Modern Authentication Hypes

Tomáš Rosa

crypto.hyperlink.cz

SMS-Based
Transaction Authentication Number (TAN)

- Very popular authentication method in contemporary banking systems.
  - http://en.wikipedia.org/wiki/Transaction_authentication_number
- Particular kind of the “must have” two-factor authentication.
  - It uses the out-of-band SMS channel to exercise the second authentication factor.
  - Also called mobile TAN – mTAN.

X-Platform Attacking

- Cross-Platform Attack (CPA)
  - *Any dishonest interoperation of several malware components running on different computing platforms.*
- Cross-Platform Infection (CPI)
  - *Any way of CPA components spreading to their respective destinations.*

True Lies

Eurograbber: A Smart Trojan Attack

Hackers' Methods Reveal Banking Know-How

By Tracy Kitten, December 17, 2012. Credit Eligible Email Tweet Like Share

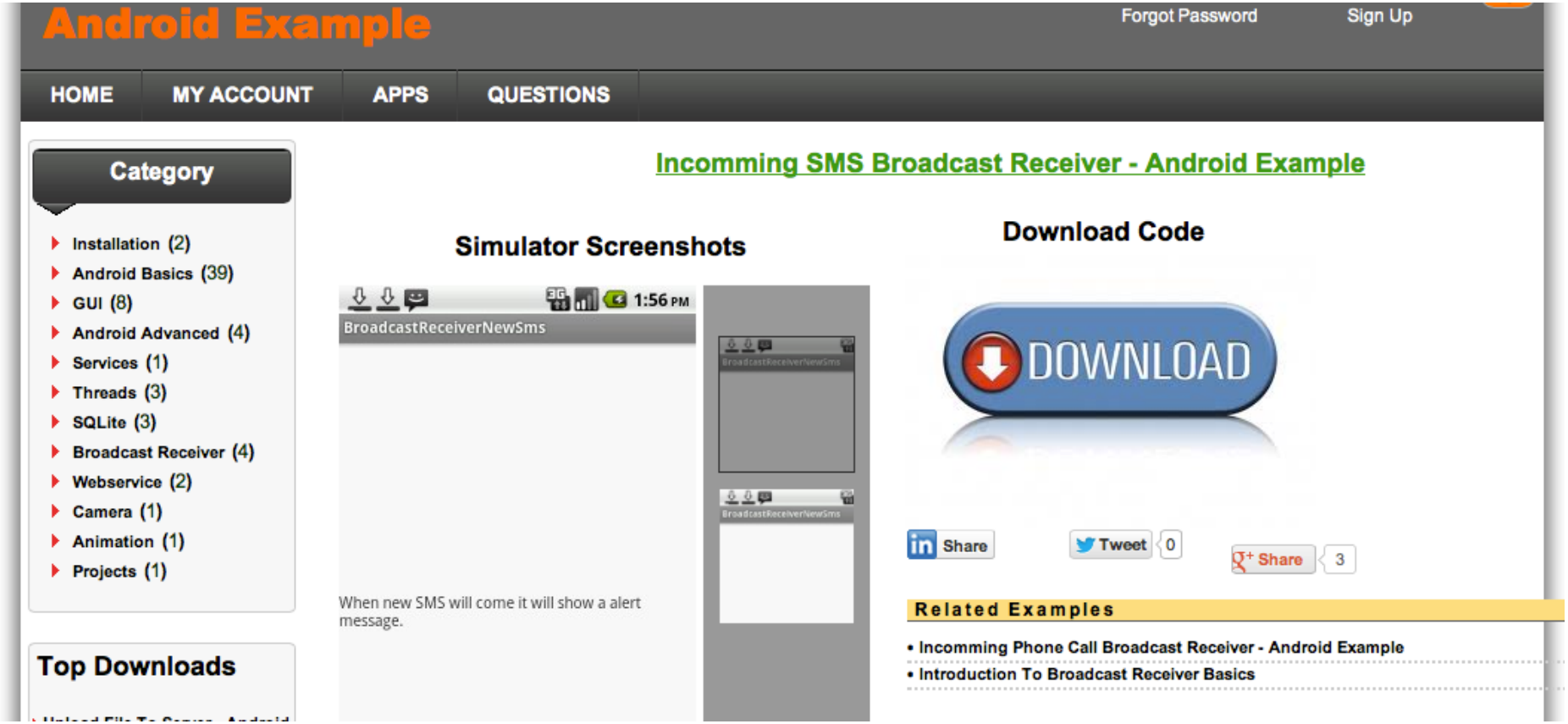
Listen to Audio

The Eurograbber banking Trojan is an all-in-one hit, researchers say. It successfully compromises desktops and **mobile** devices, and has gotten around commonly used two-factor **authentication** practices in Europe.

How can banking institutions defend themselves and their customers against this super-Trojan attack? It may seem cliché, but Darrell Burkey, who oversees intrusion prevention products at Internet-threat-protection provider Check Point Software Technologies, says defense hinges on consumer behavior.

http://www.bankinfosecurity.com/eurograbber-smart-trojan-attack-a-5359/op-1

Let's Face It

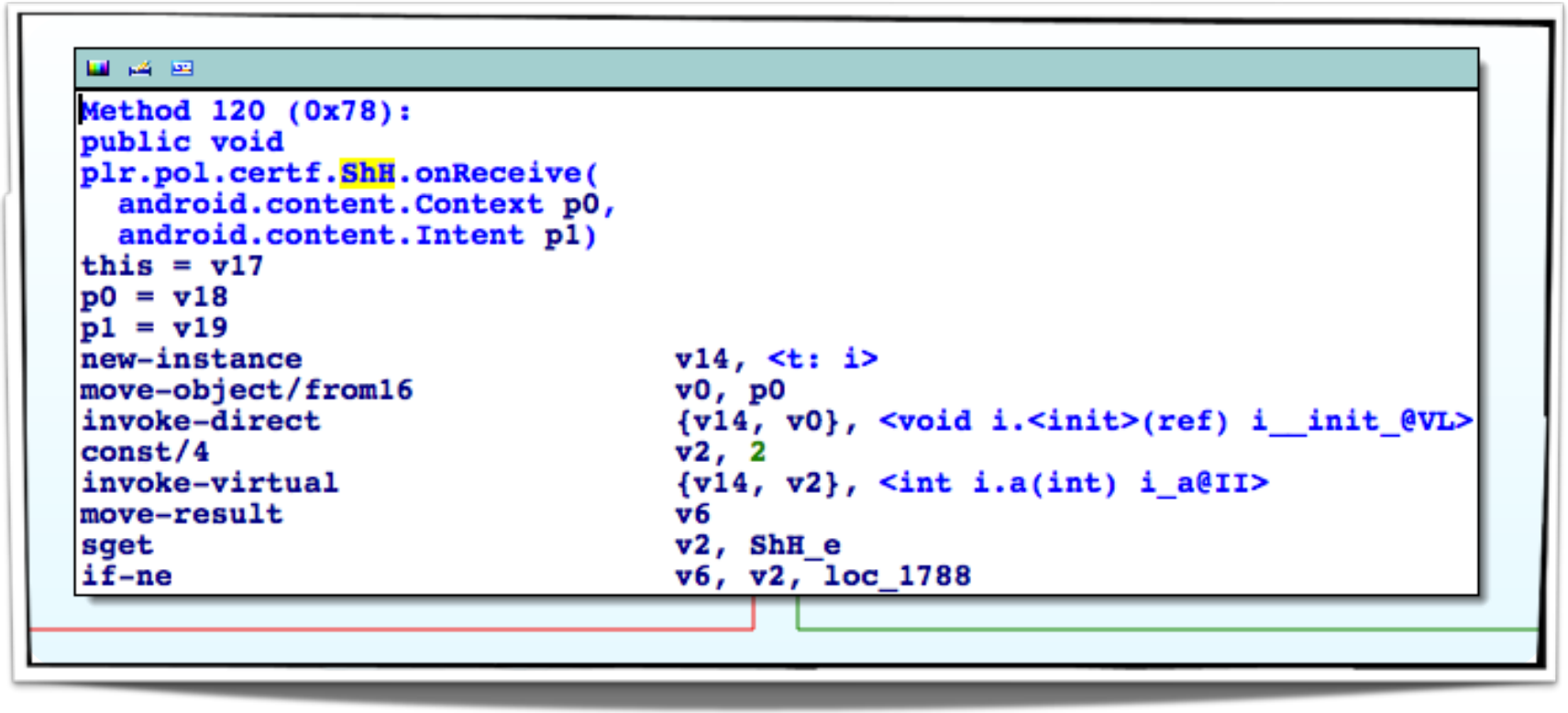

Android Example
Forgot Password
Sign Up
HOME
MY ACCOUNT
APPS
QUESTIONS
Category
Installation (2)
Android Basics (39)
GUI (8)
Android Advanced (4)
Services (1)
Threads (3)
SQLite (3)
Broadcast Receiver (4)
Webservice (2)
Camera (1)
Animation (1)
Projects (1)
Top Downloads
Incomming SMS Broadcast Receiver - Android Example
Simulator Screenshots
1:56 PM
BroadcastReceiverNewSms
When new SMS will come it will show a alert message.
Download Code
DOWNLOAD
Share
Tweet 0
Share 3
Related Examples
• Incomming Phone Call Broadcast Receiver - Android Example
• Introduction To Broadcast Receiver Basics

Sleeping With The Enemy

Incomming SMS Broadcast Receiver - Android Example

```
            android:label="@string/app_name" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />

                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>

        <receiver android:name="com.androidexample.broadcastreceiver.IncomingSms">
            <intent-filter>
                <action android:name="android.provider.Telephony.SMS_RECEIVED" />
            </intent-filter>
        </receiver>

    </application>
    <uses-sdk
        android:minSdkVersion="8"
        android:targetSdkVersion="17" />

    <uses-permission android:name="android.permission.RECEIVE_SMS"></uses-permission>
    <uses-permission android:name="android.permission.READ_SMS" />
    <uses-permission android:name="android.permission.SEND_SMS"></uses-permission>

</manifest>
```

Real SMS Trap



```
Method 120 (0x78):
public void
plr.pol.certf.ShH.onReceive(
  android.content.Context p0,
  android.content.Intent p1)
this = v17
p0 = v18
p1 = v19
new-instance                    v14, <t: i>
move-object/from16              v0, p0
invoke-direct                   {v14, v0}, <void i.<init>(ref) i__init_@VL>
const/4                         v2, 2
invoke-virtual                  {v14, v2}, <int i.a(int) i_a@II>
move-result                     v6
sget                            v2, ShH_e
if-ne                           v6, v2, loc_1788
```

It's Here!

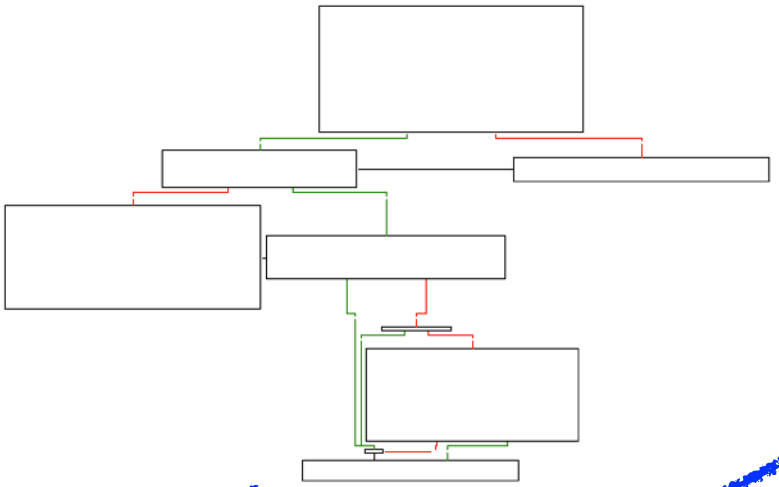
Experts Are Ready

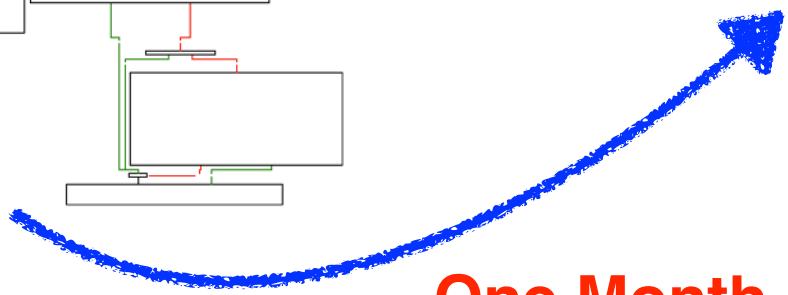
Consultants Eager To Help

Clients Take It Seriously

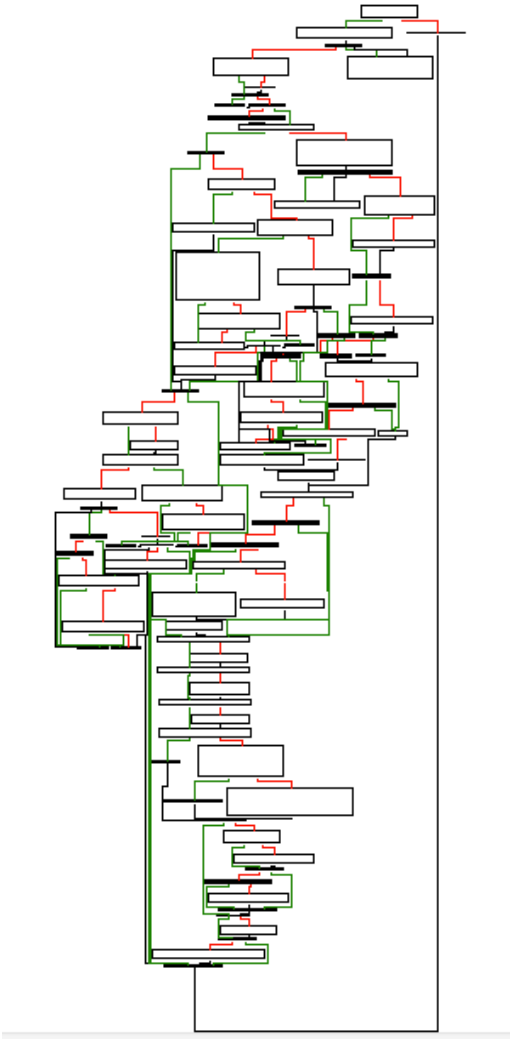
Criminals Sharpen Their Axes

Evolution of the SMS broadcast receiver's "onReceive" method spotted in the wild.

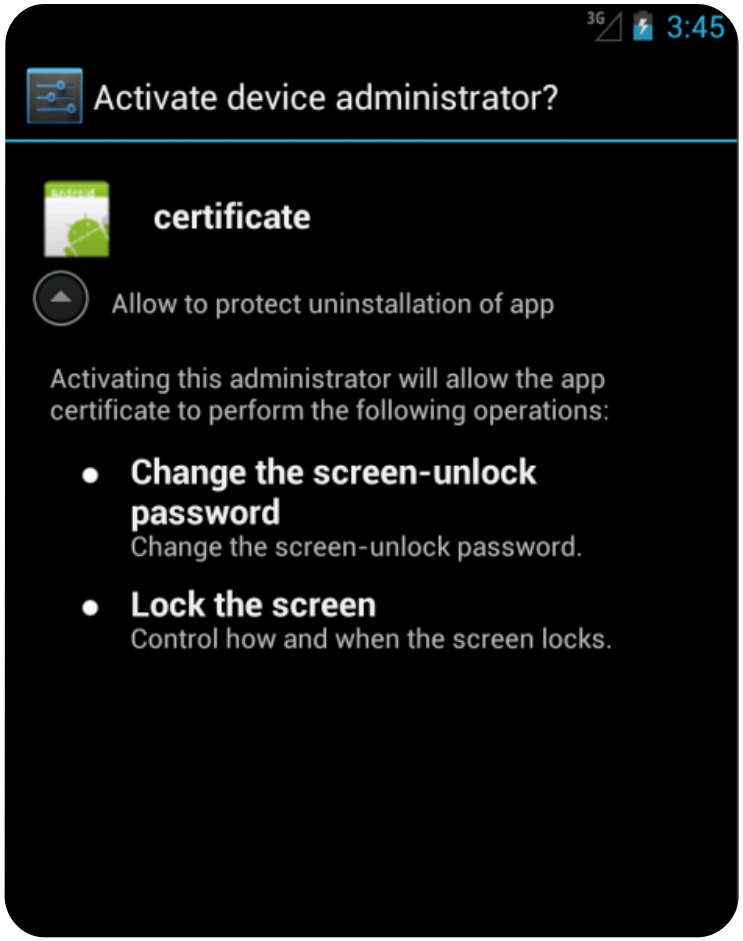




One Month

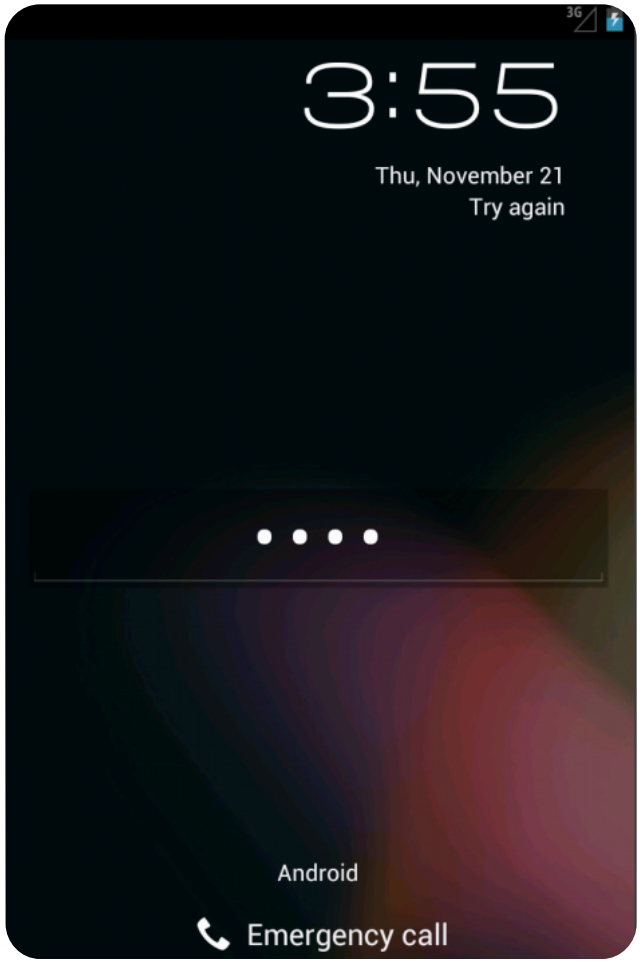


Cherry On the Cake



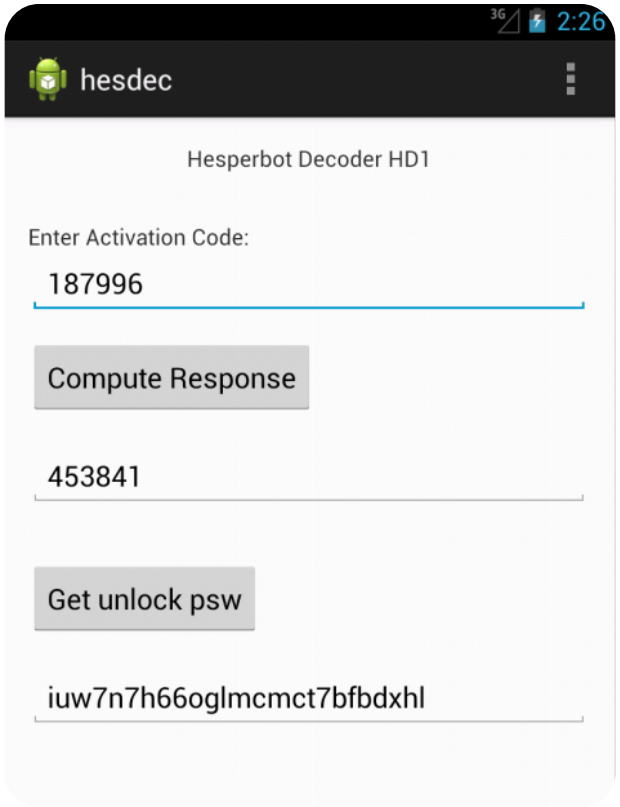
- This Trojan horse not only stole SMS.
- It enforced the user to accept it as an Mobile Device Management plugin.
- Note the permission to lock the screen with an arbitrary password…

Punished for an Uninstall

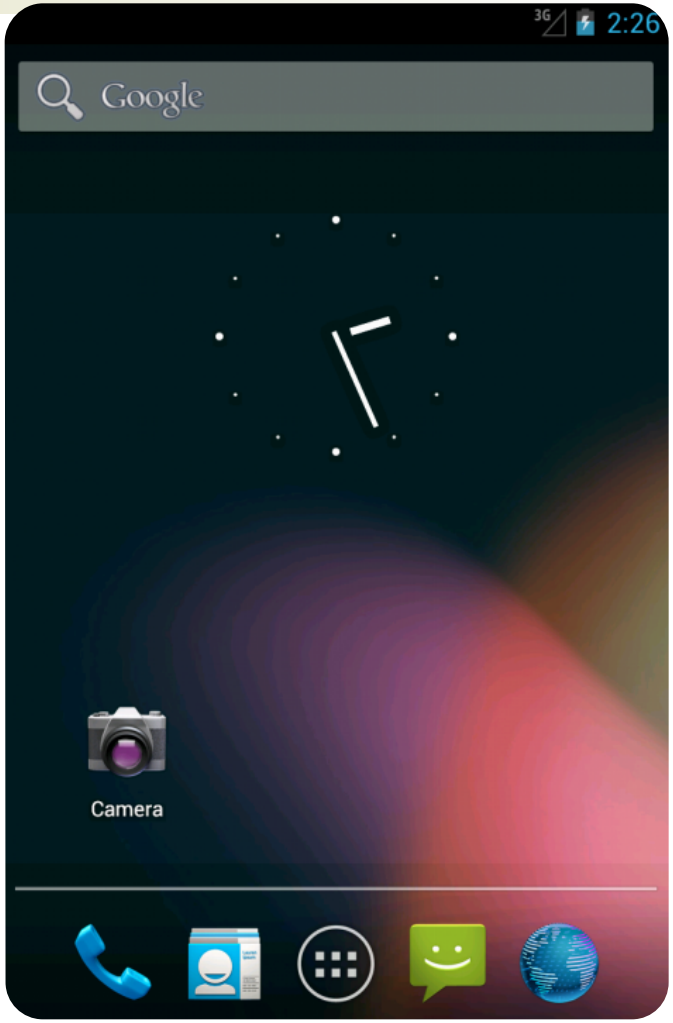


- Later on, when the client tried to uninstall the Trojan, it locked the screen with a cryptographically generated password.
- The malware author, however, was still able to generate the unlock code.
- We see a kind of ransomware extension.

Ransomware Reversed



Voilà...



Don't try this at home!

Anyway

- Attackers work hard to get better every day, now.
- We shall not be fooled by current state-of-the-art.
  - Let's envision and predict their next steps instead!
  - From this perspective - why should they limit their attention to internet banking only?
  - How about 3D payment gateways?
  - It is easy to see the same scenario, including the drive-by installation, applies here as well!

Soon: No Client Cooperation Required

- Contrary to the pioneering approaches used by ZitMo, Spitmo, and the Eurograbber scenario…
  - … the cross-platform infections envisioned in conference papers can run smoothly with no points of particular cooperation with the client.
  - We can think about generation-2 attacks.

For Instance…

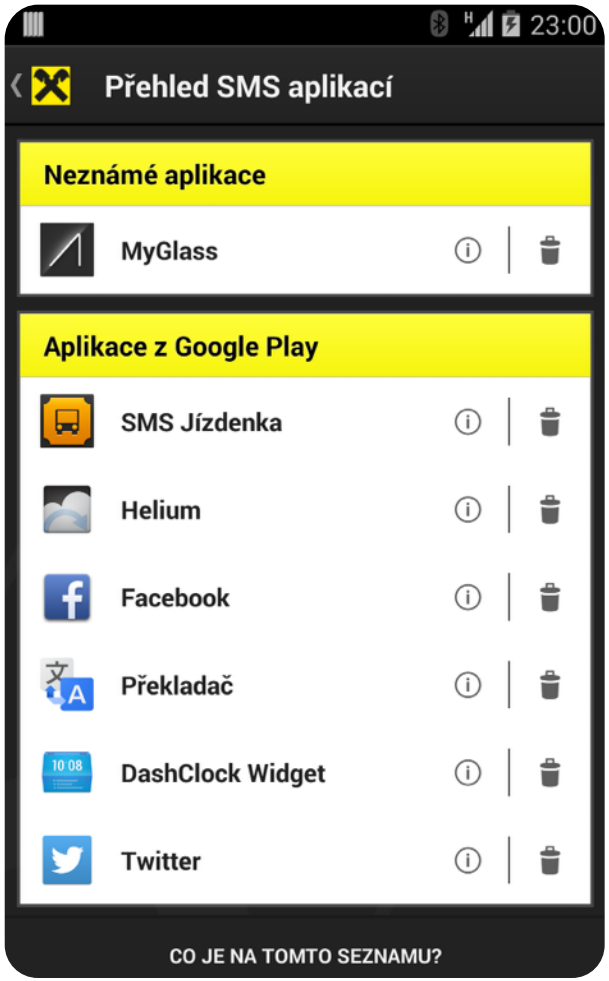
- Gmail link X-platform infection
  - Exploits Android services convergence at Google Play.
  - Discussed by Rosa in 2011 - 2012.
    - http://crypto.hyperlink.cz/files/rosa_scforum12_v1.pdf
- Wi-Fi link X-platform infection
  - Exploits implicit trust of WLAN devices.
  - Discussed by Dmitrienko et al. at BlackHat AD 2012.

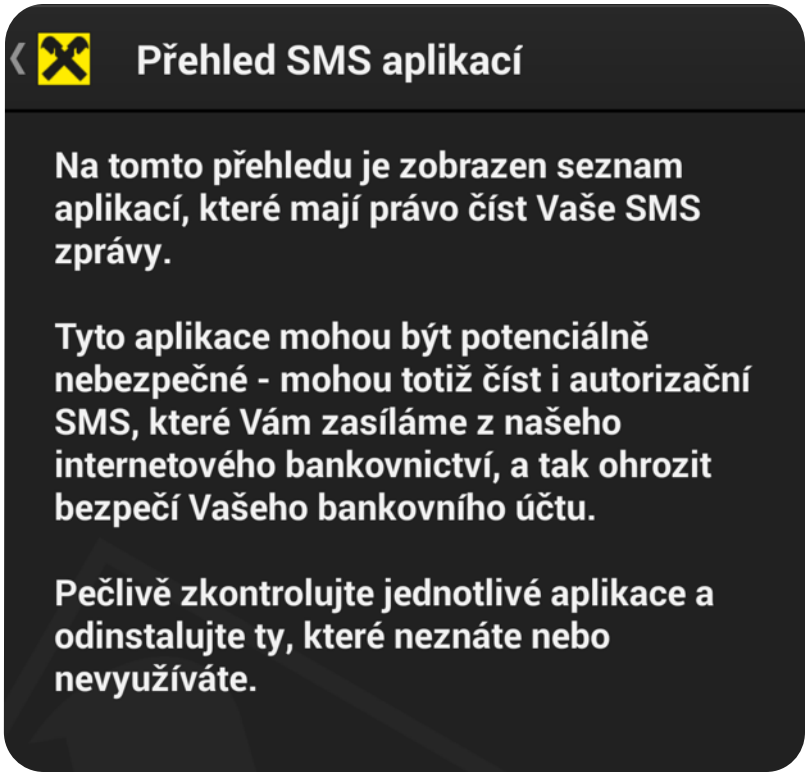
What Shall We Do?

- Start using fully-fledged mobile applications. Seriously.
  - ~~tier one attacks: SMS~~
    - ~~just a Trojan (on Android)~~
  - tier two attacks: SIM-based applications
    - requires OS exploits
  - tier three attacks: native applications
    - OS and App exploits

Note we still want to have a secure mobile banking, right? So, we have to protect those mobiles anyway!

Synergy: SAS Extension





Bluetooth Low Energy

BLE a.k.a. Bluetooth Smart

- Redesigned Bluetooth radio network
  - To consume much less power - it has to work for years with a button-cell battery.
  - To allow fast connection and pairing.
  - To enhance quick short message exchange.
- LE FFC versus NFC
  - Radiative Far Field vs. inductive Near Field
  - Comfort vs. energy feed
  - Smart devices vs. smart cards

Recently, iBeacon is a nice real-life example of FFC smashing NFC.

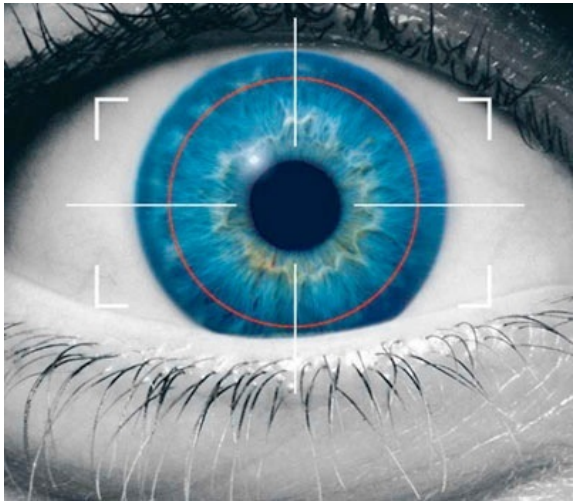
Bond. Air Bond.

- Bluetooth Low Energy authentication key-ring tag for a mobile banking.
- To make a transaction, the client needs:
  - ✓ the right mobile
  - ✓ the right PIN
  - ✓ the right AirBond nearby

Let the sky fall... we will stand tall! :-)

Biometrics

...automated establishment of the human identity based on their physical or behavioral characteristics.

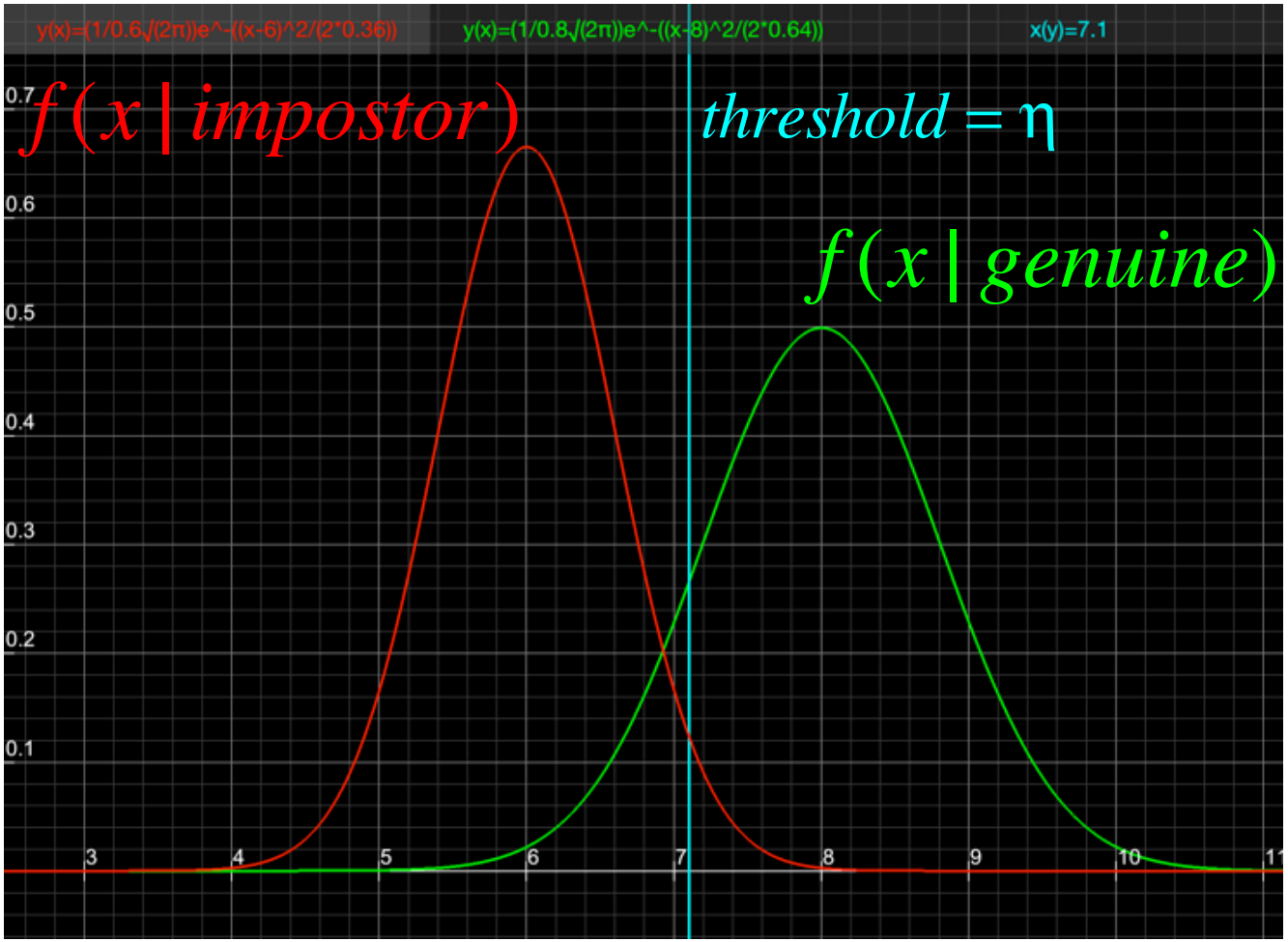


Modalities / Characteristics - Whatever You Can Get (*Politely*)

Match Score

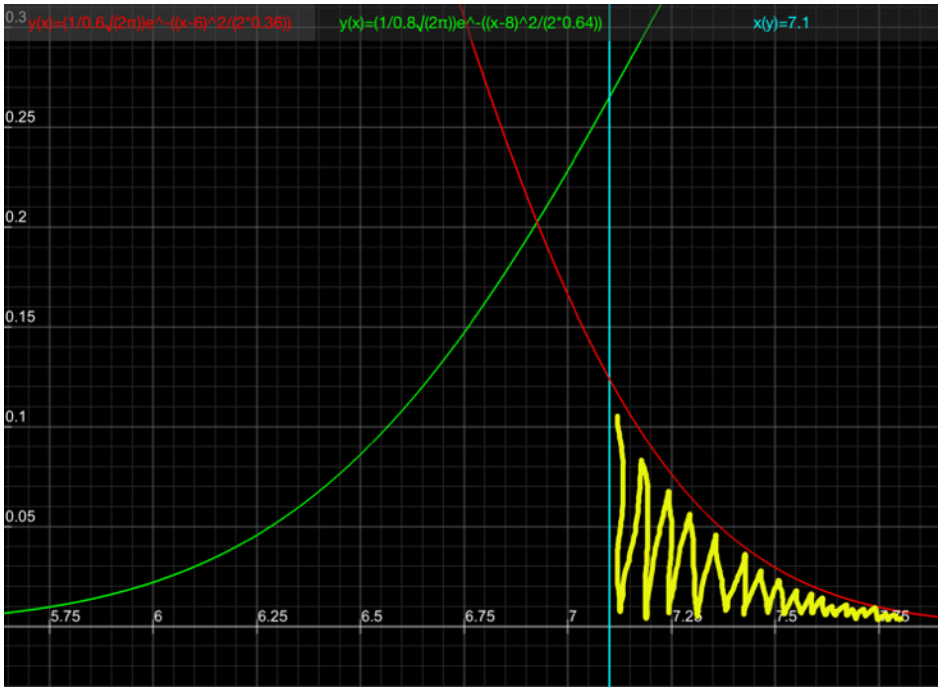
- It would be nice if we had simple true/false result.
  - As in conventional crypto.
  - But we cannot...
- All we have is a random variable *X* that follows two conditional distributions.
  - $f(x \mid \text{impostor})$
  - $f(x \mid \text{genuine})$

Match Score Evaluation



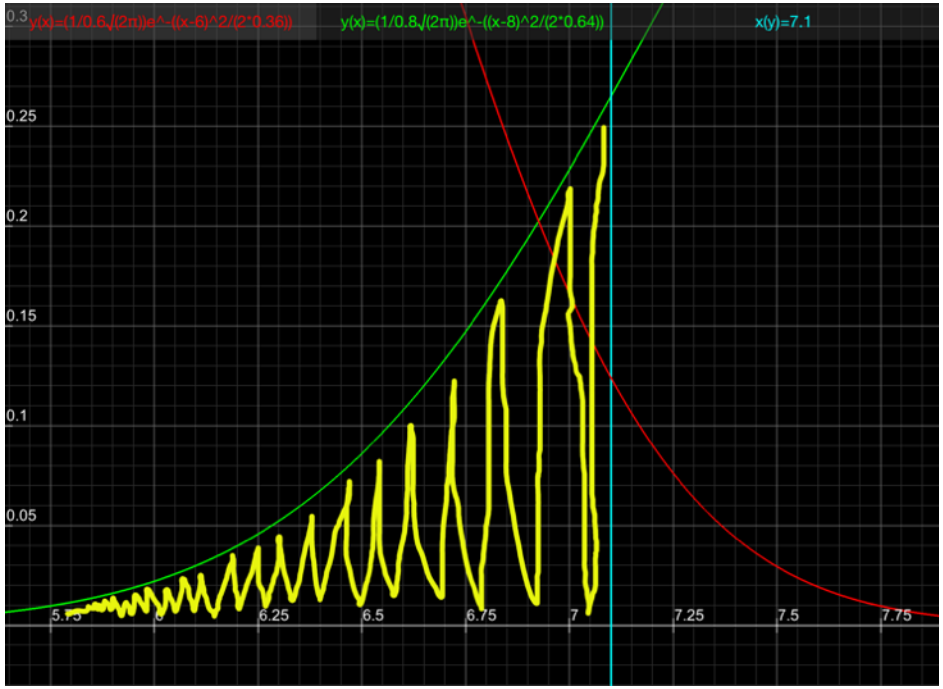
False Acceptance Rate

$$FAR = \int_{\eta}^{\infty} f(x \mid impostor)\, dx$$



False Rejection Rate

$$FRR = \int_{-\infty}^{\eta} f(x \mid genuine)\,dx$$

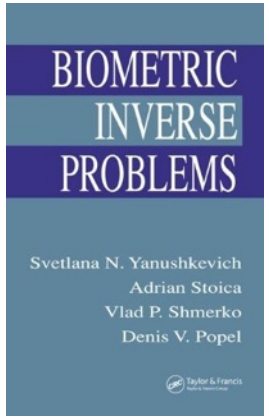


Contrasting Design Approach

- Classic cryptography
  - infeasible mathematical problems
- Quantum cryptography
  - intractable physical problems
- Biometric identification
  - statistical signal analysis
  - intractability is usually ***not*** the prime concern
  - we hope the Mother Nature complexity *somehow* guarantees the security

BIO Brute Force Attack

- Randomly generate plausible circa 1/FAR samples and put them to the test.
  - Also termed “Zero-Effort”, denoting that the attacker makes no special effort to imitate the original person characteristic.
- Synthetic samples generation is quite feasible today.



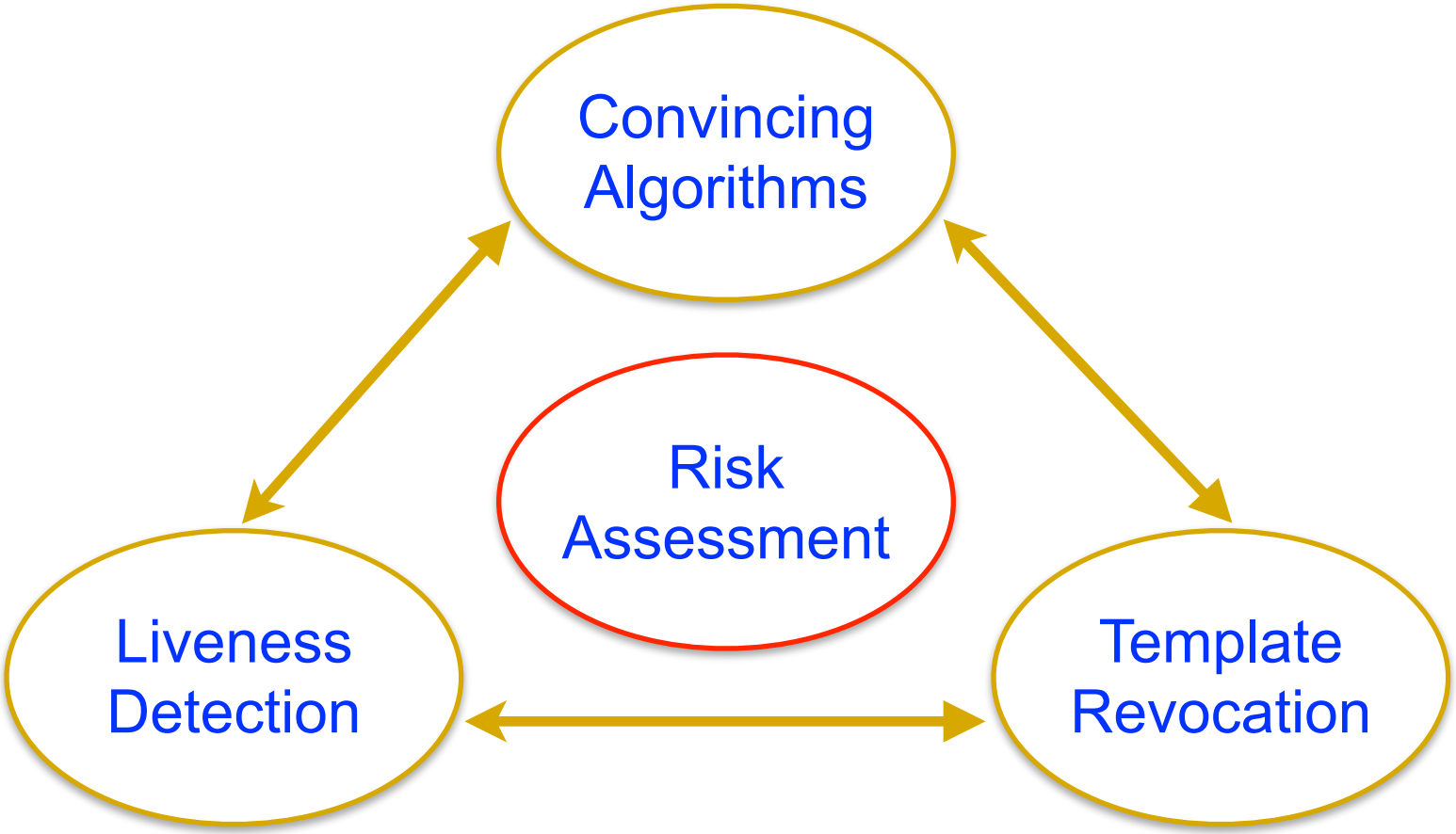
Cryptanalysis-Like Attacks

- Usually a variant of "Hill-Climbing" denoting the attacker iteratively improves the BIO sample data based on:
  - scoring feedback *(side channels)*
  - stolen template *(pre-image attacks)*
  - independent template trained from intercepted BIO samples *(correlation attacks)*
  - known scoring anomaly *(differential analysis. etc.)*
  - implementation faults *(general hacking)*

Spoofing

- *The process of defeating a biometric system through the introduction of fake biometric samples.*
  - *(Schuckers, Adler et al., 2010)*
- Particular modus operandi on how to deploy the attacking data vectors.
  - Can be seen as being orthogonal to the aforementioned hill-climbing attacks.

Open Problems



Convincing Algorithms

Liveness Detection Demystified


Safe Template Revocation

Conclusion

- SMS-based authentication is definitely smashed down for a mass market.
  - Just forget about it.
- The right way is having a fully-fledged mobile authentication application.
  - Then we can start **fortifying the mobile platform** and enjoy synergy effects for the whole banking portfolio.
- Biometrics is just another technology.
  - It has its pro et contra.
  - It is by no means a universal remedy for everything.
  - Be careful about the most trivial spoofing and brute-force attacks. Do a penetration test!

Thank You For Attention

Tomáš Rosa, Ph.D.
http://crypto.hyperlink.cz

Movie Snapshots Taken From

- *Slunce, seno, erotika*, Ateliery Bonton Zlín, a.s., ČR, 1991
- *The Magnificent Seven*, United Artists, USA, 1960
- *Slunce, seno, jahody*, ČR, 1983
- *Monsters vs. Aliens*, DreamWorks Animation, USA, 2009
- *Císařův pekař*, ČR, 1951