HOW HACKERS ARE OUTSMARTING SMART TV'S AND WHY IT MATTERS TO YOU

Raimund Genes
Trend Micro

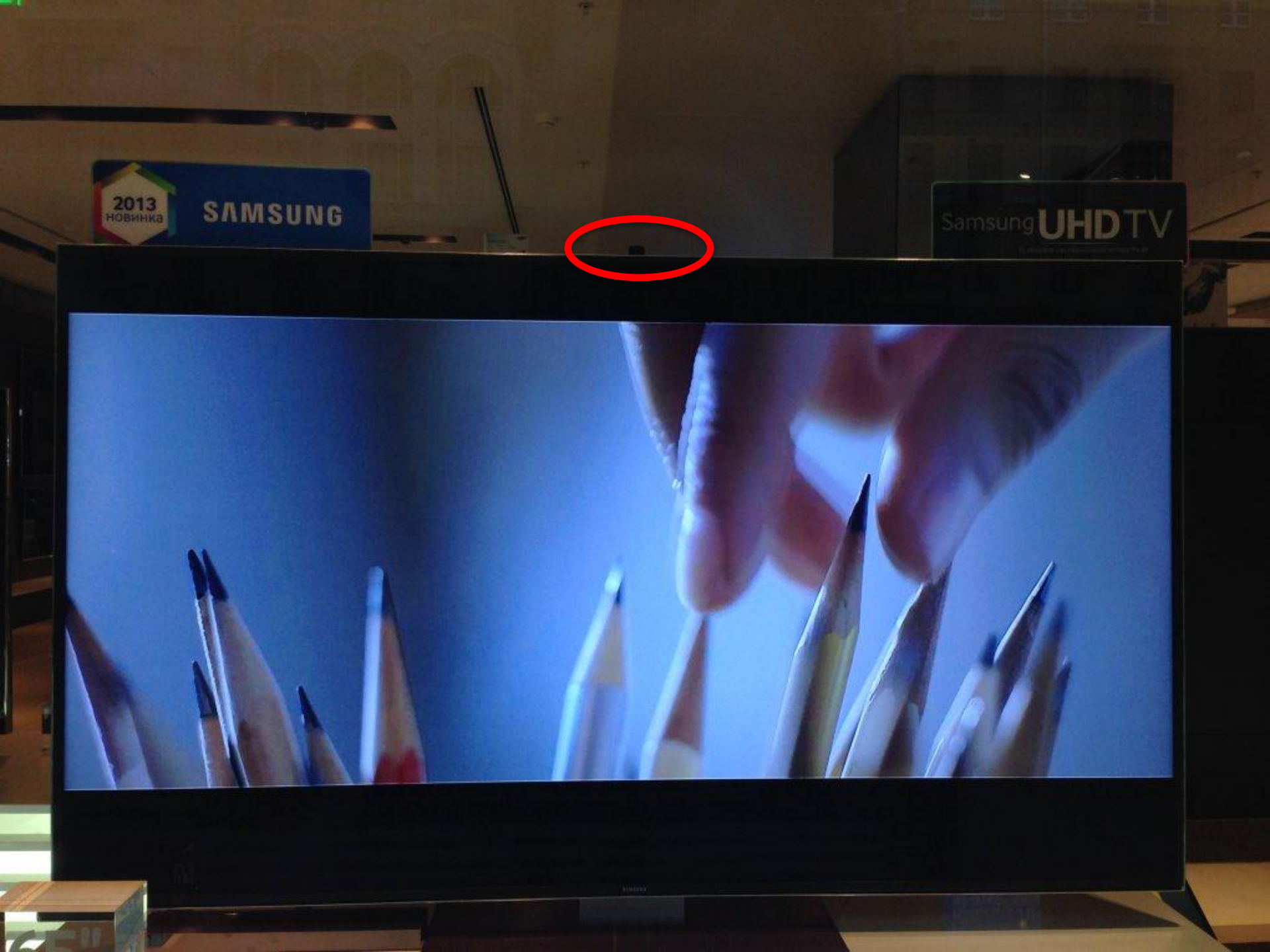
RSA CONFERENCE EUROPE 2013

Session ID: HT-R08

Session Classification: Intermediate


Trend Micro Lösungen im Überblick

Hardware!


2013
НОВИНКА
SAMSUNG
Samsung UHD TV

Smart TV

- Class of devices that is “either a *television set* with integrated Internet capabilities or a *set-top box* for television that offers more advanced computing ability and connectivity than a contemporary basic television set”

  » wikipedia

- “Smart TV” is not a trademark or a brand

Smart TV Shipments and Q1 2013 Market share

	Global TV Shipments	Global Smart TV shipments	Smart TV market share
2011	254.6 million	52 million	20%
2012	238.5 million	66 million	27%
2015	253.1 million	141 million	55%

Samsung	26%
LG	16%
Sony	11%

- Source: http://www.twice.com/articletype/news/ihs-smart-tvs-rise-27-tv-shipments/105108
- Source: http://finance.yahoo.com/news/strategy-analytics-samsung-leads-26-152500460.html

Samsung Smart TVs: The next frontier for data theft and hacking [video]

By Raymond Wong on Dec 14, 2012 at 12:40 PM

TV

12:40 PM Smart TVs, particularly Samsung's (005930) last few generations of flat screens, can be hacked to give attackers remote access according to a security startup called ReVuln. The company says it discovered a "zero-day exploit" that hackers could potentially use to perform malicious activities that range from stealing accounts linked through apps to using built-in webcams and microphones to spy on unsuspecting couch potatoes. Don't panic just yet, though. In order for the exploit to be activated, a hacker needs to plug a USB drive loaded with malicious software into the actual TV to bypass the Linux-based OS/firmware on Samsung's Smart TVs. But, if a hacker were to pull that off, every piece of data stored on a Smart TV could theoretically be retrieved.

Source: http://bgr.com/2012/12/14/samsung-smart-tv-hack-security-exploit-discovered/

From Blackhat 2013:

HACKING, SURVEILLING, AND DECEIVING VICTIMS ON SMART TV

PRESENTED BY

SeungJin 'Beist' Lee

Smart TVs sold over 80,000,000 units around the world in 2012. This next generation "smart" platform is becoming more and more popular. On the other hand, we hardly see security research on Smart TVs. This presentation will cover vulnerabilities we've found on the platform.

You can imagine that Smart TVs have almost the exact same attack vectors that PC and Smart Phones have. Also, Smart TVs have interesting new attack surface such as the remote controller. We'll talk about attack points for Smart TV platform and cover security bugs we discovered. This talk will mostly focus on what attackers can do on a hacked Smart TV.

For example, expensive Smart TVs have many hardware devices like a Camera or Mic which, if remotely controlled, means bad guys can spy remotely without you knowing. Even more, it is possible to make Smart TVs monitor you 24/7 even though users turn off their TV, meaning #1984 could be done.

In addition, we'll point out a difference of viewpoint on leaked information type among PC, Smart Phone and Smart TV. Lastly, we'll give demo of live remote surveillance cam, which is sent to attacker's server at this talk.

This talk is an extended version of one, which I gave at CANSECWEST. It will demonstrate a spoofed news story on a hacked Smart TV and possibly TVshing (Smart TV edition of phishing.)

THE OUTER LIMITS: HACKING THE SAMSUNG SMART TV

PRESENTED BY

Aaron Grattafiori

Josh Yavor

There is nothing wrong with your television set. Do not attempt to adjust the picture. We are controlling the transmission.

"Smart" TVs are becoming more and more common. Samsung and other vendors such as Sony and LG have sold more than a hundred million Smart TVs in the last few years. During this talk, Aaron Grattafiori and Josh Yavor will discuss the Samsung SmartTV design, attack surfaces and overall insecurity of the platform. A short discussion of the current application stack, TV operating system and other details will be provided to help set the stage for details of significant flaws found within the Samsung SmartTV application architecture, APIs and current applications.

A number of vulnerabilities will be explored and demonstrated which allow malicious developers or remotely hijacked applications (such as the web browser or social media applications) to take complete control of the TV, steal accounts stored within it and install a userland rootkit. Exploitation of these vulnerabilities also provides the ability for an attacker to use the front–facing video camera or built–in microphone for spying and surveillance as well as facilitate access to local network for continued exploitation. This talk will also discuss methods to bypass what (meager) security protections exist and put forth several worst case scenarios (TV worm anyone?).

Concluding this talk, Aaron and Josh will discuss what has been fixed by Samsung and discuss what overall weaknesses should be avoided by future "Smart" platforms. Video demos of exploits and userland rootkits will be provided.

Task for Trend Micro researchers:

- Is it really a risk for our corporate customers?
- Is it a risk for consumers?
- Could malware be installed on Smart TV's?
- How to protect these devices?

Openlgtv

openlgtv.org.ru/wiki/index.php/Main_Page

create account | Log in

page | discussion | view source | history

Main Page

navigation
- Main page
- Wiki index
- Forum
- Recent changes

search

Search

Go | Search

toolbox
- What links here
- Related changes
- Special pages
- Printable version
- Permanent link
- Page information

+1 1

There are security restrictions on this page

Welcome to OpenLGTV Project

OpenLGTV is a non-commercial project for legal reverse engineering and research on LG Television firmware which is partially Open Source. We make these modifications for ourselves but you are welcome to join us.

Friends, if you have an additional information that is missing on the site, please spend a few minutes and contribute. Sign up and accelerate our research!

- Wiki

You can find many interesting articles there.

- Forum

Discuss any issues related to LG tv's.

- SVN

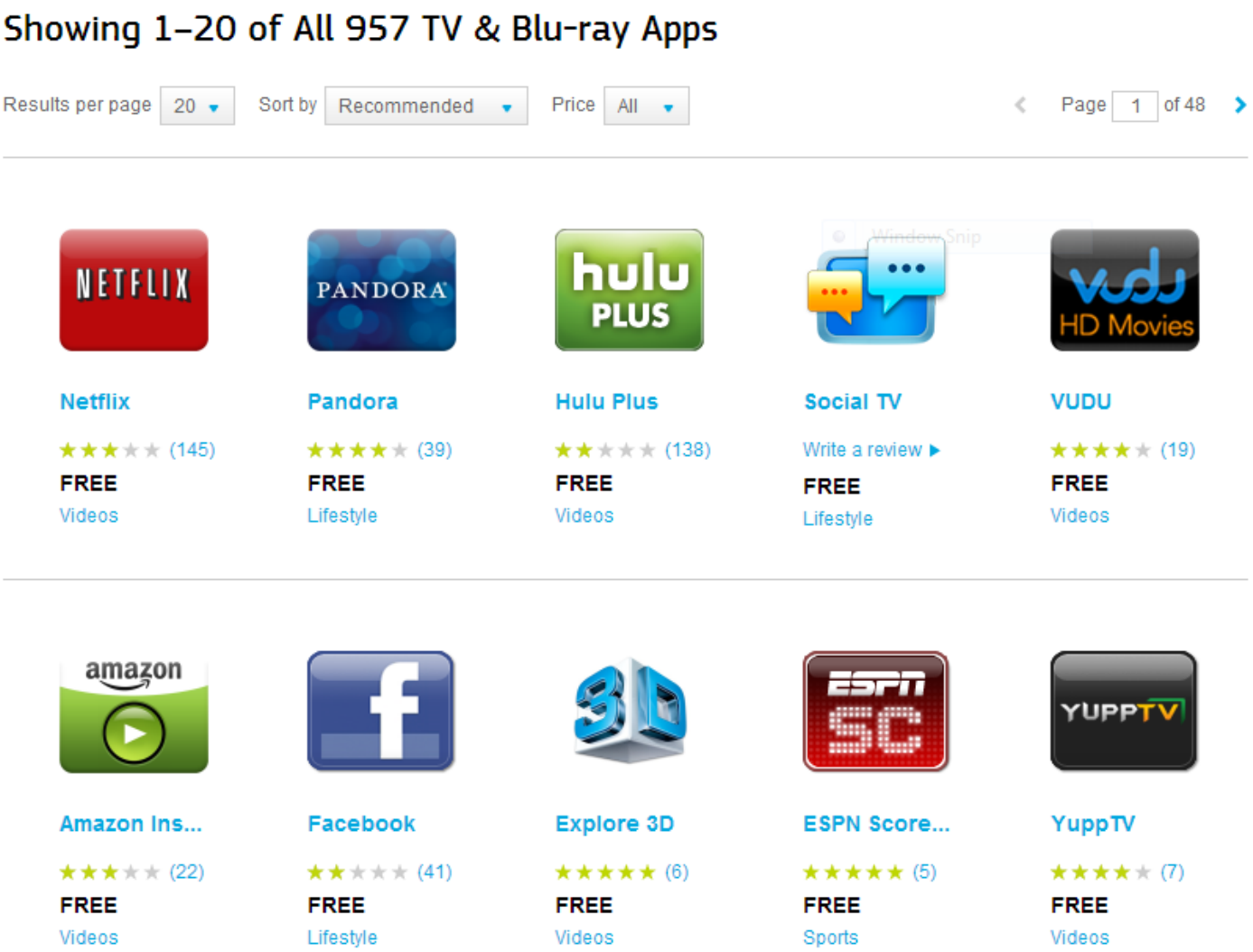
Web access to the SVN repository (svn.openlgtv.org.ru). WebSVN is temporarily unavailable.

- Chat

@ irc.freenode.net).

openlgtv.org.ru/wiki/index.php/Main_Page

Focus on Samsung



Apps

- 957 Apps. Free - 9.99 USD
- Purchased via credit card or “App cash”
- App cash works like a gift card, and refilled via credit card

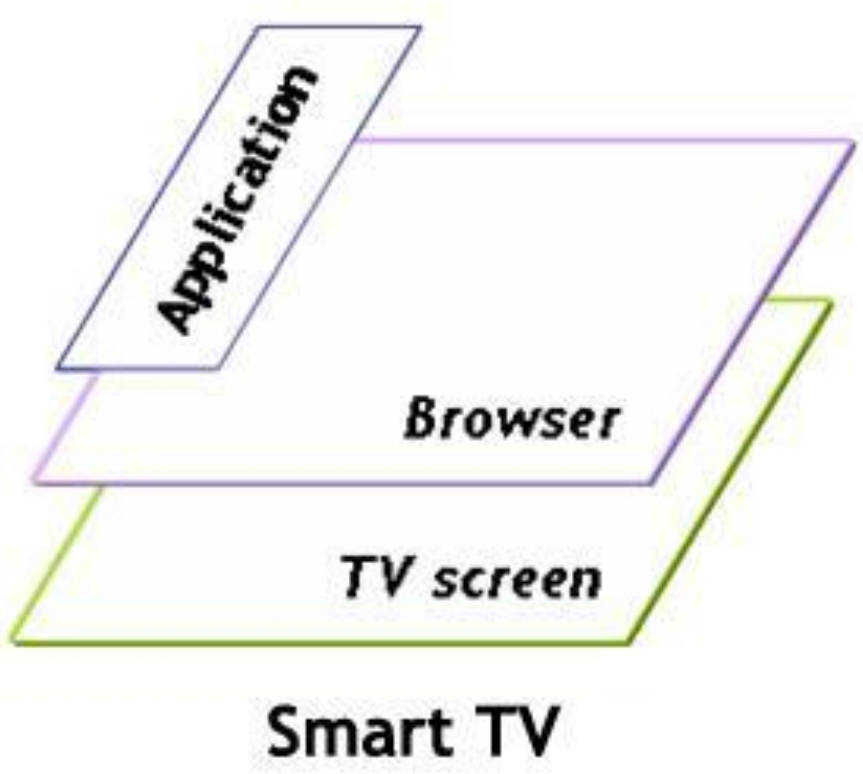
Samsung Account

- Account needed to purchase apps
- Account is protected by a 4-digit password

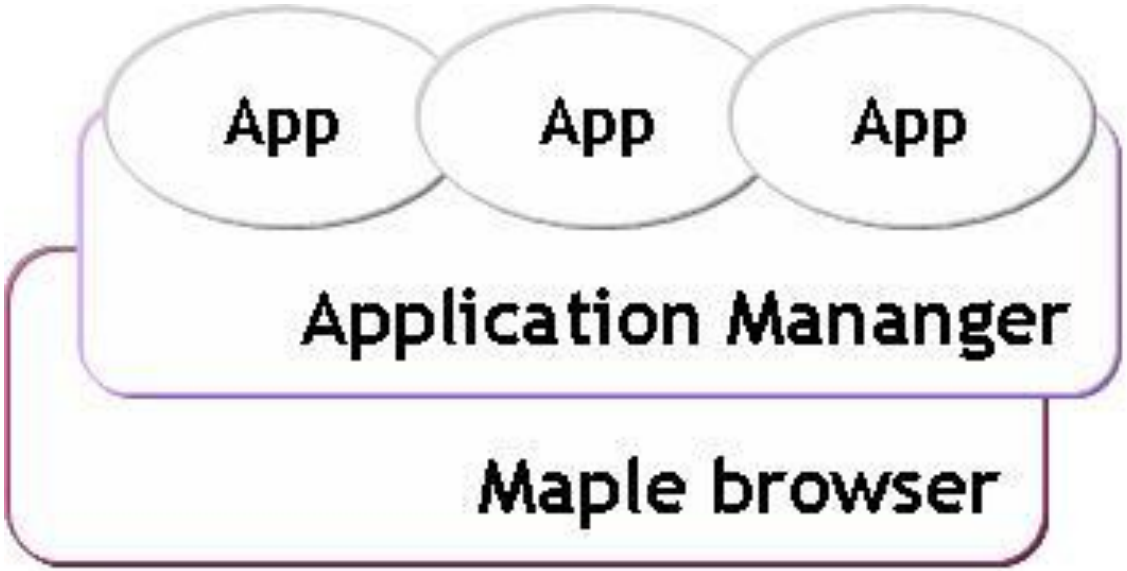
In order to purchase an app […], it needs to be activated from your account. From the Samsung Apps menu on your TV, select an app you want to purchase, and click “Buy now”. When the app window prompts you for your login password, **enter the 4-digit password and click “Ok” to access your account and App Cash**. Your new App Cash balance will appear on the screen and you’ll be prompted to click “Download now” to finish the transaction.

» http://www.samsung.com/us/appstore/faq.do#faqAnswer_5

Understanding the architecture



What about the Browser?



Browser Details

- Maple
  - MArkup engine Platform for Embedded Systems
- Based on Webkit

Mozilla/5.0 (SmartHub; SMART-TV; U; Linux/SmartTV+2013; Maple2012) AppleWebKit/535.20+ (KHTML, like Gecko) SmartTV Safari/535.20+

Browser Details

- HTML 5
- DOM 3
- CSS 3
- SquirrelFish (Javascript engine)

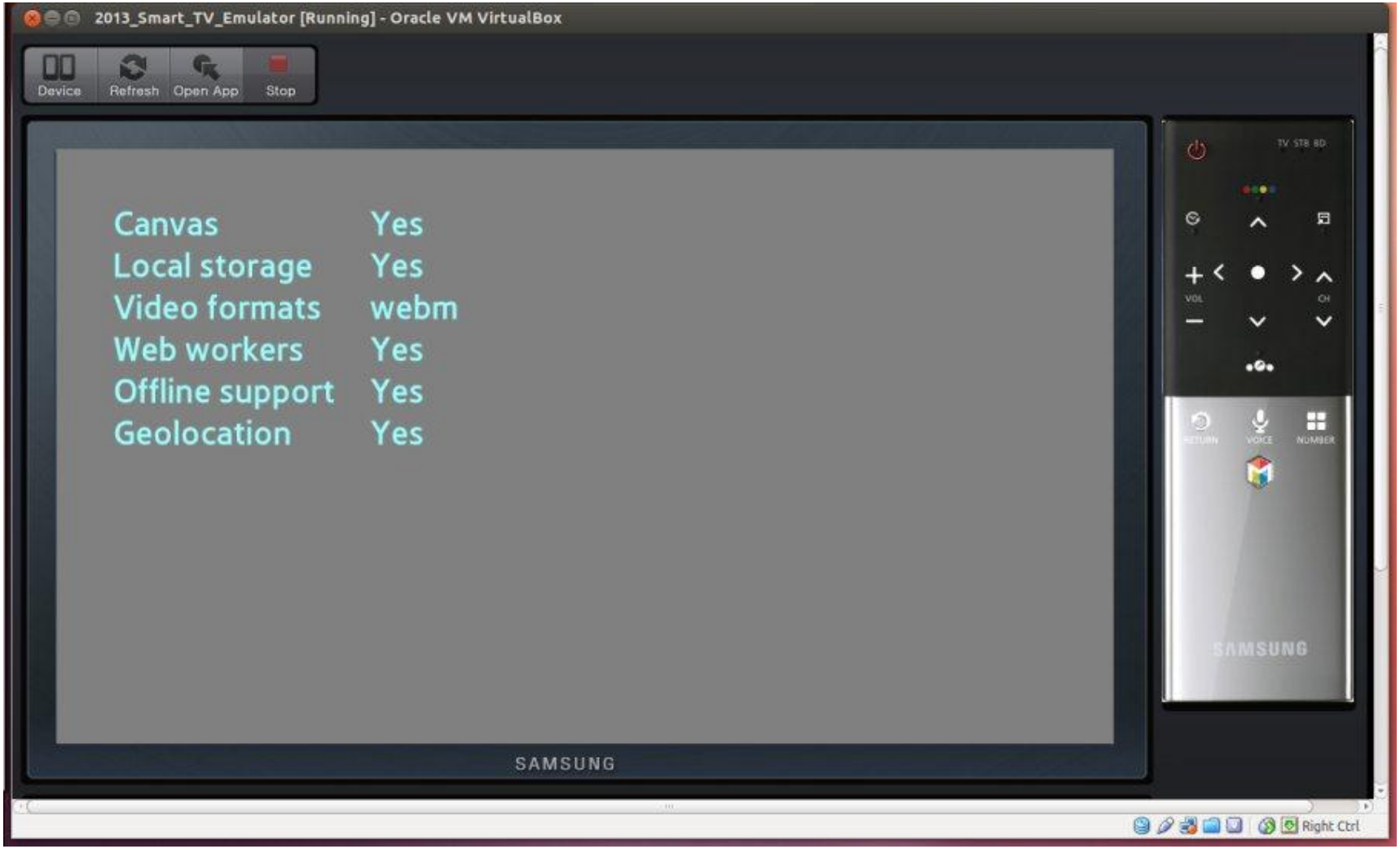
Browser Plugins

- ActionScript 3.0
- AIR for TV 2.5.1
- 2012 TVs: Flash 10.1
- 2013 TVs: Flash 11.1

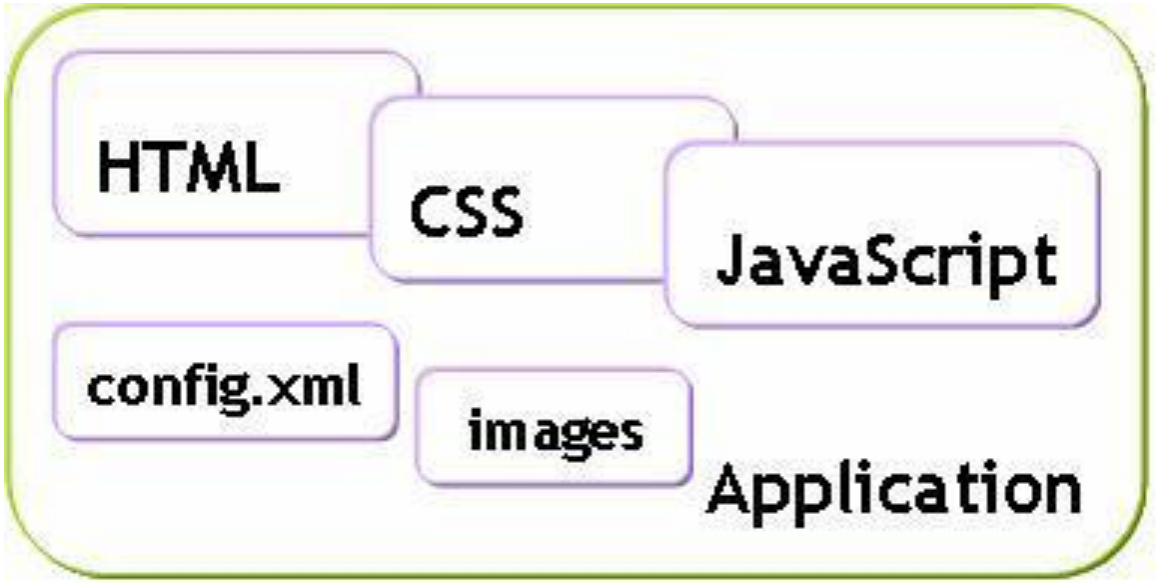
BTW, most recent Flash versions

Windows:	11.5
Mac:	11.5
Linux:	11.2

HTML 5


2013_Smart_TV_Emulator [Running] - Oracle VM VirtualBox
Device
Refresh
Open App
Stop
Canvas Yes
Local storage Yes
Video formats webm
Web workers Yes
Offline support Yes
Geolocation Yes
SAMSUNG
SAMSUNG
Right Ctrl

Application structure



App Summary

- Apps are run on top of browser
- Apps are managed by an “Application Manager”
- Apps are basically HTML5 web apps

Firmware

- Named as “InfoLink”
- On Samsung TVs since 2009 (?)
- Based on several open source projects, notably Linux

Open Source

- Samsung Open Source Release Center
  - http://opensource.samsung.com/
- Latest available source code are for Series 8 LEDs
  - (Latest models are Series 9)

Versions

- Linux 2.6.35.11
- gcc 4.2.0
- glibc-2.11-2010q1 : The GNU C Library
- binutils-2010q1
- busybox-1.18.1 : BusyBox
- xfsprogs-3.1.5 : XFS file system utilities
- iptables : iptables-1.4.10
- webkit-gtk.20120109 : WebKit

Other Software

- wireless_tools.29 : Wireless Tools (iwconfig, iwlist, etc)
- BROADCOM-bthid : Broadcom Bluetooth HID drivers (keyboards, mice, game controllers)
- BROADCOM-btusb : Broadcom Bluetooth USB drivers (keyboards, mice, game controllers)
- RALINK_RTNET5572STA_V_2_5_0_1 : Ralink RTnet RT5572 (Wifi USB dongle drivers)
- RALINK_RTUTIL5572STA_V_2_5_0_1 : Ralink RTnet RT5572 (Wifi USB dongle utilities)
- gnutls-2.6.4 : GNU Transport Layer Security Library (SSL, TLS and DTLS protocols)
- libtasn1-2.5 : The ASN.1 library used by GnuTLS
- libgcrypt-1.4.5 : general purpose crypto library
- libgpg-error-1.7 : defines common error values for all GnuPG components
- Cairo : A 2D graphics library (X Window, quartz, win32, PDF, PS, SVG file output)
- Gtk
- ffmpeg : record, convert and stream audio and video
- libgphoto2(libptp) : allow access to digital camera by external programs
- libusb 1.0 : access to USB devices
- libmms_0.6.2 : A library for parsing mms:// and mmsh:// type network streams
- libthai-0.1.6 : Thai language support
- libiconv-1.9.1 : Text encoding conversion library
- SDL-1.2.11 : Simple DirectMedia Layer (a multimedia library written in C)
- Pango : layout and rendering of multi-language text
- ATK : Accessibility Toolkit
- glibmm : A C++ interface for Glib
- alsa-lib : 1.0.23 : Advanced Linux Sound Architecture (audio and MIDI)
- libsoup.20120109 : An HTTP client/server library for GNOME

Hardware

- “Dual-core processor”
- Text seen from build instructions for ES8xxxx firmware:

This product has an MIPS processor;
the software is normally cross-compiled for that processor.
All of those softwares have to be built with the MontaVista
ARM toolchain gcc version 4.2.0 (SELP-ARM 4.3.1.30 4.2.0-16.0.58.custom.custom 2009-11-17(13:58))

Security by design

- Browser/App Engine runs as an unprivileged user
- No fine grained security models

Mod your TV scene not very active

- SamyGo
  - http://www.samygo.tv/
  - Firmware hacking
    - Rooting your TV
    - Getting console access
    - Custom firmware
    - High possibility of bricking your (expensive) TV
- Not a lot of modding communities, unlike Android (TVs are expensive)

Possible attack scenarios

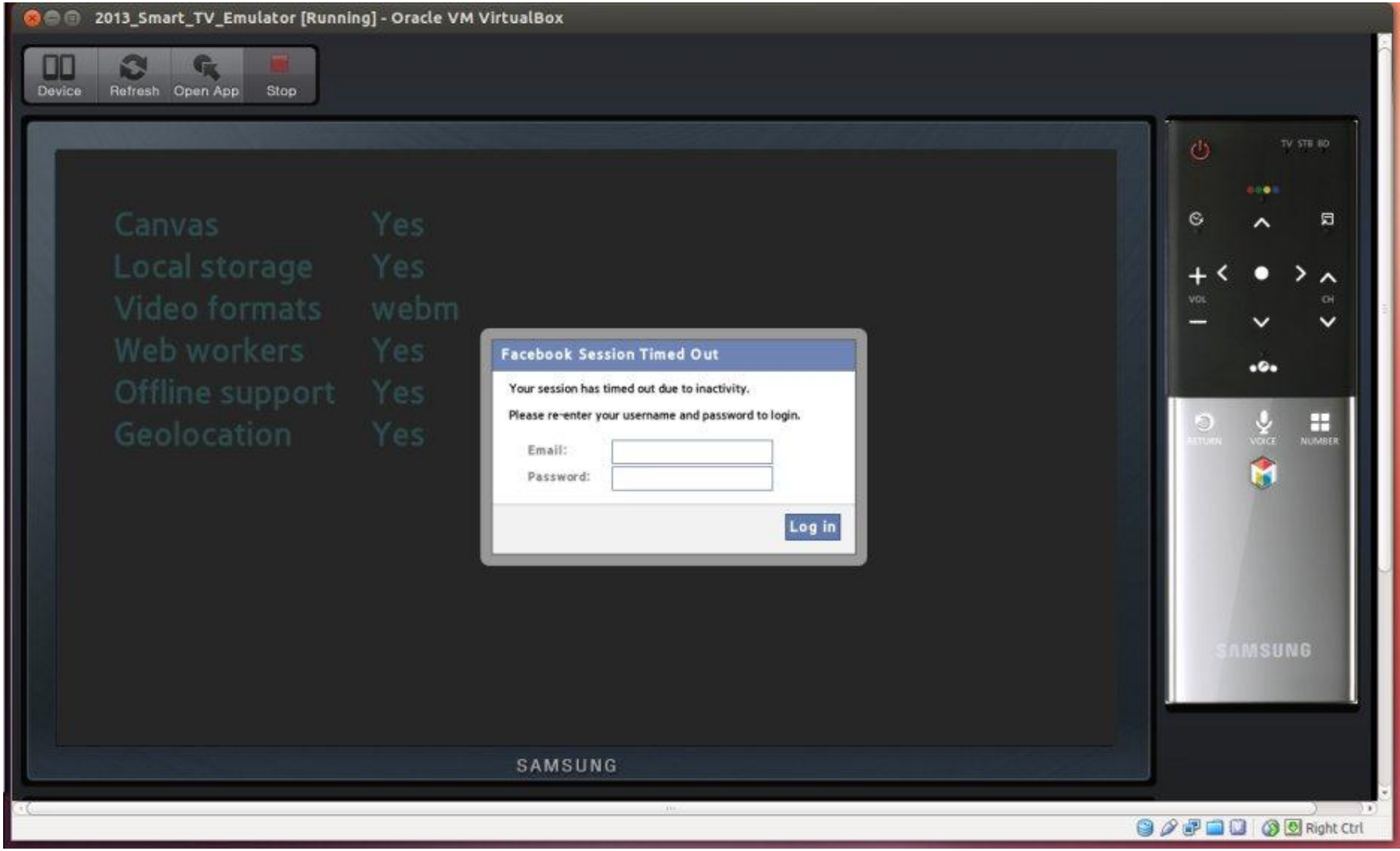
- Social engineering attacks
- HTML5 browser-based bot
- Exploits in browser plug-ins (i.e. Flash)

- If binaries are to be involved, it should be compiled to ARM v7

Most likely attack scenario: VIA HTML 5

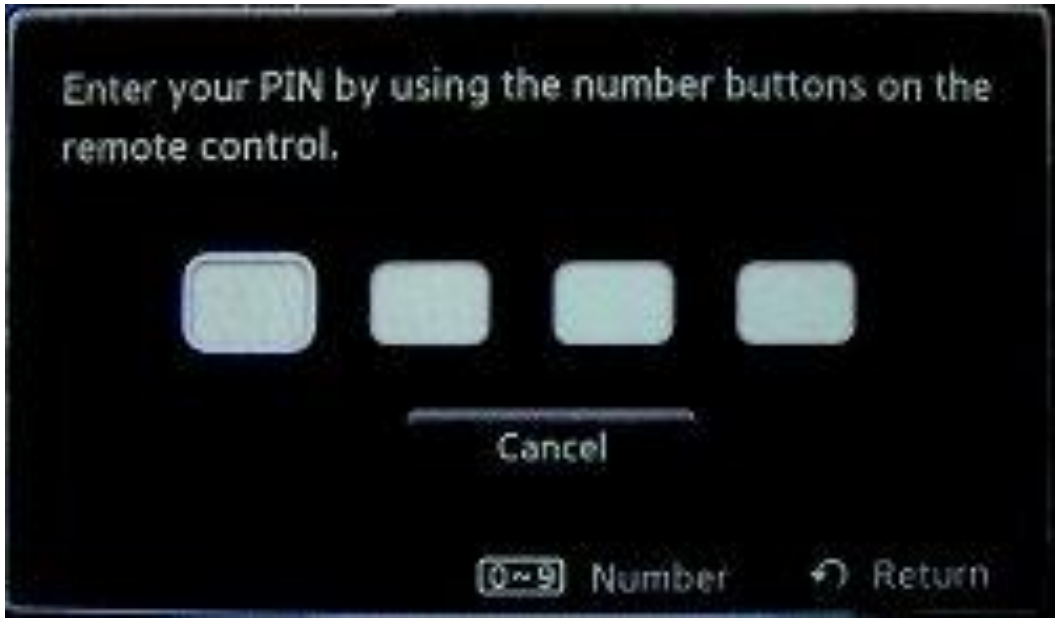
- "A Look at HTML5 Attack Scenarios"
  - http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_html5-attack-scenarios.pdf

- BeEF Project


2013_Smart_TV_Emulator [Running] - Oracle VM VirtualBox
Device
Refresh
Open App
Stop
Canvas Yes
Local storage Yes
Video formats webm
Web workers Yes
Offline support Yes
Geolocation Yes
Facebook Session Timed Out
Your session has timed out due to inactivity.
Please re-enter your username and password to login.
Email:
Password:
Log in
SAMSUNG
SAMSUNG
Right Ctrl

Easy to reset and get rid of stuff

And btw, as with every “good” consumer product - KISS



default password is “0000

Summarizing the risk

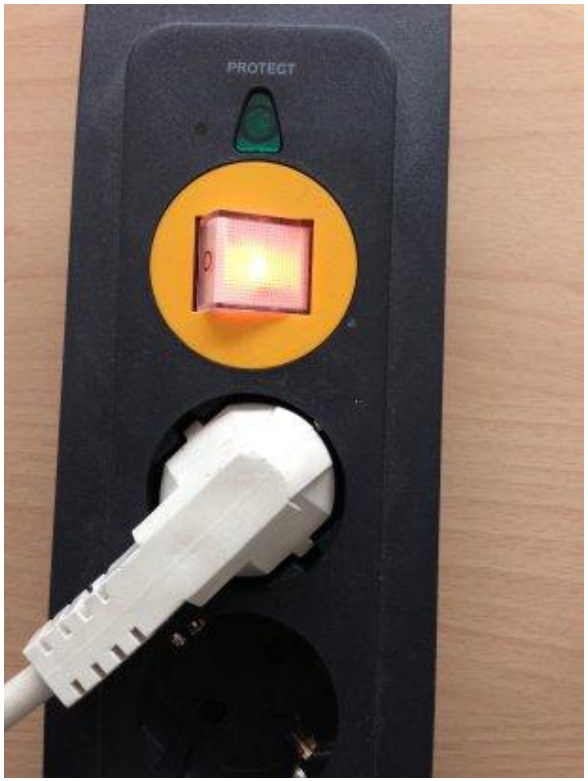
- Targeted attacks possible – with some effort
- Persistence possible (SeungJin Lee and Seungjoo KIM)
- Browser hooking possible
- Possible vulnerabilities in Flash

It will not be easy to get in and meanwhile Samsung has improved security a lot!

Persistence: http://cansecwest.com/slides/2013/SmartTV%20Security.pdf

Limiting the risk

- The 20 Euro recommendation!



The 0 Euro recommendation (for home)

A much higher risk is the other stuff in

Source: Finspy promotion video – copy found on Youtube

FinSpy is a field-proven Remote Monitoring Solution that enables Governments to face the current challenges of **monitoring Mobile and Security-Aware Targets** that regularly **change location**, use **encrypted and anonymous communication** channels and **reside in foreign countries**.

Traditional Lawful Interception solutions face new **challenges** that can only be solved using active systems like FinSpy:
- Data not transmitted over any network
- Encrypted Communications
- Targets in foreign countries

FinSpy has been **proven successful** in operations around the world **for many years**, and valuable intelligence has been gathered about Target Individuals and Organizations.

When FinSpy is installed on a computer system it can be **remotely controlled and accessed** as soon as it is connected to the internet/network, **no matter where in the world** the Target System is based.

QUICK INFORMATION	
Usage:	· Strategic Operations · Tactical Operations
Capabilities:	· Remote Computer Monitoring · Monitoring of Encrypted Communications
Content:	· Hardware/Software

Usage Example 1: Intelligence Agency

FinSpy was installed on several computer systems inside **Internet Cafes in critical areas** in order to monitor them for suspicious activity, especially **Skype communication** to foreign individuals. Using the Webcam, pictures of the Targets were taken while they were using the system.

Usage Example 2: Organized Crime

FinSpy was **covertly deployed on the Target Systems** of several members of an Organized Crime Group. Using the **country tracing and remote microphone** access, essential information could be gathered from **every meeting that was held** by this group.

Feature Overview

Target Computer – Example Features:

- Bypassing of 40 regularly tested Antivirus Systems
- **Covert Communication** with Headquarters
- Full **Skype Monitoring** (Calls, Chats, File Transfers, Video, Contact List)
- Recording of **common communication** like Email, Chats and Voice-over-IP
- **Live Surveillance** through Webcam and Microphone
- **Country Tracing** of Target
- **Silent extracting of Files** from Hard-Disk
- **Process-based Key-logger** for faster analysis
- **Live Remote Forensics** on Target System
- **Advanced Filters** to record only important information
- Supports most common Operating Systems (**Windows, Mac OSX** and **Linux**)

Headquarters – Example Features:

- Evidence Protection (Valid Evidence according to **European Standards**)
- **User-Management** according to Security Clearances
- Security Data Encryption and Communication using **RSA 2048 and AES 256**
- Hidden from Public through **Anonymizing Proxies**
- Can be **fully integrated** with Law Enforcement Monitoring Functionality (LEMF)

For a full feature list please refer to the Product Specifications.

Your mobile phone is the perfect

Source: Finspy promotion video – copy found on Youtube

If you want to try it:

Source: www.flexispy.com

Apple android NOKIA BlackBerry

Don't be the last to know

Are you a suspicious spouse, a concerned parent or worried employer — do you need to confirm that your partner is sexually faithful, that your child is safe or that your employees are behaving. Remove your doubts by spying on their smartphone or iPad.

Your spy in their pocket

Install FlexiSPY on a smartphone or iPad, and read all their communications, track locations and listen to calls and surroundings — you can even take control of the camera and microphone — all from a web browser. FlexiSPY is the private detective that lives on their phone but never sleeps.

BUY NOW

Source: www.flexispy.com

What's New in EXTREME

- See every picture, video or audio that has been taken or stored
- Read Facebook, Skype, LINE, Whatsapp, iMessage, BBM, WeChat and Viber messages — INCLUDING stickers, status, emoticons, pictures and profile details
- Take remote control of microphone and camera
- View web history, bookmarks, address book, notes , calendars
- Live Listen to phone calls and surroundings and create recordings of everything you hear
- Receive geofence and keyword alerts by email
- Faster install, improved stealth and security
- Also available for iPad
- Over 151 features

Source: www.flexispy.com

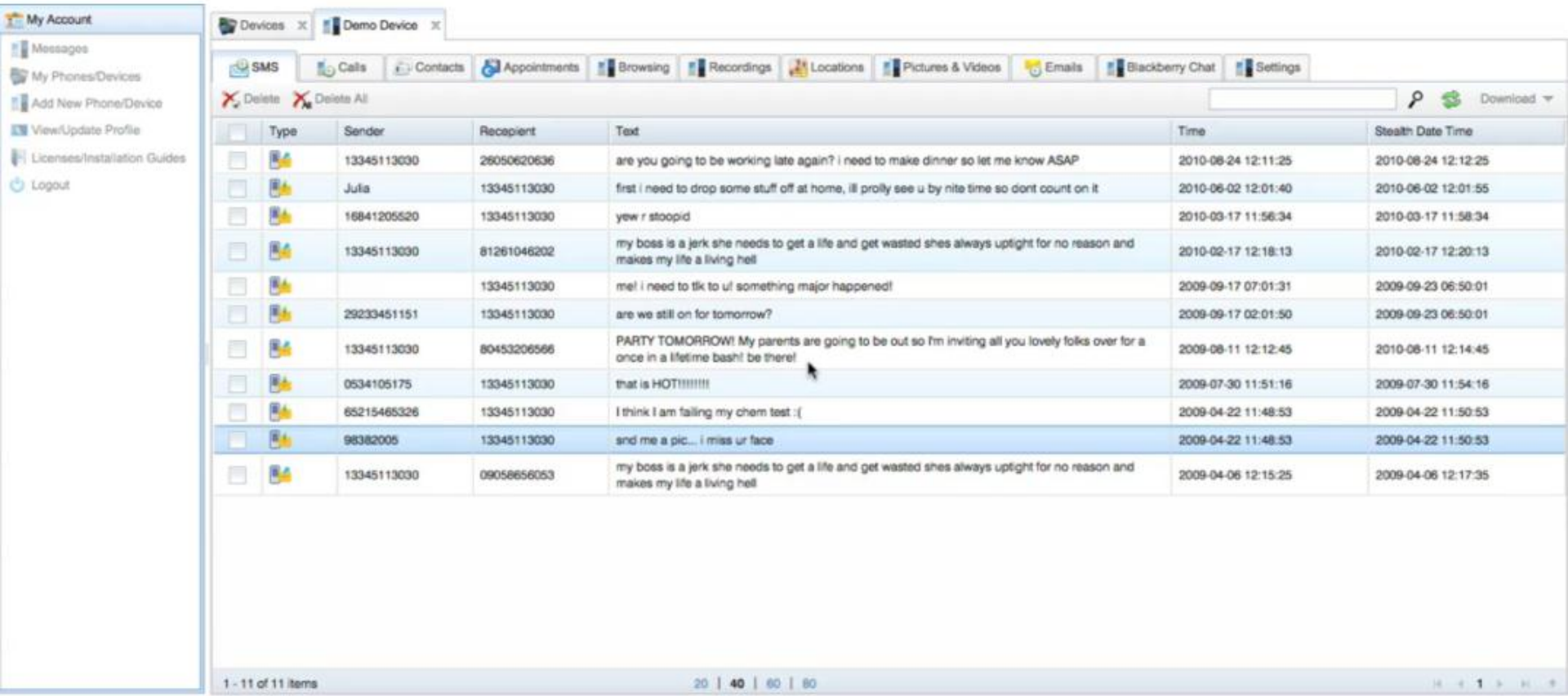
FlexiSPY EXTREME is the no holds barred, **best-selling, top of the line iPhone spy app**. It has features like **live call interception that you can't find anywhere else**. Imagine being able to be listen in to a live call from any number that you care to specify. It's also the world's first mobile spy application that will **capture WhatsApp** messages.

FlexiSPY PREMIUM is our **standard strength iPhone spy app** – this app offers spying of SMS, emails, GPS locations, call records and durations. This product will **reveal all messaging contents** and if they were where they claimed to be. This is ideal for checking their alibis.

Downloading is easy. Simply purchase FlexiSPY for iPhone and you can download directly onto a jailbroken iPhone. No complicated cables or PC are required, the entire process takes only a few minutes, and can be done anytime you have the iPhone in your hands. If you have not yet 'jailbroken' the iPhone, we show you how to do that in a matter of minutes.

Source: www.flexispy.com

Or try Mobistealth



Source: www.mobistealth.com

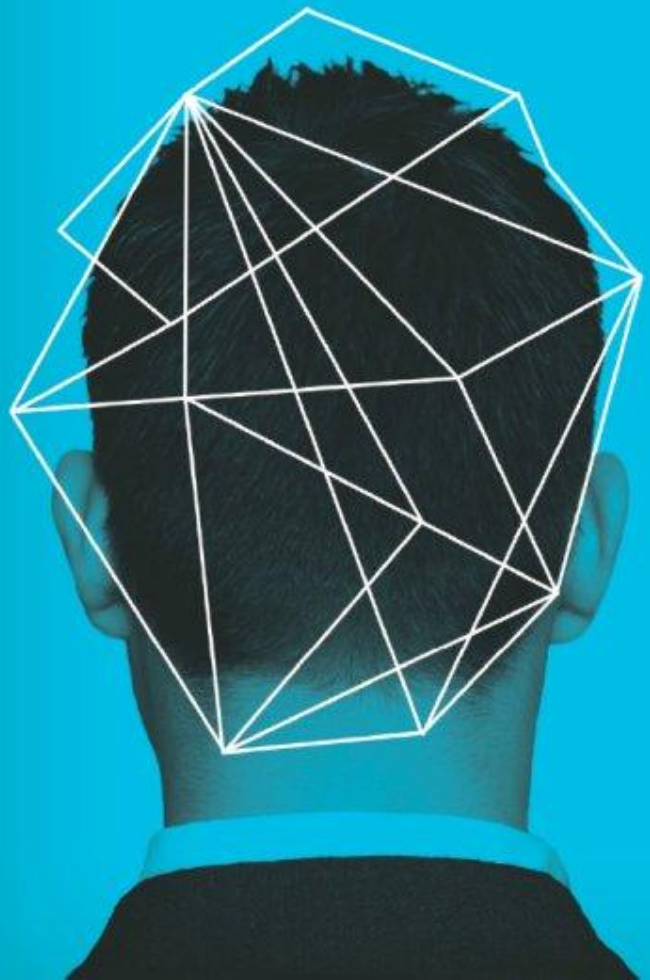
Thank you!

Raimund Genes

Trend Micro

Raimund_Genes@trendmicro.com

www.trendmicro.com



#RSAC

RSA CONFERENCE EUROPE 2013

References

Smart TV Applications
http://www.samsungdforum.com/Guide/art00005/index.html

Samsung Smart TV Apps Developer Forum Technical Guides
http://www.samsungdforum.com/Guide/

Model Guide for Samsung Apps
http://www.samsung.com/us/pdf/apps-and-product-table.pdf

Samsung Open Source Release Center (OSRC)
http://opensource.samsung.com/

Samsung TV Firmware Customization Project
www.samygo.tv/

BeEF (Browser Exploitation Framework Project)
http://beefproject.com/

Exploitation on ARM
http://www.exploit-db.com/wp-content/themes/exploit/docs/14548.pdf