From Hacking, Startups to HackLabs

Global Perspective and New Fields

Philippe.Langlois@TSTF.net

Good morning

- Bio (Worldnet, Intrinsec, Qualys, TSTF, /tmp/lab, HSF)
- Not the usual “Risks & Crimes” FUD approach
- What are we building together anyway?

Agenda

- **Evolution: Chivalry, Hired Guns, M/I Complex**
- The ongoing battle, today
- The multiple perspectives
- Natural forces and underlying dynamics of security

Hacking & Security : the origin

Different forms... and beliefs

- Wanabee & the kid who hacker DoD
- Crackers & Robin Hood
- Researchers & “only one hat?”
- Open Source developers
- Free thinker? Who is this Kant again?

Criminals?

Startups

- Natural motive “People say I’m a criminal”
- “Let me show I am much more than I appear”
- Security is the obvious field
- Other domains (P2P, ISPs, Open Source...)
- From security to surveillance or forensics, commercial slippery path

Now community space creators?

- Innovation labs called “hacker spaces” ?
- New movement, 2008 mostly. CCC pioneered.
- Mostly Hardware, Rapid Prototyping, Physical security, Chip reverse engineering
- The community “it’s possible” effect
- Old meaning of “Hacker”?

Old meaning of hacking

From: T Biehn <tbiehn@gmail.com>
Subject: **Re: [Full-disclosure] Hacker Space Fest 2009 CFP: Call For Paper**
Date: Wed 15 Apr 2009 21:54:46 GMT+03:00
To: Valdis.Kletnieks@vt.edu
Cc: full-disclosure@lists.grok.org.uk

Valdis,
Mr. Mailinglist's stated intention was ruin, as clearly can been seen
from the e-mail.
Ruiners haven't forgotten... The old definition of 'hacker' is just
archaic. Sort of like you're trying to bring back 'gay means happy.'
I bet you love the HOPE kool aid.

-Travis

Anyway, thinking out of the box

- What's the name of this conference again?
- Hack == smart piece of non-linear thinking in a box?
- Await many more non-linear experiments and successes from this community

Agenda

- Evolution: Chivalry, Hired Guns, M/I Complex
- **The ongoing battle, today**
- The multiple perspectives
- Natural forces and underlying dynamics of security

The security & hacking picture today

- Strong evolution from the “All Insecure” of the 80s/90s
- “Lethal 0-day” diminution, you **can** be ok
- Ever increasing war zone, not only IP
  - GSM, DECT, Bluetooth
  - Pre-infected Factory default USB-keys, Facebook
  - HSM & Hardware attacks

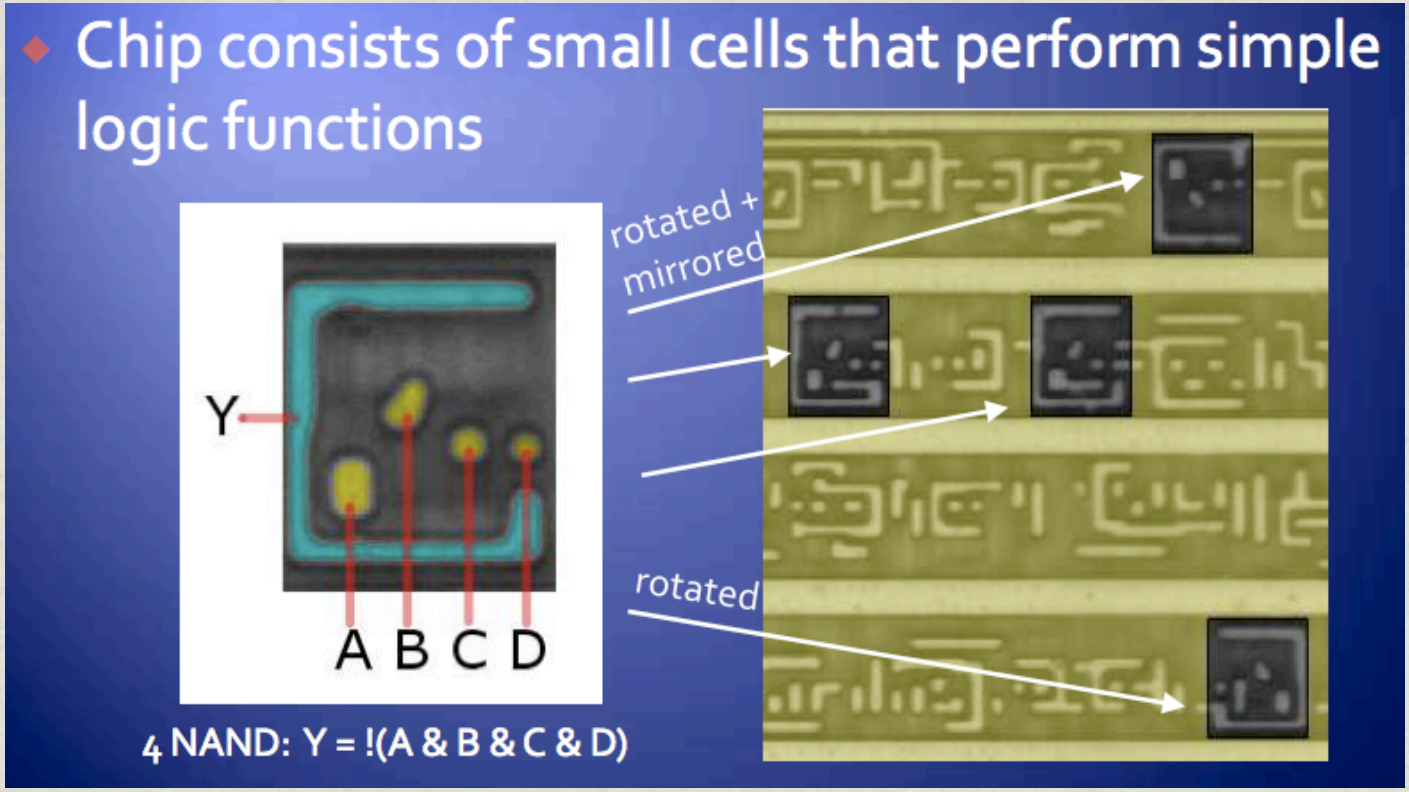
Flipside... everywhere

- GSM - Vulnerabilities, better fixes & privacy
- P2P - may well be the next distribution method for media creations
- DRM - Gaming & Mobile limitation create the future best reverse engineers
- What's next? communication methods for the masses?

Brazilian MIL sat hacking

"Brazilians all over the country are using **modified amateur radio equipment to communicate with each other using US Military communications satellites** — effectively creating their own CB radio network on the backs of the US Military. Recent efforts to crack down have resulted in arrests of some of the users, however the behavior still continues today."

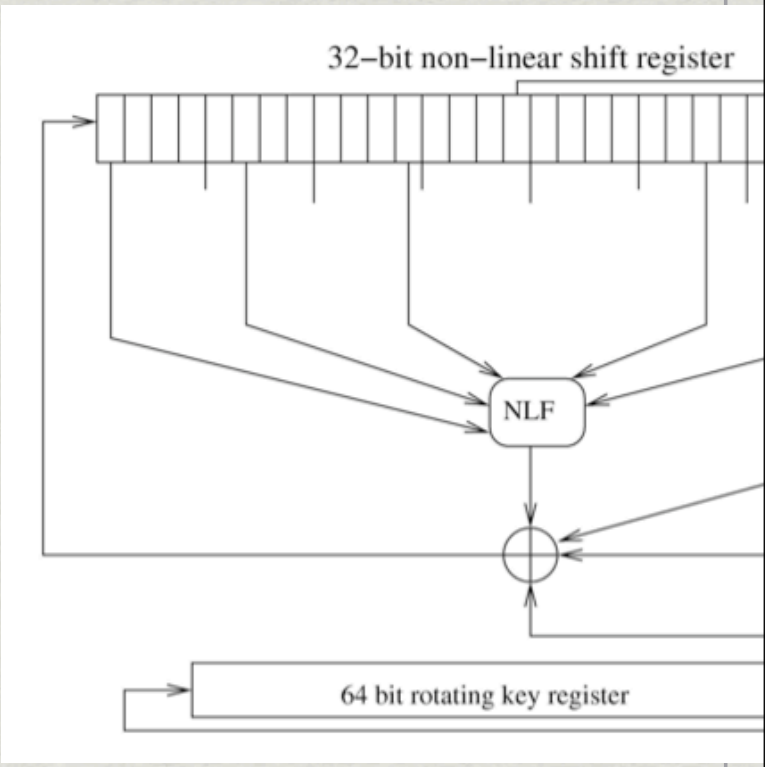
Hardware Reverse Engineering: Acid & Microphotography



- By: Karsten Nohl, Flylogic, Starbug

Crypto-linearization & SAT Solver

- Hackers & University join efforts for more security
- Bleeding edge crypto not only in theory
- Accessible to non-math geniuses



FPGA hacking & backdooring

- My rootkit in an ASIC ?
- Commoditization of military techniques
  - Iraq war printer-borne worm? anyone?
- Accessible, affordable, in full emergence

Hacking from the dead

- Old technique still working
  - Effective black hat means less 0-day, ninja hacking
  - Bruteforcing, Apps vulnerability, Sentinel-hacks
  - End-user vulnerability
  - Old vectors (X25, Modem, Email)
- Still some room to grow, products to come

Exotic network hacking

- ATM vulnerabilities
- SS7 & SIGTRAN hacking
- UMTS & Wifi radio-level overflows
- Microwave links

Battle will go on

- New technology, new ways to hack it, new way to defend
- What's important is the maturity: focus, resource optimization, vision
- And the capability to detect interesting creation on the way (hint! hint! Startups!)

Agenda

- Evolution: Chivalry -> Hired Guns -> M/I Complex
- The ongoing battle, today
- **The multiple perspectives**
- Natural forces and underlying dynamics of security

The Enterprise Domain

- User challenge, change-management challenge, maturity challenge
- Commoditization of attacks
  - Available tools
  - Research and unfixed vulnerabilities
  - Former MIL / INT domain
- Vision: the fog of war & the expertise

What about the crisis?

- Companies still have money, some people won’t
- Clear target, available workforce
- Security will be as important as today anyway

The Builders Domain

- Security got manageable!
- Tools: QA, Updaters, Online-error/crash reporting
- Methods: Risk models, Process/Workflows
- Education: Ross Anderson, Academics, Practical
- Validation: Third party help, prefer the contracted one

The Users Domain

- Loser so far, no direct benefit from security, only hassle
- Seen as a child, resource-less actor
- If involved in security and benefit, would do better
- Trust within, maturity-related problem

Future struggle zones?

- Privacy effort?
  - After Cloud computing, Surveillance hype
- Education / end-user effort
  - Self insured by the “asymetrization” of computing (TPM, DRM, lock-in) for “elite”
  - Still not enough of training combining business and security

Agenda

- Evolution: Chivalry -> Hired Guns -> M/I Complex
- The ongoing battle, today
- The multiple perspectives
- **Natural forces and underlying dynamics of security**

Balance & Equilibrium

- Security vs. Business
- Two ideal goal
- Only balance between them, compromise
- Requires maturity

Natural forces

- Any action induces a counter action if its global benefit for everyone obvious
- Heat + Pressure = Mutation
- Clear warning for some avenues (DRM, Obscurity through Security, ...)

Thank you!

- Questions
- Philippe.Langlois@TSTF.net