INTRODUCTION

Date: 1/jun/20

Sir → IT Director of NED
↳ NOC (Network operator center)
↳ data center
security → admissions / web services etc)

* visiting NOC / data center of NED
↳ server machines / physical security to server security / firewalls / dashboards of firewalls

NCCS (National center for cyber security)

→ doing certification makes you an operator i.e. how to control / implement a device But what is inside device i.e. not part of certification.

* Open source security products & Close source security produc
↳ Cisco is brand name. Its a close source company.
↳ Juniper has also close source security products.

* In open source, it is free noone has ownership
↳ there's always a matter of consent of liberty issue / whether this product will work or not, or it may crash who will take responsibility?)

* In close source security products, you will pay for this company you will get services, someone has its ownership.

* One of objective of CSS is you should be able to use open source products in a reliable way.
(configuration of open source security products)
↳ how cyber security systems work? how attacks happen? how to protect from attacks? how to deploy security products

Date:

→ to do complete POC (prove of concept) test before implementing security products.

* What is cyber security
is one of the prime factors which should be consider whenever we deploy our services over internet. cause internet is has become the excess channel for these services.

Eg. In financial system, if your bank is working ok but all your services on internet has a cyber attack than its useless. because excess media of your bank is internet. (case of bank Islami)

* Vission of NCCS → secure Pakistan's Cyberspace
↳ carry out R&D in fields of cybersecurity.
↳ Solve local cybersecurity pbs.
↳ Commercialisation (penetrate into industry)
↳ Cybersecurity ecosystem

* NCCS strategy

* Labs:

1) Air Uni → Devices & N/w security lab
2) ↳ National Cybercrime forensics lab
3) NUST → Security Auditing & Evaluation Lab
4) Bahria Uni → Cyber Reconnaissance & Combat (CRC) Lab
5) Ned Uni → Internet security & Quantum Tech. Lab
↓ domains

1) End-Point Protection
2) Internet security & Digital Forensics
3) Quantum Technology.

* IPsec (Internet Protocol Security)

Date: 1/jun/20

* Course Structure
- Introduction to Computer & Cyber security.
! * End Point Protection → laptop / desktop / server machine/ cellphones
! * Internet security
- Digital Forensics
- Quantum Technology for security.

Q/ what is inside end point? ↳ OS, DB, various excess services, Kernel modules, java script s/w, how to protect these (end point(s)) from malicious or non-malicious ~~s/w~~ attacks.

* Internet Security → Network Security.
→ Public Internet security.

a local N/w inside office has diff. security issues & requirements & if you are ~~operating~~ your service on a public internet
↳ i.e. something tricky

* there is diff. b/w security requirement of a Local N/w & other public N/w
↳ attacks / threats / hacking on public internet

learn Internet security Protocols!

Books
- Information Security 3/e 2/e by Mark Stamp ✓ main
- Computer security Principles & Practices by William Stallings 4/e or 5/e

Practicals
- NSF Funded Security Education Project (SEEDS Labs) seed

p/w → dees

Scanned with CamScanner

lec # 2 Date: 2/jun/20

CSS = OS + CCN + PL/OOP + DBMS + IC

CCN covers lower layers than transport layer.

IC → internet & computing → above trans. layer: Application layer, session ", Transport "

Simple Mail Transfer Protocol

* read SMTP for email security.
* read http

* CSS covers all of protocols that work on protocol stack

	Application	
	Presentation	→
attacker targets it ←	session	
	Transport	→ TCP / UDP
IPV4 / IPV6 ←	Network	
	DLL	→ framing of data / timing of data
wired or wireless? ← media	PHYSICAL	

* we have to secure every layer
* diff. b/w service & Protocol.

(S) → (P) service uses a protocol. If the protocol is insecure then your service will be loss.

* Physical layer security means technology which is physically secure.
Eg. Bluetooth
if we pair two devices then

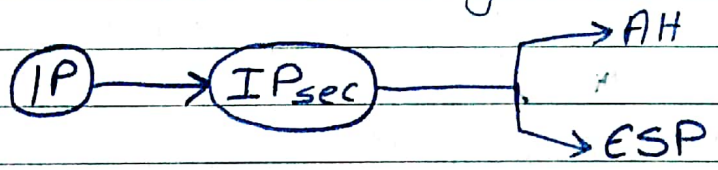
Date:

1) Eg. Bluetooth (If we pair two devices using bluetooth protocol then their operational freq. keeps changes (freq. hopping) but np cause its physically secured.

2) Eg. CDMA (code division multiple access)
↳ works below noise level i.e. why it is physically secured. (used in world war II for communication.)

* DLL security: these are protocols specially in wireless sites like WEP (wireless encryption protocol)
- different security protocols for wired & wireless media.

* N/W layer security: secure IP by using protocol IPsec
↳ IPsec is an umbrella name for Authentication Header (AH) protocol & Encapsulation security Payload (ESP)
↳ there is cmplt encryption of data end to end at network layer.



* Transport layer: governing protocol of transport layer are TCP & UDP
connection oriented protocol

↳ TCP & UDP are not inherently secure. we add additional security mechanism to ensure security.

Date:

* TCP uses 3-way handshake to establish connec
* UDP uses no handshakes, it just throws a packet & dest. has to accept it

↳ hackers exploits 3 way handshake & they do inrmpt 3-way handshake & then they misuse the operational functional usage of TCP

* Study TCP & UDP

* Main governing protocol about Transport layer is TLS and SSL

* study openSSL library

* Session layer:
↳ is a practical model not an operational model,
↳ in which session layer, presentation layer & application layer are must together.
↳ It controls transmission of data, the trunking b/w two end points so there's always a chance of hacker to takeover the chance.
Eg: dangers of "Man in the middle attack".

* Presentation layer: → data formatting.
↳ we'll study more about Encryption.

Symmetric-key cryptography — Public-key infrastructure

* Application layer:
↳ so many applications are running on this layer from clouds, from databases, from web services

Eg/ DNS (domain name system) that works on Application layer.
↳ how do secure DNS?

Date:

* SMTP is an application layer protocol which governs transmission of email from one email server (client) to another email server (server)
  ↳ how to secure SMTP?

* http is another application layer protocol
  how to secure http?

x ——— x

* we have a protocol
  https (hypertext transfer protocol over SSL)
  ↳ one of fundamental of browsing.

https → ? → email security
  → ? → cloud security
  → ? → database security.
  → ? → internet security.
  → web security.

https is just for a web security. It secures your communication b/w browsers & webservers & nothing else.

Q/ Packet Sniffing?

* End point protection Vs Internet security.

Q/ ↳ Read documentation / data sheets of
SOPHOS, Barracuda, CISCO, DELL sonicwall, FORTINET, KASPERSKY, SYMANTEC, TREND MICRO, FIRE EYE

Date:

Live session 10:30 am 11/june/20. Thursday

* production work → TCP/IP model

SMTP?? POP? POP3?

* oldest protocol of internet → HTTP, SMTP & POP & FTP

* ~~Ubuntu~~ Ubunut.com/USN

* IPV4 IP header
is there SIP address auth. in header in IPV4 ? No!

* is there SIP address auth in header in IPV6? Yes

* IPSEC

* Study TCP header. & UDP header

* 3 way TCP handshake
↳ connection oriented protocol.

* I cannot deny your sms of email from comming.
↳ protocols in which recieven can deny that is connection oriented. like calls
↳ protocols that cannot deny recievers are connection less.

* Recieven has authorities to deny in connection oriented.
* Is any connection oriented protocol is dependant on any connection less service?

Date:

* email is connection-less service.
* SMTP is protocol of email
* SMTP is based on TCP in transport layer.
* & TCP is connection oriented.
* N/w layer pay IP protocol chalta h.
* & IP is connectionless protocol.
  ↳ IP ka packet
  ↳ recievers dont have authority to deny IP packet.

Email security ?
Q/ email client like Thunderbird ? use it!
Q/ how many of you have send a secure email ?

* gmail can generate auto response acc. to your contents of mail?
  Is it not a privacy break?
  Is gmail reading my mails or end-point is doing smthing?

* PGP ⟶ is for IOS

* have you sent secure whtsp msg ?
* Try openkeychain (android app)

Assign.

1) Connect your private gmail account (incoming & outgoing emails) to email clients like Thunderbird & explore (SMTP, IMAP, POP3)

2) ... secure email ... PGP signed emails
   openkeychain

Lec#3

IDS → intrusion detection system, can be a device or an application s/w.

Date:

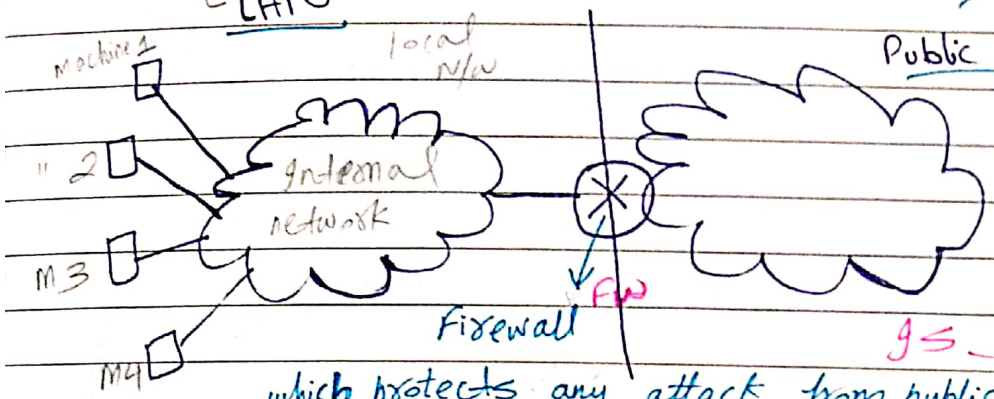
CIOs ...

Books: Information security 2nd Ed Mark Stamp John Willey & Sons.

in network i.e n/w inside a campus or office this local n/w is in your control.

↳ LAN

but this pg is emptly uncontrol media.



IS - internet security which protects any attack from public internet & it also protects or stops any attack originating from local n/w or end points to go outside.

EP
End point protection

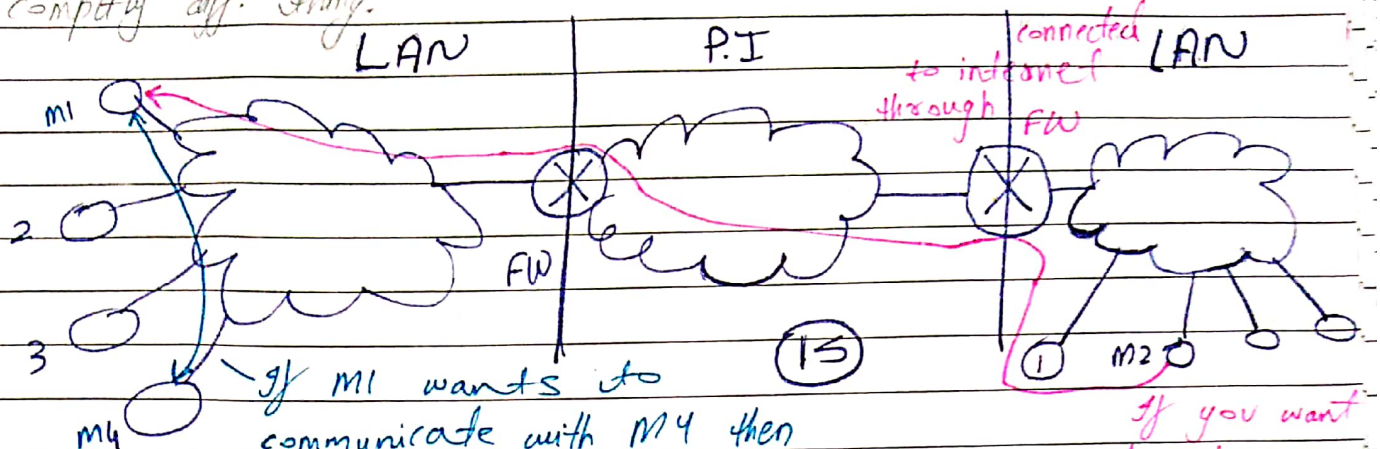
FW
protects you from internet based attacks

We've quite a diff. solutions for end point protection EP & quite diff. solutions for Internet security (IS) including Firewalls, including IDS which protects a n/w borders of any organisation from threats of public internet.

* End points are in your control.
* There is no kind of governing authority in domain of Public Internet although there are regulatory authorities which control DNS which control naming system which control IP addressing system. There is really decentralized administrative approach. We can not regulate traffic here.

Date:_____

the security of innetwork & security of internet is a complthy diff. thing.



EP

if M1 wants to communicate with M4 then what should be the security & secure methods for communication on same n/w.

If you want to communicate b/w M2 passing through this router then PJ then this router & then to this M1. This includes traversal from n/w to PJ & then back to LAN & then back. So the the security mechanisms & challenges are diff. here.

* products pertaining to EP security & the products pertaining to IS (kind of FW).

EP ⟷ IS

they do not integrate well. The Pb is that hackers/attackers take advantage of this situation. EP security protocols are not aware of the security ~~of the security~~ which is being offered by this FW.

side: End Point security Vs Internet security

Shophos is offering half half both security. Is it ideal?

It should be ideal offering both security cause if end point behaves nasty the firewall will immidiately disconnect it. which is not possible in other cases. i.e. SOPHOS will immidiately disconnect any misbehaving endpoint.

Date:

But in various n/ws such kind of behaviour leads to lack of functionality.

The goals of security & functionality are really opposite. If you want to increase the security you have to loose functionality. & if you want to offer more & more functionality then you have to sacrifice security.

Customers always want functionalities. They just ~~securit~~ trust security to you. they never apply any security method themselves. They just want ease. They will not do two factor authentication. they will not do any multi level authentication. They will simply use weak passwords. These accounts will get hack & they will blame you & you have to just accept. This is the dilemma of a n/w security specialist or a IT guy that he has to make a balance he has to take ownership of both customer & security of his/her own infrastructure.

Q/ go through the products offered by SOPHOS, CISCO, FORTINET, Symantec, FireEye.

see these end point solutions & internet security products, these data sheets. what is an OSS (open source solution)? what is an open source firewall? what is an opensource antivirus for endpoint security?

OSS

Q/ ClamAb is an opensource antivirus
↳ install it & go through it.
↳ this is for end point security

Q/ PFSENSE → open source firewall
↳ It not only controls traffic. It secures & locates bandwidth.
↳ for internet security

Introduction

Date:_____

"Begin at the beginning," the King said, very gravely, "and go on till you come to the end: then stop."

— Lewis Carroll, Alice in Wonderland

* The cast of Characters
  - Alice & Bob are the good guys
  - Trudy is the bad guy
  - Trudy is our generic "intruder"

Case study.

Alice's Online Bank (AOB)

* Alice opens Alice's online Bank (AOB)
* What are Alice's security concerns?
* If BOB is a customer of AOB, what are his security concerns?
* How are Alice's & Bob's concerns similar? How are they different? (security)
* How does Trudy view the situation?

CIA == confidentiality, integrity and Availability

* AOB must prevent Trudy from learning Bob's account balance.

Confidentiality: prevent unauthorized reading of information.
- Cryptography is used for confidentiality.

ISO27001 standard
↳ is the main security checklist which the certified organisation should follow.

Date:

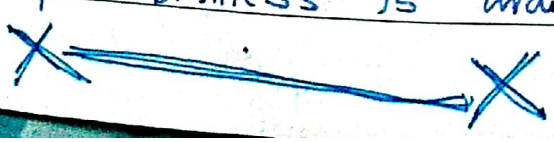
In cooperate world, every bank of every service if you want to add crediability to your business then you need to get ISO27001 certification. that increases the confidence of customers or follows on your system. This kind of certification ensures your business is safe, temper free, has business continuity plan.

* The whole standards revolves around CIA.

- confidentiality is about cryptography of your data, secure communication.
- Integrity is about ~~=~~ that your data is temper free. we ensure that through proper hash functions that if there is any tempering in data, the end point can defect it.
- Availability → the most adversary is DDOS attacks (Distributed denial-of-service) attacks. They are always happening on the Public Internet & they try to get your network down even if your service is operational your web server your email server your online business airline websites, everything is working OK. But the path which lead to physical links which lead to your business your coperate n/w are choked. So it'll be not available.

* These are firewall there are various solutions which protects from DDOS or various kinds of internet based threats.

So, ISO27001 has a checklist that ensures that confidentiality is ensure at every level, integrity of data is ensured at every point & your cmplt business is available on public internet.



Date:

CIA (cont&...)

* Trudy must not be able to change Bob's account balance
* Bob must not be able to improperly change his own account balance.

Integrity: detect unauthorized writing of information
- Cryptography used for integrity.

* AOB's information must be available whenever it's needed.
* Alice must be able to make transaction
  → If not, she'll take her business elsewhere.

Availability: Data is available in a timely manner when needed.
- Denial of service (DOS) attacks

Beyond CIA: Crypto

* How does Bob's computer know that 'Bob' is really Bob ≠ not Trudy? → this is about identity Confirmation
* Identity Confirmation of remote employees etc

* Bob's password must be verified.
  - This requires some clever cryptography

* What are security concerns of of pwds?
* Are there alternatives of passwords?
* Recently, there has been quite distrust on biometric systems cause it involves human touch so we go for image base scanning etc

Date:

Beyond CIA : Protocols

* when Bob logs into AOB, how does AOB know that 'Bob' is really Bob ?
* As before, Bob's password is verified.
* Unlike the previous ~~this~~ case, network security issues arise.
* How do we secure network transactions?
  - Protocols are critically important
  - crypto plays a major role in security protocols.

↳ Example: SMTP , the ____ of a protocol ; is inherently insecure. So, you have to go for additional security.

Q/ send secure email

Beyond CIA: Access Control

* Once Bob is authenticated by AOB, then AOB must restrict actions of Bob.
  - Bob can't view Charlie's account info
  - Bob can't install new software & so on...

* Enforcing such restrictions : authorization

* Access control: includes both authentication & authorization.
  There's a concept AAA (Authorization, Accounting & Auditing)

Date:

Beyond CIA: Software

* Cryptography, protocols, and access control are all implemented in software
  - Software is foundation on which security rests.

Software security is very imp.
there are buffer overflows, there are race conditions
these are coding issues which leads to so many hacks which tends to insecure software.

* what are security issues of software?
  - Real-world software is complex & buggy
  - Software flaws lead to security flaws
  - How does Trudy attack software? by giving an invalid i/p
  - How to reduce flaws in software department?
  - And what about malware?

Q/ what is s/w development ~~life~~ lifecycle?
↳ add security in this cycle.

Lec #4

Your Textbook

1) * Cryptography → symmetric key cryptography → data sec.
   → Public-key cryptography (PKI) → https (ssl)
2) * Access Control → Firewalls, various rules
3) * Protocols → A, P → protocols works on every layer.
   ↳ All protocols were designed to give service & functionality not security.
   ↳ there has been various attacks which exploited the use of these protocols.
   F.Eg: Transport layer uses TCP. & Tcp does a 3-way handshake before transfering actual data. 90% of internet traffic is Tcp.
4) * Software → s/w security.
   ↳ s/w is great entry point where both intentional & unintentional flaws occur. F.Eg: buffer overflow, race cond. These s/w flaws not viruses.

* data security mostly means use of symmetric key algorithm /about encryption of big data files /streaming files.

Date:

* we'll focus on technical issues.
* But people cause lots of problems.
  ethics! → ethical issues that leads to cyber crimes.

The People Problem

* People often break security.
  - both intentionally & unintentionally
  - Here, we consider an unintentional case.
* For Example, suppose you want to buy something online.
  - say, Information security : Principles and Practice, 3rd ed. from amazon.com
* To buy from amazon.com... secure socket layer. Its
  - your browser uses the SSL protocol. layer 4 security protocol. (SSL & OLS)

SSL was designed to have a secure communication b/w a web client & a web server.
inside n/w public internet.

SSL also has a very strong & secure key exchange algorithm cause any cryptographic algorithm requires a key exchange b/w two end points.
- SSL relies on cryptography
- Many access control issues arise
- All security mechanisms are in software.

* suppose all of this security stuff works perfectly
  - Then you would be safe, right?
* What could go wrong?
* Trudy tries man-in-the-middle attack → very famous attack that which works at link layer to transport layer to n/w layer. If its SSL, attack doesn't work.
  - SSL is secure, so attack does not work.

Date:

- But web browser warns of problem
- What do you, the user, do?

* If user ignores warning, attack works!

Here, None of the security mechanisms failed
- But user unintentionally breaches security

we need to understand various kinds of warnings which we usually ignore.

Cryptography.

* "secret codes"
* This section covers
  - Classic cryptography → techniques are mostly about replacement codes which cannot be uncovered by the famous textline 'a quick brown fox jumps over a lazy dog' → contains all 26 letters
  - Symmetric ciphers
  - Public key cryptography
  - Hash functions++
  - Advanced cryptanalysis. → like quantum cryptography

Access Control

* Authentication → Its really you!
  - passwords
  - biometrics
  - other methods of authentication.

* Authorization
  - Access control lists & capabilities
  - Multilevel security (MLS), security modeling, covert channel, inference control
  - Firewalls, intrusion detection (IDS)

Date:

Protocols

* "simple" authentication protocols
  - focus on basics of security protocols
  - lots of applied cryptography in protocols.
* Real-world security protocols
  - SSH, SSL, IPsec, Kerberos
  - Wireless: WEP, GSM

Software

* security-critical flaws in software } unintentional attack → s/w developer mistake.
  - Buffer overflow
  - Race condition, etc.
* Malware → malicious s/w
  - Examples of viruses & worms
  - Prevention & Detection
  - Future of malware?

} intentional → entire code is written to make sure that system crashes etc.

how to write malware?

Q/ go through TSR (Terminate & Stay Resident)

was used in DOS OS. DOS was single threaded OS. but still TSR, you can write of code. It means the C language code that runs of executes. After its termination it becomes stay Resident. It stays in your memory.

* there's function in C language.
  keep(,); → for this you've to #include <dos.h> in your code.
  ↳ that makes your pgm resident.

Date:

Q/ read documentation of keep(0, _) in C language

space of mem. req.
amount of bytes

Code... #include <dos.h>

:

void interrupt (*OldTimerInterruptFunction)();

pointer to func.

It's a pointer function. It will point to a func. of type interrupt

Due to this simple code, the capslock will always be on. Even if you try because the interupt func. of times is replaced.

There's no way to switch off capslock. → It's a simple virus of capslock.

Q/ Try to compile this code on TurboC

* Malware → these signatures
  ↳ It's very difficult to catch them bcz most of the viruses are polymorphic.

Q/ how to make a virus polymorphic.
  ↳ there's a polymorphic code etc.

Date:

Software (contd...)

* Operating systems
  - Basic OS security issues
  - "Trusted OS" requirements
  - NGSCB: Microsoft's trusted OS for the PC
* Software is a big security topic

Think like Trudy

* Good guys must think like bad guys!
  * A police detective: must study & understand criminals.
* In An information security
  - we want to understand Trudy's methods.
  - we might think about Trudy's motives.
  - we'll often pretend to be Trudy.

* Is it a good idea to discuss security pbs & attacks?

!Q/ Study document ISO 27001 Controls & Objectives

"My software never has bugs. It develops random features."

↳ developer might can say its a feature but hacker can use it as a bug!

Lec #5 (live sess #2 (absent)) ch # 11 of book: Software Security.

Date:

Why Software?

* Why software is important to security as crypto, access control, protocols?
* Virtually all information, security features are implemented in software.

Software is the base! If there is any defect in s/w so the system which is based on your s/w will be affected.

* If your s/w is subject to any attack, your security can be broken.
  ↳ Regardless of strength of crypto, access control, or protocols.
* Software is a poor foundation for security.

Hackers & attackers always look for the bugs in your s/w so that they can enter in your system or can do nasty activities etc.

In SE course, you have studied s/w development life cycles, these lifecycles used by like waterfall model, Agile model etc. They do not specifically include the security component in your s/w cause these lifecycles are designed to make your SRS ... to give proper functionality to your client.

S/w development lifecycles (SDLC) are mainly focused on functionalities & not on security aspects.

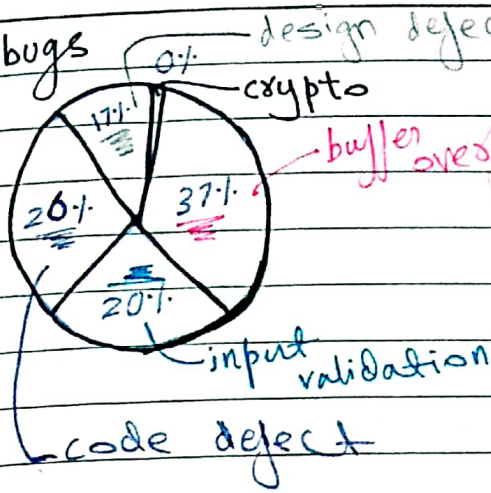
"Currently encryption is the strongest link we have. Everything else is worse: software, networks, people. There's absolutely no value in taking the strongest link & making it even stronger."

– Bruce Schneier

* Cryptography is usually not the problem.

Date:

Security bugs found in Microsoft bug fix month (2002)



* our SDLC & QA mechanisms are strong enough to reduce design defect.
↳ it will further decrease.

QA → quality assurance?

Q/ see more recent data of other vendors about security bugs.

* Bad software is Ubiquitous

1) NASA Mars lander (cost $165 million)
↳ crashed into Mars due to error in converting English & metric units of measure
↳ Believe it or not → simple error of typecasting func. that we use to use reduce mem. like integer to ascii etc
→ due to this simple s/w issue the entire project was failed.

It might've passed through several diff. quality assurance test. Not only developers were working, several QAs, several quality assurance rounds. Engineers must've gone through code But somehow this basic thing got missed & disaster happened Loss of $165 million!

2) Denver airport
↳ Baggage handling system — very buggy software
↳ Delayed airport opening by 11 months

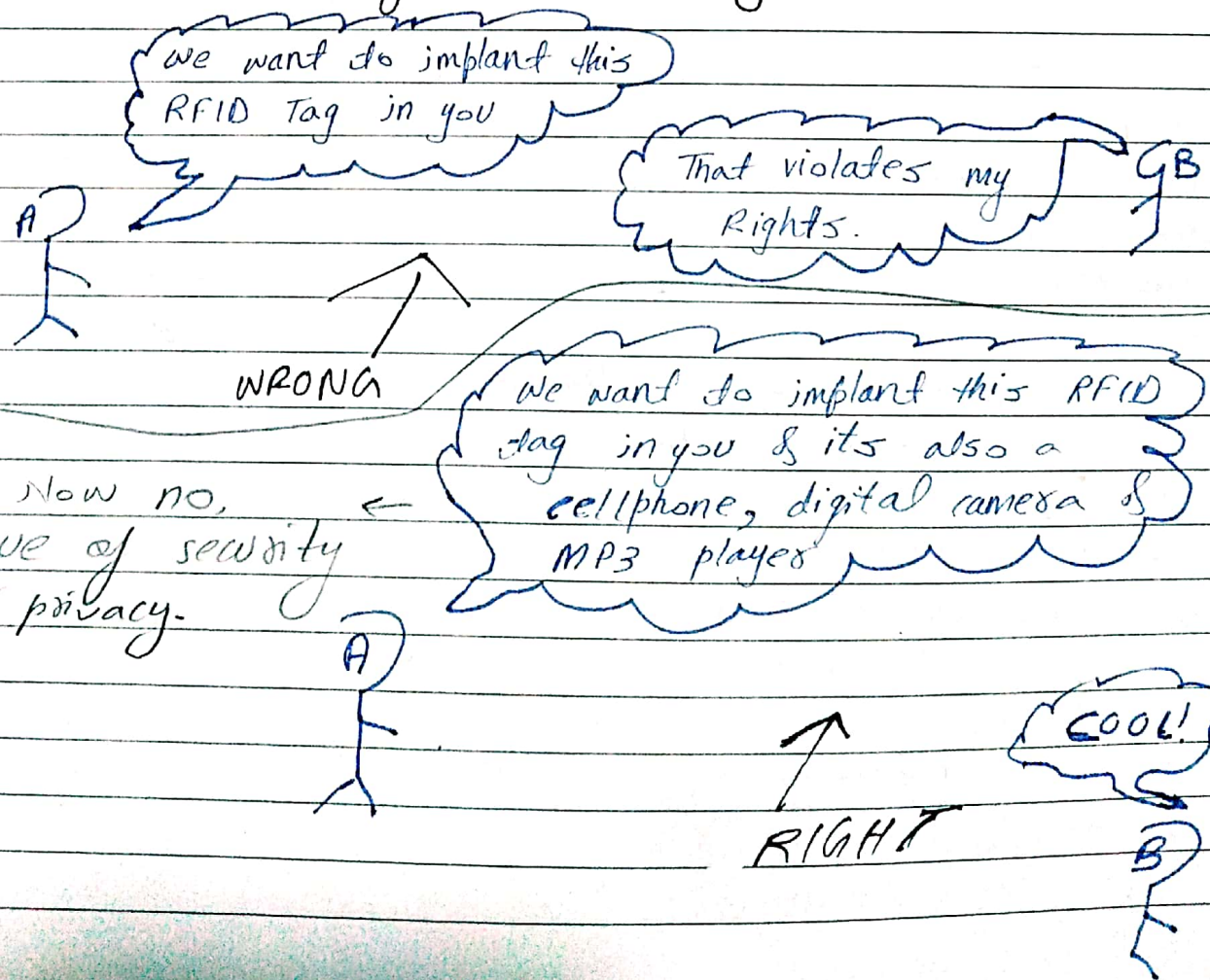
Date:

↳ cost of delay exceeded $1 million/day
what happened to person responsible for this fiasco?

3) MV-22 Osprey
Advanced military aircraft
↳ faulty software can be fatal.

4) Boeing aircraft crash 737
↳ pilot was trying to lower the aircraft but due to that AI code : pilot request was superseded by AI code.
↳ use & misuse of Artificial Intelligence
despite ~~beside~~ this that pilot controlled all the h/w issues the AI based s/w ~~res~~ cause the plane crashed.

Functionality Vs Security.



Date:

Ex) Read daily:

a) Microsoft security Bulletin 2016

URL : https://technet.microsoft.com/en-us/library/security/ms16-jan.aspx

b) Ubuntu security Notices

URL: http://www.ubuntu.com/usn/

* Book:

* 19/24 Deadly sins of software security [Howard, LeBlanc, Viega]

1) buffer overruns
2) format string problems
3) integer overflows
4) SQL injection
5) command injection
6) failing to handling errors
7) XSS.
8) failing to protect n/w traffic
9) Use of magic URLs or hidden form fields
10) improper use of TLS, SSL
11) weak passwords
12) failing to store & protect data securely
13) information leakage
14) improper file access
15) trusting n/w name resolution
16) race conditions
17) unauthentical key exchange
18) weak random numbers
19) poor usability

* Classification of Software security Errors

1) I/P validation & Representation
2) API Abuse
3) Security Features
4) Time & state
5) Errors
6) Code Quality
7) Encapsulation
8) Environment

Date:

* Two sides to software security: do's & don'ts

* what are the methods & technologies
  ↳ available to us if we want to provide security?
  ↳ security in the s/w development life cycle
  ↳ engineering & design principles
  ↳ security technologies

* what are the methods & technologies available to the enemy who wants to break security?
  ↳ i.e. what are the threats & vulnerabilities we're up against.

These two sides are actually offensive security & defensive security.

we should not always focus on the defense. we should also focus on the offensive part that how to write a malware, what are the ~~thr~~ vulnerability & how to exploit these vulnerabilities & how to find this vulnerabilities using various kinds of scanners & other techniques.

You should be aware of your own system. First of all do cmplt audit of your own computer. Do not depend on your antiviruses & windows based firewalls etc.

* How to improve software security? (lect # 5) [26:00]

- Awareness & Knowledge of vulnerabilities → don'ts
  - general (input validation...)
  ↳ specific to a kind of application (SQL injection, XSS...)
  ↳ specific to a kind of programming language (buffer overflows,...)
- Awareness & Knowledge of countermeasures → do's
  ↳ at diff. points in the development lifecycle

Date:

↳ at level of application, programming language or platform

↳ Eg security technologies such as
- access control, session management
- untrusted code security → always an issue as our SE are fan of copying code from stack overflow etc.
- type safe languages, sandboxing, code based access control → we should try to sandbox any untrusted s/w. Easiest kind of sandboxing is virtual machine.
- runtime monitoring
- program analysis: typing, information flow, static analysis, verification.

- But Beware that

security software ≠ software security } These are two entirely diff. things.

s/w security is about the coding techniques about the programing behaviour. The lifecycle which you use to develop a s/w

having so many security s/w has nothing to do with s/w security. A security s/w can inherently insecure.

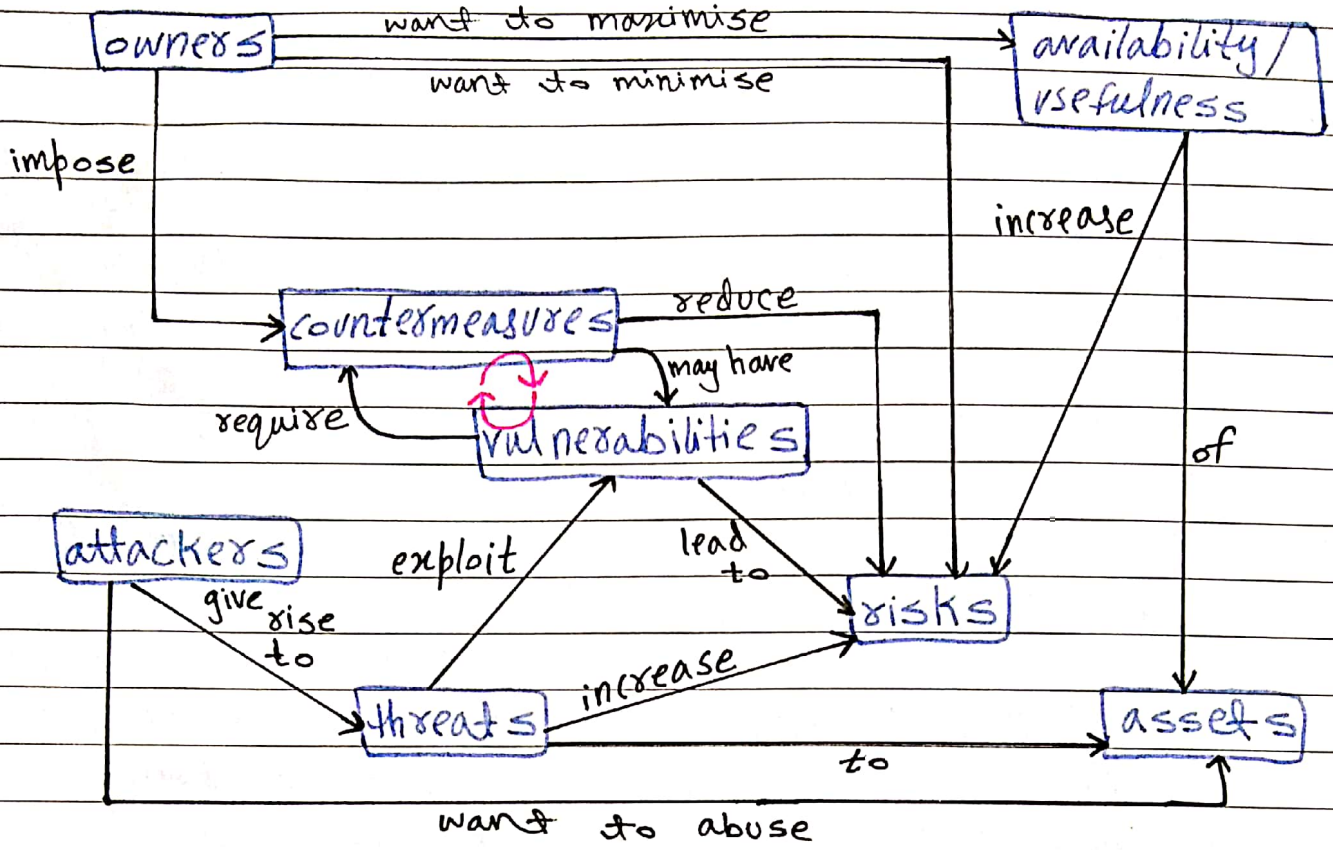
An example of security s/w is simply an antivirus. A semantic antivirus is a security s/w. A mcafee antivirus is a security s/w. A SEAM solution is a security s/w. A Firewall is a security s/w.

Security s/ws are products & these can be open source & these can be close source.

A security s/w is a kind of a defensive mechanism but it's something very diff. from s/w security.

Date:

security Concepts. (Imp.!)



*framework of 15027001 which grades the imp. of assets

It goes on & on always. Its upto the competance of the owner's team & the attacker's team.

* attacker also sees the value of asset to abuse it.

* asset is very imp.
↳ can be internal or external

* 15027001 standard.

↳ even offline user can hack your system. It is not necessary that tussle applies always applies to system which are online.

* The iranian issue: the nuclear powerplant which got damaged due to simple malware- cause they ignored this tussle.