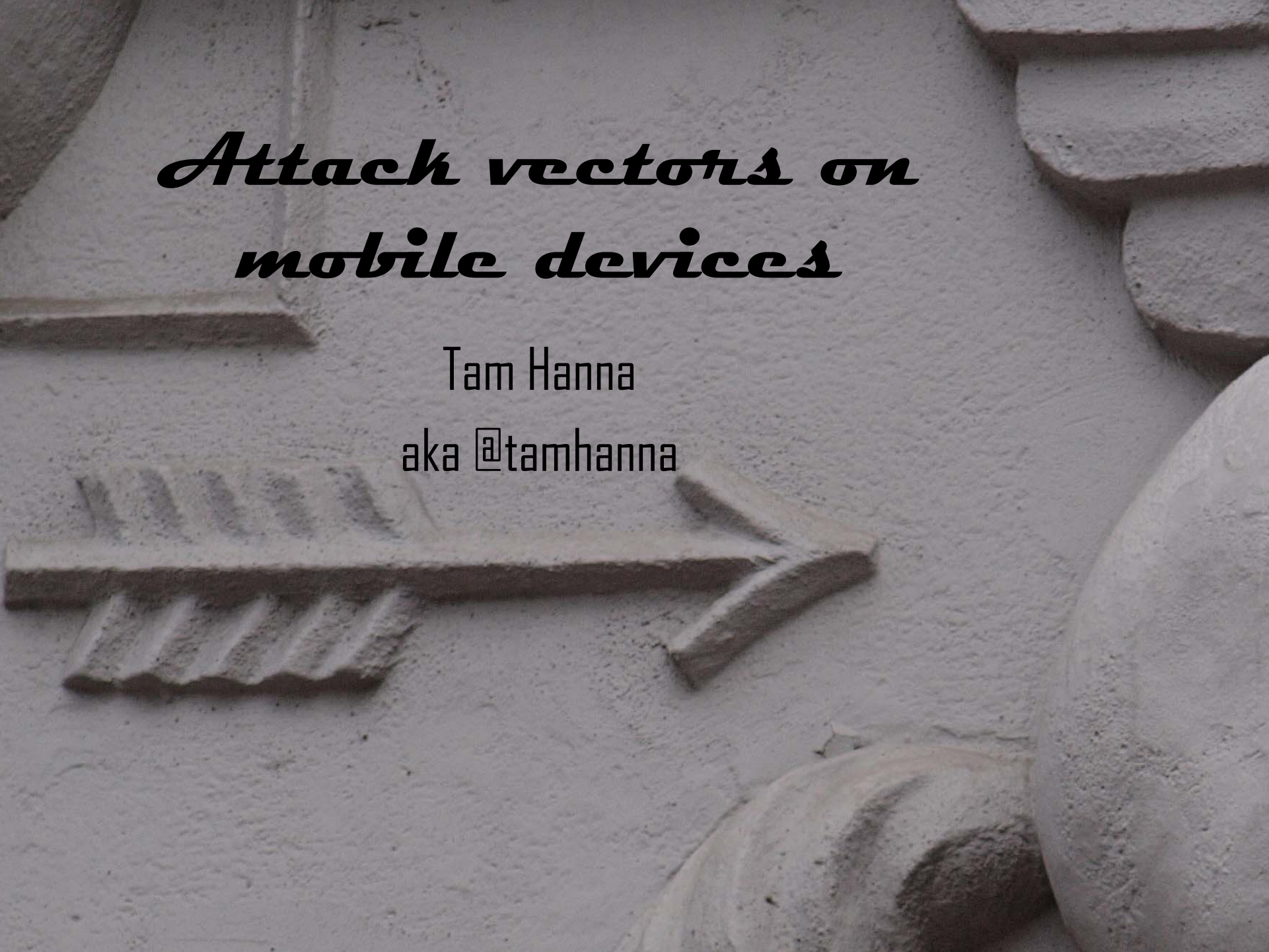
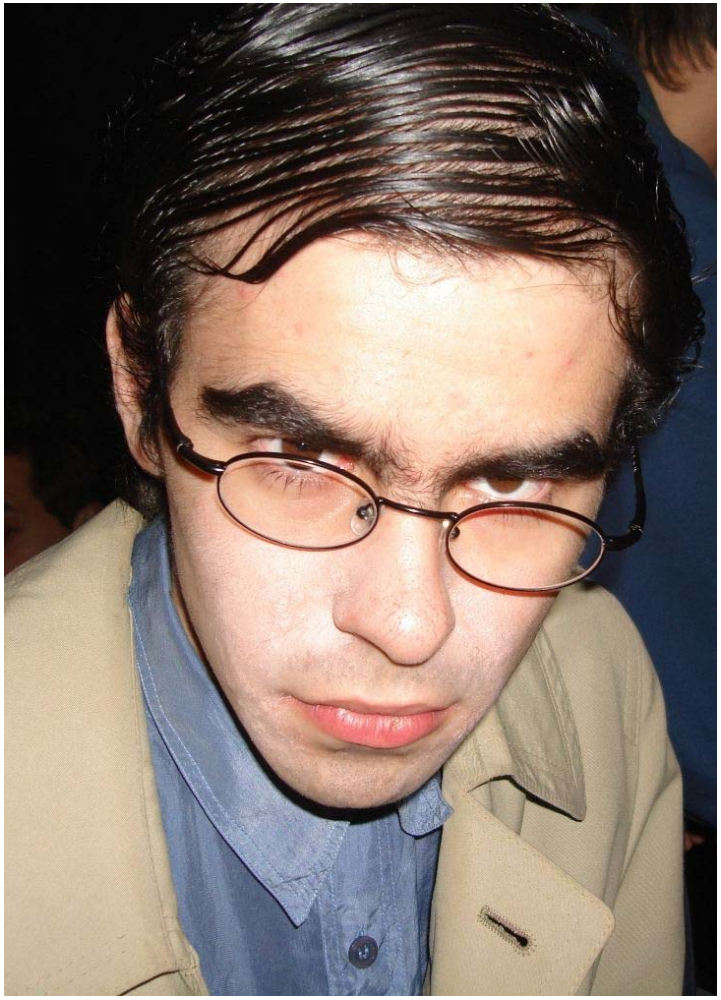


Attack vectors on mobile devices

Tam Hanna

aka @tamhanna

About /me



- Tam HANNA
  - CEO, Tamoggemon Ltd.
  - Runs web sites about mobile computing

Starting thoughts

Different user perceptions

- Mobile phones are always on the user
  - More personal
- User feels that unit "is safe"
  - No large-scale outbreaks so far
  - User is unwilling to accept implications of AV software

Users are stupid

- Cabir displayed THREE warning alerts
  - Perimeter security is not enough
- Users choose dancing pigs over security
  - Ed Felton

Soft targets

- Programmers unaware of security issues
  - HTC's Bluetooth FTP issue
  - AllAboutSymbian hack
- Systems too weak to run large AV software
  - Power drain

Open operating systems

- Symbian, etc are on the march
- Full OS access
- **Less dumbphone, more smartphone**

Smartphone = powerful

- Today's smartphone has
  - Fast CPU and Internet
  - Seamless PC connection (drive mode)
  - Access to user's wallet (in app purchase)

- Plus, the classics
  - Premium rate numbers

Carriers can't do it alone

- GSM / CDMA
  - Can be protected
- Bluetooth
  - Can't really be protected by the carrier
- WiFi
  - Don't even ask


Physical attacks
Gim'me your wallet!

Teenage thugs - I

- Phones stolen for
  - Personal usage
  - Resale
- Rampant issue in Western Europe

Teenage thugs - II

- Carriers love theft
  - Users have to buy another phone at full rate
  - Possible gain of another user

- Carrier CEO: **people with stolen phones are customers as well**

Teenage thugs - III

- Manufacturers love theft
  - Larger sell-through
  - Larger marketshare

Teenage thugs - TV

- IMEI blacklisting works
  - e.g. UK

- **Government must enforce it**
  - **Is unwilling due to PR reasons**

Targeted attacks

- Interest: data

- Trick theft
- Memory card theft
  - Usually unencrypted


NOKIA
135m Hanbury Street
Hanbury Street
Options
Stop
NOKIA
All activity
Options
Close
NOKIA
vodafone
Options
Symbian
the unseen threat

Symbian Signed

- App must be signed to access stuff
  - Express Signed available

- Not signed – no access (!)

The Process - I

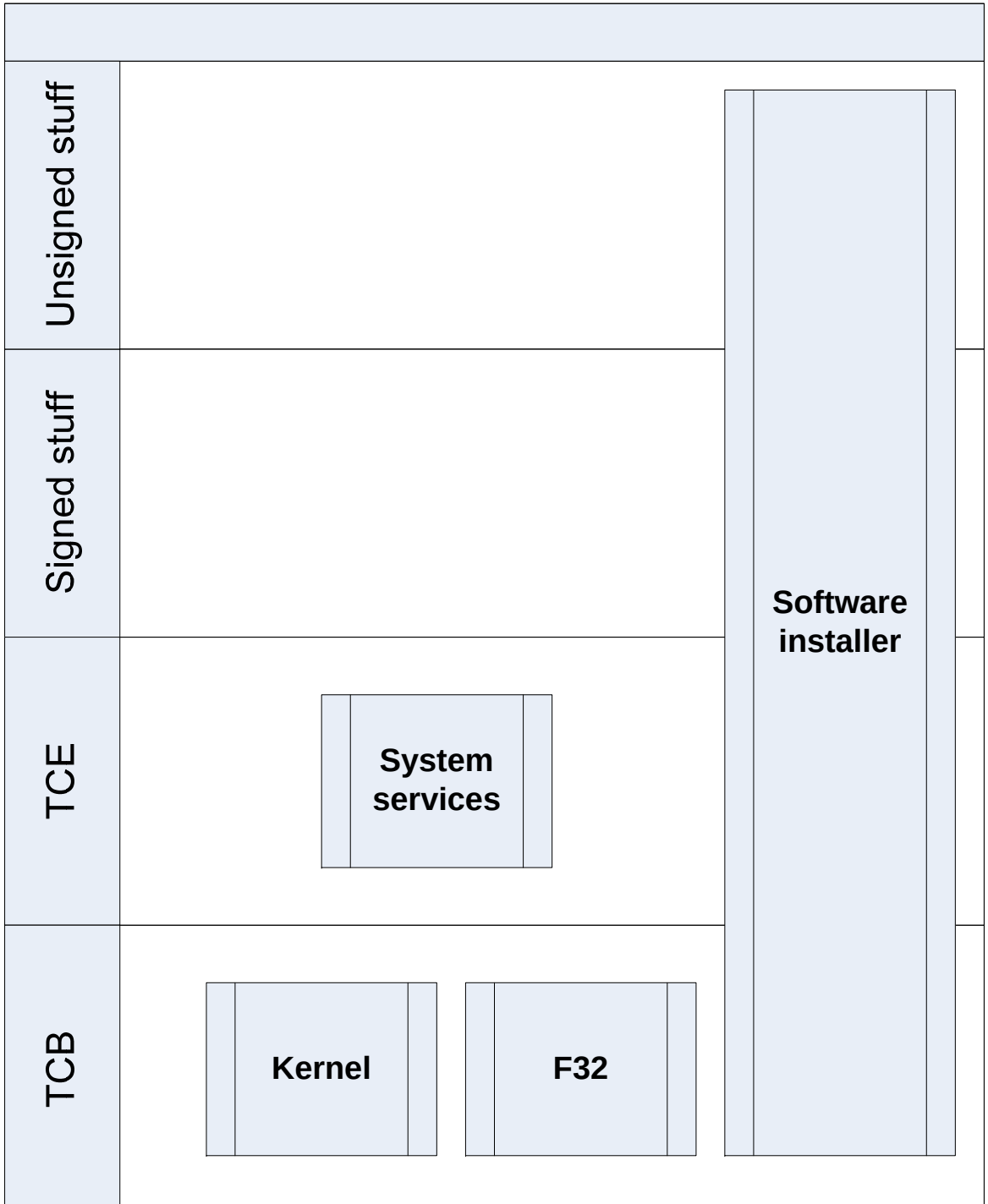
- Mobile phone users are usually "authorized"
  - No multi-user phones
  - PIN Authentication
- User-based rights management doesn't make sense

The Process - II

- Processes are the smallest sensible unit
- **The Process is the Unit of Trust**

- 1 process = 1 app

- Processes are divided into tiers


Unsigned stuff
Signed stuff
TCE
TCB
System services
Kernel
F32
Software installer

The capability

- **A capability is a token which must be presented to gain access to a privileged service**
- Come in three classes
  - TCB
  - System
  - User

The capability - II

- TCB Capabilities: TCB
- Granted to TCB processes only
- Lets them do things nobody else can

The capability - III

- System Capabilities
  - Not meaningful to user
  - Granted by a signing house
- User Capabilities
  - "Not really dangerous"
  - Granted by user (like J2ME)

Data caging

- Access to some folders is restricted
- Provides “secure storage”

- But: MMC/SD readers

Data caging - II

Path	Read	Write
/sys	AllFiles	TCB
/resource	-	TCB
/private/mySID	-	-
/private/notMe	AllFiles	AllFiles
/other	-	-

Developer certificate

- Intended to permit testing of application
  - Open almost all capabilities
- Bound to IMEI
  - One cert: 1000 devices

Developer certificate - II

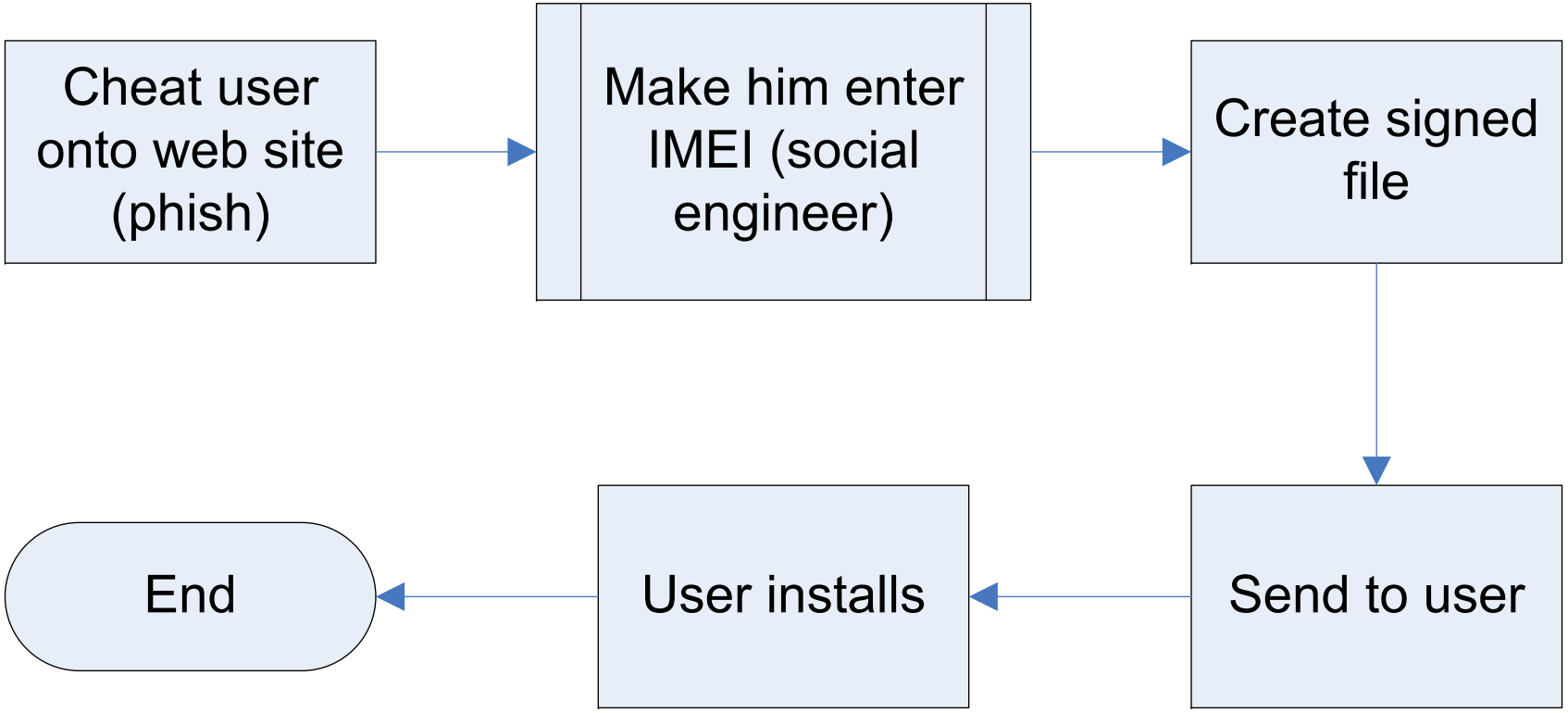
- Obtained by
  1. (Getting TrustCenter ID)
  2. Requesting Cert
  3. Requesting more certs

- Cost: 200 USD for TrustCenter
  - Requires capital company (Limited)
  - bc of OMA DRM bylaws

Dev Certs eat rice

- http://cer.opda.cn/en
- Generates DevCerts for everyone
- Sits in China

Attack flow - SpitMo



Improvement idea

- Generate certificate automatically
- Then, perform update

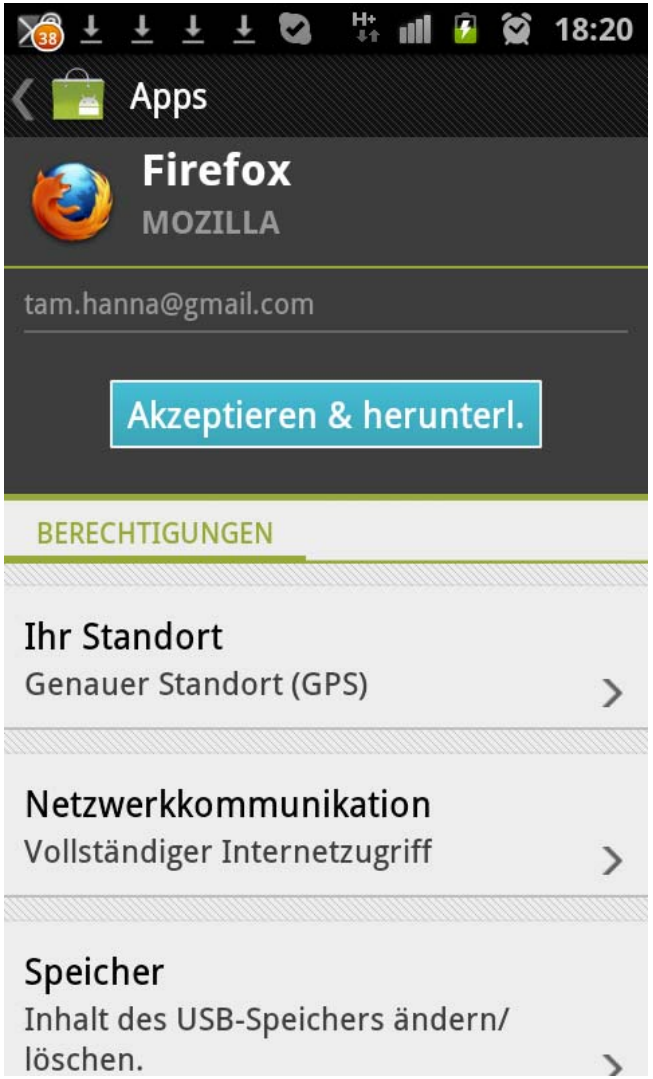

Android
Open for (dangerous) code

Android in 2 min

Android in 2 min - II

- Cloning apps is easy
- Java code can be decompiled
- Add ads, reupload
  - Ban on Google Market? Go to ESD!

Android in 2 min - III



- Security model is „transparency based“
- Apps can come from anywhere
- **USER decides**

Attack scheme

- Always the same
  1. Get onto phone
  2. Do funny stuff
     - Send data to master
     - Call premium rate number

DroidKungFu

- Abuses Android security model
- Updates are checked less stringently

DroidKungFu - II

- After installation, update is offered
- Update contains exploit
- **Gets root on some phones (why??)**
  - **Does nothing with these rights**

Carrier IQ

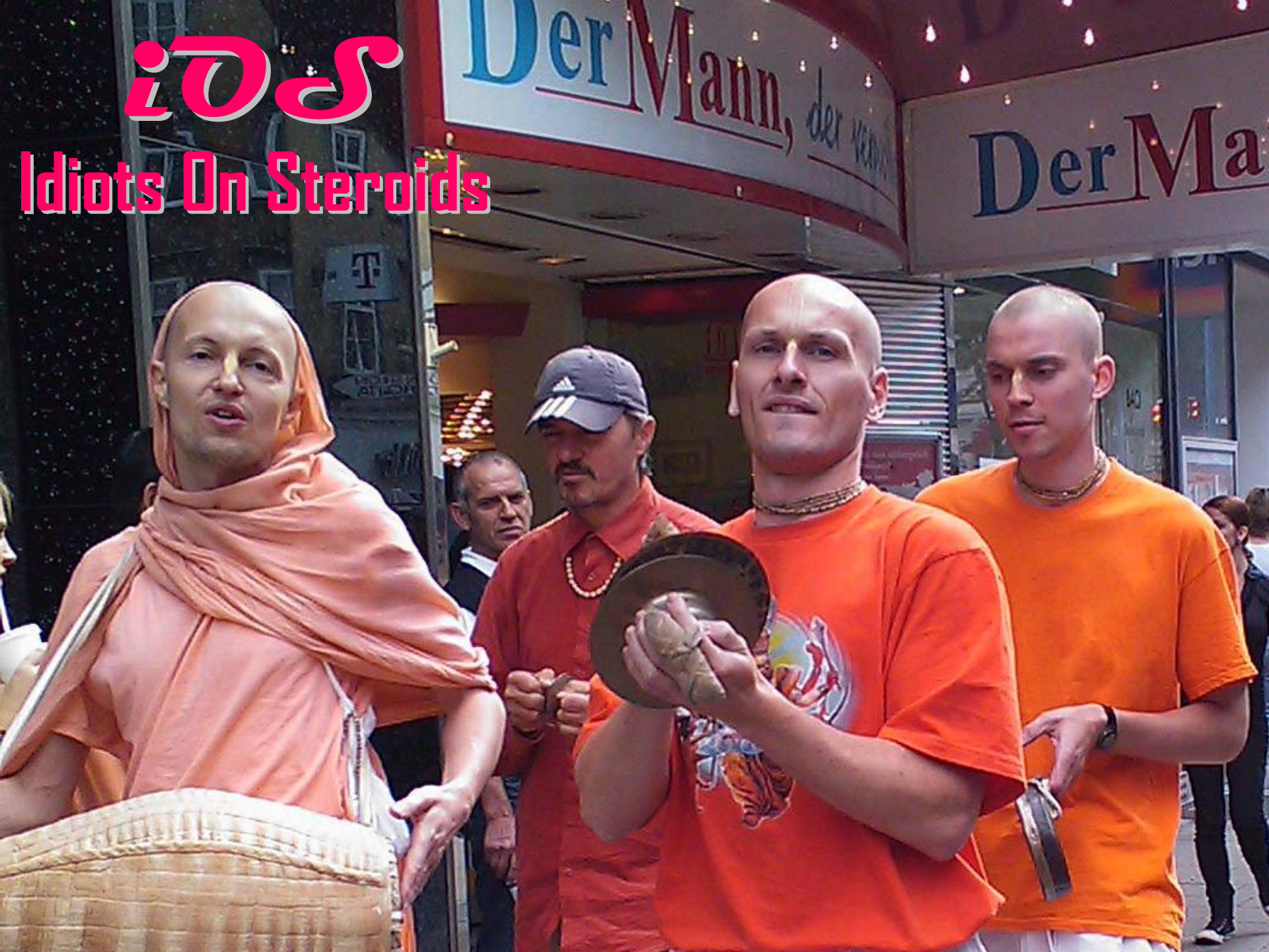
- Discovered by Trevor Eckhardt
- Created by a company
  - Won Fierce 15 in 2008
- Lives on multiple platforms
  - Comes as “gift from carrier”
  - Also on BB and iOS

Carrier IQ - II

- Records a LOT
  - App Opened
  - SMS received
  - Screen on/off
  - Call received
  - Location
  - Media

Carrier IQ - III

- Sends data to portal via HTTPS
- Visible to everyone in portal
- User can NOT opt out


iOS
Idiots On Steroids
Der Mann,
Der Ma

Dis Da EiFon Feif

JailBreakMe side effects

- If a web site can get root, so can a criminal
- So far, little used
- IDEA: www.freelouboutins.com

„RenRen“

- GERMANY only
  - Little interest by security professionals

- No idea how it installs itself (ad?)

„RenRen“ – II

- Somehow abuses iOS in app purchase
- Either:
  - Social engineering to get PW
- OR
  - Exploit in iOS

TAMHAN goes crazy

- Strange shit:
  - Non iOS owners get attacked, too
  - www.spiegel.de/netzwelt/apps/0,1518,796353,00.html
- This tells us: could it be phishing?
- Google „人人乱世天下“

TAMHAN goes crazy - 99

TAMHAN goes crazy - III

- Manufacturer string only partial
  - „Beijing Quianxiang Wangji “
- Brings us to a Chinese professor

TAMHAN goes crazy - TV

Qianxiang Wang 王千祥

Ph.D, Professor

Institute of Software, School of Electronics Engineering and Computer Science,

Peking University, Beijing, China

E-mail: wqx at pku.edu.cn, Tel: 86-10-6275 9074(O)

Research

Middleware: One layer of software that locates between Operating System and Application.

Analysis and Adjusting of Software and Service: Methods and tools for high-confidence software and service.

Developing:SEForge PKUAS

An email

Dear Professor Wang,

please forgive me for getting in touch with you so abruptely – I am Tam Hanna from Vienna, and am doing some research into a strange iPhone application which has caused large money losses to German iPhone owners.

As you can see in this screenshot (http://www.computerbild.de/fotos/Abzocke-im-iTunes-Store-Diese-China-App-klaut-80-Euro-6749398.html#2), the app's metadata contains a string (Beijing Quianxiang Wangji) which, when googled, bring straight to your web site.

I am currently preparing a talk on the topic and wanted to ask you if you know anything which could help me? Could this be part of a smear campaign against you?

Or am I just misunderstanding the string as a non-Chinese speaker.

All the best

Tam Hanna

No Reply

- Sir Wang probably thinks
  - Sha Gua (aka What a moron)

- Unlikely to have anything to do with it

TAMHAN goes crazy - V

- „Mikko cut your hair“
  - Dead end
  - Maybe revenge from student

- Lets continue
  - Second manufacturer string: renren

On RenRen

Renren Inc (NYSE:RENN) executive talks about strategy on browser games. During The 9th China International Digital Content Expo., Chuan He, Senior Vice President of Renren.com, spoke about the company's browser game strategy. **The company owns a game publishing platform where it co-operates games with developers. It also develops and publishes its own games**. Mr. He believes the current trend is that much of people's time spent on PC will be replaced by time spent on mobile devices. Developers of browser games should consider expanding their business to mobile devices. Renren.com currently has about 10 in-house developed games that are operating on its platform and over 50 licensed from third parties. Going forward, **the company believes it will be increasingly shifting toward third-party licensed games in order to leverage the platform effect of Renren.com.**

RenRen is H.U.G.E.

Renren operates an Internet website. Coming of a red hot IPO earlier in the year, they are currently sitting on **over $1 billion in cash and no debt**. For a small company like RENN, I feel that is a massive backstop even if they remain unprofitable for the foreseeable future.

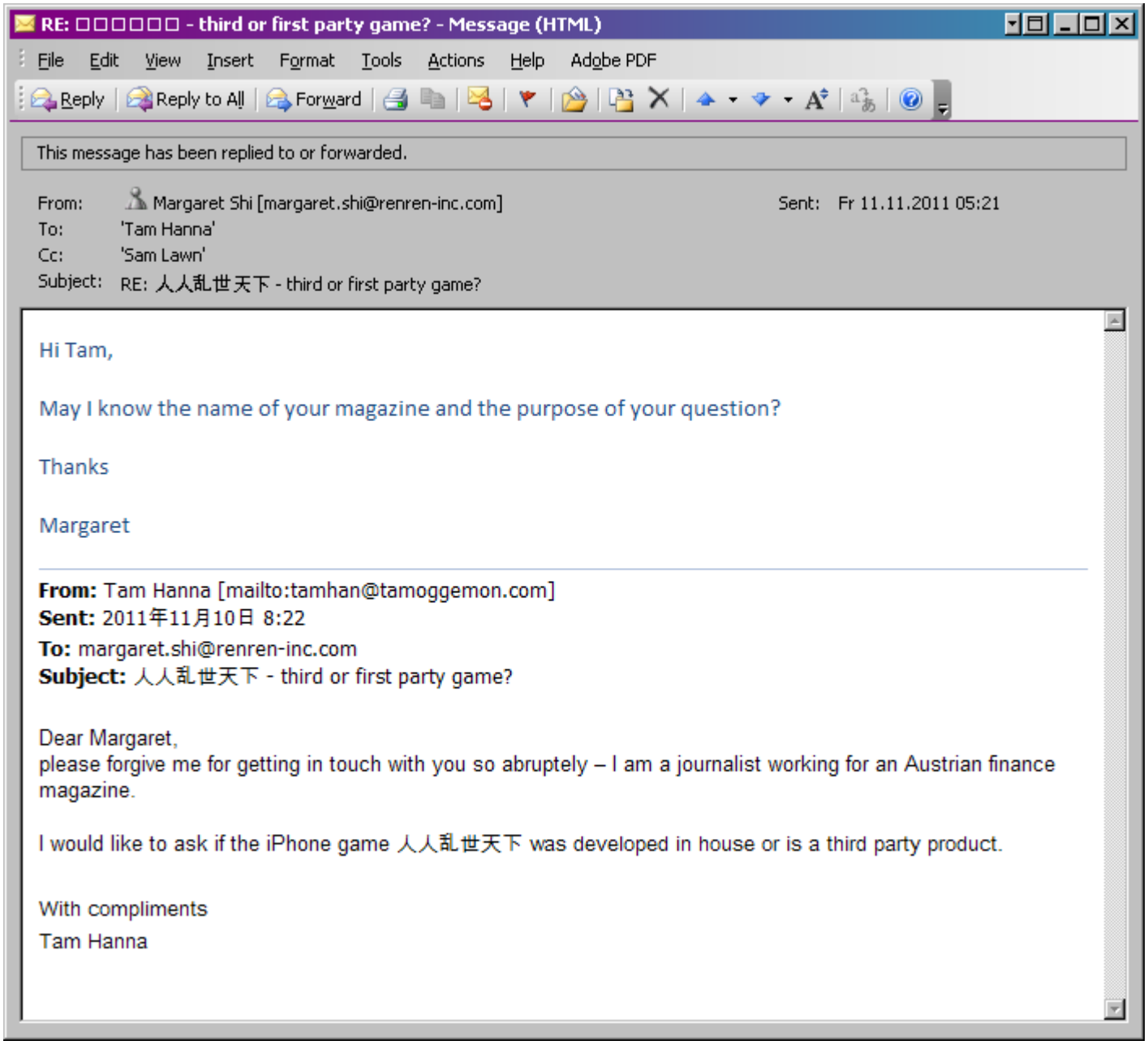
Their real-time social networking website offers users the ability to communicate, share information and content, play online games, listen to music, shop for deals, and use other services.
Read more: http://www.beaconequity.com/smw/14504/Is-Renren-RENN-Stock-Poised-for-an-Earnings-Surprise-Like-BIDU-and-SOHU-#ixzz1dFv6yYEu

Let's email them

- Dear Margaret,
- please forgive me for getting in touch with you so abruptely – I am a journalist working for an Austrian finance magazine.
- I would like to ask if the iPhone game 人人乱世天下 was developed in house or is a third party product.
- With compliments
- Tam Hanna

Response

- Came very fast
- cc'd CHIEF(!!!) of IR
- Unusual response
  - No actual info
  - Asking more info from sender



RE: □□□□□□ - third or first party game? - Message (HTML)

File Edit View Insert Format Tools Actions Help Adobe PDF

Reply | Reply to All | Forward

This message has been replied to or forwarded.

From: Margaret Shi [margaret.shi@renren-inc.com] Sent: Fr 11.11.2011 05:21
To: 'Tam Hanna'
Cc: 'Sam Lawn'
Subject: RE: 人人乱世天下 - third or first party game?

Hi Tam,

May I know the name of your magazine and the purpose of your question?

Thanks

Margaret

From: Tam Hanna [mailto:tamhan@tamoggemon.com]
Sent: 2011年11月10日 8:22
To: margaret.shi@renren-inc.com
Subject: 人人乱世天下 - third or first party game?

Dear Margaret,
please forgive me for getting in touch with you so abruptely – I am a journalist working for an Austrian finance magazine.

I would like to ask if the iPhone game 人人乱世天下 was developed in house or is a third party product.

With compliments
Tam Hanna

Response was sent

Hello Margaret,

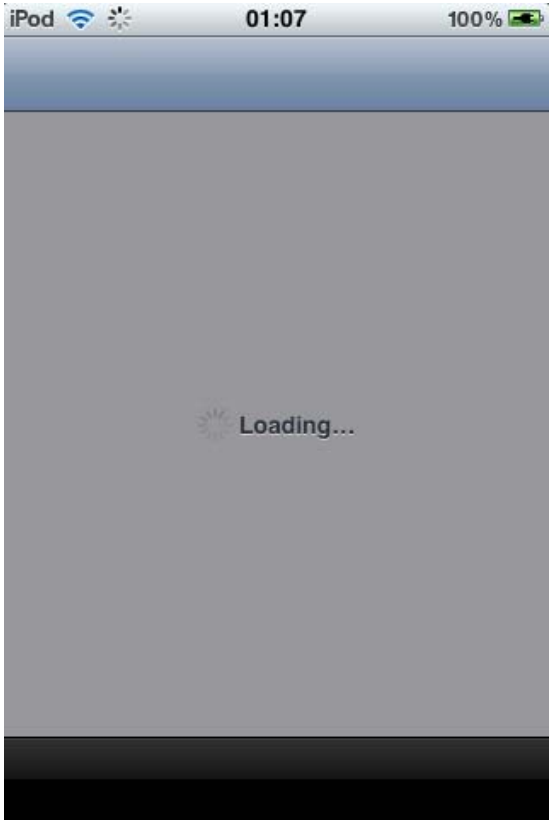
thank you so much for your email! I am working for the Software and Support media company on this assignment, the target will likely be the Entwicklermagazin.

I am interested in this game because it has made quite a splash in Germany recently due to the creative use of in app purchases – it was the top three grossing app for some time!

All the best

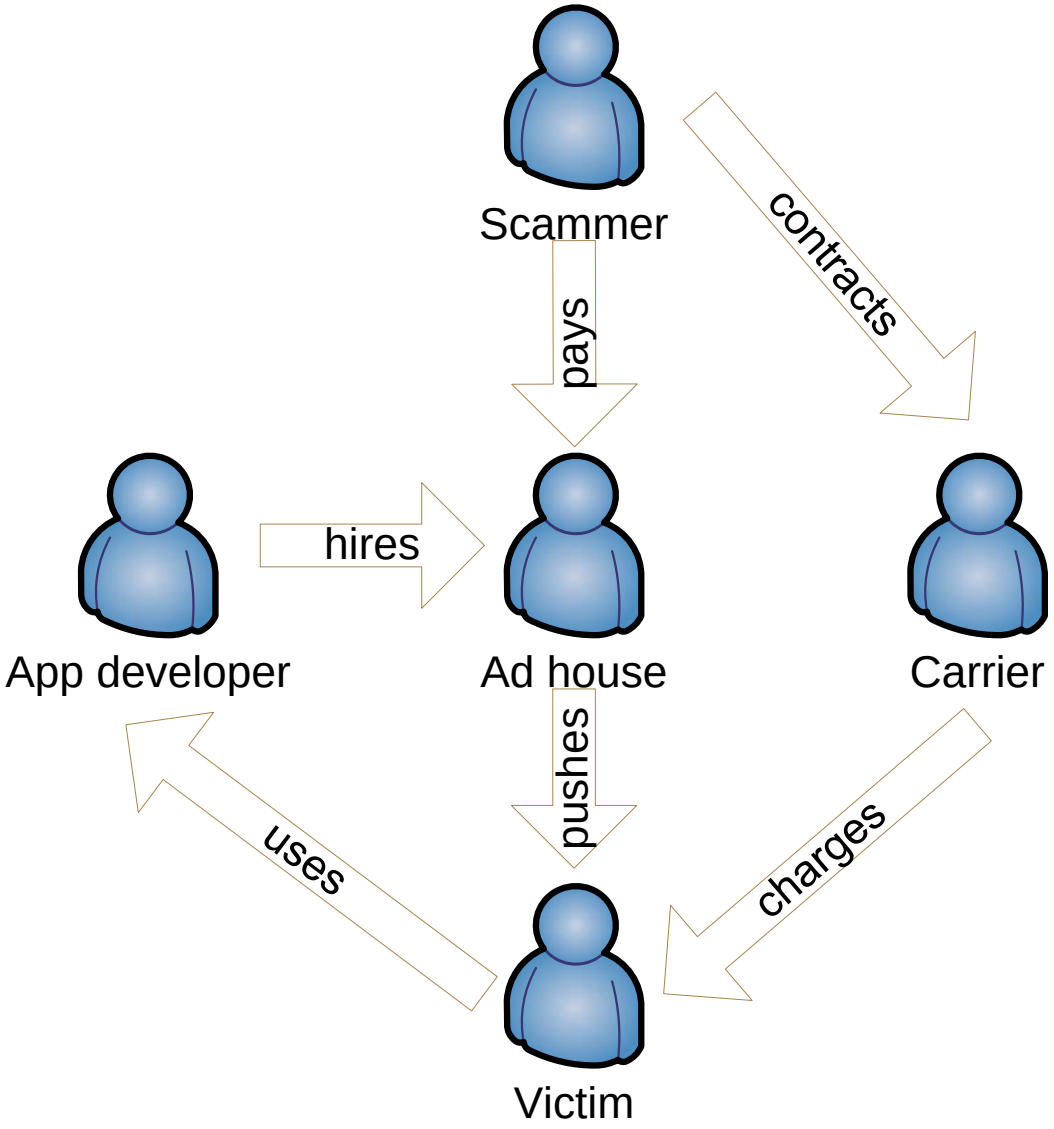
Tam Hanna

WAP „scams"



!!! NON-MALICIOUS APP !!!

WAP „scams" - II


Scammer
contracts
pays
hires
App developer
Ad house
Carrier
pushes
uses
charges
Victim

WAP „scams" - III

- User clicks ad
- WAP request for web site
- MSISDN transmitted
- Carrier charges

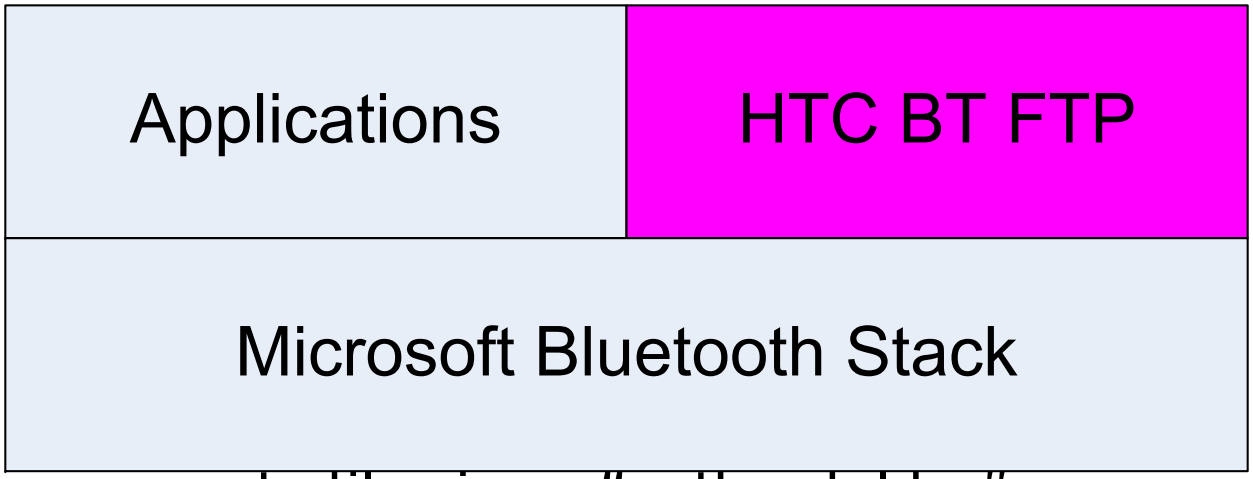

Staff questions

Programmers are unaware

- Security is perceived as a non-issue
  - Coders are unaware of risks
- No real "secure chain"
- **Loads of (unfound) exploitable errors**

HTC's Bluetooth FTP - I

- Bluetooth FTP is a "bonus service" from HTC



- Allows access to files in an "outbox folder"

HTC's Bluetooth FTP - II

- Well-mannered client
  - Detects top-level folder
  - Does not allow further traversal

- Bad-mannered client
  - Sends .. Command in root folder
  - Gets full device access

HTC's Bluetooth FTP - III

- Perimeter security works
  - Non-trusted clients can not access BT-FTP
  - Careful pairing keeps users safe

- Practical risk: low

On attackers

- Technically
  - Not particularily smart
  - Attacks = Normal apps
  - No „advanced“ code (YET)
- Socially smart
  - Mobile attack == Social Engineering

On attackers - II

- Greedy
  - No „Den Zuk“ attacks
  - No „I Love You“ tomfoolery

- Effect (IMHO)
  - **No technical development unless it is needed to make money. Current attacks make money, so . . .**

New ideas

Data theft to go

- FlexiSPY
  - Logs SMS
  - Logs calls
  - Question: is my wife safe to bonk?

- But now, for profit
  - Question changes: credit card, please

Exploits

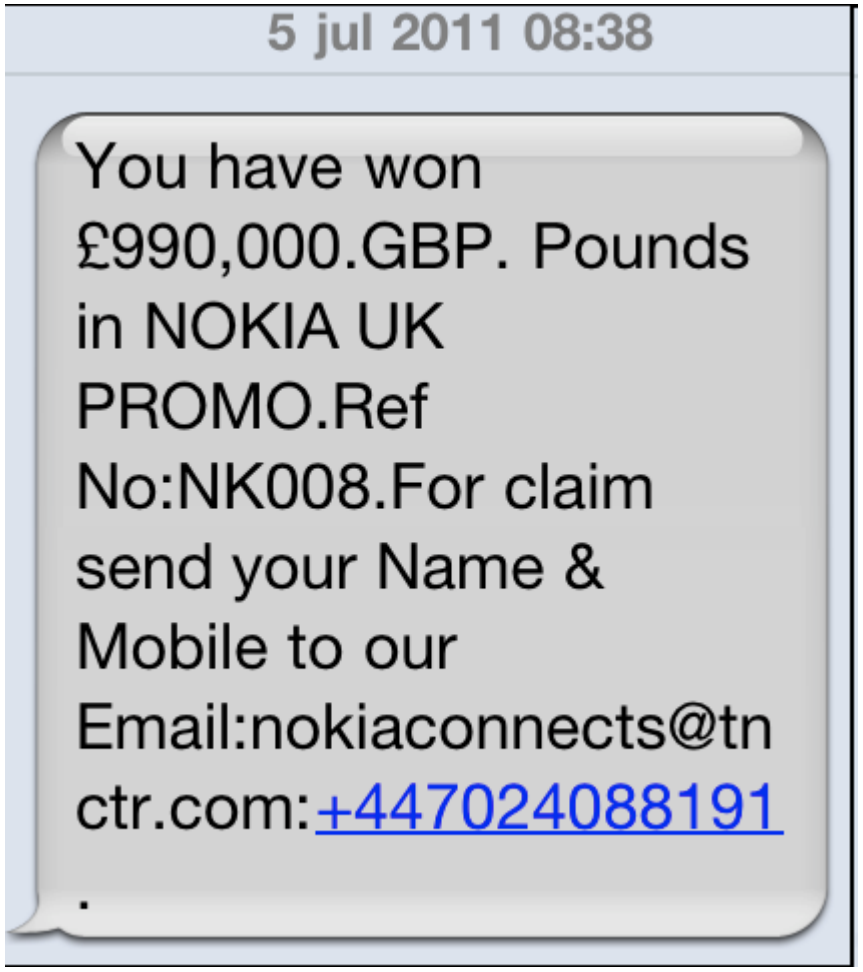
- Tons of them still open
- Who finds one first?

PC-Phone-Bridge

- Infect the PC AND the phone
  - No more local sync -> eek
  - But: autostart and USB drive mode == fun

- Has been done before
  - Palm OS infected after PC

Mobile scams



Via F-secure

Thank you!

?!? - !?!

tamhan@tamoggemon.com

@tamhanna