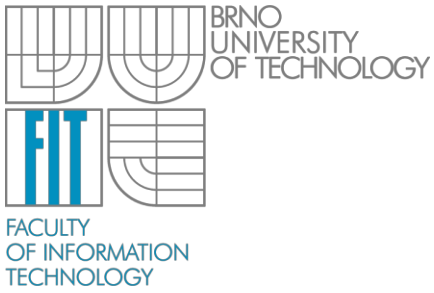
IEEE Transactions on Dependable and Secure Computing, Jan-Feb 2011

Michal Kajan

Fakulta informačních technologií, Vysoké učení technické v Brně,
Božetěchova 2, 612 66 Brno



TeamIT session

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

2011

The Geometric Efficient Matching Algorithm for Firewalls (Dmitry Rovniagin, Avishai Wool)

GEM – Geometric Efficient Algorithm

- algorithm from computational geometry
- time complexity: *O(d logn), n* is number of rules
- space complexity: $O(n^d)$, *d* is number of fields
- filtering based on 5-tuple (src+dst IP, src+dst port, protocol)
- testbed: Linux iptables filter, 1usec required for processing 1 packet
- Perimeter model – own ruleset generator

GEM – the algorithm

- every field is defined as a range of values
- every field represents a separate dimension in space
- overlapping ranges create *simple ranges* (in 1D max. 2n-1)

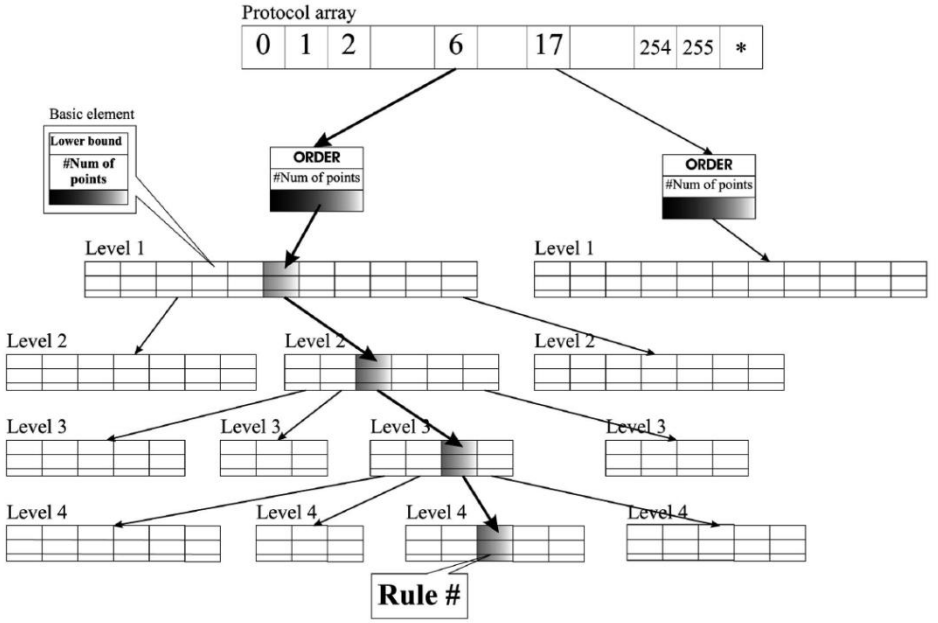
- one axe is selected and all the rules are projected to the given axe
- each simple range active rules are assigned
- process iterates till the last subdivision, where only winner rules exist

GEM – the data structure

- 3 parts:
  - array of pointers for each protocol (for protocol number)
  - protocol database header (contains order of data structure levels)
  - data structure itself
    - a cell specifies a simple range and points to the next level node
    - binary search for finding a simple range

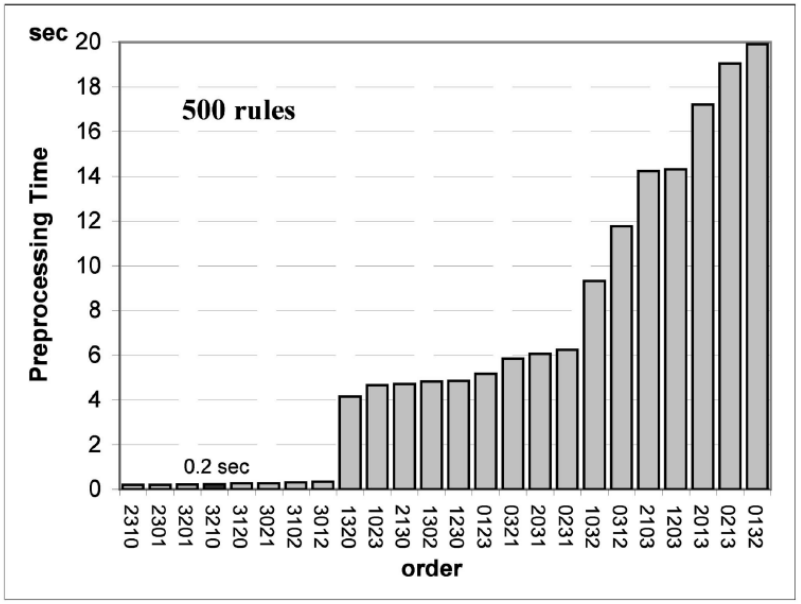
Header Field Numbering

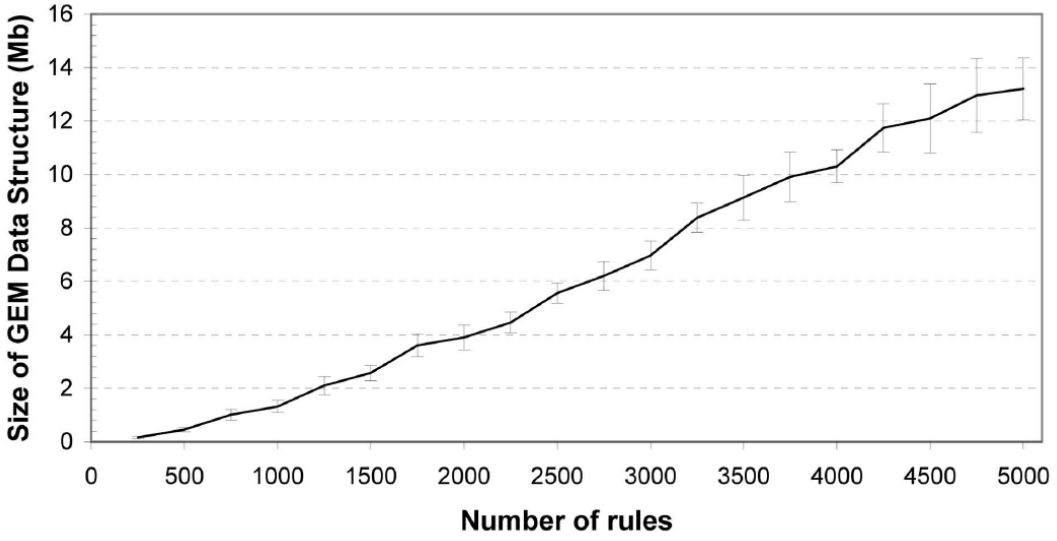
number	description	space
0	source IP address	32bit
1	destination IP address	32bit
2	source port number	16bit
3	destination port number	16bit
4	protocol	8bit



GEM – the build algorithm

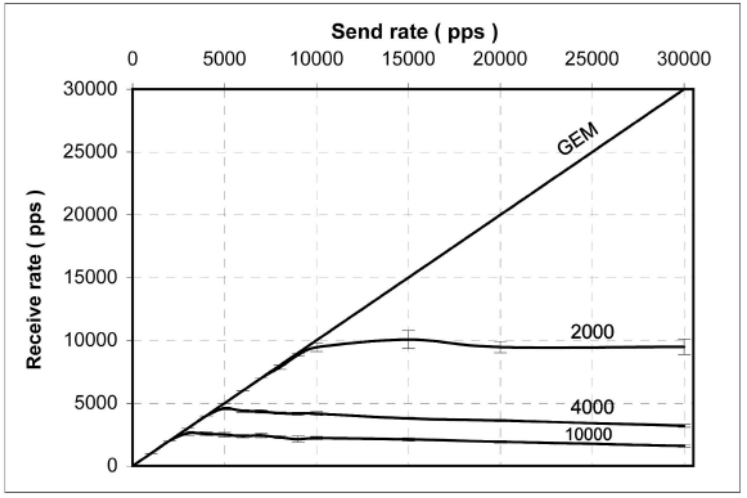
- executed for each protocol
- order of field determines the data structure levels and the search process
- used geometric-sweep algorithm (no details)
- field ordering impacts the size of data structure

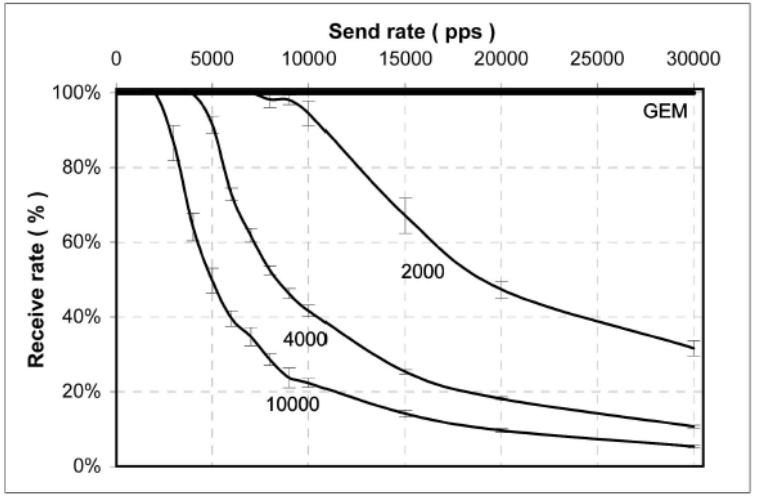




GEM – testbed

- implementation in C, Red Hat Linux 9, iptables
- firewall: 2.4 GHz Pentium 4, 512 MB RAM, 100 Mbps Ethernet interface
- packet generator: 700 MHz Pentium III, 396 MB RAM, 100 Mbps Ethernet interface
- generated 80-byte TCP packets, no TCP flags set
- comparison with iptables





GEM testbed (2)

- full (tested) throughput, max. 10 000 rules
- 30 000 packets/s ~ 19.2 Mbps (80B TCP each)
- unable to generate more packets
  - CPU bottleneck at packet generator PC – Perl script
  - estimated throughput: 100 000 pps

GEM – final notes

- Manuscript received 24 Dec. 2004
- revised 17 May 2006
- accepted 21 Apr. 2009
- published online 22 July 2009
- published in ToSDC: Jan-Feb 2011

Thank you for your attention!