University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

No Silver Bullets

CS 4950/5950
Homeland Security & Cybersecurity

Lesson 33
No Silver Bullets

Rick White, Ph.D.
University of Colorado, Colorado Springs

1
Esc

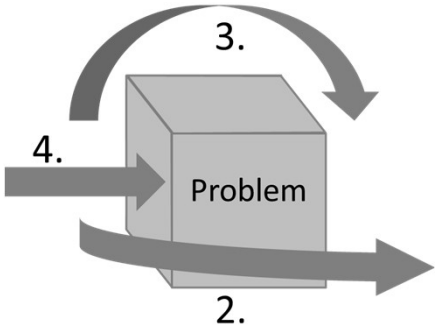
1

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

No Silver Bullets

- In the previous lesson we asserted that there are at least four general options for dealing with the cybersecurity problem: 1) ignore it, 2) go around, 3) go over, or 4) go through it.
- In that lesson we **ruled out options one and two**, and said that current approaches may be likened to option four.



2
Esc

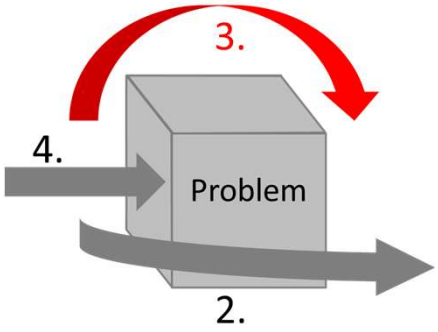
2

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

No Silver Bullets

- This leaves us with option three, “go over”.
- **Option three implies that we find an alternative solution that essentially renders cybersecurity unnecessary**.



3
Esc

3

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

No Silver Bullets

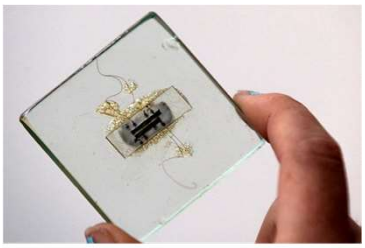
- What is needed is a revolutionary technological advance.
- It’s happened before.

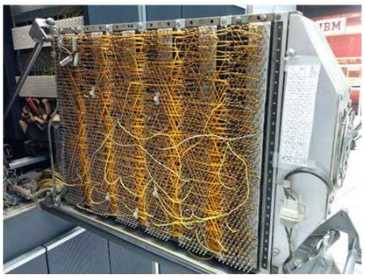
4
Esc

4

No Silver Bullets

- **The microchip was a revolutionary advance in computer evolution**.
- Before its development, computers were constrained in capacity by the problem of wiring together the increasing number of components.
- The microchip overcame this challenge by combining the fabrication of components and wires into a single step, leading to the incredible shrinking computer.

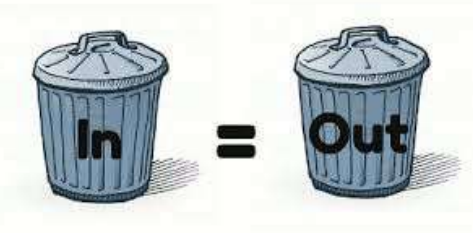




5

No Silver Bullets

- Despite its increasing power, though, the computer remains inherently vulnerable to cyber attack.
- In Lesson 10 we attributed this problem to the fact that **computers are basically stupid**.
- They are stupid because unlike humans, **computers are incapable of making value judgments** regarding their actions and will perform as directed regardless of the outcome, even if the consequences are catastrophic.



6

No Silver Bullets

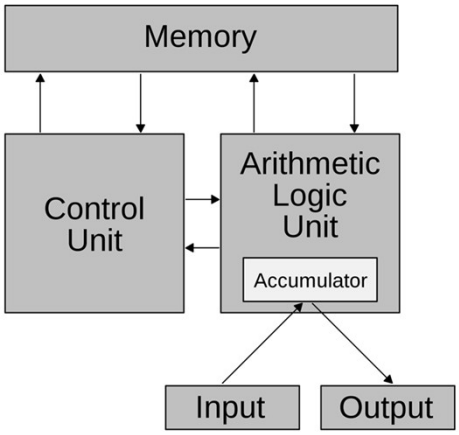
A computer's blind adherence to instructions is related to the three basic functions of its central processing unit:

1) fetch the next instruction,
2) execute the instruction, and
3) store the results.

7

No Silver Bullets

This is the **"Von Neumann Architecture",** so named for John Von Neumann, the famous polymath who first penned the concept in in his "First Draft Report on the EDVAC" in 1945.



8

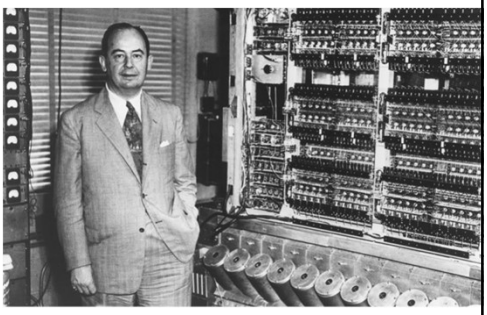
No Silver Bullets

- To be fair, the concept had occurred to J. Prespert Eckert and John Mauchly while they were building the ENIAC, the world's first electronic digital computer.
- Von Neumann drafted his report while observing construction of the ENIAC at the University of Pennsylvania.

9

No Silver Bullets

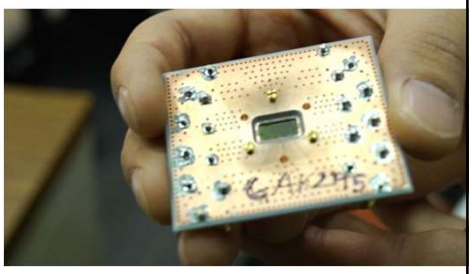
- Be that as it may, Von Neumann's report became the blueprint for 99% of today's computers, and it is this simple formula that has created the devilish problem of cybersecurity.
- **So the obvious answer is "let's find a new architecture."**



10

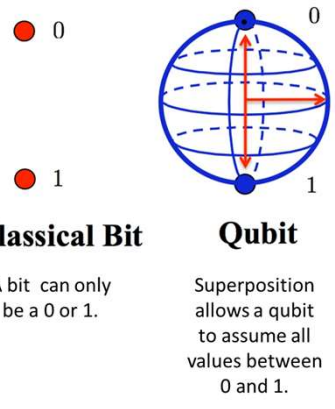
No Silver Bullets

- Perhaps the next biggest advance in computer architecture is **quantum computing.**
- Needless to say, it is completely different.



No Silver Bullets

- Computation in Von Neumann machines is predicated on the choreographed opening and closing of billions of microscopic circuits.
- **Computation in quantum computers is predicated on the quantum fluctuations of only a few atomic particles packaged into qubits.**



No Silver Bullets

- Ten years ago the prospect of building a quantum computer seemed improbable.
- Today, quantum computers are not only probable, they are commercially available.

No Silver Bullets

The state of the art for quantum computers today is comparable to the state of conventional computers in the 1940s**… it's still about getting the design and hardware right.**

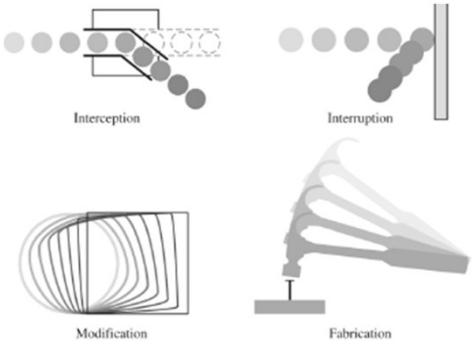
No Silver Bullets

- At any rate, do quantum computers hold the key to solving the cybersecurity problem?
- Can they lead to computers that can't be hacked?

15

No Silver Bullets

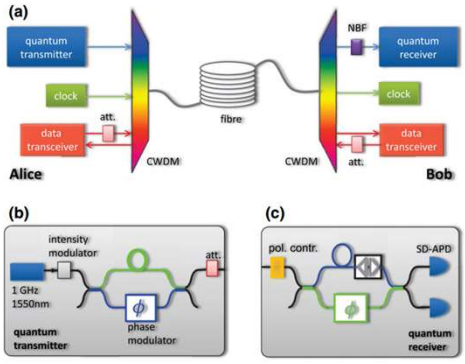
- The answer is "unlikely".
- To date, there's **nothing in their design that will inherently enforce confidentiality, integrity, and availability.**



16

No Silver Bullets

- Yes, current work on **quantum networks** make it easier to **detect interception**, but consider this may alternately be used as a means to **prevent availability**.
- **Also consider that quantum computers will make it easier to break cypher codes.**



No Silver Bullets

- And even if they don't, quantum computers **still can't overcome the insider attack**.
- So long as humans require access to a computer, conventional or otherwise, there will always be opportunity for malicious action.

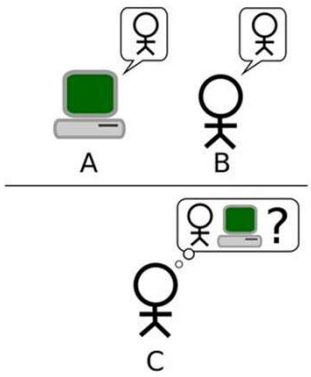
No Silver Bullets

- As of the moment, quantum computers offer no solution to the cybersecurity problem.
- **Is there something we can do, then, to make computers smarter, so they won't blindly inflict catastrophe?**

19

No Silver Bullets

- One answer might be **"artificial intelligence"**; that is, incorporate a controlling intelligence **so computers "know" not to commit actions that would result in catastrophe.**
- As humans, our bodies will process anything we ingest, but we "know" not to eat poison.



20

No Silver Bullets

- While AI has made great advances, particularly in the realm of human speech recognition, it still has a long way to go.
- The essential problem is that human intelligence is predicated on what we call "common sense".
- **The problem with common sense is that it's anything but common.**
- Put another way, **human intelligence has a great capacity for resolving ambiguity.**

No Silver Bullets

- A classic example is "a boy saw a bike in the store and wanted it."
- The question is, **what is "it"?**
- Is "it" the bike or the store?
- As humans we assume "it" is the bike, but that **reasoning rests on hundreds of subtle understandings and assumptions** that have yet to be successfully grasped by AI.

Disambiguity

A boy saw a bike in the store and wanted **it**.

No Silver Bullets

And even if these obstacles can be overcome, **do we want a computer that can countermand a human order based on its own reasoning?**

23

No Silver Bullets

- There was an interesting experiment by the Department of Defense where they trained a computer neural network to identify hidden tanks.
- **The program performed brilliantly in the lab, but failed utterly in the field.**
- The reason for the failure?

24

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

No Silver Bullets

- As it turned out, all the pictures used to train the AI program were taken of tanks on a sunny day;
- The AI program had learned to associate tanks with sunny days, but was incapable of recognizing tanks on a cloudy day.
- **The point is, we may be able to teach a computer, but we won't necessarily know what it learned.**

25
Esc

25

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

No Silver Bullets

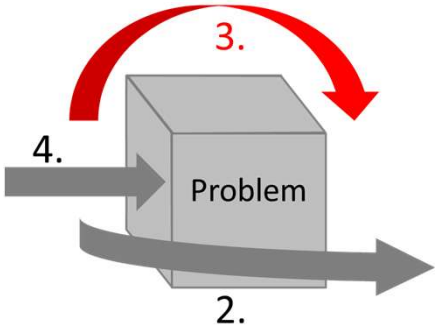
That may be acceptable for playing on Jeopardy, but not necessarily for controlling the electric grid.

26
Esc

26

No Silver Bullets

Given the current state of technological development, **there does not appear to be any technological solution on the current horizon that will eliminate the cybersecurity problem.**



27

Conclusion

Questions?

28