The Active Network Design Space
Mini-conference, Paris, FRANCE
May 17th, 2000

Jonathan M. Smith
University of Pennsylvania
http://www.cis.upenn.edu/~jms
Outline: the Design Space

- Usability vs. Flexibility vs. Security vs. Performance
- There may be unattractive tradeoffs, e.g., Performance and Security may be inversely related! (also Usability?)
- Usability and Flexibility can (mostly) be obtained with a general-purpose language such as Java, Caml or Forth
Active Network Architecture

- Application
  - Execution Environment (e.g., ALIEN)
  - Execution Environment (e.g., ANTS)
- Node Operating System (e.g., Nemesis, Scout, Linux, NT?)
Example: SwitchWare Architecture

- PLAN
- ALIEN/Caml/OS
- AEGIS
- PLAN Packet
- Caml Active Code

Node-Node Authentication
Recovery
Dynamic Integrity Checks
Static Integrity Checks
The ALIEN Approach

- Achieved by restricting a general computing model
- Realized in ALIEN, an active loader for Caml
  - General computing model
  - Interface to OS
  - Interface to active code
- Only privileged portions of the system can directly access shared resources
Decisions in the Design Space

- Usability vs. Flexibility vs. Security vs. Performance
- A General-Purpose Language gets the first two for free; other two are hard!
- Domain-specific Languages (such as PLAN) may achieve different tradeoffs
The ALIEN Active Loader

- D. Scott Alexander
- CAML runtime
- CAML capsules restricted via module thinning
- Digitally-signed certificates for remote accesses to resources
- Will use for detailed case study
ALIEN in an Active Element

- Three layer architecture
Implementation of Active Code

- **Active Extensions**
  - Loaded from disk or network (TFTP)
  - We use queues for communication
  - Could use upcalls...
    - Security?
  - ...or blocking downcalls

- **Active Packets**
  - ANEP encapsulated (over UDP or link layer)
  - Can use SANE for security
  - Linker/ procedure call for communications
Active Packets in ALIEN

- If ANEP header indicates ALIEN
  → SANE processing as part of ANEP
  → Code portion is loaded
  → func is called with code, data, and func name as arguments
saneping Performance

The graph shows ping times in usec plotted against trial number. The trend indicates an increasing ping time with each trial, suggesting a performance degradation over time.
Overall Breakdown of Costs

- Information gathering: 10%
- Marshaling: 16%
- Authentication: 25%
- Transmission related: 4%
- Caml overhead: 20%
- Kernel/wire: 26%
Major Costs

- Kernel/Wire (26%, 3078 µs)
  - Kernel time + transmission time
  - To avoid
    - Reduce size of packet
    - Reduce or avoid kernel boundary crossing cost

- Authentication (25%, 2910 µs)
  - Mostly cost of performing SHA-1 (4 times)
Cryptography is expensive

- Implemented in C because too slow in Caml
- Times to hash 4MB of data

<table>
<thead>
<tr>
<th></th>
<th>bytecode</th>
<th>native</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caml Int32</td>
<td>86.45s</td>
<td>61.99s</td>
</tr>
<tr>
<td>Caml int</td>
<td>36.03s</td>
<td>2.48s</td>
</tr>
<tr>
<td>C</td>
<td></td>
<td>0.33s</td>
</tr>
</tbody>
</table>
The take-home lesson:

- Must reduce per-packet crypto costs:
  - Active extension amortizes costs
  - ANTS caching amortizes costs
  - Smaller packets (Dense CISC, à la BBN)
- Or, find another way to avoid crypto in the common case...
Packet Language for Active Networks (PLAN)

- Hicks, Kakkar, Moore, Gunter, Nettles
- Capsule-based approach
- CAML runtime
- Highly-restricted domain specific language (a safe “glue” language, like the UNIX shell), extensible via ALIEN
- Active extensions do restricted things
The Programmable Protocol Processing Pipeline (P4)

http://www.cis.upenn.edu/~boosters
The P4 illustrates

- A restricted programming environment
  → Field-programmable gate arrays
- Very high performance; operates at OC-3c line rate with a 19.44Mhz clock
- Easily reaches to 300-400 Mbps with increases in clock rate and word size
- Can be integrated with software EE
  → A high-performance active HW/SW hybrid
Some Performance Tradeoffs

Flexibility of System as demonstrated

155 Mb/s
100 Mb/s
80 Mb/s
60 Mb/s
16 Mb/s

P4
PAN
PLAN
ALIEN
ANTS
Activation potential at various current line rates:

- POTS/ISDN
- T1
- 10M Ethernet
- OC3
- OC12
- OC192

Increasing Traffic Aggregation

More Nodes

Increasing Service Deployment Times

Increasing Preference for SW Restriction to Control Plane
Next Generation: in-Fiber A.N.

Register-Only Media Processor (ROMP)
Acknowledgments:

- All Penn work and most other work supported by DARPA ITO.
- Collaborators: Alexander, Arbaugh, Farber, Feldmeier, Gunter, Hadzic, Hicks, Keromytis, Marcus, McAuley, Menage, Moore, Nettles, Segal and Sincoskie...
- Hewlett-Packard, Intel and 3Com