International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

Data Security in Day to Day Life and Its Consequences: Case Study

Sandeep Saxena

Abstract: ***People of Metro/Smart cities use multiple mobile applications to ease up their life. Problem statement is that all different mobile Apps are mutually exclusive. Private Data (1) may be a public data for Application A i.e. Flat Number of a society, But Application B can reveal other Private Data (2) on basis on this Private Data (1). This cycle goes on and ultimately Name, Phone Number, Email ID, Flat Number, Meter Number, Electricity Consumption, everything is leaked.***

Keywords: OSINT, Information Security, Data Privacy, Data Security

1. Introduction

People of Metro/Smart cities use multiple mobile applications to ease up their life.

Problem statement is that all different mobile Apps are mutually exclusive.

Private Data (1) may be a public data for Application A i.e. Flat Number of a society, But Application B can reveal other Private Data (2) on basis on this Private Data (1)

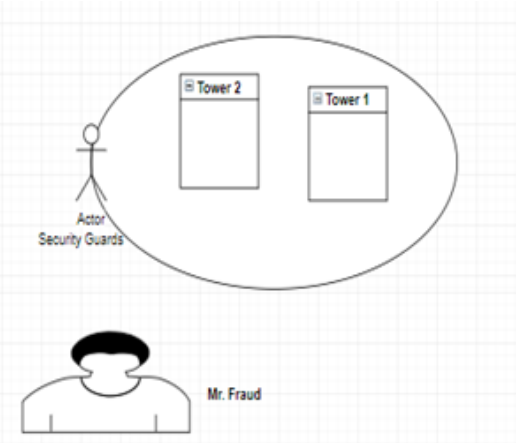
This cycle goes on and ultimately Name, Phone Number, Email ID, Flat Number, Meter Number, Electricity Consumption, everything is leaked.

Below is a **Case Study**

Let's think about a hypothetical scenario, there is a society EasyLife Apartments, Residents are Tech Savvy and use different Mobile App & utilities to ease up their life i.e.

Electricity Recharge App (Different Mobile Wallets), Visitor Management Apps, real time Electricity consumption apps etc.
This analysis is based upon particular mobile apps and may not be applicable for all societies and apps but for many of them, it may be true and for some of them it's actually true as per the analysis.

Now there is a Fraudster (Mr. Fraud) and let's examine what information he can get easily about the residents of this particular society.



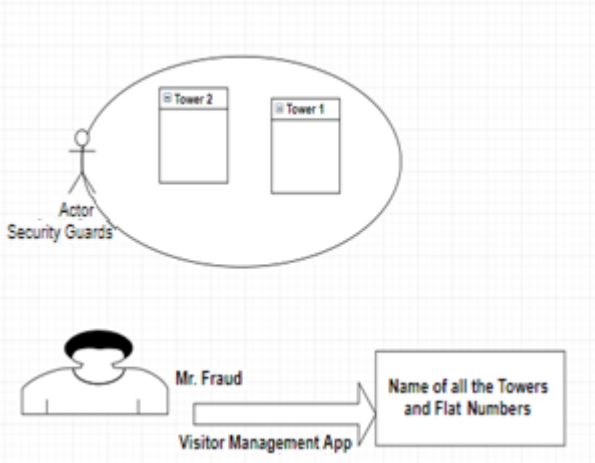
First challenge is to identify the infrastructure of the society i.e. Number of Towers, Name of Towers, number of Flats in a Tower.

Mr Fraud installs a visitor management app used by this society; it's easy to identify which app is being used for that. Some societies even put a board about this on gate.

On the Visitor Management App, Mr Fraud proceeds to register as a Resident for the society. Ideally he should be asked to enter the Flat number but for the ease of use, list of Towers are displayed after selecting the name of the society.

Mr Fraud selects a Tower and all the Flat numbers are displayed i.e. Alpha 123 or Block B 191 etc.

Now he knows the information of all the Towers and Flat Numbers i.e.

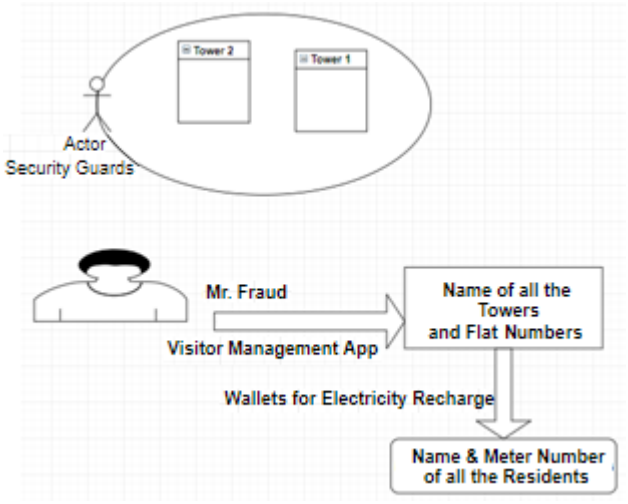


Flats
Tower Alpha 123
Tower Alpha 191
Tower Gama 104

Not a big deal, now what?

Mr. Fraud, opens a wallet for electricity recharge and selects the society and enters the Flat Number:

He gets to see the Flat Owner and the Meter Number.



After some 1000 tries, he gets a list of all towers plus their owner's name plus meter number i.e.

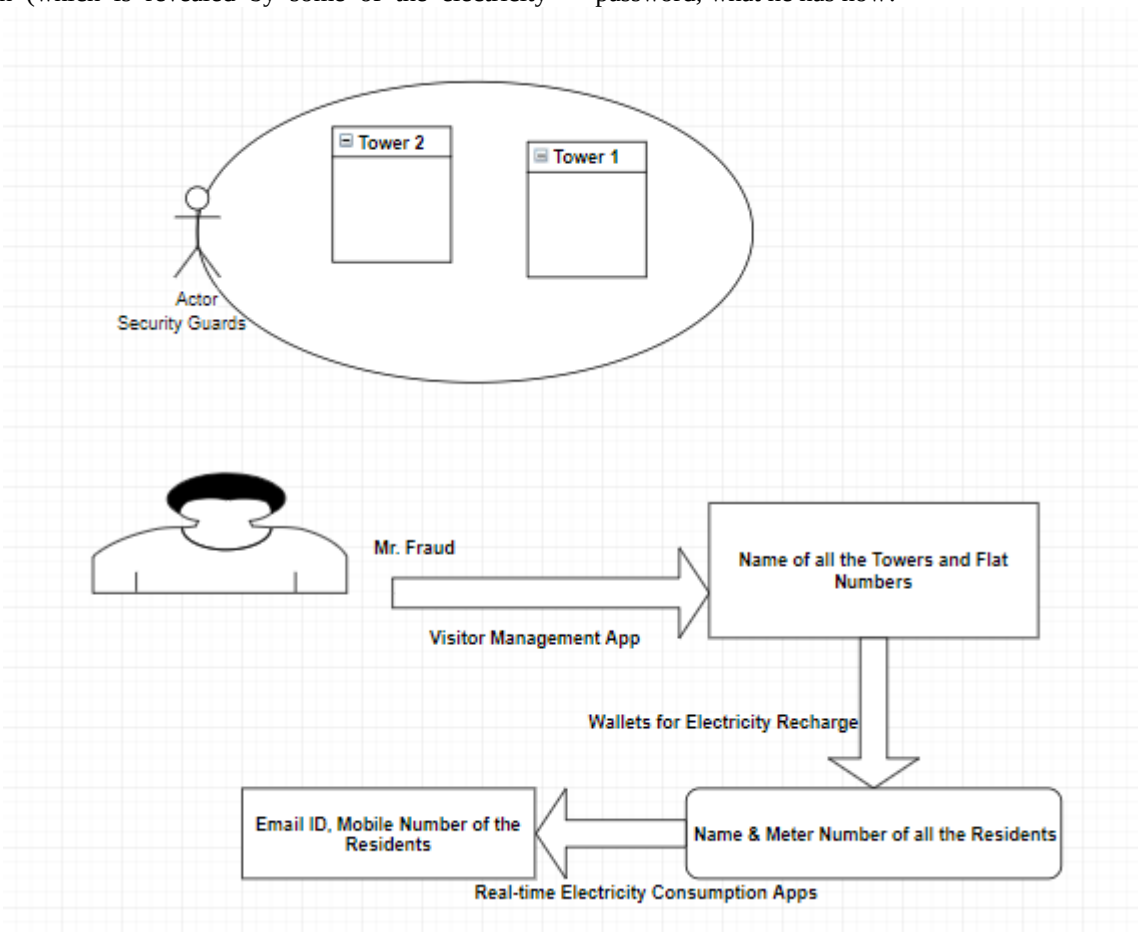
Flats	Name	Electric Meter Number
Tower Alpha 123	Mr Alex	AC-01-14567
Tower Alpha 191	Mr Tom	AC-01-14343
Tower Gama 104	Mr Henry	AC-01-14454

Still not so worrisome, what next?

Mr Fraud installs the Power Management App used by the Residents to track the electricity Bills.

Username of one such app is the meter number of connection (which is revealed by some of the electricity recharge wallets) and a simple password as its created and shared with the Residentsby the admin team i.e. aaaaaaa,123456 etc which nobody bothers to change later.

If Mr Fraud is able to login into many of the users of this society by the meter number and trying some of the common password, what he has now?



Flats	*Name*	*Electric Meter Number*	*Email ID*	*Phone Number*
Tower Alpha 123	Mr Alex	AC-01-14567	alex123@samplemail.com	9********1
Tower Alpha 191	Mr Tom	AC-01-14343	tom34@samplemail.com	8********2
Tower Gama 104	Mr Henry	AC-01-14454	henry4343@samplemail.com	9********5

This is troublesome, a list of all the Residents with their Meter Number, email ID and Mobile number.

One thing noticeable is that if someone has the access on a residents power management app, he knows one more details:

When you are out for a vacation, if consumption is zero or unusually low for 2-3 days or which Flat is not being used if there is no recharge/consumption activity for long

Things are getting scary now.

What else?

Mr. Fraud may use the private information of Residents i.e. Name, Email, Phone Number to get registered falsely as a Resident. The request to get registered is sent to the Society's administration team.

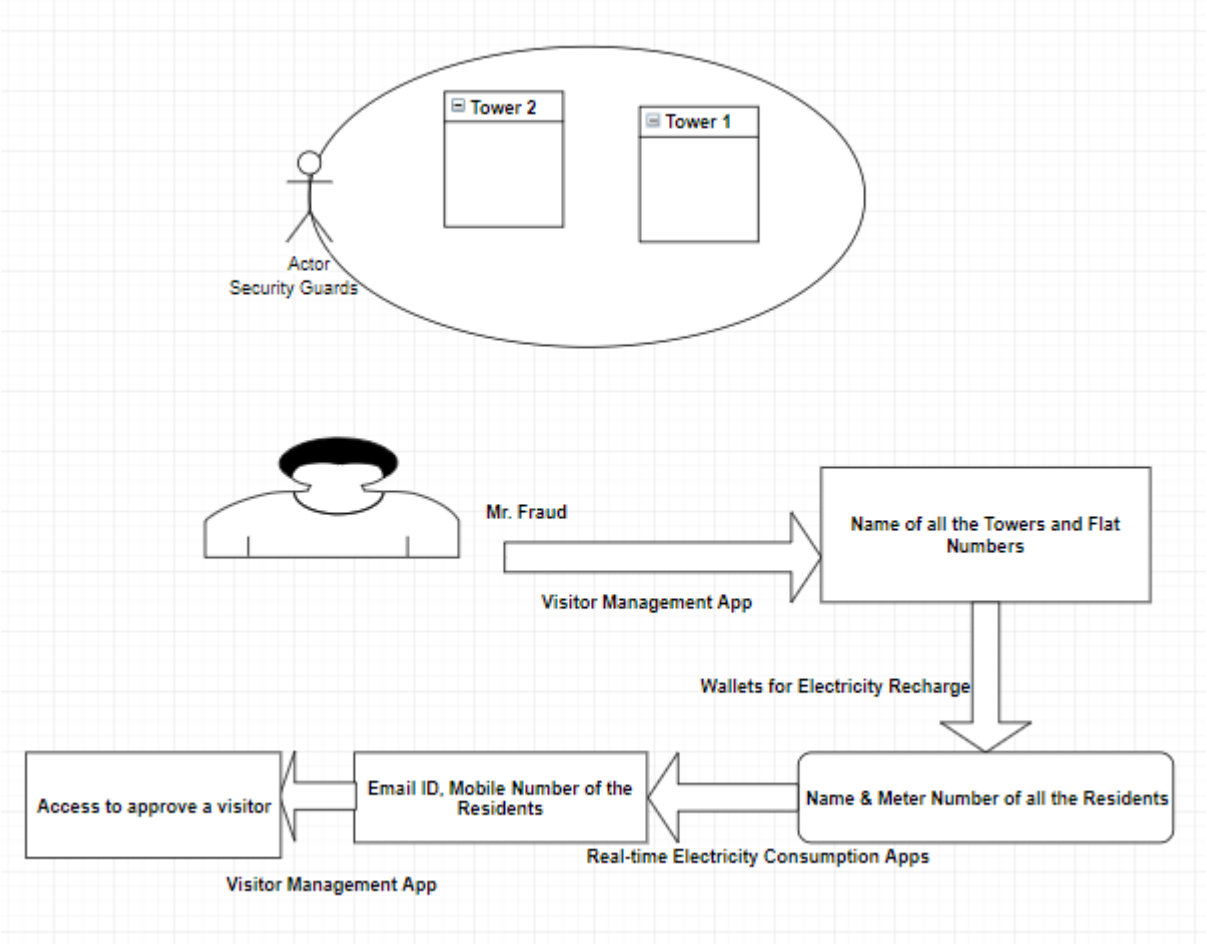
A registration request with a minor change in the original Email ID, Mobile Number of a resident can be sent to the administration team and if this goes unnoticed by the administration team (Remember, humans are the weakest link in the security chain), Mr Fraud has the access to allow any visitor to a particular Flat.

One more noticeable point is that before using such apps i.e. Visitor Management very few asks if this app is secure, complying with all the guidelines.

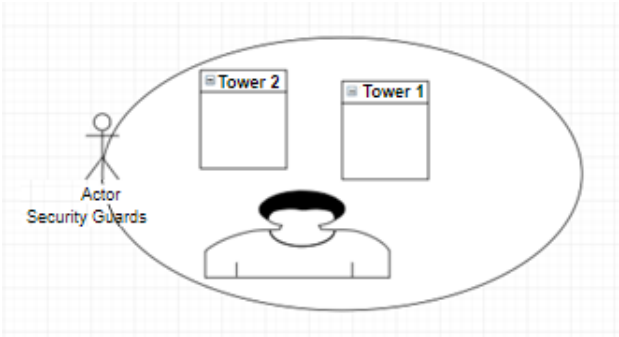
These apps may be vulnerable and allow access of anyone's account to anyone.

All the personal and sensitive data about a Resident may be leaked i.e. who visited what time, duration etc.

Let's come back to the hypothetical scenario, so Mr. Fraud can manage to enter inside the society if he compromises even one visitor management account.



So Mr Fraud is inside the society having details about all the Flats, owners, if someone out for a vacation etc.



Now It's up to the creativity (or destructivity) of Mr Fraud what he does with this access and information.

The last point here is that if someone rings bell of a house, tells owner the details about all their past electricity recharges and telling them that there is a flaw in the electric meter, most probable resident will let him in. Trust can be built by sharing all the information Mr Fraud has.

2. Conclusion

Residents should be aware about the data leaks before providing private data to any online Application/Utility

Society's Management Team should keep one App that can be used for all online purposes and security controls should be verified before using it.