The X-Bone & its Virtual Internet Architecture
10 Years Later

Joe Touch, Greg Finn, Lars Eggert, Amy Hughes and Yu-Shun Wang

Workshop on Overlay and Network Virtualization
Kassel, Germany
March 6, 2009
Talk Outline

history

Virtual Internets
  why
  what
  architecture highlights

related projects at ISI (time permitting…)
  X-Bone, DynaBone, TetherNet
History

**X-Bone** was a series of research projects at USC/ISI
- X-Bone, DynaBone, TetherNet, X-Tend, NetFS, GeoNet, …
- 1997-2005+
- initial funding from DARPA, follow-on funding from the NSF
- [http://www.isi.edu/xbone/](http://www.isi.edu/xbone/)

**key results**
- an architecture (the “Virtual Internet” architecture)
- a deployment/management system (the “X-Bone”)

**follow-on work using virtual nets:**
- **DynaBone** spread-spectrum virtual networks
- **TetherNet** rent real Internet behind firewall + NAT
- **GeoNet** geographically-routed virtual networks
Prior & Related Work

new services & protocols
  Cronus, M/6/Q/A-Bone

multi/other layers
  Cronus, Supranet, MorphNet, VANs

partial solutions
  VPN, VNS, RON, Detour, PPVPN, SOS

virtualization, revisitation, recursion
  X-Bone, Spawning, Netlab/Emulab

OS virtualization
  VMware, jails, vserver, XEN, PlanetLab
Virtual Internet – Why

“network equivalent of virtual memory”

protection
  separate topology, optionally secured
  test + deploy new protocol/service

sharing
  increase utility of infrastructure

abstraction
  adapt topology to application
Virtual Internet – What

network = hosts + routers + links

virtual network =
  virtual host → packet src/sink
  + virtual router → packet gateway
  + virtual link → tunnel X over Y

virtual Internet – ”network of networks”
use Internet as physical media
create virtual link & network layers
strong L2 vs. weak L3 host model

a virtual Internet should look exactly like the real thing
“if an app can know it runs in a VI, we did it wrong
VI Architecture Feature – Recursion

virtual Internets on top of virtual Internets

our litmus test:
  system should be able to do recursive VI-in-VI without hacks

recursion has real uses cases
  e.g., allows transparent reconfiguration
      change outer VI w/o affecting inner fault tolerance, basis for DynaBone

also allows VI “embedding”
  “router is a network inside”
VI Architecture Feature – Concurrency

one node participates in multiple virtual Internets at the same time

basis for isolation & abstraction

bind different apps/VMs to different VIs on the same physical node
VI Architecture Feature – Revisitation

one node participates in the same virtual Internet but multiple times
allows creation of VIs larger than physical resources
fully decouples virtual from physical topologies
security in the Virtual Internet architecture is a virtual link property decoupled from topology transparently coexists with end-to-end security inside the VI transparently coexists with security underneath a VI

IPIP tunnels + IPsec transport mode modular tunnel mode equivalent huge IETF debate around 2000 (draft-touch-ipsec-vpn-05.txt)
The X-Bone System

deployment + management system for virtual Internets programs → standardized API 
humans → web interface

high-level virtual network description language express virtual topology + services XML

collaborating, distributed management daemons multicast expanding-ring discovery distributed resource reservation instantiate + manage virtual network

non-goals: topology optimization, non-IP VIs, …
X-Bone Screenshots

X-Bone Overlay Creation
You are logged in with these credentials (taken from your X509 certificate):

<table>
<thead>
<tr>
<th>Login</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Yu-Shun Wang</td>
</tr>
<tr>
<td>Location</td>
<td>Marina del Rey, CA, US</td>
</tr>
<tr>
<td>Organization</td>
<td>USC Information Sciences Institute, Div 7</td>
</tr>
</tbody>
</table>

This page allows you to create a new overlay. Please fill in all remaining red fields.

Overlay Wide Properties
Name of the new overlay. Prefix “bone.net” will be added automatically. If “use DNS” is checked below, the overlay name will also become part of the DNS name of your overlay nodes.

- Use DNS

Dynamically Routed
This option will determine whether to use Static Routing or Dynamic Routing with the overlay. Only dynamic routing with IPv6 running GEDiK is supported.

- Use Dynamic Routing

Application Deployment
This overlay has been set up. You need to specify the complete URL of the deployment script, e.g. http://example.com/deployment.sh.

- Application Deployment is still Experimental

Host Properties
Number of hosts in the overlay. Hosts are overlay nodes that do not route packets.

- FreeBSD
- Linux
- Solaris
- NetBSD

Host Operating System
Operating system requirements for the hosts. Only hosts of the checked operating systems will be picked for the new overlay.

- FreeBSD
- Linux
- Solaris
- NetBSD

Router Properties
Number of routers in the overlay. Routers are overlay nodes that route packets.

- FreeBSD
- Linux
- Solaris
- NetBSD

Router Operating System
Operating system requirements for the routers. Only routers of the checked operating systems will be picked for the new overlay.

- FreeBSD
- Linux
- Solaris
- NetBSD

Link Properties
IPsec encryption algorithm used to authenticate all overlay traffic.
IPsec encryption algorithm used to encrypt all overlay traffic.
Per-link transmission delay in milliseconds.
Per-link bandwidth limit.
Per-hop queue length limit.
Per-hop loss probabilities.

X-Bone Overlay Status
You are logged in with these credentials (taken from your X509 certificate):

<table>
<thead>
<tr>
<th>Login</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Yu-Shun Wang</td>
</tr>
<tr>
<td>Location</td>
<td>Marina del Rey, CA, US</td>
</tr>
<tr>
<td>Organization</td>
<td>USC Information Sciences Institute, Div 7</td>
</tr>
</tbody>
</table>

Overlay Parameters

- None

Authentication
- Dynamic Routing
- Dynamic Routing

Diameter
- Yes

Nodes

<table>
<thead>
<tr>
<th>Role</th>
<th>Resource Domain</th>
<th>Local Tunnel End</th>
<th>Remote Tunnel End</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>128.9.160.78</td>
<td>172.26.1.2</td>
<td>172.26.1.1</td>
</tr>
<tr>
<td>User</td>
<td>128.9.160.78</td>
<td>172.26.1.5</td>
<td>172.26.1.1</td>
</tr>
<tr>
<td>User</td>
<td>128.9.160.78</td>
<td>172.26.1.3</td>
<td>172.26.1.14</td>
</tr>
<tr>
<td>User</td>
<td>128.9.160.78</td>
<td>172.26.1.7</td>
<td>172.26.1.18</td>
</tr>
<tr>
<td>User</td>
<td>128.9.160.78</td>
<td>172.26.1.9</td>
<td>172.26.1.10</td>
</tr>
<tr>
<td>User</td>
<td>128.9.160.78</td>
<td>172.26.1.10</td>
<td>172.26.1.9</td>
</tr>
<tr>
<td>User</td>
<td>128.9.160.78</td>
<td>172.26.1.8</td>
<td>172.26.1.17</td>
</tr>
<tr>
<td>User</td>
<td>128.9.160.78</td>
<td>172.26.1.11</td>
<td>172.26.1.12</td>
</tr>
<tr>
<td>User</td>
<td>128.9.160.78</td>
<td>172.26.1.6</td>
<td>172.26.1.6</td>
</tr>
</tbody>
</table>

Back to the main X-Bone page.
X-Bone Status

current release: 3.2
  mature: 10 years of open source availability

platforms: FreeBSD, Linux
  unofficial: NetBSD, Cisco

widely used (by 2003):
  UCL, UPenn, Aerospace, DOD Canada, Sinica Taiwan + more
Related Work at USC/ISI
DynaBone

parallel inner virtual networks = algorithmic & protocol diversity

spread-spectrum multiplexer, wrapped inside outer virtual network
TetherNet

issue: firewalls, NATs, clueless ISPs
broken end-to-end connectivity

solution: relocate real Internet subnet
real = routable IP + DNS + no fw + …
tunnel subnet from anchor router to tether router at remote site
TetherNet Features

true Internet behind NATs and firewalls
  IPv4 + IPv6
  multicast
  fwd/rev DNS
  traffic shaping
  802.11b AP
  secure: IPsec for traffic, X.509 for user auth
  web interface configuration

U.S. patent filed, talks with licensees
TetherNet Screenshots

TetherNet Rental

Required rental parameters:
- Rental Site: Marina del Rey, USA
- Subnet Size: [ ] hosts
- Access Code: 

Optional rental features:
- Relay Type: TCP, UDP, IPv4
- Local Port: [ ]
- Remote Port: [ ]
- Relay Encryption: [ ]

Optional advanced networking features:
- IPv6: [ ]
- Multicast: [ ]
- DHCP Server: [ ]

Start TetherNet Service

Rental Server Response

Rental information:
- Rental Server: anchor.postal.org <lars@isi.edu>
- Organization: USC/ISI, TetherNet
- Location: Marina del Rey, CA, US
- Local Time: Tue Sep 17 15:13:00 2002

Rented network block:
- IP Block: 206.117.27.16
- Size: 16

TetherNet properties:
- Rental Site: 198.32.16.91
- LAN Size: 206.117.27.16/28, 9 hosts, IP addresses 206.117.27.22 - 206.117.27.30
- DNS Suffix: tethered.net
- Tunnel Type: UDP (local port 35770, remote port 34213)
- DHCP Service: on, handing out the range from 206.117.27.22 to 206.117.27.22
- Tunnel Enterprise: njndael-cbc
- IPv4: on, allocated prefix is 3ffe:8251:17:27:16/64
- IPv4 Multicast: on

Check status:
- It may take several seconds to bring up the rental.
Other Projects

**X-Tend**

maintain + extend X-Bone as tool for research + education

**GeoNet**

geographically-addressed overlays

**NetFS**

access control for the network stack via a pseudo file system
THANK YOU!