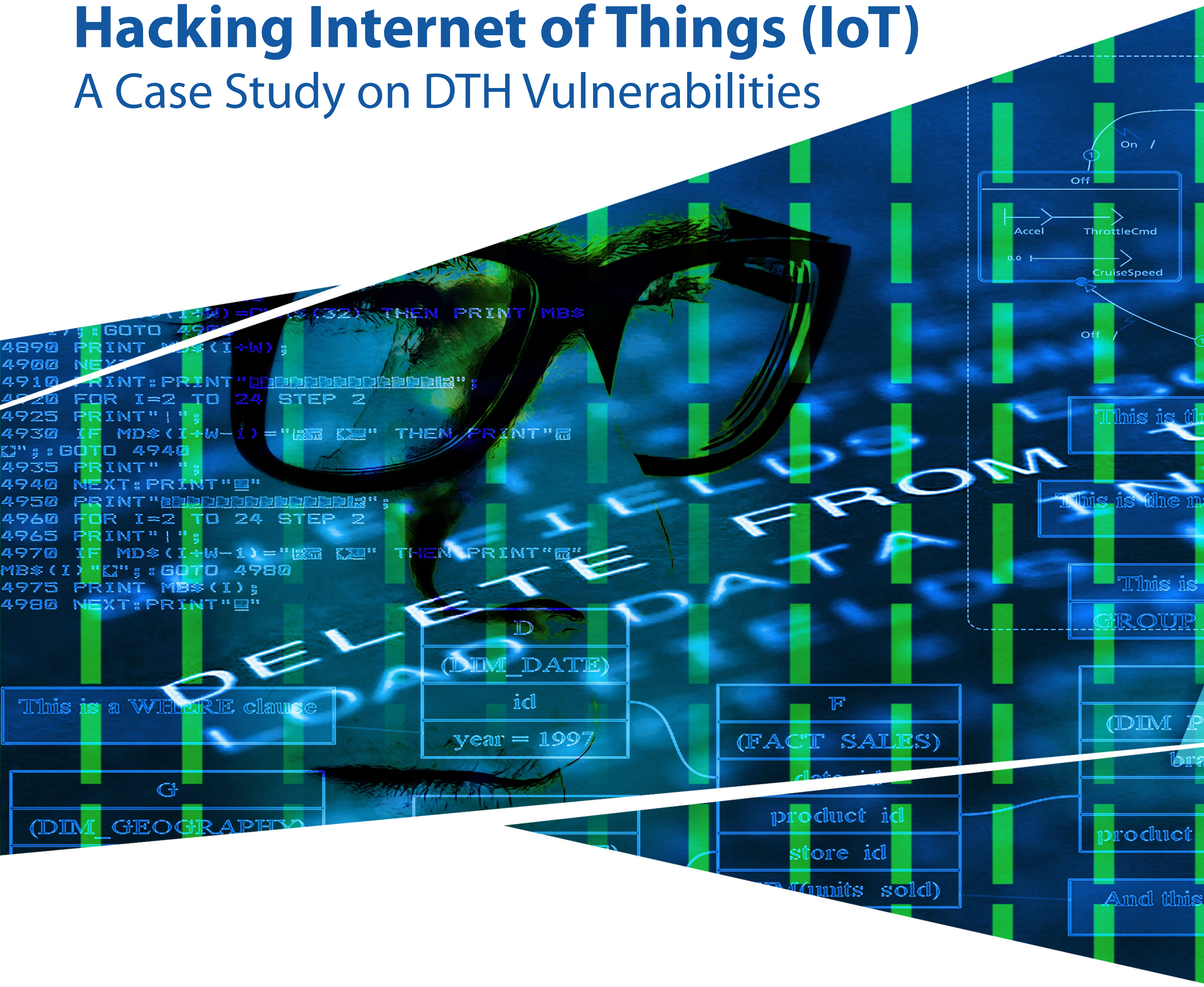
Hacking Internet of Things (IoT)

A Case Study on DTH Vulnerabilities



Author: Veerendra G.G

Introduction

The Internet of Things (IoT) is the network of physical objects—devices, vehicles, buildings and other items—embedded with electronics, software, sensors, and network connectivity that enable these objects to collect and exchange data as defined in Wikipedia. In simple words, the devices connected to the internet irrespective of computational power, price, and size of the device.

The IoT extends internet connectivity other than traditional devices such as desktops and laptop computers, and smart mobile phone devices to a diverse range of real world devices such as a refrigerator, air conditioner, television, washing machine, water purifier, door locks, cars, DTH set top box, and many more which are connected to the internet and become part of IoT.

As per Gartner forecasts 6.4 billion IoT will be in use by 2016, which is 30 percent more from 2015, and will reach nearly 21 billion by 2020. In 2016, 5.5 million new things will get connected every day.

As IoT grows, the attack surface also grows and all the loopholes/vulnerabilities present in the digital world will flow into our real world. Before IoT, attackers used vulnerabilities for data theft or to make money or sometimes just for fun, but with IoT, the attack surface has grown to such extent that attacker can use vulnerabilities or loopholes in the car, smart sniper rifle etc., to kill a person remotely with a few strokes of the keyboard.

Attackers are constantly finding the vulnerabilities to break into IoT and use those vulnerabilities for many illegal purposes.

In this paper, we will learn, how easy it is to hack IoT devices with few real scary attacks and important IoT security cases, followed by current challenges in IoT devices and general guidelines to improve IoT security with respect to the vendor, developer, and users.

At the end, we will demonstrate hacking actual IoT devices by using DTH as an example. With this simple demo, we will understand how to hack interconnected devices and exploit simple vulnerabilities with ease.

Hacking Internet of Things

A few real existing scary attacks are mentioned below

Hacking Car

Figure 1 - Hackers Remotely Kill a Jeep on the Highway - With Me in it [Courtesy: wired.com]

Cars are part of IoT now; attackers find vulnerabilities in the car. Once they find it, it can be used to hijack the car controls completely, and they will be able to apply the brakes, accelerator, steering, open the doors etc. Two security researchers Charlie Miller and Chris Valasek showed a demo on how they kill a Jeep on the highway and Jeep vendor recalled 1.4M vehicles for security fix. What if the attackers find these vulnerabilities and use it for dangerous purposes like killing people by crashing their cars or damaging their properties?

Figure 2 - Miller attempts to rescue the Jeep after its brakes were remotely disabled, sending it into a ditch [Courtesy: wired.com]

Hacking Hospitals

Figure 3 Hospitals Hacked [Courtesy: colocationamerica.com]

Attackers can break into hospitals in many different ways and they can use medical records for different purposes. They can sell the medical records for money which can be used for some dangerous purposes or attackers can hit the hospital with ransomware and encrypt patient's record and threaten the hospital to pay ransom to get the data back by putting the patient's life at risk. Hospitals have no other option but to pay the ransom to get the data back as the patient's data will be critical for the patient's operation or recovery. In April 2016, two hospitals were hit by ransomware in California and Indiana, find more details here. Hospitals are a soft and perfect target for ransomware attacks.

Hacking Smart Sniper Rifle

Figure 4 - Security Researcher Hacking TP750 Smart Sniper Rifle [Courtesy: wired.com]

Smart weapons can save people's lives if used properly. With smart rifle, the accuracy, and efficiency can be increased. At the same time, it's vulnerable to attacks. Attacker can find vulnerabilities and compromise the rifle via its wireless connection. Exploiting those vulnerabilities to jam the rifle and more deadly, attacker can change the scope of the target system, literally changing the target leading to an innocent person's death. Security researchers Runa Sandvik and Michael Auger showed how smart sniper rifle can be hijacked.

Figure 5 - Security Researcher Aiming Target with TP750 Smart Sniper Rifle [Courtesy: wired.com]

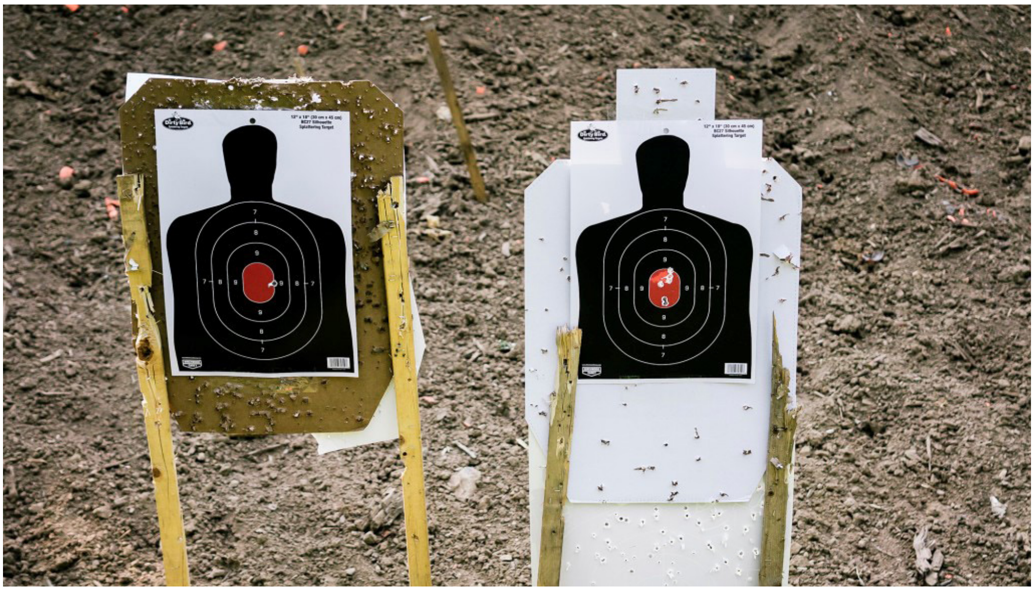


Figure 6 - Rifle seemed to be pointed at the target on the right; the researchers were able to make it hit the bull's-eye on the left instead. [Courtesy: wired.com]

These are a few examples, and all these can be done just by sitting and controlling IoT from somewhere in the world. Attackers can hack into smart homes, nuclear plant, thermal power plant, food productions, manufacturing, telecom; the list goes which makes the world not a safe place to live in.

Important IoT Security Cases

The following examples show how IoT can be a threat to life. While the examples are only illustrations there are many possible ways that an insecure device can pose a threat to life and property.

- German Nuclear Power Plant Shut Down due to Malware Infection
- Everything We Know About Ukraine's Power Plant Hack
- After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix
- Hackers Can Disable a Sniper Rifle - Or Change Its Target
- Two more hospitals struck by ransomware, in California and Indiana
- How One Health Care Organization Dodged the Ransomware Bullet
- Hackers exploit SCADA holes to take full control of critical infrastructure
- Banking Trojans Disguised As ICS/SCADA Software Infecting Plants
- Russian Hackers Hijack Satellite To Steal Data

IoT Challenges

- IoT devices have less resource such as less processing power, storage space, memory etc.
- Firmware up-gradations are not straight forward.
- Not easy to apply security patches.
- Current antimalware, endpoint security software can't be installed on all IoT's.

How to Improve IoT Device Security

Product vendors/developers and customers are all responsible for improving IoT device security. These are general guidelines, may not be applicable for all the IoT devices in all the scenarios.

Product vendors/developers should consider steps below to improve IoT security

- Secure web/desktop/mobile applications with proper authentication and authorization.
- If feasible, Implement and enable 2-factor authentications by default, it will considerably improve IoT device security.
- Follow secure coding methods and always perform input validation to avoid Cross-site scripting (XSS), SQL injection and Buffer Overflow (BoF) vulnerabilities. Follow hyperlinks to understand more on these vulnerabilities.
- Enforce an effective password policy, at least 8 -10 characters long with a mixture of letters, numbers, and special characters.
- Use captcha, account lockout policy methods to avoid brute force attacks.
- Vendors should provide security updates including details on security fixes, the impact of the vulnerability and provide simple steps to deploy security updates.
- If feasible, always use encryption for communication.
- Ensure regular backups (at least two or more data) in a secure place.
- Avoid information disclosure. i.e avoid publishing customer's data such as name, phone number, DoB etc., publicly.
- While adding new features to the product, vendors should make sure it will not create or be used as a security hole.
- Vendors should think on ease of use vs security.

- Make sure below mentioned OWASP Top 10 IoT Vulnerabilities should be addressed, while IoT design and development.

Users should consider steps below to improve IoT security

- Users should download software's and updates only from vendors and trusted source, and always verify the integrity of downloaded software's/updates with md5 or SHA.
- Apply security updates regularly.
- Users should be educated on the importance of security and its impacts.
- Always enable 2-factor authentications, if available in the product.
- Use strong and unique passwords at least 8-20 characters with a mixture of letters, numbers and special characters.
- Ensure regular important data backups (at least two or more) in a secure place.
- Stop unwanted services.

Steps below are indirectly crucial for IoT security

- Don't open email attachments from an unknown sender, as they may contain malware**.**
- Don't reply to spam emails asking about personal and banking details, it can be used to steal money from a bank or use it other advanced attacks.
- Don't visit links sent by unknown people.
- Don't install cracked software's, applications or games as they might contain malware.
- Don't disclose sensitive information, such as DoB, phone number, email id etc., publicly.

OWASP Top 10 IoT Vulnerabilities (2014)

The Open Web Application Security Project (OWASP) Top 10 IoT Vulnerabilities are as follows:

1. Insecure Web Interface
2. Insufficient Authentication/Authorization
3. Insecure Network Services
4. Lack of Transport Encryption/Integrity Verification
5. Privacy Concerns
6. Insecure Cloud Interface
7. Insecure Mobile Interface
8. Insufficient Security Configurability
9. Insecure Software/Firmware
10. Poor Physical Security

In this paper, we will show how easy it is to hack IoT devices by using DTH as an example. With this simple demo, we will understand how easy it is to hack interconnected devices and exploit simple vulnerabilities. With this exploit, it is possible to, disturb the service to the user, record any shows without user permission, and steal the recorded shows/videos. Securing against this kind of attacks is ignored by vendors.

We have experimented with **Tata Sky DTH set top box, because it was easily available** and found these vulnerabilities. These vulnerabilities are likely to be present in other DTH set top box from different vendors.

We have contacted Tata Sky vendor multiple times giving complete technical details about these vulnerabilities.

Before we start the demo let's have a look at DTH set top box and its features, so that we understand the attack.

Demo - Hacking IoT (DTH Setup box)

What is DTH?

DTH stands for Direct to Home service. DTH is a digital satellite service that provides television viewing services directly to subscribers through satellite transmission anywhere in the country. In this, a personal dish is placed outside a home which helps in receiving the signals and broadcasting the transmission onto a television. The signals are digital by nature and are received directly from the satellite.

Like most of the DTH providers offer multiple services, Tata Sky offers customers interactive services as well as a variety of channels ranging from entertainment, sports, movies and music to news and documentaries in DVD quality picture and CD quality sound.

Before we demonstrate how we can hack into Tata Sky DTH set top box and exploit a few simple vulnerabilities discussed above, we need to understand Tata Sky DTH set top box and its features. This will help us understand how these features can be used to hack the Tata Sky DTH Set top box.

Understanding DTH set top box

There are different kinds of setup box based on the features it offers. In this paper, we concentrate on DTH set top box with Record and Transfer capabilities.

DTH set top box Transfer HD unique features

- ✓ Recharge and select different packages online
- ✓ Recording and Remote Recording
- ✓ View recorded content anytime, anywhere
- ✓ Record, Transfer, Carry recorded content

Many other features are available but in this demo, we will make use of these features to exploit vulnerabilities.
Recording Limitation: At a time only 2 channels can be recorded, if we start the third recording then DTH set top box will prompt a message box on the TV to select which channel to watch or which channel to cancel.

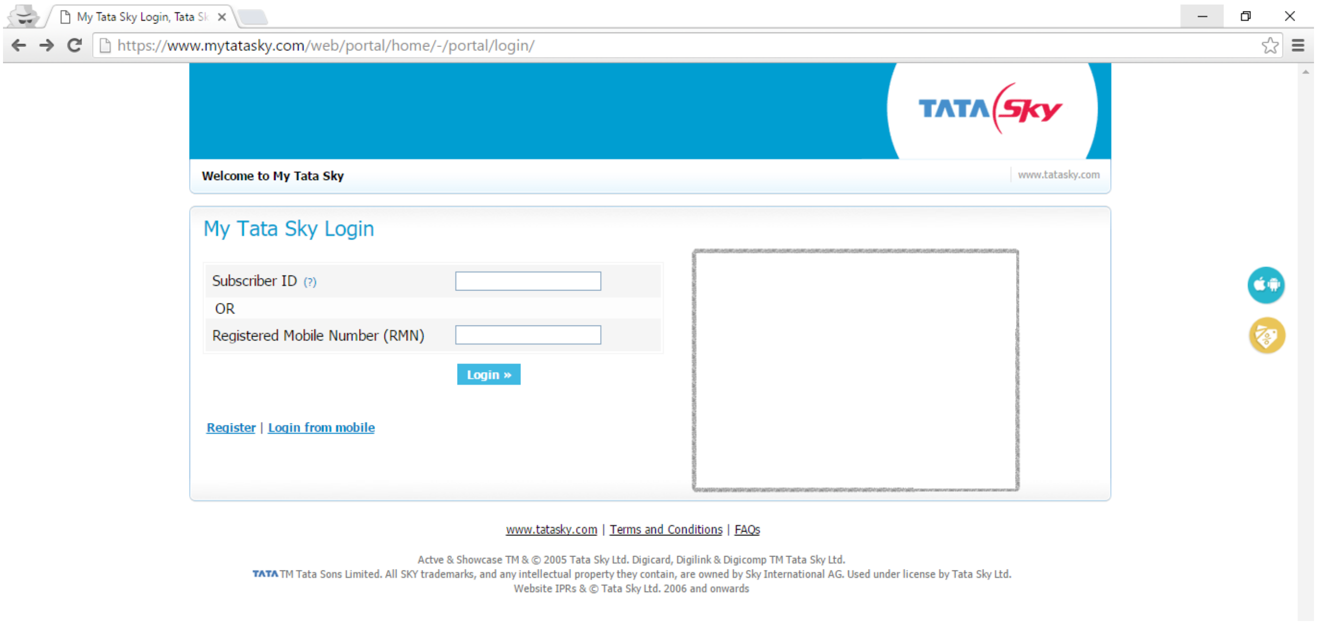
Vulnerabilities in DTH set top box and vendor website

1. Personal information disclosure (Privacy Concerns)
2. Remote Recording (Insufficient Authentication/Insecure Mobile Interface)
3. Disturb the service (Denial of Service)
4. Stealing recordings (Privacy Concerns)

How to exploit vulnerabilities?

Vulnerability 1 - Personal information disclosure (Privacy Concerns)

1. Visit DTH provider website. In our case, we experimented with Tata Sky.


My Tata Sky Login, Tata Sk

https://www.mytatasky.com/web/portal/home/-/portal/login/

Welcome to My Tata Sky

www.tatasky.com

My Tata Sky Login

Subscriber ID (?)

OR

Registered Mobile Number (RMN)

Login »

Register | Login from mobile

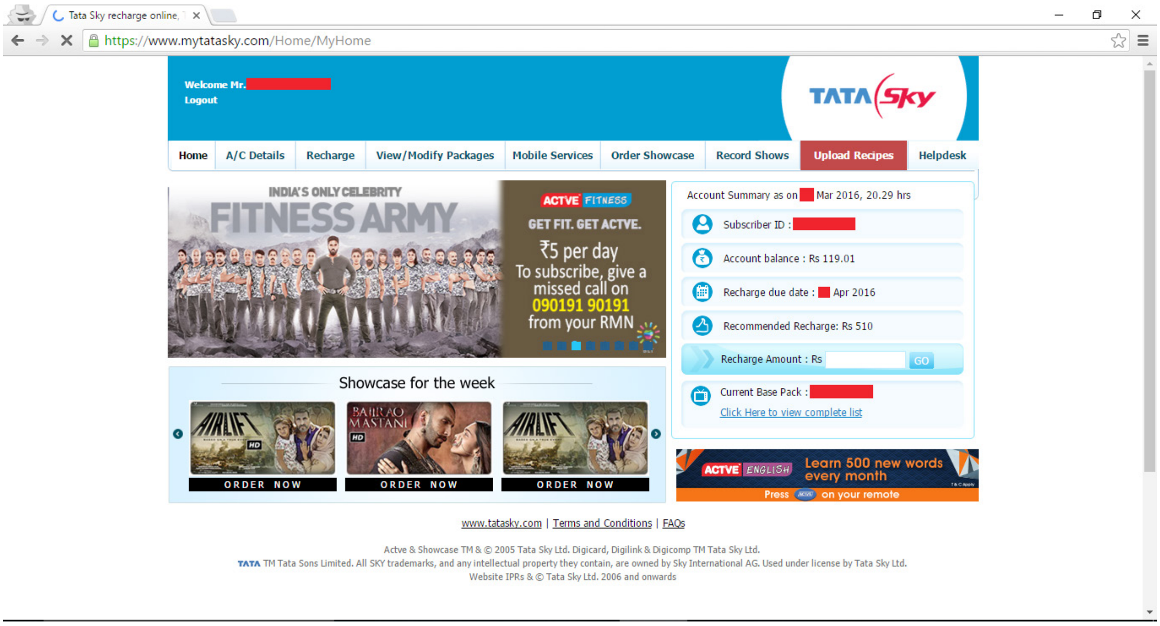
www.tatasky.com | Terms and Conditions | FAQs

Actve & Showcase TM & © 2005 Tata Sky Ltd. Digicard, Digilink & Digicomp TM Tata Sky Ltd.
TATA TM Tata Sons Limited. All SKY trademarks, and any intellectual property they contain, are owned by Sky International AG. Used under license by Tata Sky Ltd.
Website IPRs & © Tata Sky Ltd. 2006 and onwards

DTH Provider website: Login Page

2. Enter a mobile number (which is easy to get from many sources such as Facebook, True caller etc.) or brute force mobile number as there is no captcha or any other security mechanism to prevent brute force attack.

3. Just by entering the mobile number, other private information is available without authentication such as Subscriber Name, Subscriber ID, Account balance, Current Base Pack etc., as shown in the below image, some of this private information can be used for various advanced attacks.


Tata Sky recharge online,

https://www.mytatasky.com/Home/MyHome

Welcome Mr.[redacted]
Logout

Home | A/C Details | Recharge | View/Modify Packages | Mobile Services | Order Showcase | Record Shows | Upload Recipes | Helpdesk

Account Summary as on [redacted] Mar 2016, 20.29 hrs

Subscriber ID : [redacted]

Account balance : Rs 119.01

Recharge due date : [redacted] Apr 2016

Recommended Recharge: Rs 510

Recharge Amount : Rs GO

Current Base Pack : [redacted]

Click Here to view complete list

Showcase for the week

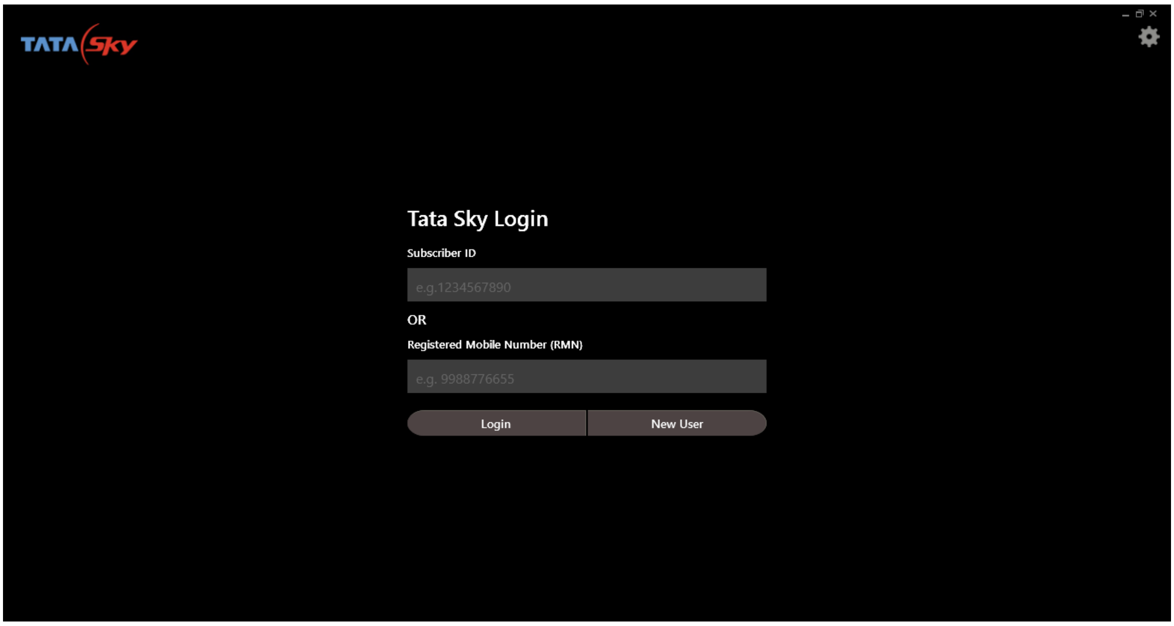
www.tatasky.com | Terms and Conditions | FAQs

Actve & Showcase TM & © 2005 Tata Sky Ltd. Digicard, Digilink & Digicomp TM Tata Sky Ltd.
TATA TM Tata Sons Limited. All SKY trademarks, and any intellectual property they contain, are owned by Sky International AG. Used under license by Tata Sky Ltd.
Website IPRs & © Tata Sky Ltd. 2006 and onwards

DTH Provider website: After Entering Registered Mobile Number

Vulnerability 2 - Remote Recording (Insufficient Authentication/ Insecure Mobile Interface)

1. Download DTH Mobile app which is available for Android Mobiles/Tablets, iPhone, iPad, Mac and for Desktop.
2. Start the application and enter subscriber ID (or mobile number) which is disclosed in Vulnerability 1.



Tata Sky Login

Subscriber ID

e.g.1234567890

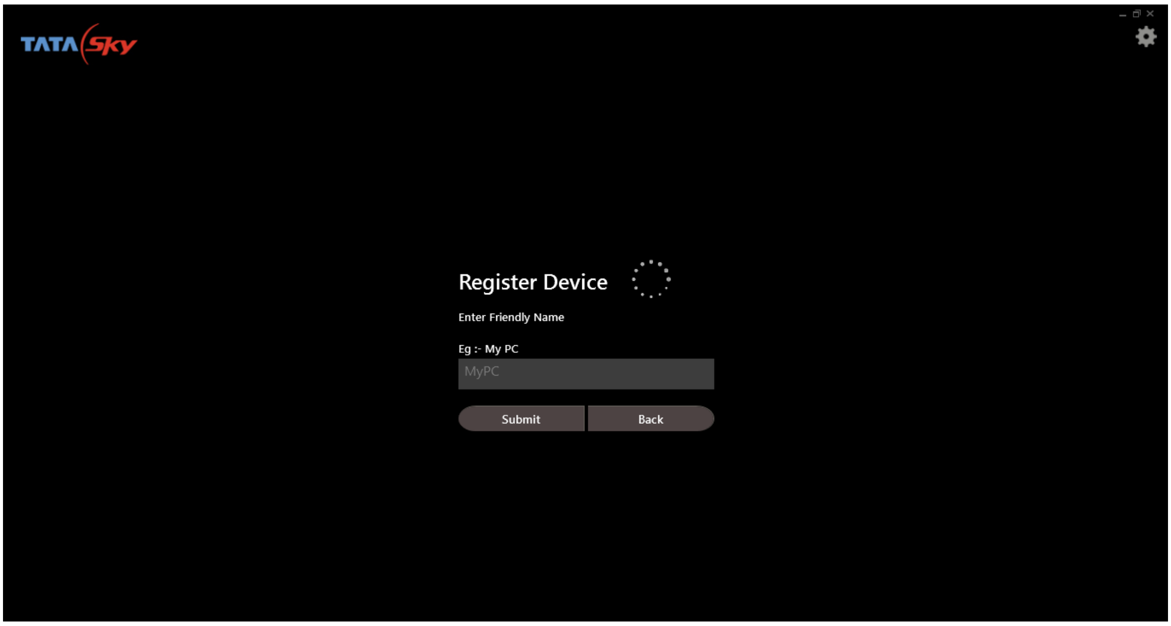
OR

Registered Mobile Number (RMN)

e.g. 9988776655

DTH Provider Desktop App: Login Page

3. Enter register device friendly name and click on submit.



Register Device

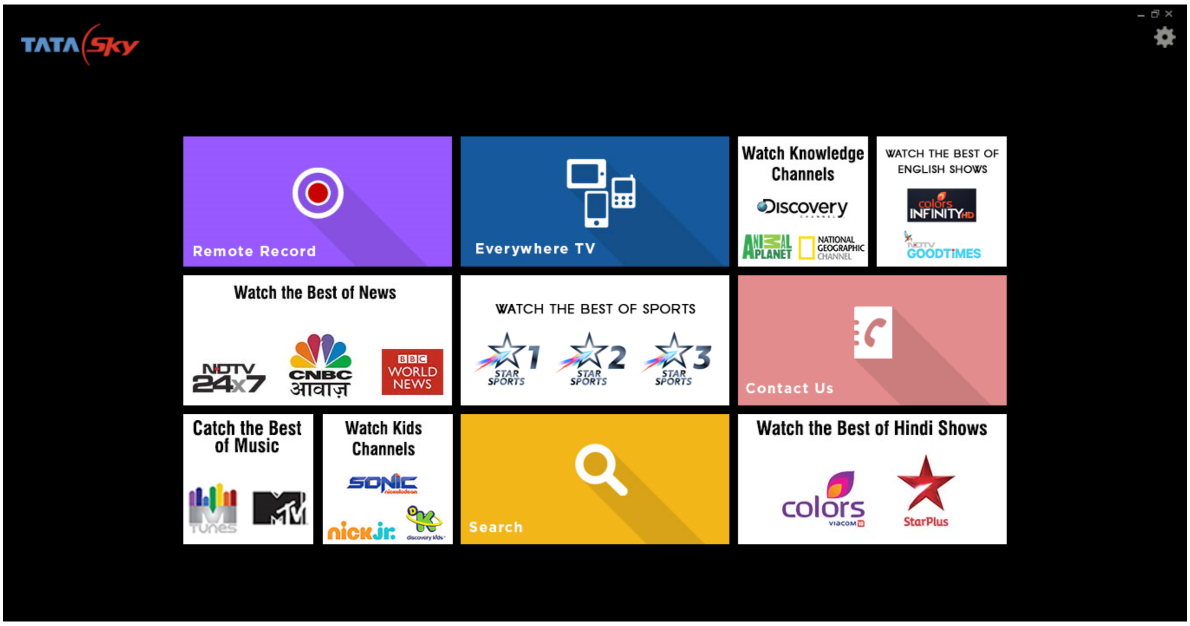
Enter Friendly Name

Eg :- My PC

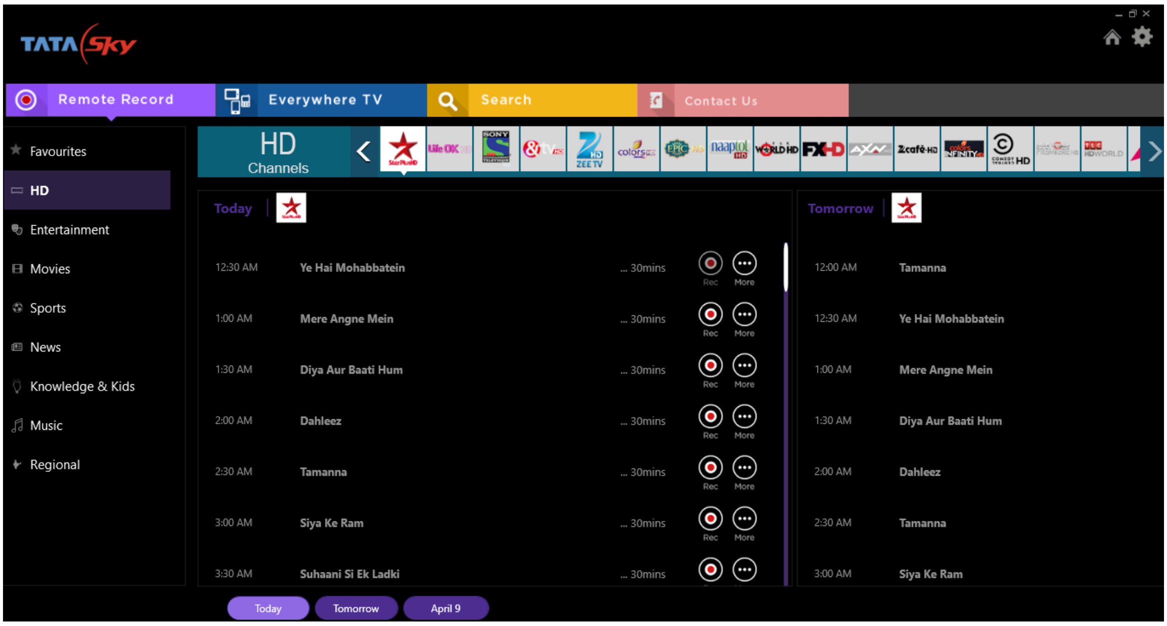
MyPC

DTH Provider Desktop App: During Registration

4. Click on "Remote Record", from there the attacker can record any TV shows without authentication or authorization.



DTH Provider Desktop App: After login



Today			
12:30 AM	Ye Hai Mohabbatein	... 30mins	Rec More
1:00 AM	Mere Angne Mein	... 30mins	Rec More
1:30 AM	Diya Aur Baati Hum	... 30mins	Rec More
2:00 AM	Dahleez	... 30mins	Rec More
2:30 AM	Tamanna	... 30mins	Rec More
3:00 AM	Siya Ke Ram	... 30mins	Rec More
3:30 AM	Suhaani Si Ek Ladki	... 30mins	

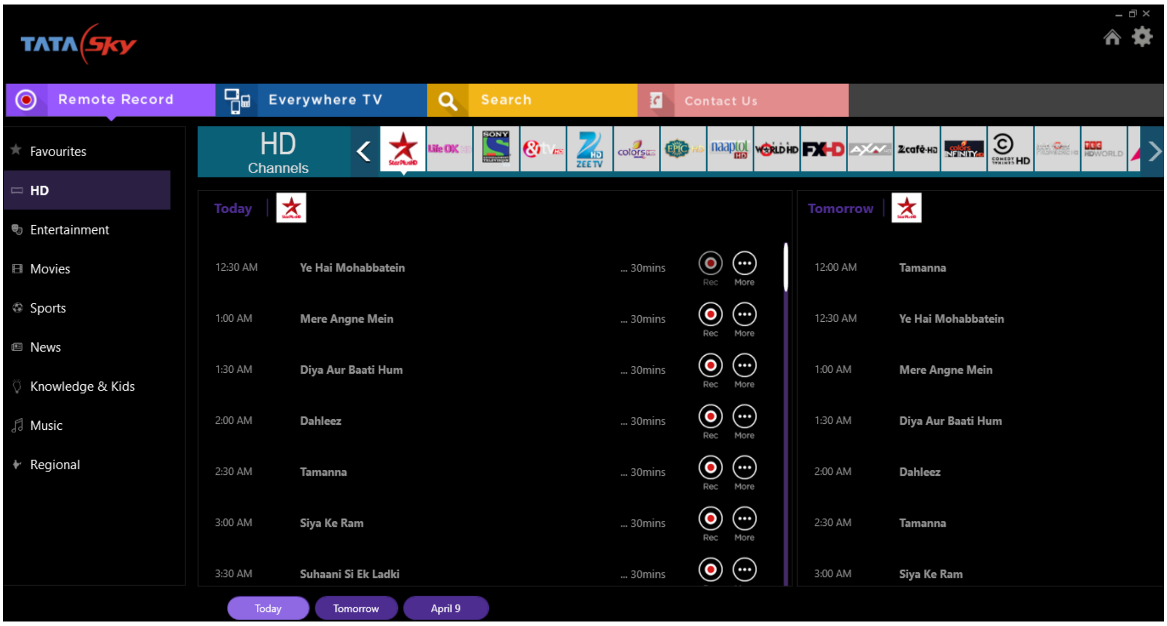
Tomorrow	
12:00 AM	Tamanna
12:30 AM	Ye Hai Mohabbatein
1:00 AM	Mere Angne Mein
1:30 AM	Diya Aur Baati Hum
2:00 AM	Dahleez
2:30 AM	Tamanna
3:00 AM	Siya Ke Ram

DTH Provider Desktop App: Inside Remote Record Section

NOTE: In future, if the set-top box comes with a camera then the attacker can turn on the camera, which is a real privacy concern.

Vulnerability 3 - Disturb the service (Denial of Service)

1. After exploiting **Vulnerability 1 and 2**, now the attacker can initiate remote recording using DTH Mobile app, which does not require any authentication or authorization and there are no restrictions to limit how many remote recordings can be initiated.



Today

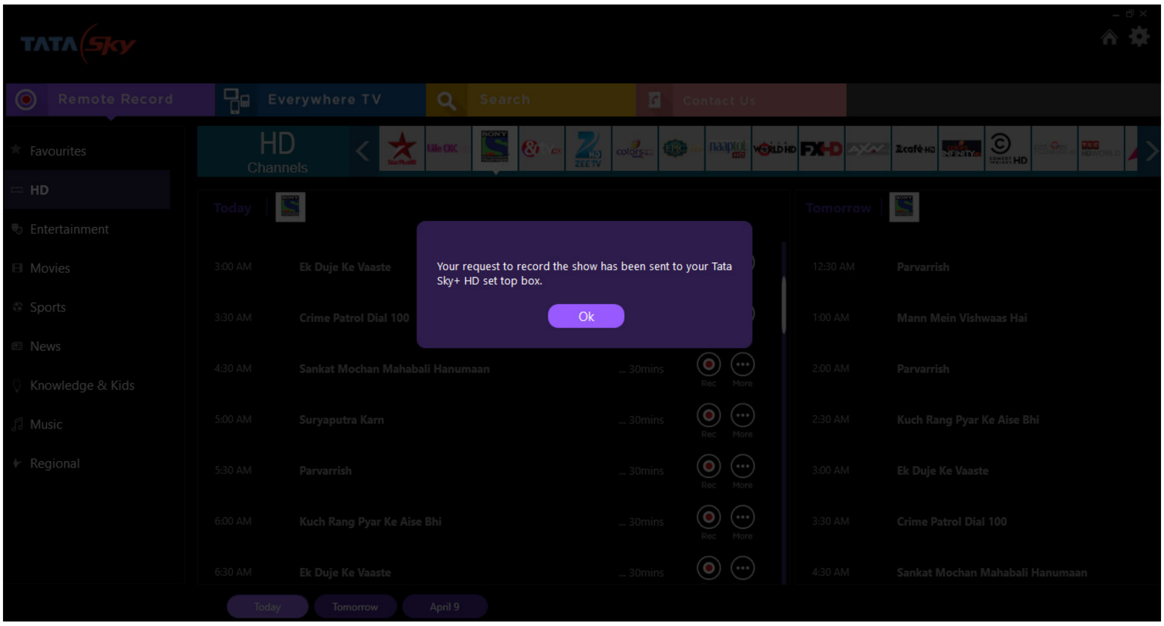
12:30 AM Ye Hai Mohabbatein ... 30mins
1:00 AM Mere Angne Mein ... 30mins
1:30 AM Diya Aur Baati Hum ... 30mins
2:00 AM Dahleez ... 30mins
2:30 AM Tamanna ... 30mins
3:00 AM Siya Ke Ram ... 30mins
3:30 AM Suhaani Si Ek Ladki ... 30mins

Tomorrow

12:00 AM Tamanna
12:30 AM Ye Hai Mohabbatein
1:00 AM Mere Angne Mein
1:30 AM Diya Aur Baati Hum
2:00 AM Dahleez
2:30 AM Tamanna
3:00 AM Siya Ke Ram

DTH Provider Desktop App: Inside Remote Record Section

2. The attacker can initiate remote recording on all the shows in all the channels. Due to recording limitation (as discussed earlier), only 2 channels can be recorded at a time. Now the user will be prompted on the TV to choose which channel to record or which channel to discard. As the attacker initiated too many remote recording requests, the user needs to keep selecting the channels leading to a denial of service to the user.



Your request to record the show has been sent to your Tata Sky+ HD set top box.

Today

3:00 AM Ek Duje Ke Vaaste
3:30 AM Crime Patrol Dial 100
4:30 AM Sankat Mochan Mahabali Hanumaan ... 30mins
5:00 AM Suryaputra Karn ... 30mins
5:30 AM Parvarrish ... 30mins
6:00 AM Kuch Rang Pyar Ke Aise Bhi ... 30mins
6:30 AM Ek Duje Ke Vaaste ... 30mins

Tomorrow

12:30 AM Parvarrish
1:00 AM Mann Mein Vishwaas Hai
2:00 AM Parvarrish
2:30 AM Kuch Rang Pyar Ke Aise Bhi
3:00 AM Ek Duje Ke Vaaste
3:30 AM Crime Patrol Dial 100
4:30 AM Sankat Mochan Mahabali Hanumaan

DTH Provider Desktop App: During Registration

Vulnerability 4 - Stealing recordings (Privacy Concerns / Digital theft)

1. After exploiting Vulnerability 1 and 2, now the attacker can use DTH set top box features such as Record, Transfer, Carry, where the attacker can transfer previously recorded content to his device anytime, anywhere without authentication or authorization.

2. The attacker can make money by selling these recordings or attacker can just distribute the recording leading to digital theft.

This way inter-connected IoT device can be hacked. This is one small demo on how features and simple insecure authentication/authorization can be used to attack IoT devices.

To make it scary, attackers can write **simple worm** to collect phone numbers from different sources (such as facebook, true caller) or brute force to get customer information (along with subscriber id) from DTH Provider website and use the stolen information to disrupt DTH provider service or to steal recorded videos badly affecting DTH provider reputation.

Also, stolen information can be used in social engineering or many other advanced attacks which are limited to attacker's imagination.

Business Impact on DTH Provider

- Stolen customer information can be used for social engineering or many other advanced attacks.
- Service Disruption
- Decrease in vendor trust and reputation
- Loss of money
- Data theft

Conclusion

The Internet of Things (IoT) industry is still evolving and growing rapidly and exposing IoT devices to zero-day attacks, new attack methods/vulnerabilities. Securing the IoT devices is challenging due to size, memory, processing power etc. Securing IoT devices is a responsibility of vendors, developers, and users. All of them need to be educated about security and impact if ignored. Vendors should design and implement IoT devices with device security in mind and provide ways to apply security updates in a simple way. Users have to make sure that they do what is required. Even if the vendor provides for security the user can ignore things and cause issues.

We have shown it is how easy to hack IoT devices with Tata Sky as an example. This may not be life threatening but other IoT's can be life threatening. IoT vendors should take extraordinary precautions with respect to IoT security and make harder for an attacker to find and exploit security vulnerabilities in IoT devices.

Acknowledgement

I thank Sateesh S Kannegala, Chief Consultant Technology Management, SecPod Technologies Pvt. Ltd. for comments that greatly improved the manuscript.

About Us

Founded in 2008 and headquartered in Bangalore with operations in USA, SecPod Technologies creates cutting edge products to ensure endpoint security. We strongly believe in the principle 'Strong Defense, Not a Weak Cure' and our product Saner Business reflects this ideology by proactively detecting and eliminating vulnerabilities before they can be exploited. We have been entrusted by Enterprise and mid level organizations in various verticals including Government, Healthcare, and IT/ITES.

Contact Us

Web: www.secpod.com Tel: +91-80-4121 4020
Email: info@secpod.com +1-918-625-3023