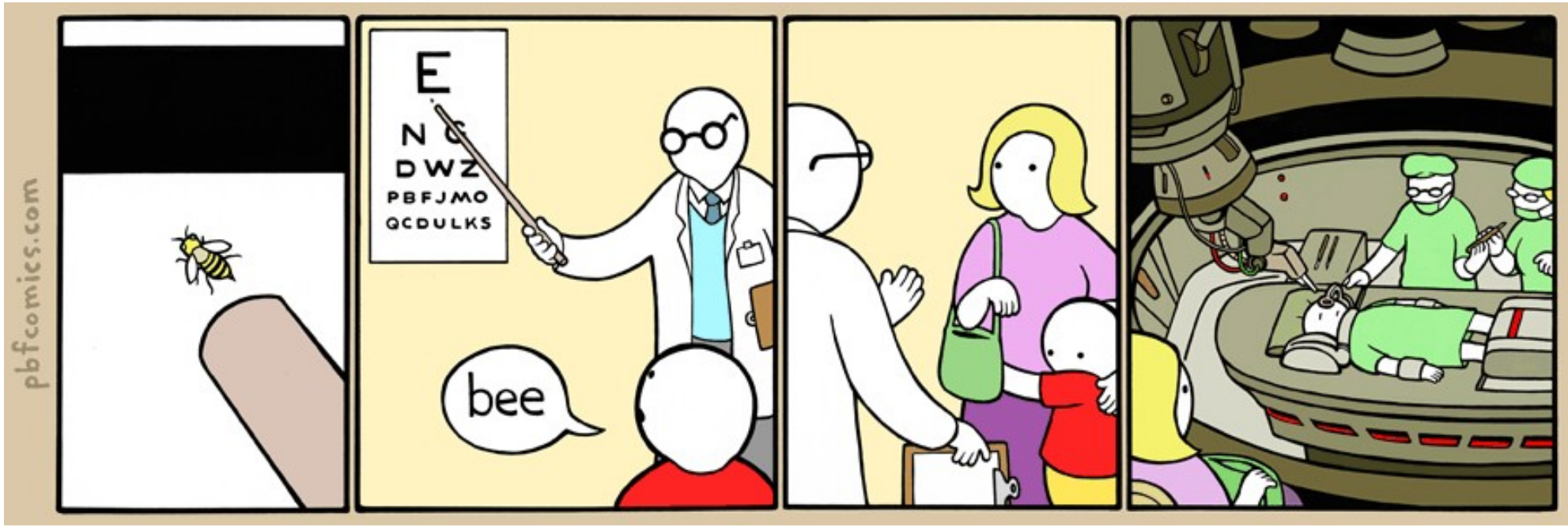
2020 Foresight: Web application security in 11 years

Trevor Jim
AT&T

Dagstuhl


pbfcomics.com
E
N C
DWZ
PBFJMO
QCDULKS
bee

It takes decades to make a technology an overnight success

Example:

Multiprocessors

(early 1960s)

Example:

Virtual memory

(late 1950s)

So what?

- Expectations
- What to work on
- What not to work on
- Lessons from past overnight successes

Example:

“Safe” programming languages

(1959)

“Safe”

- Low-level memory ops are correct
- Don't write where you shouldn't
- Don't write value you shouldn't
- Not safe: buffer overflow, format string attacks, integer overflows

Safety == garbage collection

- First safe language: LISP 1959
- LISP has won: all new languages are LISP
- Milestones: Java (late 1990s) and Javascript (mid 2000s)

Mid 80s GC: FAIL

2009 C programming: FAIL

"There's been a meme going around the open source community for a while now. That programming in C is somehow dirty, distasteful and worst-of-all inefficient compared to programming in a high-level language such as C# or Python."

2009 C programming: FAIL

"Don't feel tempted at this point to counter with a discussion about how great and flexible pointers are. You'll receive a lashing about how they're even more evil than people who talk in the theatre. The rant about the C problems of uninitialised memory, out of bounds pointer errors and segmentation faults is a timeless classic. Especially when they get to the bit about how much time was lost debugging them."

What changed?

- Dozens of GC theses improve GC
- Dozens of safer C theses do not improve C
- Moore's Law
  - Zorn study: 2.5 x overhead
- Web
- Different programmers

Prediction:

Prediction:

(Public key)
Encryption

(1970s)

1980s GC vs Encryption now

- Both failures
- Advantages obvious
- Not a total solution, but helps quite a bit
- Easy to deploy, easy for developers
- Perceived cost

Current uses

- Skype
- Blackberry, VPN, disk encryption
- Web app login (not whole session)
- Web banking
- Gmail (optional)
- Salesforce.com

Encryption FAIL

Last week of March, 2009

Vast Spy System Loots Computers in 103 Countries

By JOHN MARKOFF
Published: March 28, 2009

TORONTO — A vast electronic spying operation has infiltrated computers and has stolen documents from hundreds of government and private offices around the world, including those of the Dalai Lama, Canadian researchers have concluded.

Enlarge This Image

Tim Leyes for The New York Times

The Toronto academic researchers who are reporting on the spying operation dubbed GhostNet include, from left, Ronald J. Deibert, Greg Walton, Nart Villeneuve and Rafal A. Rohozinski.

In a report to be issued this weekend, the researchers said that the system was being controlled from computers based almost exclusively in China, but that they could not say conclusively that the Chinese government was involved.

The researchers, who are based at the Munk Center for International Studies at the University of Toronto, had been asked by the office of the Dalai Lama, the exiled Tibetan leader whom China regularly denounces, to examine its computers for signs of malicious software, or malware.

“In a puzzling security lapse, the Web page that Mr. Villeneuve found was not protected by a password, while much of the rest of the system uses encryption.”

Amazon wish lists

"By examining the source of Amazon's Universal Wish List toolbar bookmarklet, we find something suspicious: an HTTP GET that seems to modify data on behalf of the signed-in Amazon user. This is trouble, since Amazon is depending only on browser cookies to verify user identity."

Why not encryption?

- Cost: 12x (???)
- Verisign
- Green bar doesn't work

!!! Work on those things !!!

Also:

assuming encryption,
what would you build?

Don't work on:

- Non-encryption defenses for attacks which would be prevented by SSL, i.e., technology that tries to replace encryption with something faster
- DNS, ARP poisoning; DNSSEC ???