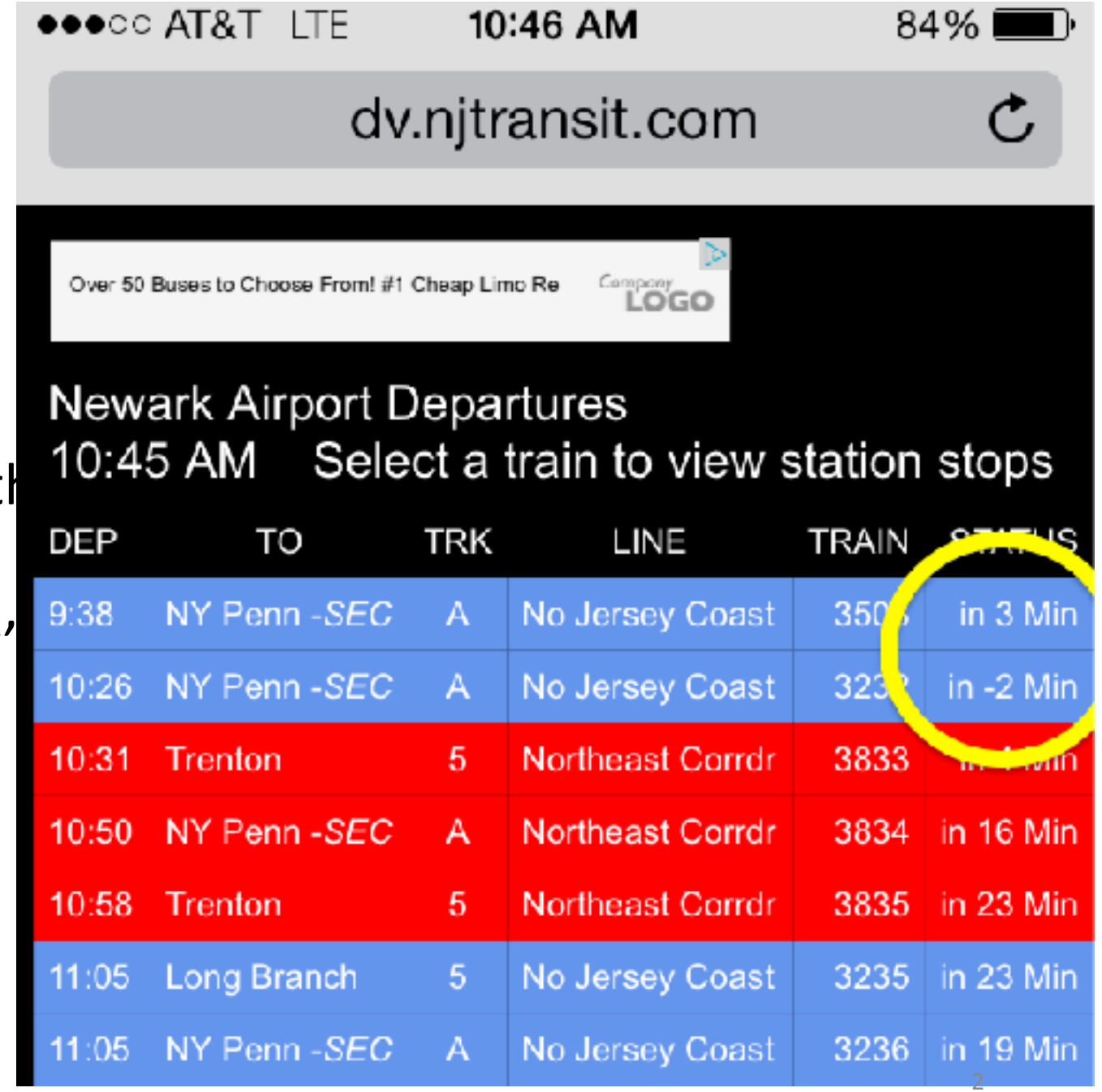
Software Complexity

Steven M. Bellovin

https://www.cs.columbia.edu/~smb

What Happened?

- Why is a train arriving in -2 minutes?
- Is the 10:26 running ahead of th 9:38?
- (We'll ignore the fact that they' both quite late.)



A Train Status Display

And in Washington…

The Washington Post

National Security

Chinese breach data of 4 million federal workers

By Ellen Nakashima June 4, 2015

Hackers working for the Chinese state breached the computer system of the Office of Personnel Management in December, U.S. officials said Thursday, and the agency will notify about 4 million current and former federal employees that their personal data may have been compromised.

The hack was the largest breach of federal employee data in recent years. It was the second major intrusion of the same agency by China in less than a year and the second significant foreign breach into U.S. government networks in recent months.Last year, Russia compromised White House and State Department e-mail systems in a campaign of cyberespionage.

Optimism

“The programmer, like the poet, works only slightly removed from pure thought-stuff. He builds his castles in the air, from air, creating by exertion of the imagination. Few media of creation are so flexible, so easy to polish and rework, so readily capable of realizing grand conceptual structures.”

Fred Brooks, *The Mythical Man-Month*

Reality Check

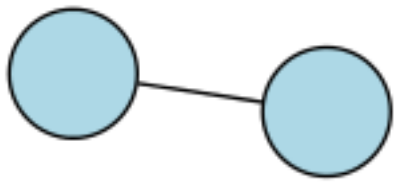
"[O]ne must perform perfectly. The computer resembles the magic of legend in this respect, too. If one character, one pause, of the incantation is not strictly in proper form, the magic doesn't work. Human beings are not accustomed to being perfect, and few areas of human activity demand it."

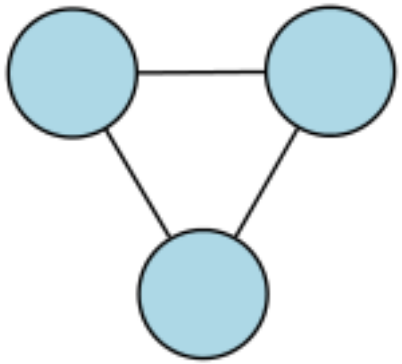
Fred Brooks, *The Mythical Man-Month*

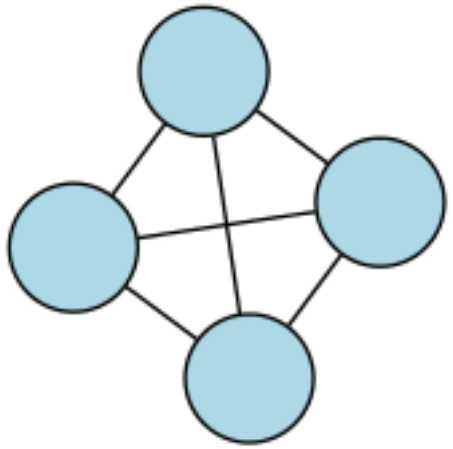
Real Software

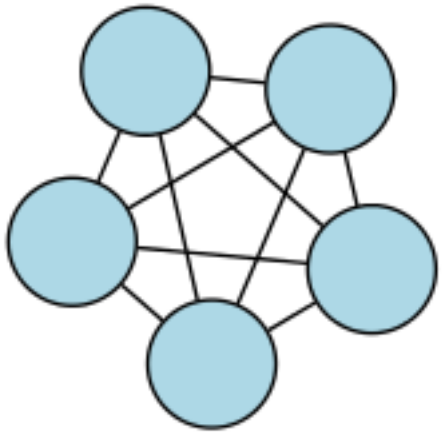
- Software is buggy
- Software is *always* buggy
- The bigger the program, the buggier the software—*always*

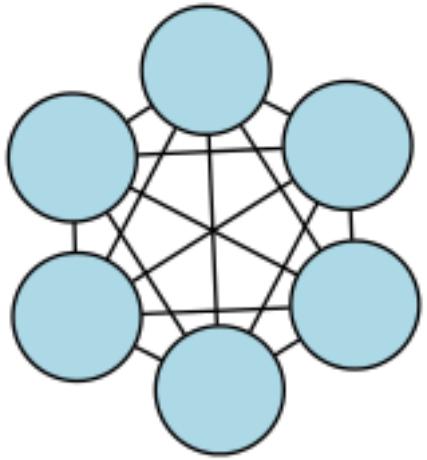
Why? Interactions

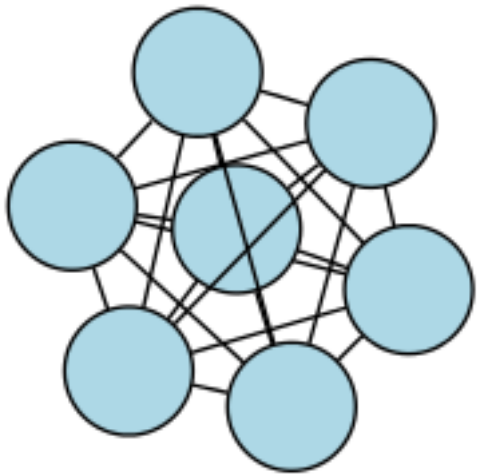






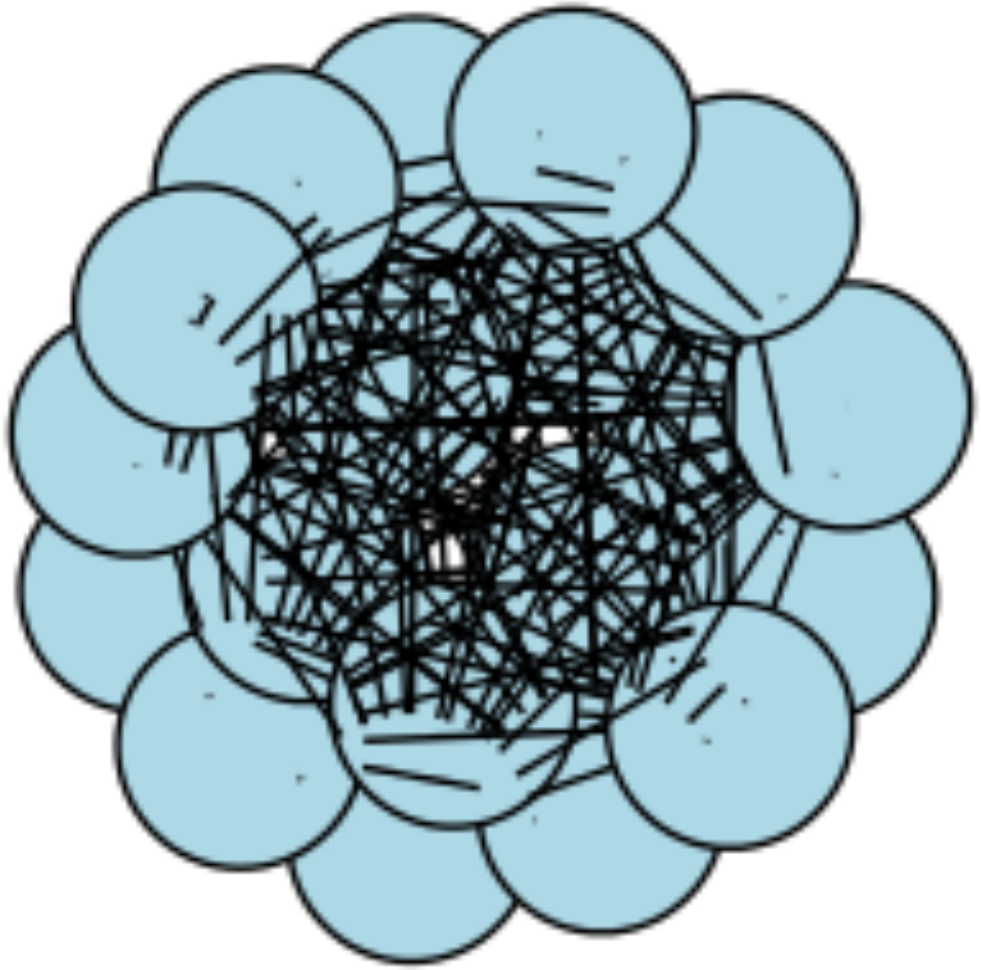






Complexity Kills…

With n components, there are roughly n^2 interactions



So?

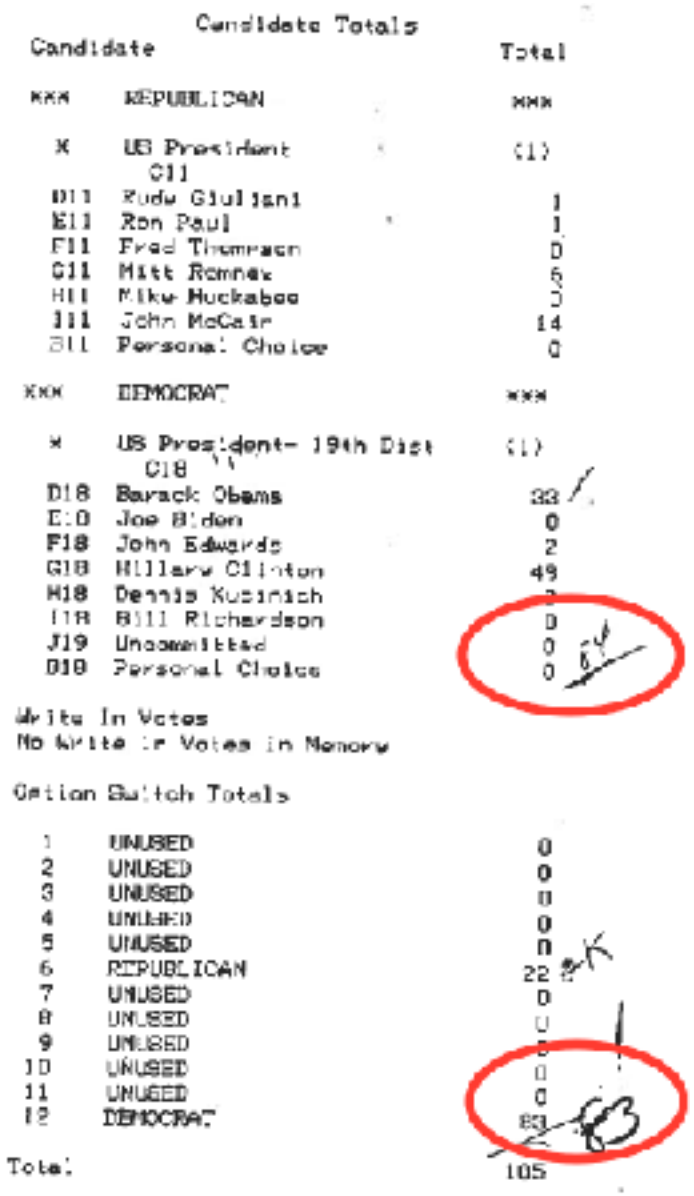
- There are limits to how good our software can be
- There are therefore things we can’t do
- More precisely, when we increase complexity we
  a) Increase the bug rate dramatically
  b) Increase the development cost dramatically
  c) Both!

Complexity and Current Events

- We bank online
- We buy things online
- We communicate online
- Why can’t we vote online?

Probably Just a Bug

A voting machine tape from the 2008 presidential primary in a New Jersey precinct.



Candidate Totals

Candidate		Total
***	REPUBLICAN	***
X	US President C11	(1)
D11	Rudy Giuliani	1
E11	Ron Paul	1
F11	Fred Thompson	0
G11	Mitt Romney	5
H11	Mike Huckabee	3
I11	John McCain	14
J11	Personal Choice	0
***	DEMOCRAT	***
X	US President- 19th Dist C18	(1)
D18	Barack Obama	33
E18	Joe Biden	0
F18	John Edwards	2
G18	Hillary Clinton	49
H18	Dennis Kucinich	2
I18	Bill Richardson	0
J19	Uncommitted	0
D19	Personal Choice	0

Write In Votes
No Write In Votes in Memory

Option Switch Totals

1	UNUSED	0
2	UNUSED	0
3	UNUSED	0
4	UNUSED	0
5	UNUSED	0
6	REPUBLICAN	22
7	UNUSED	0
8	UNUSED	0
9	UNUSED	0
10	UNUSED	0
11	UNUSED	0
12	DEMOCRAT	83

Total 105

(Photo by Ed Felten)

Enter the Adversary

U.S. Says Russia Directed Hacks to Influence Elections

By DAVID E. SANGER and CHARLIE SAVAGE OCT. 7, 2016

WASHINGTON — The Obama administration on Friday formally accused the Russian government of stealing and disclosing emails from the Democratic National Committee and a

NY Times

Going Dark

"As a result, although the government may obtain a court order authorizing the collection of certain communications, it often serves that order on a provider who does not have an obligation under CALEA to be prepared to execute it."

Valerie Caproni, General Counsel of the FBI

The FBI's Solution

- All communication systems need some form of access for law enforcement
- All encryption systems need a "back door" (which they call a "golden key")
- Can we do it?

Wiretap Interfaces are Hard

- Some years ago, the NSA evaluated the standardized wiretap interface on 26 different phone switches
  - *All* had security flaws
- Someone (probably an intelligence agency) hacked a cell phone switch in Athens and abused the wiretap interface
  - About 100 phones were illegally tapped, including the Prime Minister's

Cryptography is *Hard*

"Finally, protocols such as those developed here are prone to extremely subtle errors that are unlikely to be detected in normal operation."

Roger Needham and Michael Schroeder, "Using Encryption for Authentication in Large Networks of Computers"

From “Keys Under Doormats”

“We have found that the damage that could be caused by law enforcement exceptional access requirements would be even greater today than it would have been 20 years ago. In the wake of the growing economic and social cost of the fundamental insecurity of today’s Internet environment, any proposals that alter the security dynamics online should be approached with caution... The complexity of today’s Internet environment, with millions of apps and globally connected services, means that new law enforcement requirements are likely to introduce unanticipated, hard to detect security flaws.”

Abelson *et al.*

Why Technologists Oppose Golden Keys

- It has nothing to do with dislike of the FBI or the NSA
- Technologists can be victims of criminals and terrorists, too
- Rather, it's a question of crime *prevention*—the software necessary to permit law enforcement access has a high probability of opening up new security holes
- The root cause is the complexity of software

The Internet of Things

- We're connecting more and more "things" to the Internet
- These run on software; this software is often poorly written and *never* patched

Self-Driving Cars

- Almost certainly, we will see some crashes due to buggy code
  - Possibly (though not certainly), there will be crashes due to hacking
- Even today's "dumb" cars contain 50-75 networked computers
  - A modern car is actually a mobile data center!
- But—self-driving cars, flaws and all, will almost certainly be safer than human-driven cars
  - Cars don't get drunk, sleepy, distracted, etc.

Users Don’t See Most of the Complexity

- Good software often hides how complex it is
- But—the complexity is still there
- Often, it’s the parts you don’t know about that can cause the most trouble

So What Do We Do?

- Give up?

So What Do We Do?

- Give up?
- No; that sacrifices the benefits of computers. There are reasons (and generally good ones) why we rely on software

So What Do We Do?

- Give up?
- No; that sacrifices the benefits of computers. There are reasons (and generally good ones) why we rely on software
- Often, some small rate of failure is quite acceptable—nothing else is perfect, either

So What Do We Do?

- Give up?
- No; that sacrifices the benefits of computers. There are reasons (and generally good ones) why we rely on software
- Often, some small rate of failure is quite acceptable—nothing else is perfect, either
- The trick is knowing how to decide. We want major benefits, comparatively low risks, and acceptable consequences if there is a failure

“The competent programmer is fully aware of the strictly limited size of his own skull; therefore he approaches the programming task in full humility…”

Edsger Dijkstra, “The Humble Programmer”

Some Suggestions

Good

- Self-driving cars
- Communications apps

- The smart grid?

Bad

- (Residential) light bulbs
- Bike locks
- Anti-missile systems
- Voting machines

- Networked sex toys?

Questions?