

Mobile Security In Practice - Autumn 2013

Tomáš Rosa

crypto.hyperlink.cz



[Jailbreak (And Root)]



“Potřebuju vybavení, které lze snadno modernizovat.”

Karel Ševčík Majitel rodinného pekařství



evasi0n - iOS 6.x Jailbreak



AdChoices

**Bluetooth
Module Ios**
www.Bluegiga.com

Order Complete
Wireless
Bluetooth
Solutions From A
Market Leader.

[What Does It Mean Anyway]

- Besides obvious warnings, there is one more thing to add.
- Do you wonder whether smart phone OS security can be broken?
 - You do not need to ask anymore.
- The worldwide verified proof is right here.
 - It is the Jailbreak in itself!

[Failbreak]

- Privilege escalation exploit that does *not* end up with the full-fledged Jailbreak or Root.
 - Just a suitable exploit and payload.
 - Can pass through *Jailbreak* detection.
 - Developer's profile is a perfect position to perform a kind of Failbreak.

[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.*

[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.

[mTAN Becomes Risky]

- CPA is becoming more and more feasible every day, now.
 - In other words, there is non-negligible amount of cases where mTAN security is not guaranteed anymore.
- Furthermore, such attacks usually only get better.
 - We shall be prepared this will get worse.

[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]

The screenshot shows a website with a dark header containing the title "Android Example" in orange, and links for "Forgot Password" and "Sign Up". Below the header is a navigation bar with "HOME", "MY ACCOUNT", "APPS", and "QUESTIONS".

The main content area features a green title "Incoming SMS Broadcast Receiver - Android Example". On the left is a "Category" sidebar with a list of topics: 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), and Projects (1). Below this is a "Top Downloads" section.

The main content is divided into two columns. The left column, titled "Simulator Screenshots", shows two screenshots of an Android emulator. The top screenshot shows a status bar with the time 1:56 PM and a notification for "BroadcastReceiverNewSms". Below the screenshots is the text: "When new SMS will come it will show a alert message." The right column, titled "Download Code", features a large blue "DOWNLOAD" button with a red arrow icon. Below the button are social sharing options: "in Share", "Tweet 0", and "Share 3". At the bottom of this column is a yellow "Related Examples" section with two links: "Incoming Phone Call Broadcast Receiver - Android Example" and "Introduction To Broadcast Receiver Basics".

[Sleeping With The Enemy]

```
Incomming SMS Broadcast Receiver - Android Example
android:name="com.androidexample.broadcastreceiver.BroadcastNewsSms"
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>
```

It's Here!



Experts Are Ready



[Consultants Eager To Help]

They fought like seven hundred

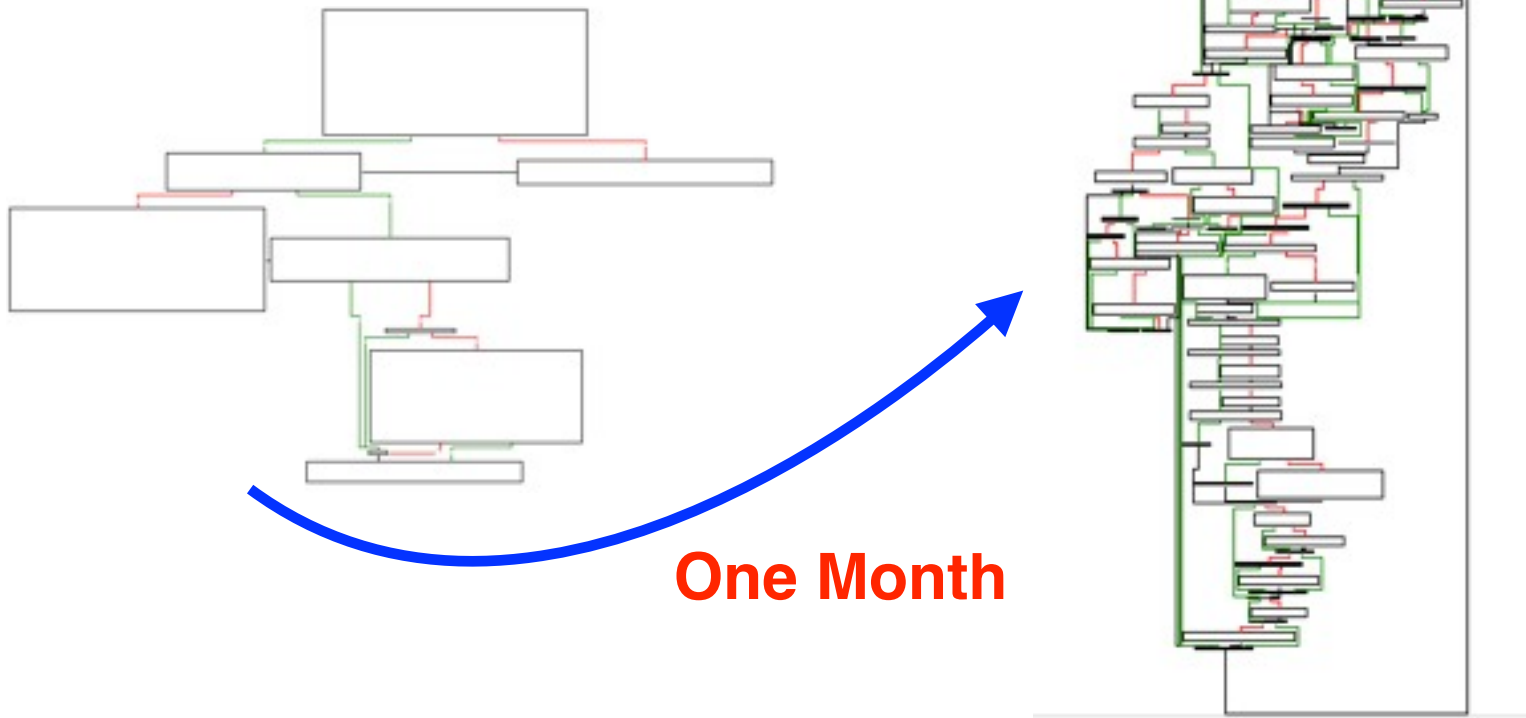


Clients Take It Seriously



[Criminals Sharpen Their Axes]

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



[No Client Cooperation Required]

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

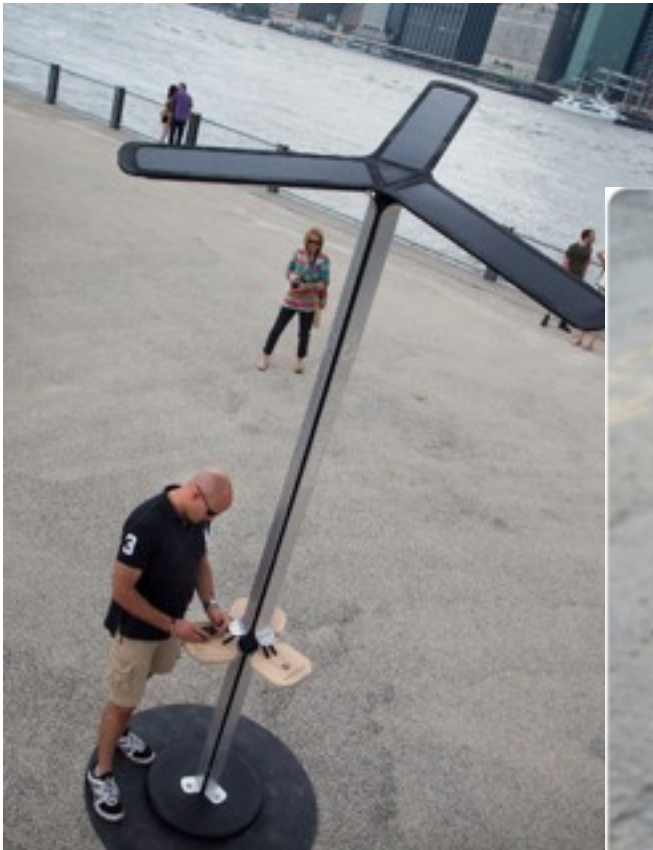
USB Link Cross-Platform Infection

- Discussed by Stavrou and Wang at BlackHat DC 2011.
 - Exploits USB protocol stack vulnerabilities for infection spreading in both ways (CPI computer ↔ mobile).
- The original proof-of-concept can be further extended.

[Yet-Another Incarnation]

- Discussed by Lau, Jang, and Song at BlackHat US 2013 this summer.
 - Malicious public charging station silently installs malware into connected iDevices.
 - Exploits weak authorization concept of USB protocol stack under iOS 6.
 - Does not require (but allows instead) Jailbreak or Failbreak.
 - Employs otherwise honest X-platform library www.libimobiledevice.org.
 - Protection is expected to get better with iOS 7.

[NY: Solar Malware For Free



[Show Goes On...]

- 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.

[Bring Your Own Device]



[On the Other Hand Bring *Break Your Own Device*]

- Since: "*By agreeing to the profile installation, the user's device is automatically enrolled without further interaction.*"

-- http://images.apple.com/iphone/business/docs/iOS_6_MDM_Sep12.pdf

- Zdziarski in "*Hacking and Securing iOS Applications*", 2012
- Schuetz at BH US 2011 and Shmoocon 2012
- Sharabani at Herzliya 2013
- Medin at Shmoocon 2013

[Hackers Are Ready...]

Apple malware 'mobileconfig' allows remote hijacking of iPhones, iPads

March 25, 2013 10:52am

Recommend 78 Share 83 Tweet 144 Email 0 ShareThis 1417

Still think your iPhone and iPad are safer than their Android counterparts? Don't get too smug yet.

Malicious profiles, or so-called "mobileconfigs," may yet show hackers the way into your Apple devices running iOS, security firm Skycure warned.

"A malicious profile could be used to remote control mobile devices, intercept network activity and hijack user sessions," it said in a [blog post](#).

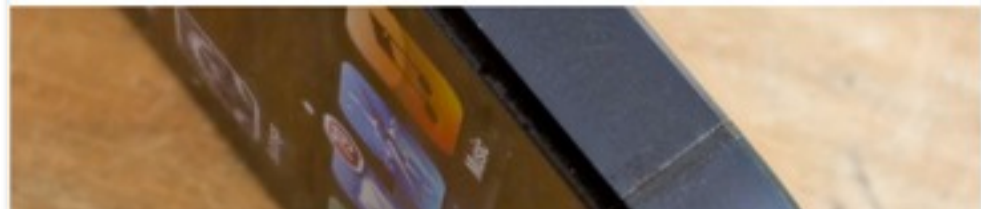
Configuration profile warning reminds us not to carelessly tap and install things on our iPhones and iPads

By Rene Ritchie, Wednesday, Mar 13, 2013 at 11:06 am

12

Security firm: iOS Configuration Profiles could be vector for Apple's first big malware wave

By Matthew Panzarino, Tuesday, 12 Mar '13, 10:00am



[iOS Peripheral Channels]

- They are managed by the External Accessory framework.
 - Actually, this is a dynamic library that provides streaming Objective-C interface in between application processes and the operating system drivers.
- Communication with external iPhone NFC controllers is provided this way.
 - In particular, this concerns PIN verification.
 - Even with iPhone 5S, there is still no internal NFC controller available.

[Sniffing in Action]

EASniFF> EAOutputStream<0x00453be0> wrote 9 B (of 9)

EASniFF> <00453be0> 0000: c5 b1 05 00 20 00 80 08 dd

|

EASniFF> EAInputStream<0x004534f0> read 4 B

EASniFF> <004534f0> 0000: c5 b1 03 00

|

**PIN
12 34**

EASniFF> EAInputStream<0x004534f0> read 3 B

EASniFF> <004534f0> 0000: 00 20 67

| . g

EASniFF> EAOutputStream<0x00453be0> wrote 13 B (of 13)

EASniFF> <00453be0> 0000: c5 b1 09 24 12 34 ff ff ff ff 00 fb

| ...\$F!.....

EASniFF> EAInputStream<0x004534f0> read 4 B

EASniFF> <004534f0> 0000: c5 b1 04 00

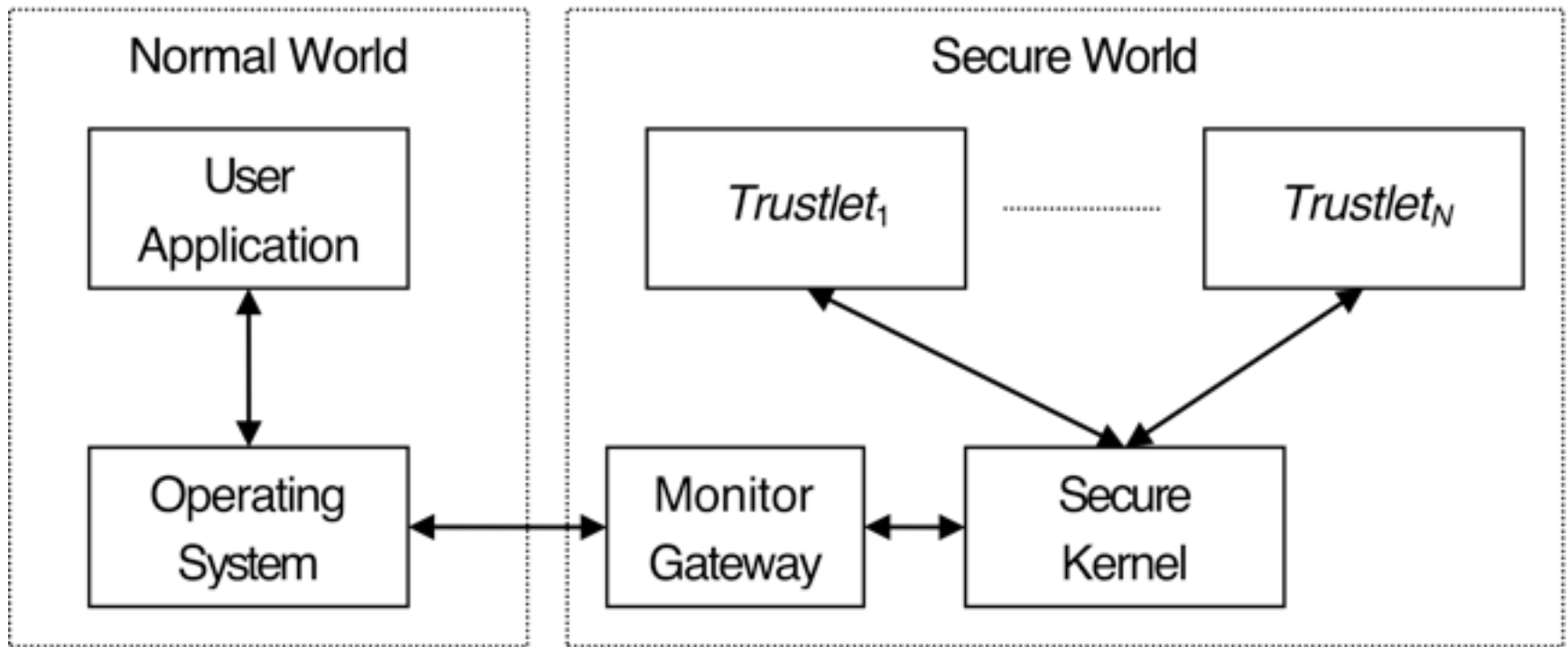
|

EASniFF> EAInputStream<0x004534f0> read 4 B

EASniFF> <004534f0> 0000: 00 90 00 f6

|

TrustZone Illustration



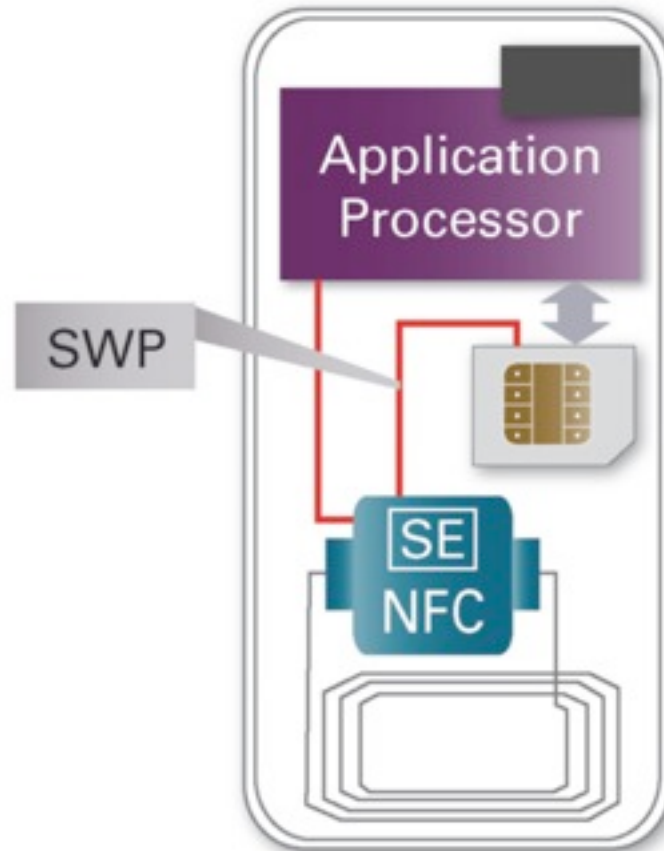
ARM Security Technology - Building a Secure System using TrustZone Technology, whitepaper, ARM Limited, 2009

[Here Comes the Sticker]

- Cool option if your device lacks NFC.
- But... what if your device **does have** NFC already?

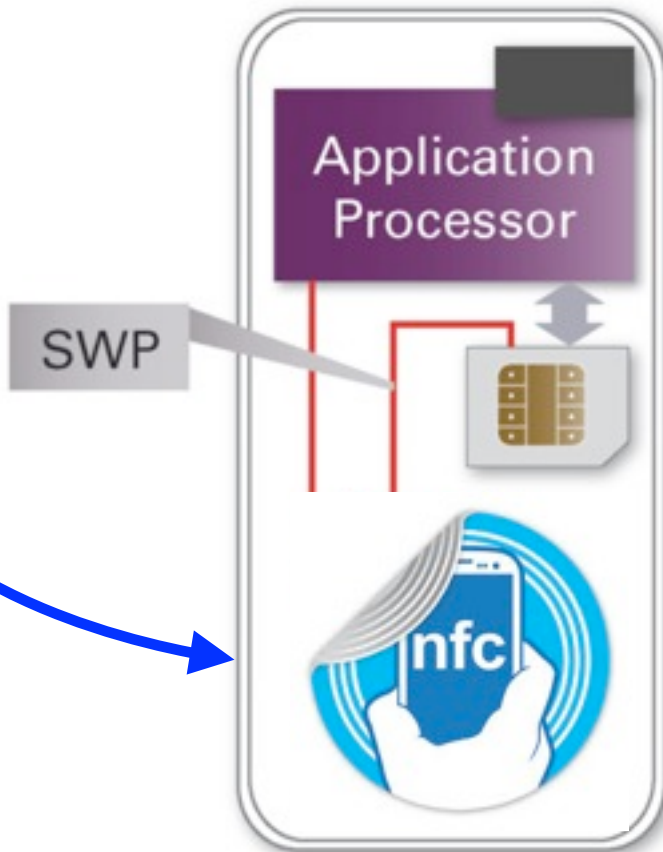
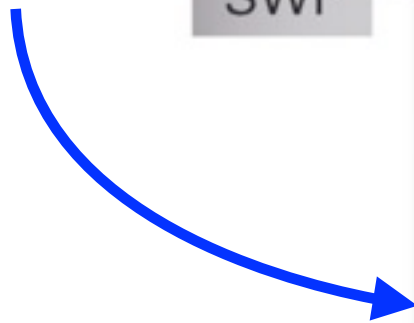


[NFC Internals]

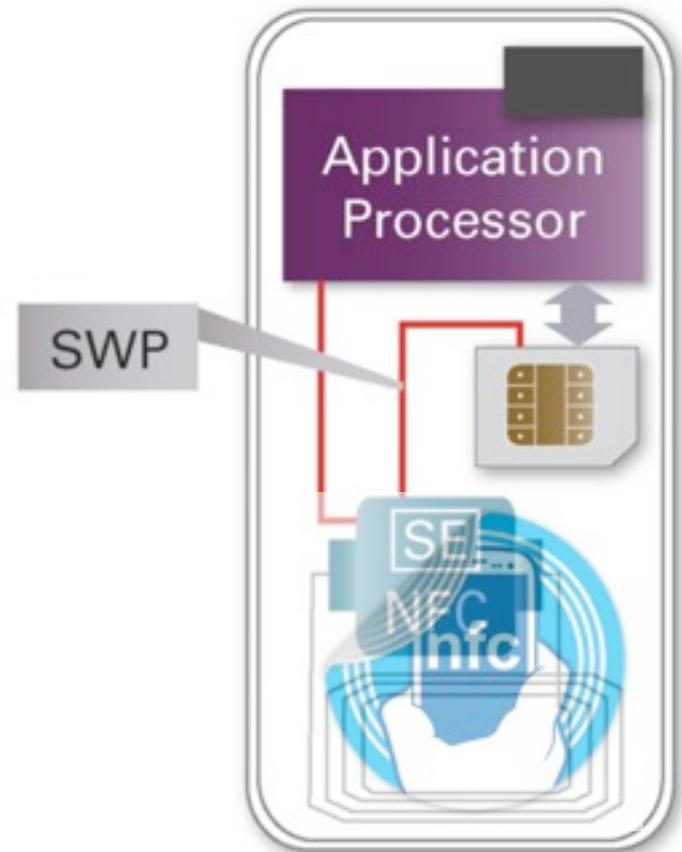


NFC CLF with Built-in
SE + SIM (SE)

[So, You Want a Sticker]



NFC CLF with Built-in
SE + SIM (SE)



NFC CLF with Built-in
SE + SIM (SE)

[Be Aware of Mobile Malware!]

- Malicious application can transparently skim the sticker (almost) any time it wants to (obviously).
 - On Android, no special exploit is needed. Just as in the case of mTAN interception...
- The NFC controller shall be turned off or strictly managed.
 - On the other hand, it would not be that useful with the transponder attached permanently anyway...



[Bluetooth Low Energy]



[BLE a.k.a. Bluetooth Smart]

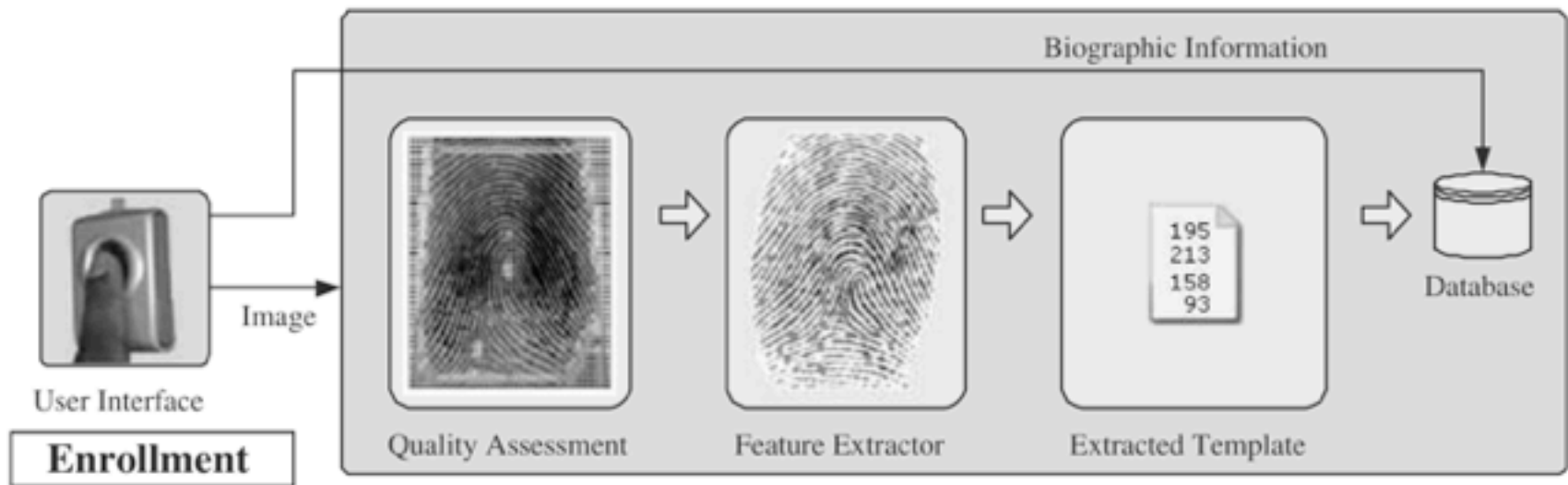
- Redesigned Bluetooth radio network
 - To consume much less power - it has to work for years with a button-cell battery.
 - To allow fast connection and pairing.
 - To enhance quick short message exchange.
- LE FFC versus NFC
 - Radiative Far Field vs. inductive Near Field
 - Comfort vs. energy feed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

[Biometric Identification]

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

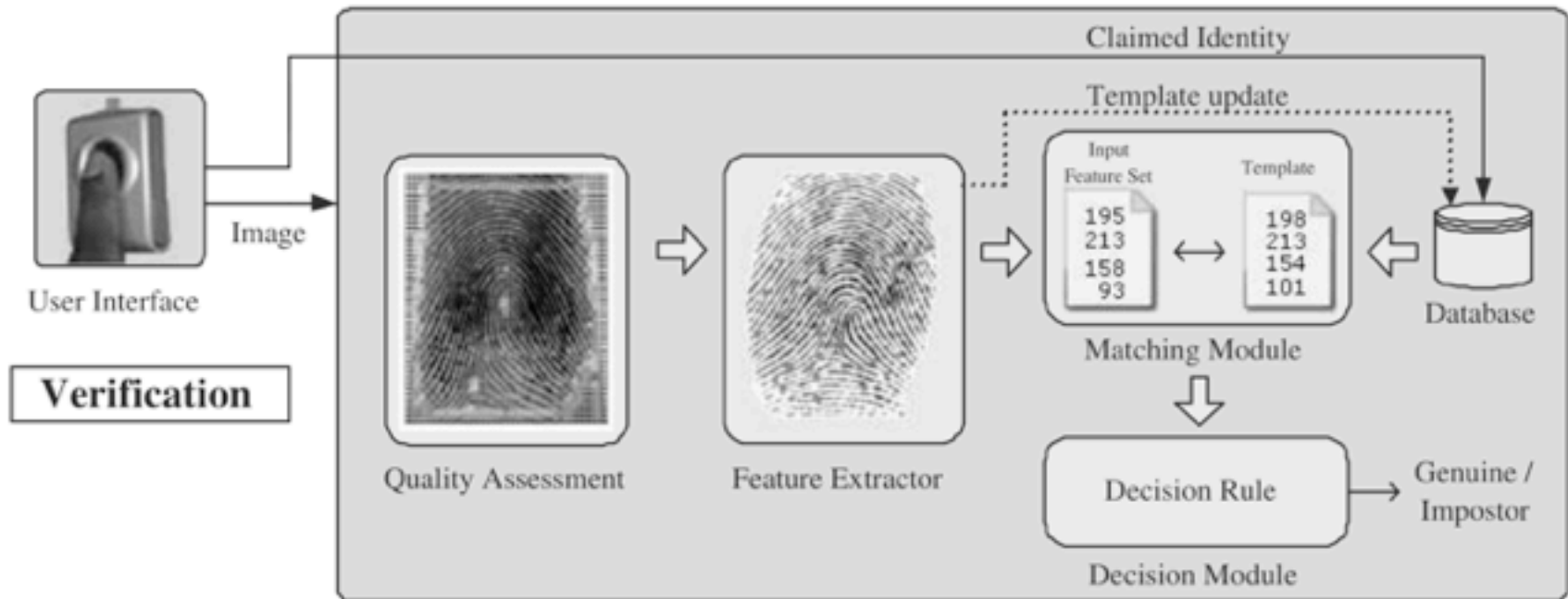


[Enrollment Phase]



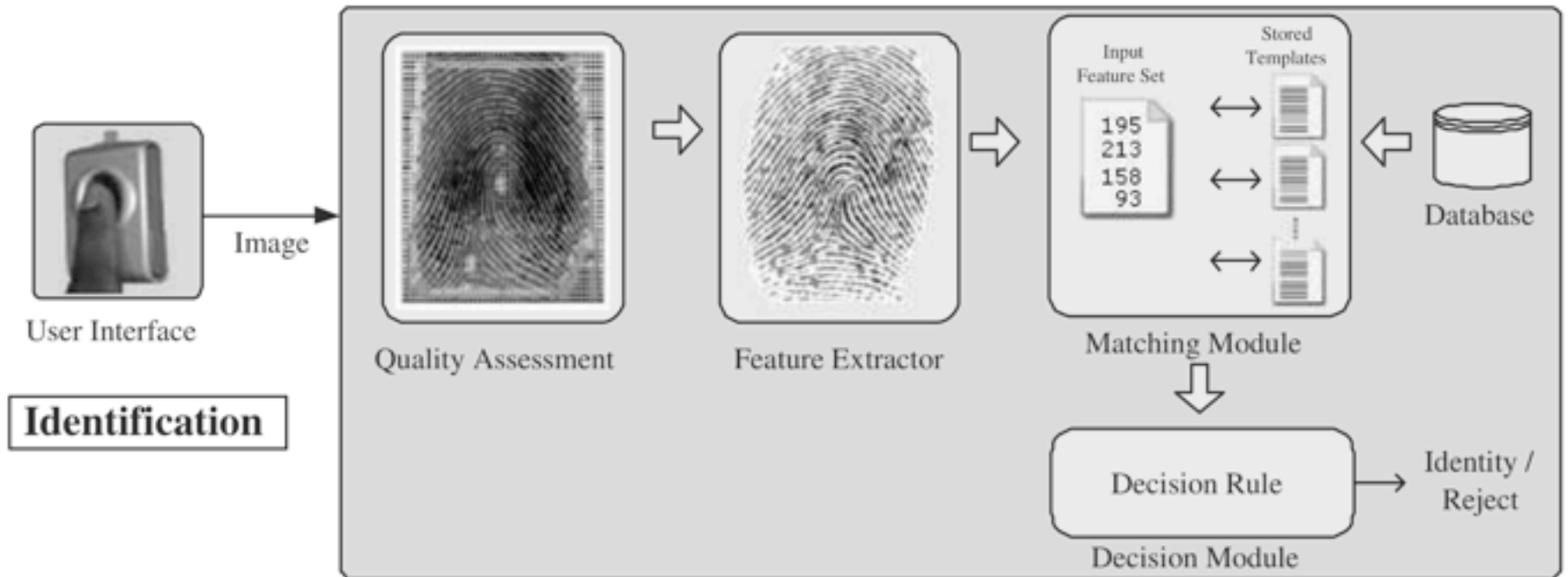
Jain, Ross, Nandakumar: *Introduction to Biometrics*, Springer, 2011

Verification (1 : 1)



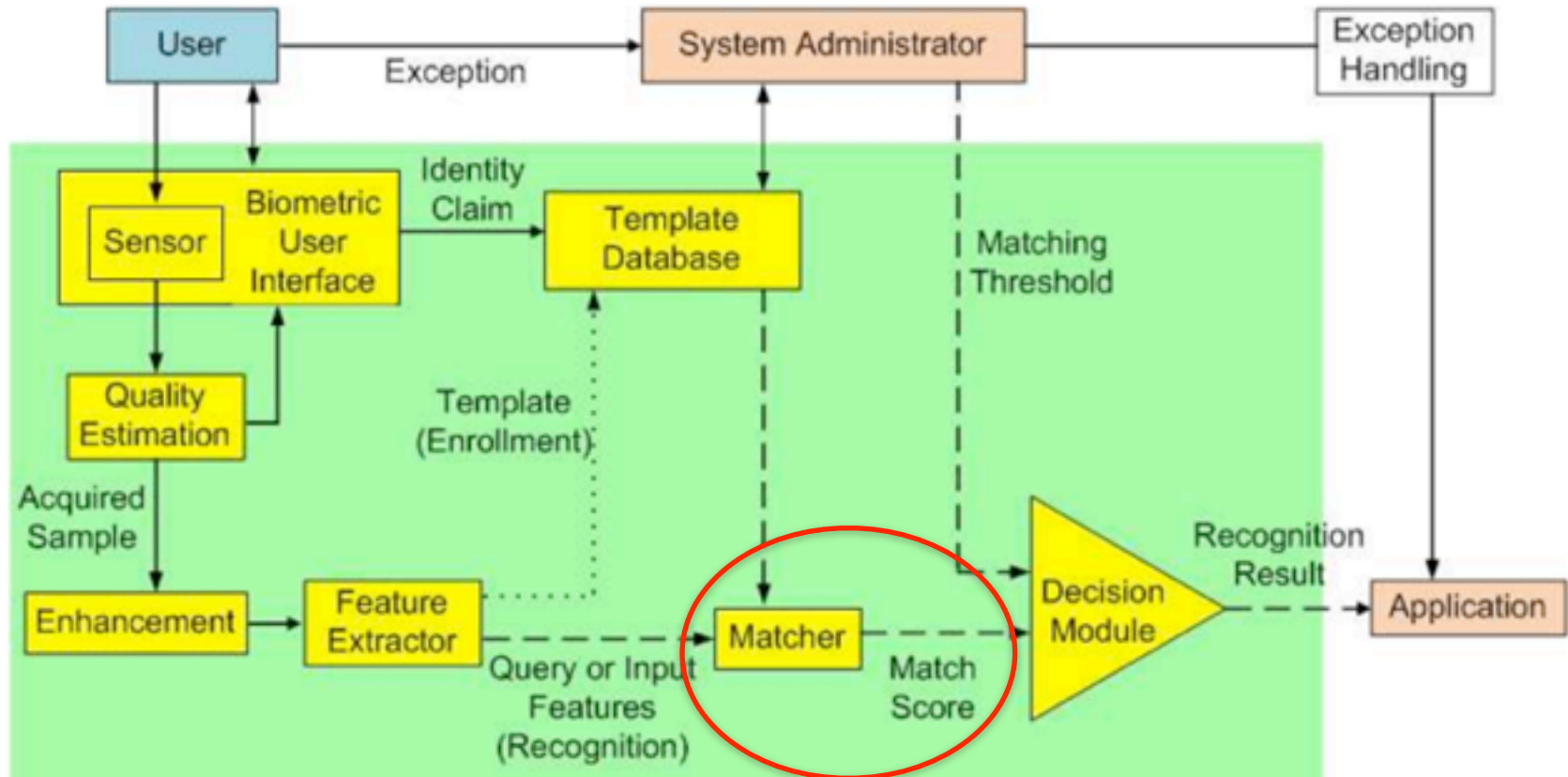
Jain, Ross, Nandakumar: *Introduction to Biometrics*, Springer, 2011

[Identification (1 : N)]



Jain, Ross, Nandakumar: *Introduction to Biometrics*, Springer, 2011

Biometric System Topology

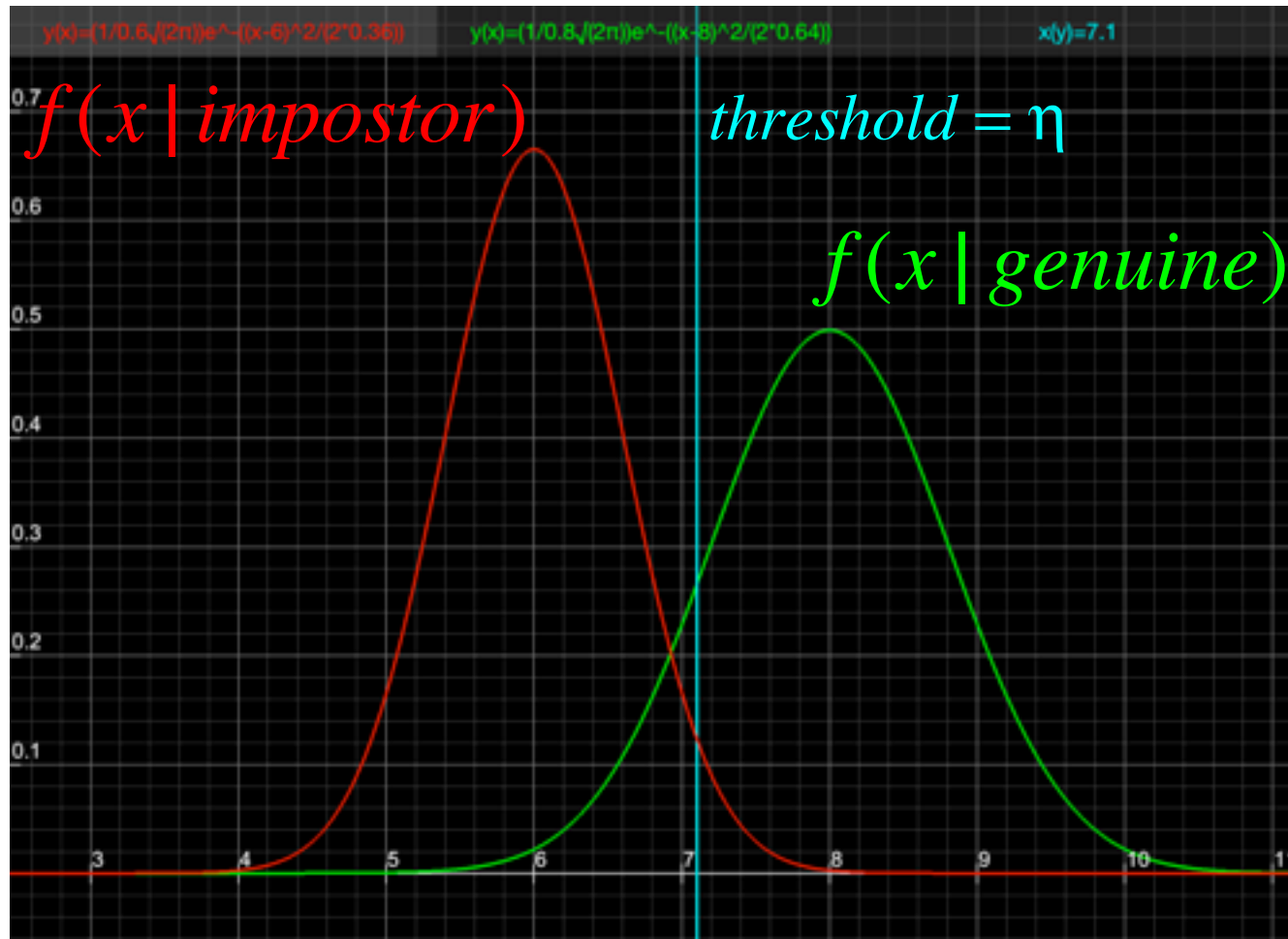


Jain, Ross, Nandakumar: *Introduction to Biometrics*, Springer, 2011

[Match Score]

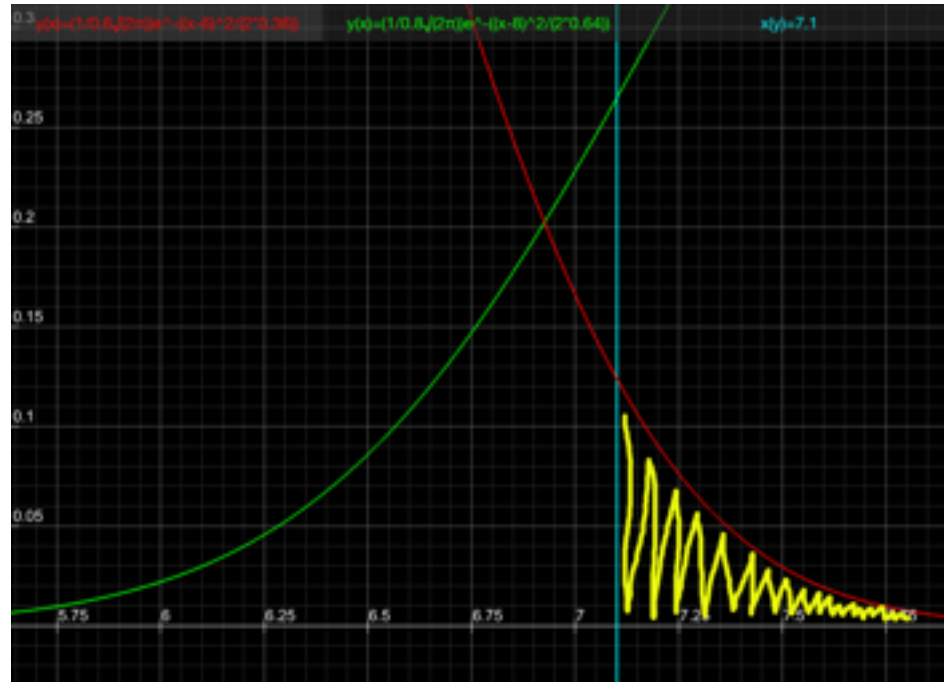
- It would be nice if we had simple **true/false** result.
 - As in conventional crypto.
 - But we cannot...
- All we have is a random variable X that follows two conditional distributions.
 - $f(x \mid \text{impostor})$
 - $f(x \mid \text{genuine})$

[Match Score Evaluation]



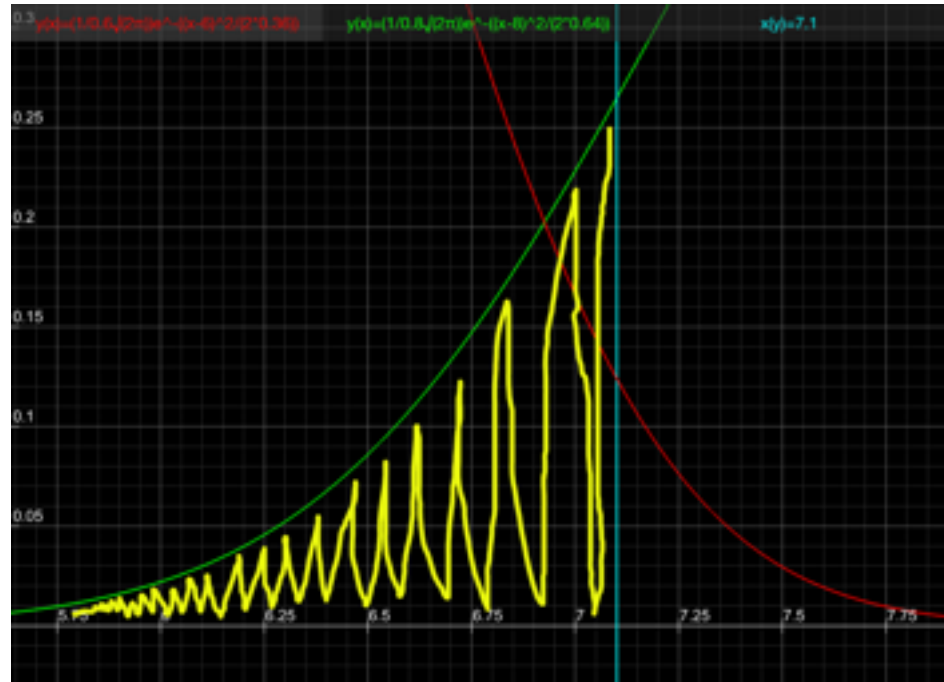
[False Accept Rate]

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

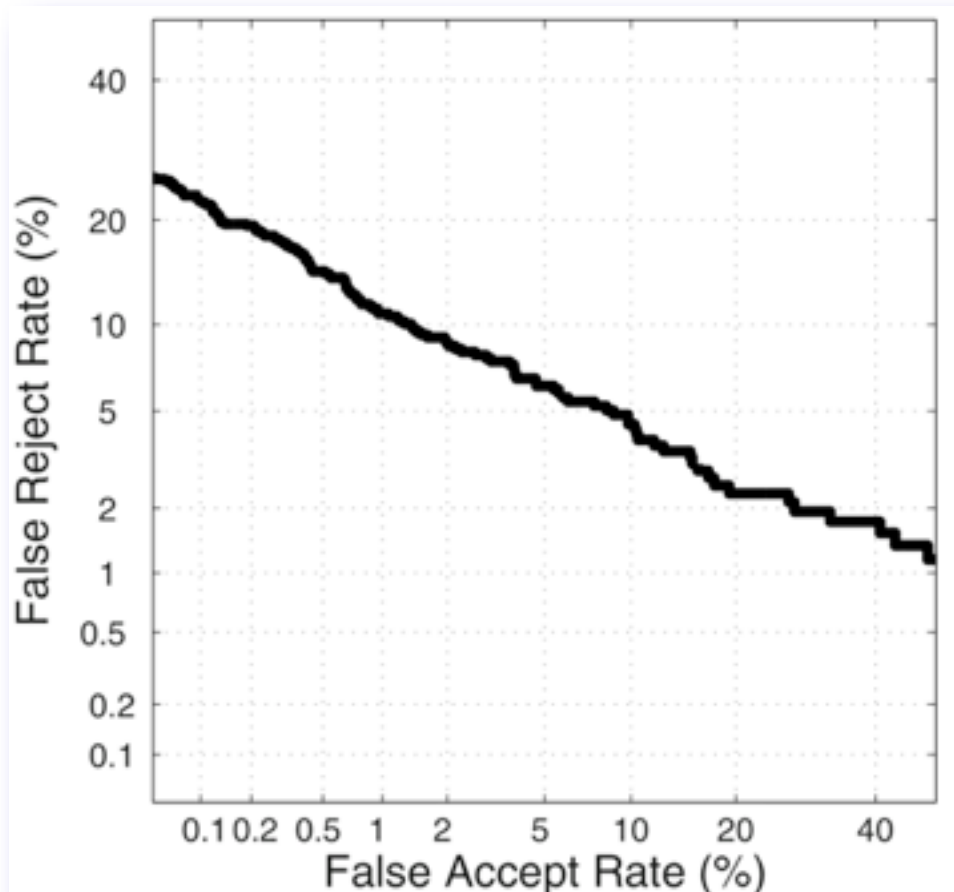


[False Reject Rate]

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



[Real DET Curve]



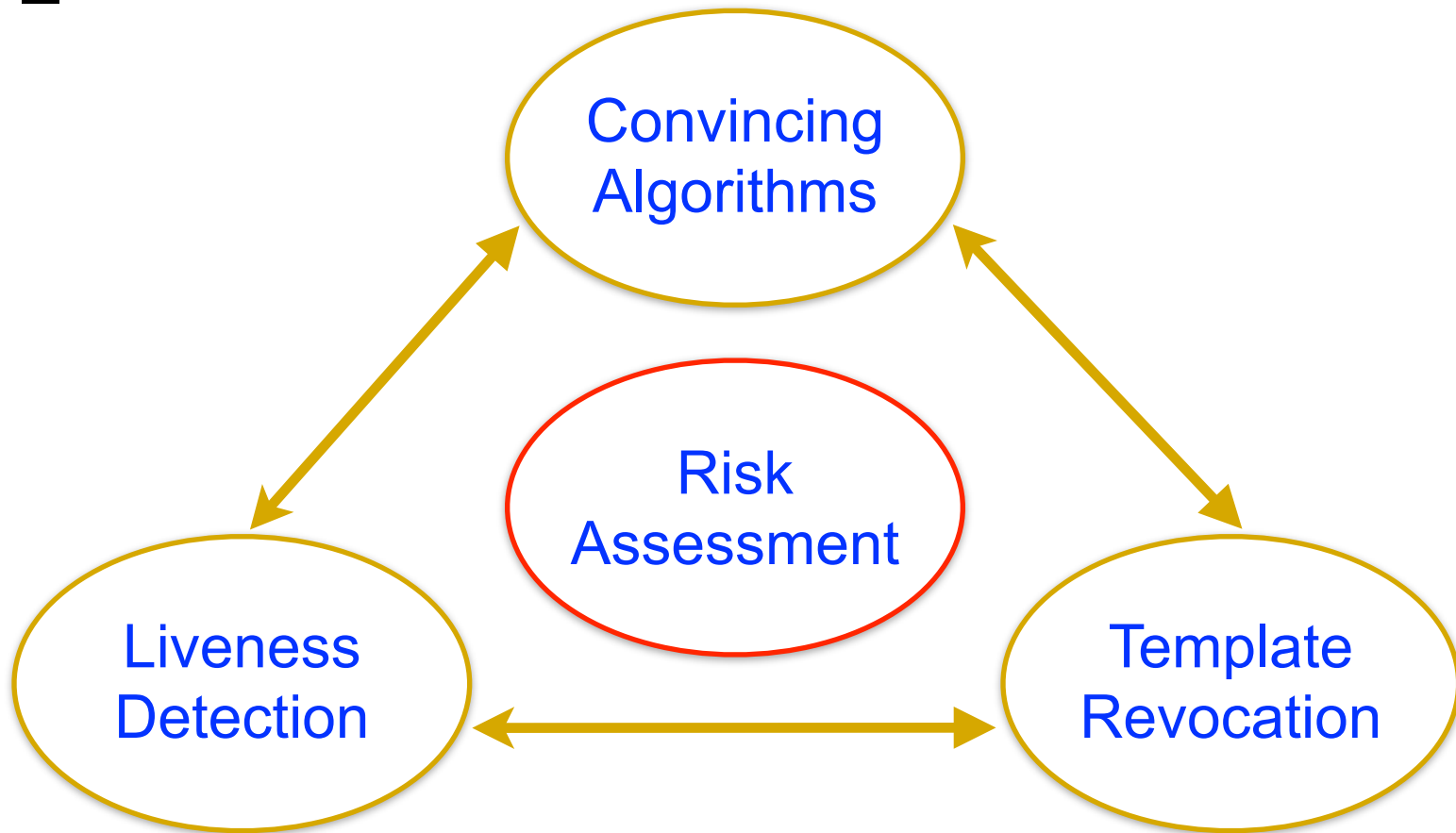
Detection Error Tradeoff

Jain, Ross, Nandakumar,
2011

[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

[Open Problems]



Convincing Algorithms



Liveness Detection Demystified





Safe Template Revocation

[Conclusion]

- We have the best security mechanisms we ever had.
- However, the attacks intensity is also very high and still increasing.
- The threat model is changing significantly.
 - New attacks induced by new use-cases, rather than by e.g. astonishing cryptanalytic advances (X-platform, SSL/TLS, etc.).
- Biometric identification is here and we have to face it.
- We really need to move very fast to even stand still.

--JFK

[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
- *Slunce, seno, jahody*, ČR, 1983
- *Císařův pekař*, ČR, 1951