Network Security

A Holistic Approach

Jun Li

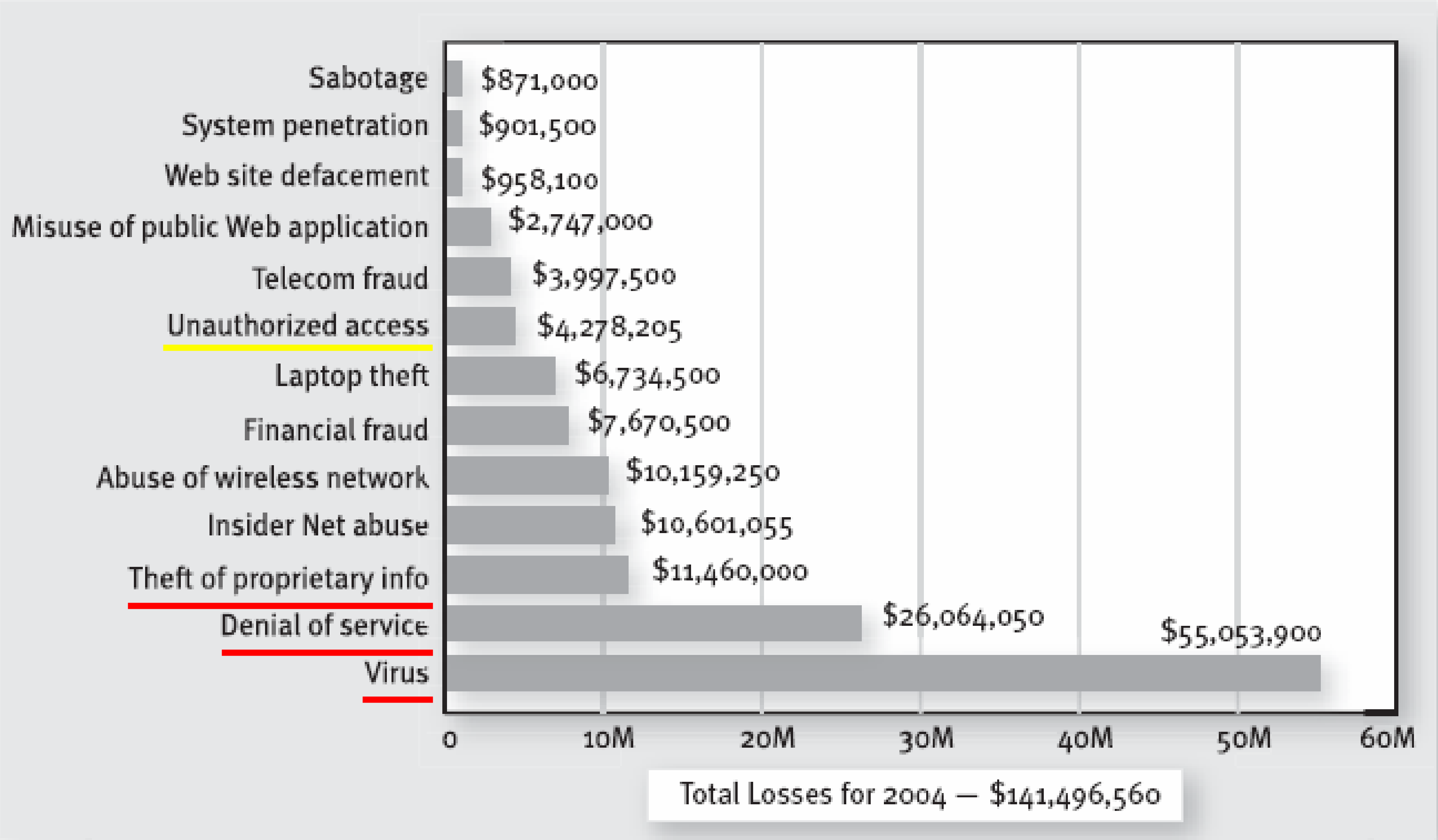
Tsinghua University

Outline

- Information Security Challenges
- Scope of Network Security R&D
- Market Demand & Technology Trend
- Holistic Approach: the Big Picture
- Integrate firewall and IDP: a Small Task

Information Security Challenges

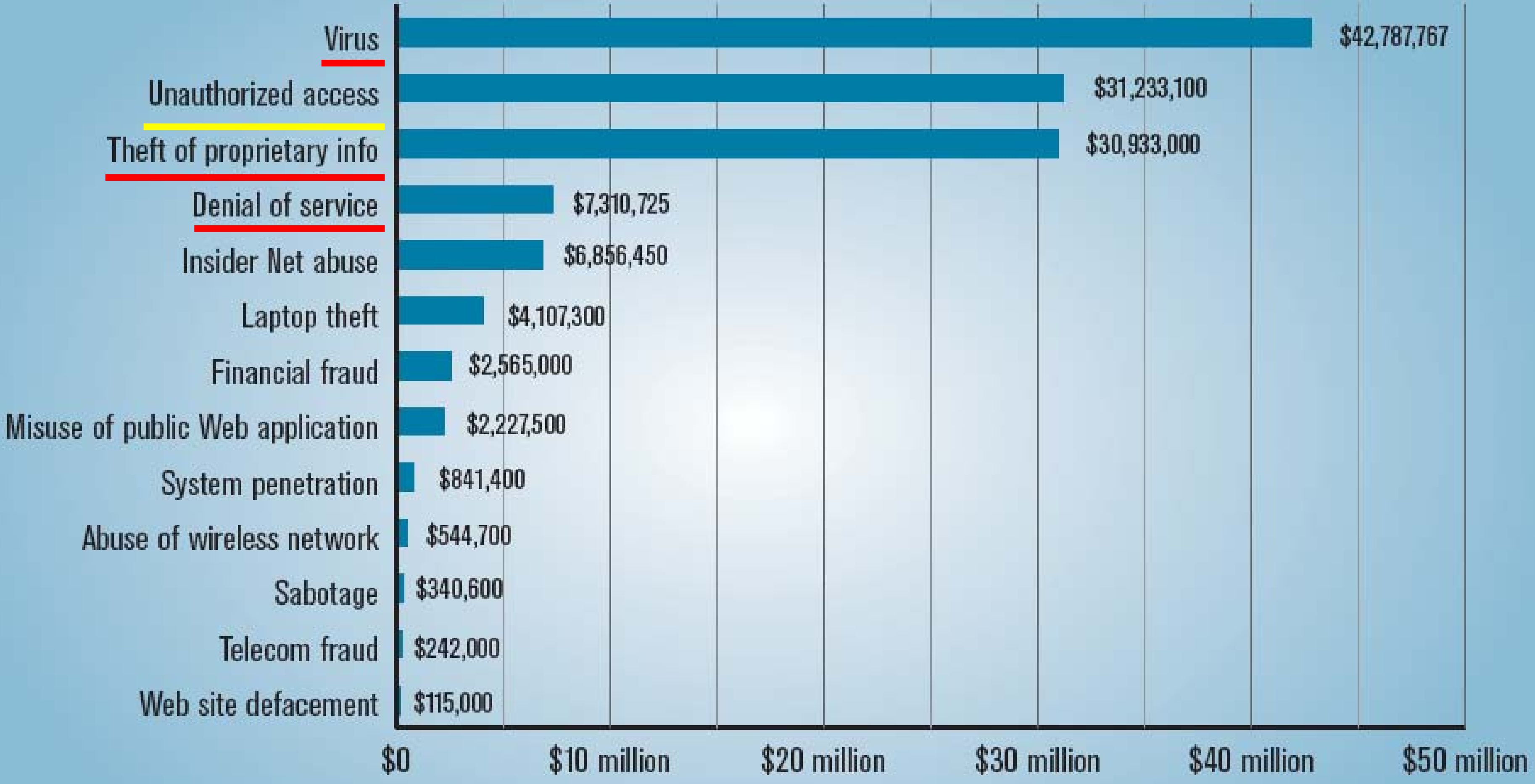
Information Security Survey '04



CSI/FBI 2004 Computer Crime and Security Survey
Source: Computer Security Institute

2004: 269 Respondents

Information Security Survey ‘05



Total Losses for 2005 were $130,104,542

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 639 Respondents

Information Security Challenges

- Malware (not an ideal classification)
  - Virus: (host-) dependent; (self-) replication
  - Worm: independent (or self-contained); replication
  - Trojan: independent; no replication
    - Communication/access tool: dropper of other malware, such as virus or spyware
  - Spyware/Adware: independent; no replication
    - Collection/advertisement tool: privacy/proprietary data/pattern collection; unsolicited advertising

McAfee reports

100,000th piece of known malware code, Sept. 2004 (18 yrs)
200,000th July 6, 2006 (2 yrs for the 2nd 100k malware code)

Information Security Challenges

- DoS & DDoS
  - Targeting weak point: “killer with silver bullet”
  - Gathering the troop: “organized crime”
    - Bot-net

Microsoft reports (February 2005 – June 2006)

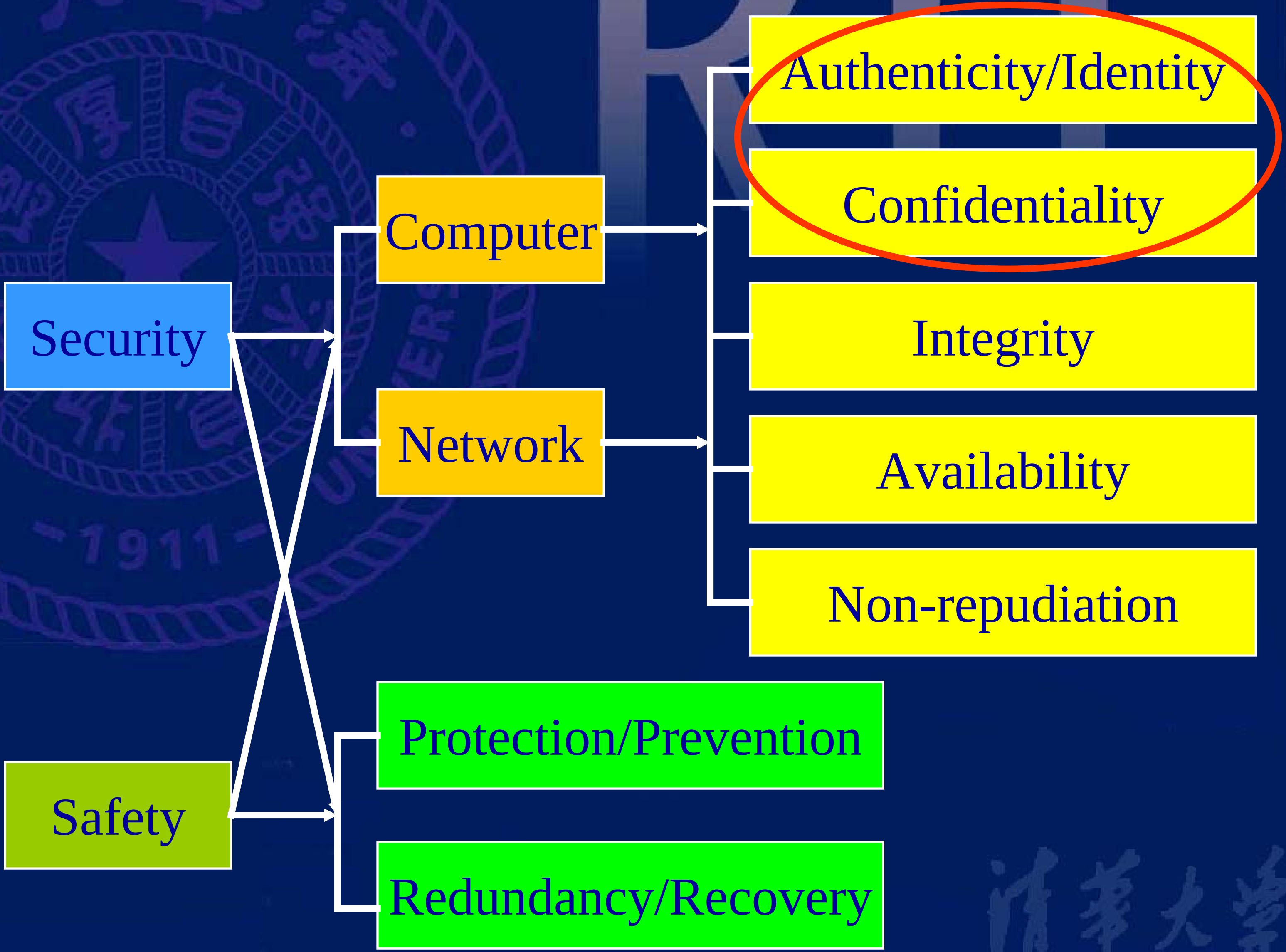
Among 5.7 million infected Windows machines, 62% with Trojan or bot, and top 3 most-removed malware families are bots.

- Theft of Propriety Info
  - Passive Leakage (Accessed by unauthorized)

    Active Leakage (Passed by authorized to outside of controlled areas)
  - Interface Level; Application Level; User Level

R&D Scope of Network Security

Information Security



Security

Safety

Computer

Network

Authenticity/Identity

Confidentiality

Integrity

Availability

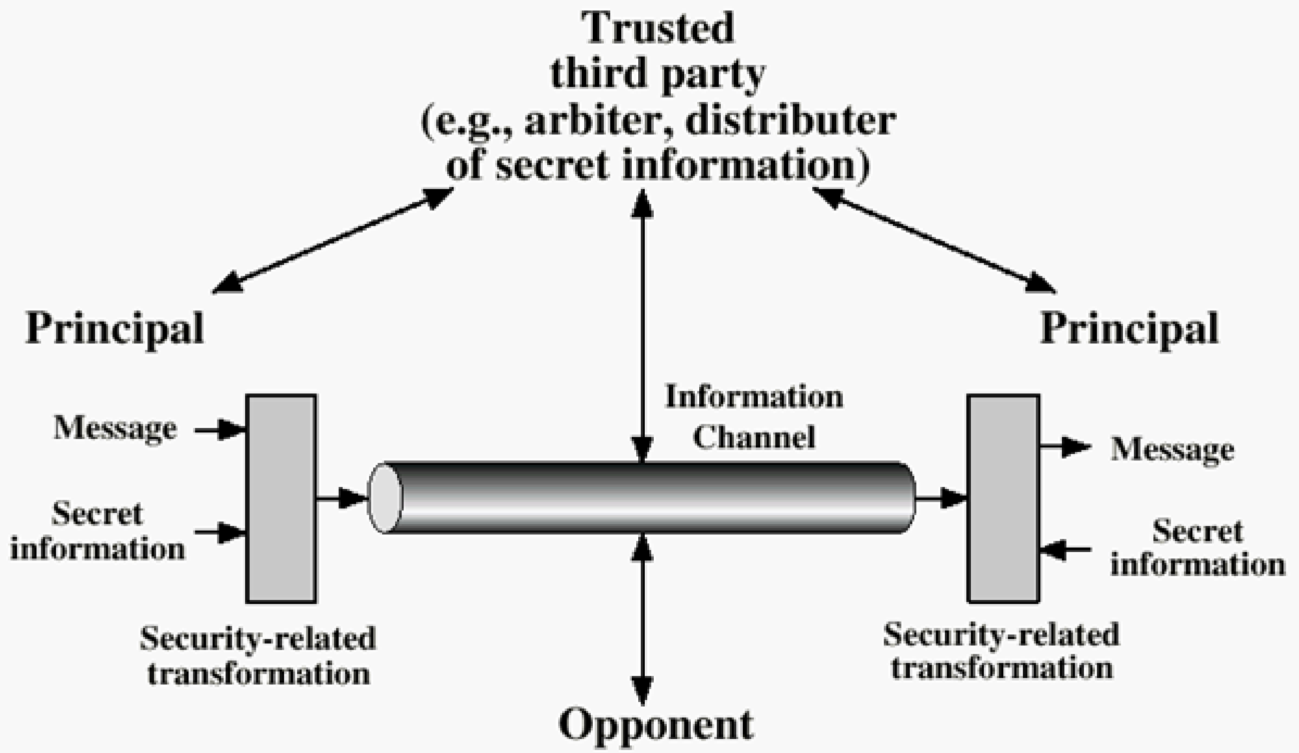
Non-repudiation

Protection/Prevention

Redundancy/Recovery

Network Security Models

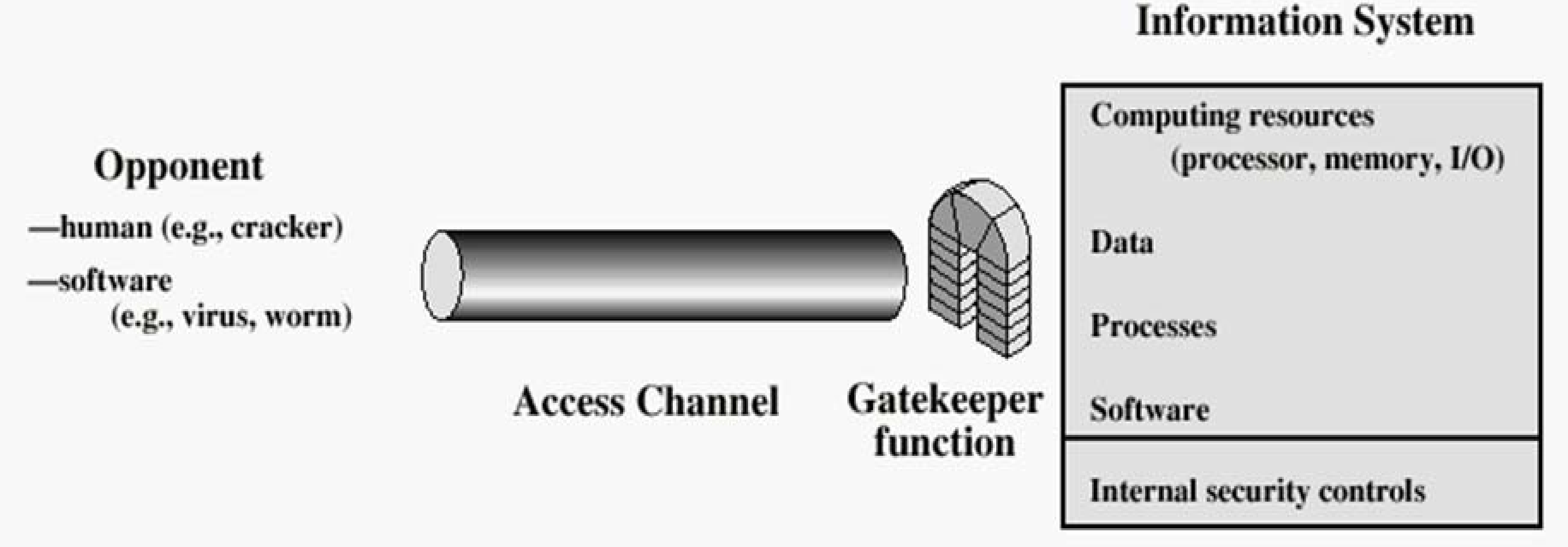
Information security issues in data transmission and/or by networking means.


Trusted third party (e.g., arbiter, distributer of secret information)
Principal
Principal
Message
Secret information
Information Channel
Message
Secret information
Security-related transformation
Security-related transformation
Opponent

William Stallings, Network Security Essentials: Applications and Standards, Principles and Practice (2nd Ed)

Network Security Models

Information security issues in data transmission and/or by networking means.



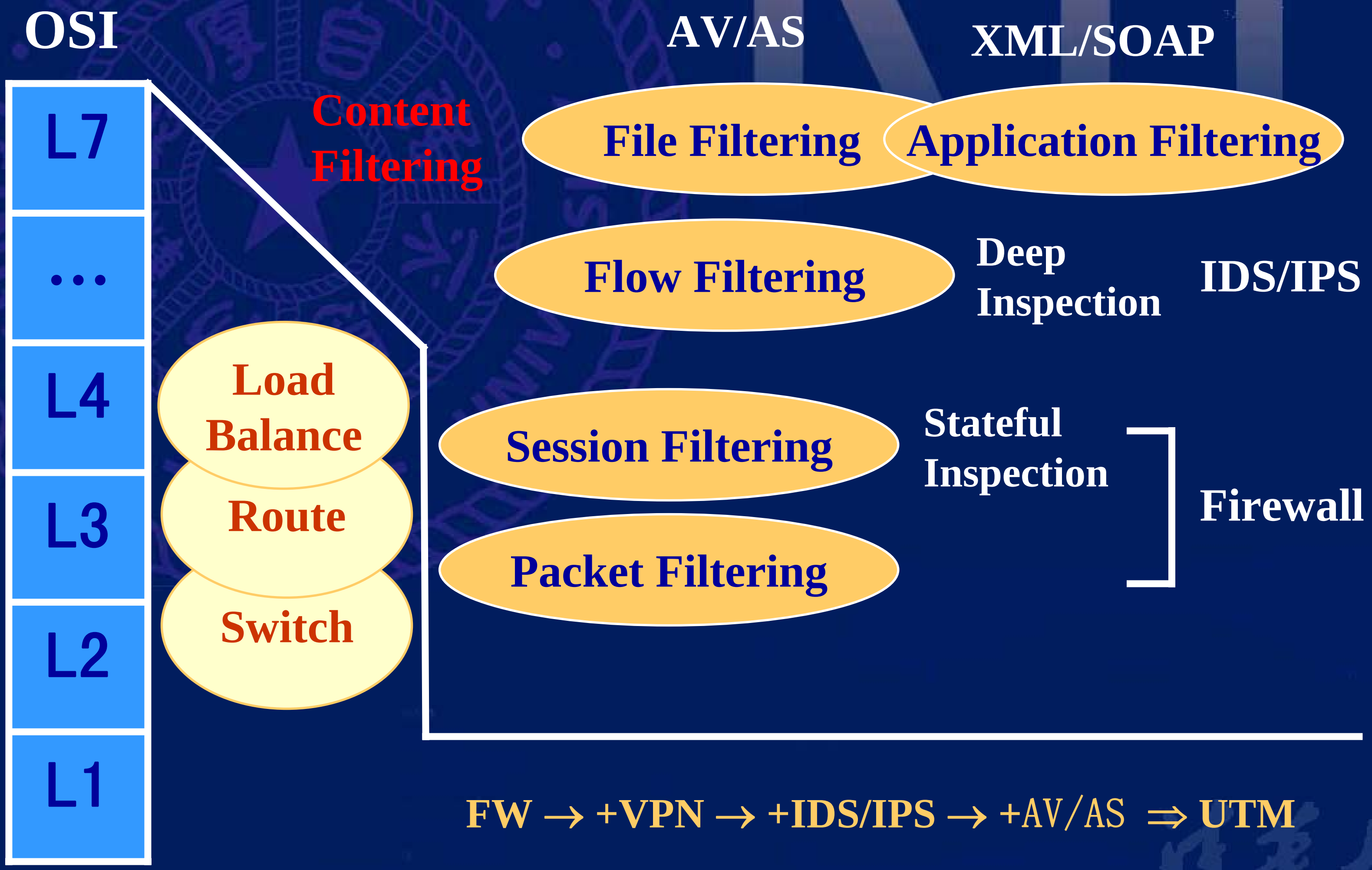
William Stallings, Network Security Essentials: Applications and Standards, Principles and Practice (2nd Ed)

Better Defense Demanded

- The “traditional” way of network security research cannot meet the ever renewed challenges
- A holistic approach is demanded to have all components participant in the overall defense
- Like “making CIA, FBI, FIMA, INS, and everyone else involved all work together” — hard but no other choice

Market Demand & Technology Trend

Network Security Gateways



OSI

L7

…

L4

L3

L2

L1

Content Filtering

AV/AS

XML/SOAP

File Filtering

Application Filtering

Flow Filtering

Deep Inspection

IDS/IPS

Load Balance

Route

Switch

Session Filtering

Stateful Inspection

Firewall

Packet Filtering

FW → +VPN → +IDS/IPS → +AV/AS ⇒ UTM

Three Firewall Generations

- 1G (early ‘90s)
  - Server-based (CPU) software solution
  - Simple functionality
- 2G (mid/late ’90s)
  - Appliances (ASIC) hardware solution
  - Firewall + VPN and anti-attack, traffic shaping, authentication, high availability
- 3G (now)
  - Modular (NPU/ASIC + CPU) hybrid solution
  - Firewall + VPN + NIDS + AV/AS and content filtering/switching, dynamic routing

Integrated Gateway for SME?

In-Stat/MDR report (2004)

- Over the next 12-24 months, a new breed of small business and branch office multi-service devices as the "Business Gateway" could be responsible for turning the networking equipment industry upside down with market size growing from $1.2 billion in 2004 to $16.6 billion in 2008.
- The Business Gateway will be a modular, standards-based device, offering high-availability, a wide variety of service modules, and integrated system management that meets the full spectrum of small and medium business applications as an “office-in-a box” device. Rather than being optimized for data networking, or as a security appliance, it will serve the entire data, security, and voice communications needs.

UTM vs Firewall/VPN

	2003	2004	2005	2006	2007	2008	2003 Share (%)	2003-2008 CAGR (%)	2008 Share (%)
Firewall/VPN	1,479.1	1,667.7	1,791.6	1,804.4	1,623.5	1,462.3	93.4	-0.2	42.4
UTM	104.9	225.0	517.5	828.0	1,324.8	1,987.2	6.6	80.1	57.6
Total	**1,584.0**	**1,892.7**	**2,309.1**	**2,632.4**	**2,948.3**	**3,449.5**	**100.0**	**16.8**	**100.0**

Source: IDC 2004

* CAGR = Compound Annual Growth Rate

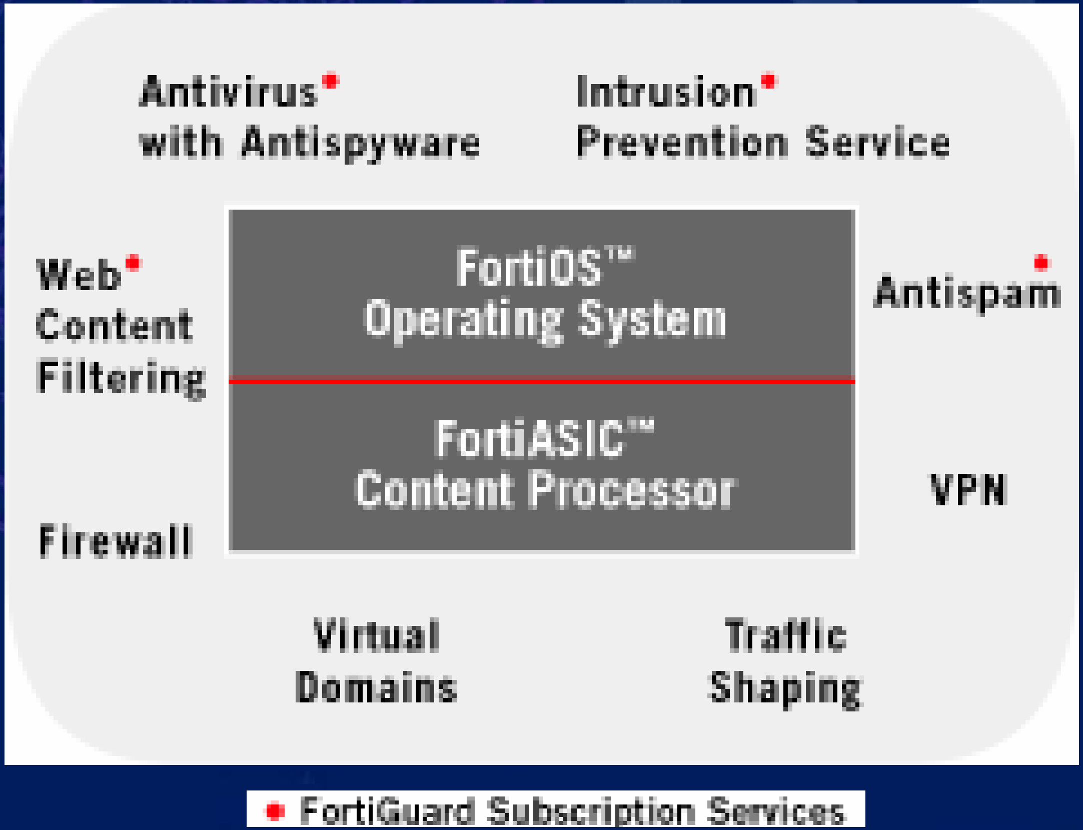
- <$1,000 UTM: CAGR 37%; ’08 share 26.9%; both #1
- $3,000-$5,999 UTM: #2 ’08 share 19.5% (CAGR 12.1%)
- >$50,000 UTM: #2 CAGR 36.8% (’08 share 14.5%)

The Battle for UTM Leadership

- From Fortinet, based on Q2’06 IDC report:
  - Fortinet was the fastest growing vendor quarter over quarter in the high-end UTM market ($50,000 and $99,900 price band segment), growing revenue at more than 300 percent quarter over quarter, while all other tracked competitors in this space - including Crossbeam -- had negative growth rates (or lost market share).
  - Fortinet is the fastest growing vendor quarter over quarter for unit growth in the mid-range UTM appliance segment (from $1,000 to $2,999 price band).
  - Fortinet also maintains its leading position in UTM in Western Europe and Asia Pacific (including Japan), based on strong revenues and success in all market segments.
- From Crossbeam (3COM), based on Q1’06 IDC report
  - Data contained in the IDC report showed that Crossbeam was No. 1 in sales and revenue among top security appliance vendors, including Fortinet, in the high-end UTM market for the fifth consecutive quarter. IDC defines this category as UTM products that cost at least USD 50,000 per unit.

The battle for UTM leadership

- Homegrown: “Best-in-Class”



Antivirus● with Antispyware

Intrusion● Prevention Service

Web● Content Filtering

FortiOS™ Operating System

FortiASIC™ Content Processor

Antispam●

Firewall

VPN

Virtual Domains

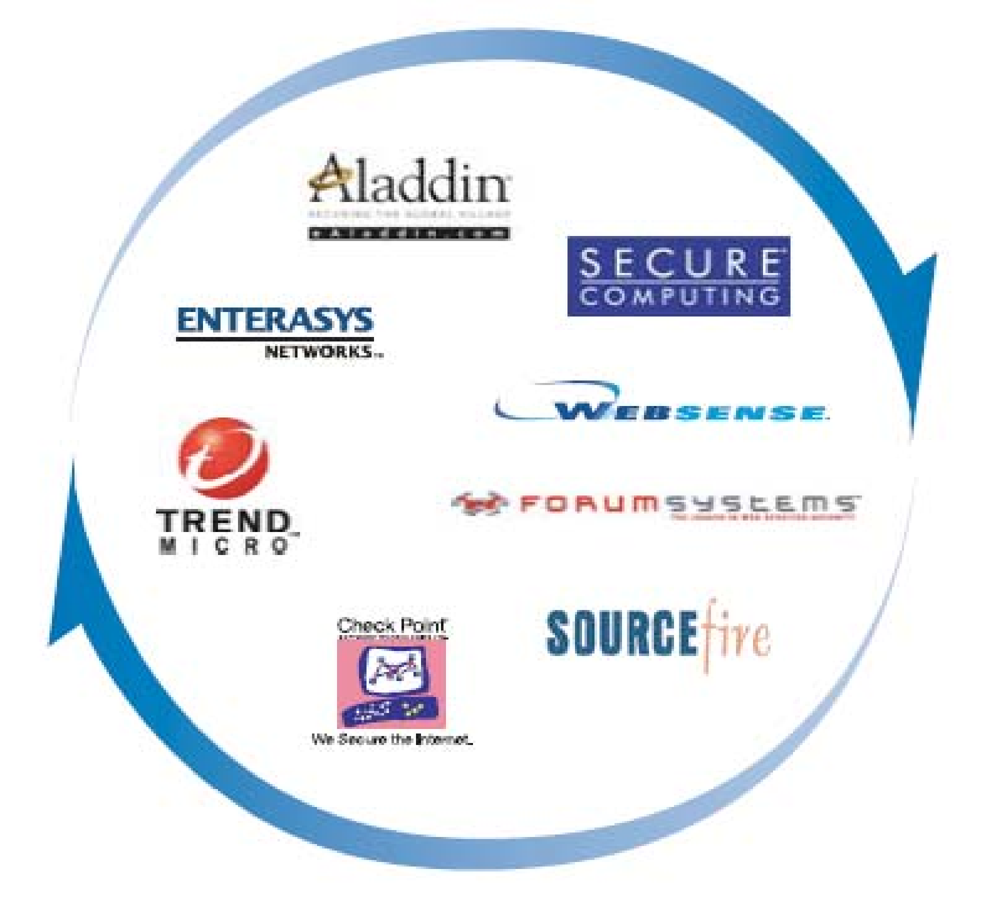
Traffic Shaping

● FortiGuard Subscription Services

http://www.fortinet.com

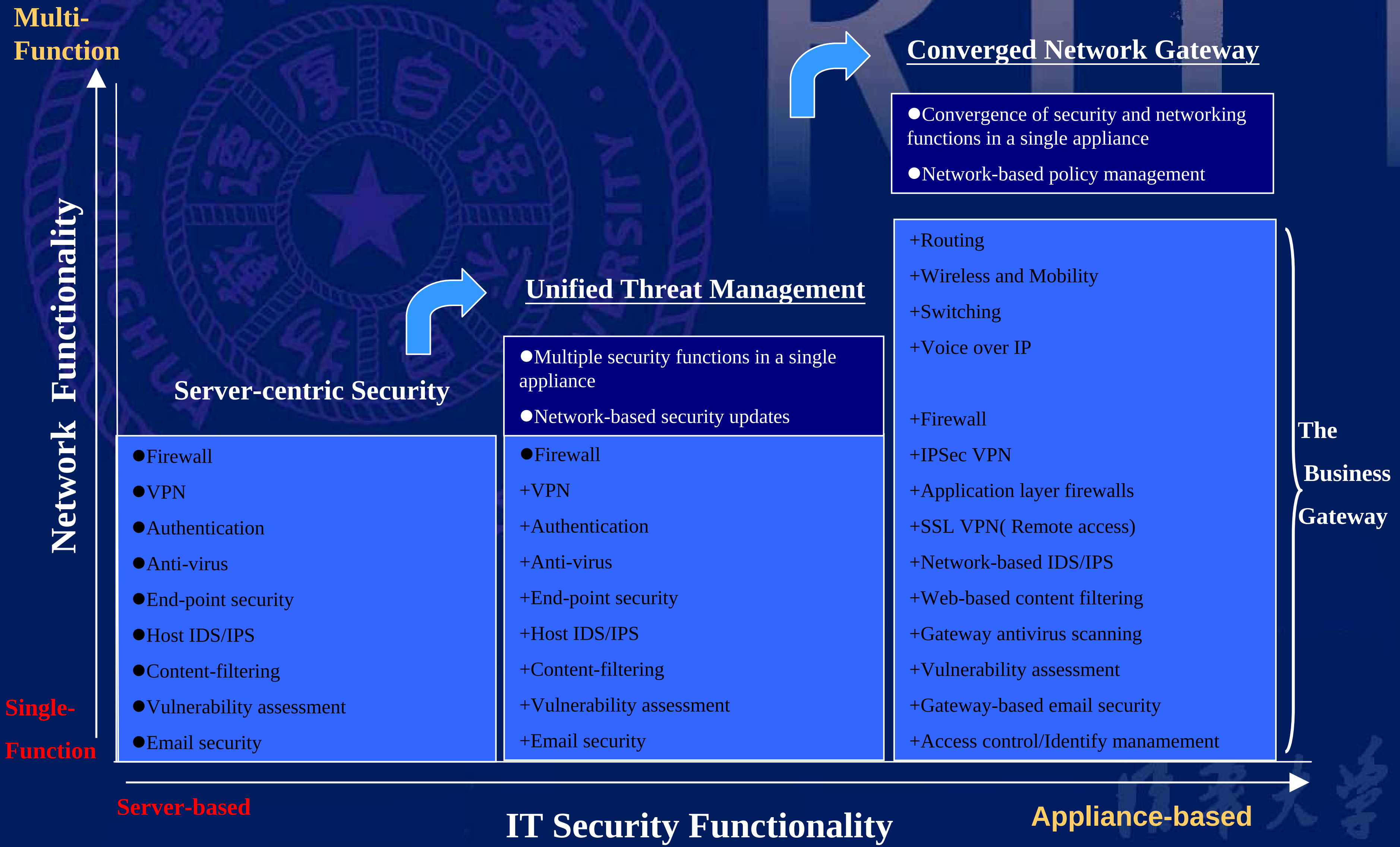
The battle for UTM leadership

- Platform: “Best-of-Breed”



http://www.crossbeamsystems.com

From UTM to Business Gateway?



Multi-Function

Network Functionality

Single-Function

Server-centric Security

- ●Firewall
- ●VPN
- ●Authentication
- ●Anti-virus
- ●End-point security
- ●Host IDS/IPS
- ●Content-filtering
- ●Vulnerability assessment
- ●Email security

Unified Threat Management

●Multiple security functions in a single appliance

●Network-based security updates

●Firewall

+VPN

+Authentication

+Anti-virus

+End-point security

+Host IDS/IPS

+Content-filtering

+Vulnerability assessment

+Email security

Converged Network Gateway

●Convergence of security and networking functions in a single appliance

●Network-based policy management

+Routing

+Wireless and Mobility

+Switching

+Voice over IP

+Firewall

+IPSec VPN

+Application layer firewalls

+SSL VPN(Remote access)

+Network-based IDS/IPS

+Web-based content filtering

+Gateway antivirus scanning

+Vulnerability assessment

+Gateway-based email security

+Access control/Identify manamement

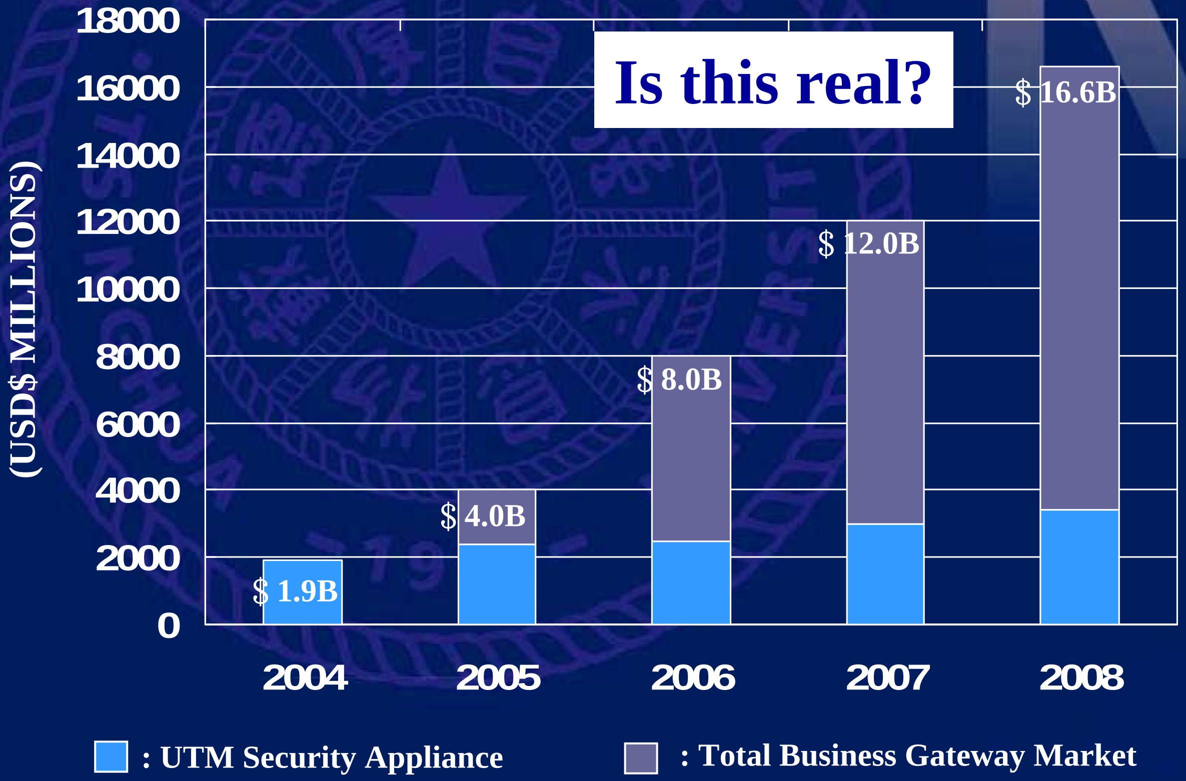
The Business Gateway

Server-based

IT Security Functionality

Appliance-based

Business Gateway Market ('04-'08)



Is this real?

- IDC forecasts the global Threat Management Market will exceed $ 3.4billion in 2008, representing a GAGR of 16.8%
- In-Stat/MDR forecasts broader Business Gateway market (including converged UTM, WLAN, VoIP appliances) will exceed $ 16.6 billion in 2008

IDC
Analyze the Future

In-Stat

"(We expect) UTM appliances to overtake conventional firewall/VPN devices in the near future. By 2007, 80 percent of security solutions will be delivered via a dedicated appliance."

-IDC,2004

"The Business Gateway could be responsible for turning the networking equipment industry upside down. Business Gateways will serve a small business entire data, security, and voice communications needs."

-In-Stat/MDR ,2004

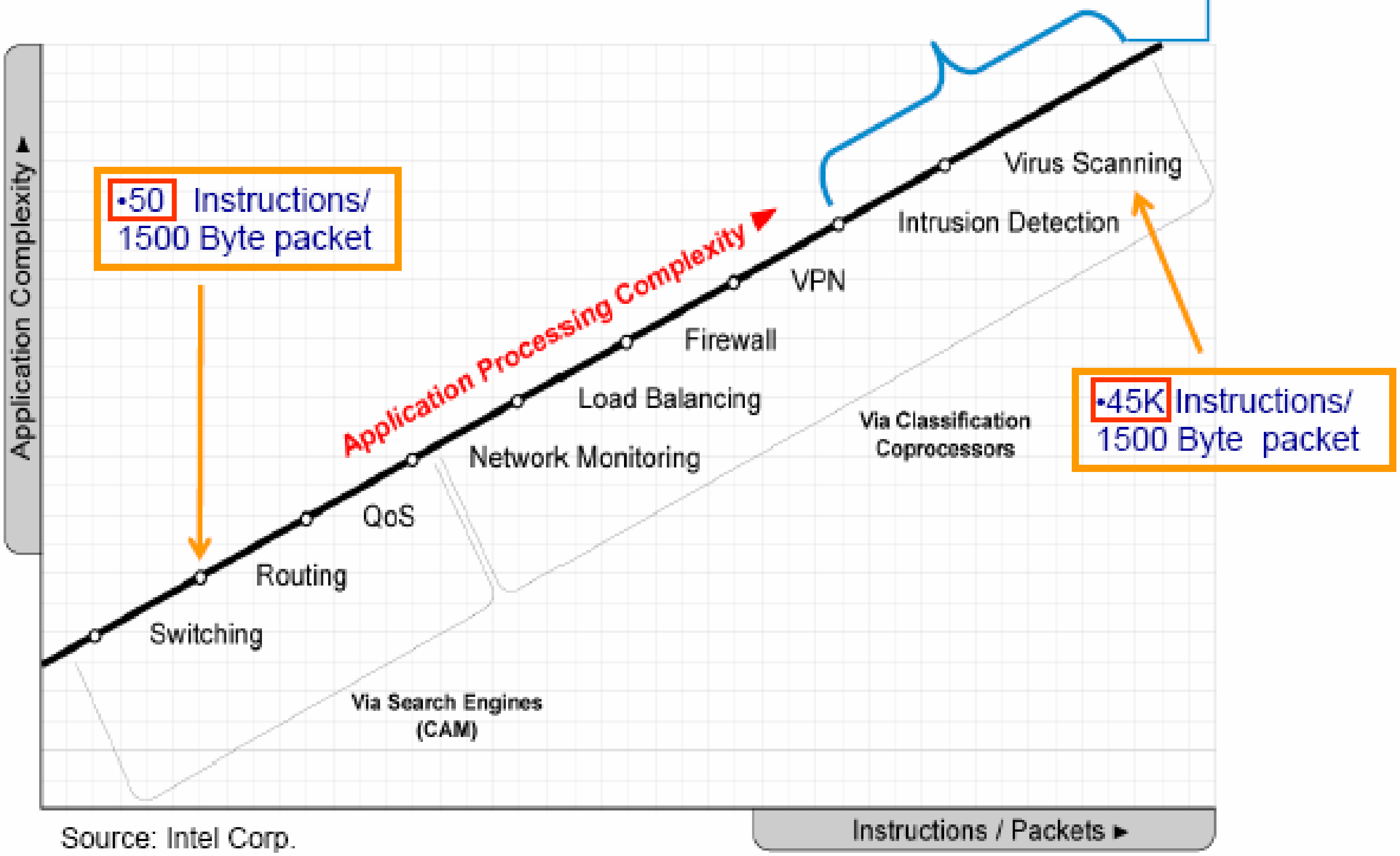
State-of-the-Art Firewall

- Low-end (Sub-Gbps)
  - From ASIC back to CPU/NPU
  - All layer 3G firwalling
- Mid-end (Multi-Gbps)
  - From ASIC to CPU+NPU
  - From 2G to 3G
- High-end (>= 10Gbps)
  - ASIC/NPU, multi-core, multi-processor
  - Stay at 2G with more lower layer functions

Holistic Approach: the Big Picture

New HW/SW Solutions Needed

- L7 (content) lookups ≈ 900 times of Layer-2/3/4 lookups
- Our solution overcomes this computing intensive task.



•50 Instructions/ 1500 Byte packet

•45K Instructions/ 1500 Byte packet

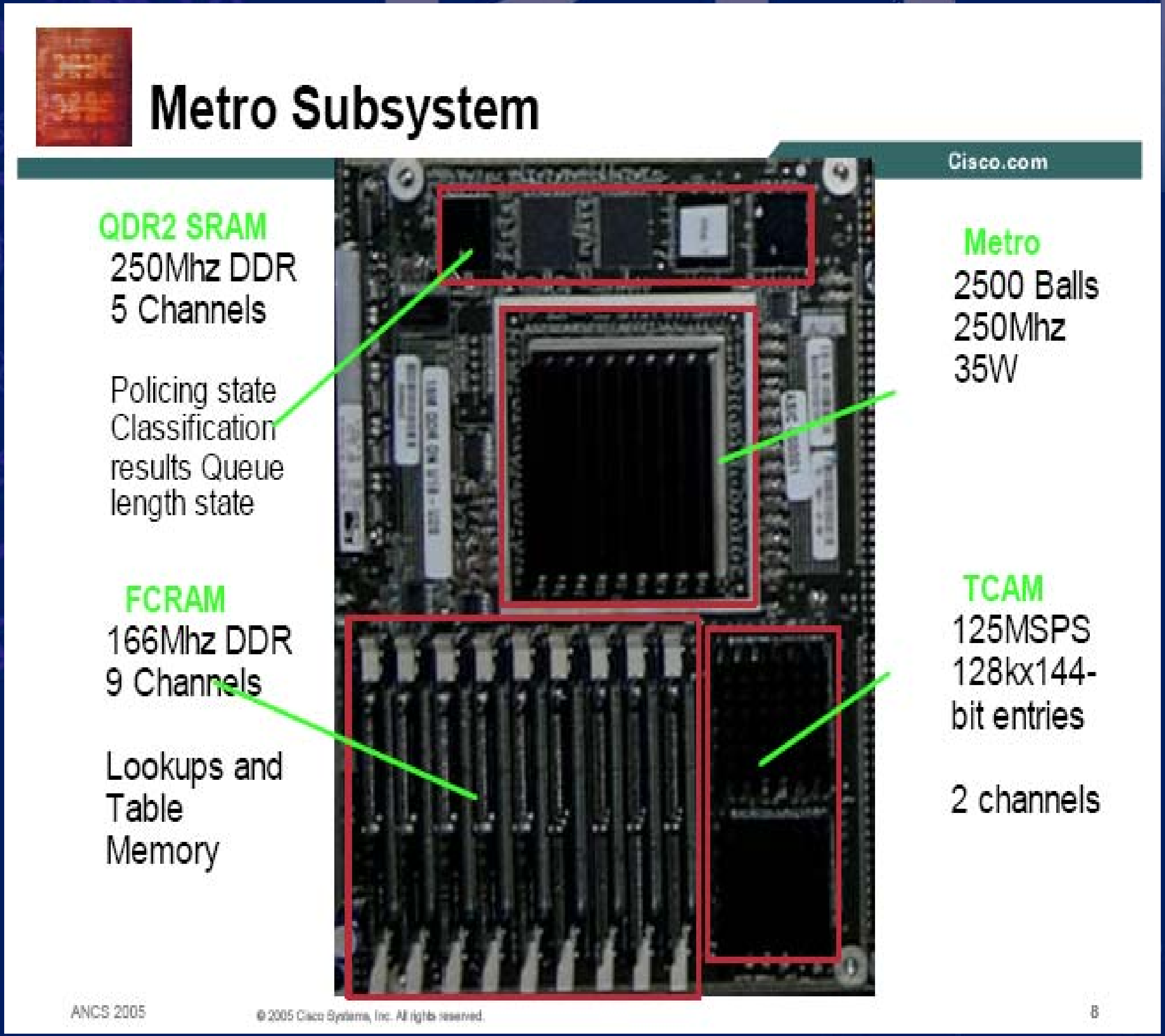
Source: Intel Corp.

HW Platform Solutions

- Network Processor
  - Many players in mid ’90, big and small
  - Intel’s IXP, EZchip’s NP, and a few more today
- MIPS based Multi-core
  - RMI’s XLR, Cavium’s Octeon, PMC-Sierra’s PM, and Broadcom’s BCM
- In-house Development
  - Cisco: 188 cores
  - Redback: PPA2 (18 Mpps and 12 Gps processor)
- Crypto chip being absorbed
  - CPU: VIA’s C7 and PMC’s MSP8520;
  - NPU: Hifn (IBM), FreeScale (Seaway), and many others
- Content chip emerging
  - Cisco’s acquisition of NetSift & Vihana;
  - Tarari’s RegEx; Xambala’s Panini

Metro in Cisco CRS-1

- Will Eatherton, The Push of Network Processing to the Top of the Pyramid, ANCS, 2005



Metro Subsystem

Cisco.com

QDR2 SRAM
250Mhz DDR
5 Channels

Policing state Classification results Queue length state

FCRAM
166Mhz DDR
9 Channels

Lookups and Table Memory

Metro
2500 Balls
250Mhz
35W

TCAM
125MSPS
128kx144-bit entries

2 channels

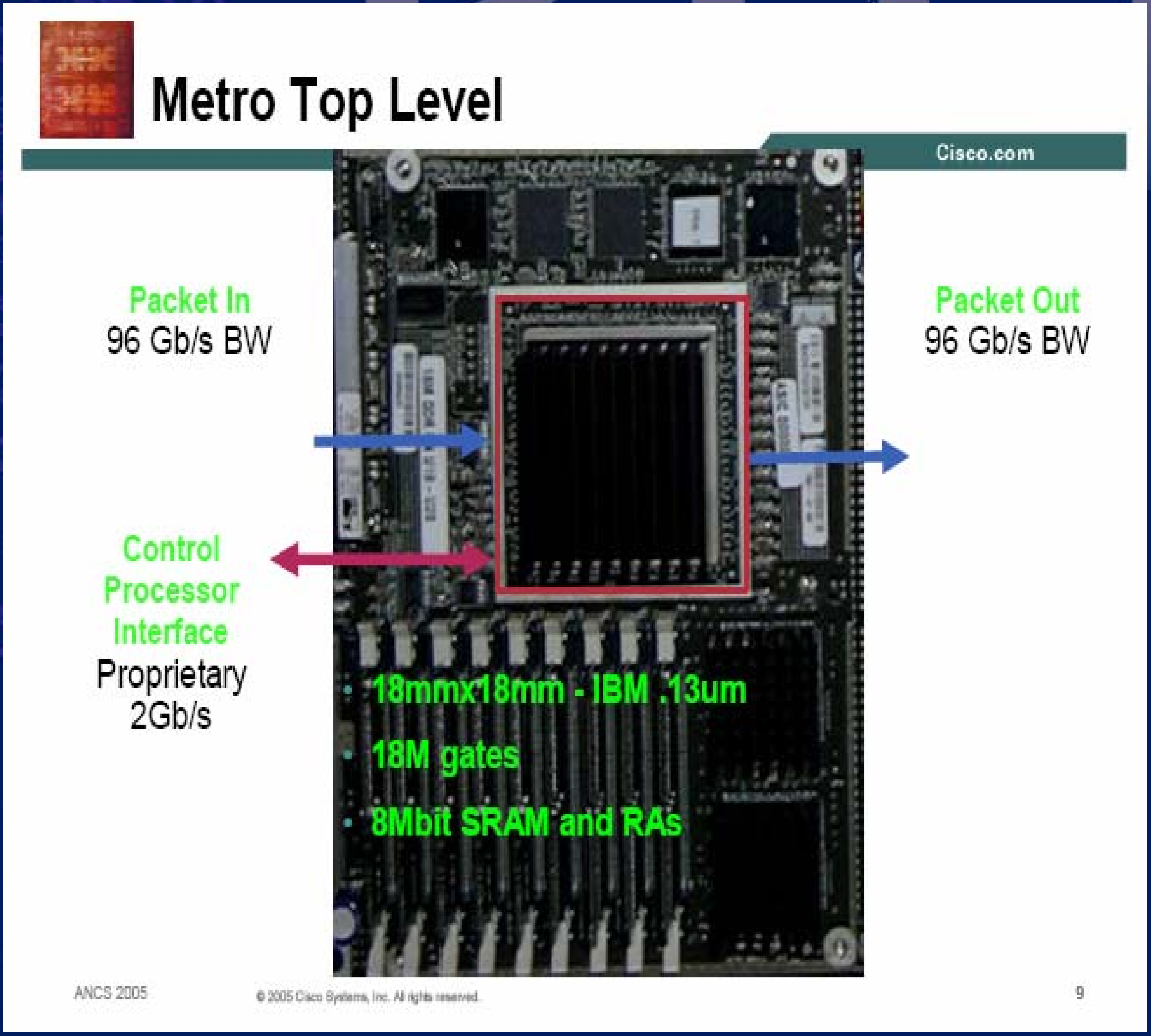
ANCS 2005

© 2005 Cisco Systems, Inc. All rights reserved.

8

Metro in Cisco CRS-1

- 188 32-bit embedded Risc cores
  - ~50 Bips
- 175 Gb/s Memory BW
- 78 MPPS peak performance



Metro Top Level

Cisco.com

Packet In
96 Gb/s BW

Packet Out
96 Gb/s BW

Control Processor Interface
Proprietary
2Gb/s

- 18mmx18mm - IBM .13um
- 18M gates
- 8Mbit SRAM and RAs

ANCS 2005

Recent Acquisitions

- Vertical Consolidation
  - Juniper took Netscreen (OneSecure & Neoteris) for $4.3B
  - Symantec took Sygate
  - CheckPoint attempted to take SourceFire for $225M
- Horizontal Consolidation
  - Symantec took Veritas for $13.5B
  - NetApp took Decru for $272M
  - EMC is taking RSA for $2.1B

- It's becoming increasingly difficult for large security vendors to remain competitive when they participate in just a select few market niches.
- Security is becoming something that's being embedded in the infrastructure. Once you get to a certain size, you see a market gets folded into what the big vendors do.

— SearchSecurity

History of Endpoint Security

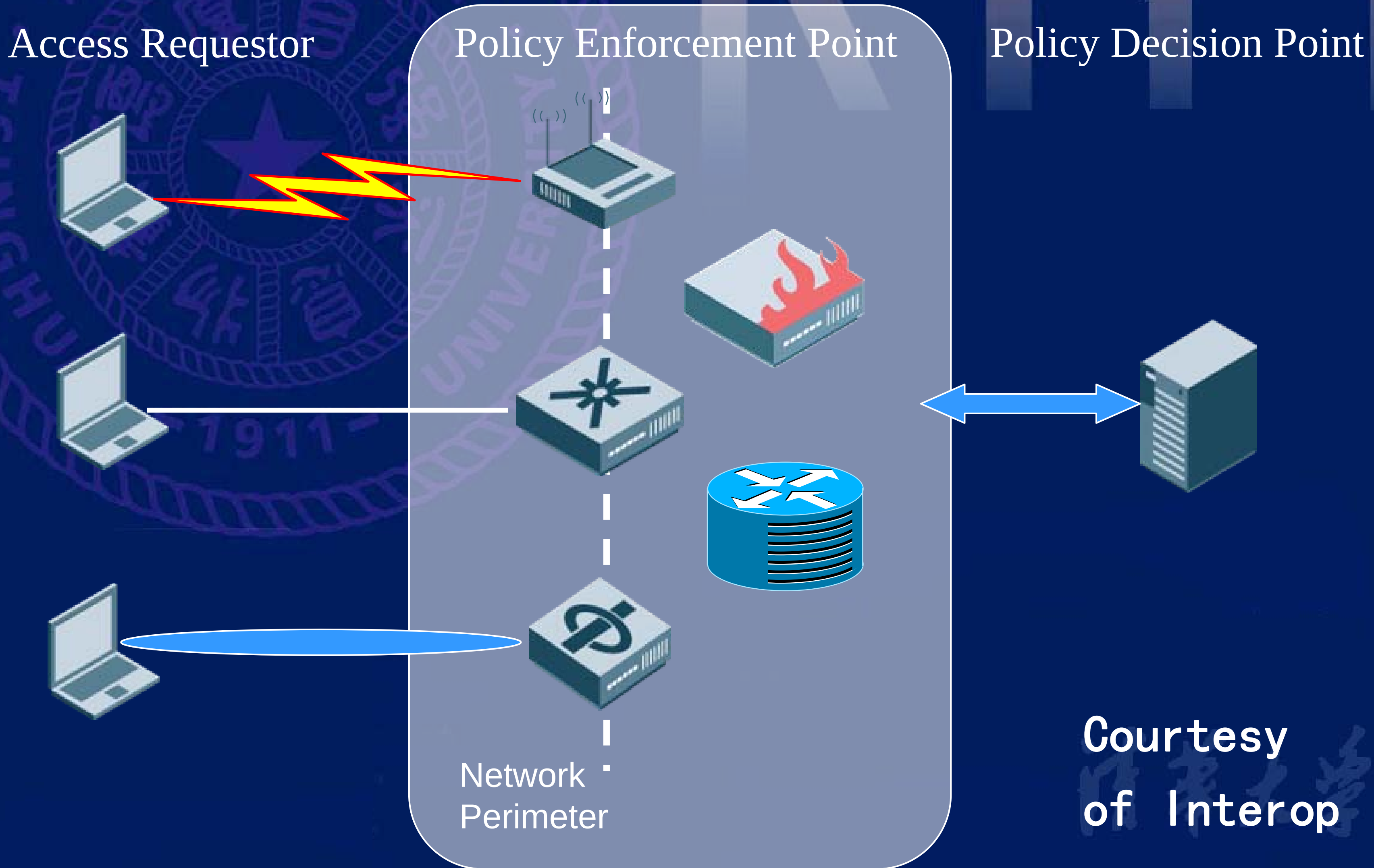
- 2001: Personal Firewall/IDS
  - Zone Labs (Now CheckPoint)
  - NetworkICE (Now ISS)
- 2003: OS Protection
  - Okena (Now CISCO)
- 2004: LAN Access Control
  - Sygate (Now Symantec)
- 2005: All the top players were acquired by large security vendors – market matured and absorbed
- ! Microsoft is coming !

Courtesy of Chris Guo

Holistic Approach
— think of gateway and endpoint as a whole

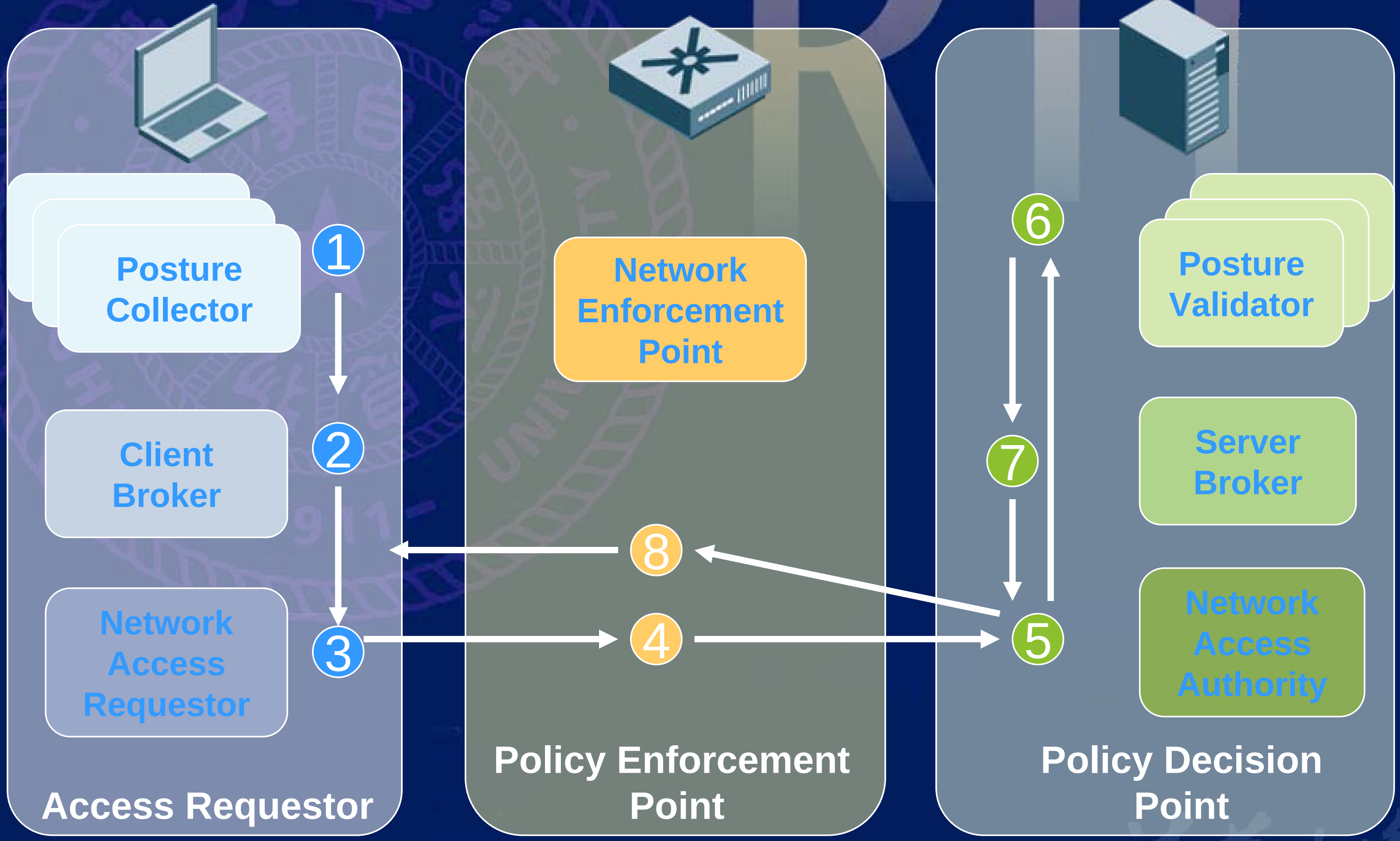
- Admission Control
  - Cisco： NAC (Network Admission Control)
  - Microsoft： NAP (Network Access Protection)
  - TCG： TNC (Trusted Network Connect)
- Policy Enforcement
  - Juniper： Does more with advanced firewall?
  - 2006.05.01 Juniper to support TNC

Generic NAC Components



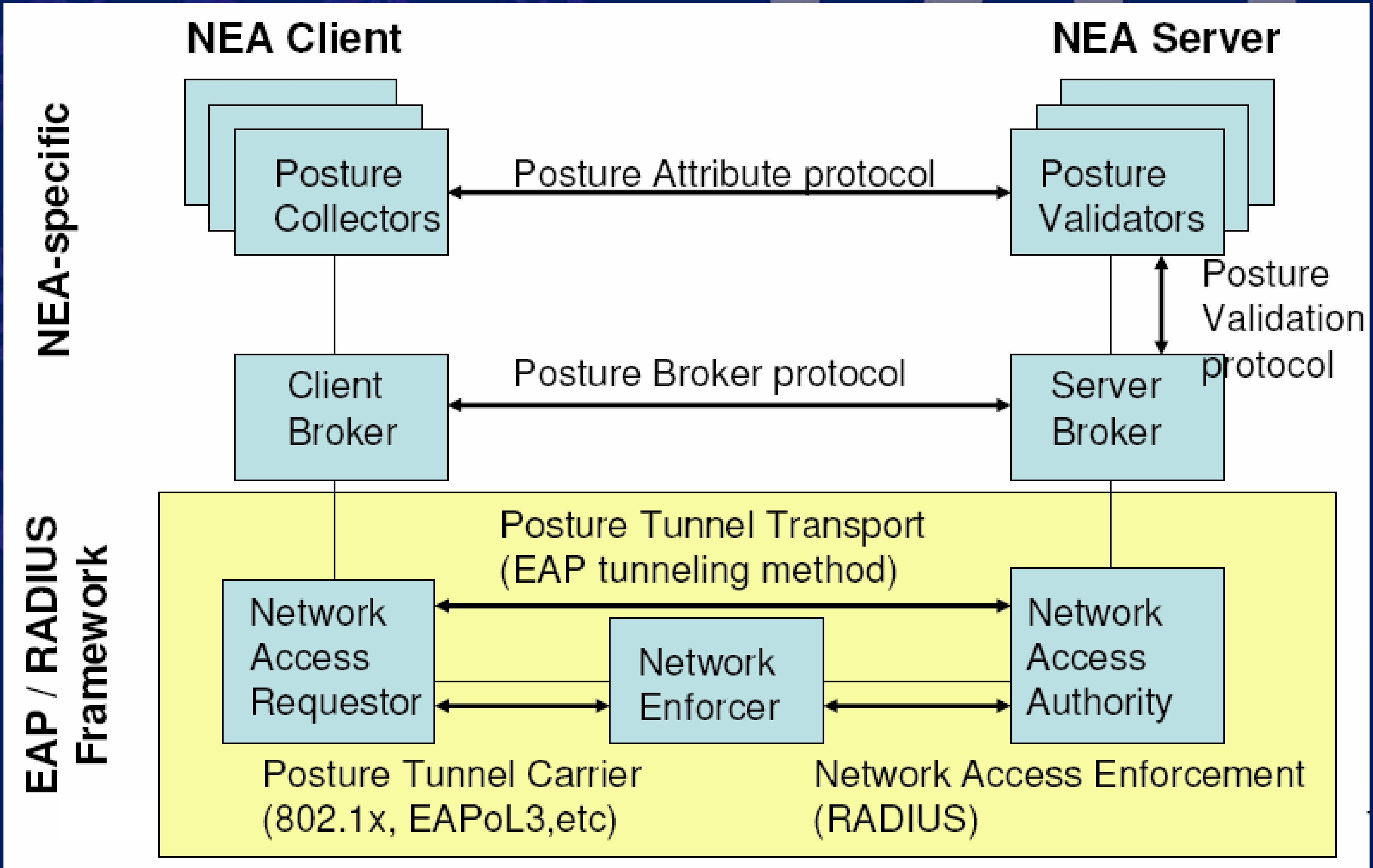
Courtesy of Interop

Sample NAC Transaction



Courtesy of Interop

Generic Architecture



Source: NEA BOF at IETF65

Holistic Approach
— prevent both intrusion and extrusion

- Information leakage prevention, ILP
  Extrusion detection system, EDS (EPS?)
- Passive Leakage
  Solution: Authentication and Encryption
  Active Leakage
  Solution: Content Filtering
- ERM (Enterprise Rights Management), incl. MS' RMS (Rights Management Server), similar to DRM (Digital Right Management)

The Threat From Devices

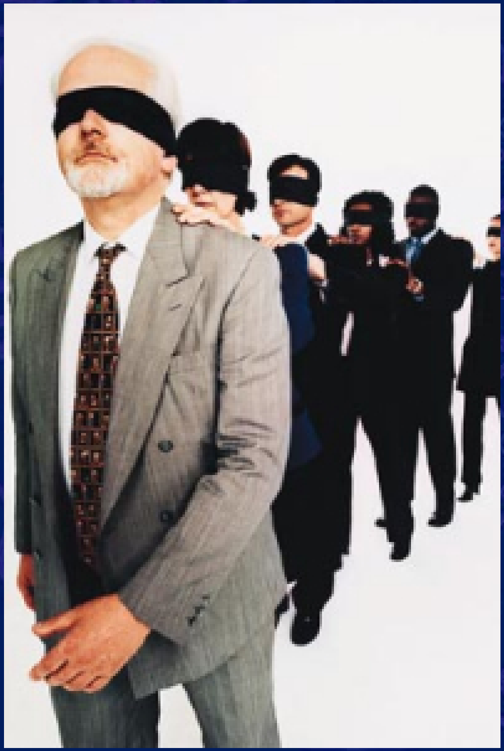
- Over 26,000 different USB products exist, 700M shipped in 2004
  - Storage devices
  - Networking adapters
  - Printers, scanners, webcams
  - Coffee warmers, hand massagers…

- Over 2 billion devices have been sold to date
  - Over 14 million iPods sold in 2005
  - Over 5 million Bluetooth devices are sold every week
  - Their capacity keeps growing – 10GB drive for $50 by 2010
  - They are virtually impossible to trace

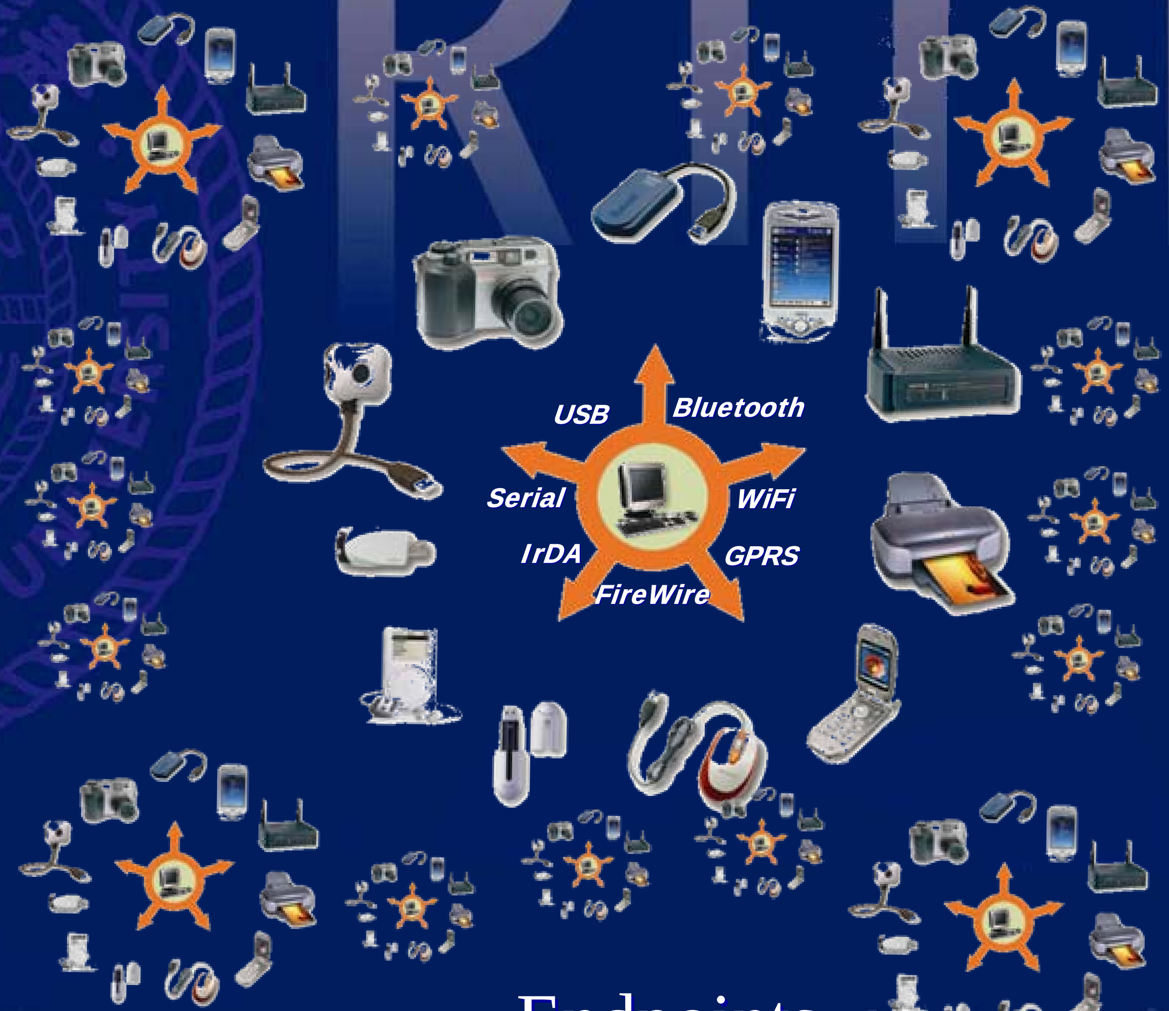
Courtesy of Safend

Current Situation:

Devices can connect to each PC – no visibility, no control



Info-sec Team



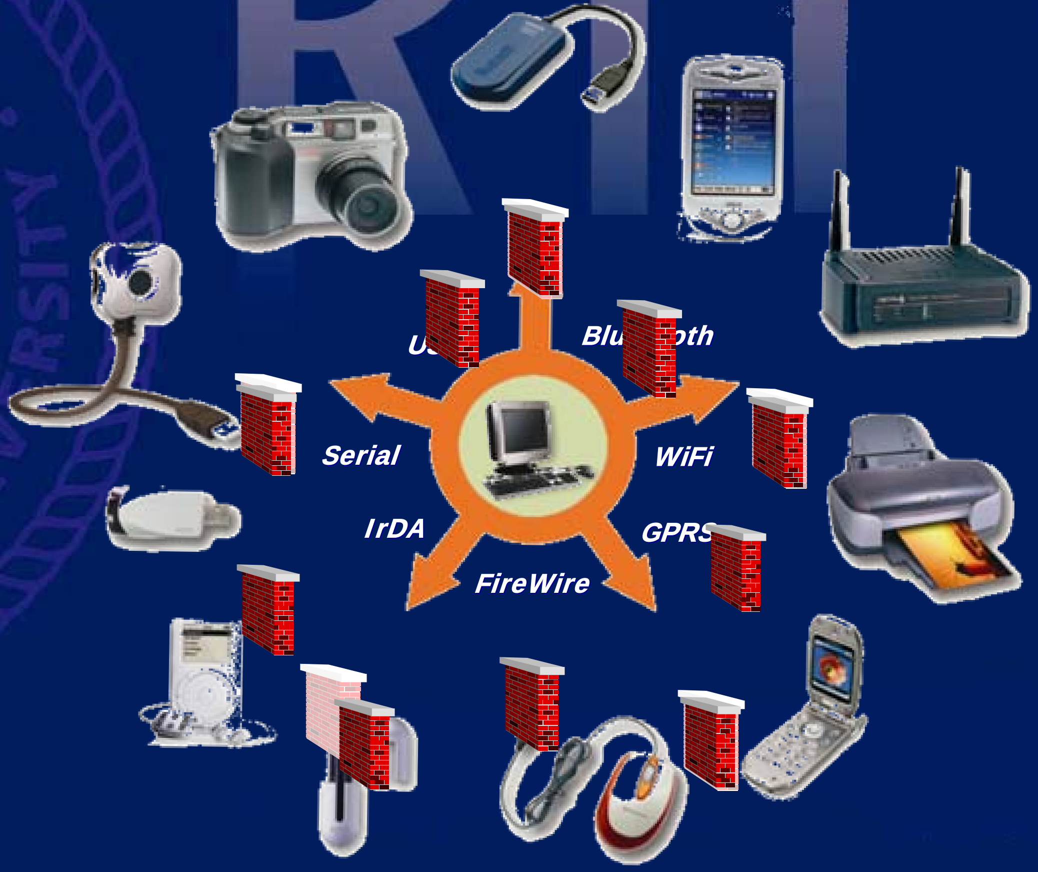
Endpoints

Courtesy of Safend

With Safend

Visibility and Granular Control

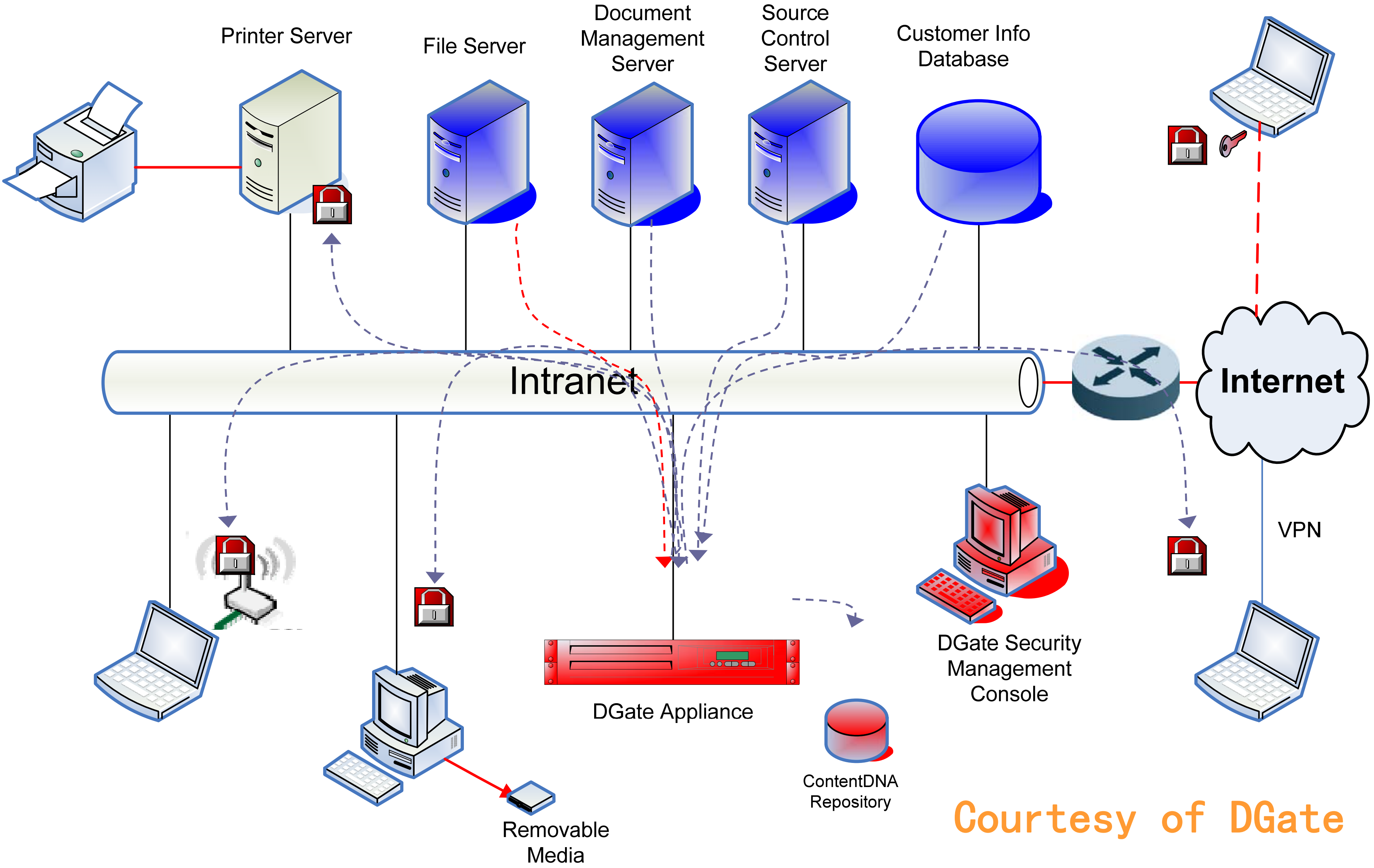
Info-sec team



Endpoints

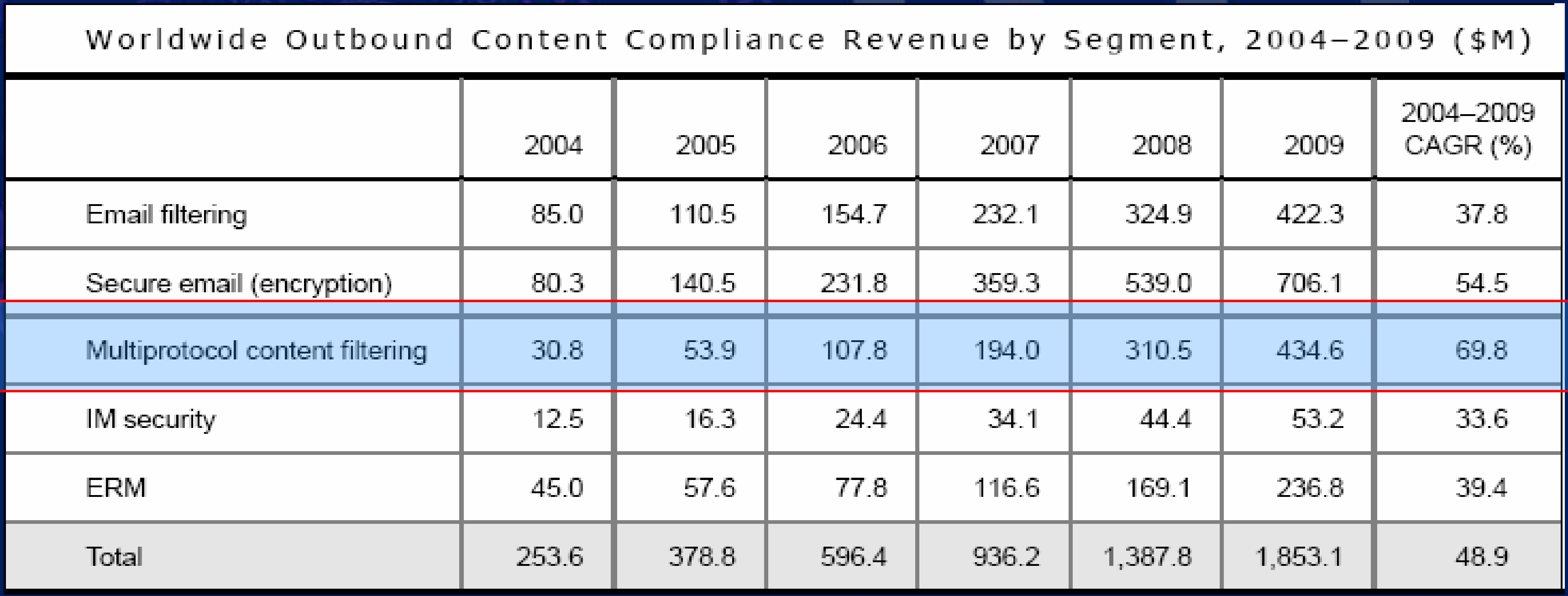
Courtesy of Safend

With DGate



Courtesy of DGate

“OCC” Market Growth



Worldwide Outbound Content Compliance Revenue by Segment, 2004–2009 ($M)

	2004	2005	2006	2007	2008	2009	2004–2009 CAGR (%)
Email filtering	85.0	110.5	154.7	232.1	324.9	422.3	37.8
Secure email (encryption)	80.3	140.5	231.8	359.3	539.0	706.1	54.5
Multiprotocol content filtering	30.8	53.9	107.8	194.0	310.5	434.6	69.8
IM security	12.5	16.3	24.4	34.1	44.4	53.2	33.6
ERM	45.0	57.6	77.8	116.6	169.1	236.8	39.4
Total	253.6	378.8	596.4	936.2	1,387.8	1,853.1	48.9

Data Source: IDC

Holistic Approach
— from network to application

- UTM
- P2P
- HTML (port 80) and XML/SOAP

Holistic Approach
— from wired to wireless

- WiFi, WiMAX
- 3G

(Customers) don’t want security bolted on. They want it woven in.
— Joe Tucci, CEO of EMC

Integrate FW & IDP: a Small Task

Firewall Procedure

- Packet comes in
- Check for existing session
  - If no, check against ruleset
    - If no, drop the packet, etc.
    - If yes, create session
- Packet goes out

Packet Classification

IDS/IPS Procedure

Packet Classification

- Packet comes in
- Check for protocol and applications (ports)
- Matching against corresponding sub-pattern-set
  - If yes, check for (source) IP addresses and other fields against rules of the matching patterns
    - If yes, drop the packet, etc.
- Packet goes out

Pattern Matching

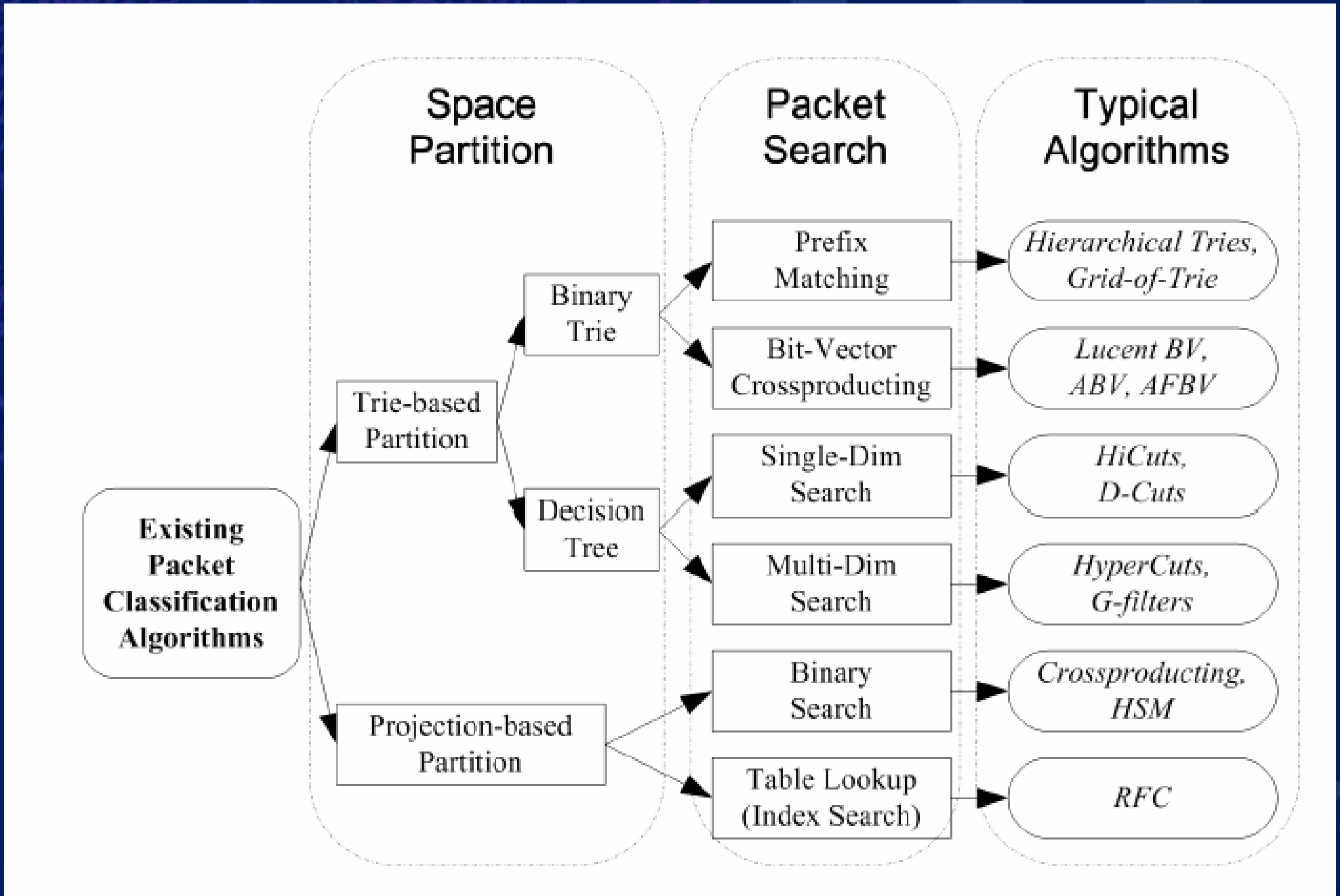
Packet Classification

Existing Algorithms

- Trie-based Algorithms (HiCuts, HyperCuts)
  - Memory efficient
  - No explicit worst-case bound, not fast enough
- Projection-based Algorithms (RFC, HSM)
  - Fast search speed
  - Not memory efficient

Packet Classification

- Categorization



Packet Classification

— New Directions (1)

Exploration of Data Characteristics

- Ruleset Redundancy
  - *The theoretical bounds tell us that it is not possible to arrive at a practical worst case solution. Fortunately, we don't have to; No single algorithm will perform well for all cases. Hence a hybrid scheme might be able to combine the advantages of several different approaches. -- P. Gupta, Stanford*
- Search Structure compression
  - Trie path compression: *Packet classification for core routers: Is there an alternative to CAMs?, UCSD, 2003.*
  - Search Index compression: *Towards Effective Multidimensional Packet Classification, TsinghuaU, 2006.*

Packet Classification
— New Directions (2)

Introduction of Traffic Statistics

- Most of the existing algorithms assume all incoming packets are distributed uniformly in the search space.
- However, it is unlikely that the traffic in a certain network evenly spread over all IP addresses and/or port numbers.
- Related Research
  - *Adaptive Statistical Optimization Techniques for Firewall Packet Filtering, Infocom, 2006*
  - *Dynamic Cuttings: Packet Classification with Network Traffic Statistics, TIW, 2004*

Packet Classification

— New Directions (3)

Leveraging on New Hardware

- TCAM
  - Related work: *TCAM-based distributed parallel packet classification algorithm with range-matching solution, Infocom, 2005.*
- ASIC/FPGA
  - Related work: *Performance Evaluation of Multidimensional Packet Classification on Network Processor, TsinghuaU, 2006.*

Pattern Matching

— Algorithm on CPU

- Achieving bigger shift number
  - Related work: *Recursive Shift Indexing: A Fast Multi-Pattern String Matching Algorithm, ACNS, 2006.*
- Utilizing the specific characteristics of network flow or pattern set
  - Related works: *Memory Efficient String Matching Algorithm for Network Intrusion Management System, TsinghuaU, 2006.*
- Hybrid Algorithm: triggering different algorithm according to different application conditions
  - Improved MWM algorithm in Snort

Pattern Matching

— Algorithm on NPU

- Utilizing the hardware unit in NP to accelerate some operations in pattern matching
  - Related work: *A fast string-matching algorithm for network processor-based intrusion detection system, ACM Trans. on Embedded Computing Systems, 2004, 3(3): 614-633.*
- Combining the multi-thread and multi-processor architecture with algorithm design
  - Related works:
    - *A parallel NIDS pattern matching engine and its implementation on network processor, SAM, 2005.*
    - *Optimizing Multi-thread String Matching for Network Processor-based Intrusion Management System, CNIS, 2006.*

Pattern Matching

— Algorithm on FPGA

- Reduce the storage requirements of pattern matching data structure so data could fit into the on-chip memory or consume less logic cell
- Related works:
  - *Deterministic memory-efficient string matching algorithms for intrusion detection, Infocom, 2004.*
  - *High-performance Pattern Matching for Intrusion Detection, Infocom, 2006.*

Integrate Firewall and IDP

- Packet comes in
- Check for existing session
  - If no, check against firewall ruleset
    - If no, drop the packet, etc.
    - If yes, create session
- Matching against corresponding sub-pattern-set
  - If yes, check for special fields against rules of matching patterns
    - If yes, drop the packet, etc.
- Packet goes out

Advanced algorithms and integrated procedure!

What's Left for Research

- Firewall and IDP seamless integration seems intuitive, but available products today are still software or hardware blades stack up
- An optimized system is not simple add up of best components
  - What is the best way to merge the two rulesets?
  - Will the characteristic change after merging firewall and IDP rulesets?
  - How do we optimize memory bandwidth utilization after the procedure change?
  - What is the best way to parallelize the new procedure
  - What is the best way to take care of packet ordering now?

Conclusion

- Network security is challenged from all direction at all level
- Network security is not just security gateways working at network layer
- Holistic approach is the way, a long way, to go for overall defense
- R&D has green field for everyone to contribute; we are working on integrated firewall and IDP, as an example

Thank You

junl@tsinghua.edu.cn