Three main uses of arch

training

comm with stakeholders

system analysis and construction

prescribe and describe

View creation

build stakeholder view stable

combine

prioritize and stage

arch

complicated represented by view

eval method

designer inside

outside inside

peer

metrics

what artifacts are avaiable

who sees result

who performs eval

whats avaiable

which stakeholders

what are business goals

ATAM

Purpose

to asses archicture in light of the quality attributes

Benefits

clarify req attributes

improved documentation

documented basis for decision

ID risk early

increase comm between stakeholders

improved architecture

Participants

3-5

compentent unbaises outsiders

architect is always included

project decision makers

stakeholders

Output

clear cut understanding of arch

does it meet business goals

prioritize QA req

identify risk and non risk

condensing risks into risk themes

prioritize based on themes

comaparing decisions to qaulity requirements

sensitivty point

- is when there is a fork

- parameter in architecture to which some QA is highly correlated

tradeoff - is the difference in benefit of the choice

-affects to more than 1 QA and is a sensitivty point for more than one QA

present ATAM

present business drivers

present arch

ID arch approaches

generate util tree

risk analysis

brainstorm prioritized scenarios

risk analysis

present output

Process of design

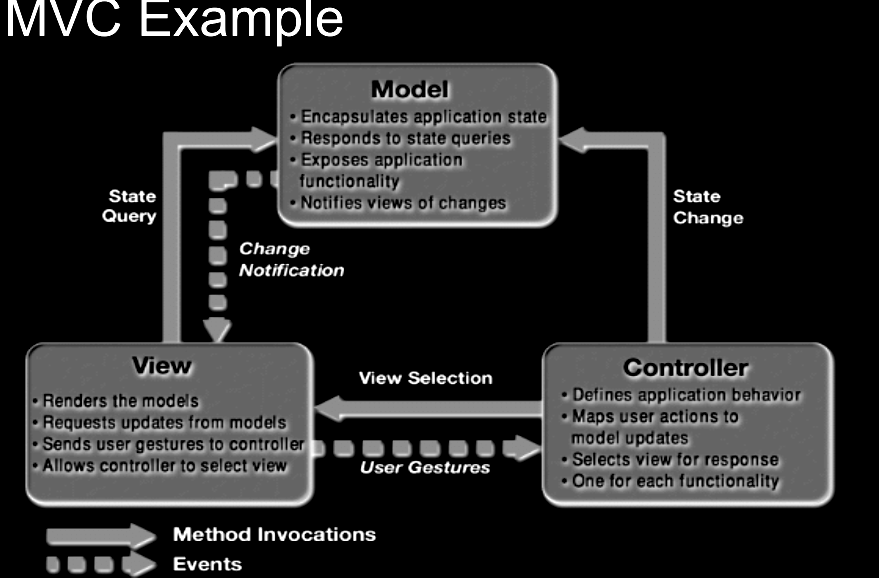
ID problem, find solutions, make decision

problem space

design problem, sub problems

decision space

alternative solutions



Depends on reusable

Depends on obsolete

No to portable

Computer Criminal

Cracker, computer sauvy criminals

Script kiddy, launch scripts

Criminals create bots, scam, sell credit

Virus

Trojan, masquerades as benefical program

Worms, replicate with execution

Logic bomb, executes under conditions

Social engineering, manipulates people into giving information

Phishing, collecting data through email

Farming, fake webpage

Bot net, hack in multiple computers use

Root kit, backdoor

Firewall

Keys

Double key

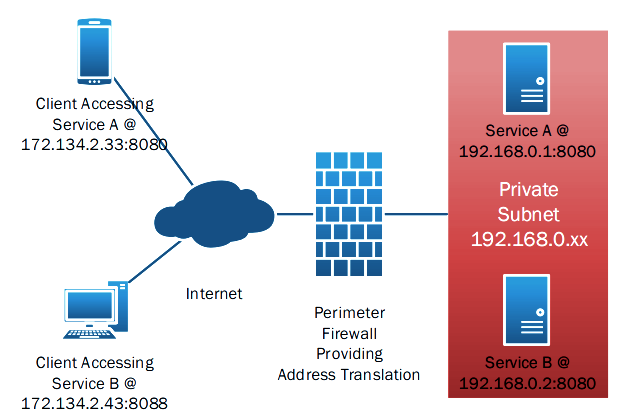
ASymetric

Different key to encrypt and decrypt

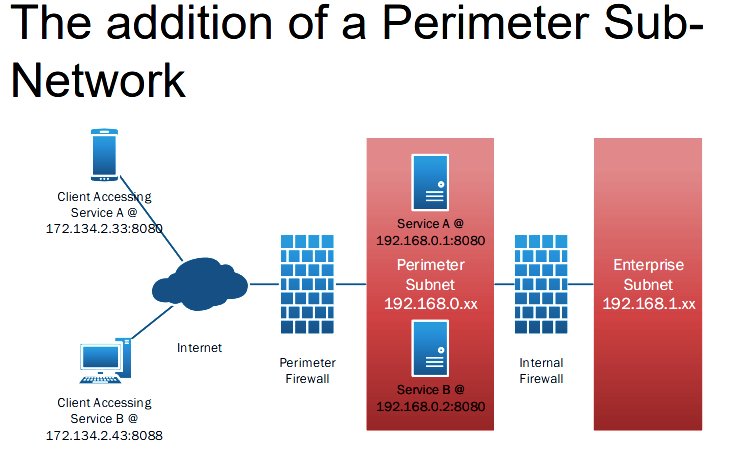
Single key

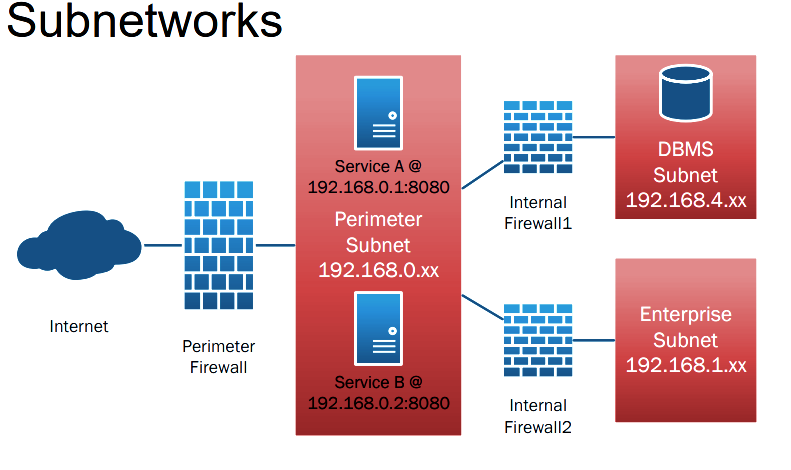
Symetric

Same key to decrpyt

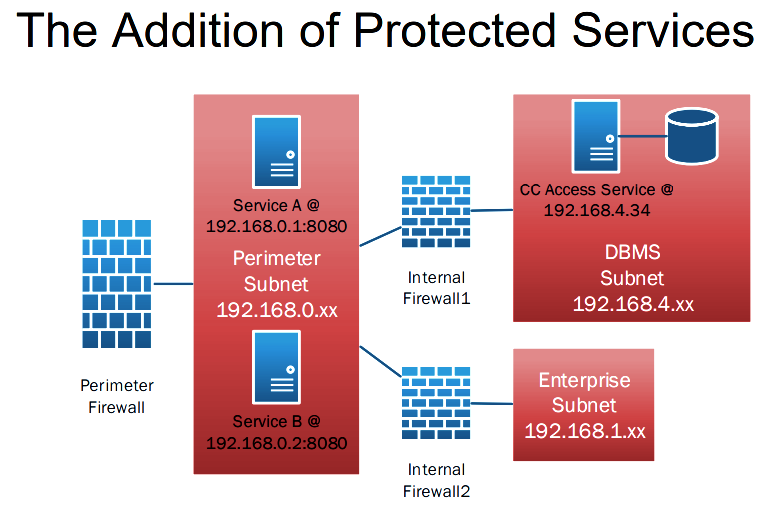


DMZ





Service API



Confidentiality – unauthorized cannot read

Integrity – unauthorized users can not alter

Availability – authorized users can always access