

NON-TECH EDITION!

PWN

SAMSUNG SMART TV

(PWNED TV MAKES YOU *NAKED*)

BEIST / Korea University CIST IAS LAB

<http://grayhash.com>

<http://twitter.com/beist>

beist@grayhash.com

About me

- Lee Seungjin (aka beist)
- Ms-Phd course at Korea University (CIST IAS LAB)
- Principal Security Consultant at GrayHash
- BoB Mentor
- Many wins at hacking contests
- 5 times Defcon CTF finals (First asian)
- Speaking at security conferences
- Run hacking contests/conferences (Now, secuinside organizer)
- Love hunting 0days

Research motivation

- Smart TV being super popular
- In 2012, over 80,000,000 smart TV sold
- It is going to be more popular over the world
- But it seems no security research for Smart TV yet
- Smart TV is like “*home-version* smartphone”
- Might be more scary than smartphone (if it's infected)
 - 24 hour surveillance

Smart TV

- Smart TV is now used in many fields already
 - Home entertainment
 - Office purpose
 - Educational purpose
 - Business purpose (Even you can find SmartTV in restaurants)

Smart TV

- Smart TV is not just TV
 - Changing psychological consumer behavior and its impact on the commercial sector
 - The feasibility of potential applications for smart TV in the consumer electronics market
 - The integration of smart TV platforms with IC technology solutions

Why dangerous?

- Smart TV has a lot of features
 - It recognizes your voice and motion (sensors)
 - Even you can turn Smart TV on using your voice
 - “하이 티비 전원켜기” (“Hi, TV, turn it on”)
 - Changing channels, volume up/down, launching apps
 - Camera and voice recorder
 - You never know if your Smart TV camera is working or not

Why dangerous?

- Very hard to detect attacks
 - Basically, you don't have any access (shell) to the TV unless you hack your TV
 - There is no way to detect threats/attacks yet
 - No Anti-Virus program on TV
 - But this is not a solution

Quick question

- Does samsung really do something for TV security? Are security issues you found really security issues? Maybe they're just features?
- Unfortunately, it looks Samsung is trying to do something very hard for TV security
- They're hiring hackers as well
- And, check this out: <http://www.samsungdforum.com/Support/TVAppsSecurity>

Quick and worst scenarios

- Hackers can do traditional logging like key-strokes
 - Even cam-logging and voice-recording
 - You can't detect if your cam/voice sensors are working
- Hackers can make Smart TV network-working always
 - Even when you think your TV is off (24-hour surveillance)
- Hackers can steal personal information (picture/videos/etc)
- Hackers can steal users' financial information

Target

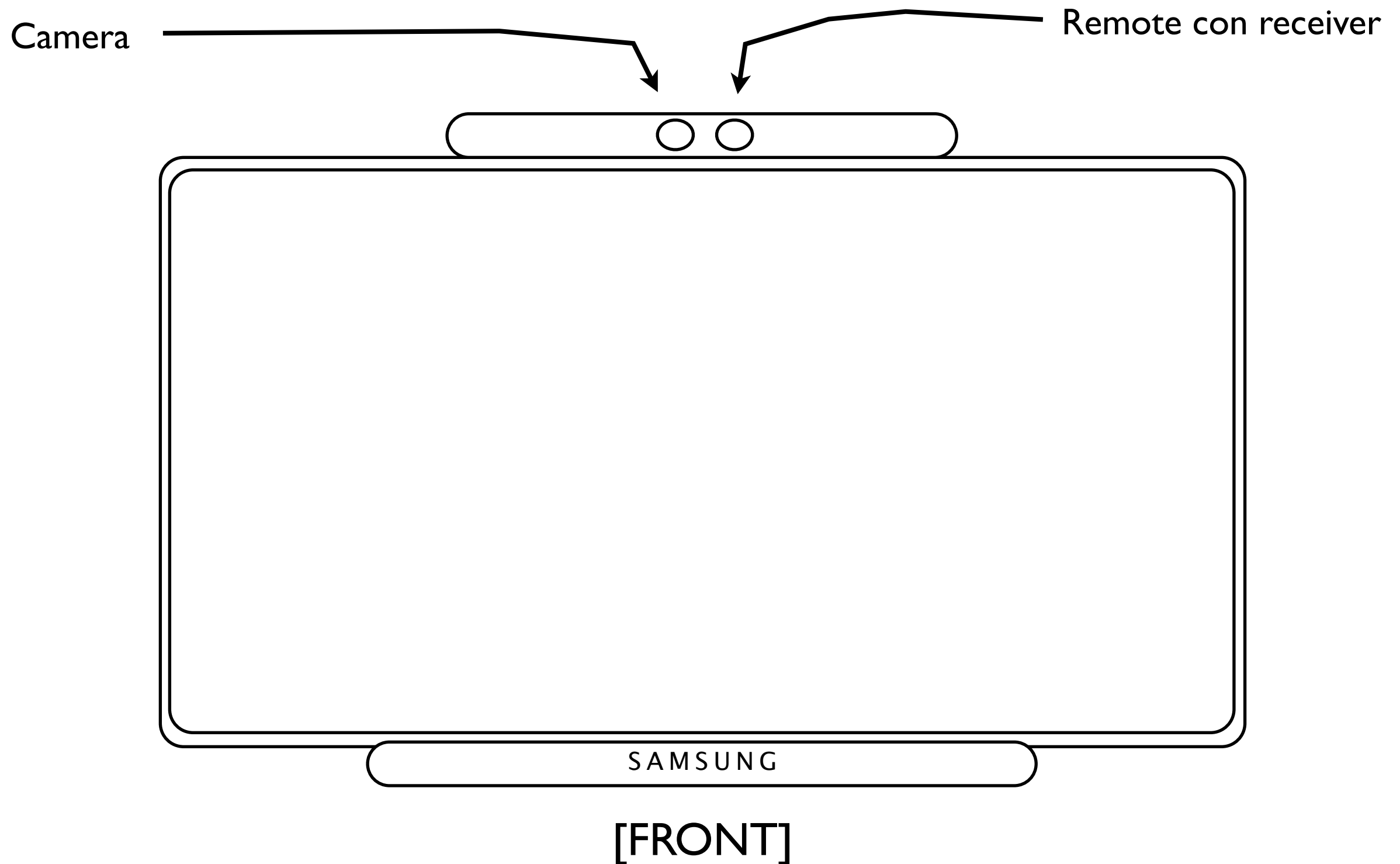


- Samsung Smart TV
 - Why: Because Samsung is No.1 in Smart TV business
- Samsung Smart TV ES8000
 - Why ES8000: Because this is the latest samsung smart TV
 - “Home Cinema Choice”
 - “Queen Royal Warrant” (first time for TV manufacturer)

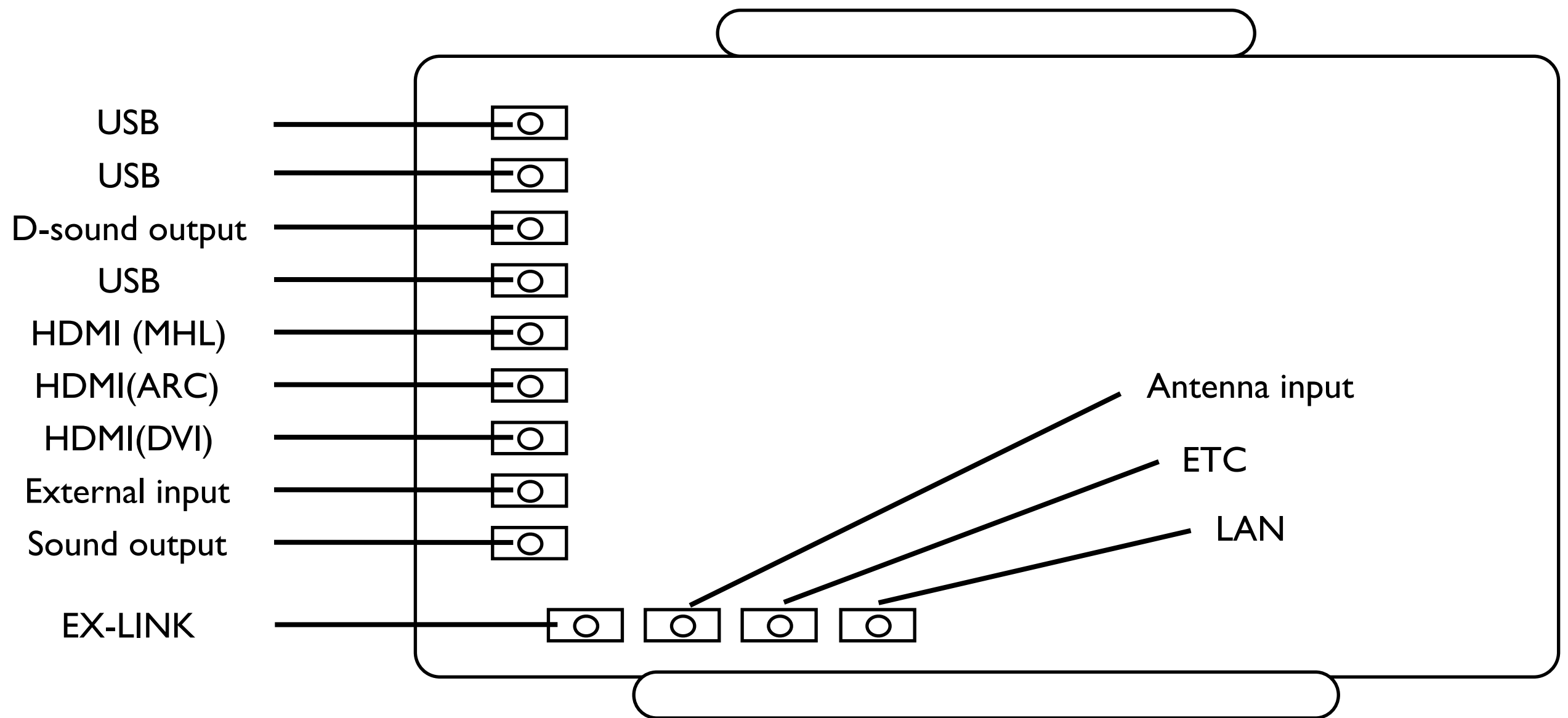
Samsung Smart TV ES8000

- CPU: ARMv7 Processor
- OS: Linux 2.6.35.13
- Disk: almost 1 GB free space (But you can use USB storages)
- Interfaces: usb, hdmi, voice/record input/output ports
- Devices: camera, voice recorder, wifi, bluetooth, irda and etc

Samsung Smart TV ES8000



Samsung Smart TV ES8000



[THE BACK]

Samsung Smart TV ES8000

- INSIDE of ES8000
 - Many modules inside
 - WIFI
 - Bluetooth
 - UART (of course!)
 - JTAG possible, but didn't check out

Attack vectors

- Samsung apps (Samsung stores)
- Network
- Physical attack
- Broadcast signal
- Contents (DRM)
- Default installed apps minor issues

Samsung apps attack vectors

- Samsung has its own app-store called Samsung Apps
- They don't allow developers to make native applications
 - Except for serious partners
 - Serious partners can make native apps (ex: Skype)
- Only javascript or flash is allowed.

Network attack vectors

- Network
 - Internet
 - Web browser, Family story and other applications
 - Remote management
 - MITM
 - Pwning
 - Sniffing sensitive/media data

Network attack vectors

- Network
 - Local network (Intranet)
 - It has over 10 tcp listening ports
 - WIFI module, Bluetooth module

Physical attack vectors

- Physical
 - USB
 - Filesystem bugs, parsing USB, upgrading using USB
 - Remote controller (IrDA)
 - Many input/output ports for devices

Broadcast attack vectors

- Broadcast signal
 - Samsung provides “firmware upgrade” using Broadcast signal (Not internet)
 - No idea how this works, but would be interesting if attackers can broadcast signal

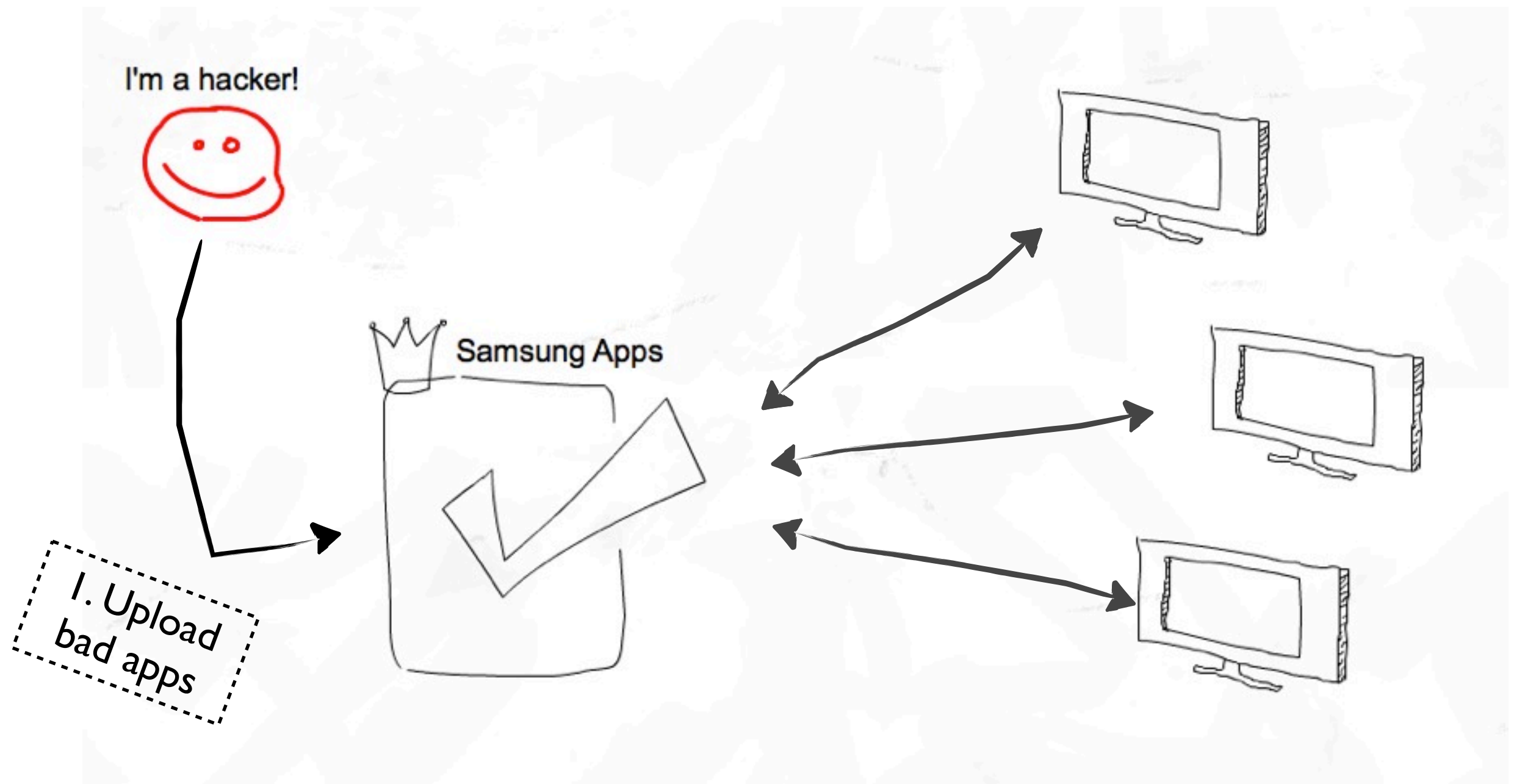
Contents (DRM)

- Samsung cares a lot for contents protection
 - No copy DRM contents
- Smart TV has ARM TrustZone to use PlayReady
- Coping DRM contents with some ways will be interesting

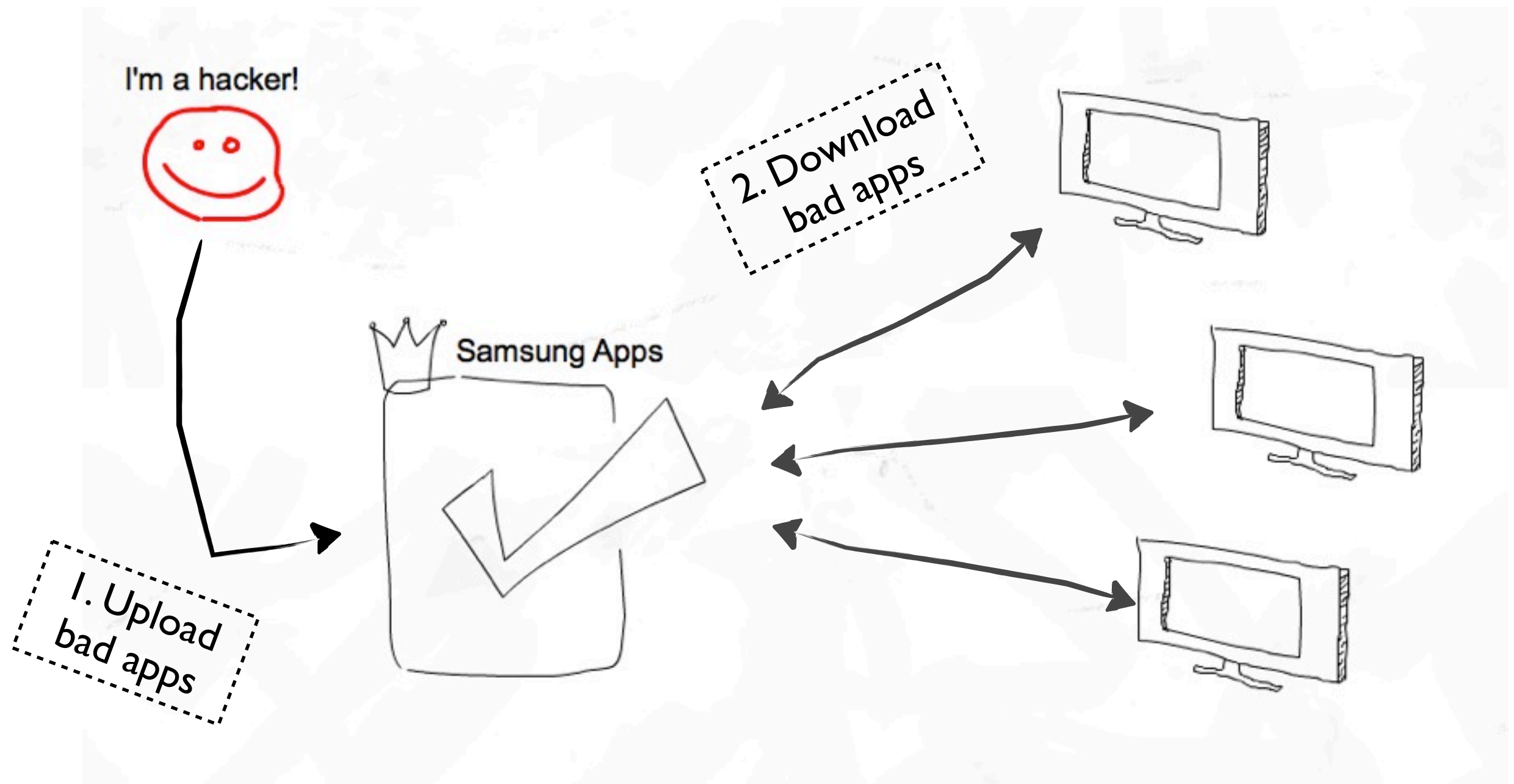
Default installed apps minor issues

- If they use SSL
- Insecure storage method
 - API key management (Facebook, etc)
 - Other important information (login credential, etc)

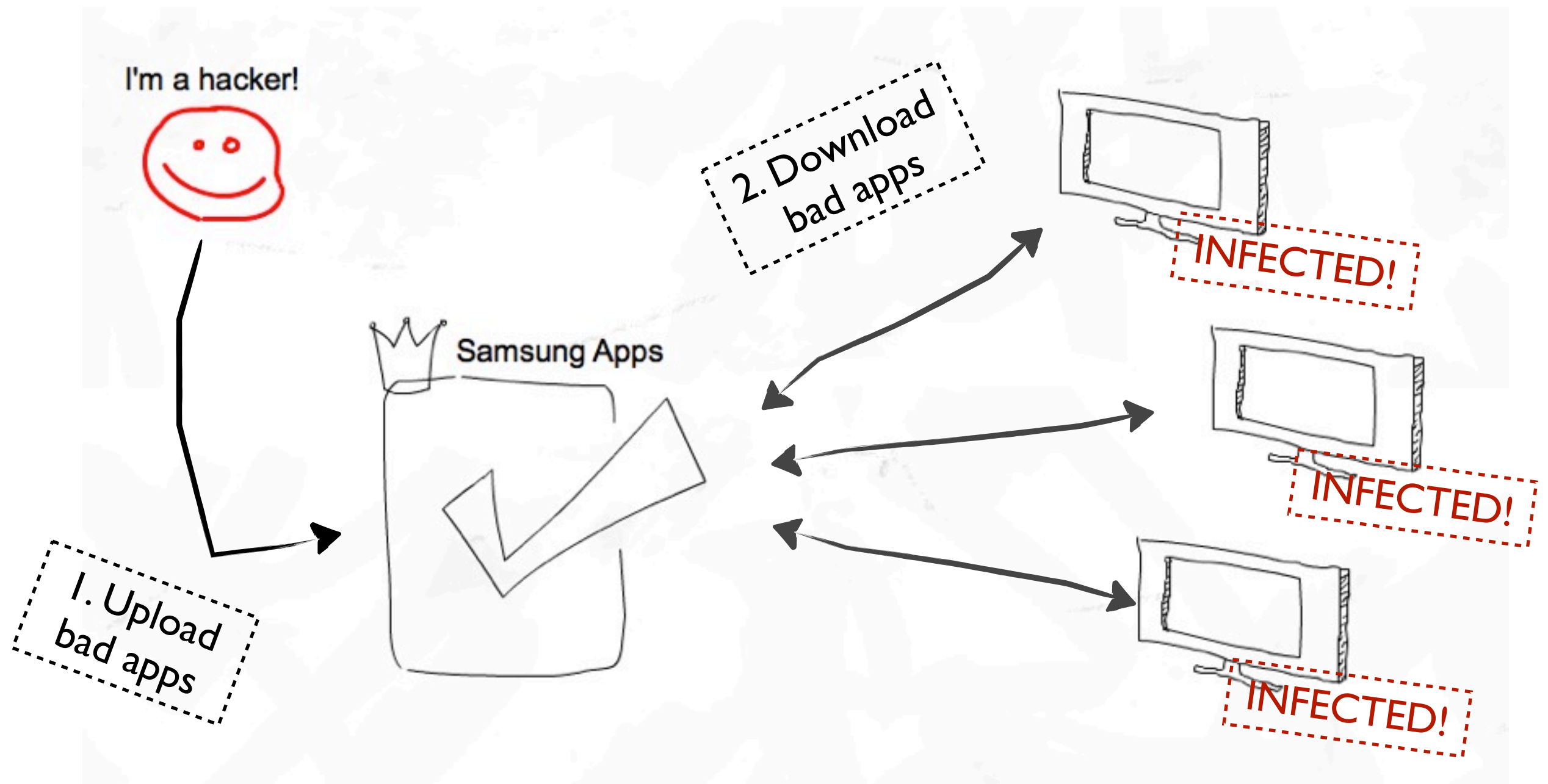
Samsung Apps Market



Samsung Apps Market



Samsung Apps Market



Samsung Apps Market

- As we said, you can make Smart TV apps only written in Javascript/HTML/Flash
- They provide Smart TV SDK for developers
- They offer you APIs that you can use in Javascript
 - File I/O, video and audio control, camera and etc

Samsung Apps Market

- They try to prevent from making malicious Apps
 - <http://www.samsungdforum.com/Support/TVAppsSecurity>
- Unfortunately, it looks they're not doing so well
- We've found a lot of security holes and wrong security policy

Samsung Apps Security Holes

- We can divide the holes as 7
 - Wrong design (architecture)
 - Directory listing
 - Arbitrary file copy
 - Arbitrary file write
 - Arbitrary file read
 - Arbitrary file delete
 - Arbitrary command execution

Wrong security policy #1

- They give developers these APIs
 - open/close/delete/create/isValidCommonFile
 - Those APIs works in a shared directory (like '/tmp/')
 - /mtd_down/common
- But, all apps are running as 'root'
 - Actually, apps are not processes but javascript/flash/etc
 - Only one process (No different privilege)
- So, you can read/write any file which is created by another application in the shared directory

Wrong security policy #2

- Again, all apps are running as 'root'
 - There is only 'root' account in /etc/passwd
- Which means if there is anything wrong in an application, a hacker can compromise the whole TV
- There are default installed apps
 - MITM might be a very good target for hackers
 - Will cover this issue later

Wrong security policy #2

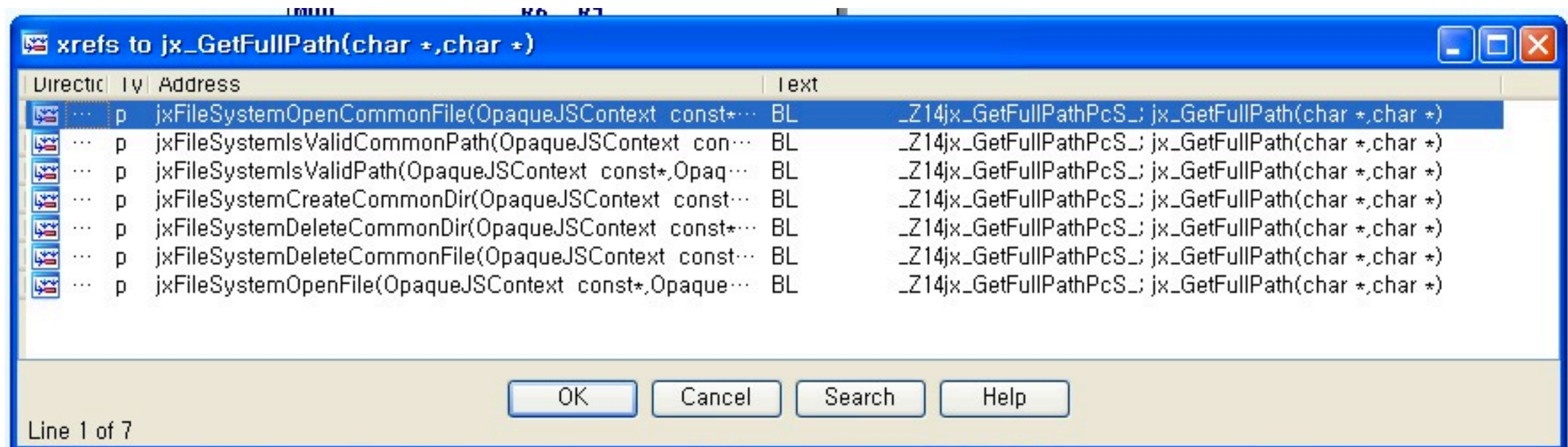
PID	USER	VSZ	STAT	COMMAND
1	root	1688	S	init
2	root	0	SW	[kthreadd]
3	root	0	SW	[ksoftirqd/0]
4	root	0	SW	[migration/0]
5	root	0	SW	[migration/1]
6	root	0	SW	[ksoftirqd/1]
7	root	0	SW	[events/0]
8	root	0	SW	[events/1]
9	root	0	SW	[khelper]
10	root	0	SW	[async/mgr]
11	root	0	SW	[sync_supers]
12	root	0	SW	[bdi-default]
13	root	0	SW	[kblockd/0]
14	root	0	SW	[kblockd/1]
15	root	0	SW	[kmmcd]
16	root	0	SW	[kdtvlogd]
17	root	0	SW	[kswapd0]
18	root	0	SW	[xfs_mru_cache]
19	root	0	SW	[xfslogd/0]
20	root	0	SW	[xfslogd/1]
21	root	0	SW	[xfsdatad/0]
22	root	0	SW	[xfsdatad/1]
23	root	0	SW	[xfsconvertd/0]
24	root	0	SW	[xfsconvertd/1]

25	root	0	SW	[mmcqd]
37	root	1692	S	-/bin/sh
58	root	1692	S	/bin/sh /mtd_exe/rc.local
67	root	1502m	S	./exeDSP
88	root	0	SW	[aeMsgTask]
149	root	0	SW	[khubd]
247	root	0	SW	[flush-179:0]
256	root	17692	S	/mtd_cmmlib/BT_LIB/bsa_server -all=0
265	root	0	SW	[usbhid_resumer]
458	root	234m	S	/mtd_appdata/Runtime/bin/X -logfile
579	root	486m	S	/mtd_appdata/InfoLink/lib/WidgetEng
657	root	16632	S	HAControl 37039 -1
678	root	0	SW	[scsi_eh_0]
679	root	0	SW	[usb-storage]
709	root	0	DW	[scsi-poller]
880	root	0	SW	[RtmpTimerTask]
881	root	0	SW	[RtmpMlmeTask]
882	root	0	SW	[RtmpCmdQTask]
883	root	0	SW	[RtmpWscTask]
1047	root	1688	S	udhcpc -i ra11n0 -t 5 -T 5 -b
1067	root	3684	S N	/mtd_exe/Comp_LIB/UEP.b
1075	root	10680	S	./MainServer /mtd_rwarea/yahoo
1079	root	10072	S	./PDSServer
1080	root	18656	S	./AppUpdate com.yahoo.connectedtv.up
1112	root	18956	S	./BIServer com.yahoo.connectedtv.sam
1133	root	361m	T	/mtd_down/emp/empWebBrowser/bin/Bro
1368	root	9592	S	Download 42060 -1

[Result of 'ps']

Broken sandbox

- It seems samsung tries to put applications into sandbox
 - They don't want you to do file i/o out of sandbox
 - Example)



Broken sandbox

```
.text:0004BDFC ; jx_GetFullPath(char *, char *)
.text:0004BDFC          EXPORT _Z14jx_GetFullPathPcS_
.text:0004BDFC
.text:0004BDFC var_820      = -0x820
.text:0004BDFC s          = -0x420
.text:0004BDFC ptr        = -0x20
.text:0004BDFC
.text:0004BDFC          STMFD      SP!, {R4-R8,R11,LR}
.text:0004BE00          ADD       R11, SP, #0x18
.text:0004BE04          SUB       SP, SP, #0x800
.text:0004BE08          MOV       R4, #0
.text:0004BE0C          SUB       SP, SP, #0xC
.text:0004BE10          MOV       R5, R0
.text:0004BE14          MOV       R2, #0x400 ; n
.text:0004BE18          MOV       R6, R1
.text:0004BE1C          SUB       R0, R11, #-s ; s
.text:0004BE20          MOV       R1, R4 ; c
.text:0004BE24          STR       R4, [R11,#ptr]
.text:0004BE28          BL        memset
.text:0004BE2C          MOV       R1, R4 ; c
.text:0004BE30          SUB       R0, R11, #-var_820 ; s
.text:0004BE34          MOV       R2, #0x400 ; n
.text:0004BE38          BL        memset
.text:0004BE3C          LDRSB     R3, [R5]
.text:0004BE40          CMP       R3, #0x2F ; /
.text:0004BE44          BEQ       loc_4BEC0
.text:0004BE48          CMP       R3, #0x2E ; .
.text:0004BE4C          BEQ       loc_4BEC8
```

Broken sandbox

```
.text:0004BE50 loc_4BE50 ; CODE XREF: jx_GetFullPath(char *,char *)+D4j
.text:0004BE50 SUB R8, R11, #-ptr
.text:0004BE54 SUB R7, R11, #-s
.text:0004BE58 MOV R1, R6
.text:0004BE5C SUB R4, R11, #-var_820
.text:0004BE60 MOV R0, R8
.text:0004BE64 BL _Z20STR_AllocCopyDefaultPPcPKc
.text:0004BE68 MOV R1, R5
.text:0004BE6C MOV R0, R8
.text:0004BE70 BL _Z19STR_AllocCatDefaultPPcPKc
.text:0004BE74 MOV R1, R7 ; resolved
.text:0004BE78 LDR R0, [R11,#ptr] ; name
.text:0004BE7C BL realpath
.text:0004BE80 MOV R1, R4 ; resolved
.text:0004BE84 MOV R0, R6 ; name
.text:0004BE88 BL realpath
.text:0004BE8C MOV R0, R4 ; s
.text:0004BE90 BL strlen
.text:0004BE94 MOV R1, R7
.text:0004BE98 MOV R2, R0
.text:0004BE9C MOV R0, R4
.text:0004BEA0 BL _Z12STR_NcasecmpPKcS0_i
.text:0004BEA4 CMP R0, #0
.text:0004BEA8 LDR R0, [R11,#ptr] ; ptr
.text:0004BEAC BNE loc_4BEB8
```

Broken sandbox

```
.text:0004BEB0 loc_4BEB0 ; CODE XREF: jx_GetFullPath(char *,char *)+C8j
.text:0004BEB0 ; jx_GetFullPath(char *,char *)+DCj ...
.text:0004BEB0 SUB SP, R11, #0x18
.text:0004BEB4 LDMFD SP!, {R4-R8,R11,PC}
.text:0004BEB8 ; -----
.text:0004BEB8 loc_4BEB8 ; CODE XREF: jx_GetFullPath(char *,char *)+B0j
.text:0004BEB8 CMP R0, #0
.text:0004BEB8 BNE loc_4BEDC
.text:0004BEC0 loc_4BEC0 ; CODE XREF: jx_GetFullPath(char *,char *)+48j
.text:0004BEC0 MOV R0, #0
.text:0004BEC4 B loc_4BEB0
.text:0004BEC8 ; -----
.text:0004BEC8 loc_4BEC8 ; CODE XREF: jx_GetFullPath(char *,char *)+50j
.text:0004BEC8 LDRSB R3, [R5,#1]
.text:0004BECC CMP R3, #0x2E
.text:0004BED0 BNE loc_4BE50
.text:0004BED4 MOV R0, #0
.text:0004BED8 B loc_4BEB0
.text:0004BEDC ; -----
.text:0004BEDC loc_4BEDC ; CODE XREF: jx_GetFullPath(char *,char *)+C0j
.text:0004BEDC BL free
.text:0004BEE0 MOV R0, #0
.text:0004BEE4 B loc_4BEB0
```

Broken sandbox

- Pseudo code)

```
- openCommonFile() calls jx_GetFullPath()

jx_GetFullPath(filepath, stricted_directory) {
    ...
    if not filepath starts with stricted_directory:
        exit
    ...
}
```

- Stricted_directory example) “/mtd_down/common”
- Looks no problem in the function
 - Prevent from directory traversal (Notorious “../”)
- But..

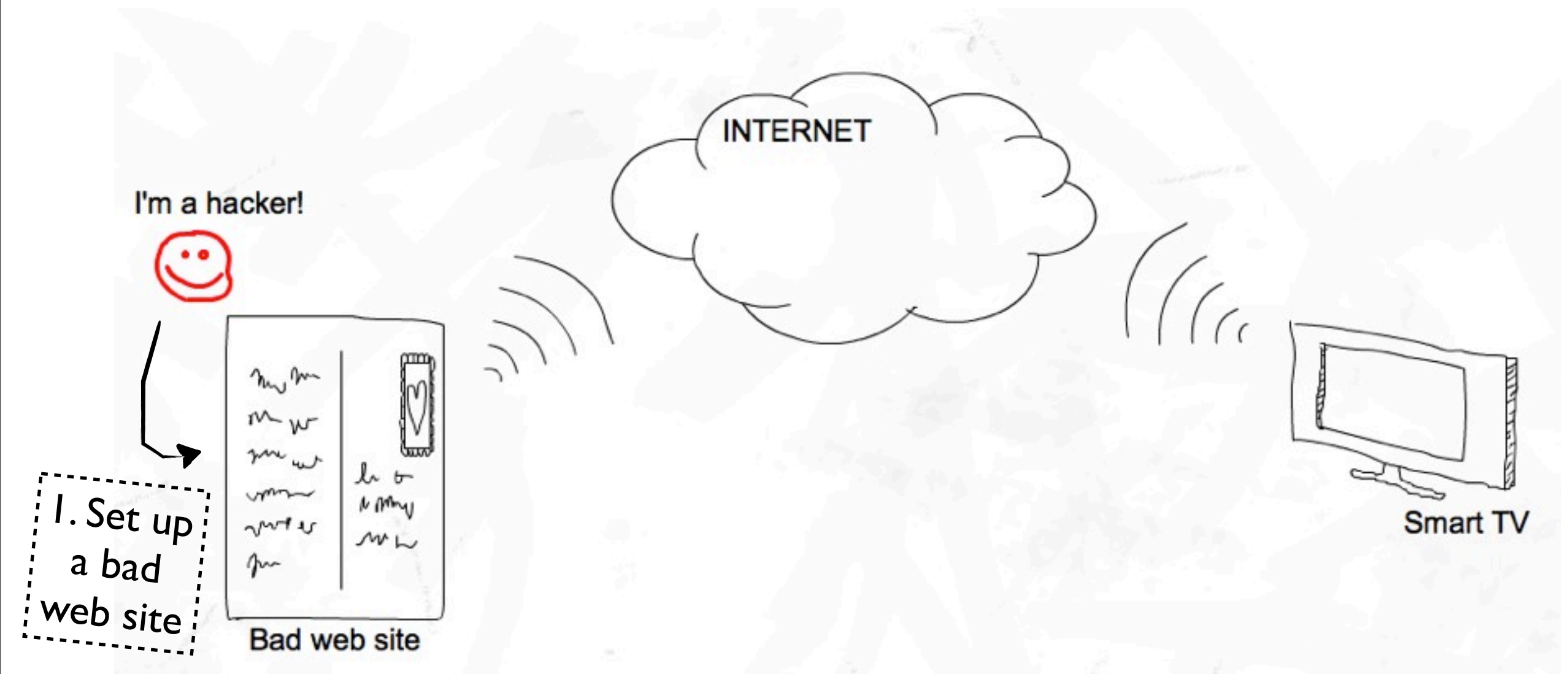
Broken sandbox

- But Samsung Smart TV sandbox for File I/O is totally broken
- There are a lot of ways to access files out of sandbox
 - Bypassing!
- We'll show some cases of arbitrary directory listing, file copy/write/read/delete

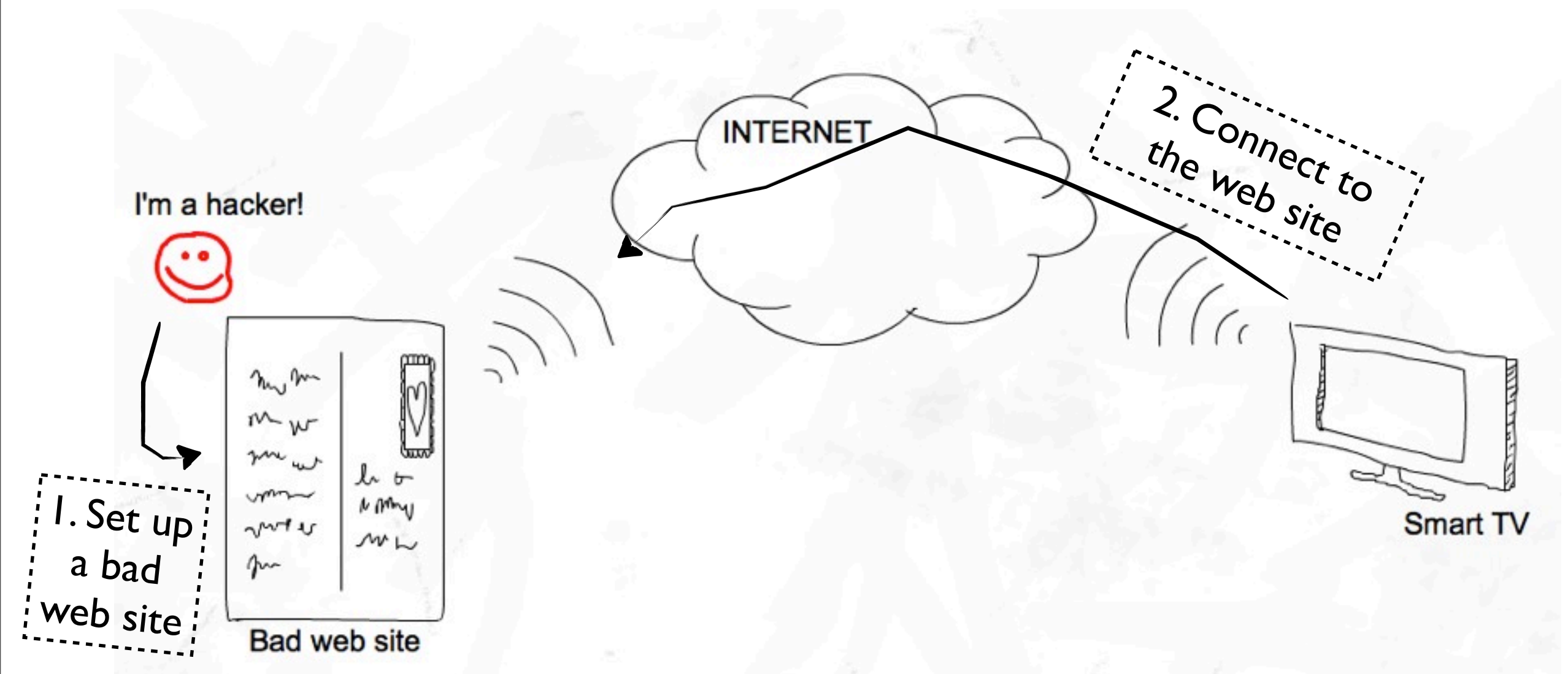
File I/O API

- Samsung provides a set of File I/O APIs
- You can use those APIs in your javascript/flash application
- Reference
 - <http://www.samsungdforum.com/Guide/ref00001/index.html>

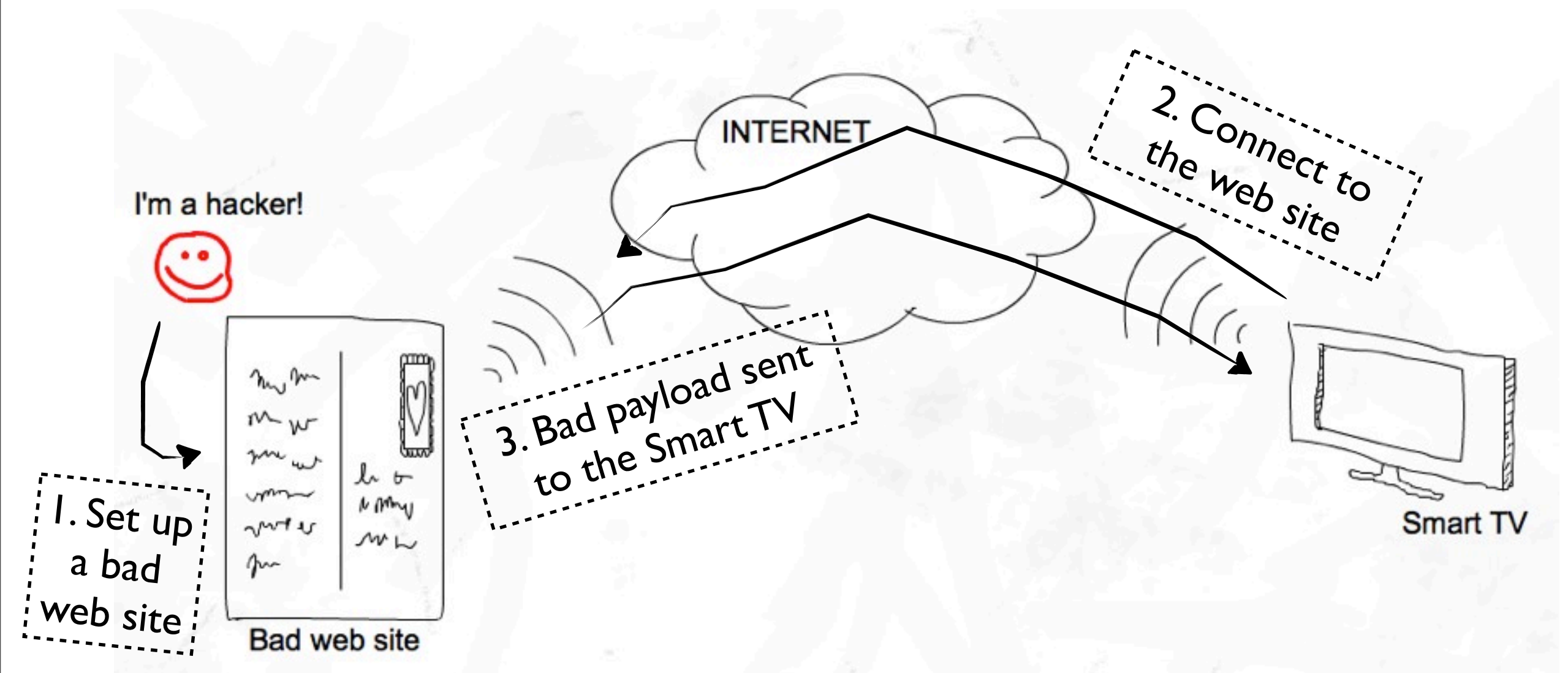
Network attack vectors



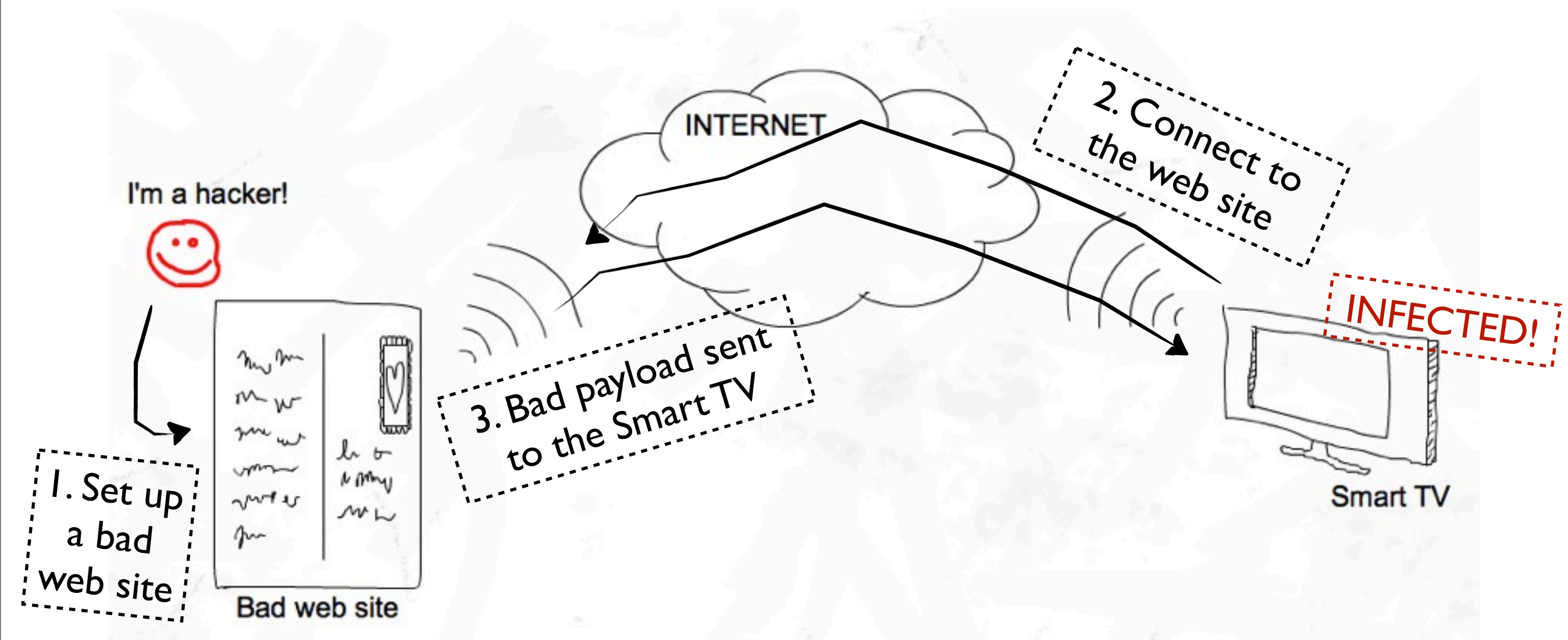
Network attack vectors



Network attack vectors



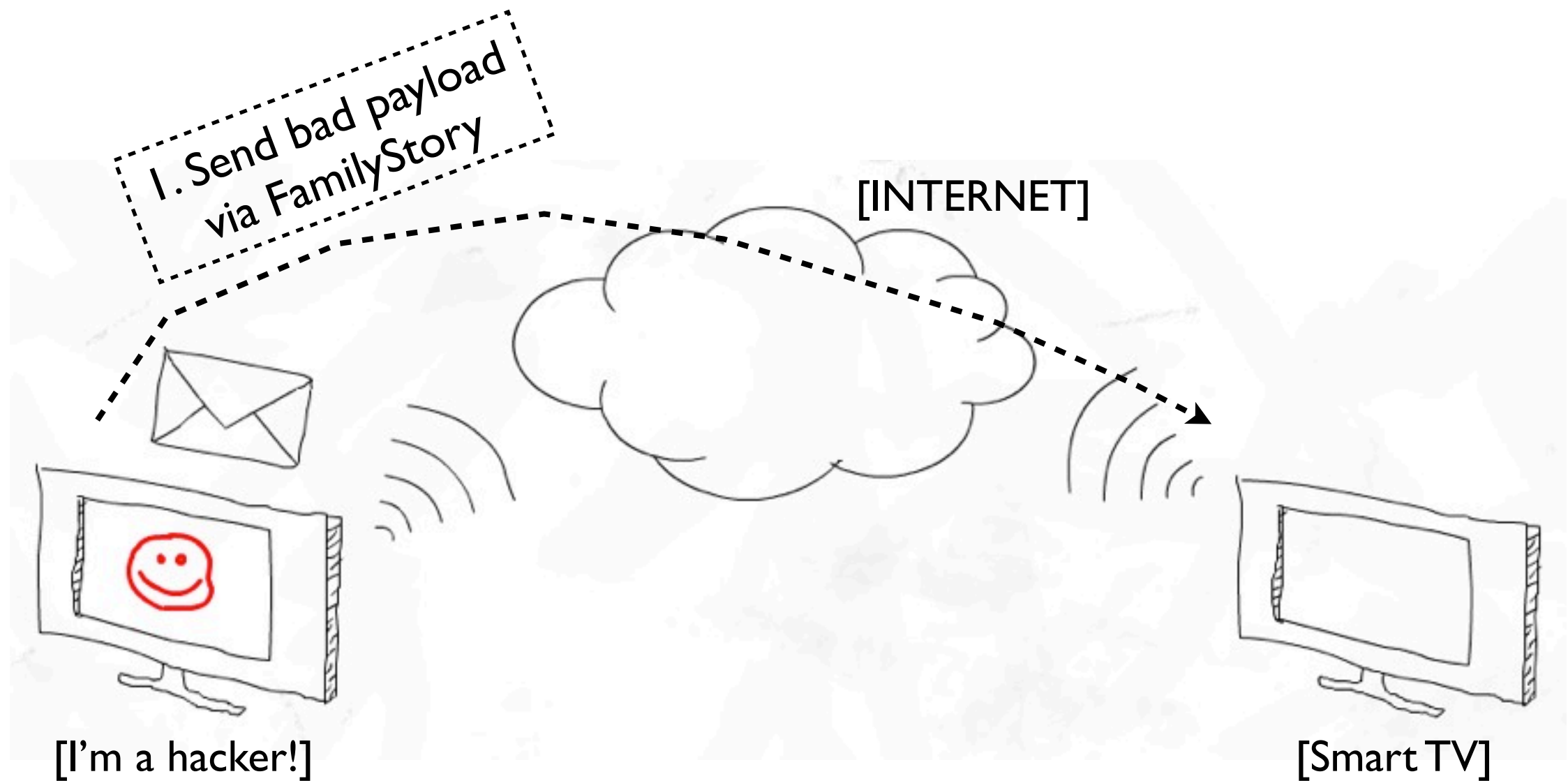
Network attack vectors



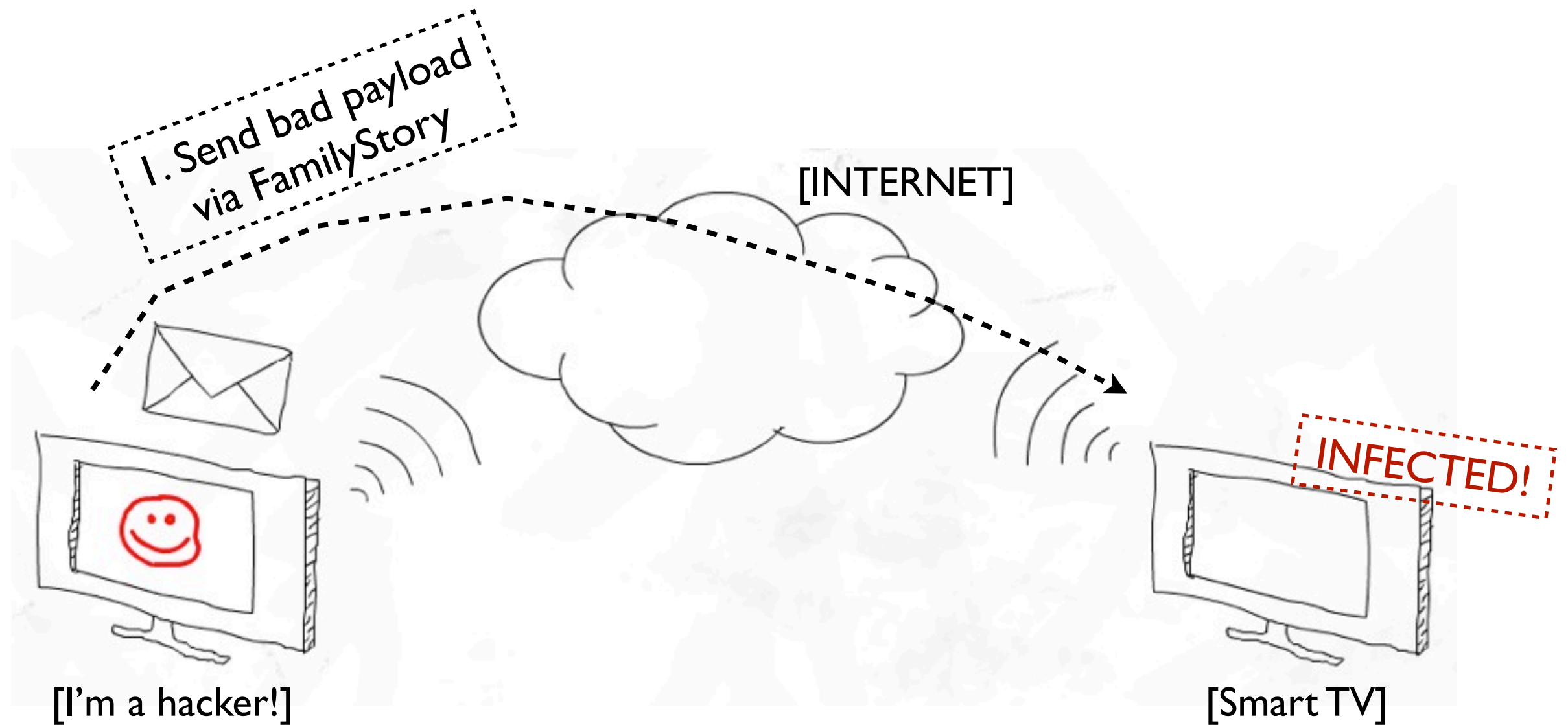
Network attack vectors

- Web browser
 - Samsung has its own built-in web browser
 - User agent string is
 - Mozilla/5.0 (SmartHub; SMART-TV; U; Linux/SmartTV; Maple2012) AppleWebKit/534.7 (KHTML, like Gecko) SmartTV Safari/534.7
 - You see “Webkit”
 - There are a ton of bugs in old version webkit
 - And having the latest version webkit is hard

Network attack vectors



Network attack vectors



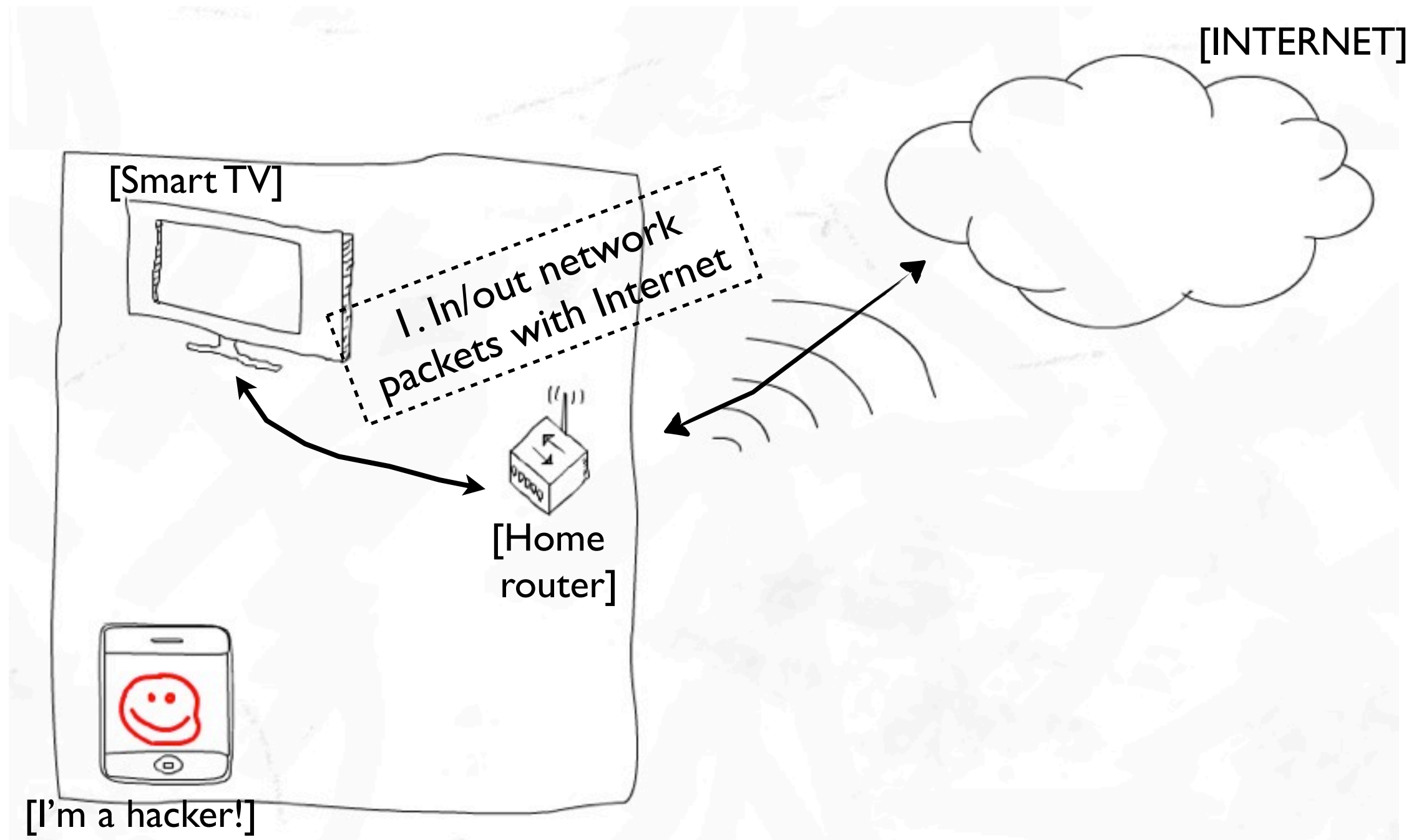
Network attack vectors

- Family story
 - Samsung makes a social network app called Family story
 - You create a group and invite people
 - Then, you can share posts/photos/videos

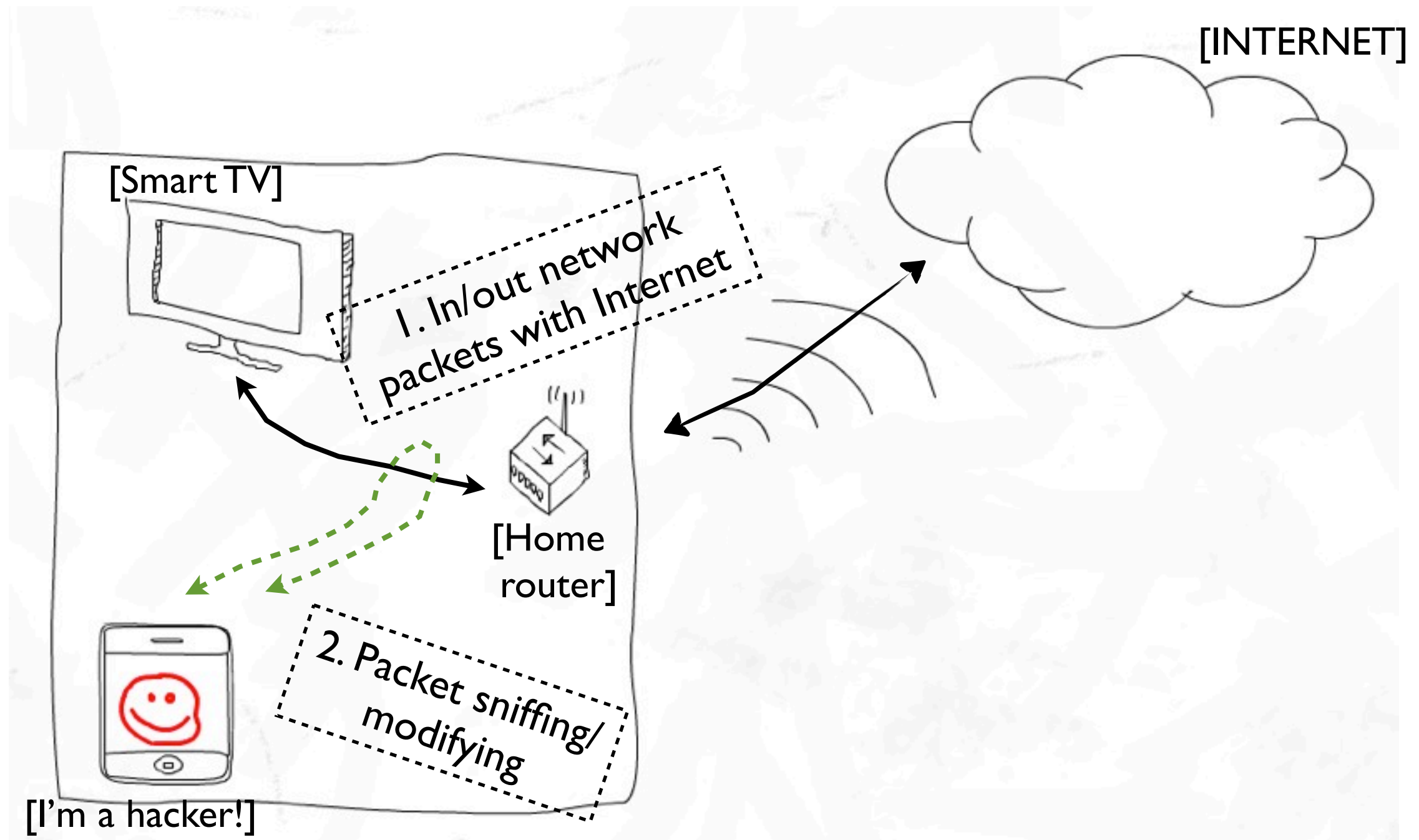
Network attack vectors

- Remote help service
 - Samsung Smart TV helps you for troubleshooting
 - You make a call to the company's service team
 - And you go to a menu "remote control service"
 - At the moment, you get a PIN code
 - You tell the team the PIN code
 - Then the team now controls your Smart TV remotely

Network attack vectors



Network attack vectors



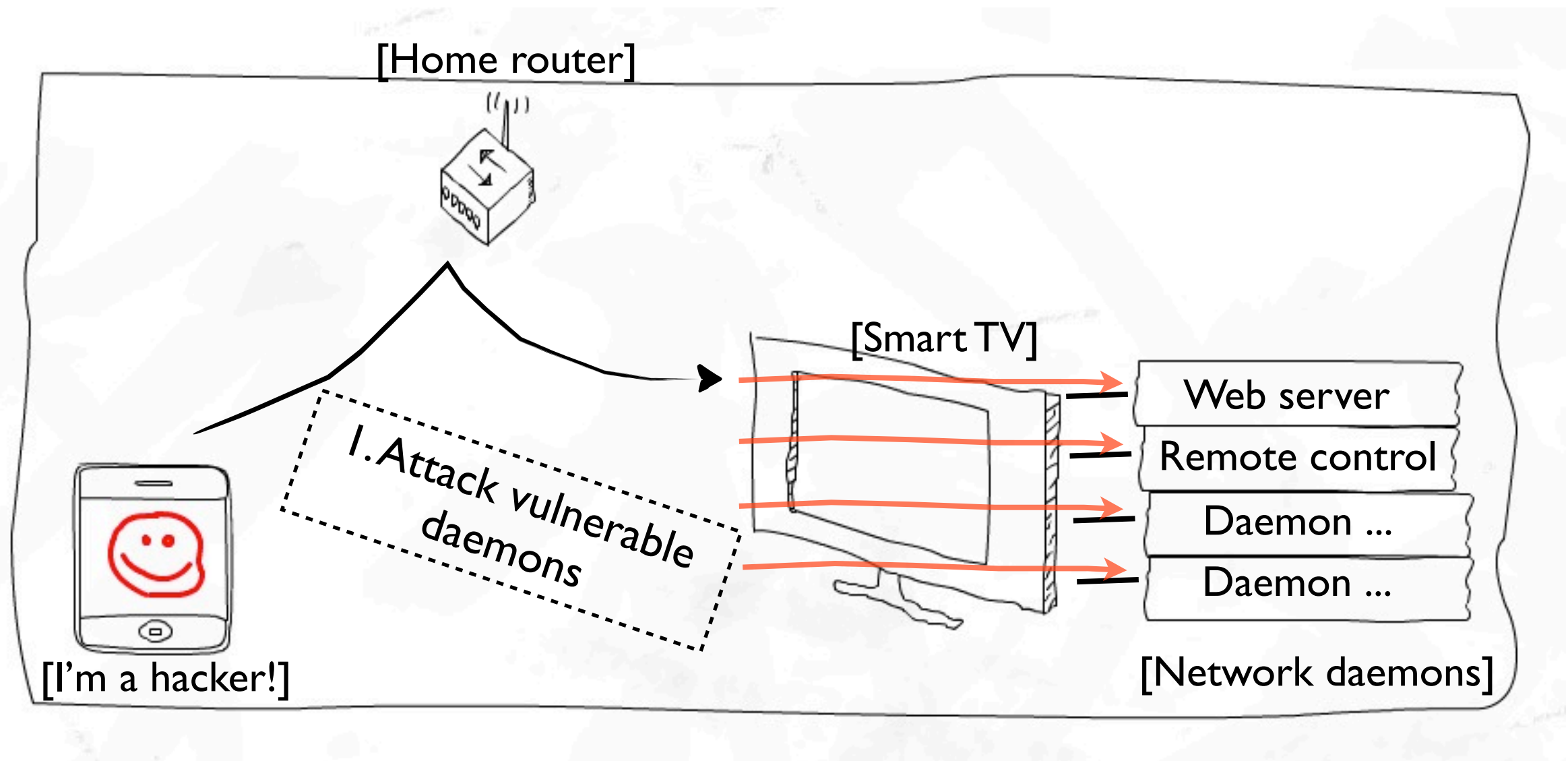
Network attack vectors

- Man in The Middle (For Pwning)
 - As all apps are running as 'root' privilege, MiTM is a very good attack surface for hackers
 - If there is any single app vulnerable to MiTM, hackers can compromise the whole Smart TV
 - There are many default installed apps on Smart TV
 - Attack methods
 - Upgrade hijack, memory corruption while protocol, etc

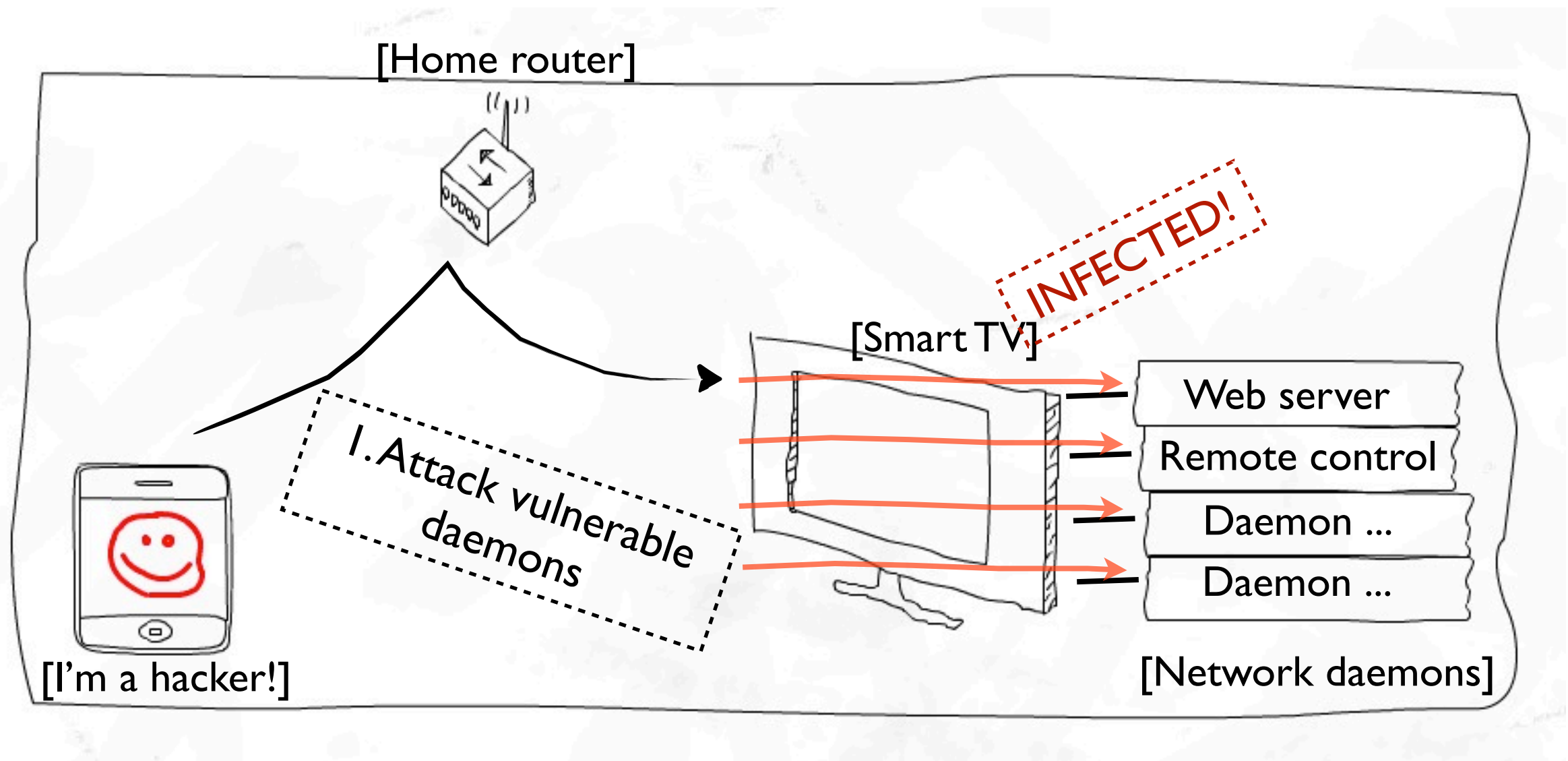
Network attack vectors

- Man in The Middle (For Sniffing)
 - Sensitive information
 - Login credential
- AllShare
 - AllShare is for sharing music/photo/video wirelessly
 - The protocol is basically DLNA
 - You can share media data with Smart TV using your smartphone/camera

Network attack vectors



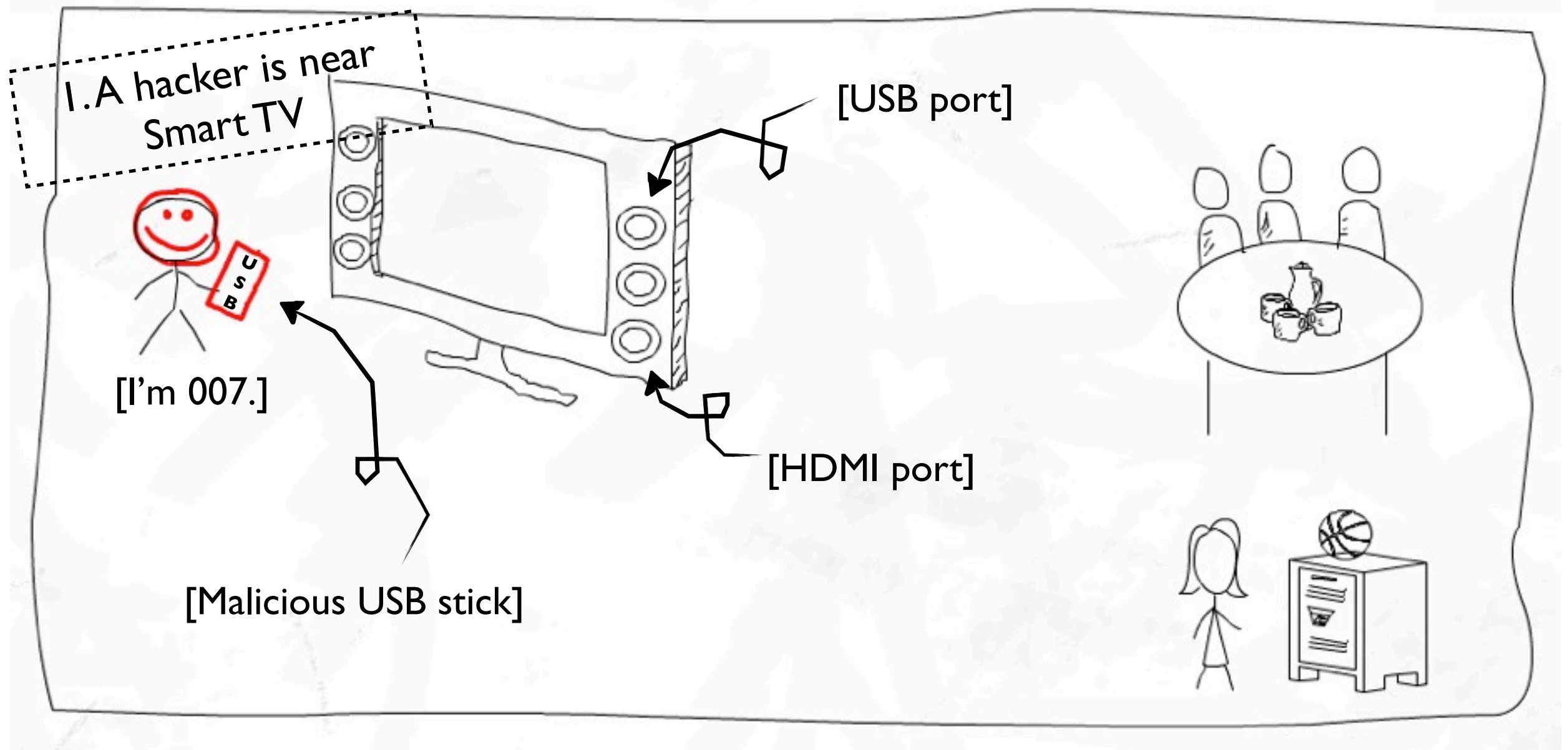
Network attack vectors



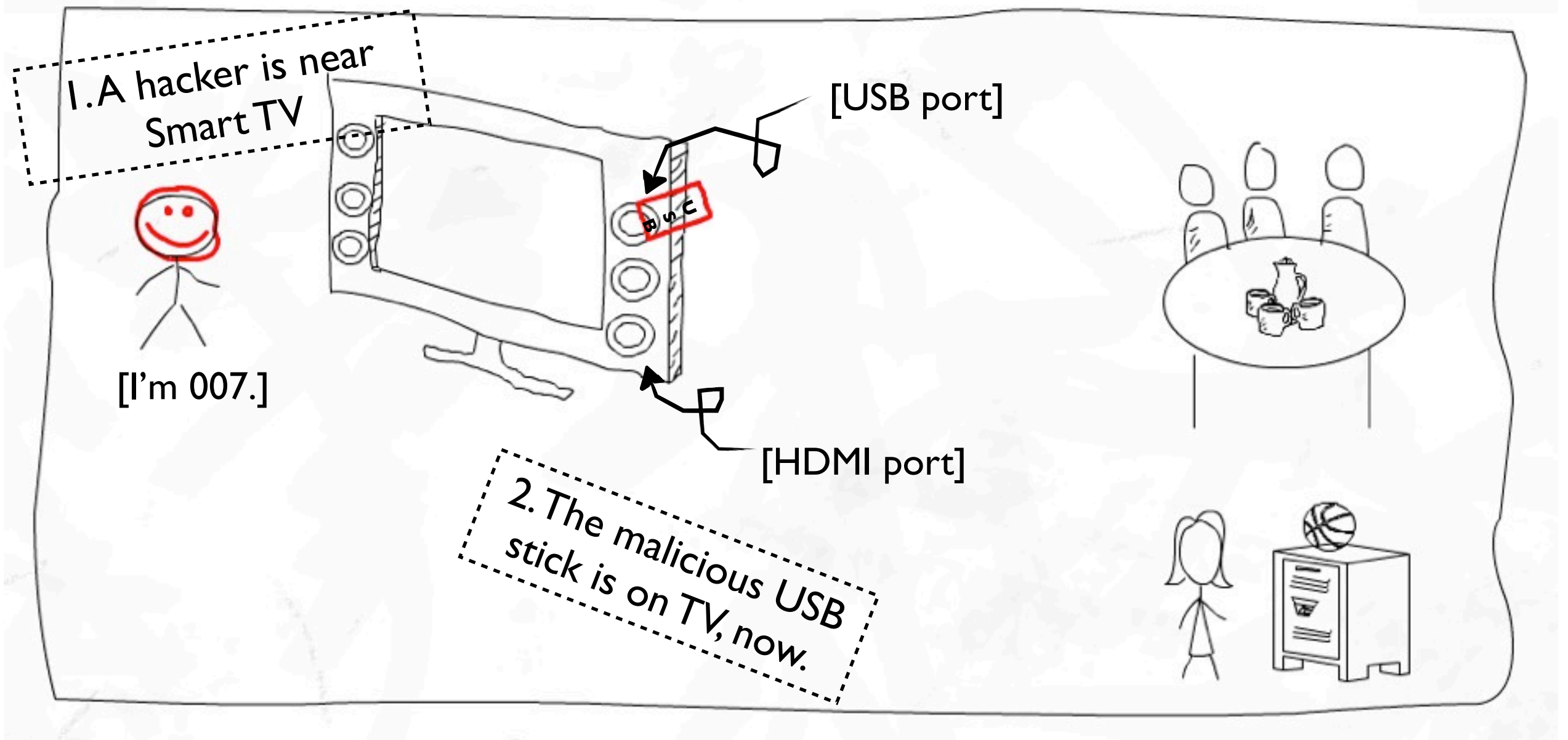
Network attack vectors

- Network daemons
 - Web server
 - For convergence between devices and TV
 - The other network based daemons
 - There are over 10 TCP and UDP based daemons
- Network device drivers
 - Also, network device drivers are also targets
 - WIFI, Bluetooth drivers

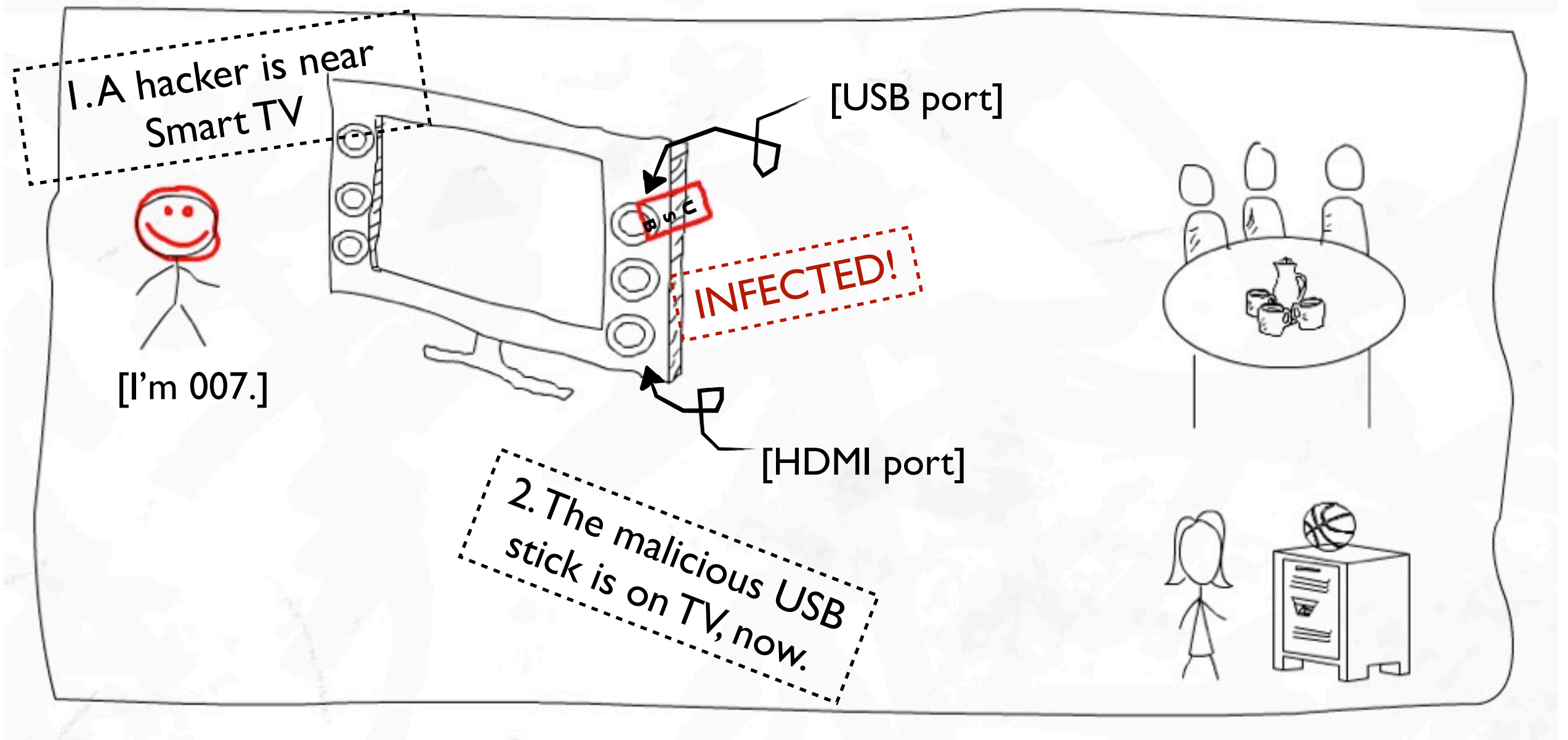
Physical attack vectors



Physical attack vectors



Physical attack vectors



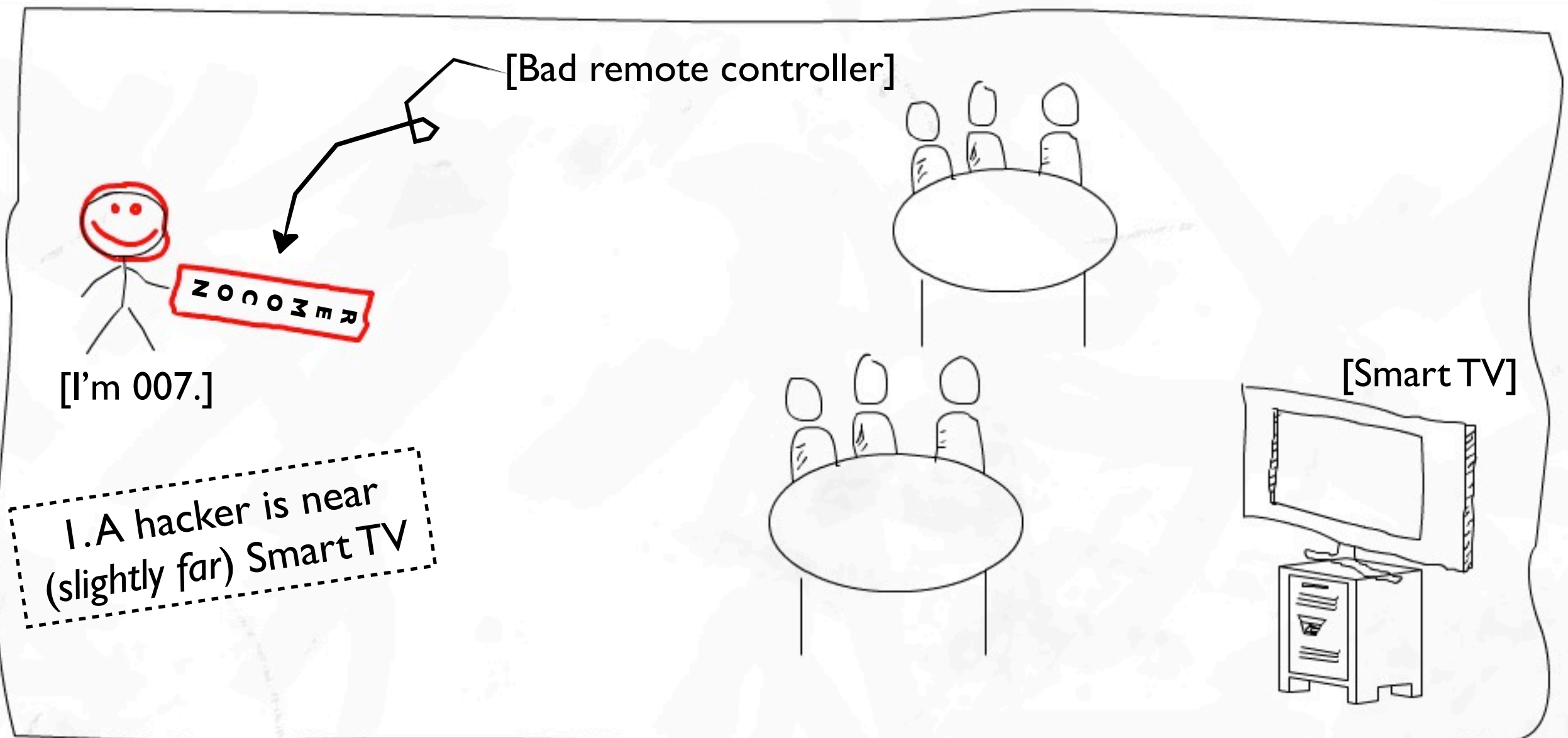
Physical attack vectors

- Parsing USB
 - You can input USB sticks into Smart TV
 - Then Smart TV automatically recognizes your USB
 - USB information, filesystem and etc
 - When parsing, it is the spot to look for vulnerabilities

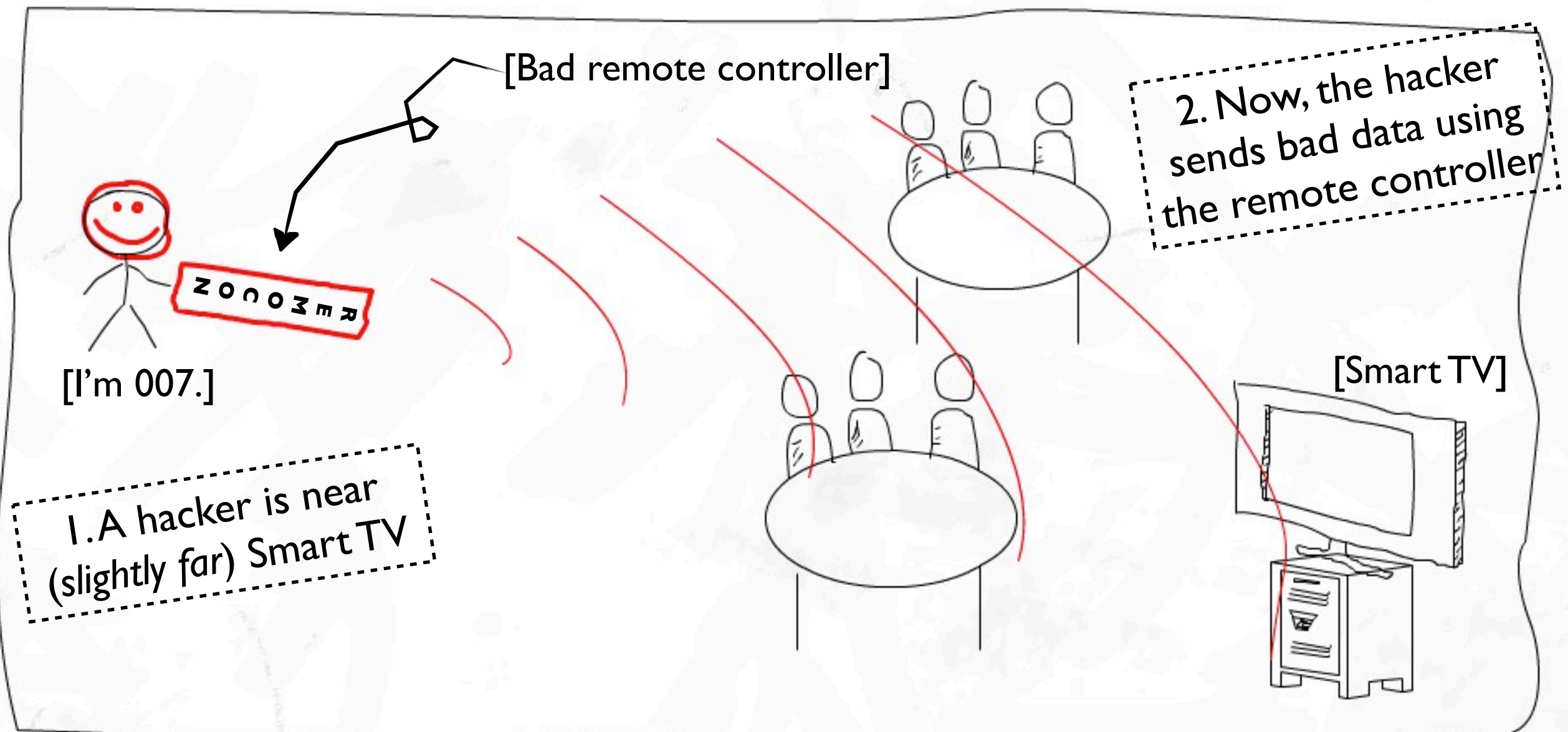
Physical attack vectors

- Upgrade firmware by USB
 - You input USB stick within firmware into TV
 - And by remote controller, you can get into the menu
 - “Upgrade firmware by USB”
 - It needs a legal firmware image
 - Which means we have to find a RSA private key and AES key

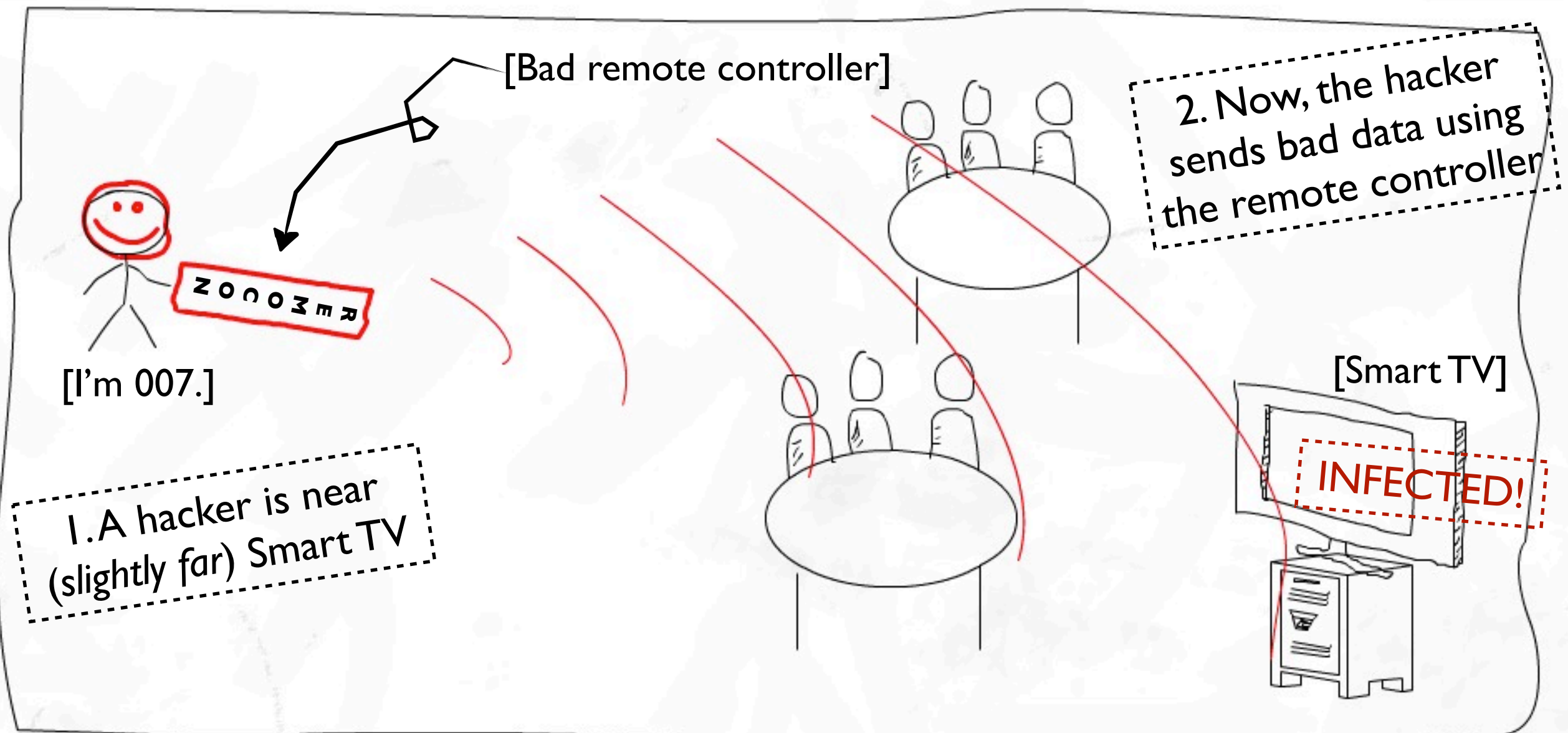
Physical attack vectors



Physical attack vectors



Physical attack vectors



Physical attack vectors

- Parsing data from remote controller
 - Default remote controller is IrDA
 - Possible to code execution if there are parsing bugs
- Reference
 - http://www.samsung.com/global/business/semiconductor/file/product/S3F80KB_RemoteController_AN_REV000_090108-0.pdf

Physical attack vectors

- More input devices
 - 3 USB ports, 1 digital voice output port
 - 3 HDMI ports (MHL, ARC, DVI), 1 DVI voice input port
 - 2 external input ports (video/voice)
 - 1 voice output port
 - 1 EX-LINK port, 1 antenna input, LAN port
 - And etc

Broadcast attack vectors

- Broadcast signal
 - Samsung provides “firmware upgrade” by Broadcast signal
 - If you can have a legal firmware and transmit it to Smart TV widely, you hack a lot of people
 - *But we’ve not figured anything how this mechanism works yet*

DRM contents

- DRM
 - As Samsung Smart TV has a lot of *smart* features, of course there are many multimedia vendors on Smart TV
 - The problem is TV companies have to make their Smart TV platforms strong against DRM hacking
 - Because copyright companies would not give their contents to weak platforms
 - Example) Warner Brothers Pictures Inc.
 - I heard they ask Smart TV vendors to have TPM

DRM contents

- Programmers who don't know security are there always
 - TPM itself is a very nice and strong solution
 - If there is a well-written TPM based DRM program, it would be very hard to break
 - But what if programmers who don't know security make programs poorly written?
 - Poorly written TPM client side programs probably will be good targets for at least 1 ~ 2 years
 - And probably attacking TPM client side programs will be a night-mare for Smart TV vendors

Default installed apps minor issues

- There are default installed apps in Smart TV
 - TVing, facebook, family store, etc
- Packet sniffing issue
 - It's not that common that embedded software use SSL
- Insecure storage information
 - Facebook API key is hardcoded (*but how important is this?*)
 - ID and Password credential

Default installed apps minor issues

```
-rwxr-xr-x    1 root    0  
emps/empHAControl/client.pem
```

1745 Jul 8 2011

```
cat emps/empHAControl/client.pem  
-----BEGIN RSA PRIVATE KEY-----  
Proc-Type: 4,ENCRYPTED  
DEK-Info: DES-EDE3-CBC,6D3B09E4CA5421FF
```

- Insecure storage information

- There are private key files in the TV

- *Not sure what they're used for yet*

- Example)

```
SaDJA2MhJ12ZmDxfGkSLhQgjYPEQYqVfs5b4DZTz+9pJqzuNxHrZZU43oArbWBdB  
3DKc1THEjbyHF2lY7xgPLk/5iax5r+CXesDKZroSLiHyERBIOCUgDN6ecwvVGtYv  
C8IhlwGPEXyxr59lyV37RjkSUVXYBqiRbLlNlCQtp5T6GkFe+yftOnv6/UADCLTS  
Pu8xwkda1rf7dgPwYIKuk2SOTTe1VMDtWacRUGu8NteTJ4aiVaeo9wdsKId5U2b  
Z7NTJj0jvdX0LRonfkGvDXmrmN4eICks0bV0ZBtkULAfGjKNGs6riY+XNGKNRmjI  
idRRB0za+EGorpiJ/vbe7n7uaFXIJlFqCwhTi4Up3mS8sR4tLHfmdjp85GV9P9B3  
xX3CHIEG5/EYDt0Qn1gRL50DL/007nFGJslhcQUS6bMmcg9nSzhClTE2gREz0j9g  
pwzvRpEkIl3Tw4niZLIX8fW2cEIyKTBMCCG2MDwHHgXRL3SUXk0GeitFefkcXN/z  
/UWRS8XQcX7/lGWCiuEpgn+esoirjf8lFNVsx60T0UXj3oBxGrz1iB/vpu/PMBVQ  
JsbEPSh/ElHSDUItw2ytjJmkoLRtM01b7cFj16ZxbHjinXWTIGZFWUYIlaeA2zHK  
D/NRMFJwjrQYhjRgPqltvbw7M01Co7SNFBwSotARr36FBjsxb0H3F1jY6w+kXvJU  
X5m83C9UONM2K7kkKYXbE2yW+kzJF2LFX0Uu4yDluxNG767/WwqiQSI63aIzNAPp  
rSsaIMBSbVZia8q49gcvGyuvqBZpwm/PcZwr/PHJjvGs8hdU1ACmyQ==  
-----END RSA PRIVATE KEY-----  
-----BEGIN CERTIFICATE-----  
MIICFTCCAX4CAgECMA0GCSqGSIb3DQEBAUAMFcxCzAJBgNVBAYTA1VTMRMwEQYD  
VQQKEwpSVEZNLCBJbmMuMRkwFwYDVQQLExBXaWRnZXZlZXRpdmlzaW9uMRgwFgYD  
VQQDEw9UZXRN0IENBMjAwMTA1MTcwHhcNMDEwNTE3MTYxMTM2WhcNMDEwNTE3MTYx  
MTM2WjBOMQswCQYDVQQGEwJVUzETMBEGA1UEChMKU1RGTSwgSW5jLjEjE2MBcGA1UE  
CxMQV2lkZ2V0cyBEaXZpc2lvdjEPMAMGA1UEAxMGY2xpZW50MIGfMA0GCSqGSIb3  
DQEBAQUAA4GNADCBiQKBgQCHNWS0Nh6msUwYGGd7TYQDsdSG0ao6QXaYjk+78ZyM  
QeZUBu2dZFjG4wnzkKwrD4rp/J5PLR9AdxR72lb9AavE0KL2UDHJGssCZkGVw/bz  
ZbxrKF2rvdpZSvKP10hV1M0ds/WTpRm1gcmVSoV5vLOMqVjzjHoxQ/+1zpjzMxWL  
0wIDAQABMA0GCSqGSIb3DQEBAUAA4GBACTJhRR5tv8A7dc5+zmKR1Q/i8qE3Mrn  
mp/MOXHfX+ifJ/w+twoc/yd4En+7pr+hGsiTofct1JOZDW9Akq/ZGu1+NpVRT7Cw  
53EdMwpi7ArwZAsLIUBsKA7QmLTbdwjU5S7WlZ24eygZHyqZrK4Few+JuzlFkkoI  
FIDCfinyz24m  
-----END CERTIFICATE-----
```

Open source license issue

- Still many vendors don't understand open source license
 - Or just ignore
- If you use open source and don't follow the license, you may get sued
 - Then, this is a disaster
- It seems Samsung cares a lot to avoid having problem of it
- But Samsung codebase is huge
 - Possible to find spots they don't follow the rule
 - And this might be a disaster

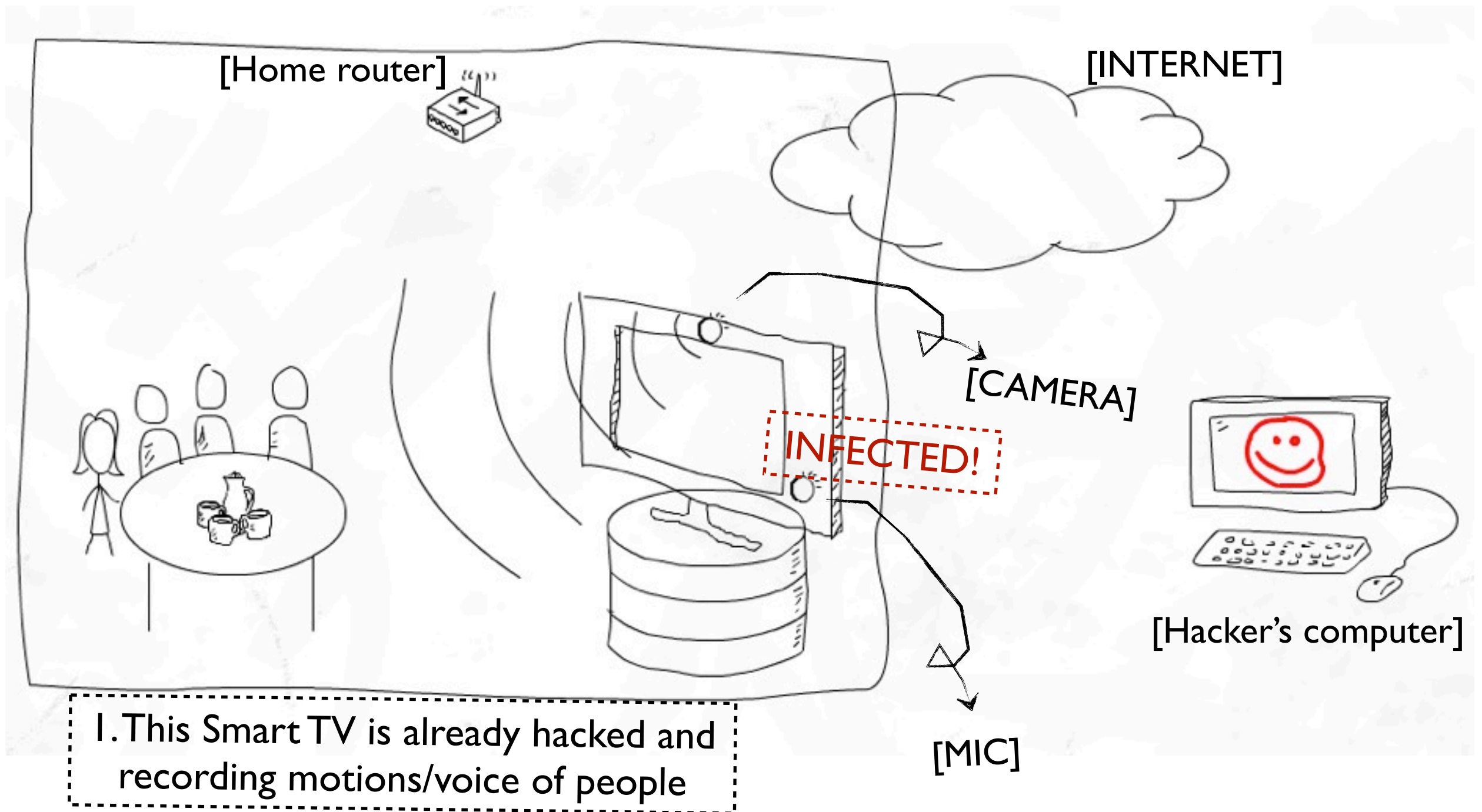
Open source license issue

- We found many open source that Samsung Smart TV is using
 - Modified device drivers
 - Open source library
 - But obviously, code of Smart TV is not open
- We're checking if they legally use the open source

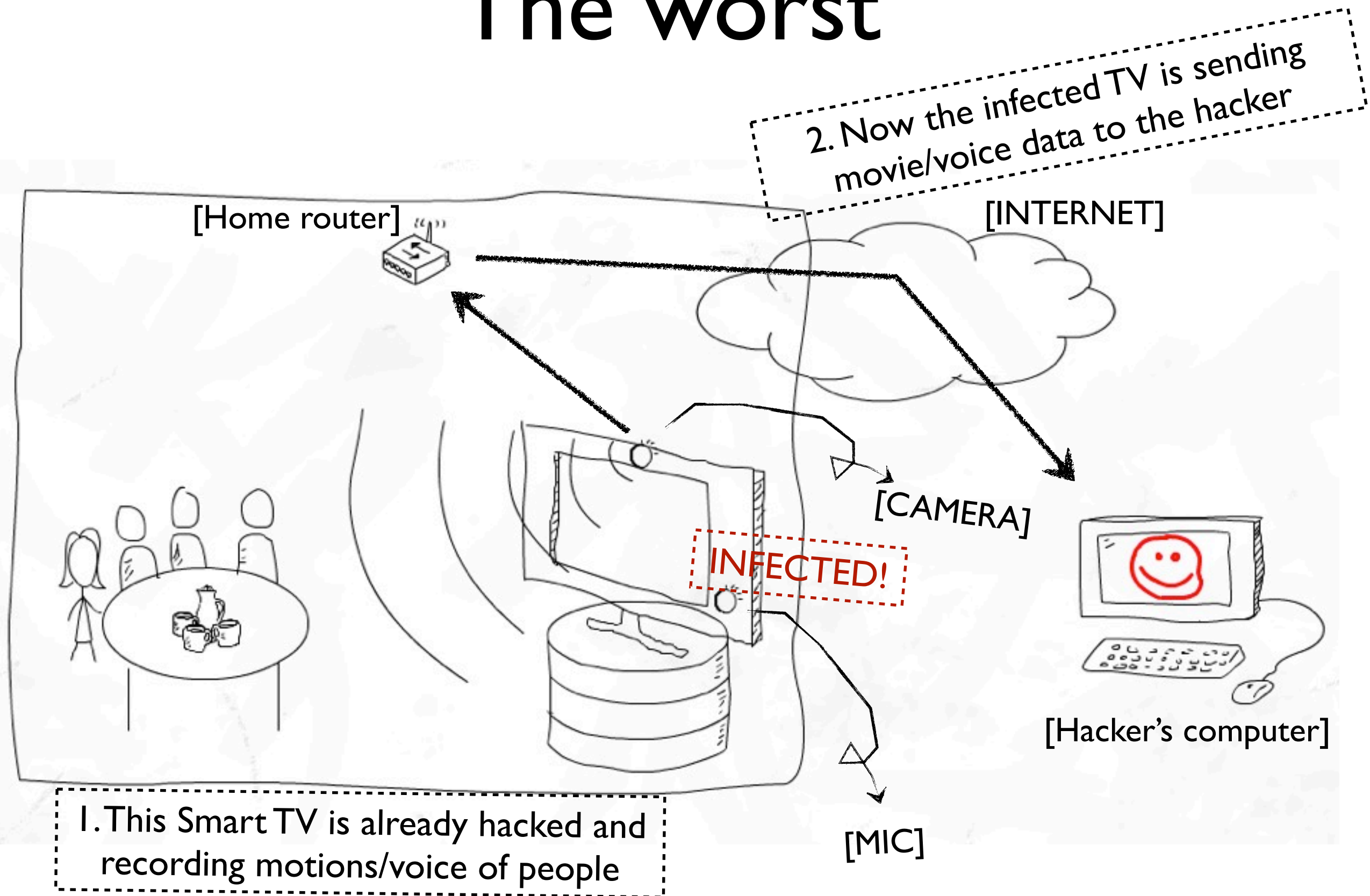
The worst

- What is the worst case if Smart TV got hacked?
 - Stolen financial information could be
 - But most of people would say
 - *A video which has my naked body*
 - Sound so scary?
- Recording camera and voice and sending to a hacker's server might be good demo

The worst



The worst



Conclusion

- Smart TV industry will be getting more popular
- But, the security mechanism for Smart TV is very weak
 - No mitigation or protection like sandbox
 - Even no separated privileges
 - It doesn't make the best use of the linux's mitigations

Conclusion

- Soon or later, some hackers will come to Smart TV hacks
- 24 hour surveillance is definitely scary
- There should be more researches and efforts to make Smart TV products secure
- Last, some companies don't allow employees to use their own smartphone at work
- Then, need to think about if having Smart TV at work would be risky or not

Q&A

- Thanks!
- A lot of nice comments from
 - Mongii (hackerschool)
 - Tora (Google security team)
 - Donato (<http://revuln.com>)
- Greetz to CIST IAS LAB, Korea University.