An Architecture A Day Keeps The Hacker Away

David A. Holland, Ada T. Lim, Margo I. Seltzer

Harvard University
Division of Engineering and Applied Sciences

{dholland,ada,margo}@eecs.harvard.edu

We’ve got a problem.

Why?

- Attacks are increasing.
- More exposed bad code than ever before.
- Patching systems doesn’t scale.
- Mindless automated attacks do scale.

Monoculture makes the world more fragile.

System/390 to the rescue!

Many, perhaps most, attacks are

- binary;
- not portable;
- written for the most popular platforms.

Use something else!

- Anecdotally, widely done.
- Doesn’t scale.

Well, we can fix that.

Making your own is too hard...

- Design and fab chips?
- Port the compiler and OS?

...or is it?

- Virtual machine monitors.
- Machine descriptions.

This scales, too.

Now anyone can make up their own machine.

Or you can generate machines randomly.

How does that work?

Simpleminded example:

Pick the byte size:

- 8 bits, 16 bits...
- 9 bits? 10 bits?

Pick the word size:

- 32 bits, 64 bits...
- 36 bits? 40 bits?

Pick the endianness.

What does this buy us?

A lot:

- Rules out a broad class of attacks.
- Blocks even novel exploit techniques.
- Single comprehensive approach.
- Puts script kiddies out of business! Maybe.

Doesn’t walk the dog, though.

Are there enough machines?

We draw a distinction:

- Code injection attacks;
- State corruption attacks.

We have overkill for code injection.

State corruption is harder to handle.

Caveats

Can exploits be generated from machine descriptions?

Is your machine description secret?

Can one attack whole sets of machines at once?

Reliability

QA is going to *love* this.

Reliability

QA is going to *love* this.

QA is going to *love* this.

What will it take?

Making the general source base portable.

Lots of toolchain engineering.

Some research remains.

Should we take the trouble?

It costs a lot.

But it buys us a lot.

Should we take the trouble?

Yes.

An Architecture A Day Keeps The Hacker Away

David A. Holland, Ada T. Lim, Margo I. Seltzer

Harvard University
Division of Engineering and Applied Sciences

{dholland,ada,margo}@eecs.harvard.edu

`http://www.eecs.harvard.edu/~syrah/`