Software and Security Engineering Case Studies

Kevalee Shah

May 27, 2019

Contents

1 Electric Bike **2**

2 Hacking Jeep **2**

3 Nuclear Bombs **2**

4 Genziah Collection **2**

5 Role Based Access Control **3**

6 Chevrolet 1959 vs 2009 **3**

7 Infusion Pumps **3**

8 LinkedIn Password Compromise **4**

9 John Podesta Email Compromise **4**

10 Lottery Scam **4**

11 Volvo accidents **4**

12 Apple and Amazon Security Flaws **5**

13 Ordering wine in a restaurant **5**

14 DigiNotar **5**

15 Patriot Missile Failure **5**

16 Apple's goto fail bug **6**

17 Clallam Bay Jail Inmate **6**

18 Morris Worm **6**

19 London Ambulance Service Disaster **7**

20 Barry Boehm **7**

21 Mythical Man Month **7**

22 Tacoma Narrows Bridge **7**

23 Ariane 5 1996 **7**

24 Therac-25 Radiotherapy Machine 1985-1987 **8**

25 Boeing 737 Max Crashes **8**

26 Panama Crash 1992 **8**

27 Kegworth Air Disaster **8**

1 Electric Bike

Electric bikes have a maximum speed. This would be enforced by counting the number of revolutions the rear wheel makes by counting the times it passes the sensor in a certain period of time. A 'badassbox' supresses the sensor for every other revolution and therefore can travel at double the speed.

This example shows how humans affect seemingly secure systems. Shows the definition of a system can be quite broad

2 Hacking Jeep

Hackers were able to remotely hack a jeep and while on the motorway. First they did harmless things like turn the radio up and the windows down. But then they started affecting the steering and the wipers so the driver couldn't see

This example shows the architecture matters, defence should be done in depth, have seperate subnets and capable firewalls. Lots of legacy protocols trust *all* networks - which allowed things like this to happen

3 Nuclear Bombs

Nato countries require three things before a bomb can go off: authorisation (code), intent (pilot presses release), environment (N seconds 0 gravity). Need all three to make it work.

Shows how there can be independent and multiple mechanisms to increase safety.

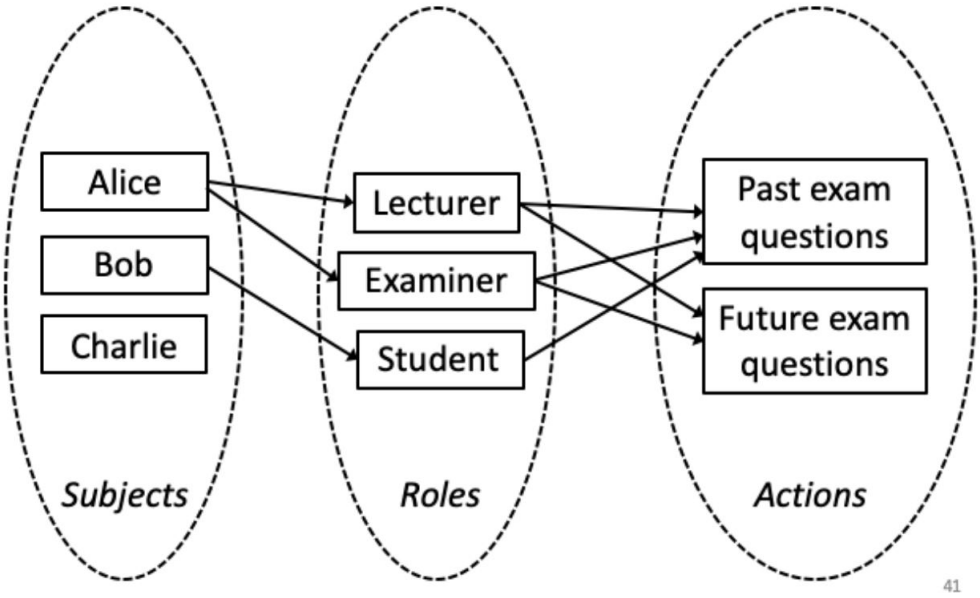
4 Genziah Collection

Jewish Bankers in Old Cairo used a double-entry book keeping system even in 11th century AD. Double-bookkeeping is when each entry in one ledges is

matched by an opposite entry in another. A different subject manages each ledger and therefore both bookkeepers have to collude to defraud.

5 Role Based Access Control

Add a level of indirection between subjects and actions a subject can carroy out - e.g. roles:



6 Chevrolet 1959 vs 2009

The crash test done between the 2009 Chevrolet Malibu and the 1959 Chevrolet Bel Air. New cars show how much more protection is provided by the new car. The new cars control the dummy movement a lot more and minimise injury.

This case study is to show how companies often used to blame users when things went wrong, however over a few decades the motor industry is starting to take responsibility. Same needs to be done for the computer industry.

7 Infusion Pumps

Infusion pumps used in hospitals all have different controls and therefore tired and overworked nurses often end up administrating the wrong doses. Even same models have different interfaces and the pumps have a range of keyboard layouts and even how key presses are interpreted are different.
11% of patients in UK hospitals suffer adverse events - half are preventable. Medication errors are one of the most preventable errors. 17% of medicatiton errors involve miscalculation of doses, incorrect expression of units or incorrect

administation rates. E.g. comparable to road accidents
All designed with different controls to retain customers (i.e. too difficult to retrain staff on different systems). Lead to errors in operating although this was often blamed on the nurses operating them. Issues with device included allowing multiple decimal points to be added and the first one chosen (arbitrarily). Some devices allowed non numerical input for numerical fields. Inputs sometimes truncated also leading to generally incorrect inputs. (Thimbleby paper). Need to standardize but shouldn't kill off competition.

The importance of user testing is high lighted and how much humans affect a seemingly robust system. Also the blame is put onto nurses when really bigger stakeholders should be taking responsibility. Incentives are vital.

8 LinkedIn Password Compromise

June 2012 6.5 million LinkedIn passwords were stolen, cracked and posted on a Russian forum. It was relatively easy to crack as the encryption used by LinkedIn did not have a salt. Since people often tend to resuse passwords, the hacked passwords were used on third-party sites as well such as paypal.

This hack demonstrated the dangers of cybersecurity and resulted in a push for legislatiton. Once again shows victim blaming - LinkedIn were the ones not using salting, unecessarily exposing their users to attack,

9 John Podesta Email Compromise

He was the White House Chief-of-staff and the chair of Clinton's presidential campaign. His Gmail was compromised and 20 000 emails were published by WikiLeaks. Authencity of the emails was questioned

10 Lottery Scam

Choose a mark and make them think that by helping you get some profit. Then make them think they're actually going to get a lot more profit if they lie a bit, which appeals to their sense of greed.

Scam to show the importance of physchology.

11 Volvo accidents

For a car that is known for safety, Volve drivers are involved in the most accidents as (1) Bad drivers buy volve or (2) Volvo drivers drive faster as they think they are protected in a Volvo.

Shows the idea of risk compensation

12 Apple and Amazon Security Flaws

Led to Mat Honan's entire digital life to be destroyed. The hackers wanted his twitter handle and so from his twitter they were able to find out his gmail and since the 4 digits that Amazon think are safe enough to display of your credit card, it's the same 4 digits that Google use as verification ID. From amazon they got his apple id, from his apple id they got his gmail and then with that they got his twitter. Using one website to find out information about the other, the hackers were able to piece together all information to get into his twitter. However it led to all his apple devices being wiped, email being hacked and twitter hacked.

Highlights the importance of secure passwords, and how everything is linked

13 Ordering wine in a restaurant

First the sommelier presents the wine list to the host, the host chooses the wine and the sommelier fetches it. He presents the bottle to the host, who then checks its the right one and samples it. It is then served to guests.

Shows confidentiality, integrity and non-repudiation

14 DigiNotar

Dutch certificate authority. A security breach led to the fraudulent issue of certificates. Dutch government took over the management of the company's systems, the same month the company was bankrupt. Iranian Gmail users were found to have been given fake certificates for Gmail, allowing a Man-In-The-Middle attack (MITM). Over 500 certificates were issues. Iranian Government and the NSA are both potential attackers.

Behvaiour of the government has a huge impact on the security of everyone

15 Patriot Missile Failure

During the Gulf War an American Patriot Missile failed to track and intercept an incoming Saudi Middle. The missile ended up killing 28 people. The cause was an inaccurate calculation of time since boot due to arithmetic errors. The time in tenths of seconds as measured by the system clock was multiplied by $\frac{1}{10}$ to produce the time in seconds. $\frac{1}{10}$ is infinite in binary and it was chopped after 24 bits as a 24-bit register was being used. The chopping error multiplied by the large number (number of tenth of seconds in 100 hours) led to a significant error of 034 seconds. The Saudi Scud travels around 1.5 km per second and therefore 0.34 seconds makes a huge difference. The bad time calculations had been improved in some parts of the code and not all which led to the errors not cancelling out and therefore resulted in this disaster.

Highlights the impacts of arithmetic errors. Critical system failures are multifactorial

16 Apple's goto fail bug

```
{
OSStatus err;
//...
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
   goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
   goto fail;
   goto fail; //error: this line should not exist
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
   goto fail;
//...
fail:
     SSLFreeBuffer(&signedHashes);
   SSLFreeBuffer(&hashCtx);
   return err;
}
```

The second goto fail results in the unconditional exectution of the code at fail.

Highlights the importance of testing - e.g. more unit tests

17 Clallam Bay Jail Inmate

The inmates were able to choose the language which language they wanted their message in and therefore they were ablr to send a message intentionally in a different language to make the person they called press a number to hear the message in English. They used this to make a company pay for all of their calls.

Code injection, remmember protecting whole system including against malicious users.

18 Morris Worm

Meant to be an intellectual exercise to highlight the security flaws but actually turned out to be a virulent denial of service attack. Exploited vulnerablities in Unix and weak passwords. The spreading mechanism was what made it much more serious - the worm would ask the computer if the worm was already running on it and even if the answer was yes,1 out of 7 times the worm would duplicate and reinfect the computuer.

First person convicted under the Computer Fraud and Misuse Act. Easy to exploit vulnerabilities.

19 London Ambulance Service Disaster

(*See supervision work for detail*) Change from manual to automated dispatch service with software filled with errors and untrained staff led to the collapse of the system in October 1992. Estimated deaths around 20.

Combines many of the errors and difficulties in large projects becomes apparent in the case. Shows how incentives play a huge role

20 Barry Boehm

Famous software engineer who is responsible for surveying relative costs for software development. He observed effort put into testing is more than the effort put into programming.

Important to build tools to support software development as well as the tasks of specification and testing. Many more errors in the design stage than the coding stage.

21 Mythical Man Month

Brook's Law: ' *Adding manpower to a late software project makes it later*

Communication overhead in large projects often means that adding more people just ends up taking more time. The idea of a man-month is a myth.

22 Tacoma Narrows Bridge

Bridge that collapsed in November 1940 due to aeroelastic flutter - the solid sides did not allow the wind to pass through, meaning the bridge caught the wind and would sway.

Often it takes a disaster for research in the field to be boosted. All future bridges shouldn't make the same mistake. The same case with the computer field - need to look at past failures to learn

23 Ariane 5 1996

Rocket expolded just 40 seconds after lift off. The cause of the failure was a software error in the inertial reference system. Specifically a 64 bit floating point number relating to the horizontal velocity of the rocket with respect to the platform was converted to a 16 bit signed integer. The number was larger than 32,767, the largest integer storeable in a 16 bit signed integer, and thus the conversion failed. The explosion was a result of a complete loss of guidance and altitude information. Resulted in a loss of billions of dollars of development and cargo.

Float-interger conversion importance

24 Therac-25 Radiotherapy Machine 1985-1987

(*See supervision work for detail*) Programming errors led to 3 deaths and 3 injuries. The removal of hardware check for software checks resulted in a previous bug from manifesting. If the nurses mistyped the settings, and the changed the input the magnets would be in place for a setting different to that being displayed (concurrency bug).

Incentives, usability issues, poor safety engineering and testing

25 Boeing 737 Max Crashes

Faulty sensor erroneously reported that the airplane was stalling - the false report triggered an automated system known as MCAS to point the aircraft's node down so that it could gain enough speed to fly safely. MCAS is used to take reading from two sensors to determine how much the nose is tiling, if it detects it is pointing up at a dangerous level then it automatically pushes down the nose of the plane.

Automation isnt always better. Inadequate training leads to disaster. Hardware faults equally as important

26 Panama Crash 1992

47 people died in a crash which was causes due to faulty instrument readings and several other contributing factors, including incomplete training. The trouble was later traced to a faulty wiring harness in the Attitude Director Indicator (ADI) instruments. The wires were frayed due to damage by long term over-stress, which caused an intermittent short circuit in the flow of data

Importance of training and hardware

27 Kegworth Air Disaster

Fan-blade broke in the left engine, filling the flight deck with smoke. Pilots though this meant the right engine was faulty, since earlier models ventilated from the right engine. (They were wrong). Crew shut down a functioning engine and pumped more fuel into the malfunciotning one which led to that one bursting into flames. Lead do 47 deaths and 74 injuries. Fan fracture attributed to metal fatigue due to heavy vibration in the new engines - which had only been tested in the lab and not under flight conditions

Results of poor testing and incomplete knowledge of the system