Thinking Outside the Box

Eugene H. Spafford

Purdue University

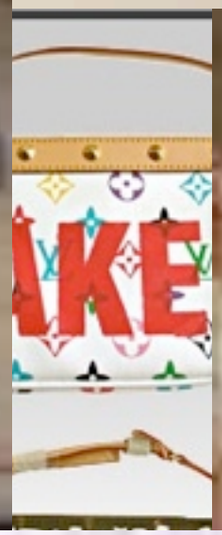
http://spaf.cerias.purdue.edu

Historical National Security

Transition of the Threat

To which we responded in kind. Security was not so much defense as MAD.

Further Transition to Crime



Terrorists are Criminals

From 1900 to 2000, 260 people were killed in acts of domestic terrorism – 168 by Timothy McVey in Oklahoma City, 4/19/95

Bringing it to the Fore

September 11, 2001

2993 people killed in 3 coordinated attacks.

National Response?

- Attack in Afghanistan
- Invade Iraq – a country uninvolved with Al Qaeda.
- Cost to U.S. to date:
  - $2+ TRILLION
  - 5130 service personnel killed
  - Over 1 million people killed, perhaps as many missing, injured, maimed.

Source: Washington Post, others

National Response?

$675,000,000 per US victim

Almost 2 new military U.S. deaths for each

334 foreign civilians casualties per US victim

Loss of International Support

Radicalization of more terrorists

Source: Washington Post, others

Exactly What Al Qaeda Wants

"All that we have to do is send two mujaheddin to the furthest point east with a flag on which is written the words al-Qaeda, and the Americans will panic and send a general and an army there, and engage in military operations which cost them blood and money and political capital, and then we'll just do it again. … so brothers, we're pursuing this strategy of bleeding the United States to exhaustion and bankruptcy."

– Osama bin Laden

Some Perspective

- Over 400,000 people will die *this year* from smoking
- Over 600,000 will die from heart disease
- In 2001, over 20,000 people died in car crashes because they did not wear a seatbelt – 7 times the 9/11 total

Source: CDC, McAfee

Our Priorities?

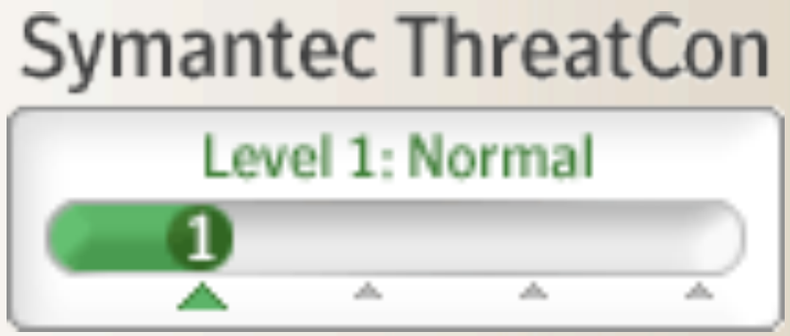
- Department of Defense is 2+ million people
- State Department and USAID combined have 10,000 people
- DOD budget is $700 billion
- Justice+Science+Foreign Affairs+Education is $100 billion …
  which is about the expected loss
  in cyber crime this year.

Source: CBO(2007), David Kilcullen, McAfee

So How Does This Apply to Cyber?

- The national posture is to
  - Make minimal investment until a crisis
  - Focus on a military response
  - Seek to "patch" rather than address root causes
- The same is how we have been approaching cyber security!

The State of Cybersecurity?



But the Situation is Grim

- Over 15,000 new malware instances per day
- 10,000+ hosts/day join botnets
- Thousands of unique phishing e-mails/ day
- 25% to 50% growth in incidents per year every year for a decade

Sources: John Thompson, Dan Geer, McAfee

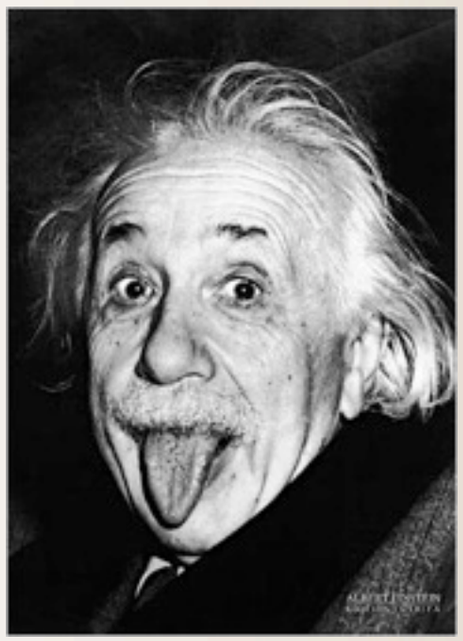
Big Picture

- Things are clearly getting worse!
- Trends over the last 15 years indicate *nothing* related to overall information security is getting better
  - except perhaps the market...
- Consumer confidence is waning, too

What are we doing to solve the problem?

To Date: Summed Up

Insanity: doing the same thing over and over again and expecting different results.



(Widely attributed to Albert Einstein)

To Date: Summed Up

Insanity: doing the same thing over and over again and expecting different results.

(Actually by John Dryden
[1631-1700],
from his play *The Spanish Friar* (act II)

Breaking With the Past

How can we do things differently?

Are we condemned to continue patching broken software?

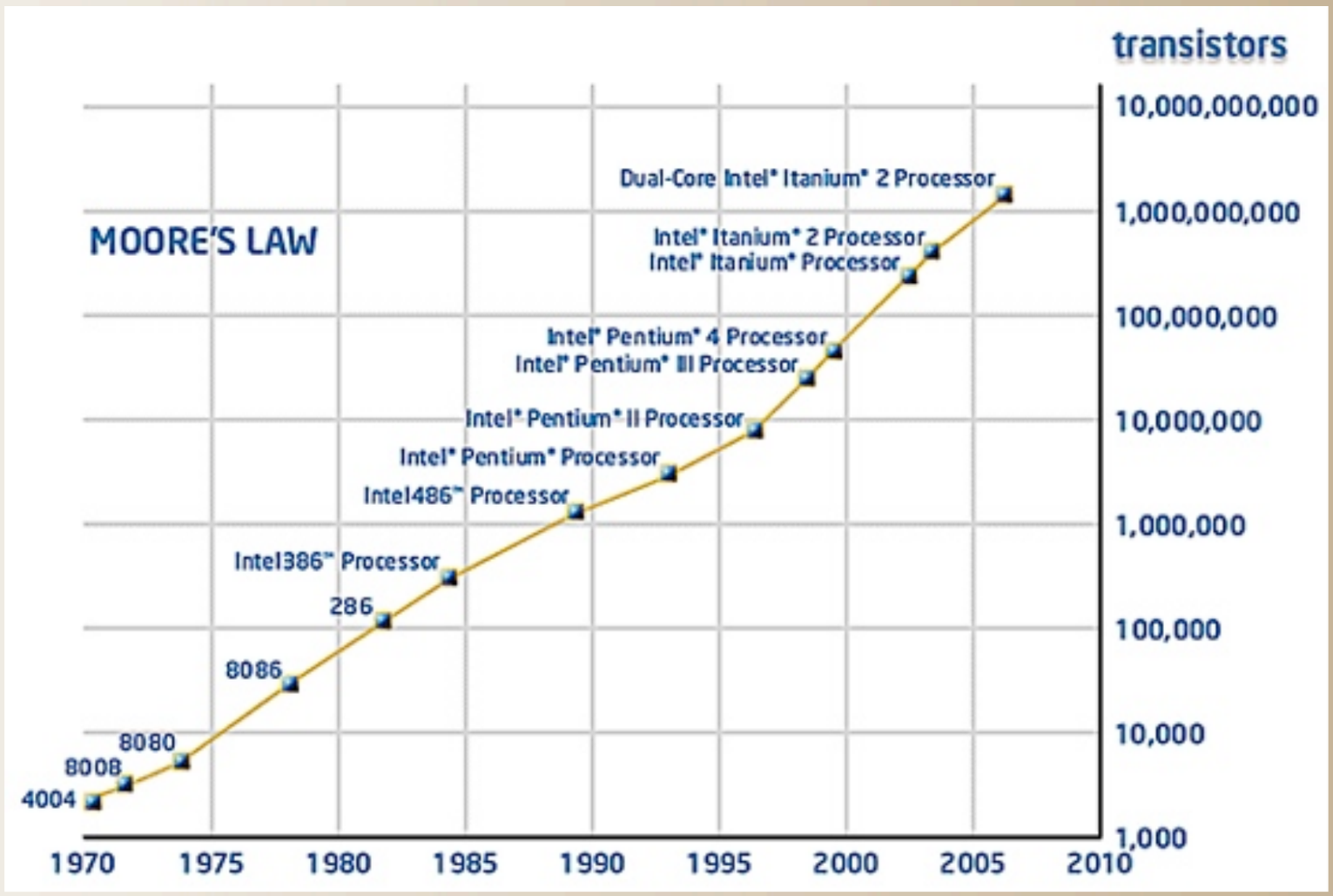
As researchers and educators, we can try to think about the world a different way.

Thinking Outside the Box

We should start by looking at computing itself.

What are some things we might do differently?

Computing has changed in 50 years!



Computing has changed in 50 years!

- In 1958 transistors were about $60 apiece (using current $$)
- In 2008 transistors were about $1/800,000 apiece – a drop of 7 orders of magnitude

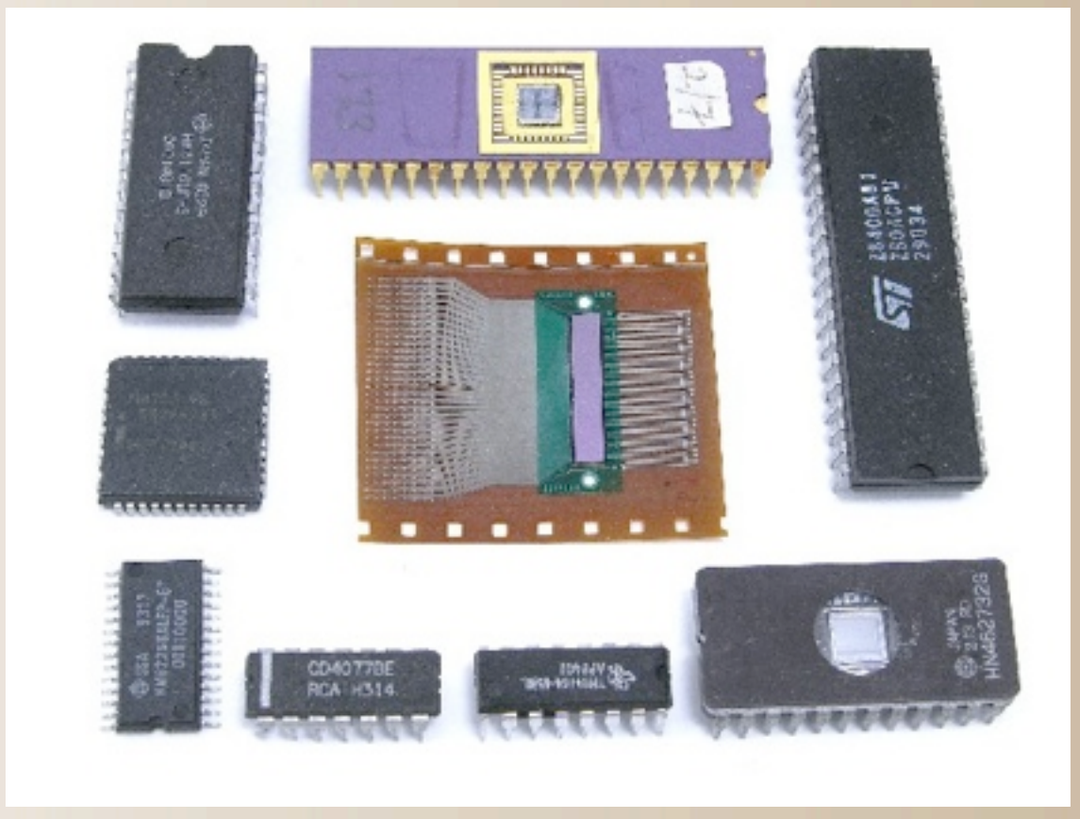
10,000,000,000,000,000,000
ten quintillion

- 10^{18}
- Grains of rice harvested in 2004

Courtesy of Ed Lazowska

10,000,000,000,000,000,000
ten quintillion

- 10^{18}
- Transistors manufactured in 2004



Disk storage, too

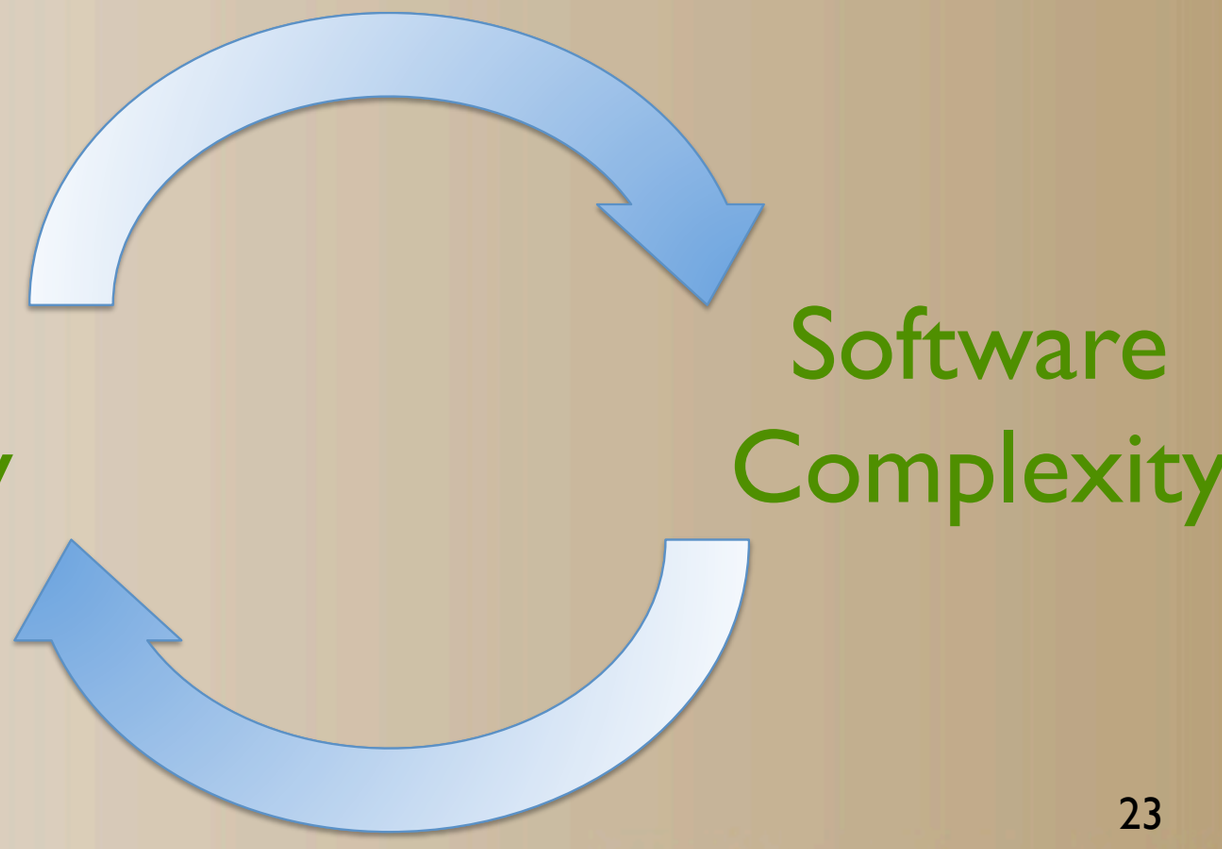
- Storage density in 1958 of about 2000 bits per cubic inch, about $.10 per byte (in current dollars)
- Storage in 2008 of about 425 Gbit per cubic inch, at about $.20 per 1 Gb
- ☆Price drop of $1.3*10^7$
- ☆Density increase of $2.3*10^8$

Consider

Courtesy of Ed Lazowska

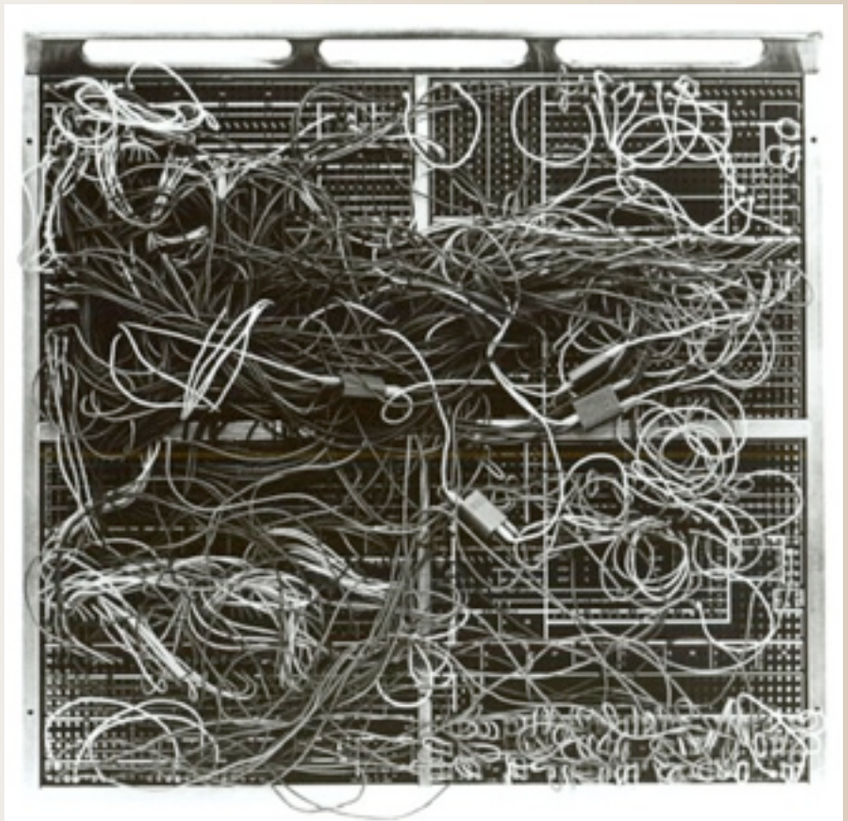
So why are we continuing to build on the past?

Engineering decisions based on available and affordable technology of their era still haunt us….

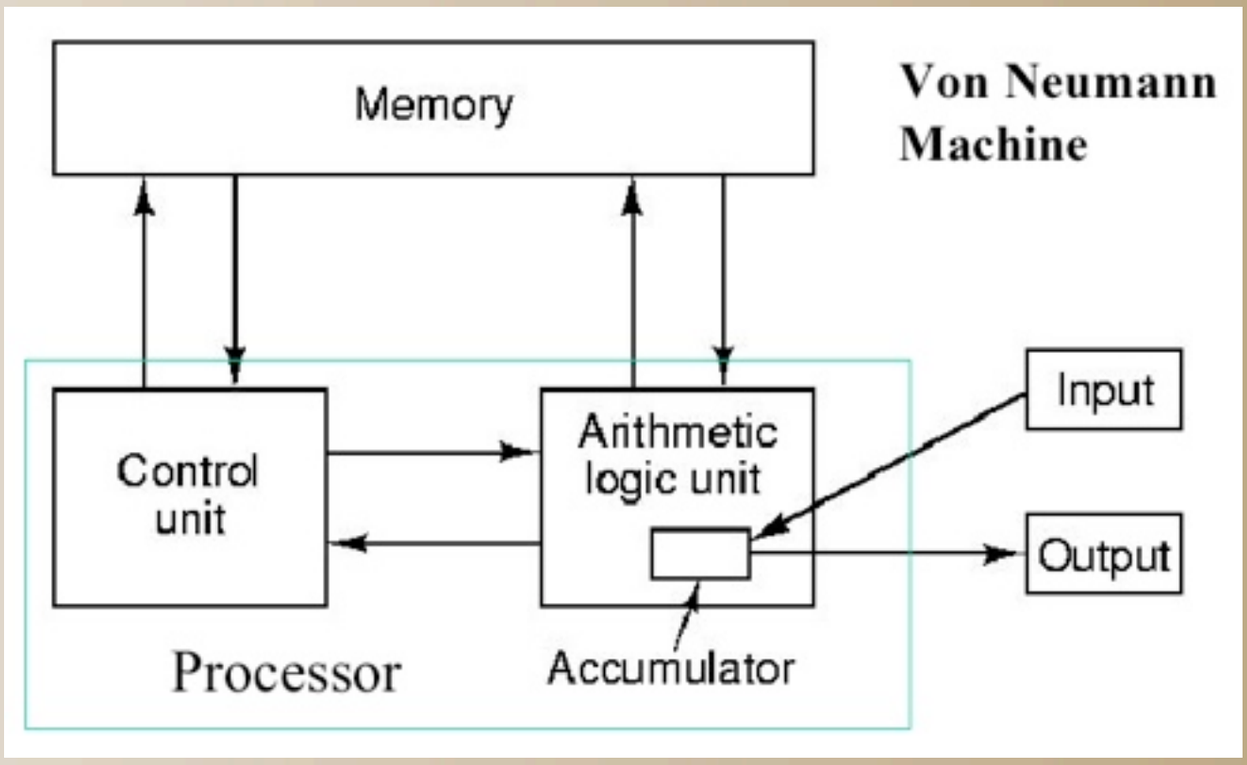


Example: von Neumann Architcture

- A breakthrough – programs were hard-wired prior to this.



- Some buffer overflow attacks enabled by executing data on the stack
- Code faults when errant programs overwrite memory
- What can we do by otherwise segregating memory?



Example: Paging

- Ferranti Atlas, 1961
- Memory was expensive
- Today, many (most?) systems don't need paging!

Example: Programming

- Once upon a time, we excluded array bounds checking and argument matching because of memory
- We also leave out pre-conditions, post-conditions, recovery blocks, and assertions.

  Why do we still do that?

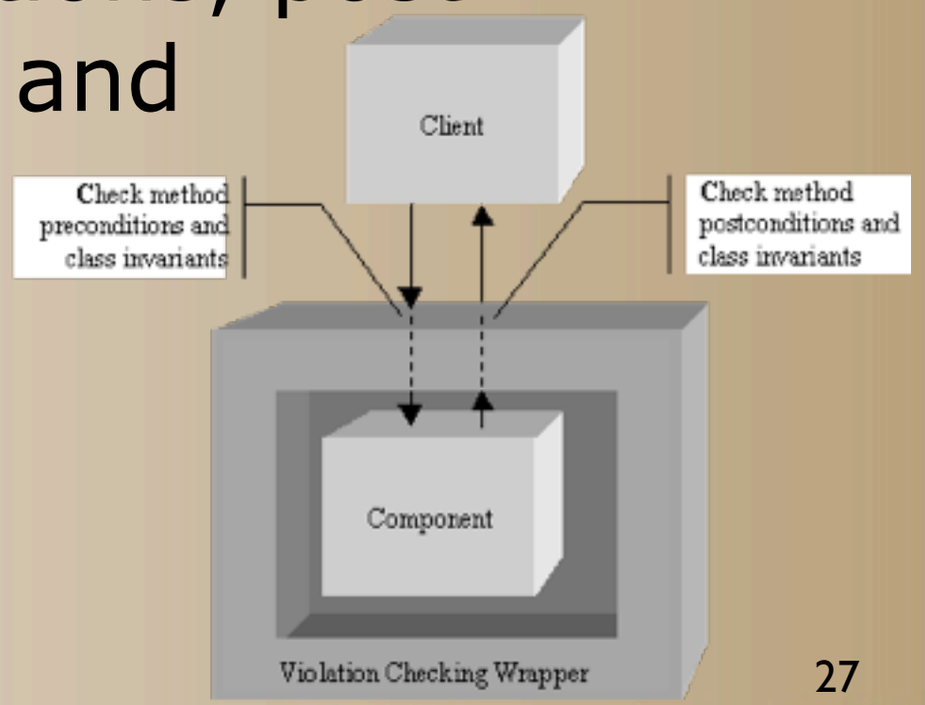
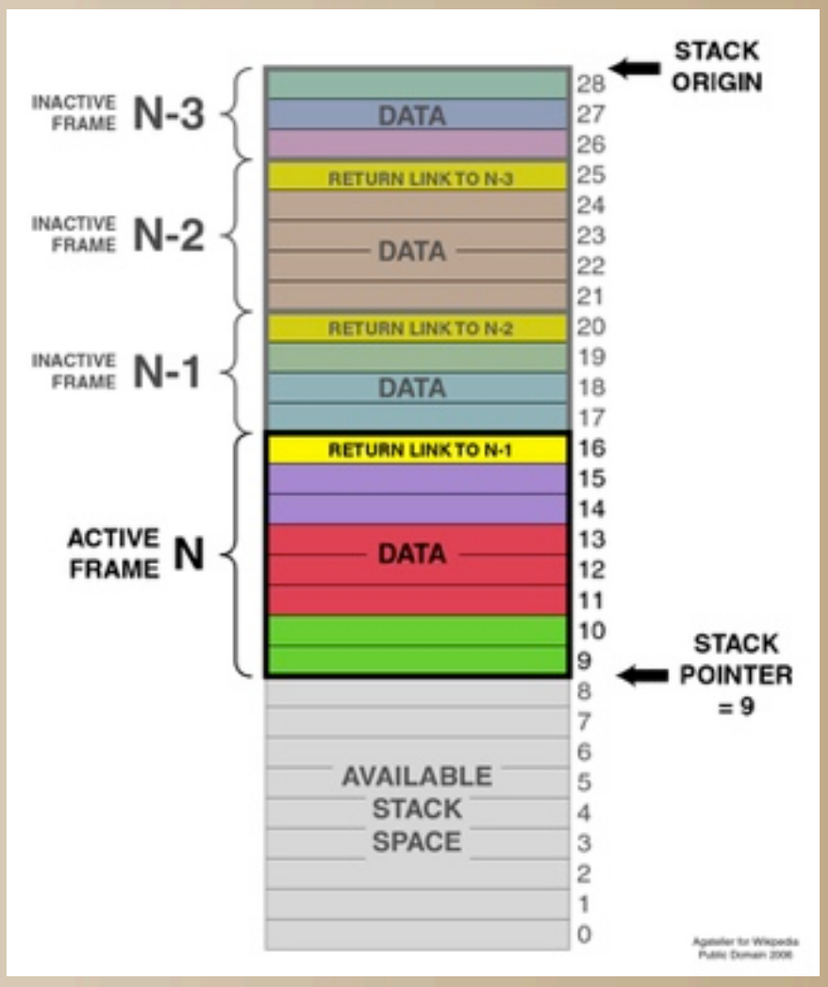


Figure 1. A wrapper subpoints the component implementing it.

Example: Stacks

- Prior to Algol 61, procedure calls used static control blocks co-located with code
- First stack machine ca 1958



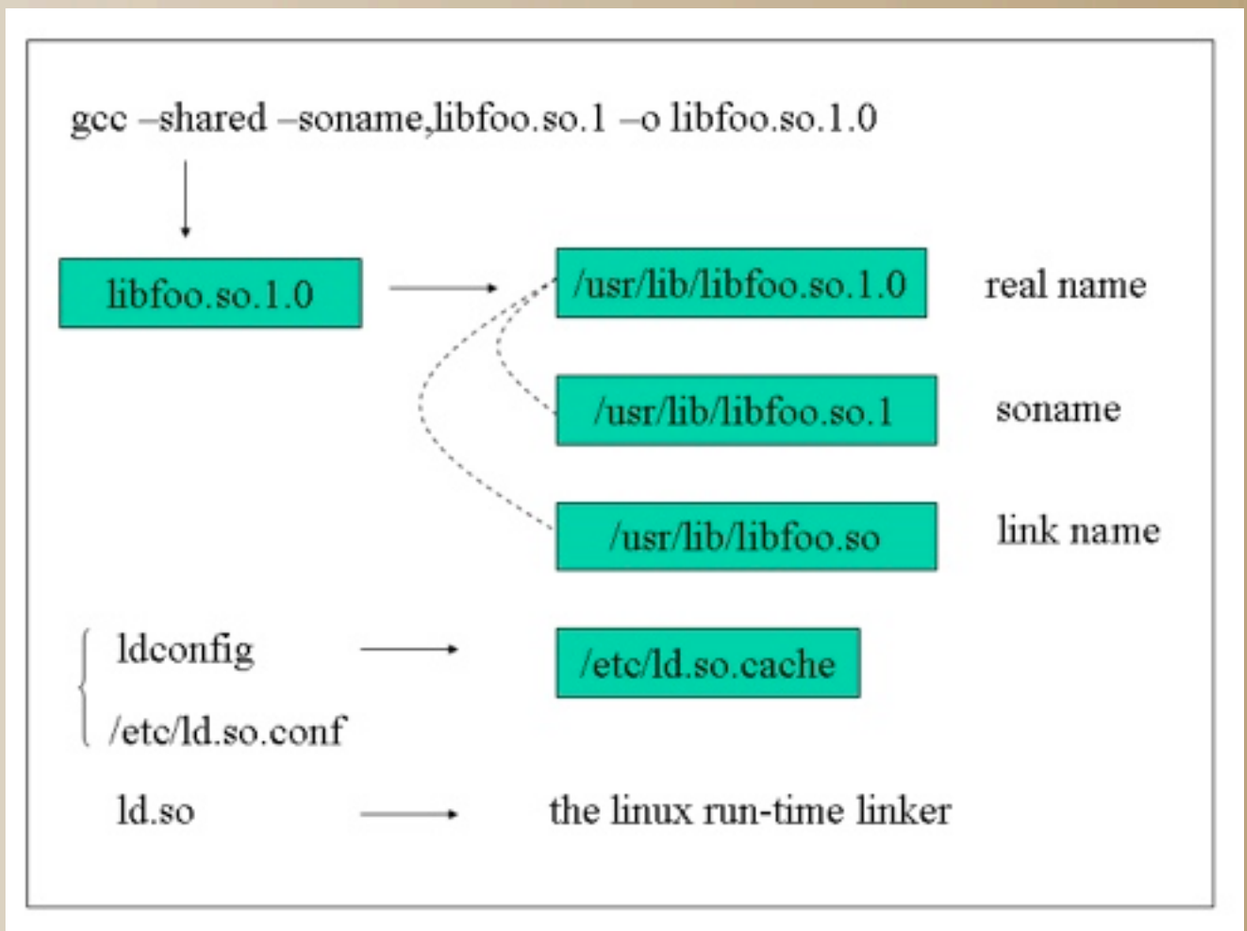
Why only a single stack?

Multiple stacks

- 1 for variables, 1 for subroutines, 1 for system calls….
- Or perhaps we can do something special with k stacks?
- Stacks of displays?

Example: Shared Libraries

- Memory is cheap
- Security is important
- Why don't we do them some other way?



Example: Testing

- Basic problem: thoroughly test software
- Methods explored
  - Symbolic execution
  - D-U path testing
  - Mutation analysis

Mutation concept

FinalQ := InitQ + 4.5 * Input - XSet;

FinalQ := InitQ - 4.5 * Input - XSet;

FinalQ := InitQ + 4.5 / Input - XSet;

FinalQ := InitQ + 4.5 * InitQ - XSet;

FinalQ := InitQ + 4.5 * Input - 4.5;

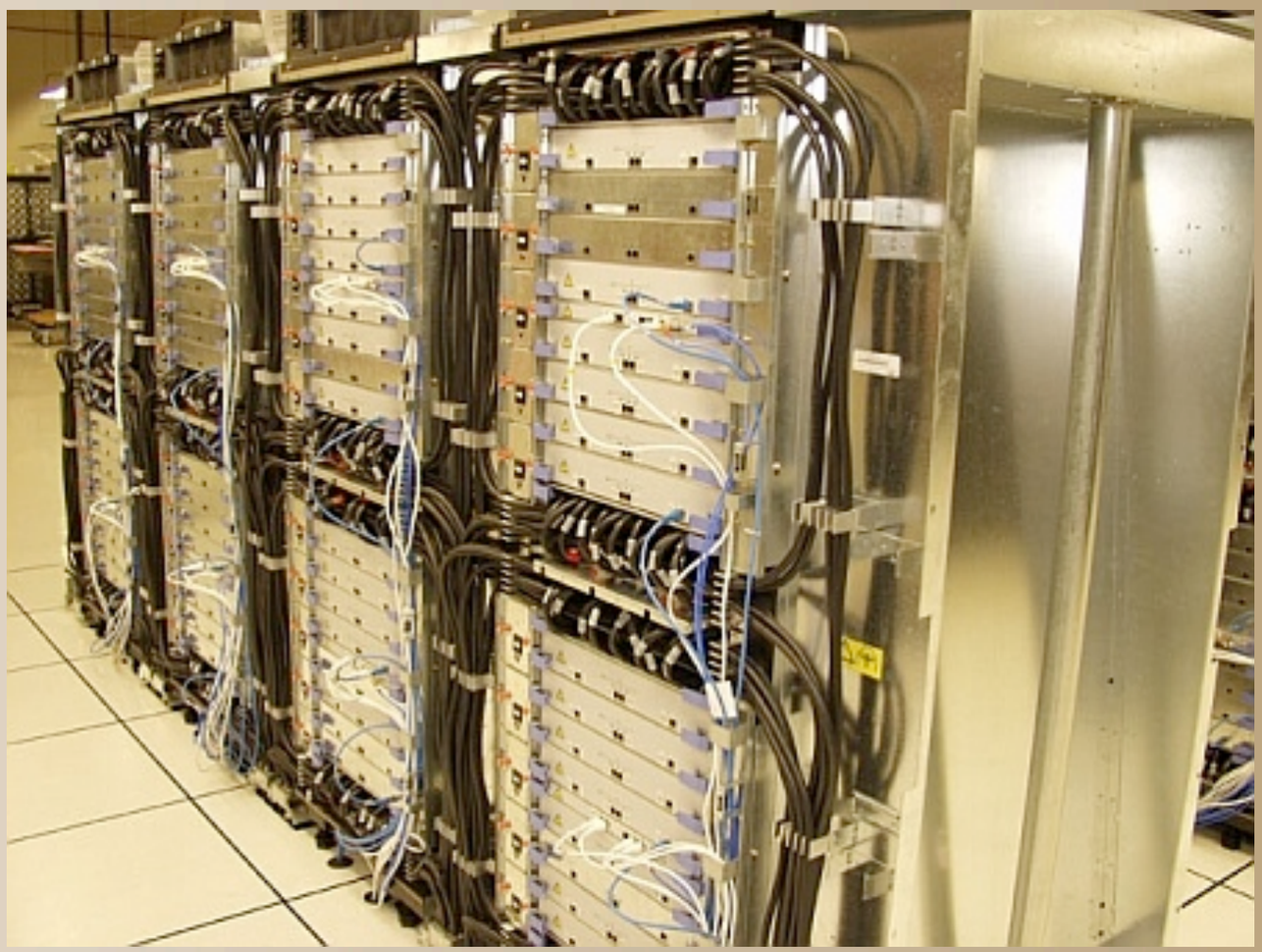
Mutation Goal

- Build a data set that can differentiate all non-benign "mutants" from the program, thus "killing" them.
- This takes a lot of time to generate and run each case!

But that was then…

This is now.

- Clusters are cheap
- Multicore is arriving
- Threads are a basic construct



Example: All-in-one OS

- Provide standard interface to devices
- Control sharing

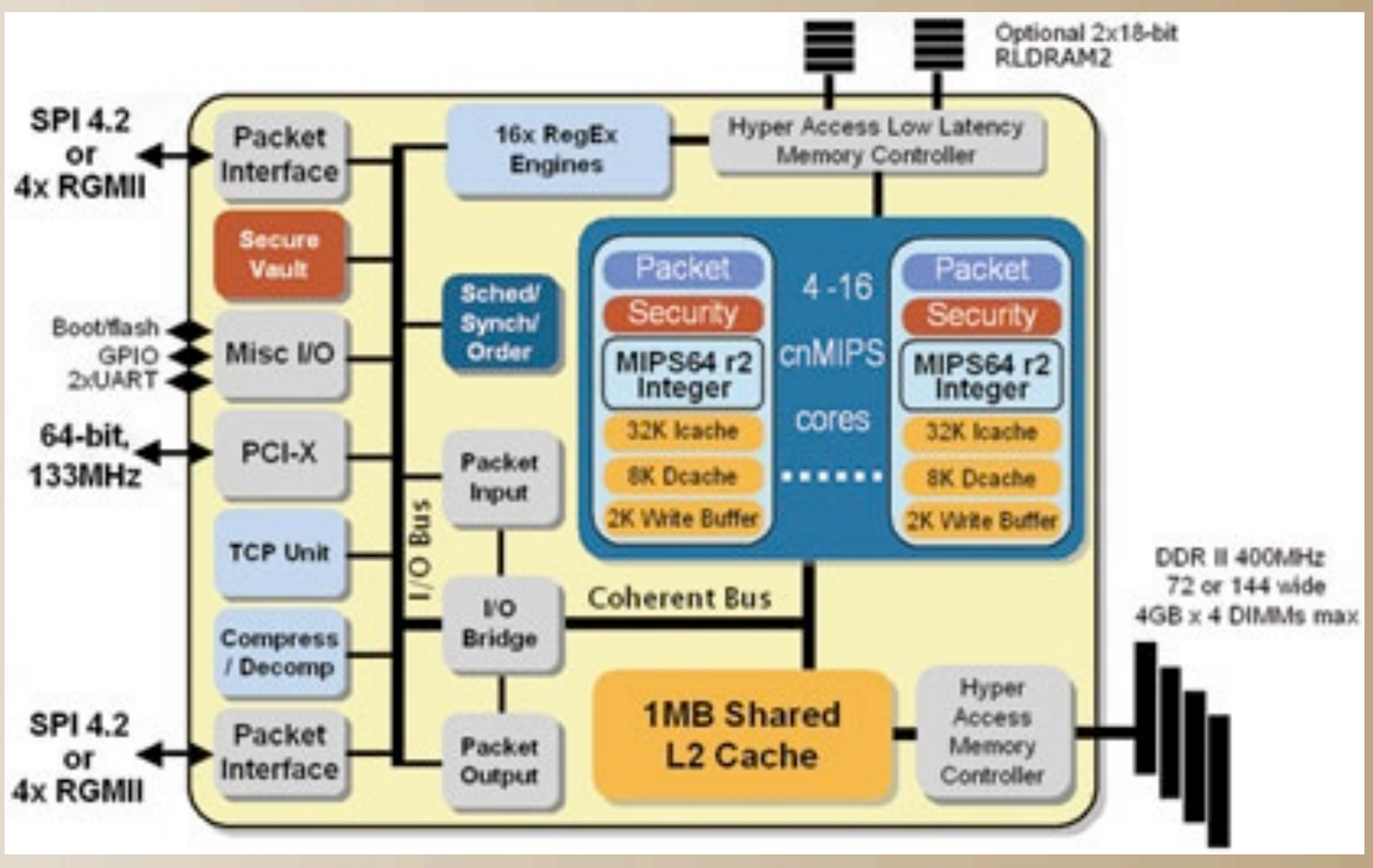
- But what if we didn't need to share? Could we dispense with the OS altogether?

Not so far-fetched

Use multiple processors!

Have each processor dedicated to small non-shared tasks

Idea behind the CERIAS Poly^2 Project



Think Minimization (Good Security)

- No need for a file system or disk if all state is temporary
- No need for address translation if it knows what it is connected to
- No need for extra device drivers
- No need for user shells or libraries

Other candidates

- File systems – big problems with latency and thruput, backups, and more
- Language design – need better mechanisms for reuse and testing.
- Databases – need provenance and self-checking built in
- Audit and forensics – need better support, including privacy

Complexity

$O(n) < O(n^2) < O(e^n)$

Right?

Complexity

Actually….

$O(n) < O(n^2) < O(e^n)$

means

$b_1n + c_1 < a_2n^2 + b_2n + c_2 < d_3e^n + ...$

More complex

- So, if you have an algorithm with the right coefficients, $O(n) > O(n^2) > O(e^n)$!
- What does this mean for design? Some tradeoffs that have traditionally been made — space vs. time, for instance — might be re-evaluated for some known cases...or multiple processors!

We have tremendous computational power at our disposal, and five decades of discovery behind us.

Discovery lies off the beaten path.

We should be thinking of how best to solve problems, rather than how to retrofit the tools at hand.

But, Some Results Take Time

http://www.physics.uq.edu.au/pitchdrop/pitchdrop.shtml

Think Outside the Box!

- Don’t assume current architectures
- Don’t waste effort answering the wrong questions
- Don’t be afraid to fail occasionally
  - But do document the issues!

Security in the 21st Century

It is not the enemies outside the gates that threaten us – it is the enemies within. Some we invited, and some have broken in. They are not a military problem, but a problem of crimes against civil society.

You, the specialists in information, are the front line defense as well as the targets. Don’t be constrained by the past when envisioning your future.

Thank You!