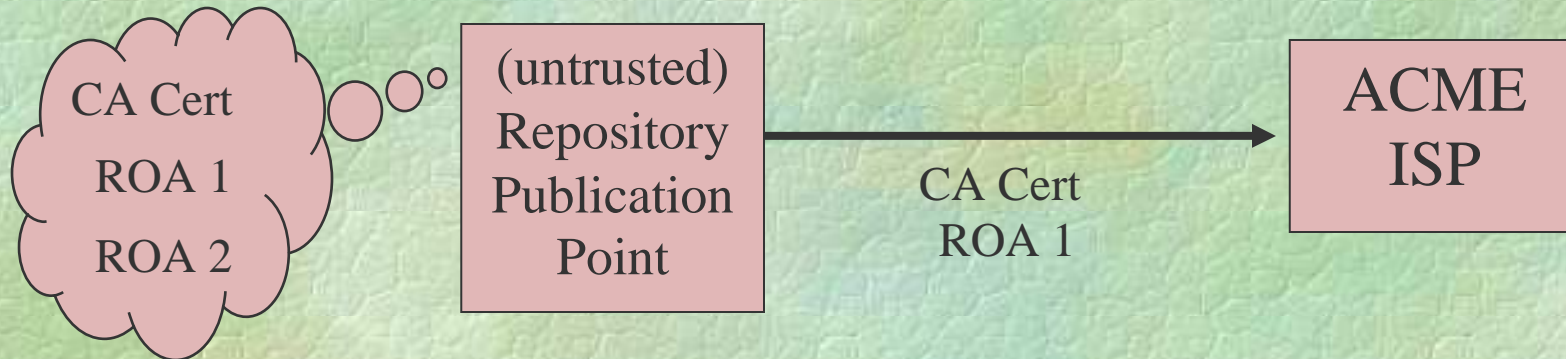
- ❑ Upon receiving a ROA, the recipient does the following to establish the ROA's validity:
  - Check that the ROA is a syntactically valid CMS object indicating appropriate digest and signature algorithms
  - Examine the enclosed EE certificate and check that the IP address extension in the cert matches the IP address prefix(es) in the ROA
  - Verify the signature on the ROA using the public key in the EE certificate
  - Check that the EE certificate is a valid certificate within the RPKI
- ❑ Note: This implies that a ROA can be revoked by simply revoking its EE certificate

# ROAs: Challenges for a Transition

---

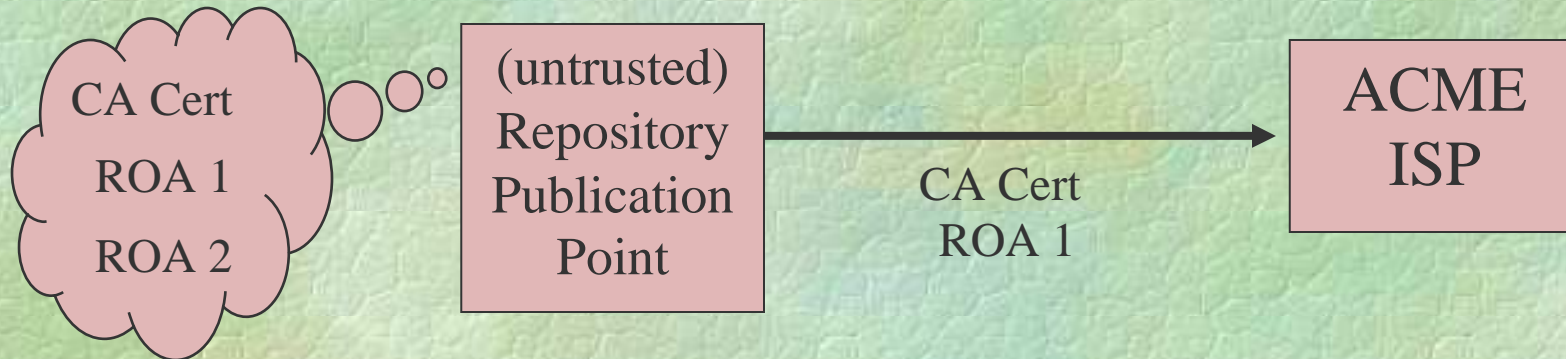
- ❑ ROAs work best when everyone is using them
  - I.e., if all IP address space holders participated in the RPKI then absence of a ROA implies that an advertisement is unauthorized
- ❑ During the (long) transition to full RPKI utilization, absence of a ROA could mean that the address space holder isn't using the RPKI
- ❑ For a given prefix, a ROA for AS 123 implies that the address holder is using the RPKI, thus no AS 456 should originate a route
- ❑ How do you know if an address holder uses the RPKI for prefixes that are not to be routed?
  - One option is to use a ROA for a “dummy” AS 0 to signal RPKI use

# Manifests: The Problem to be Solved



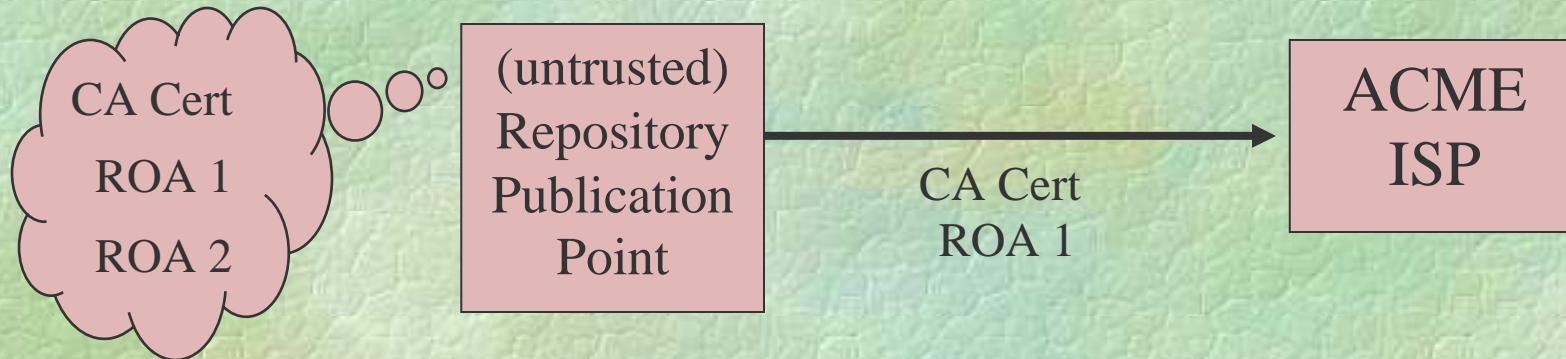
- ❑ A repository publication contains a CA certificate and two ROAs
- ❑ It is infeasible for a distributed repository system to be completely trusted (see DNS)
- ❑ Due to malicious attack on the repository system or the communication channel, ACME ISP does not receive ROA 2

# Manifests: The Problem to be Solved



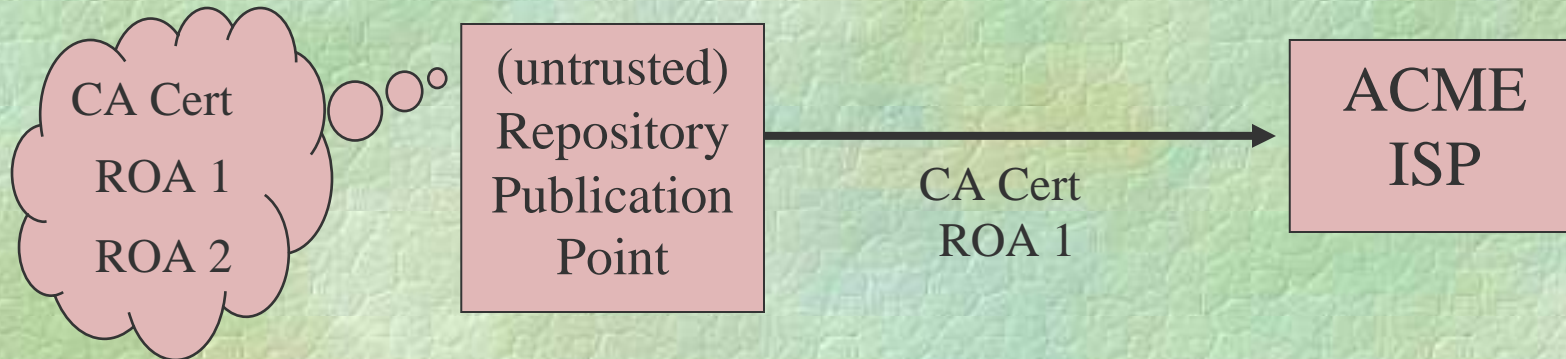
- ❑ ACME ISP has no way to determine that it has failed to receive the complete contents of the repository
- ❑ Thus, ACME ISP will treat the route authorized by ROA 2 as though it were unauthorized
- ❑ Similarly, failure to receive a new CRL could result in ACME ISP treating an unauthorized route as authorized

# Manifests: Overview of a Solution



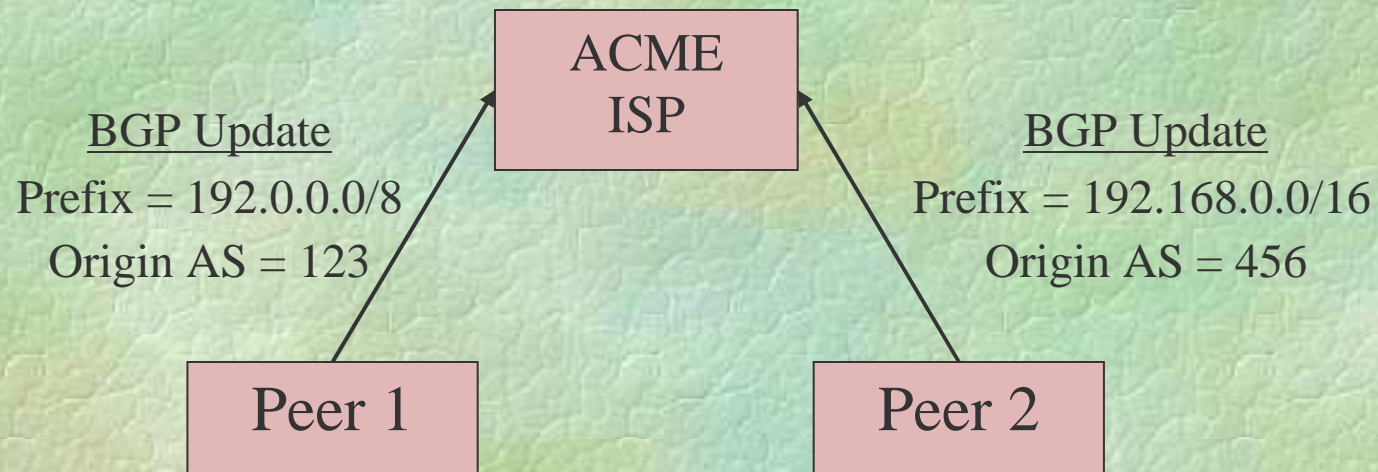
- ❑ A Manifest allows a CA to list all of the signed objects that should be present at its repository publication point  
E.g., ROAs, certs, and CRLs
- ❑ Since the Manifest is digitally signed, it cannot be modified or forged by a malicious party
- ❑ Enables the detection of attacks that corrupt the repository system as well as man-in-the-middle attacks

# Manifests: Overview of a Solution



- ❑ If ACME ISP receives a valid Manifest, it can determine that it failed to receive all of the ROAs issued by the CA
- ❑ If ACME ISP fails to receive a valid Manifest, it can also determine that a problem has occurred
- ❑ If ACME ISP receives a valid Manifest along with all objects listed on the Manifest, knows that it has the complete contents of the repository at the time of Manifest issuance

# Manifests: Overview of a Solution



- ❑ In this example, the legitimate holder of 192.0.0.0/8 would issue a ROA stating that AS 123 is authorized to originate routes to 192.0.0.0/8
- ❑ Upon validating the ROA, ACME ISP could, for example, choose to filter advertisements for 192.0.0.0/8 (or any subset thereof) originated by an AS other than 123.

# Manifests: What exactly is a Manifest?

---

- ❑ A Manifest uses Cryptographic Message Syntax (RFC 5652) to encapsulate the following data:
  - A list of all filenames of all objects issued by the CA
  - A hash of the contents of each of these files
  - Digest and signature algorithms  
(ROAs currently use SHA-256 with RSA signatures)
  - A digital signature
  - An RPKI end-entity certificate

# Manifests: Use of Manifests

---

- ❑ FooBar, a legitimate holder of IP address space has an RPKI CA certificate corresponding to its address space holdings
- ❑ Whenever FooBar changes the contents of its repository publication point (e.g., issues a new cert or ROA)
  - Revokes the EE cert associated with the previous manifest  
I.e., issues a new CRL that contains this EE cert
  - Issues a new EE cert corresponding to the new manifest
  - Constructs a new Manifest listing all valid objects (other than the new Manifest)
  - Signs the new Manifest using the private key associated with the new EE cert
- ❑ FooBar publishes the Manifest in the RPKI repository

# Manifests: Use of Manifests

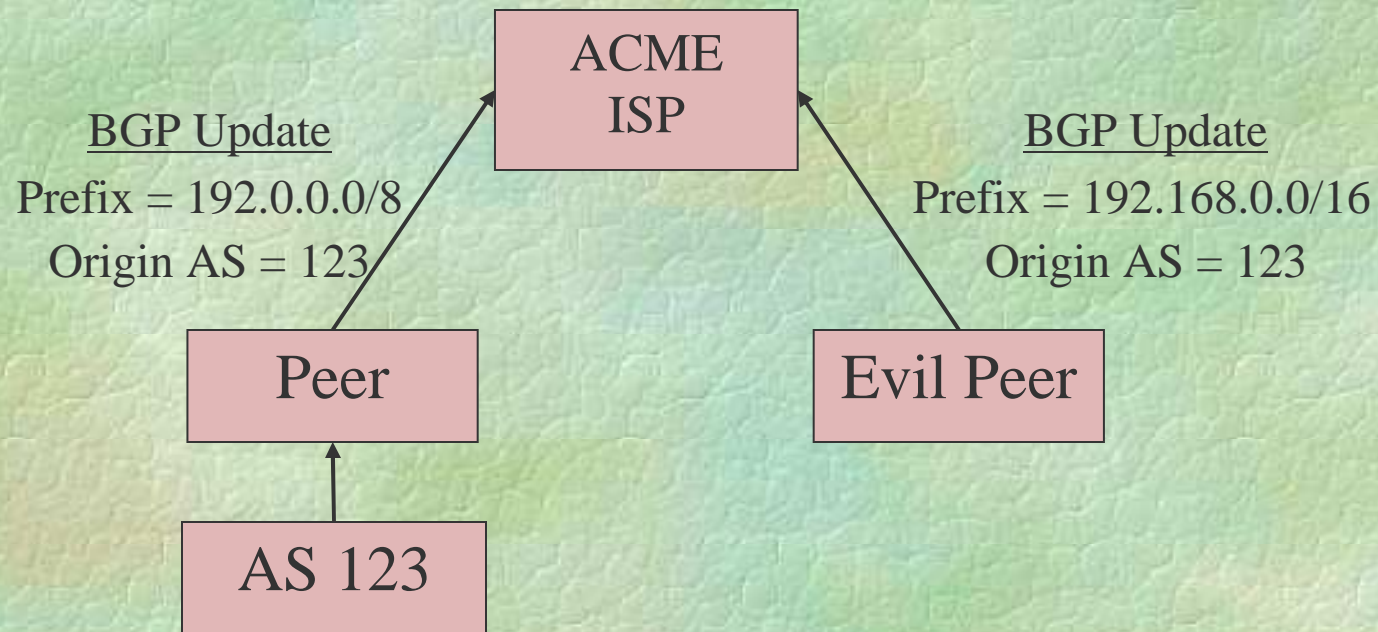
---

- ❑ FooBar, a legitimate holder of IP address space has an RPKI CA certificate corresponding to its address space holdings
- ❑ Whenever FooBar changes the contents of its repository publication point (e.g., issues a new cert or ROA)
  - Revokes the EE cert associated with the previous manifest  
I.e., issues a new CRL that contains this EE cert
  - Issues a new EE cert corresponding to the new manifest
  - Constructs a new Manifest listing all valid objects (other than the new Manifest)
  - Signs the new Manifest using the private key associated with the new EE cert
- ❑ FooBar publishes the Manifest in the RPKI repository

# ROAs and Manifests: Only the Beginning

- ❑ ROAs and Manifests are only the first examples of RPKI use:
  - Manifests can provide detection of attacks against the repository system
  - ROAs can provide protection against advertisements that are *originated* by an unauthorized AS
- ❑ What about invalid advertisements that contain the correct origin AS?
  - Further work is required to completely secure interdomain routing
  - But the RPKI is a necessary component of the solution

# ROAs and Manifests: Only the Beginning



- ❑ Evil peer forges an advertisement that was allegedly originated by AS 123
- ❑ ACME ISP has no way to know that Evil Peer did not actually receive the advertisement from AS 123

Thank You

