Classic software disasters

- Summaries of some of the big software and hardware disasters of the last 40 years
- Look at what went wrong, how it could have been prevented
- Lots of other examples, big and small
- The industry is evolving and adapting, just slowly

Mariner 1 Rocket (‘62)

- Rocket had to be destroyed ~5 minutes after takeoff, seemed to be responding incorrectly to ground guidance
- Programmer mistake reading a handwritten formula (missed a superscript), resulting errors sent rocket off course

Hartford Coliseum collapse (‘78)

- Programmer of CAD software did not anticipate extra load the roof supports would face if one failed
- Resulting chain reaction brought down most of roof

Soviet gas pipeline explosion ‘82

- Soviet pipeline explodes in world’s largest non-nuclear blast
- CIA, working with pipeline software developers, injected flaws into the control software to trigger the blast

Early warning system false alarm ‘83

- Soviet early warning system indicated US launched five ballistic missiles, fortunately the duty officer reported it as a false alarm
- Software misdiagnosed sunlight reflecting off clouds, treating them as missile launches

Therac-25 radiation overdoses ‘85

- Therac-25 radiation therapy machine fires in high-power mode, subjecting patients to massive radiation doses
- During transition from old physical system to new software, became possible for operators to enter commands faster than system responded, resulting in theoretically “impossible” settings being used on live patients
- Race-conditions long recognized in hardware, this highlighted problem of software controlled timing systems

Wall Street crash ‘87

- Black Monday, DOW and S&P each drop >20%
- Sudden sales by wide range of investors triggered computer trading programs to invoke mass sell-offs, which in turn provoked more aggressive sell-offs, etc ... system overwhelmed with flood of sell orders and eventually crashed

AT&T outage ‘90

- 75 million calls and 200,000 airline reservations dropped, 9 hour outage
- A faulty switch took down one of 114 centers, but when the center came back up it auto-notified the others of a problem, causing them all to shut down
- The auto-notification was due to bug in one line of code in a software upgrade

Patriot Missile system failure ‘91

- Missile defense system failed to intercept incoming missile
- Caused by incorrect rounding in software system

Pentium division failure ‘93

- Intel pentium chip sometimes made mistakes in floating point division (off by ~0.0006%), resulting in lack of user confidence in the chip
- Problem came from a flawed division table in the chip (missing entries)

Ariane 5 rocket failure ‘96

- Rocket intentionally destroyed on first flight
- Guidance computer tried to convert velocity from 64-bit format to 16-bit format, overflow error resulted, sending control to a backup system which (of course) contained the exact same software error and also failed

Mars Climate Orbiter ‘98

- Orbiter fell into Mars atmosphere and crashed
- Software controlling orbiter thrusters assumed imperial measures (pounds of force) while other systems used metric (newtons)

Passport system failure ‘99

- UK passport agency implemented new software system, system was overwhelmed by demand and failed to issue passports on time for >500,000 citizens
- System lacked adequate testing and staff training, at same time as change in passport laws required many more people to get passports in a short time frame

Love virus ‘00

- Computer worm infected millions of computers, becoming most damaging in history (deleted files, altered registry, altered pages)
- Users infected via attachment in email, chat, worm propagated by sending itself to everyone in victim’s address book
- For many this was the first lesson in email security

FBI Virtual Case File project ‘05

- Massive attempt to upgrade FBI computer systems, eventually abandoned after four years of development
- Poor project management, outdated technology led to unusable system

Vaporware

- Software promised or announced but never released, particularly prominent in gaming
- Half-life 2 Episode 3, most infamous vaporware project in gaming? Periodically “in development” since ‘07
- Duke Nukem Forever, announced in ‘97, mostly unheard of for a decade before ‘10 release

US National Grid Gas project ‘12

- Software upgrade goes $1billion over budget
- Initial software upgrade resulted in incorrect wage and bill payments, subsequent fixes quadrupled cost of project

Heartbleed SSL flaw ‘14

- Widely used OpenSSL routine contained flaw allowing users to scrape memory from systems using heartbeat feature
- Feature allows regular timed pinging of server by sending a message and having server copy it and send it back
- Sender would specify length of message and the message, but correctness of length was never checked
- If sender sent 5 byte message but said it was 1000 bytes, server would send back 1000 bytes of memory

Prius software recall ‘15

- Hybrid systems would shut down while driving, >2.6 million vehicles recalled
- software glitch in engine control unit caused transistors to overhead, triggering fail-safe mode and causing hybrid system to shut down

Starbucks shutdown ‘15

- Register malfunctions prevent stores from processing payment transactions, causing 60% of US/Canadian stores to close
- Software malfunction in registers caused by “internal failure” during routine refreshes

Royal Bank Scotland missing payments ‘15

- 600,000 payments go missing overnight
- Bank was unable to process third-party file containing payment information

Early release from prison ‘15

- >3,000 prisoners released from prison early
- Software that calculates prison sentence miscalculated effects of good behaviour, triggering early release (average of 49 days early)
- Indications the problem had been ongoing for 13 years

Nest thermostat failure ‘16

- Nest ‘smart’ thermostat batteries suddenly drained, leaving its owners unable to control home temperatures in mid-jan
- Software update to device malfunctioned, causing the battery drains

WannaCry ransomware ‘17

- Ransomware cryptoworm attack on >200,000 machines running Windows XP/Server 2003
- Exploit (EternalBlue) takes advantage of Windows Server Message Block protocol
- Exploit believed to have been stolen from NSA
- takes down (among others) FedEx, Honda, Hitachi, Boeing, NHS England, Nissan UK