Slide 1

SECURITY INFRASTRUCTURE FOR ACTIVE NETWORKS

Carl A. Gunter

Univerisity of Pennsylvania

Slide 2

Active Networks

- IP routers are based on a 'store and forward' model.
- Active routers are ones that extend this to a 'store, compute, and forward' model.
- It is hoped that a network based on active routers can evolve more quickly to provide new network services.

Slide 3

AN Design Spectrum

There are many questions about how far to go in providing programability for routers. Here are two extremes:

- Basic services are provided by routers which a packet may select. Such services are installed 'out of band' by switch owners.
- All packets are programs whose evaluation on the router *is* their routing. ('Capsules')

Slide 4

Sample Services

1. Safe routing: packets use a service that restricts the path that the packet may take.
2. Nice routing: packets seek to reduce load by using router or user communication state. Examples:
   - 'Drop me if you're busy'.
   - Video: 'drop me if another packet from my frame was dropped'.
3. Striping: packets in a single communication are dispatched over multiple output ports to increase effective bandwidth.

Slide 5

More sample services.

- Fusion or filtering of packet streams.
- Toll charges for packets: self-paying information transport.

Slide 6

Shared Resources

Since routers are shared resources, there are two key problems involved in increased flexibility:

1. Fair (or at least intended) resource allocation.
2. Security (privacy and integrity).

Slide 7

Models for Sharing

There are three possible approaches to sharing:

1. Anonymous general service.
2. Authentication (out-of-band 'payment').
3. Self-paying information transport (in-band 'payment').

It is very likely that the second option will be basic to a useful active network.

Slide 8

Security Assumptions and Strategy

1. Routers may be untrustworthy, but there will be very few security guarantees if untrustworthy routers are used.
2. Trustworthy routers should provide clear standardized guarantees about partitions between packets.
3. Experience from operating systems should provide guidance.
4. New ideas from programming languages and mobile code will be important.

Slide 9

Partition Issues

The issues involved in partition depend on the application:

- Safe routing: requests can be on a per-packet basis.
- Nice routing: nice video frames require flow-dependant state.
- Striping: basic resource allocation issues are involved.
- Maintenance: a wide range of privileges (per-user to root) may be required.

Slide 10

SwitchWare Project Approach

Three levels of privilege form the basis of our current approach to SwitchWare.

- 'Non-active' packets receive ordinary IP routing.
- 'Active' packets evaluate a limited 'wire' language. No authentication is used.
- Services are installed in a separate protocol. Authentication may be used in service installation or in packet use of the service.

Slide 11

Trust Management

- Pivotal to the development of an network-wide approach to authentication is a collection of programs that describe *policies* determined by hosts and routers.
- Public key cryptography could be the underlying technology.
- *Trust management* is a general term for the task of developing policies on a mass scale using trusted third parties.
- Sample current support for public key infrastructe: X.509.
- Other on-going efforts: PolicyMaker, SDSI, SPKI.

Slide 12

A SDSI Membership Certificate

```
( Membership.Cert:
  ( Member: ( Principal: q ) )
  ( Group: user )
  ( Reply: true )
  ( Signed:
    ( Object-Hash: ( SHA1 &345678 ) )
    ( Date: 1996-02-14T11:46:05 )
    ( Signer: ( Principal: p ) )
    ( Signature: &8dff4123 ) ) )
```

Slide 13

Semantics of Certificates

- Standard certificate formats are essential, but what one does with certificates defines their semantics.
- Deferred trust always runs risks of error (if a trusted third party makes an error).
- However, some basic consistency guarantees can be provided by policy-language semantics.
- Group definition languages also require interfaces to other software: our approach is based on *distributed database* languages and techniques.
- We need a language for dealing with distributed relations and authentication, that is: *queries* and *certificates*.

Slide 14

Information Integration

1. Data Warehousing.
2. Distributed Query Decomposition.
   (Information Manifold and TSIMMIS Projects)
3. Query Certificate Managers.
   (Joint work at Penn with Trevor Jim and Bow-Yaw Wang.)

Slide 15

Data Warehousing

[Hand-drawn picture omitted from online version, sorry!]

Slide 16

Distributed Query Decomposition

[Hand-drawn picture omitted from online version, sorry!]

Slide 17

Query Certificate Managers

QCM's differ in three respects

1. Recursive decompostion of queries.
2. Queries and responses are signed.
3. Certificates can be supplied along with queries.

Slide 18

A Sample QCM Application

[Hand-drawn picture omitted from online version, sorry!]

Slide 19

QCM System

We are beginning to build a QCM prototype.

- Java Remote Method Invocation (RMI).
- JDBC: SQL database access interface.
- Weak public key cryptography for certificates.

Slide 20

Conclusions

- Active networks will require an authentication infrastructure.
- Existing infrastructural systems need adapatation based on different assumptions.
- QCM's provide an essential element of the required infrastructure.