cybersecurity centre
GCHQ Academic Centre of Excellence EPSRC

UNIVERSITY OF
Southampton
Electronics and Computer Science

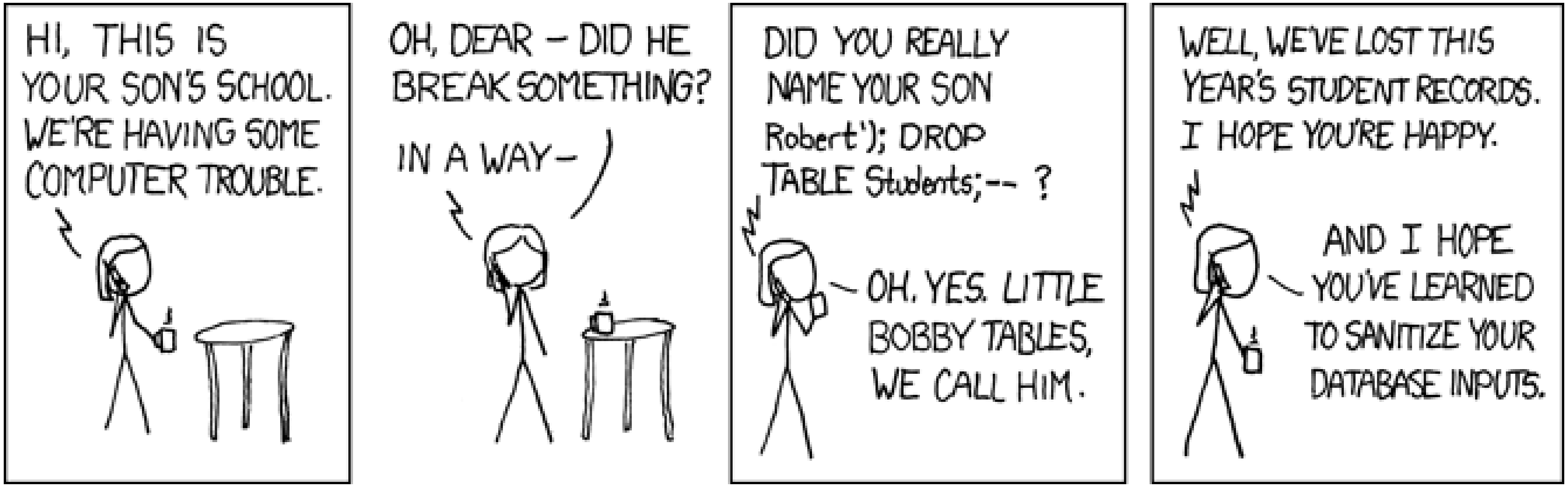
Software Vulnerabilities

at the South East Cyber Crime Workshop

Denis A Nicole
dan@ecs.soton.ac.uk

2014-01-30

Traditional SQL injection


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Has been supplanted by "fuzzing"

http://xkcd.com/327/

Poor quality commercial software

- There are very few real standards to assure the quality of commercial software

- Sony

Sony BMG wanted Digital Rights Management

Sony tests technology to limit CD burning
Go back to review | Print
http://news.cnet.co.uk/digitalmusic/0,39029666,39189658,00.htm
June 1, 2005

As part of its mounting US rollout of content-enhanced and copy-protected CDs, Sony BMG Music Entertainment is testing technology solutions that bar consumers from making additional copies of burned CD-R discs.

Since March, the company has released at least 10 commercial titles -- more than 1 million discs in total -- featuring technology from UK antipiracy specialist First4Internet that allows consumers to make limited copies of protected discs, but blocks users from making copies of the copies.

The concept is known as 'sterile burning'. And in the eyes of Sony BMG executives, the initiative is central to the industry's efforts to curb casual CD burning.

"The casual piracy, the schoolyard piracy, is a huge issue for us," says Thomas Hesse, president of global digital business for Sony BMG. "Two-thirds of all piracy comes from ripping and burning CDs, which is why making the CD a secure format is of the utmost importance."

Names of specific titles carrying the technology were not disclosed. The effort is not specific to First4Internet. Other Sony BMG partners are expected to begin commercial trials of sterile burning within the next month.

To date, most copy protection and other digital rights management (DRM)-based solutions that allow for burning have not included secure burning.

Early copy-protected discs as well as all DRM-protected files sold through online retailers like iTunes, Napster and others offer burning of tracks into unprotected WAV files. Those burned CDs can then be ripped back onto a personal computer minus a DRM wrapper and converted into MP3 files.

Under the new solution, tracks ripped and burned from a copy-protected disc are copied to a blank CD in Microsoft's Windows Media Audio format. The DRM embedded on the discs bars the burned CD from being copied.

"The secure burning solution is the sensible way forward," said First4Internet CEO Mathew Gilliat-Smith. "Most consumers accept that making a copy for personal use is really what they want it for. The industry is keen to make sure that is not abused by making copies for other people that would otherwise go buy a CD."

As with other copy-protected discs, albums featuring XCP (extended copy protection) will allow for three copies to be made.

However, Sony BMG has said it is not locked into the number of copies. The label is looking to offer consumers a fair-use replication of rights enjoyed on existing CDs.

A key concern with copy-protection efforts remains compatibility.

It is a sticking point at Sony BMG and other labels as they look to increase the number of copy-protected CDs they push into the market.

Among the biggest headaches is that secure burning means that iPod users do not have any means of transferring tracks to their device, because Apple Computer has yet to licence its FairPlay DRM for use on copy-protected discs.

As for more basic CD player compatibility issues, Gilliat-Smith says the discs are compliant with Sony Philips CD specifications and should therefore play in all conventional CD players.

The moves with First4Internet are part of a larger copy-protection push by Sony BMG that also includes SunnComm and its MediaMax technology.

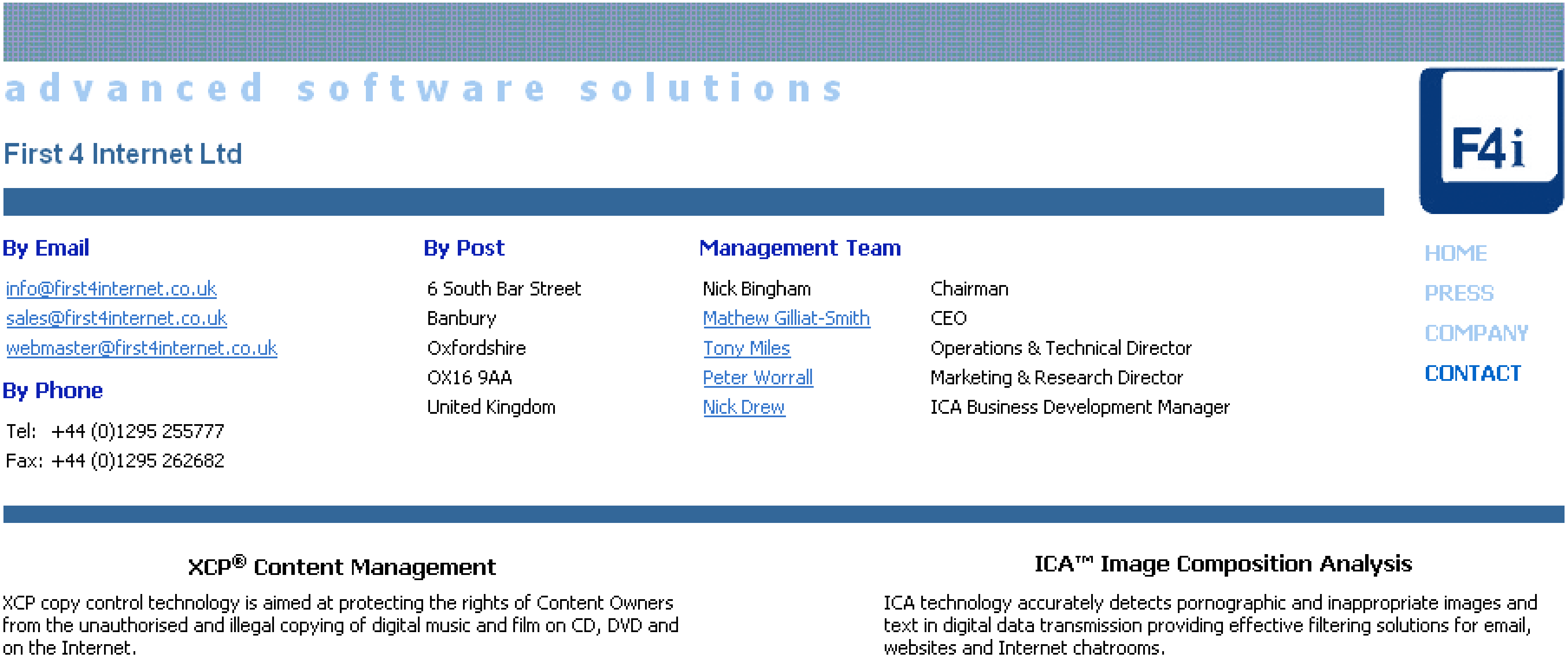
To date, SunnComm has been the music giant's primary partner on commercial releases -- including Velvet Revolver's *Contraband* and Anthony Hamilton's solo album. In all, more than 5.5 million content-enhanced and protected discs have been shipped featuring SunnComm technology.

First4Internet's XCP has been used previously on prerelease CDs only. Sony BMG is the first to commercially deploy XCP.

First4Internet's other clients -- who include Universal Music Group, Warner Music Group and EMI -- are using XCP for prerelease material.

Sony BMG expects that by the end of the year a substantial number of its US releases will employ either MediaMax or XCP. All copy-protected solutions will include such extras as photo galleries, enhanced liner notes and links to other features.

They hired these people



advanced software solutions

First 4 Internet Ltd

F4i

HOME
PRESS
COMPANY
CONTACT

By Email

info@first4internet.co.uk
sales@first4internet.co.uk
webmaster@first4internet.co.uk

By Phone

Tel: +44 (0)1295 255777
Fax: +44 (0)1295 262682

By Post

6 South Bar Street
Banbury
Oxfordshire
OX16 9AA
United Kingdom

Management Team

Nick Bingham	Chairman
Mathew Gilliat-Smith	CEO
Tony Miles	Operations & Technical Director
Peter Worrall	Marketing & Research Director
Nick Drew	ICA Business Development Manager

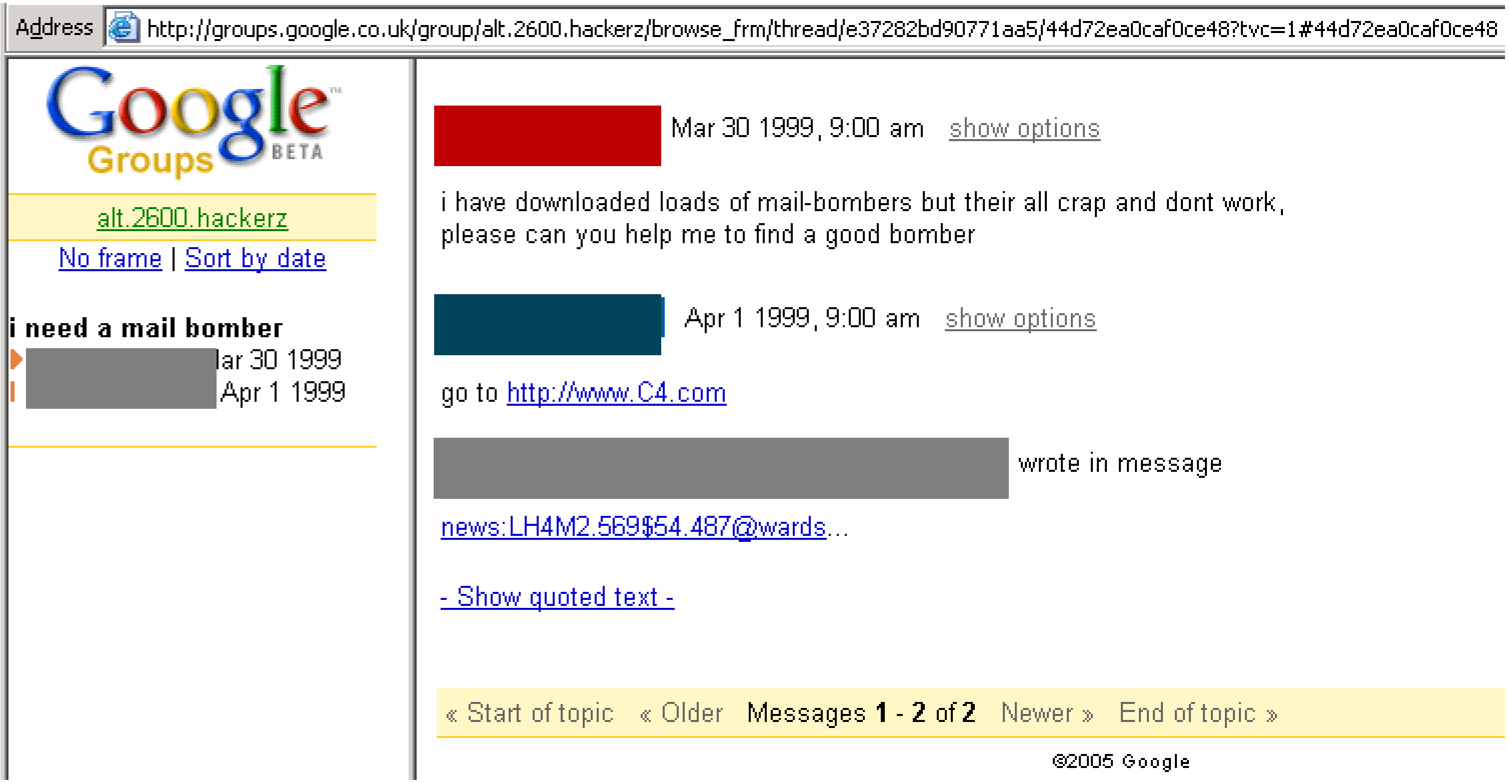
XCP® Content Management

XCP copy control technology is aimed at protecting the rights of Content Owners from the unauthorised and illegal copying of digital music and film on CD, DVD and on the Internet.

ICA™ Image Composition Analysis

ICA technology accurately detects pornographic and inappropriate images and text in digital data transmission providing effective filtering solutions for email, websites and Internet chatrooms.

Is this the author in an earlier life?



Address http://groups.google.co.uk/group/alt.2600.hackerz/browse_frm/thread/e37282bd90771aa5/44d72ea0caf0ce48?tvc=1#44d72ea0caf0ce48

alt.2600.hackerz

No frame | Sort by date

i need a mail bomber

[redacted] ar 30 1999
Apr 1 1999

[redacted] Mar 30 1999, 9:00 am show options

i have downloaded loads of mail-bombers but their all crap and dont work,
please can you help me to find a good bomber

[redacted] Apr 1 1999, 9:00 am show options

go to http://www.C4.com

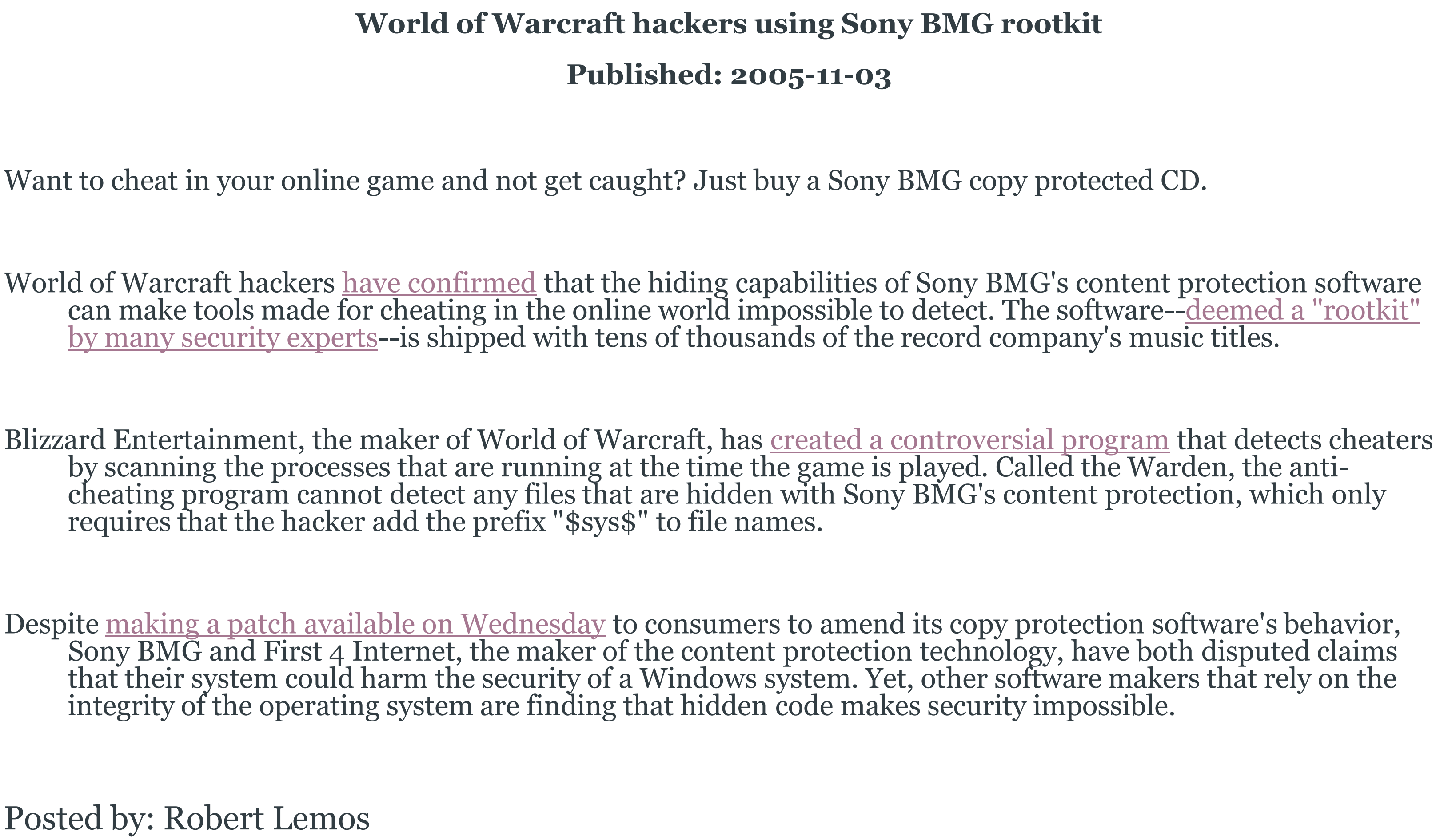
[redacted] wrote in message
news:LH4M2.569$54.487@wards...

- Show quoted text -

« Start of topic « Older Messages **1** - **2** of **2** Newer » End of topic »

©2005 Google

It undermined system security



World of Warcraft hackers using Sony BMG rootkit

Published: 2005-11-03

Want to cheat in your online game and not get caught? Just buy a Sony BMG copy protected CD.

World of Warcraft hackers have confirmed that the hiding capabilities of Sony BMG's content protection software can make tools made for cheating in the online world impossible to detect. The software--deemed a "rootkit" by many security experts--is shipped with tens of thousands of the record company's music titles.

Blizzard Entertainment, the maker of World of Warcraft, has created a controversial program that detects cheaters by scanning the processes that are running at the time the game is played. Called the Warden, the anti-cheating program cannot detect any files that are hidden with Sony BMG's content protection, which only requires that the hacker add the prefix "sys" to file names.

Despite making a patch available on Wednesday to consumers to amend its copy protection software's behavior, Sony BMG and First 4 Internet, the maker of the content protection technology, have both disputed claims that their system could harm the security of a Windows system. Yet, other software makers that rely on the integrity of the operating system are finding that hidden code makes security impossible.

Posted by: Robert Lemos

Microsoft classed it as *malware*

Sony DRM Rootkit

I've been getting a lot of questions in the last week about Microsoft's position on the Sony DRM and rootkit discussions, so I thought I'd share a little info on what we're doing here. We are concerned about any malware and its impact on our customers' machines. Rootkits have a clearly negative impact on not only the security, but also the reliability and performance of their systems.

We use a set of objective criteria for both Windows Defender and the Malicious Software Removal Tool to determine what software will be classified for detection and removal by our anti-malware technology. We have analyzed this software, and have determined that in order to help protect our customers we will add a detection and removal signature for the rootkit component of the XCP software to the Windows AntiSpyware beta, which is currently used by millions of users. This signature will be available to current beta users through the normal Windows AntiSpyware beta signature update process, which has been providing weekly signature updates for almost a year now. Detection and removal of this rootkit component will also appear in Windows Defender when its first public beta is available. We also plan to include this signature in the December monthly update to the Malicious Software Removal Tool. It will also be included in the signature set for the online scanner on Windows Live Safety Center.

I'll update you if any more information comes up.

best,
-jasong

```
------------------------------------------------------------
Jason Garms
Architect & Group PM
Anti-Malware Technology Team
Microsoft Corporation

Team Blog: http://blogs.technet.com/antimalware
```

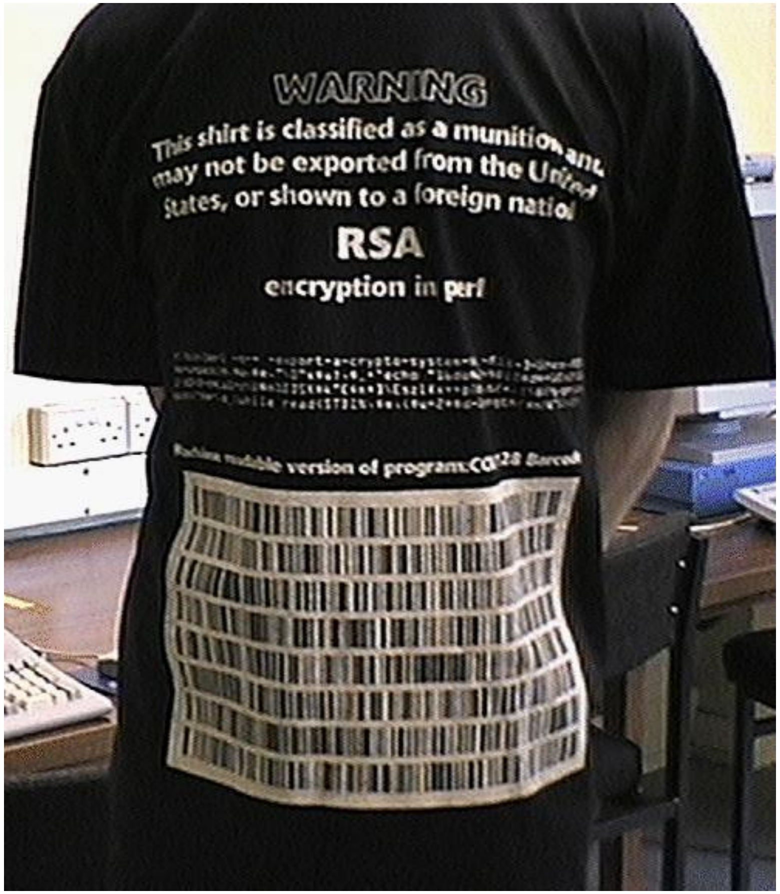
Very old commercial software

- Many ATMs still run on Windows XP. Normal security support terminates in April this year.
- Banks still use IBM batch processing systems dating from the 1960s—designed for punched cards.

Restrictions on cryptography

The (US) Government did not carry the community with it

- The crypto wars: Clipper and key escrow
- Export controls


WARNING
This shirt is classified as a munition and
may not be exported from the United
States, or shown to a foreign national
RSA
encryption in perl
Machine readable version of program:

“Backdoors” become public, and vulnerable

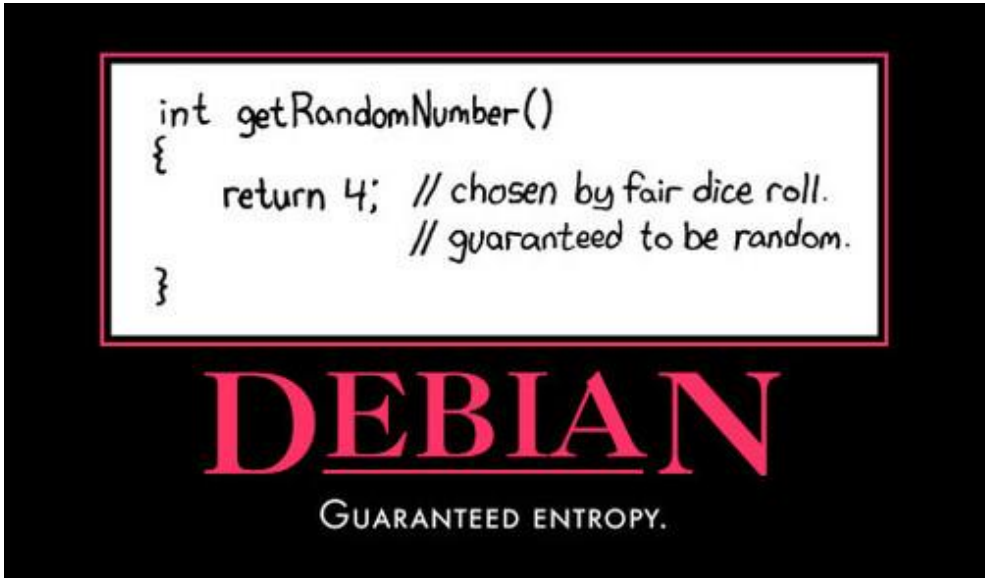
Andrew Fernandes discovered a back door for the NSA in every copy of Win95/98/NT4 and Windows2000.

In this service release of software from Microsoft, the company crucially forgot to remove the symbolic information identifying the security components. It turns out that there are really two keys used by Windows; the first belongs to Microsoft, and it allows them to securely load CryptoAPI services; the second belongs to the NSA. That means that the NSA can also securely load CryptoAPI services on your machine, and without your authorization. The result is that it is tremendously easier for the NSA to load unauthorized security services on all copies of Microsoft Windows, and once these security services are loaded, they can effectively compromise your entire operating system.

It turns out that there is a flaw in the way the function is implemented. Because of this, users can easily eliminate or replace the NSA key from the operating system without modifying any of Microsoft's original components. Since the NSA key is easily replaced, it means that non-US companies are free to install "strong" crypto services into Windows, without Microsoft's or the NSA's approval.

http://cryptome.org/

Poor random numbers are a big vulnerability, particularly in small embedded systems.

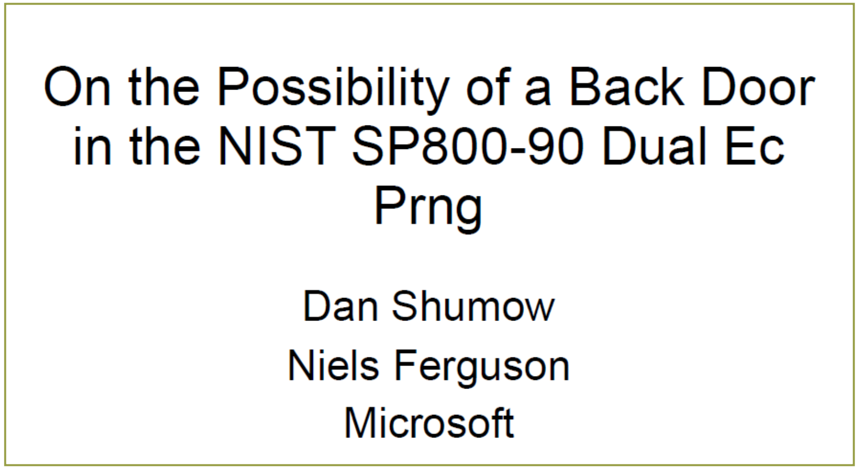


```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

The cartoon refers to a vulnerability introduced into the Debian version of the `openssl` library; this was commonly used to generate `https:` server keys.

Protected backdoors

It is technically possible to craft software backdoors which can only be exploited by law enforcement.



On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng

Dan Shumow
Niels Ferguson
Microsoft

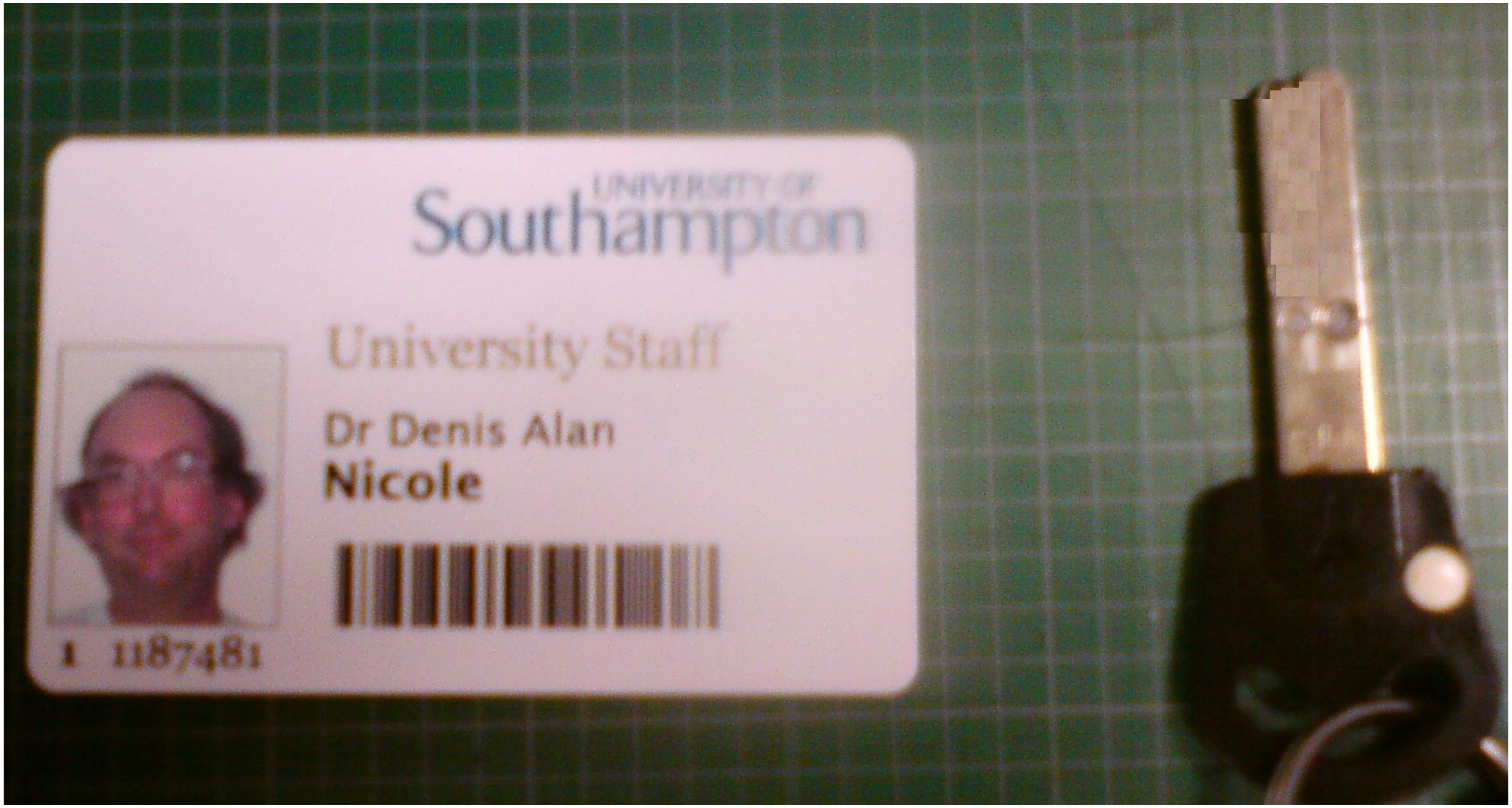
But it is hard. This one was rapidly detected by “academic” researchers.

And has led (recently) to reputational damage for NSA, NIST and RSA.

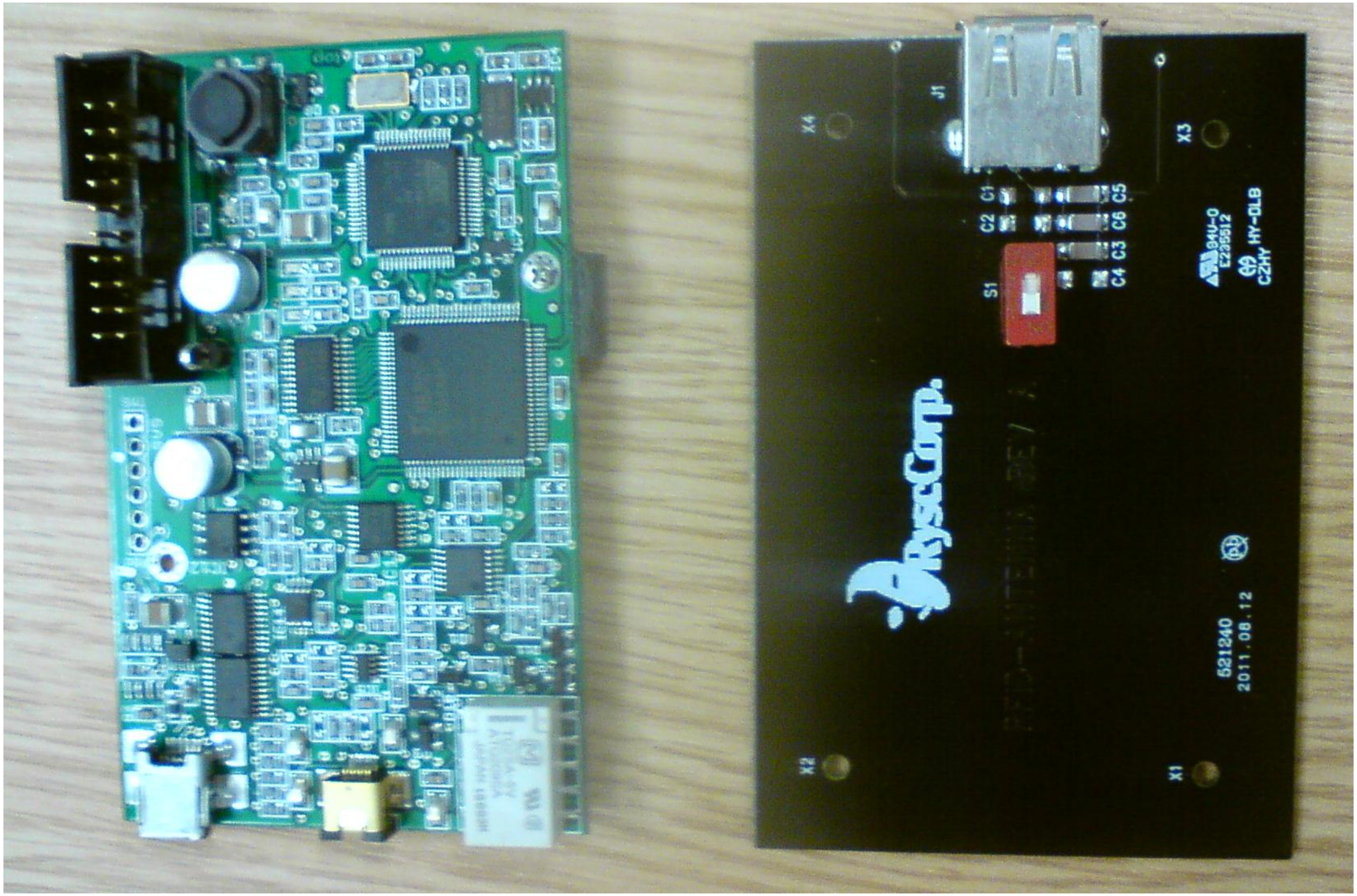
Hardware and software locks

- Software “hacking” tools are cheap and easy, and
- widely discussed in the “respectable” community. http://media.ccc.de/browse/congress/2013/

Which do you trust?

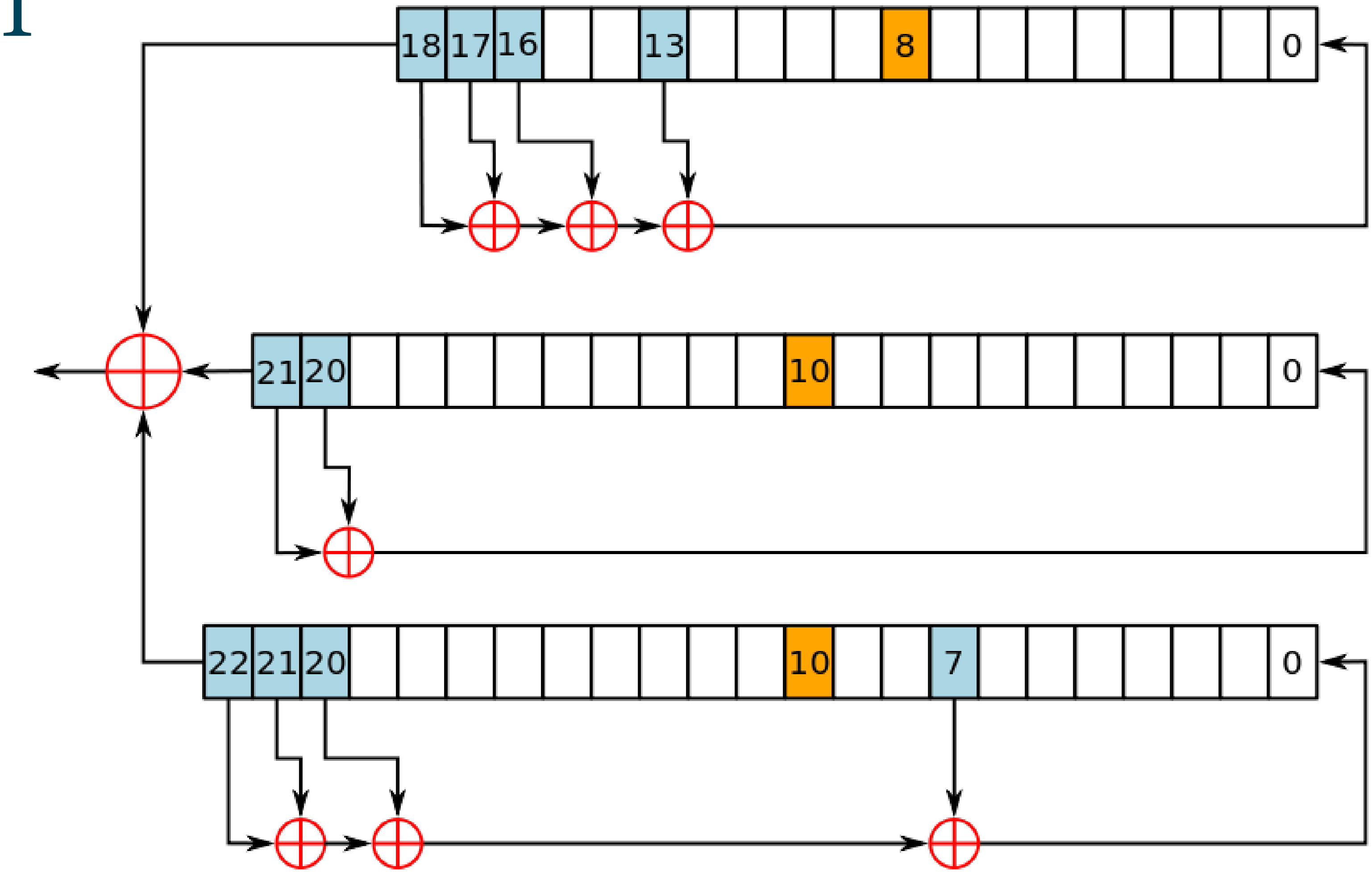


This is the “expensive” tool



GSM security

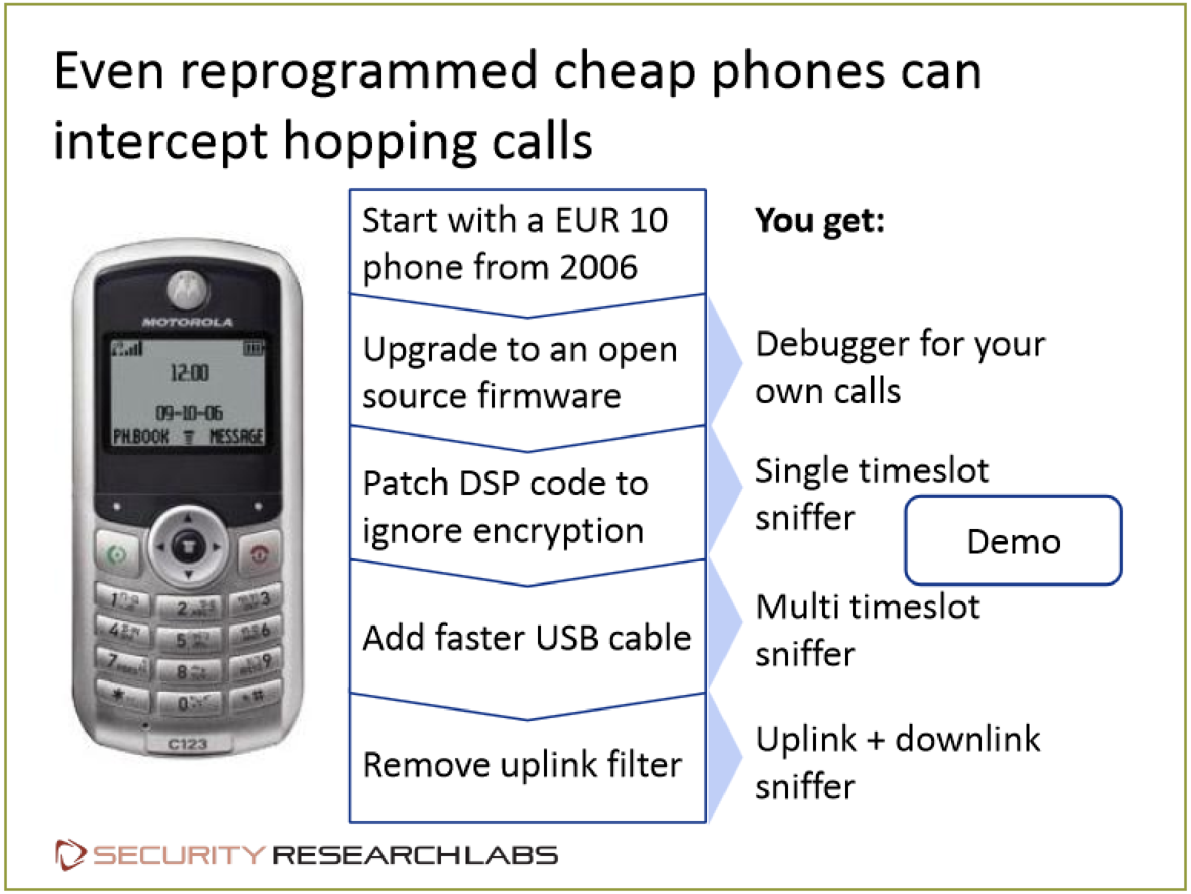
A5/1



LFSR clocks if its yellow bit is in the majority

http://en.wikipedia.org/wiki/File:A5-1_GSM_cipher.svg

A5/1 Easily broken on-air (2010)



Even reprogrammed cheap phones can intercept hopping calls

Start with a EUR 10 phone from 2006

Upgrade to an open source firmware

Patch DSP code to ignore encryption

Add faster USB cable

Remove uplink filter

You get:

Debugger for your own calls

Single timeslot sniffer

Demo

Multi timeslot sniffer

Uplink + downlink sniffer

SECURITY RESEARCHLABS

http://events.ccc.de/congress/2010/Fahrplan/attachments/1783_101228.27C3.GSM-Sniffing.Nohl_Munaut.pdf

Our contribution to security

- A whole new class of software vulnerabilities arise in "multicore" chips: all modern phones, desktops and servers.
- The vulnerabilities are timing-dependent and cannot usually be found by conventional testing.

ESBMC is a Collaboration between

- University of Southampton
  - Jeremy Morse and Denis Nicole
- Federal University of Amazonas, Brazil
  - Mikhail Ramalho, Mauro Freitas, Felipe Sousa, Hendrio Marques and Lucas Cordeiro
- University of Stellenbosch, South Africa
  - Bernd Fischer

UNIVERSIDADE FEDERAL DO AMAZONAS
IN UNIVERSA SCIENTIA VERITAS

UNIVERSITY OF Southampton
Electronics and Computer Science

UNIVERSITEIT
STELLENBOSCH
UNIVERSITY

ESBMC is a *bounded* model checker

- It exhaustively analyses all possible behaviours of a (multithreaded) C or C++ program up to a *fixed* depth of
  - loop iteration (including backward jumps and recursion),
  - thread interleaving.
- Within these bounds, it checks for
  - C errors: pointer errors, arithmetic errors, array bounds, **`malloc()`**/**`free()`**, **`assert()`** failures, data races, etc.
  - Violation of *Linear Temporal Logic* specifications.

Model Checking is not Simulation

- *Simulation* (testing) checks correctness for a particular input and a particular thread interleaving.
- You need to run multiple simulations with different data and different timing before you get *some* assurance.
- *Model Checking* exhaustively analyses all possible behaviours over a range of possible inputs and generates a *witness*, a trace of program state, if there are any possible failures.
- Good-coverage simulation may be effective against “random” errors; it offers little protection against tailored attacks.

Improvement by competition

- The field of C model checking research is now large enough to support annual competitions; perhaps the best known is that held in conjunction with the *International Conference on Tools and Algorithms for the Construction and Analysis of Systems* (TACAS).
- The team is proud to report that ESBMC v1.17 won the Gold Medal in the *SystemC* and *Concurrency* categories and the Bronze Medal in the overall ranking of the first *International Competition on Software Verification* at TACAS 2012.
- ESBMC v1.20 won the Bronze Medal in the overall ranking of the second competition at TACAS 2013.