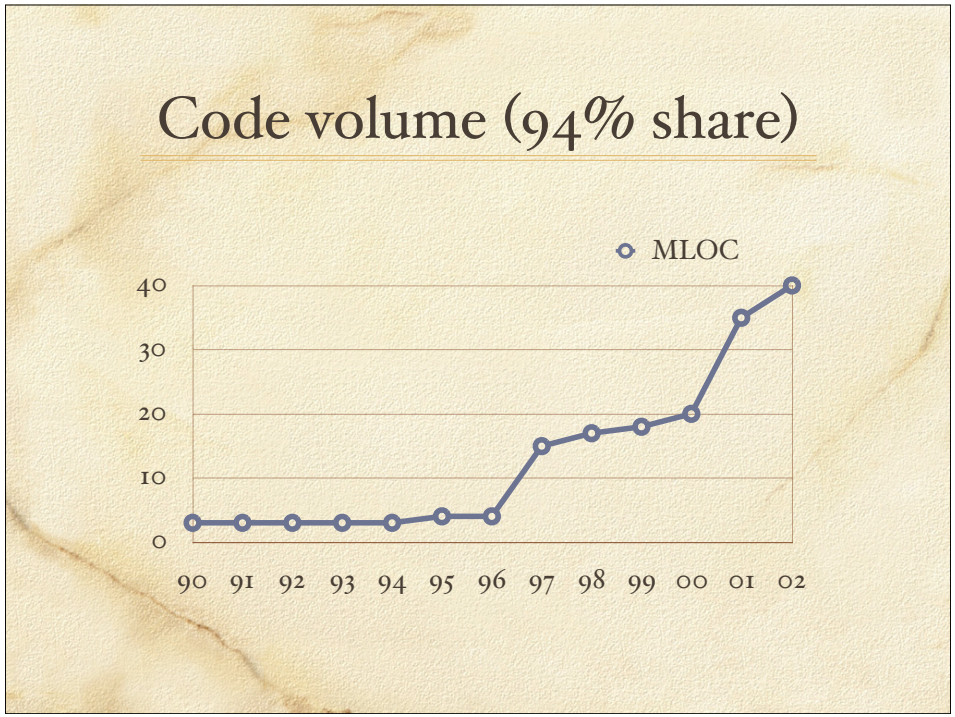
Cascade, Monoculture, Policy

Daniel E. Geer, Jr., Sc.D.

1

Daniel E. Geer, Jr., Sc.D.
Principal, Geer Risk Services
Post Office Box 390244
Cambridge, Mass. 02139

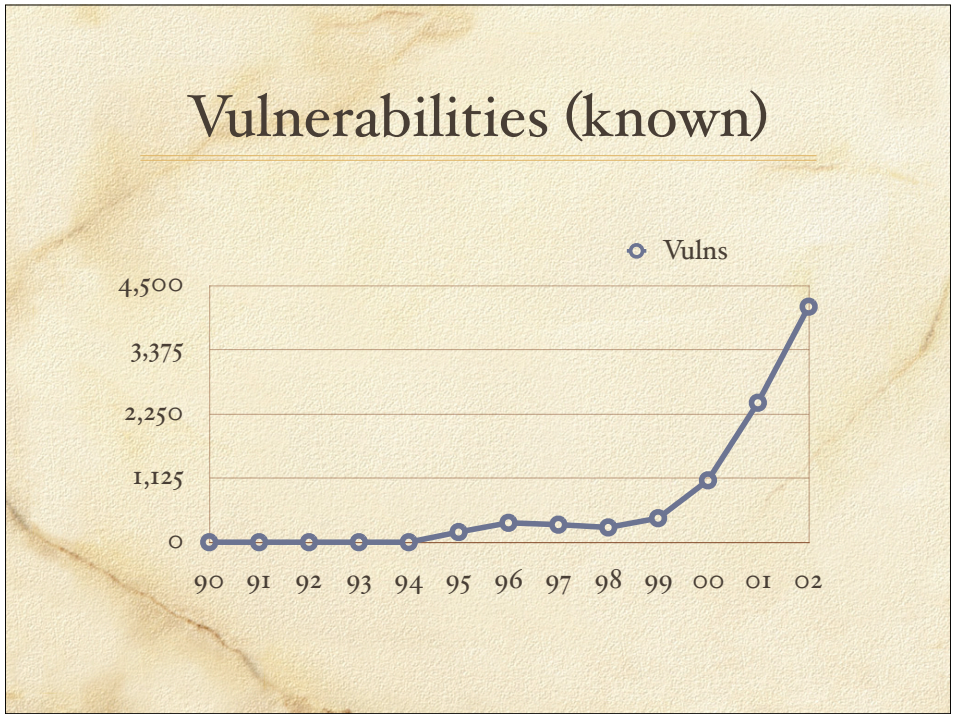


2

Windows 94% market share per IDC

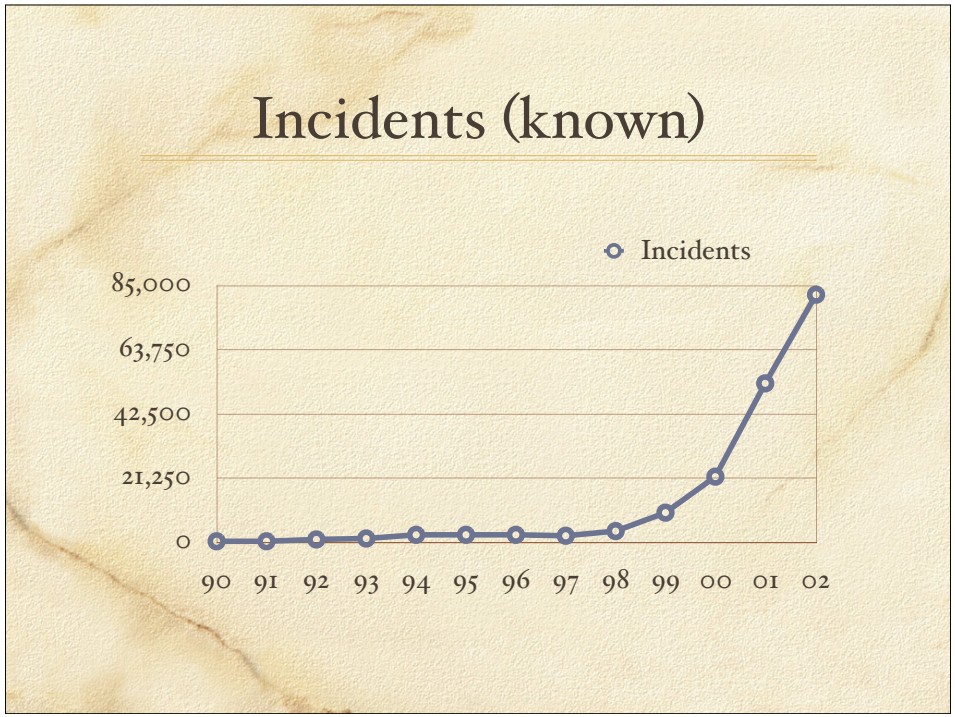
Code volume as observed:

Win 3.1	Win NT	Win 95	NT 4.0	Win 98	NT 5.0	Win 2K	Win XP
3	4	15	17	18	20	35	40
1990	1995	1997	1998	1999	2000	2001	2002

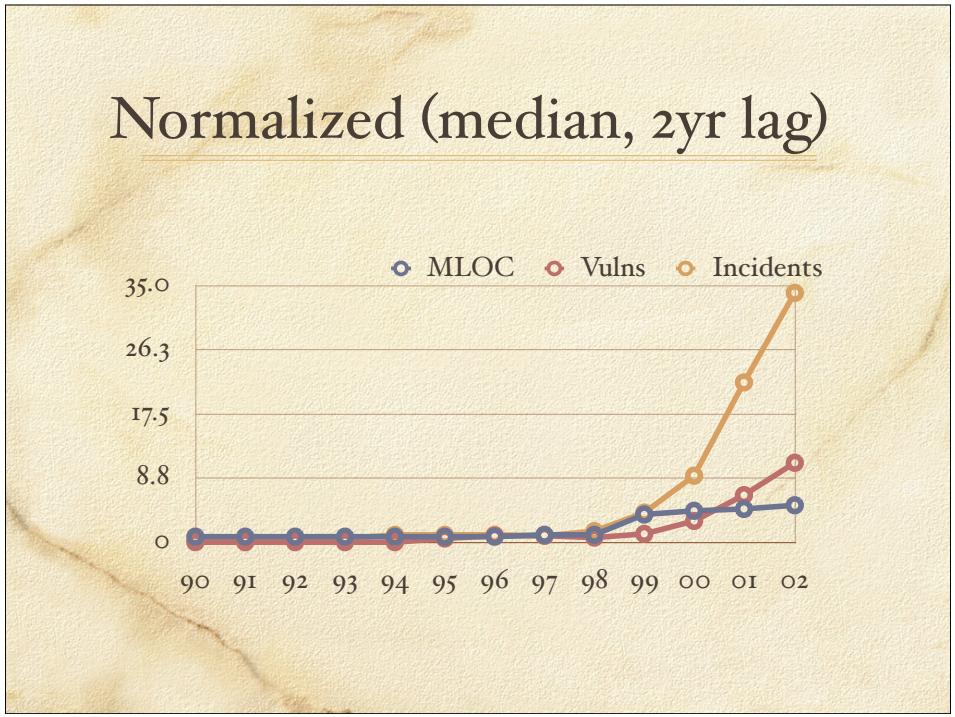


3

Public CERT data

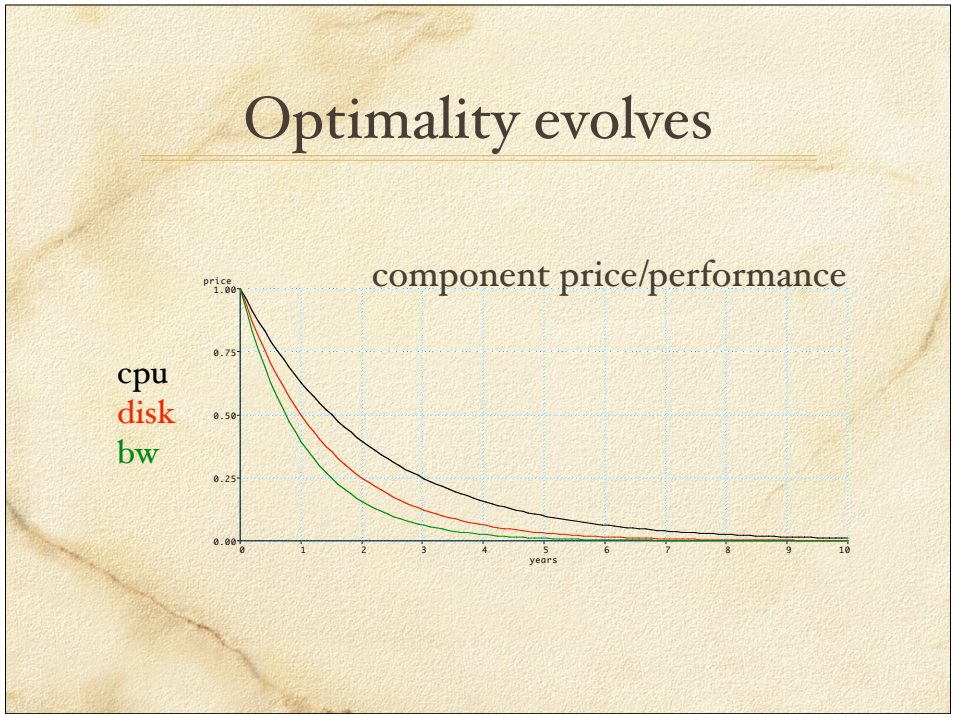


Public CERT data



Each curve is normalized against its own median over this period.

Code volume curve is shifted right two years to simulate diffusion delay.



6

Moore's Law is "cpu" curve, i.e., price/performance falls by 50% every 18 months.

Similar curves for data storage (halving at 12 months) and bandwidth (halving at 9 months). [These are lab results; market introduction is a lagged step function.]

Ten year outlook is, for constant dollars, two orders of magnitude for processing power, three orders of magnitude for data capacity, and four orders of magnitude for transmission capacity. This changes the economically optimal computing platform.

Thus do countermeasures

- WAS trust-mediated => the firewall
- IS application-mediated => the code scanner
- WILL BE data-mediated => tracking & sync

... As the threat rises the perimeter contracts

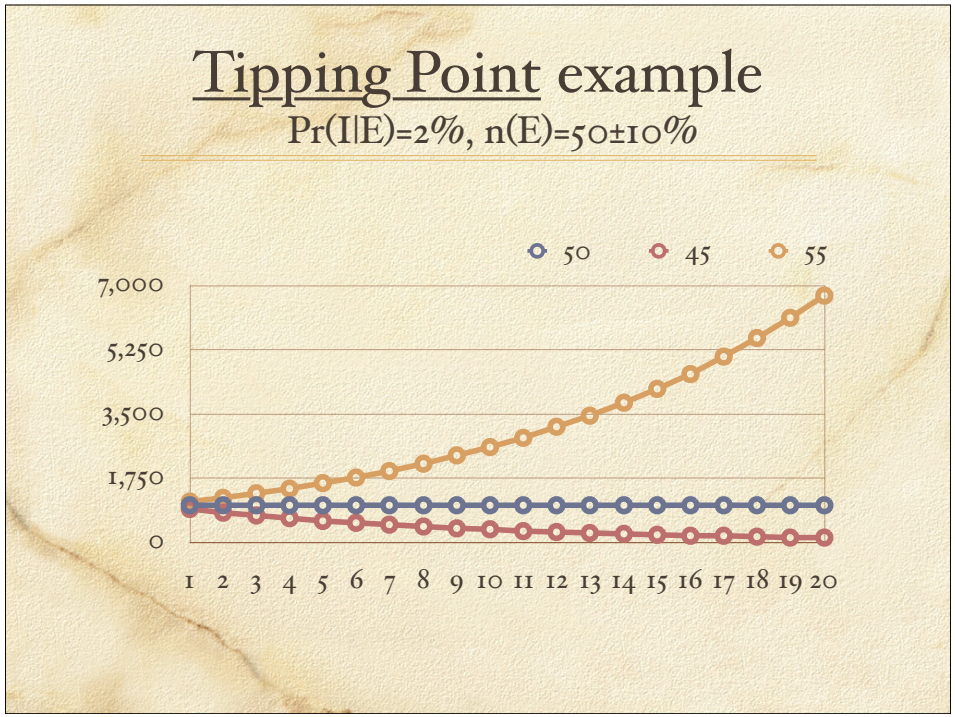
Security must be designed for what will be. Note that the change in optimality makes the question of external vs. internal attack scenarios largely moot.

Epidemics

- Characteristics of infectious processes
  - Pr(infection|exposure)
  - interval from infection to infectiousness
  - duration of infectiousness
  - interval from infection to symptoms
  - duration of acquired immunity

8

The math for modeling epidemics is well developed, as is the math for accelerated failure time testing, actuarial science, portfolio management, and others. There is no need, and no time, to invent new science before progress can be made. Steal these skills, and do so while the senior practitioners in security still include people with these sort of skills learned elsewhere. The hybrid vigor in the security field is at a maximum today before formal education begins to supply trained practitioners, rather than self-selected career changes as been the case heretofore.



This is simply the example used in Gladwell's The Tipping Point. It illustrates the chaotic nature of epidemics which is to say that small changes in initial conditions produce large changes in downstream values. This example is where the initial number of cases is 1,000, the probability of infection given exposure is 2%, the number of exposure events while infectious is 50 plus or minus 5 (10%), and the downstream shows that in only 20 days at -10% the disease will die out while in only 20 days at +10% the epidemic will be well underway.

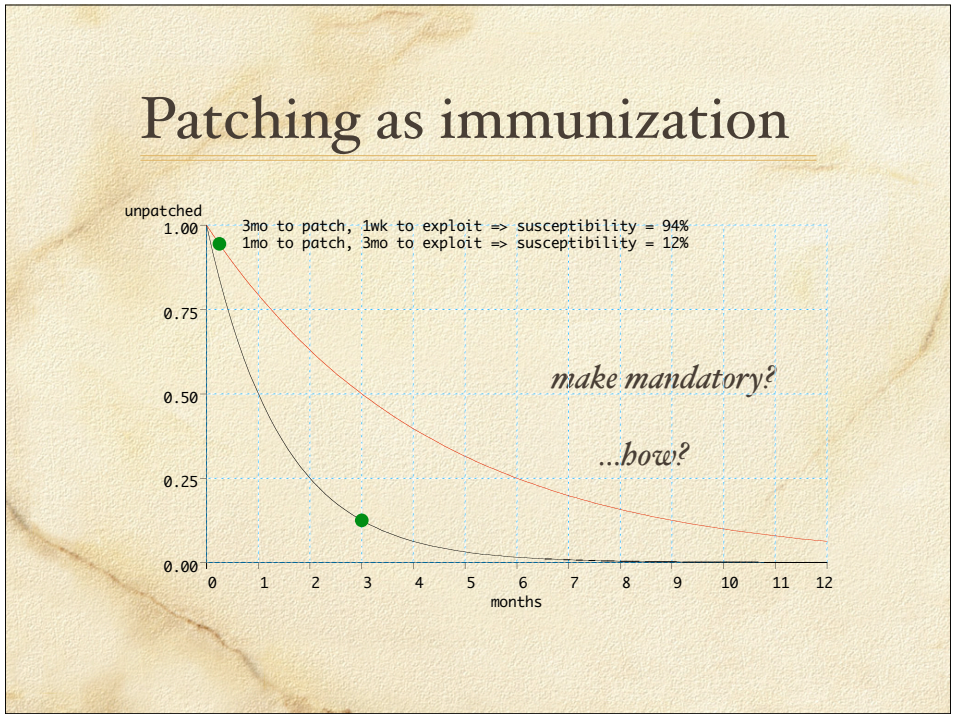
Worst case disease

- Pr(infection|exposure) = 1.0
- interval from infection to infectiousness = 0
- interval of infectiousness = open ended
- interval from infection to symptoms = indef
- duration of acquired immunity = 0 (mutates)

10

If you were designing a pessimal disease, it would be perfectly transmissable (100% chance of getting the disease once exposed and no acquired immunity), no symptomatic sign of infection, and an instantaneous conversion from pre-infection to infections (or from prey to predator, if you prefer).

The above describes worm propagation, or DDOS zombies, or the stockpiling of unannounced vulnerabilities.



11

Qualys, Inc., has data that implies patching is like radioactive decay in that 50% of the remaining unpatched systems will be patched in each succeeding “half-life.” Qualys’s figure is 30 days.

Posting a patch starts a race wherein the patch is reverse-engineered to produce exploits. The two data points are intended to bracket current reality. In the one case, if patching does have a one-month half-life while the reverse engineering interval is 90 days, then the susceptibility would be 12% at the moment of exploit. By contrast, if patching has a three-month half-life while the reverse engineering interval is one week, then the susceptibility would be 94% at the moment of exploit.

Time-to-exploit is shrinking while the time-to-patch is lengthening (if you factor in the growth of always-on, always-connected home machines) so the question becomes whether “mandatory” is a word we must use and, if so, what would it mean.

never enough time...
...so let's talk

Daniel E. Geer, Jr., Sc.D.
Principal, Geer Risk Services
Post Office Box 390244
Cambridge, Mass. 02139