Security on server

People will hire a bunch of security experts to guard the server or network, however, this was not considered as secure. Let's use a real life example.

Let's suppose you come from a wealthy background, you converted some of your asset to money. You're pretty scared and afraid that people want to steal your money. Hence, you hire some physical security guard to guard the place where you store your money. There're several things which can go wrong here.

Can the physical security guard be trusted? If they can't then there's a possibility that they will steal the money or help the coordination of money stealing from potential thief. You may notice something goes wrong but given that you hire a lot of physical security guards, it's just impossible to know the "traitor". Even if you do found the traitor, what you will realized was traitors keep on appearing which makes catching the traitor an endless bad cycle.

Let's say you trust the physical security guard, having so many security guards to guard money. Let me ask you a question, don't you feel tempted in stealing the money? After all, there're approximate 1 million guards there, the amount of money should be really huge or uncountable. I don't know about what you think but it's really tempting. I can simply find some way which render the security guards safety measure useless and steal any amount of the money that I see fit.

These problems exist in company/corporate or businesses. The right way to do it was not to prevent these kinds of problems from even happening. Hence, it's better that you put less money or don't put any valuable asset. What this does is to reduce the likelihood of traitor or outsider thief from appearing. Let's say that I still want to put money, I will put the money into a safety safe and hand it to the guards. I don't give the guards any keys to unlock the safety safe.

If you have summed up what I have stated, my security measure on the server was never to stop the money getting stolen or the appearance of traitor/thief from being appearing. The security measure is quite simple and straight forward which is by considering that the money will definitely get stolen by others be it traitor or thief, what I can do to potentially reduce the damage of such incident.

It's always recommended that I hire guards as well because there're cases where I

can’t use only this approach. In scenarios where I can use only this approach, this way of dealing with money (data) is sufficient and more secure compare to hiring lots of security experts or guards to guard the money (data).

Problem with using this security approach

Information that you have sent to me may not be really as secure as you and I thought. It’s not about confidentiality which you could imagine as you put your money into a safety safe and you hold the key instead of the other person holds it for you.

It’s about integrity. Assume that you were born in XXX-hospital in the year of 1980. You have a blood type of A. 25 years later which was 2005 you go to the XXX-hospital to attend for regular medical checkup. What you have realized was that your blood type had been changed from type A to type O. The initial blood type paper was given to you during your birth but then why and how it was changed into type O? This was called as integrity issue/problem.

The safety safe you send to the server don’t have a rightful owner as I intend to leave your purchase email at my PayPal’s merchant account. One of the potential issues is the thief or the traitor could change the safety safe without any notice and the other much more serious and unsolvable issue will be swapping the public keys that you have sent to the server. There’s also one more obvious issue which is also very serious and unsolvable. Let’s say there’s no integrity problem on the server side, originally the file storage or the storage you own belongs to you. However, as time goes on your device have been changed or get stolen by physical thief. In this specific case, this is also consider as an integrity issue/problem as I can’t determine whether the owner have been changed due to the lack of “private identity such as email/phone number” in server side.