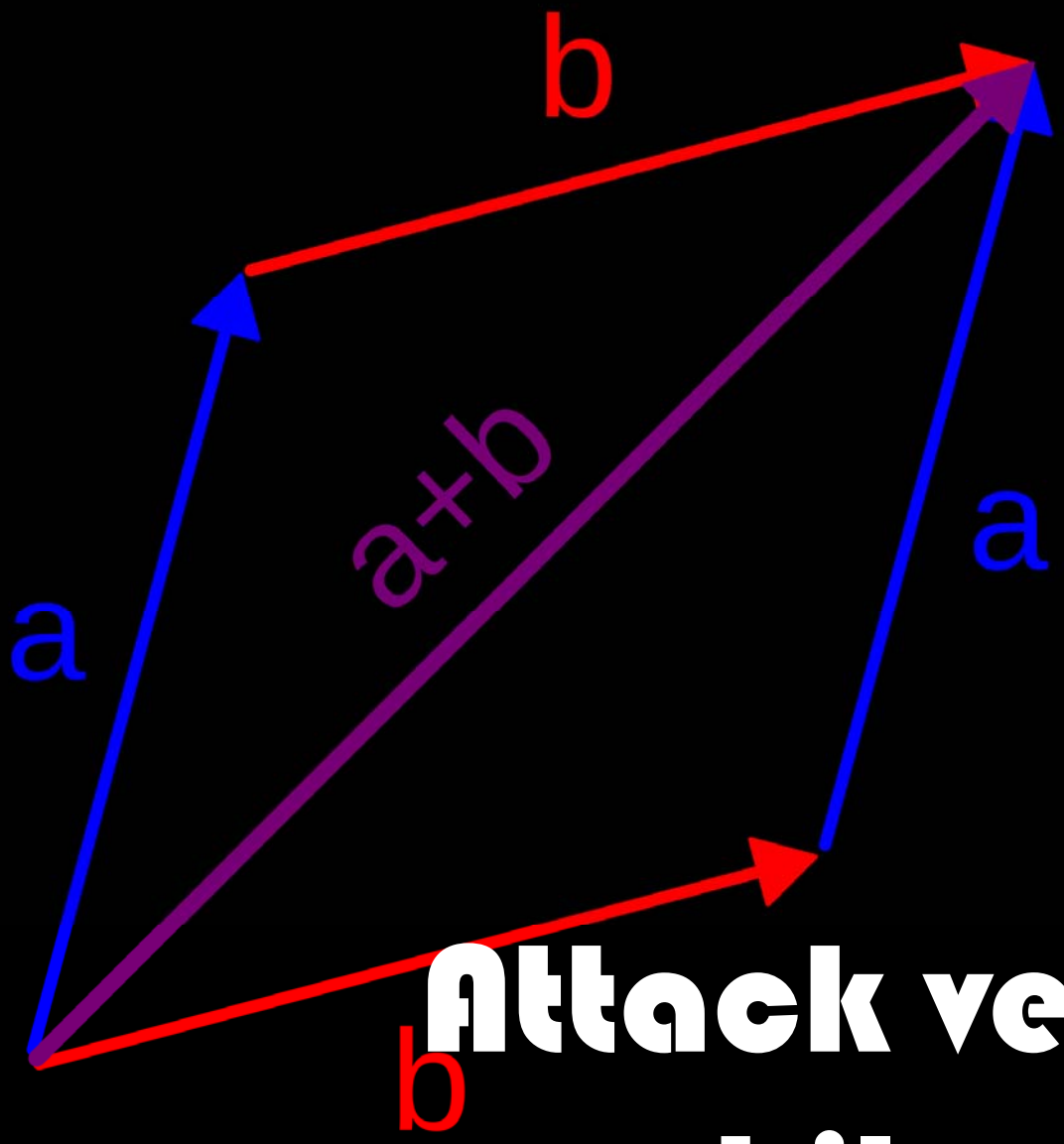


Attack vectors on mobile devices

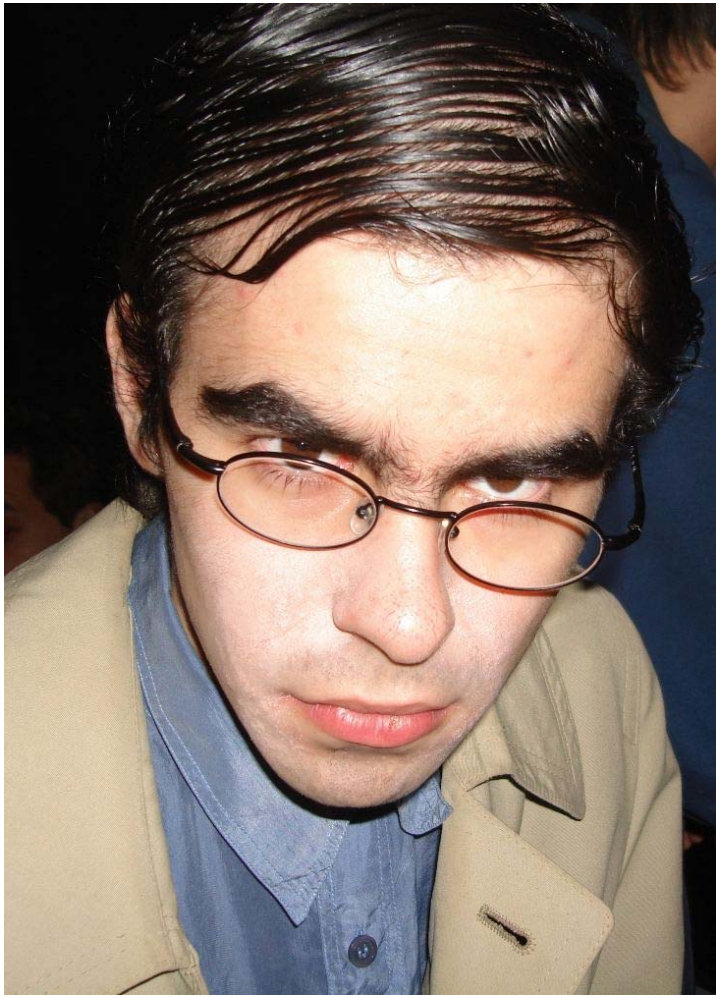
Oh, what horrors have we created

Overview of topics

- Why attack mobiles

- Physical attacks
- Malware
- Exploits
- Scams

About /me



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

Why attack mobiles

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

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**


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 - IV

- 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

Malware

Why Malware

- No AV protection
- “Can-do”-factor

Why no malware

- Non-homogenous OS landscape
- Code signing, etc
- Low-power devices
  - Makes hiding difficult

libertyCrack

- Targets Palm OS devices
  - Deletes data, etc
- Developed as a test for "CleanSweep4Palm"
  - Testers broke NDA

- **First "outbreak"**

Phage

- First "self-replicating virus"
  - Partially overwrites first code segment
  - Damages host
- Infects all other PRC files
  - PDB data is left alone

MTX_II.A

- "Greeting card application"
- Dispatched by Windows virus

The Nokia 7650

- Symbian OS
- Bluetooth
- MMS / TCP/IP – capable
- Blockbuster

Cabir A

- Spread via Bluetooth only
- No real harm done
  - Power drain
  - Nuisance
- Proof of concept, leaked out

Mabir / CommWarrior

- Cabir + MMS
- Causes high phone bills
- **Ouch!**

S60v3

- Renamed due to virus problems
- Introduces mandatory signing
  - Binary break
- **More in next talk**

FlexiSPY

- Managed to get signed
- "Total remote control"
- But: must be installed by hand
  - Not really malware, but worth a mentiomn


Scams

Call me back

- User is called via premium-rate number
- Call is terminated before user picks up
- Uncareful user calls back

Pay-or-Pay

Sent from: premium-rate number

Do not want to disturb you, but you have just used up 10 Euros. Enjoy!

Premium-rate SMS

- (Austria-specific issue)

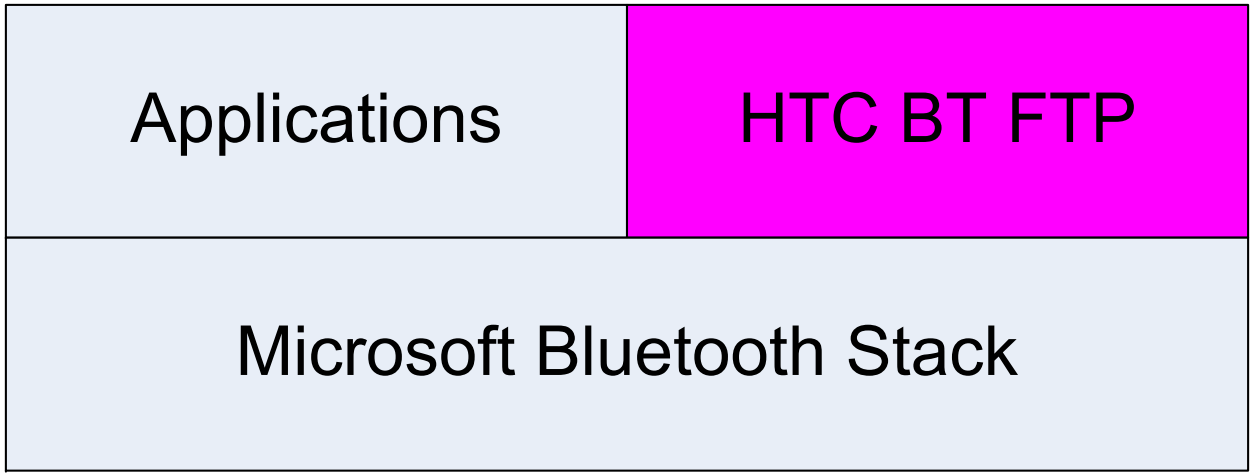

Exploits

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

iPhone SSH - 1

- Jailbreaks are "fun"
  - Free tethering
  - Unlocking
  - Various other features
- Jailbreaks are easy
- Dumb users jailbreak

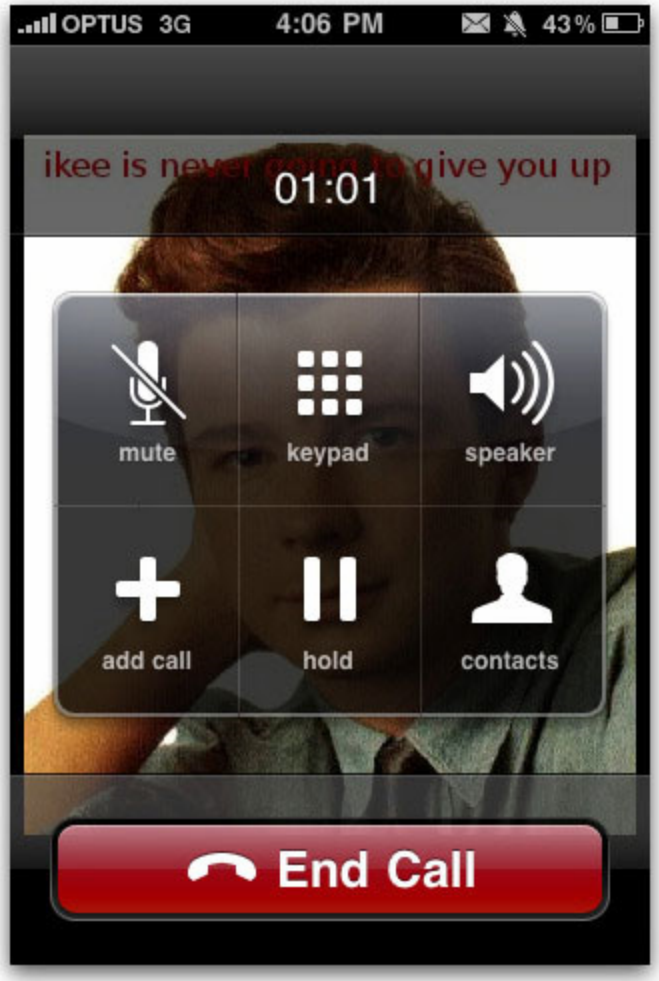
iPhone SSH - 2

- Some packages install an SSH server
- Default password is not changed

- **alpine**

iPhone SSH - III

- Loads of vulnerable devices on networks
- Attacks go 1-2-3



iPhone SSH - IV

1. Port scan
2. Connect
3. Install exploit
4. Enjoy

The end

Questions?

Answers at tamhan@tamoggemon.com

Photos by tomisti, Willtron, Holger.Ellgaard, Booyabazooka .