RSVP Cryptographic Authentication

F.Baker, B.Lindell, M.Talwar. January 2000,
IETF (Internet Engineering Task Force) RFC 2747

"...RSVP requires the ability to protect its messages against corruption and spoofing. This document defines a mechanism to protect RSVP message integrity hop by hop." - RFC 2747

Presented by: Colin Coghill
September, 2000.

Contents

* What is RSVP?

  When might we need it? How does it operate? What would we lose if we don't protect it?

* RSVP Authentication.

  Overview. Some details.

* Notes and Conclusions.

* Questions.

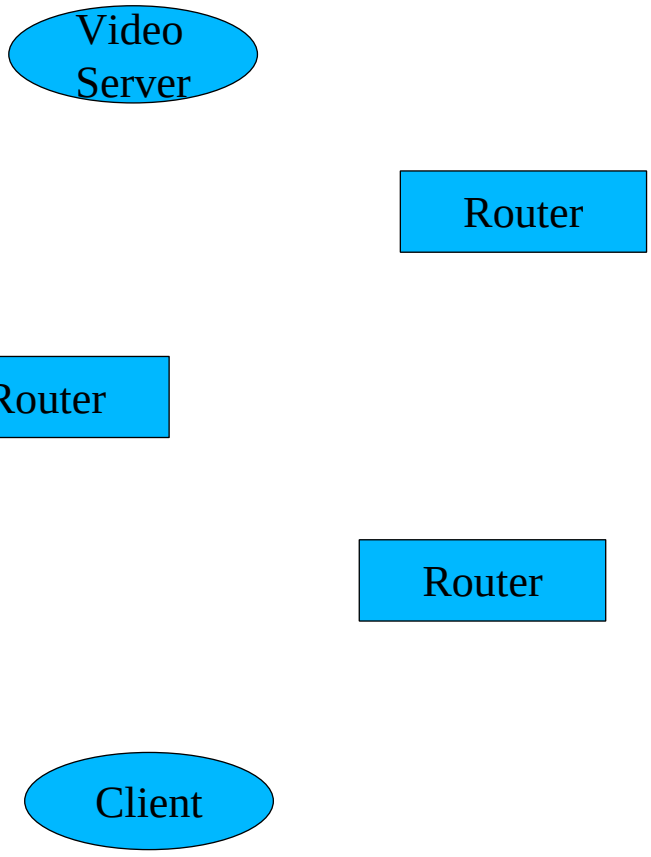
What is RSVP?

* Resource ReSerVation Protocol
* RSVP is defined in RFC 2205.

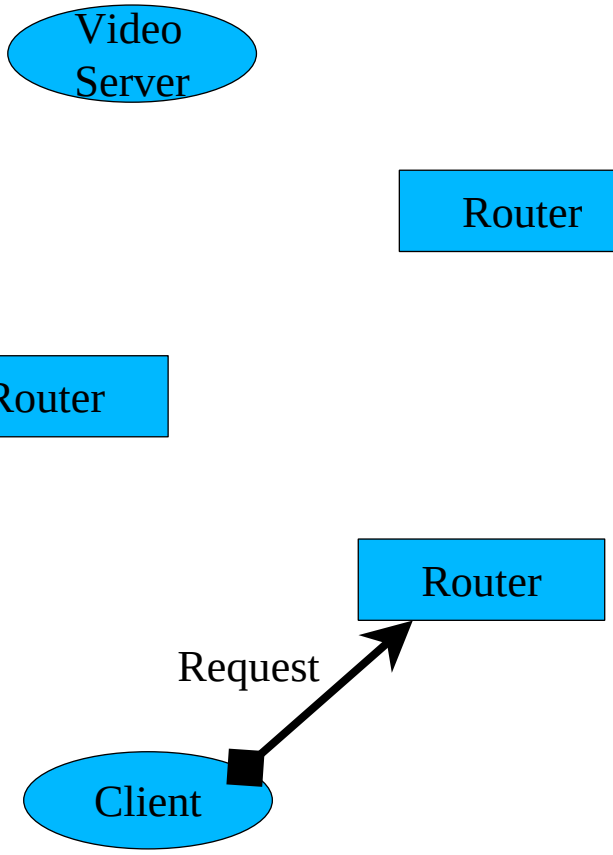
  "The RSVP protocol is used by a host to request specific qualities of service from the network..."

* It is an "Out of Band" signalling protocol.
* RSVP messages travel only in one direction.

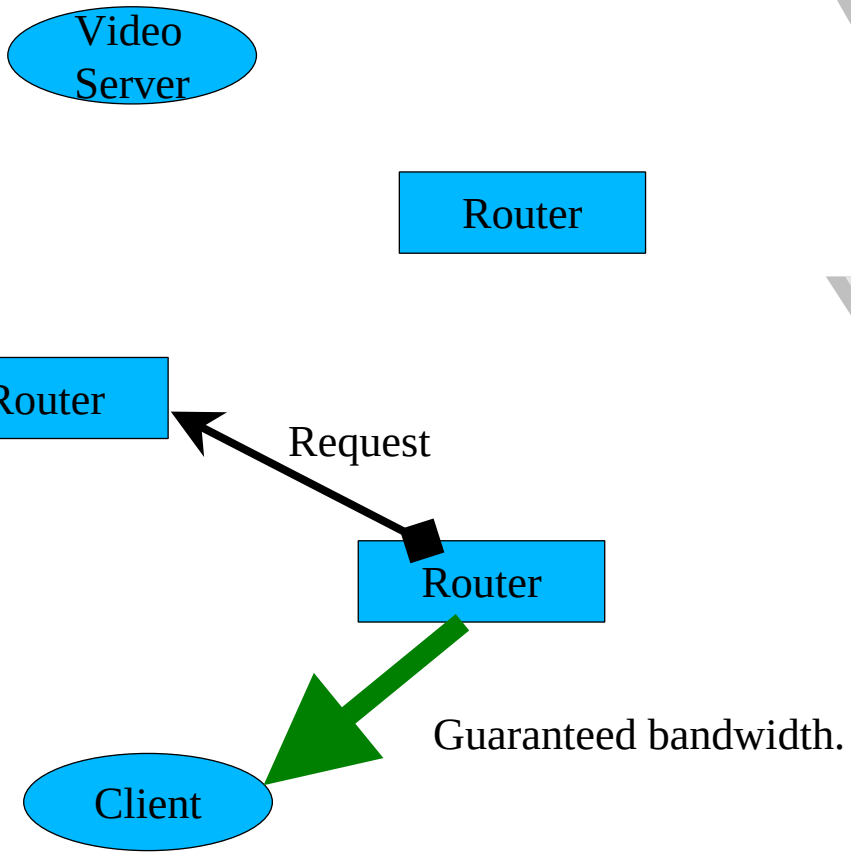
An RSVP Conversation



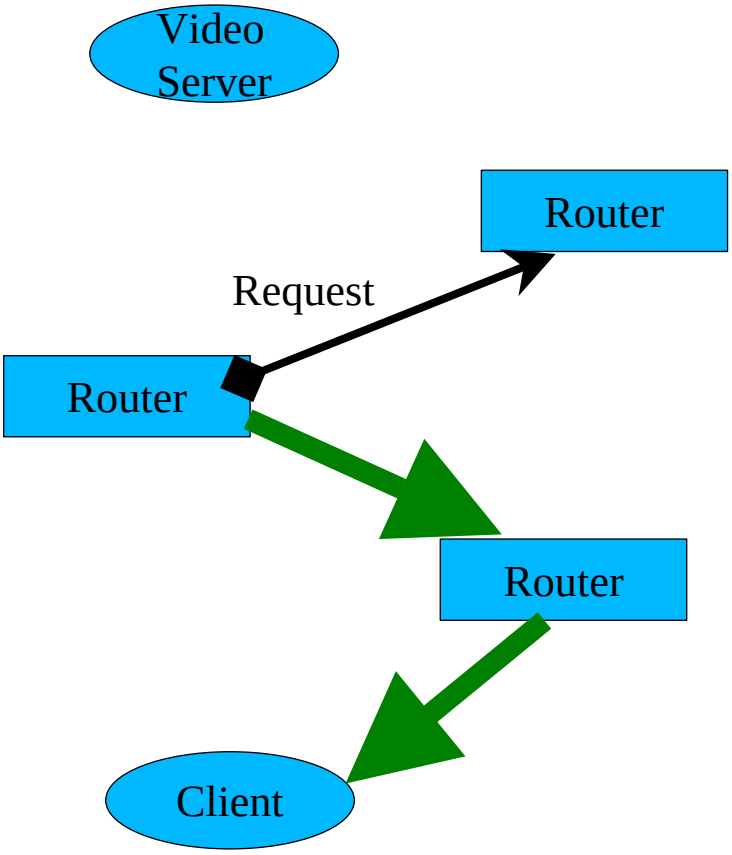
An RSVP Conversation



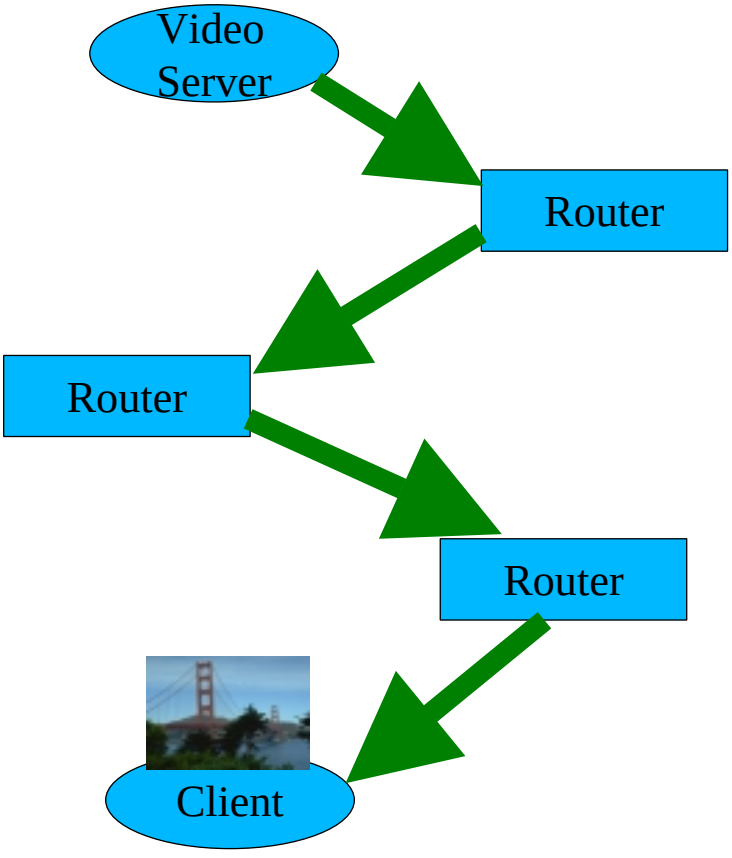
An RSVP Conversation



An RSVP Conversation



An RSVP Conversation



What is at risk?

What do we stand to lose if RSVP is successfully attacked?

* Network Resources.

  (Bandwidth, Real-time traffic, Reliability)

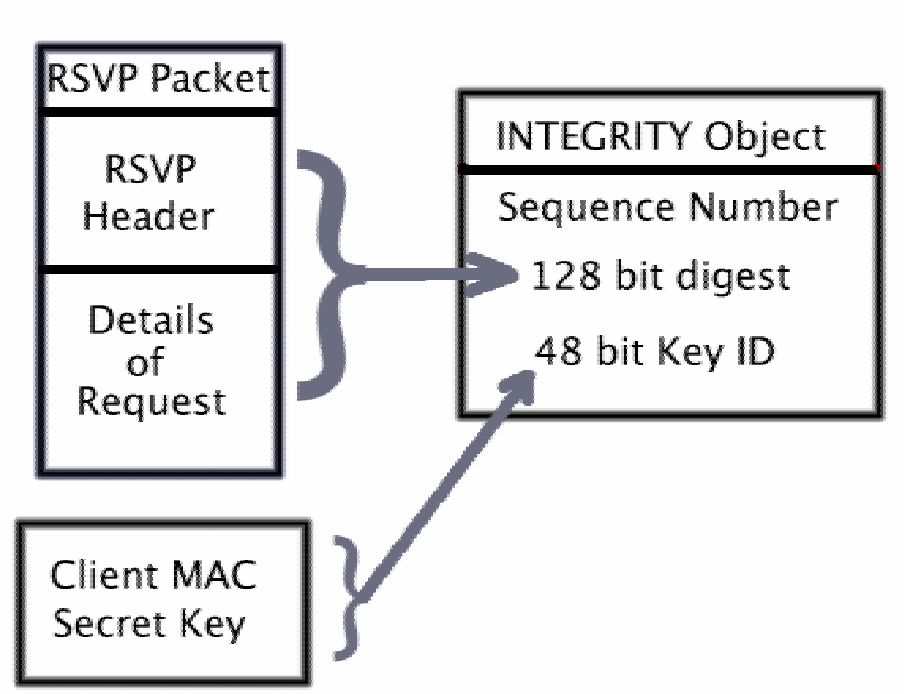
* Service or Quality.

  (A denial of service attack on a competitor might make them lose customers)

Authentication Overview

* RSVP Authentication gives us message integrity and node authentication.
* It leaves us with a choice of algorithms, although HMAC-MD5 is suggested.
* Both the message, and the authentication information are not confidential.
* If a message fails to authenticate, it will usually be ignored.

INTEGRITY Object



Sequence Number

* Provides protection from replay attacks.
* Can be any increasing value. eg. A counter, or maybe based on a realtime clock.
* 64 bit number. May wrap.
* The server should not accept out-of-order packets.

Notes

* RFC 2747 contains a lot of detail.
* It is expected that a standard key management system will be used.
* Receiver will ignore invalid messages, hoping that a correct one will be received before a timeout.
* IPsec wasn't chosen because it has issues with firewalls.

Conclusions

* I think the subject of network resource allocation will become important over the next few years.
* RSVP Authentication is protecting resources which are tempting for the amateur cracker to attack.
* While RSVP Authentication seems sensible and secure, I believe there may still be a way to attack RSVP itself.

Question 1

The RSVP Protocol will usually ignore packets that fail to authenticate correctly.

* Could this be abused by someone who can alter packets "on the wire"?

Question 2

I've included a summary of RSVP itself, whereas the main point of the presentation is supposed to be on a proposed authentication method for it.

* When evaluating a security method, should you spend much time investigating its environment?

* If so, how much?