

# The cybercrime threat on mobile devices

Chris Mitchell

Royal Holloway, University of London

[www.chrismitchell.net](http://www.chrismitchell.net)

# Agenda

1. Introduction – mobile devices
2. The security landscape
3. The problem – case studies
4. The way forward
5. Concluding remarks

# Agenda

1. Introduction – mobile devices
2. The security landscape
3. The problem – case studies
4. The way forward
5. Concluding remarks

# Mobile devices

- A wide range of mobile devices are in use: (smart)phones, media players, tablets, notebook PCs, ...
- These devices are typically network-connected for most of the time they are switched on.
- This poses a well-known (if not well-understood) threat from cybercriminals.

# We all know about mobile devices ...



# But these are mobile too



# More mobile devices

- Apart from the ‘obvious’ mobile devices, a growing number of everyday objects are also ‘always/often connected’, including:
  - cars and lorries/trucks;
  - RFID tags (embedded in all sorts of devices);
  - payment cards (chip/proximity);
  - electronic key fobs;
  - public transport; ...
- These are just the *mobile* devices.

# Cybercrime and security

- Traditional mobile devices (phones, PCs, etc.) have been the main focus of security and privacy concerns.
- Whilst there are very major issues for such systems:
  - perhaps other devices pose an even greater threat?
  - maybe the possibilities for crime (and countermeasures) have not been properly thought through?



# Case studies

- In this presentation, the main cyber threats to mobile devices are reviewed.
- We then look at how these threats apply to some of the less well-studied classes of mobile device.
- The news is not always good ...

# Ubiquitous computing

- One reason for the problems we have, is that systems have evolved piecemeal:
  - there is no overall security architecture for mobile devices.
- As with all IT products, the pressure to release the latest innovation always beats the need for security.
- Systems are interconnected because we ‘might as well’, without thought about the possible consequences.

# Agenda

1. Introduction – mobile devices
2. The security landscape
3. The problem – case studies
4. The way forward
5. Concluding remarks

# Threats

- Key threat classes for mobile devices:
  - **communications-based:**
    - access network impersonation;
    - mobile device impersonation;
    - man-in-the-middle attacks (active/passive);
  - **system-based:**
    - software vulnerabilities;
    - side channel attacks;
    - social engineering attacks (including malicious apps.).

# Cybercrime goals

- The cybercriminal may have many different objectives:
  - hardware theft;
  - information theft;
  - denial of service/sabotage;
  - ...
- Difficult to enumerate all ways a criminal might seek to gain – where does criminality end and terrorism begin?
- So only solution is to look at all security issues.

# Security measures

- On the network:
  - authentication (of network to device and device to network);
  - secure channel establishment.
- Within the system:
  - software design (reduce patching of vulnerabilities);
  - reduce attack surface (reduce impact of vulnerabilities);
  - hardware/firmware design (reduce risk of side channel attacks);
  - user interface design;
  - user education regarding threats.

# How are we doing?

- Not very well ...
  - **Network security:**
    - security measures very patchily applied (deploy first and then make secure later);
    - quick and dirty solutions often prove ineffective (many unpatched vulnerabilities known).
  - **System security:**
    - first mobile virus reported in 2004;
    - huge numbers of vulnerabilities recently reported in Android systems.

# Network access security

- Network access protocols offer very limited security (device authentication of network is sometimes non-existent).
- Can give rise to:
  - ‘fake network’ attacks (GSM, 802.11, ...);
  - compromised access points (either by software or hardware attack).
- The technology for fake access points is readily available (Airsnarf etc., around since early 2000s) – see ...



[Find Local Wifi Access](#)

Locate WiFi access areas near you - Try Google Maps.



[WIFI-Link antennas online](#)

Buy Hi-Gain Wi-Fi / Wlan antennas  
Booster your wireless signal.

Ads by Google

## News

### Watch out! That's not a real hotspot!

by [Guy Kewney](#) | posted on 19 May 2004

You're in a public hotspot, and logging onto the Internet. ID and password? Sure. Connected! Well, yes, but that's not all. You may have logged onto an Airsnarf box, which is busily faking the connection, and meanwhile, stealing all your details.



And the danger is: this is a very attractive exploit to juvenile hackers because, potentially, it would allow several users to share a single expensive subscription.

The Airsnarf exploit is in most respects identical to an ordinary access point. But it is a private one. It belongs to a hacker; and it logs onto the public AP as if it were an ordinary client. Then it puts up an imitation login that looks just like the public one. And while it does a wonderful job at passing on all your Web packets, and sending the replies back to you, it also keeps track of all the data it handles.

"Airsnarf was developed and released to demonstrate an inherent vulnerability of public 802.11b hotspots - snarfing usernames and passwords by confusing users with DNS and HTTP redirects from a competing access point," says the [instigator](#), at [The Shmoo Group](#).

It's effectively using the techniques of network address translation (NAT) to fool the real hotspot into thinking that several other subscribers are all one. "Basically, it's just a shell script that uses open source software to create a competing hotspot complete with a captive portal."

Well, **as a risk, it would initially look to be quite a low one**. It allows the snarfer to collect email IDs and logins, or other passwords for other Internet services; but it takes quite a lot of work - compared to how much you can get by smuggling a trojan onto the Internet.

The typical script kiddie probably doesn't want your email login. Your email would bore a SK solid in an hour. But your credit card details might be worth sitting in a coffee bar to catch.

And of course, if a bunch of kids all want access through a high-cost (like, BT OpenZone) hotspot, all they have to do is set up a laptop to act as the rogue AP, and then they all log in through it, sharing the cost.

Here's the sweet part, for the kids: they can use your account to do the next log-in, once they have your password. One paid-for hour is all they need. After that, they can be any of the other subscribers who used the spot.

"With a setup like Airsnarf one can obviously create a 'replica website' of many popular, nationally recognised, pay to play hotspots. That's as simple as replacing the index.html file Airsnarf uses, with your own custom web page - one that still points its form field variables to the Airsnarf.cgi."

Combined with sitting at or near a real hotspot, hotspot users will associate and unknowingly give out their username and password for the hotspot provider's network. "The usernames and passwords can then be misused at will to utilise other hotspots of the same provider, possibly anywhere in the nation, leaving the original duped user to pay the bill."

If it catches on, it would discourage flat rate hotspots. They're far more vulnerable. If your subscription is snarfed, you'll spot it on the next bill - and probably, you'll be able to show that you were nowhere near most of the hotspots you appeared to

sponsored by...

horus  
web engineering

### in News

[First WiFi "RFID" tags appear - to track office equipment](#)

[What's Palm up to? The wireless shutter opens Monday at Lehman's conf](#)

[Palm boasts about the number of corporate developers it has already](#)

### you're reading:

[Watch out! That's not a real hotspot!](#)

["Up skirt" photography. Would anybody really, truly, do it? Yes!](#)

[Your car keys can call your phone. No charge.](#)

[Glyndebourne music festival tunes into Wi-Fi](#)

Home

Blog

Comment

Events

News

Features

Gossip

Sponsors

PR releases

about Guy

contact

Search



site by

horus web  
engineering  
ltd

- HOME
- CHANNELS
  - Health Information Exchange
  - Coordinated Care Management
  - Medical Software
  - Medical Hardware
- FREE RESOURCES
  - Universal Healthcare
  - Healthcare Insurance
  - Healthcare Reform
  - White Papers
  - Free eNewsletter
  - Exclusive Articles
  - Advertise With Us
  - 2012 Media Kit (PDF)
  - Contact Us

### Healthcare Technology - INDUSTRY NEWS

SHARE

[April 26, 2011]

## Front: Public Wi-Fi users risk identity theft as fraudsters create 'Evil Twin' fake hotspots: Openzone hotspots can be mimicked with pounds 49 device Police warn of risks from insecure web connection

(Guardian (UK) Via Acquire Media NewsEdge) Millions of smartphone users and BT customers who use Wi-Fi wireless internet "hotspot" connections in public are vulnerable to fraud and identity theft, a Guardian investigation has established.

In tests conducted with volunteers - to avoid breaching telecommunications and computer misuse laws - security experts were able to gather usernames, passwords and messages from phones using Wi-Fi in public places.

In the case of the best-selling Apple iPhone 4 and other smartphone handsets, the information could be harvested without the users' knowledge and even when they were not actively surfing the web if the phone was turned on.

BT, the UK's biggest provider of such hotspots with five million of its "Openzone" connections in the UK in train stations, hotels and airports, admitted that it has known of the weakness for "years" and that it is working on a permanent fix. But it has no timetable for when it might be implemented.

Using a pounds 49 piece of communications equipment and software freely available for download from the internet, the investigation established that "Evil Twin" hotspots can be mimicked with pounds 49 device Police warn of risks from insecure web connection

### Featured White Paper

#### Six Things Hospitals Need to Know About Supporting the Adoption of Smartphones

Pagers have been an essential part of healthcare communications for a long time due to their ability to provide reliable communications at a low cost. When pagers emerged on the healthcare scene, they fundamentally changed the way doctors, nurses, and administrators could be notified that... [DOWNLOAD NOW >>](#)



**FREE eNewsletter**  
Click here to receive your targeted Healthcare Technology Community eNewsletter.  
[\[Subscribe Now \]](#)

### From White Paper Library

- Maimonides Medical Center Leads Healthcare IT Transformation
- State Success Spurs National Innovation in Health Information Exchanges
- Best Practices in Complex Chronic Care Management at Home

[View all](#)



The most Customizable, End-to-End CRM

We are proud that a Soffront Customer took home the Gold Award at the Gartner Customer 360 Summit this year.

**FREE WHITE PAPER**  
**Mobile Health 2010**  
By: **renu** mobile solutions [DOWNLOAD NOW!](#)



### MedHealth RSS

# Communication security

- Pair-wise device authentication is sometimes not robust.
- Methods used to protect channels are known to have major vulnerabilities.
- Apart from poor security fundamentals, privacy is a major issue – device tracking is far too simple.

# Crypto attacks

- Attacks against the crypto-algorithms employed in widely used networks continue to be published.
- WEP (the first suite of algorithms for Wi-Fi) was quickly broken; the replacement suite (WPA) has also been attacked.
- This is not an issue about availability of technology – it is about cost pressures trumping security requirements.

The ultimate resource for navigating the world of apps. Available on newsstands, or click here to get it digitally now: **BUY IT NOW** GIZMODO

Hardware Looking inside the box



## New attack cracks WEP in record time

By Eric Bangeman | Published 4 years ago

Your home or office WiFi network may be even less secure than you think. Researchers have now shown that they can break 104-bit WEP, a common 802.11b/g/n security mechanism, in as little as one or two minutes. A team at the Technische Universität Darmstadt said that they can grab the key with a 95 percent probability of success in as little as two minutes using a 1.7GHz Pentium-M machine to do the calculations.

Here's how the attack works: in order to find the key, a would-be attacker has to have enough traffic to analyze. Therefore, the researchers forced the protected network to start generating packets. Once they have 40,000 packets to analyze, they have a 50 percent success rate in grabbing the key; an additional 20,000 packets nudges the success rate up to 80 percent. Reaching the 95 percent threshold requires 85,000 data packets. As they were able to generate 764 packets per second, they were able to hit the 85,000 mark in 1:51. At this time, the researchers' tool, [aircrack-ptw](#) (source code)—which they say is similar to [aircrack-ng](#)—does not work on 256-bit WPA.

The attack itself is nothing new. As early as 2001, researchers demonstrated vulnerabilities in the RC4 stream cipher that forms the basis for WEP. It wasn't long before 40-bit WEP was cracked; by 2004, 104-bit WEP could be broken with as few as 500,000 recovered packets.

The news here is not that WEP isn't especially secure—that fact is already well-known. What is important to note is the speed with which someone with a Centrino laptop and the proper tools can compromise a WEP-protected network.

If you want the most-secure wireless network possible, WPA2 is the way to go. It's part of the 802.11i standard, which specifies security mechanisms for 802.11 networks. Enterprise users can use an authentication server, while home or small business users can use a passphrase. Neither WPA nor WPA2 are subject to known cryptographic attacks, but we recommend WPA2 due to the additional security it offers, including support for infrastructure and ad-hoc networks, preauthentication, and the CCMP encryption mechanism. Of course, if you've got a Nintendo DS, you'll need to stick with WEP if you want to play online; the PSP, Wii, Xbox 360, and PS3 all support WPA.

Increase text size  
Reduce text size  
Print this story  
Leave a comment




Get the ultimate app resource. Available on the iPad<sup>®</sup> now. **BUY IT NOW** GIZMODO

LATEST TOP STORIES

- Revenge is ours: extracting energy from a cockroach
- Raspberry Pi's \$35 Linux computer on track to launch later this month
- ITC lawyers argue that Barnes & Noble didn't infringe Microsoft's patents

User comments Click here to view comments on this story



Brocade. The world leader in cloud-optimized networks.

Learn about private cloud infrastructures. [VIEW VIDEO FEATURING JASON NOLET, BROCADE VP »](#)

BROCADE

## New attack cracks common Wi-Fi encryption in a minute

Attack works on older WPA systems that use the TKIP algorithm

By [Robert McMillan](#), IDG News Service  
August 27, 2009 02:30 AM ET

[21 Comments](#) [Print](#)

28

[Tweet](#)

147

[Like](#)

0

+1

0

[Share](#)

0

[Submit](#)

3

[Email](#)

Computer scientists in Japan say they've developed a way to break the WPA encryption system used in wireless routers in about one minute.

The attack gives hackers a way to read encrypted traffic sent between computers and certain types of routers that use the WPA (Wi-Fi Protected Access) encryption system. The attack was developed by Toshihiro Ohigashi of Hiroshima University and Masakatu Morii of Kobe University, who plan to discuss further details at a [technical conference](#) set for Sept. 25 in Hiroshima.

Last November, security researchers first showed how WPA could be broken, but the Japanese researchers have taken the attack to a new level, according to Dragos Ruiu, organizer of the PacSec security conference where the first WPA hack was demonstrated. "They took this stuff which was fairly theoretical and they've made it much more practical," he said.

They Japanese researchers discuss their attack in a [paper](#) presented at the [Joint Workshop on Information Security](#), held in Kaohsiung, Taiwan earlier this month.

The [earlier attack](#), developed by researchers Martin Beck and Erik Tews, worked on a smaller range of WPA devices and took between 12 and 15 minutes to work. Both attacks work only on WPA systems that use the Temporal Key Integrity Protocol (TKIP) algorithm. They do not work on newer WPA 2 devices or on WPA systems that use the stronger Advanced Encryption Standard (AES) algorithm.

The encryption systems used by wireless routers have a long history of security problems. The Wired Equivalent Privacy (WEP) system, introduced in 1997, was cracked just a few years later

Brocade. The world leader in cloud-optimized networks.

[VIEW VIDEO FEATURING JASON NOLET, BROCADE VP »](#)

Learn about private cloud infrastructures.

BROCADE

**Most Read**

- IT job spotting: Top 20 metro areas for tech jobs
- Highly anticipated net virtualization startup Nicira exits stealth mode
- The When, Where and How of Cisco versus Microsoft for Unified Communications
- The Apple iPad quiz
- Apple forcing IT shops to 'adapt or die'

[View more Most Read](#)

**Videos** [RSS](#)

**Latest News** [RSS](#)

**LAN & WAN White Papers**

[Speeding Oracle Database Replication with F5 WAN Optimization Technologies](#)

# More crypto attacks

- A wide range of attacks have been demonstrated against GSM cryptography.
- Not so surprising – GSM is 25 years old.
- However, this is not all ancient history – a very recent announcement from Ruhr University Bochum (work led by Christof Paar and Thorsten Holz) shows that satellite phones are not immune from simple crypto attacks ...



Bochum, 8.2.2012

### Satellite telephony is unsafe

*RUB scientists break security standards  
Encryption algorithms have security gaps*

Satellite telephony was thought to be secure against eavesdropping. Researchers at the Horst Görtz Institute for IT-Security (HGI) at the Ruhr University Bochum (RUB) have cracked the encryption algorithms of the European Telecommunications Standards Institute (ETSI), which is used globally for satellite telephones, and revealed significant weaknesses. In less than an hour, and with simple equipment, they found the crypto key which is needed to intercept telephone conversations. Using open-source software and building on their previous research results, they were able to exploit the security weaknesses.

### Telephoning via satellite

In some regions of the world standard cell phone communication is still not available. In war zones, developing countries and on the high seas, satellite phones are used instead. Here, the telephone is connected via radio directly to a satellite. This passes the incoming call to a station on the ground. From there, the call is fed into the public telephone network. So far this method, with the ETSI's encryption algorithms A5-GMR-1 and A5-GMR-2, was considered secure.

### Simple equipment – fast decryption

For their project, the interdisciplinary group of researchers from the areas of Embedded Security and System Security used commercially available equipment, and randomly selected two widely used satellite phones. A simple firmware update was then loaded from the provider's website for each phone and the encryption mechanism reconstructed. Based on the analysis, the encryption of the GMR-1 standard demonstrated similarities to the one used in GSM, the most common mobile phone system. "Since the GSM cipher had already been cracked, we were able to adopt the method and use it for our attack", explained Benedikt Driessen, of the Chair for Embedded Security (Prof. Paar) at the RUB. To verify the results in practice, the research group recorded their own satellite telephone conversations and developed a new attack based on the analysis. „We were surprised by the total lack of protection measures, which would have complicated our work drastically", said Carsten Willems of the Chair for System Security (Prof. Holz) at the RUB.

### Invasion of privacy

Encryption algorithms are implemented to protect the privacy of the user. "Our results show that the use of satellite phones harbours dangers and the current encryption algorithms are not sufficient", emphasized Ralf Hund of the Chair for System Security at the RUB. There is, as yet, no alternative to the current standards. Since users cannot rely on their security against interception, similar to the security of standard cell phones, they will have to wait for the development of new technologies and standards, or make use of other means of communication for



# System security

- Old news:
  - The Register (12/2/07) reported:
    - 3G malware attacks in mobile networks have reached a new high, according to McAfee.
    - 83% of mobile operators were hit by mobile device infections in 2006, according to analyst group Informa. The number of reported security incidents in 2006 was more than five times as high as in 2005.
    - 200 strains of mobile malware discovered.
- It's getting worse, as more recent reports show
- ...

### MARKET SNAPSHOT

U.S.	EUROPE	ASIA
STOXX 50	2,488.82	-19.07 -0.76%
FTSE 100	5,859.25	-32.95 -0.56%
DAX	6,692.40	-72.43 -1.07%

# Bloomberg TV

 Download the iPad app for FREE. 

↓ STOXX 50 2,488.82 -0.76%   ↓ DAX 6,692.40 -1.07%   ↓ Oil (WTI) 96.19 -0.74%   ↓ U.S. 10-year 1.898% -0.009   ↑ 8411:JP 121.00 +0.83%   ↑ 1821:JP 116.00 +1.7   Pause

Sign in

Related News: U.S. · Technology · Media

## Google's Android Faces More App Attacks in New Frontier

By Jonathan Browning - Apr 21, 2011 3:06 PM GMT+0100

ADD TO QUEUE

Recommend  
 Tweet 93  
 Share 36  
 +1 0  
More  
 Print   Email

Google Inc. (GOOG)'s Android mobile-phone platform faces soaring software attacks and has little control over the applications, according to security firm Kaspersky Lab.

Applications loaded with malicious software are infiltrating the Google operating system at a faster rate than with personal computers at the same stage in development, said Nikolay Grebennikov, chief technology officer for Kaspersky. The company identified 70 different types of malware in March from just two categories in September.

"The growth rate in malware within Android is huge, in the future there will definitely be more," Grebennikov said in an interview in London. Kaspersky will offer security on Android in the third quarter of this year.

Hacking into mobile-phone software has become increasingly sophisticated, forcing Mountain View, California-based Google to remove malicious applications that were available from its Android Market store last month. The applications, which were remotely



Google Inc.'s Android mobile-phone platform faces soaring software attacks and has little control over the applications, according to security firm Kaspersky Lab. Photographer: Tony Avelar/Bloomberg

disabled, gathered information about mobile devices and could be used to access personal data.

### More Stories

- [Carbon Capture Projects Imperiled by Worst-Case Scenario: Energy](#) Updated 25 minutes ago
- [Cliffs Becomes Easy Target With Cheapest Mining Value in America: Real M&A](#) Updated 26 minutes ago
- [U.S. Stock Futures Little Changed on Greece](#) Updated 34 minutes ago
- [Russia Seeks to Prod Syria's Assad](#) Updated 1 hour ago

Rate These Stories   More News >>

Advertisement

See how we helped Marriott.com become one of the top 10 retail websites.

[Learn more](#)

accenture

### Most Popular Stories >>

[Time Is Running Out for Greece to Accept Bailout Conditions, Merkel Says](#)



## THE LOOKOUT BLOG

Learn More Download Free

MAY 30, 2011

# Update: Security Alert: DroidDreamLight, New Malware from the Developers of DroidDream

By tim wyatt 34 Comments

Tweet 0 Recommend

### The Threat

This weekend, multiple applications available in the official Android Market were found to contain malware that can compromise a significant amount of personal data. Likely created by the same developers who brought **DroidDream** to market back in March, 26 applications were found to be infected with a stripped down version of DroidDream we're calling "Droid Dream Light" (DDLight). At this point we believe between 30,000 and 120,000 users have been affected by DroidDreamLight.

The Lookout Security Team identified the malware thanks to a tip from a developer who notified us that modified versions of his app and another developer's app were being distributed in the Android Market. Our security team confirmed that there was malicious code grafted into these apps and identified markers associating this code with previously analyzed **DroidDream** samples. We discovered 24 additional apps repackaged and redistributed with the malicious payload across a total of 5 different developer accounts.

Lookout users are automatically protected from this malware. Google has removed all of the apps known to be infected from the Android Market while they investigate.

Search GO

**About this blog**  
This is the official blog of Lookout, a mobile security company in San Francisco. Find out more [about us](#) or [our product](#).

**Subscribe**  
Stay up to date with the latest in mobile security. [Subscribe to our RSS feed](#).

**Twitter**  
**Lookout @Lookout** infographic: Smartphone and app adoption are soaring with no signs of letting up: [bit.ly/yyNlnr](#) #mobilesecurity  
17 hours ago · reply · retweet · favorite  
**Follow us @lookout**

Archives

SOPHOS

IT Security Blog of the Year  
**nakedsecurity**

News. Opinion. Advice. Research



Search articles

Archive by date | author | category  
Send us a tip | Subscribe by RSS



malware | spam | social networks | data loss | law & order | apple | podcast | video | more ▶ about

0  
Like  
0  
+1  
0  
Tweet  
in  
in Share

◀ Another iPhone worm - and this time... Password recovery for the latest iPh. ▶

# Lightning strikes again: iPhone malware gets truly malicious

Join thousands of others, and sign up for Naked Security's newsletter

you@example.com

Don't show me this again X

by [Graham Cluley](#) on November 23, 2009 | Comments Off  
FILED UNDER: [Apple](#), [Data loss](#), [Malware](#), [Mobile](#)

Two weeks ago I reported on Ikee, the world's first iPhone worm which was spreading between jailbroken devices in Australia, replacing wallpaper with an image of Rick Astley.

As [Chet reports on his blog](#), this weekend has seen the discovery of a new example of iPhone malware in the shape of a worm (dubbed "Duh" after a section of its code) that is reported to be much more malicious in intent than Ikee.

The new worm is similar to the original Ikee worm (and the recently discovered iPhone hacking tool) in so much as it only infects jailbroken iPhones, where users have installed OpenSSH and not changed the default password ("alpine").



However, it is much more serious than the original Ikee worm because it is

**Sophos** on Facebook  
Like 167,233

Popular Recent Related

- Best practices for reporting malicious URLs
- iPhone 5 emails infect Windows PCs with malware
- JailBreakMe site rings security alarm for iPhone and iPad users
- Android malware spies on your SMS messages - but is it part of the Zeus family?
- Did anti-virus company hire convicted Chinese malware author?
- First malware using Android



**Try Windows Azure free for 90 DAYS >** Microsoft  
It's the cloud platform for building, hosting and scaling applications. Windows Azure

Print Tweet Like 1 Alert

### Apple security update leaves iPhone 3G users unprotected Security FAIL

By **John Leyden** - [Get more from this author](#)

Posted in [Malware](#), 10th March 2011 16:10 GMT

[Create, deploy and manage web apps in the cloud with Windows Azure - 3 Month free trial](#)

Apple is leaving some of its older mobile devices unprotected with its latest patch batch.

An iOS 4.3 update, which includes a number of critical security fixes, is incompatible with the still widely used iPhone 3G and older versions of the iPod Touch. The latest version of Apple's mobile software can only be applied on the iPhone 3GSs and later models; the iPod Touch 3rd generation and later models; as well as all versions of the iPad.

Security fixes bundled with the release include protection against the risk posed by maliciously-crafted TIFF image files and security fixes against multiple memory corruption issues in WebKit, the engine behind the Safari browser.

Security firm Sophos warns that the omission of the fixes leaves users of older iPhone and iPod Touches at heightened risk of drive-by download attacks from booby-trapped websites. The latest version of the OS includes tethering functionality and the ability to stream music between devices across home wireless networks, among other functionality improvements.

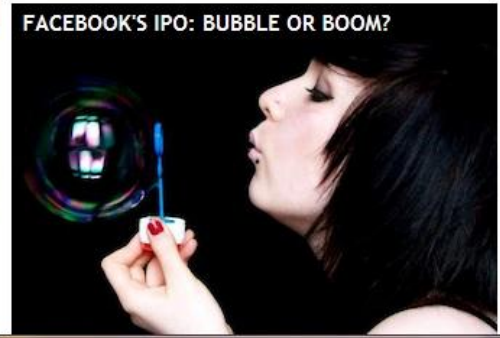
Microsoft  
**Try Windows Azure free for 90 DAYS >**  
It's the cloud platform for building, hosting and scaling applications. Windows Azure

**MOST READ** **MOST COMMENTED**

- Job-seeking Marriott hacker gets 30 months' porridge
- Avast false alarm hits Steam's weekend gamers
- Trojan smuggles out nicked blueprints as Windows Update data
- Mac malware uses Windows-style PDF camouflage ruse
- Kelihos botnet BACK FROM THE DEAD

Sign up, sign up for The Register's weekly IT security newsletter - [click here](#)

Windows Server Choose a Private Cloud Solution Microsoft  
System Center Click to explore >



# Is this as bad as it gets?

- So far we have looked at the traditional notion of mobile systems.
- This involves relatively closed systems, sometimes carefully designed from a security perspective.
- What's the worst that can happen?
  - loss of hardware (relatively small impact);
  - loss of data – not good, but limited impact (corporates can protect back end).

# The emerging threat scenario

- The much larger world of everyday devices with embedded IT functionality and connectivity is far more scary ...
- We now have systems often thought of as not having major security requirements:
  - typically designed without concern about, or knowledge of, security threats;
  - potentially much more serious threats apply – valuable hardware at risk, and even major safety implications.

# Agenda

1. Introduction – mobile devices
2. The security landscape
3. The problem – case studies
4. The way forward
5. Concluding remarks



# Why are we here?

- There is huge business pressure to market products first and worry about security second.
- Technology gets used in ways unanticipated by designers (e.g. SMS, IP for everything), which means initial threat analyses no longer hold.
- Retrofitting security is very difficult – perhaps impossible in practice.

# More why?

- Available ‘retrofit’ security technology is not used (e.g. trusted computing, identity management, SET, ...).
- Improving security and privacy rarely has a big pay-off to the user (individual or corporate) – except perhaps **after the event**, i.e. after a major security breach.

# Conflicting pressures

- **Security requirements:**
  - High robustness – because of criticality of IT;
  - Privacy protection – growing legal frameworks and user interest.
- **Economic/technological factors:**
  - Increasing complexity (inevitable technological drift) directly threatens robustness;
  - Increased connectivity and use of third parties (outsourcing) makes privacy and security assurance very hard.
  - Smarts everywhere (flexibility) also threatens robustness.
  - Speed to market and desire for minimum cost (leads to disregard for/ignorance of security requirements).

# Case study I – door openers

- Christof Paar and his collaborators at the Ruhr University of Bochum have looked at attacks on a variety of real world hardware systems.
- One system they studied extensively is based on a cipher called KeeLoq.
- KeeLoq is widely used in remote keyless entry (RKE) systems.

# KeeLoq

- KeeLoq widely used for garage door openers and car door systems.
- The cipher is not terribly strong.
- More serious is the fact that the key management system design means that all devices for a single system share the same key.
- Compromising this key (can be done by analysis of a single consumer device) breaks entire system.
- Means that cloned keys could be simply and cheaply manufactured – crime possibilities are clear.

**UNIVERSITY OF LONDON**  
INTERNATIONAL PROGRAMMES

**Be more**  
Get ahead with postgraduate study in **Information Security** from the experts at Royal Holloway.

Royal Holloway University of London  
**FIND OUT MORE >>**

Google Custom Search  **GO**

### Researchers crack KeeLoq RFID technology - Again

by Steve Ragan - Apr 3 2008, 19:39

Like Tweet 0 +1 0 Share



Researchers from Ruhr University Bochum, Germany, have cracked the security on keyless entry systems based on KeeLoq RFID [technology](#) (IMG:J.Anderson)

Researchers from Ruhr University Bochum, Germany, have cracked the security on keyless entry systems based on KeeLoq RFID technology. The announcement was made Monday, and follows a recent trend in research on RFID. The research will allow anyone to access the KeeLog based devices from a distance of three hundred feet without a trace.

The research applies to all known car and building access control systems that rely on the KeeLoq cipher. The Communication Security Group in the Electrical Engineering and Information Sciences Department, at Ruhr University, targeted and ultimately cracked the KeyLoq RFID as part of their research in embedded security.

**SECURITY**

Index Features  
News Reviews

SUPPORT TTH ON FACEBOOK

**APPLY NOW**  
for **LSBF's Undergraduate Plus**

Start **Feb 2012**

London School of Business & Finance

**IRONKEY**  
MODEL **S 200**

THE WORLD'S FIRST  
**FIPS 140-2**  
**LEVEL 3**  
FLASH DRIVE

# Other work

- The RKE/KeeLoq attacks were done a couple of years ago.
- More recently the Bochum team have successfully attacked a range of other real-world systems, including:
  - FPGA software downloads;
  - personal wireless systems (including electronic passports, contactless payment cards, RFID, ...).

## Case study II – cars

- Focus on recent work of group of researchers at UCSD and University of Washington (two major papers in 2010 and 2011).
- They have performed a detailed study of attack vectors on cars (involving purchasing a complete car).



# Evolution of cars

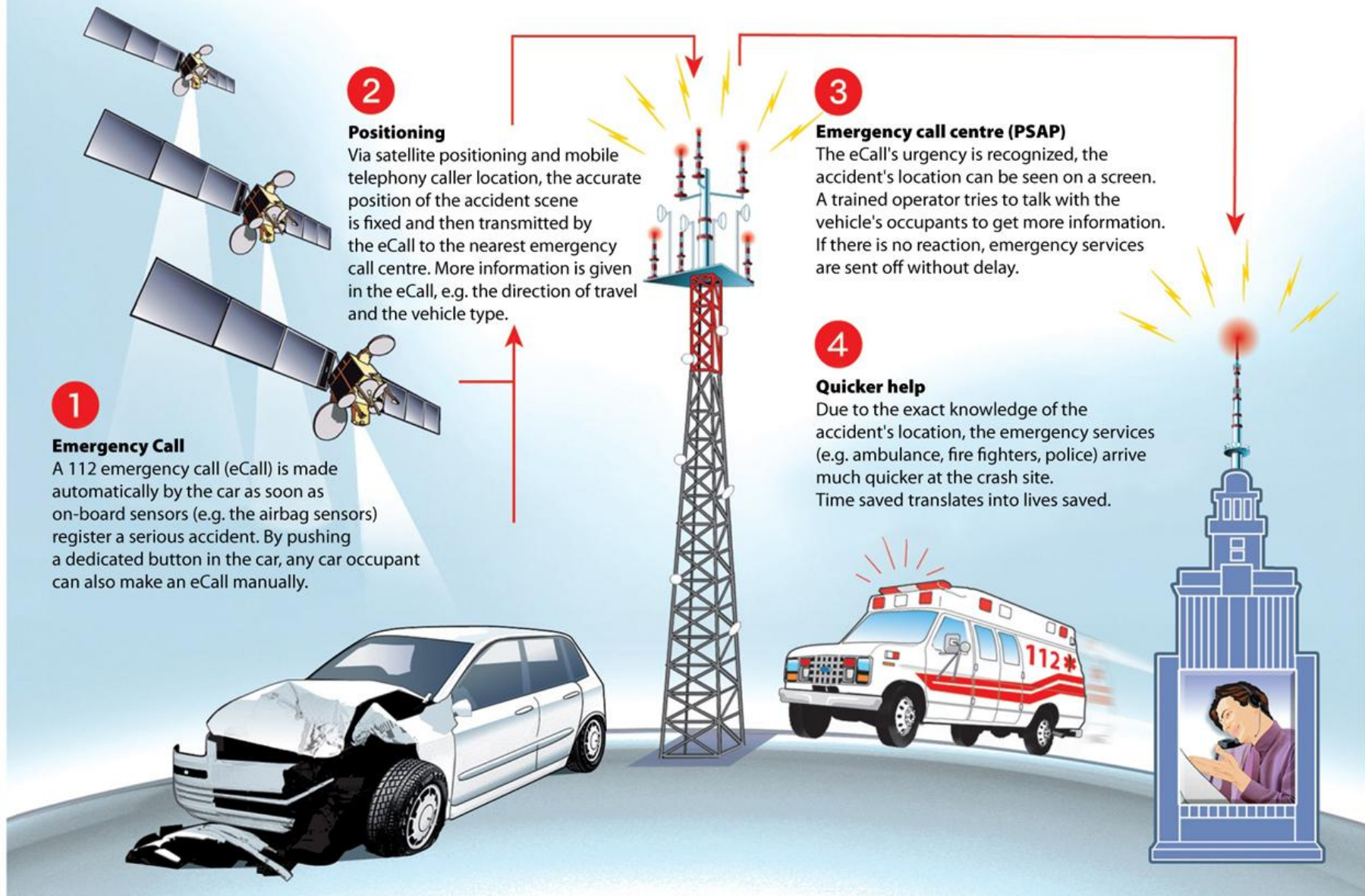
- A modern car contains networks of communicating devices (computers/ECUs).
- They control most aspects of its operation, including:
  - brakes (anti-lock mechanisms);
  - gears;
  - throttle and engine management.
- This includes external connectivity, e.g. including mobile telephony.

# Attack surface

- In US, the mandatory Onboard Diagnostics Unit (OBD-II) port provides direct access to the internal network.
- User-upgradeable systems (e.g. audio players) routinely connected to internal networks.
- Wireless devices (e.g. Bluetooth) also connected to internal networks.
- Most seriously, remote telematics systems (for safety, diagnostics, anti-theft) provide continuous connectivity via mobile phone networks.



# eCall: The crashed car calls 112!



# Results I

- The team performed experiments using two cars purchased specifically for purpose:
  - car's internal CAN bus has little security – any compromised component can impersonate any other component;
  - many other security issues.
- Demonstrated remote attacks via broad range of attack vectors, including: mechanics tools, CD players, Bluetooth and **mobile telephony**.

# Results II

- They reverse-engineered the telematics protocol, and used a buffer overflow vulnerability in the car gateway to take over the car telematics unit.
- Attacks works completely ‘blind’, i.e. without listening to responses from vehicle.
- Demonstrated ability to compromise internal car systems, and thereby systematically control:
  - engine, brakes, lights, instruments, radio, locks, ...
- Could be exploited for theft, surveillance, ...

# Why?

- Why are such serious attacks feasible (and arguably even easy)?
  - Manufacturers integrate components provided by third party suppliers.
  - Users add third party systems (e.g. audio players) with serious security ramifications, yet systems are low cost consumer items.
  - Suppliers subject to cost pressure:
    - do not take security seriously;
    - do not understand nature of threats (security is not their field of expertise).

# Agenda

1. Introduction – mobile devices
2. The security landscape
3. The problem – case studies
4. The way forward
5. Concluding remarks



# Where we are

- Perhaps most serious problem is that we are adding communications functionality (and so serious security vulnerabilities) and internal inter-connectivity to systems without thinking through security issues.
- Manufacturers & users are encountering major security (and cybercrime) problems they have no previous exposure to.
- Danger is that the sorry cycle of security problems with PCs will endlessly repeat itself with new classes of product.

# It'll get worse

- I am (un)happy to predict that the situation will get worse before it gets better.
- It is the usual pattern with new technology that allows ubiquitous connectivity:
  - first generation mobile phones had no security so a major crime problem arose;
  - once the Internet became widely used, PCs and servers were (and are) subject to many attacks.
- This pattern is now repeating itself with smart phones, and, more worryingly, looks set to arise with many other consumer products.

# In the words of Private James Frazer:



We're all doomed!

# The really scary stuff

- No-one in academia (as far as I know) has worked on understanding the security properties of plane or train systems (which are increasingly network connected).
- However, exactly the same issues as arise for cars may well apply.
- That is, have these systems been designed to counter the kind of adversarial threat mode encountered on the Internet?
- I fear not ...

# Educating manufacturers I

- How do we start to address these problems?
- Well, my intention in talking here is to try to raise awareness of the threat.
- Most generally, producers of systems need to be aware of two main things:
  - security is **your problem**;
  - getting security right is non-trivial.
- Perhaps most importantly, it is not just a question of randomly adding some crypto functionality ...

# Educating manufacturers II

- The good news is that it does not need to be expensive. For example:
  - Eliminating unnecessary functionality (reducing the attack surface) can solve many problems.
  - Following good software engineering practices can minimise risk of buffer overflow vulnerabilities.
  - Robust crypto and sound security protocols are widely available and standardised.

# Educating users

- What can consumers/end users do?
- Well, sadly, we must be prepared to pay just a little more for devices which make life harder for cybercriminals.
- We must put pressure on manufacturers to make more secure products, and on governments to legislate and regulate, where appropriate.
- At this point it is also tempting to ask users to be less easily duped – however, ultimately users need to be protected.
- It is unreasonable to expect users to become security experts.

# Regulation/standardisation I

- Perhaps our best hope in the long run is that governments and trade bodies will act.
- We rely on regulation to ensure that cars, airliners and trains are safe.
- These regulators need to take on board the new mobile threat – this is serious!



# Regulation/standardisation II

- However, a closed ‘conformance mentality’ by manufacturers is not always good.
- I recently heard an employee of a manufacturer of HSMs saying that FIPS 140 has had a negative effect on overall HSM security.
- The focus has been too much on compliance (and addressing issues covered by standard) at expense of worrying about security in general.
- The standard does not focus on most important issues, but those easiest to standardise.

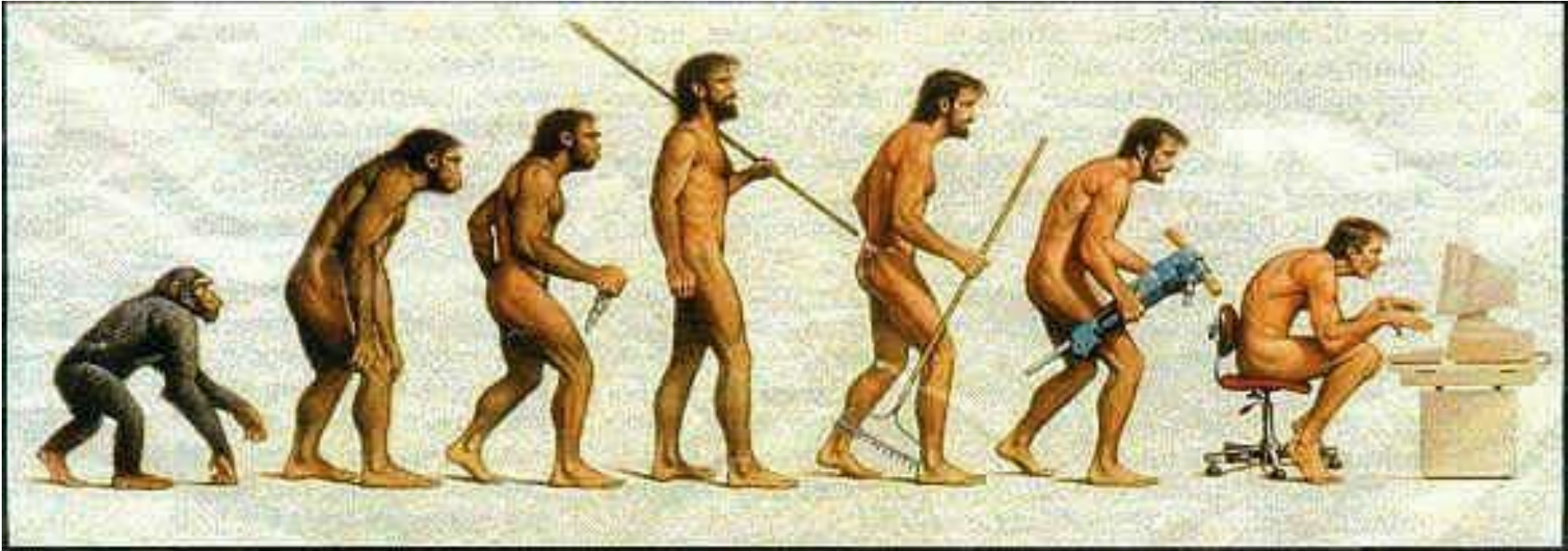
# Agenda

1. Introduction – mobile devices
2. The security landscape
3. The problem – case studies
4. The way forward
5. Concluding remarks

# Sleepwalking to disaster

- There are ways in which disasters can be avoided.
- However, right now I don't sense much urgency to try to fix the problems.
- In the past, manufacturers and network operators have been left to clear up the mess they have created.
- This may be 'just', but what happens in the mean time to the victims of cybercrime?

# Where did it all go wrong?



**Somewhere, something went terribly wrong**

# Security

- Making connected systems secure is non-trivial.
- It needs specialist expertise.
- However, **we have the technology ...**



# The last slide

- **Thanks for your attention ...**
- I am happy to take questions now or later, in person or by email:  
[me@chrismitchell.net](mailto:me@chrismitchell.net)
- See also:  
<http://www.chrismitchell.net>