http://www.mobilephonesecurity.org

COPPER HORSE

Mobile Phone Hacking: A lucrative, but largely hidden history

DC4420

David Rogers

27th May 2014

Car Radio Hacking – 1990s / 2000s

- PIN locks to deter and remove value of theft
- Hacking tools reset / calculate / remove security codes

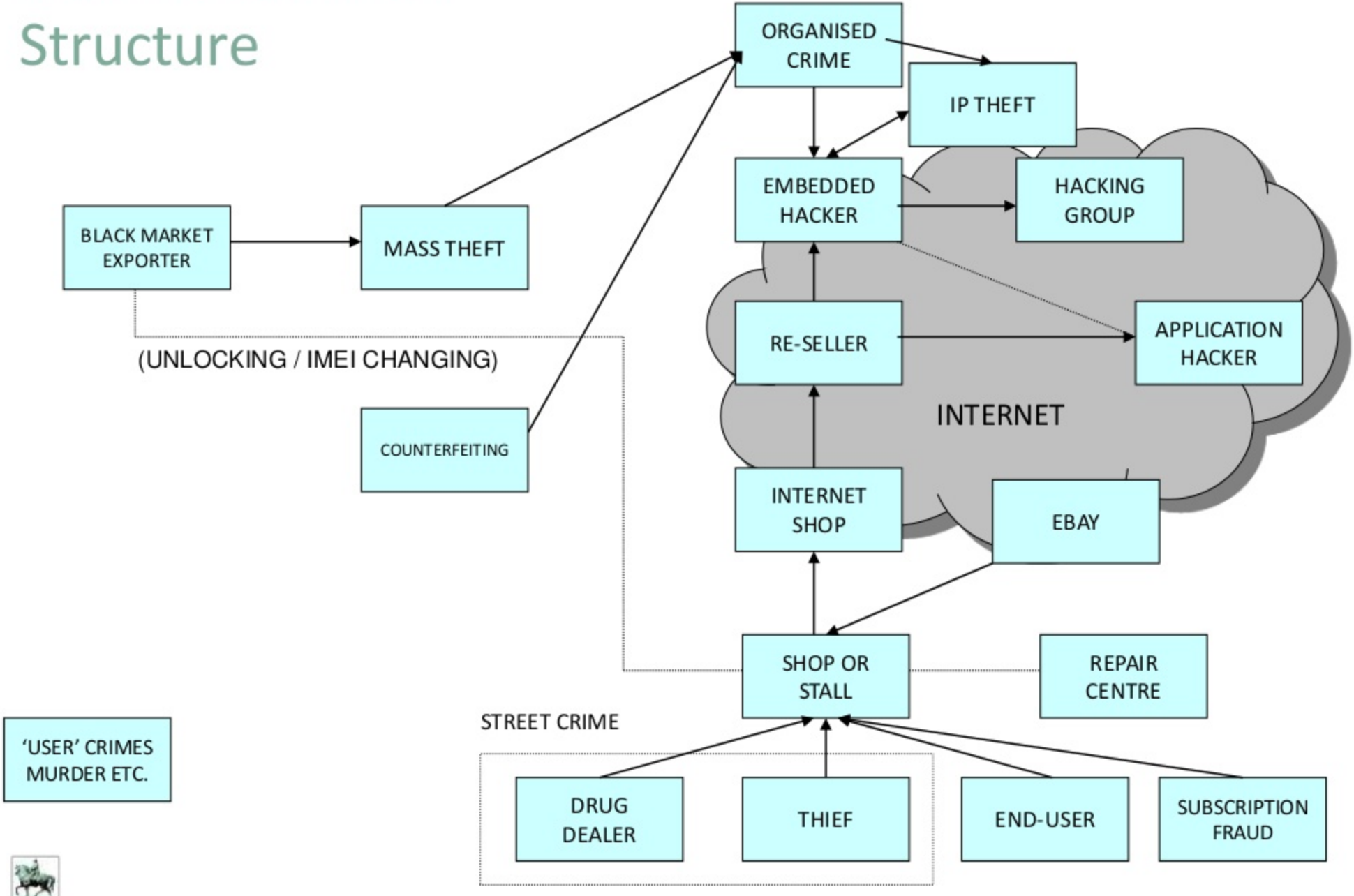
Some Phone Terms: SIMlock & IMEI

- SIMlock:
  - used to secure the device to a particular network during the period of the subsidy, can be unlocked with CK codes by calling operator
  - Different variants of locks
  - Recent court case in the US over legality (and lots of other previous fights)
- IMEI :
  - the International Mobile Equipment Identity number
  - unique to each device
  - can be blocked if device is stolen
- Other interesting information on device that would be hacked
  - E.g. to change language packs, phone lock removal, text etc.
- Big battle between mobile industry and hacking groups between c.1999 and now – has evolved to jailbreak / root community

‘Unlocking’ and IMEI changing

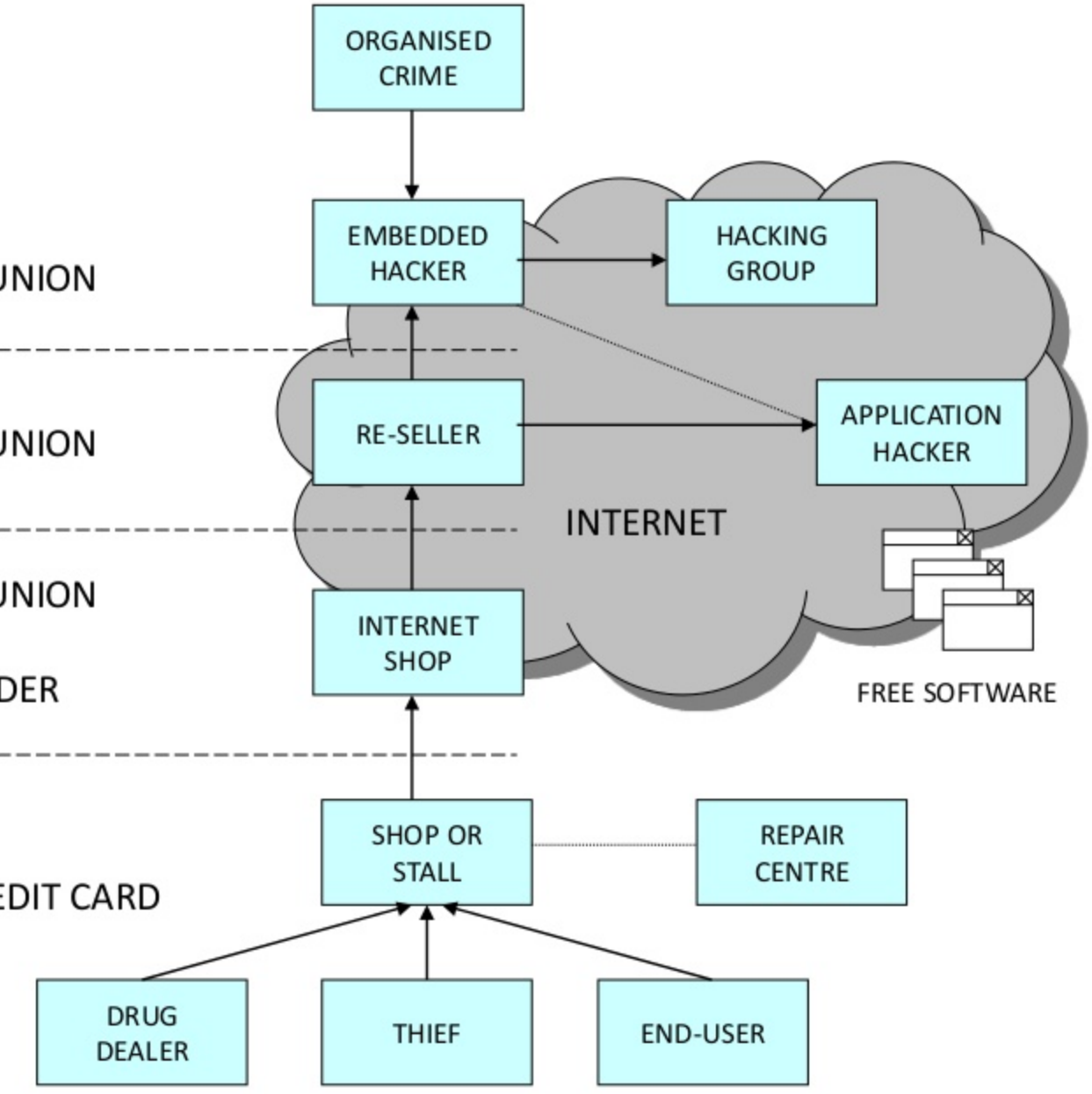
- What is ‘unlocking?
  - SIMlocks
  - Most hacking used to be aimed at the SIMlock area
- The security area in the handset would protect all sensitive data – including IMEI and SIMlock
- What is a dirty hack?
  - Hacks targeted against the security area would often cause corruption to data – including the IMEI.
  - Data such as RF calibration settings would often be wiped out
- Hacking tools usually dual-use (SIMlock and IMEI)
  - Causes problems in countries where IMEI changing is illegal – difficult and costly to get direct proof

Historic Criminal Structure



Historic Financial Structure

VALUE	METHOD
£5000+	WESTERN UNION
£500 - £5000	WESTERN UNION
£50 - £500	WESTERN UNION PAYPAL POSTAL ORDER
£10 - £30	CASH DEBIT / CREDIT CARD



Examples of Hacking Hardware

- Standard service repair equipment
  - Fraudulent purchasing of manufacturer's equipment
- Mass produced hardware by hacking groups
  - Griffin Box
  - UFS-3 (Twister)
  - Blazer
  - Clips

- Evolution
  - New equipment was constantly developed as new models were released
  - New technologies and hardware security to ensure revenue

Mass Manufacture of Hacking Hardware

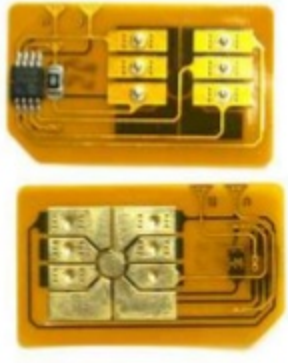
Examples of Hacking Hardware (2)

- Most hacks steal their solutions from already existing hacks
  - May seem to be 22 hacks available – just old hacks re-packaged.
    - Different front-end to software
    - Different hardware
  - the 'golden' part of the source code is from 1 hack

- Lots of 'ghost' hacks that are aimed at defrauding people
  - same in 2012 with jailbreaking on iOS6

Hardware Hacking Methods

- EEPROM cloning or ‘Chipping’
  - Old method
  - Copied EEPROM with basic equipment
  - Main aim to put EEPROM with no SIMlock on
  - Result: IMEI number was cloned
- PIC’s (Programmable Integrated Circuits)
  - Execute small sequences of commands
  - Placed in-line to ‘snatch’ or modify data
- Flash device hot-swapping (almost impossible now)
- Exploitation of boundary scan ports
- External clips and dongles
- Note: less economical than software hacks

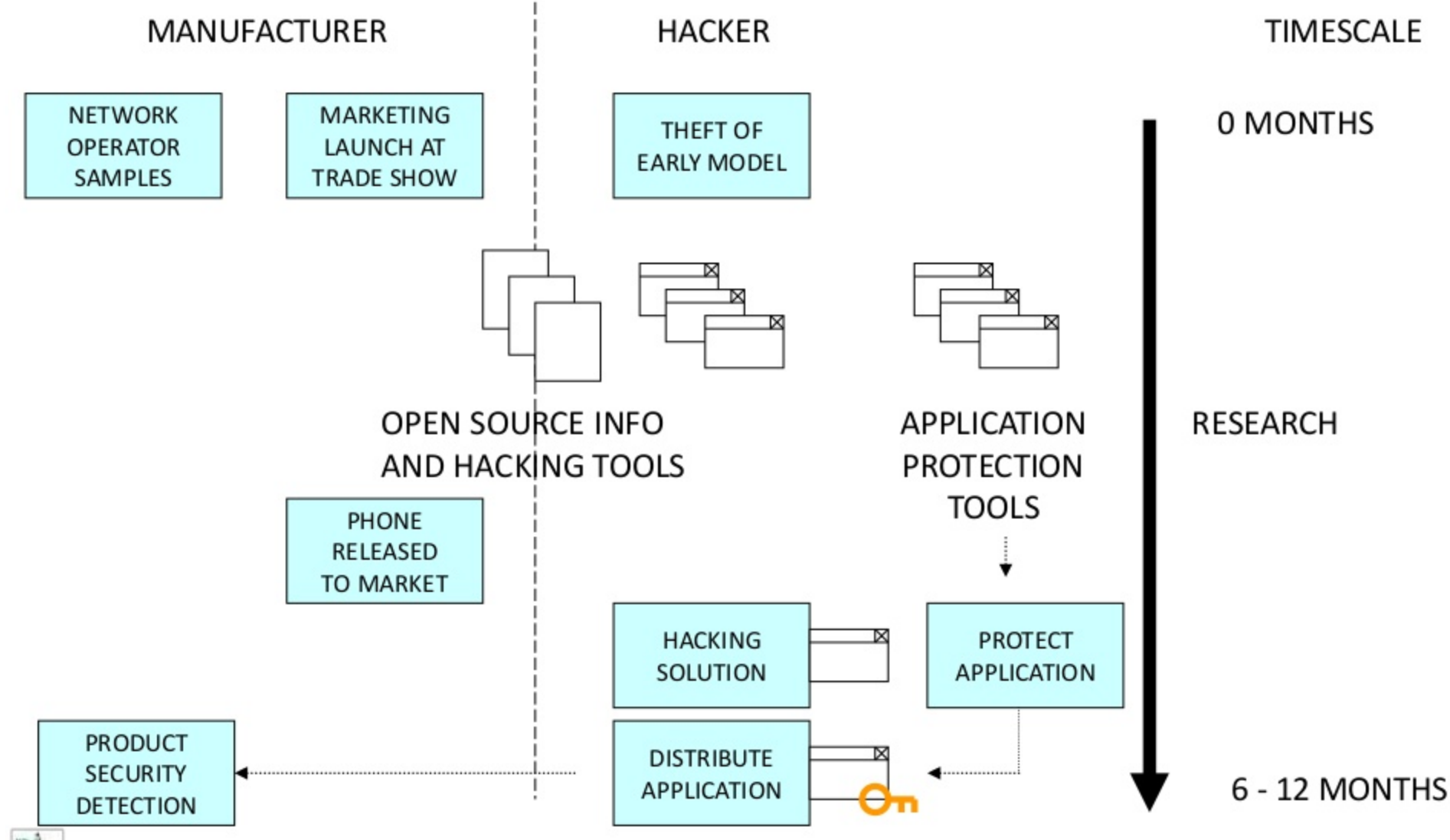


In-line PIC Between SIM and Device

Software Hacking Methods

- Direct change
  - Breaking a programming algorithm
  - Finding the correct test interface protocol command
    - Still used(!) serial communications / USB monitoring equipment
- Modifying binary files (software download files)
  - Inserting jump code
  - Hijacking other functions in the code to subvert security
  - Taking advantage of software design flaws
- Abuse of boundary scan to monitor phone processes
- 'Dumping' to logs of data from secure areas
- Brute force cracking of algorithms
- Theft of information from Design Centres / Factories / Service Centres
- "Voodoo Galaxy SIII SIM unlock" tool required device to be rooted…

Typical (Old) Software Hack Methodology



Use of Hardware Clips – 5 Second Unlocking!

- Simple to use, takes it's power from the handset
- Contains a Programmable Integrated Circuit
- Bombards the handset with commands in a repetitive sequence
- The handset eventually gives up and resets itself – unfortunately resetting the SIMlock!

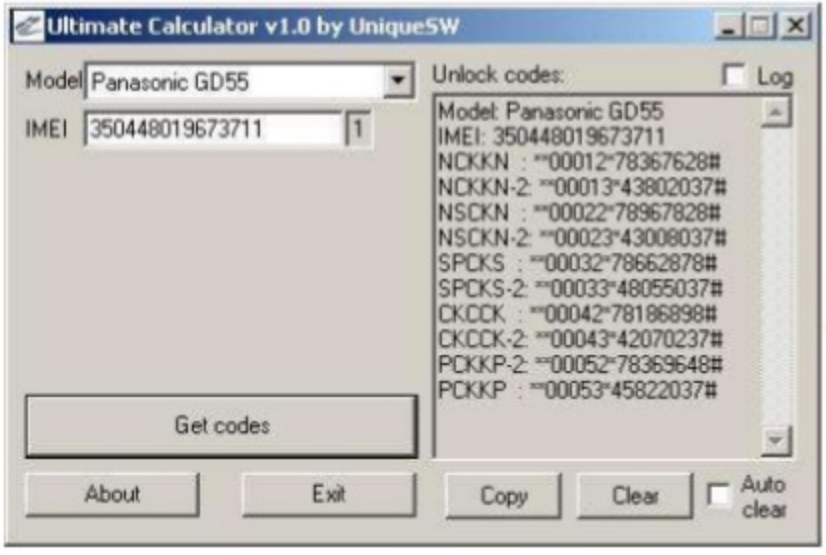
- This type of attack was used on many different makes of handsets
- Clips have now evolved and the term is usually used in reference to dongles

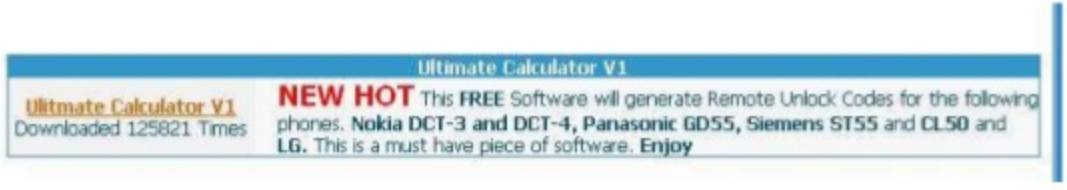
“Logs”

- Used as a method of continually generating revenue for the real hackers and re-sellers at the top of the food chain – a historical issues for hackers
- Original concept by 3 Nokia hackers and dealers from Serbia:
  - George, Boban (Slobodan Andrics) and Dejan (Dejan Kaljevic)
- How do logs work?
  - Encrypted by hackers to avoid cracking by other hackers
  - An example:
    - Crack the master security locks -> generate an encrypted log of security area information -> close the security lock on the handset again!
- ‘Logs’ will be available only if the hacking solution is two part
  - ‘Dumb’ client application to communicate with handset
  - Data is sent to hacker / re-seller
  - Corresponding data to unlock / change IMEI received from hacker / re-seller

CK Algorithm Breaches

- Some manufacturers and ODMs used symmetric algorithms based on the IMEI number to generate CK codes
  - Broken and every possible iteration for each IMEI available
- Later versions cracked the factory / service tools because they were leaked rather than cracking the handset





- Down to poor manufacturer security and breaking principle of no stored, shared secrets!

De-capping and Focused Ion Beam Equipment

Newer Hardware and System Level Attacks

- George Hotz – original iPhone jailbreak
  - Used hardware flaw to XOR data address and insert jump code to empty memory where he could execute his own bootloader
  - Allegedly assisted by European Infineon hacking teams
- Rooting
  - Various methods, exploiting vulnerabilities
  - Usually used as a staging area for other attacks (e.g. malware)
  - Examples:
    - RageAgainstTheCage, uboot, zergRush, gingerbreak
    - Other private exploits
  - Some manufacturers providing it as a service in order to prevent people hacking
- Legal battles around this area (e.g. US copyright office 2010, 2012)
  - OK to remove SIMlocks and root devices

Newer Motivations

- Main targets / motivations recently have been:
  - **Rooting / jailbreak device** – for piracy / other apps / custom OS / spyware
  - **SIM unlocking** – break out of subsidy (cheap device) / fraud / export of stolen devices
  - **IMEI changing** – re-enable stolen handsets in same country
  - **Launchpad attacks** – spyware / malware / anti-theft tools / in-app billing
  - **Fixing issues** – e.g. old SIMlocked device, can't contact operator

Handset Embedded Security Evolution (to 2012)