



Security Management – 5000 events/sec, half an engineer, and automation discouraged

or: Challenges in Intrusion Detection

Michael Behringer <mbehring@cisco.com>

Distinguished Engineer

July 2006

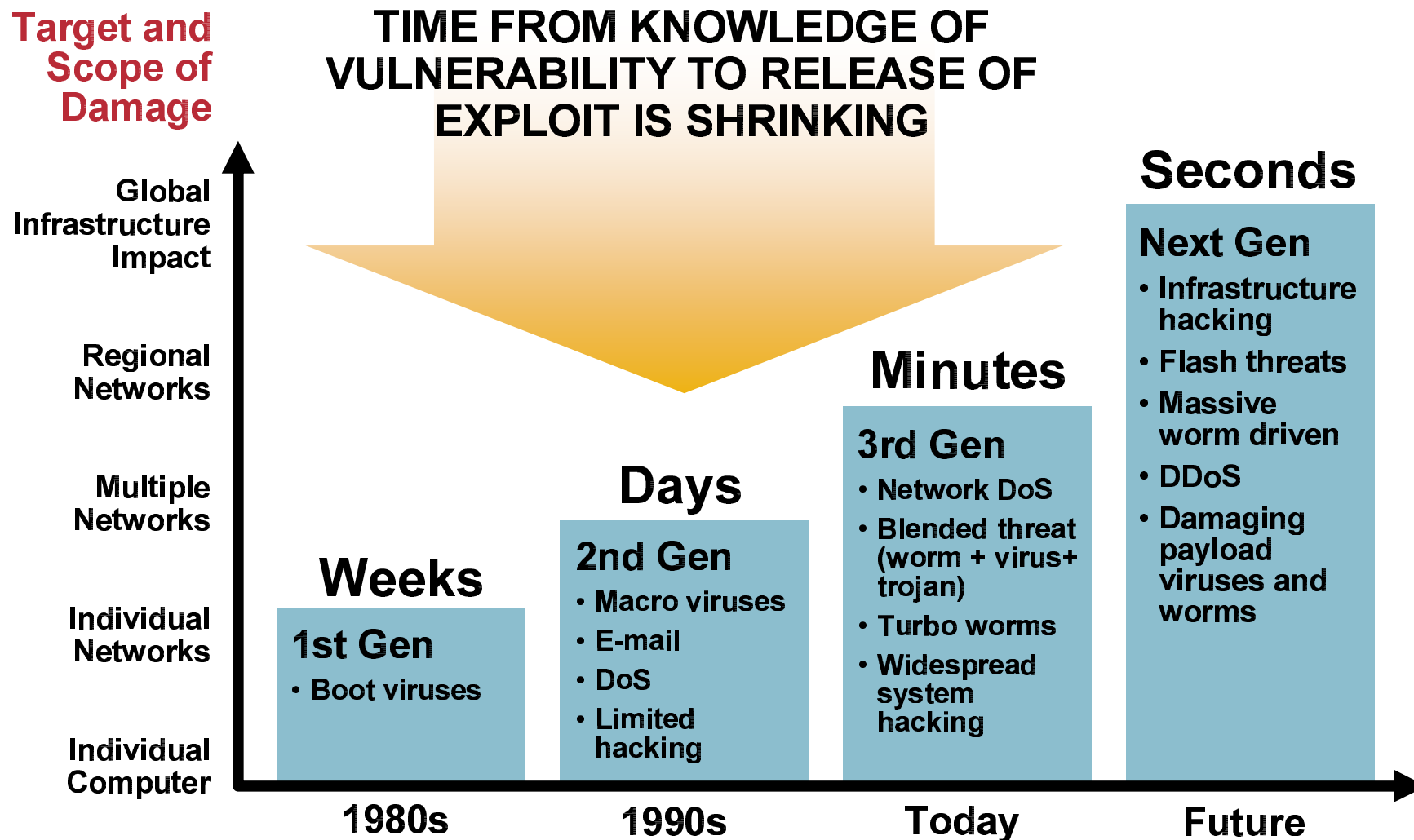
RFC 1925: The Twelve Networking Truths

- **“With sufficient thrust, pigs fly just fine.”**

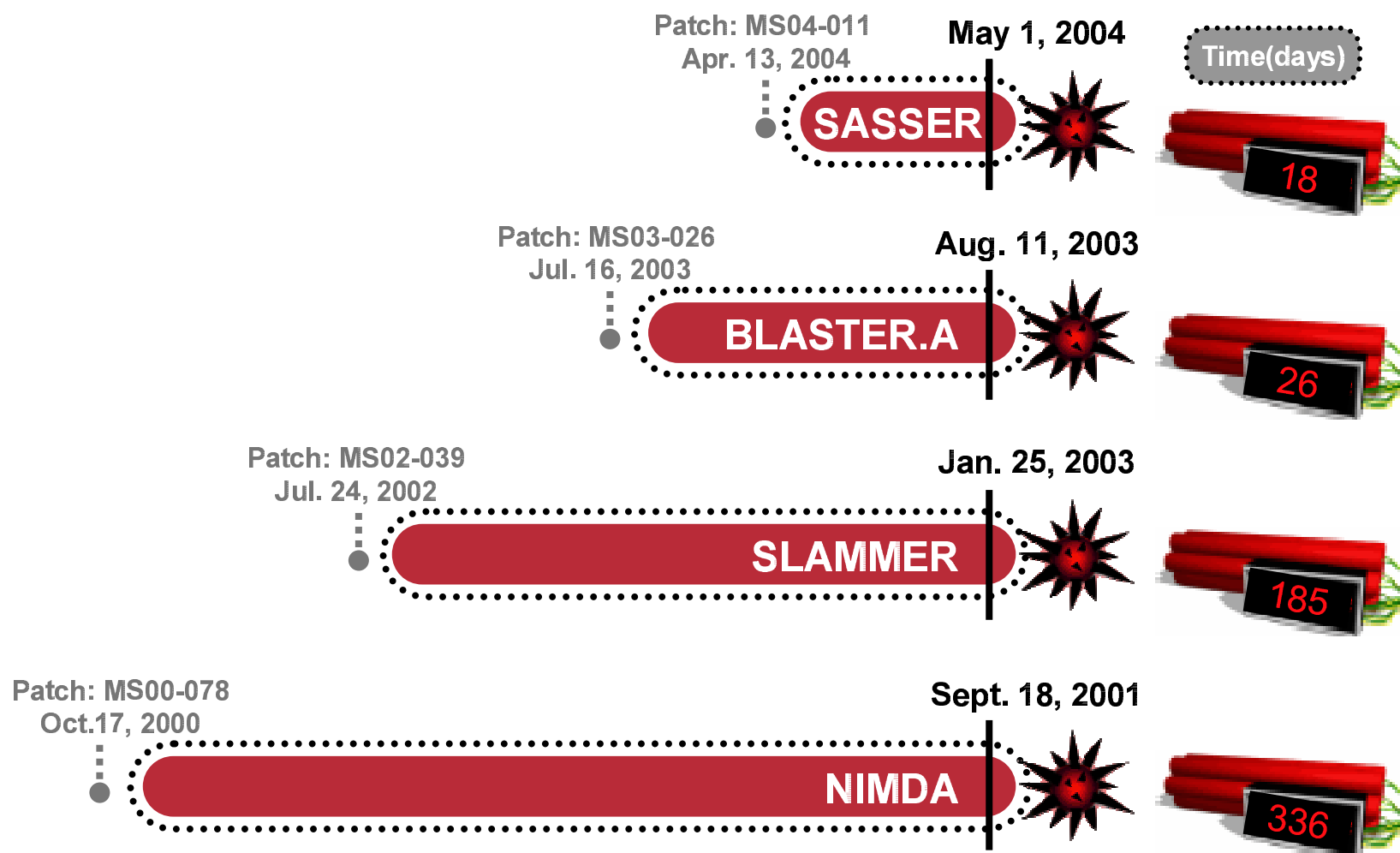
Michael’s corollary:

“With sufficient effort, you can make your IDS work.”

The Threats Have Evolved: Increasing Speed and Damage




Worms: Vanishing Patch to Outbreak Window



The Problem Space

- **Signature management**
 - **Many different IDS approaches**
 - **False positives**
 - **Day-0 recognition**
 - **Scale of alerts**
 - **Complexity of decision**
 - **Network scale**
 - **Visibility (encryption, location, ...)**
 - **...**
-
- Manageability**
- Intelligence**
- Performance**

The Goal



4:45PM SARAH VISITS DAD'S OFFICE
5:05PM SARAH DOWNLOADS
FUNNYBUNNY.EXE **5:06PM NETWORK**
KILLS FUNNYBUNNY **5:14PM DAD**
TAKES SARAH TO KARATE PRACTICE

Sometimes threats don't look like threats. They look like your mobile workers, your sales department or your CFO's daughter. Even the innocent act of downloading a file—one that looks like any other, but is in fact corrupt—can create a costly security breach that can take your business off-line for days. So how do you defend against threats that take the shape of productive employees? A network with integrated security can detect and contain potential threats before they become actual ones. Whether they're worms, hackers or even well-meaning humans. Security starts about prevention. Not reaction. To learn more about how Cisco can help plan, design and implement your network security, visit cisco.com/securitynow. **SELF-DEFENDING NETWORKS PROTECT AGAINST HUMAN NATURE.**

- **Manageability** → **Automation**
- **Intelligence** → **Correctness**
- **Performance** → **Completeness**

IDS: Approaches

- **Signature based (define “bad”)**

Needs to know attack up front; hard to manage

- **Behaviour based**

Complex to manage; up front config

- **Honeypots**

Good for worms and scanning, not much else

- **Statistical Analysis**

Only detects big changes

+ quite precise
- complex
- slow

+ performant
- not precise enough

Two Generic Approaches

1. Full packet / session inspection

Precision!!!

But: Mostly signature based, see next section

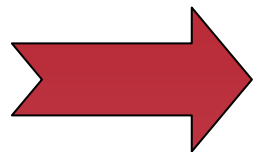
But: Performance required, see later

2. Header inspection: Flow based, honeypot

Statistics based → heuristics are simple

Can catch day-zero, quite efficient

But: Not precise enough!!!

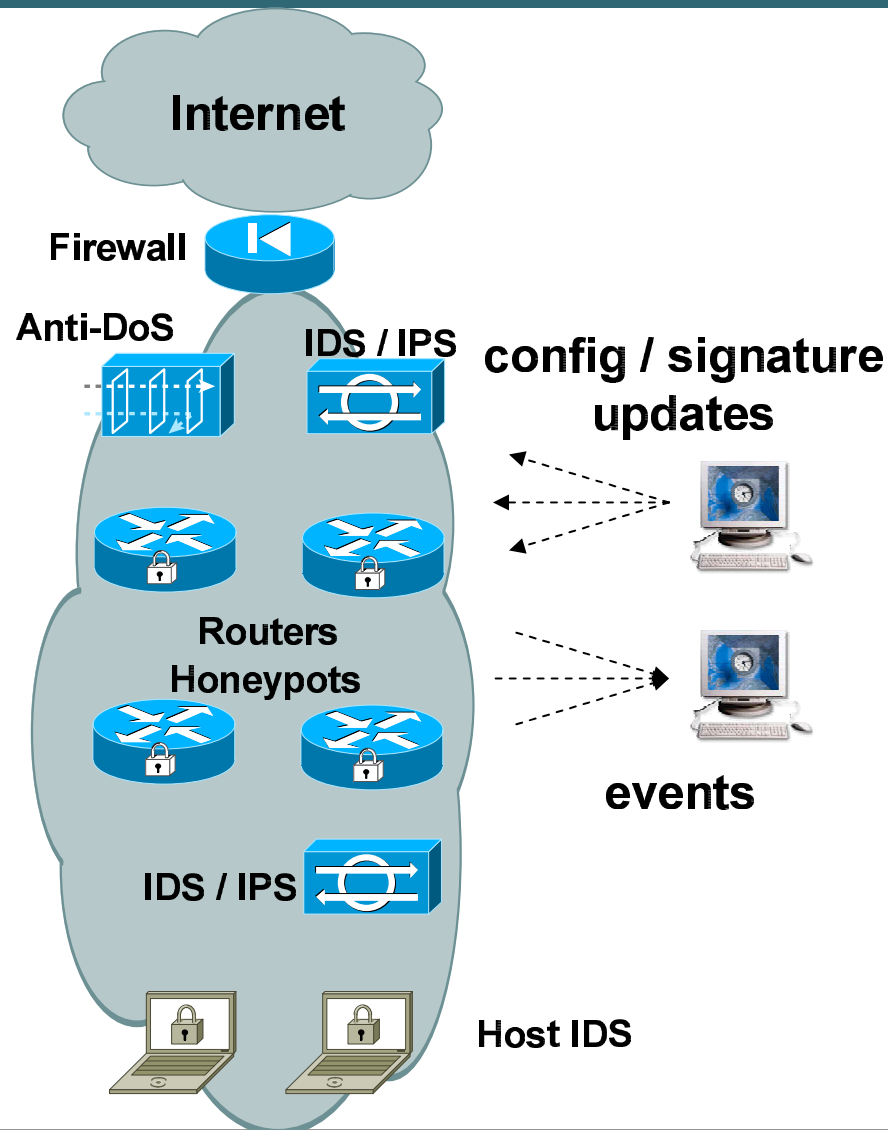


Probably both required!

Manageability



Manageability Challenges: Overview



- **Different device types**

Router, firewall, IDS, HIDS, DDoS protection, honeypot, ...

→ Different IDS capabilities

→ Different management

→ Different signatures

→ Different event types


- **Scaling issues:**

Updating N devices

Receiving lots of events

Correlation

Number of Events, Network Wide

| Model | Performance Events/Sec* | Performance NetFlows/Sec |
|--|----------------------------|-----------------------------|
|  Marketing Stuff irrelevant here | 50 | 7,500 |
| | 500 | 15,000 |
| | 1000 | 30,000 |
| | 3000 | 75,000 |
| | 5000 | 150,000 |
| | 10,000 | 300,000 |

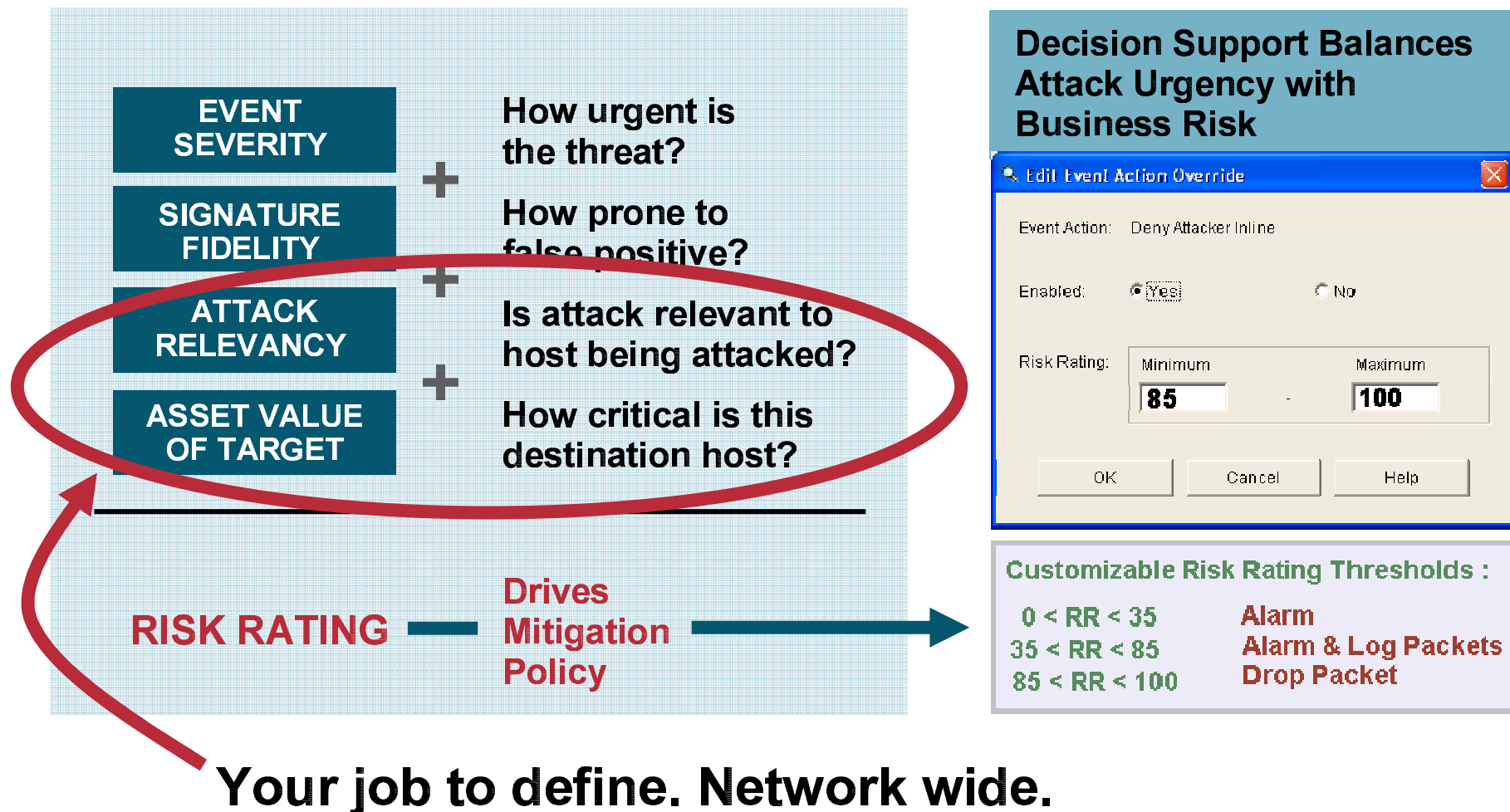
1000s of events per second
10,000s of flows per second

Intelligence



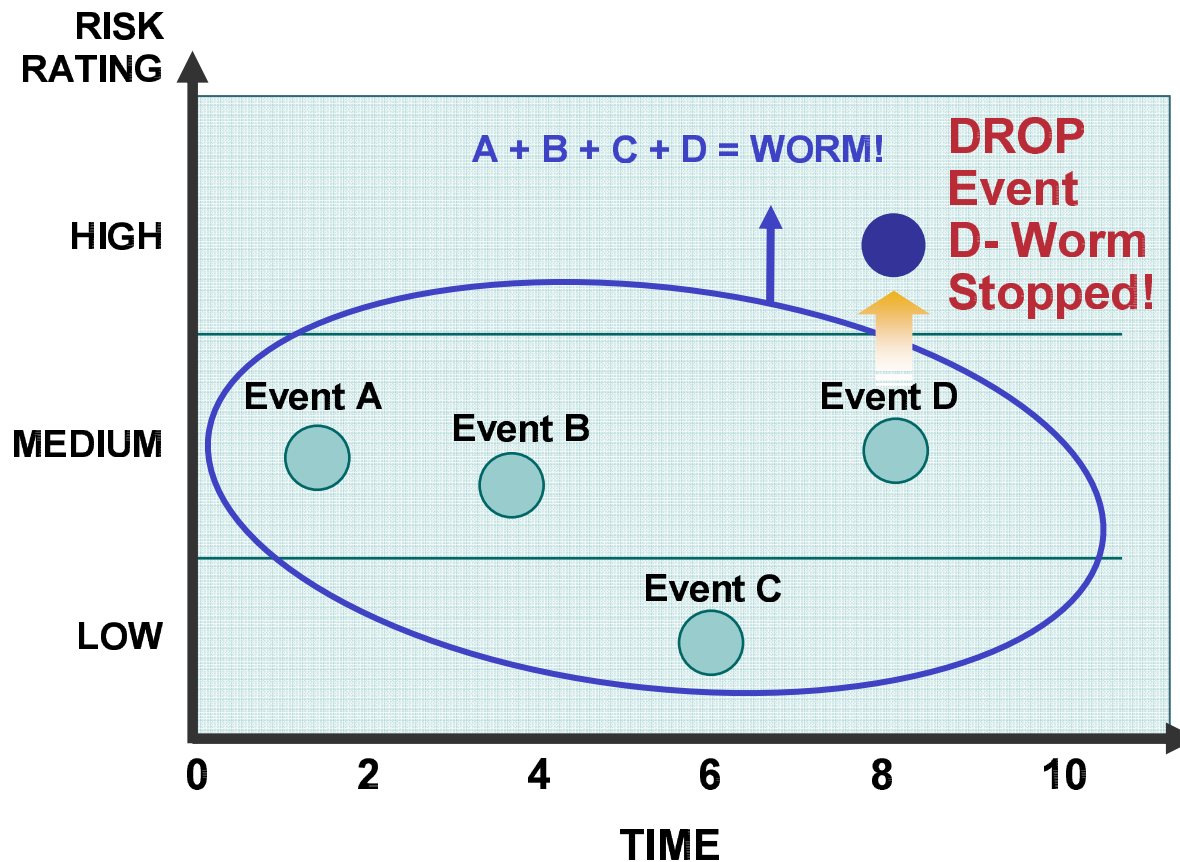
Process for Accurate Threat Mitigation:

Rating Alarms for Threat Context



Process for Accurate Threat Mitigation: *Integrated Event Correlation*

**On-Box Correlation Allows
Adaptation to New Threats in
Real-Time without User Intervention**



- Links lower risk events into a high risk meta-event, triggering prevention actions
- Models attack behavior by correlating:
 - Event type
 - Time span

Example for Increasing Complexity: Obfuscation

IDS looking for “..\” to detect attacks like:

...\WINNT\SYSTEM32\CMD.EXE

IDS needs to look for “\”:

- \ or /
 - %5c (%5C is hexa code for \)
 - %255c (%25 is hexa code for %)
 - %%35c (%35 is hexa code for 5)
 - %%35%63 (%63 is hexa code for c)
 - %c0%af (using Unicode)
 -
- } Double decode !



IDS must parse! → Complex!

By the way...

- **How do you upgrade from IDS to IPS?**

Intrusion Detection

Intrusion Prevention

s/D/P/

Performance



Performance: Goal

- **Inspect:**

Each packet header

Each packet payload

At full line rate

- **Checks:**

against 1000s signatures

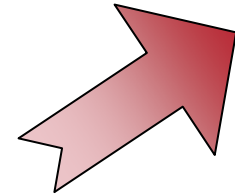
do virtual reassembly

be stateful (track connections)

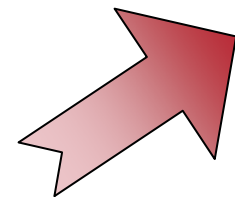
application awareness

BUT:

**Network Speed
Development:**

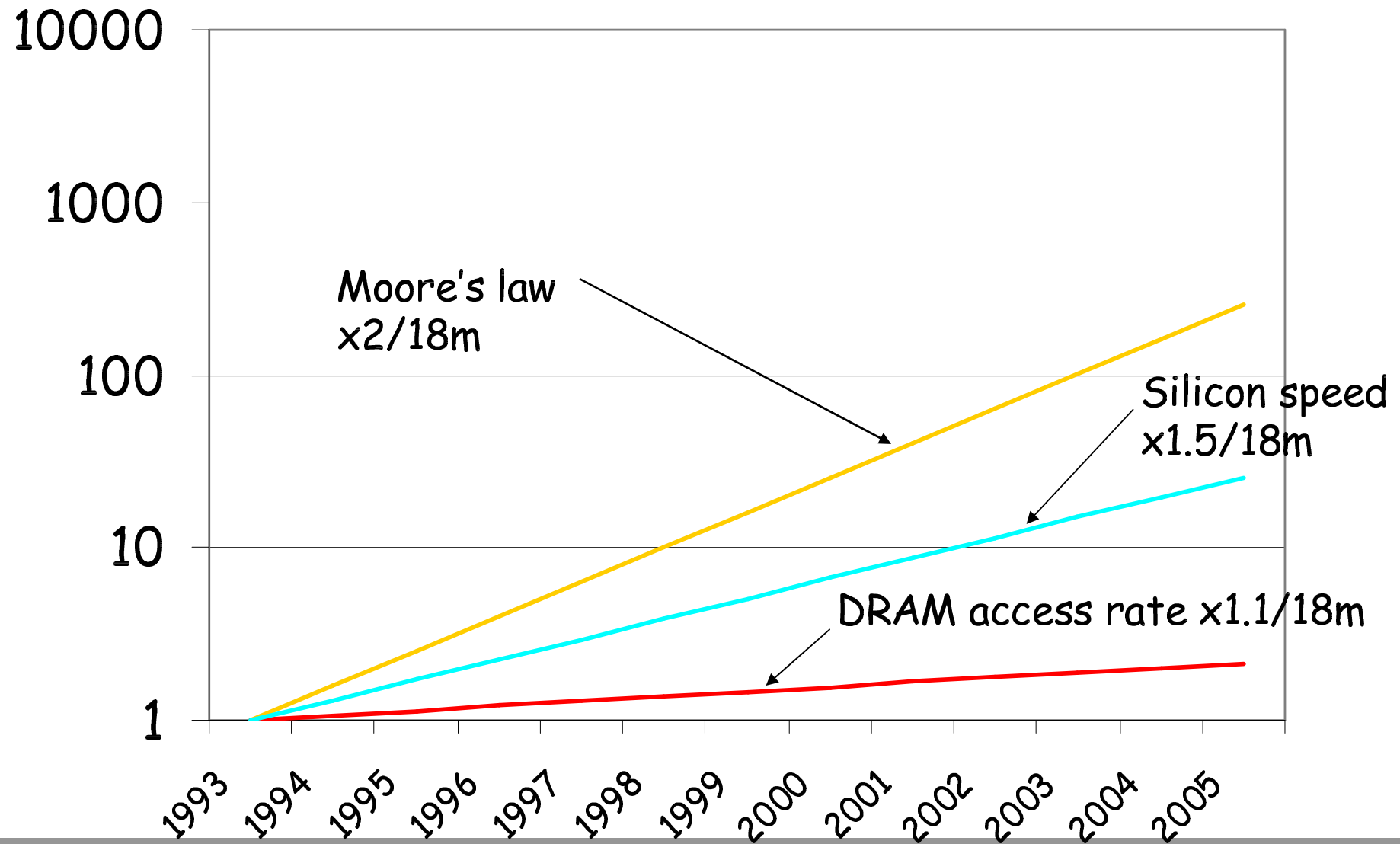


**Complexity
Development:**

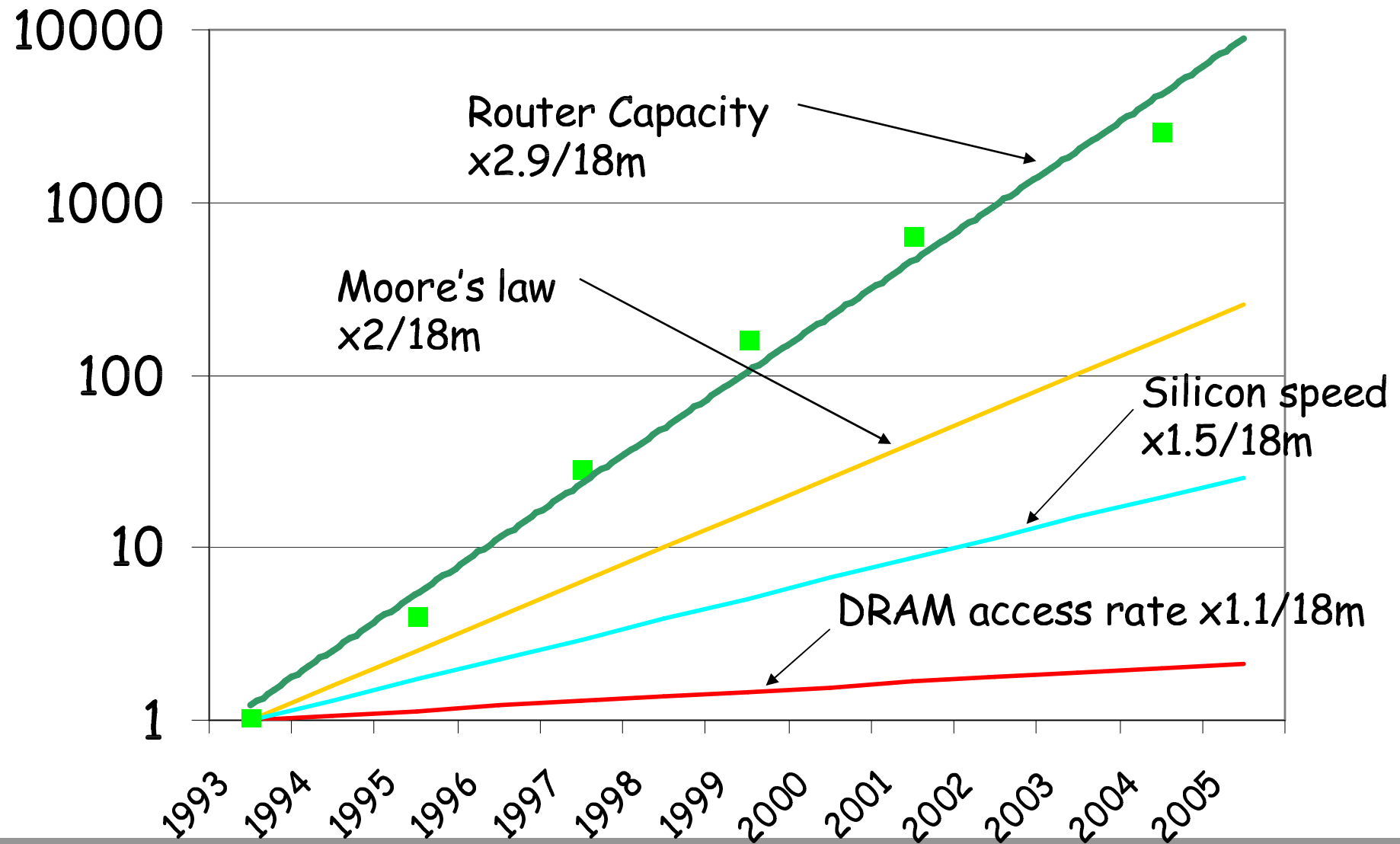


... so: “just build faster chips!”

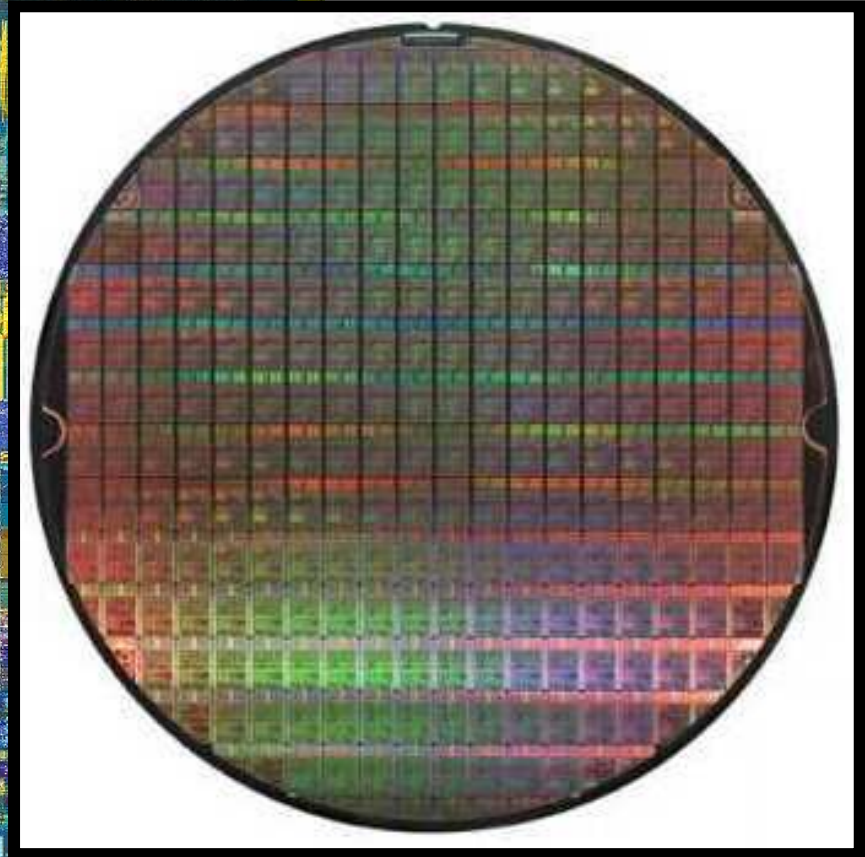
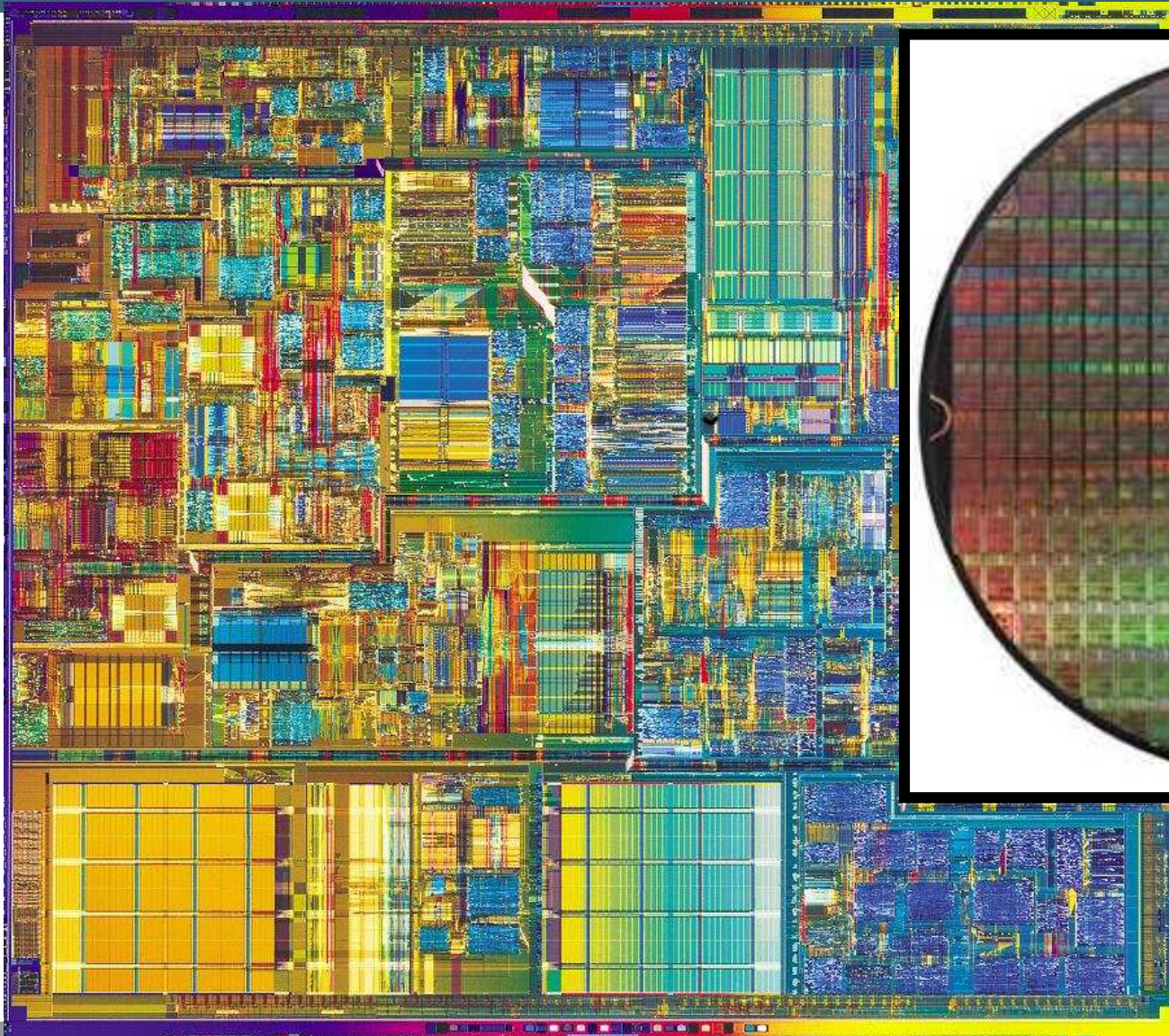
Silicon Industry Challenge



Silicon Industry Challenge



Silicon Density – Touching the Limits

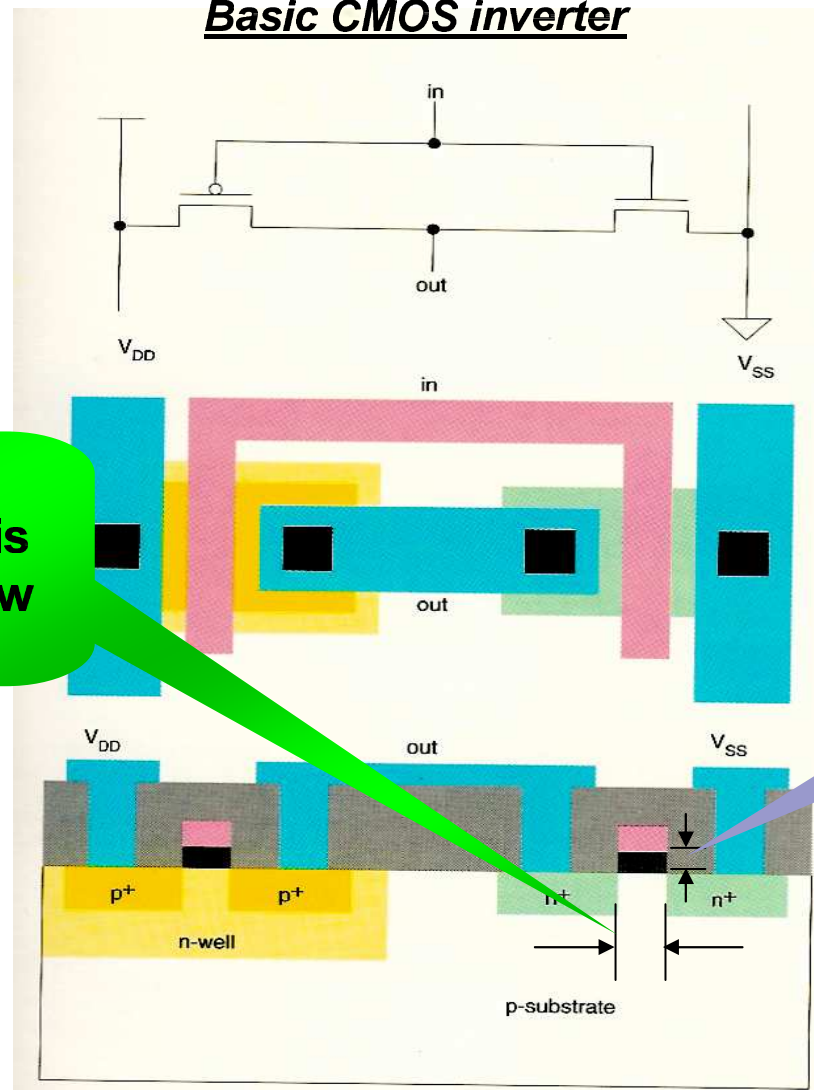


Wafer

Intel Pentium 4

Silicon Density and Moore's Law

Basic CMOS inverter



"Feature size"
This dimension is
what Moore's Law
is all about!

Gate Oxide Layer
For 90nm process,
this is approx 1.2nm
= 5 Atoms!

ASIC Feature Size Evolution

| Feature size <small>(drawn)</small> (μm) | Qual. Year | Usable Gates (M) | DRAM density (Mbit/mm ²) | Gate delay (ps) | Power (nW/MHz/gate) | Core Voltage | Metal layers |
|--|------------|------------------|--------------------------------------|-----------------|---------------------|--------------|--------------|
| 0.25 | 1999 | 10 | - | ? | 50 | 2.5/1.8V | 5/Al |
| 0.18 (0.15) | 2000 | 24 | 0.81 | 23 | 20 | 1.8V | 6/Cu |
| 0.13 (0.10) | 2002 | 40 | 1.5 | 20/15 | 9 | 1.2V/1.5V | 7/Cu |
| 0.09 (0.07) | 2004 | 72 | 2.9 | 11/7 | 6 | 1.0V/1.2V | 8/Cu |
| 0.065 | 2005 | 120 | ? | 6/8 | 4.5/5.0 | 1.0V/1.2V | 9/Cu |

Source: IBM SA-12E, SA-27E, Cu-11, Cu-08, Cu-65



Biggest Scaling Issue: Power!

The constraints of 'standard' cooling and packaging of networking systems are very significant...

| Device | Power |
|--|-------|
| '486 | < 5W |
| Pentium | 10W |
| Pentium II (400MHz) | 28W |
| Pentium III (1.33GHz, 0.13um) | 34W |
| Pentium IV (3.2GHz, 0.09um) | 103W |
| Pentium "Extreme Edition 840" 3.2GHz, HyperThreading | 180W |

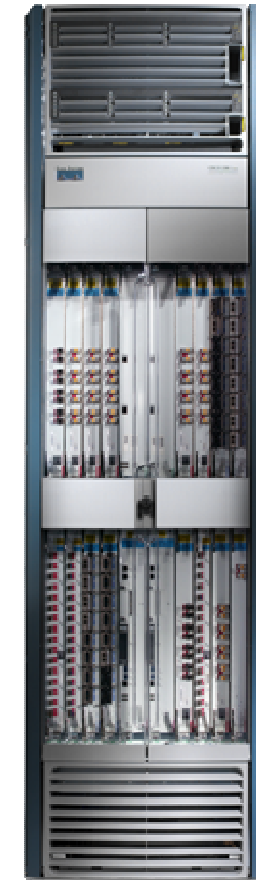


Source: Intel datasheets

CRS-1 System Mechanical

Line Card Chassis Overview—Full Rack Unit

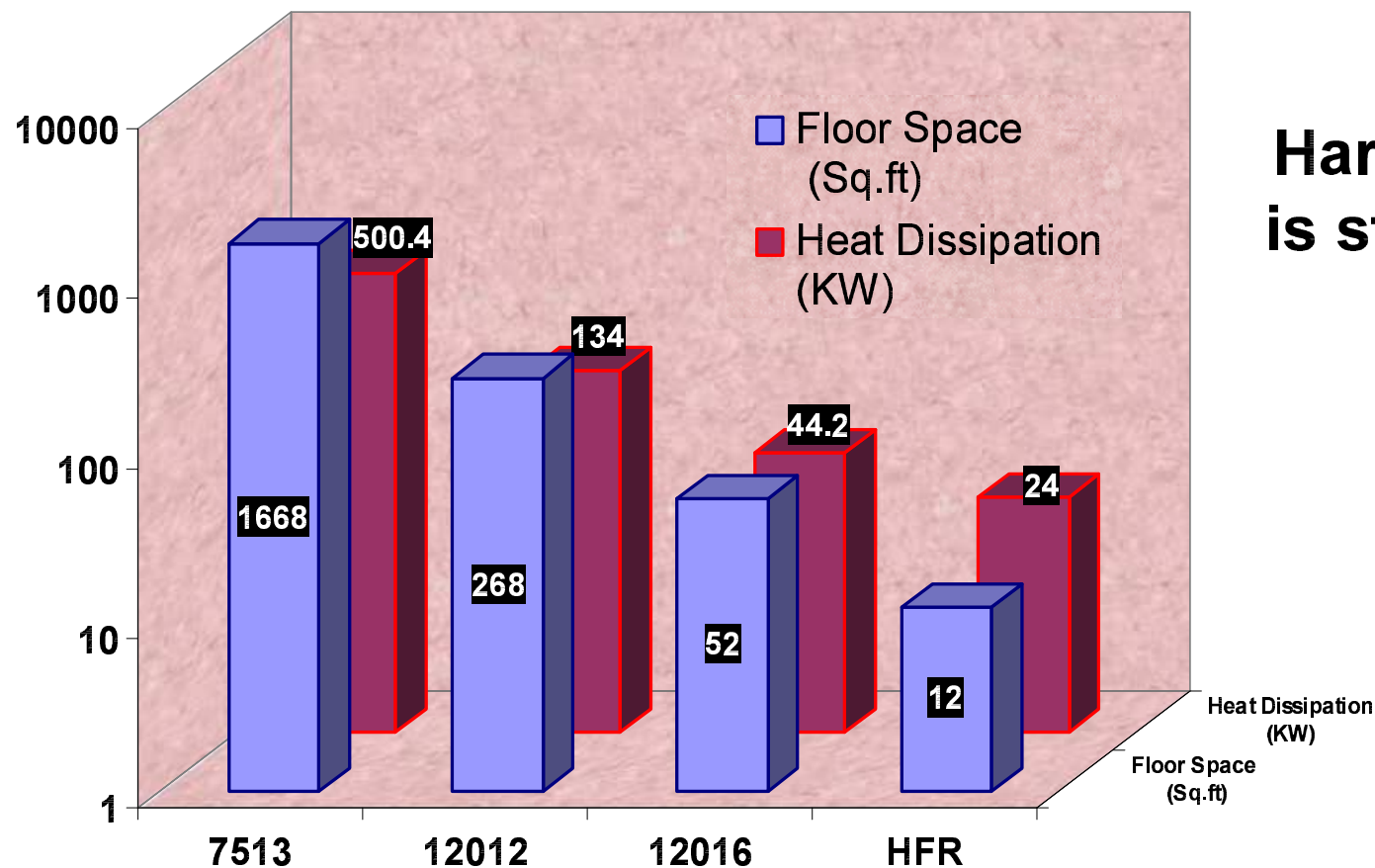
- **Slots (Midplane design):**
 - Front**
 - 16 PLIM slots**
 - 2 RP slots + 2 Fan Controllers**
 - Back**
 - 16 LC Slots**
 - 8 Fabric cards**
- **Dimensions:**
 - 23.6" W x 41" D x 84" H**
(60 W x 104.2 D x 213.36 H (cm))
- **Power: ~12 KW (AC or DC)**
- **Weight: ~ 707kg**
- **Heat Dis.: 33000 BTUs (AC)**



***For standalone Chassis Depth = 35" (no fabric chassis cable management)**

But: Efficiency is Still Increasing!!

Resources for a 1 Terabit Router



**Hardware design
is still improving!!**

Scaling Performance

- **Not just “faster, faster, faster”**
- **Need new approaches for h/w and s/w**
- **Distribute processing:**
 - Host – switch – edge router – core router**
 - Each device what it knows best**
- **But: Challenge in Management!**

So What Now?



So, Host IDS is “the” solution, right?

- **Performance distributed**
- **Encryption not an issue**
- **Stateful**
- **Application awareness**

**Sounds ideal,
doesn't it?!?**



BUT:

Can you trust the host?

- **may be subverted**
- **User might switch HIDS off / bypass it**
- **Service Provider Case: no control over host!**

Ways Forward for Intrusion Detection

- **Distribute processing**

Host, router, access switch, honeypot, ...

- **More “intelligence”**

Innovative, simple, approaches

- **Evolve management**

Distributed, “intelligent”

- **Combine approaches**

Signature based, flow based, behaviour based, ...

... more research needed!

Summary

- **Today:**

- Need expert to operate IDS!**

- Significant effort (opex) required to make IDS useful**

- **Work needed to:**

- Make network wide IDS manageable**

- Increase intelligence → low false positive, negative**

- **Tomorrow:**

- Self-updating**

- Self-correlating**

- Self-defending**

Q and A

