TECHNISCHE UNIVERSITÄT DRESDEN

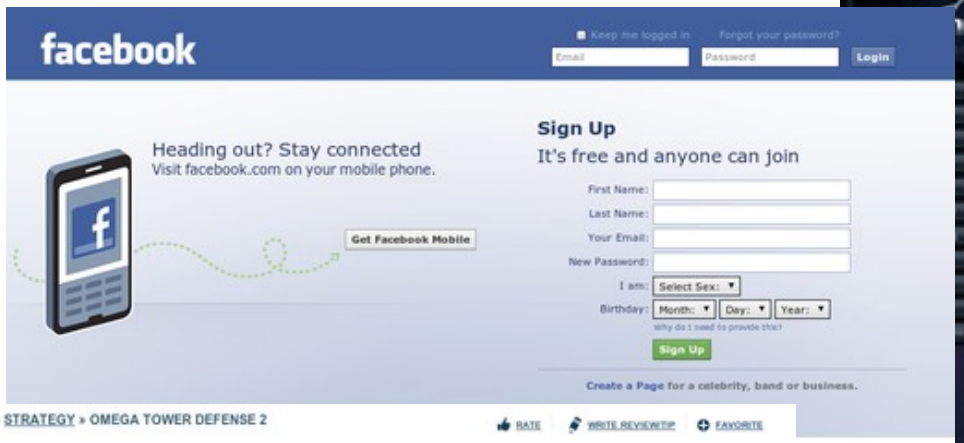
Faculty of Computer Science Institute for System Architecture, Operating Systems Group

Native Client: A sandbox for portable, untrusted x86 native code

Bennet Yee, David Sehr, Gregory Dardyk, J. Bradley Chen, Robert Muth, Tavis Ormandy, Shiki Okasaka, Neha Narula, Nicholas Fulgar (Google Inc.)

Dresden, 2010-04-27

Web 2.0


facebook
Keep me logged in
Forgot your password?
Email
Password
Login
Heading out? Stay connected
Visit facebook.com on your mobile phone.
Get Facebook Mobile
Sign Up
It's free and anyone can join
First Name:
Last Name:
Your Email:
New Password:
I am:
Select Sex:
Birthday:
Month:
Day:
Year:
Why do I need to provide this?
Sign Up
Create a Page for a celebrity, band or business.


Forschung - Arakis

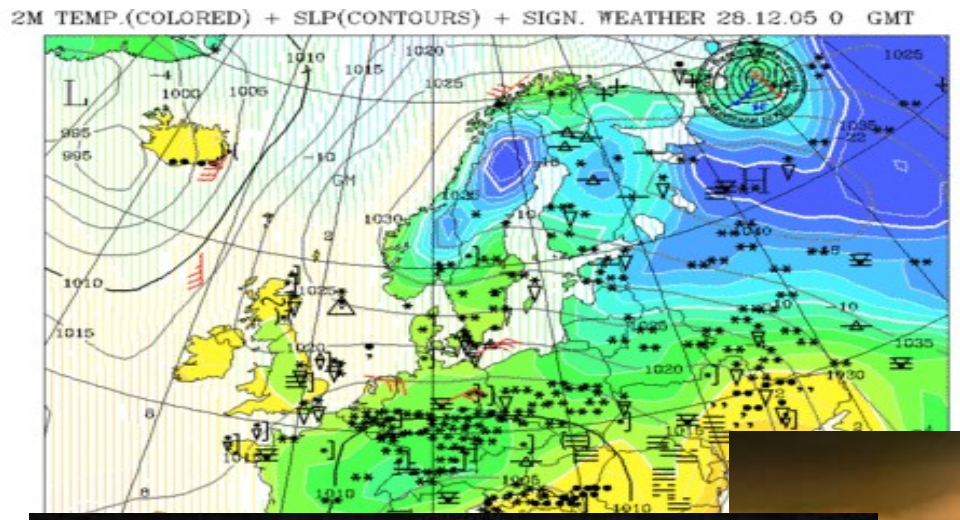
GAMES » STRATEGY » OMEGA TOWER DEFENSE 2
RATE
WRITE REVIEW/TIP
FAVORITE

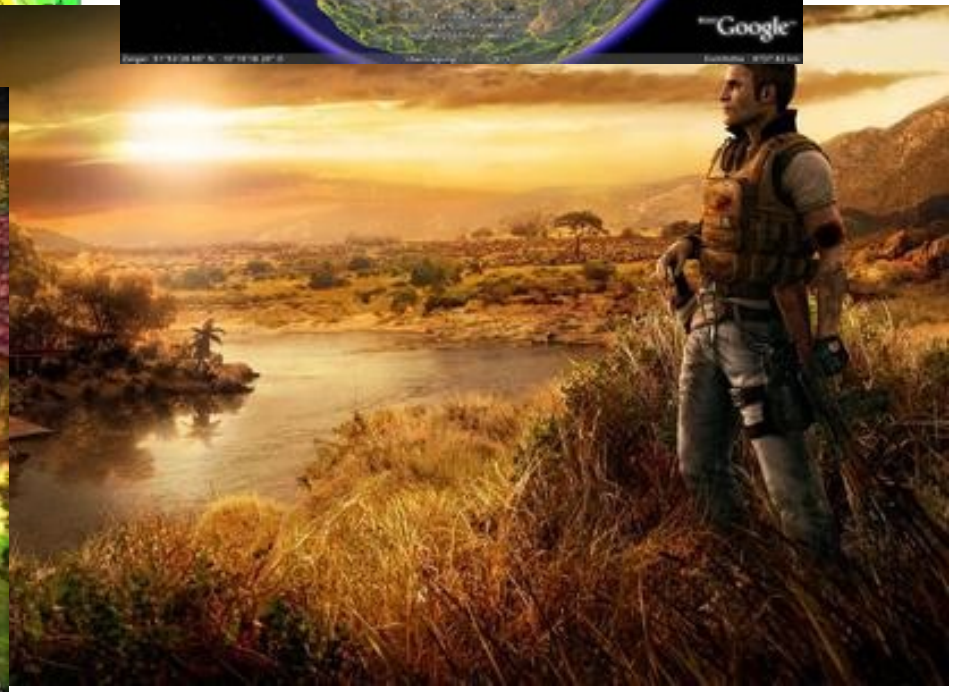

Score: 1715
Life: 6
Money: 43
Wave: 12
PAUSE
EXIT
Click to build this tower. If it is red you can't build it. Press space to cancel this tower.


twitter
Search
Discover what's happening right now, anywhere in the world
Justin Bieber
Dear Haters
Lakers
LeBron
TRENDING TOPICS
OKC
See who's here
Friends and industry peers you know. Celebrities you watch. Businesses you frequent. Find them all on Twitter.
Top tweets
View all
Creflo_Dollar Your attitude determines your mood and your mood determines your results. Set your attitude in line with God's word and get great results!!!
7 hours ago
danielliejonas Sooooo proud of my husbad!!! He killed it!! <3
7 hours ago
WBrettWilson 18 hours 2 add followers - to kick up my donation 2 Military Families Fund - and 2 be eligible for an iPad draw. If you can help - pls do!!
7 hours ago
New to Twitter?
Twitter is a rich source of instant information. Stay updated. Keep others updated. It's a whole thing.
Give it a try ›
Customize Twitter by choosing who to follow. Then see tweets from those folks as soon as they're posted.
Using Twitter for a business? Check out Twitter 101
© 2010 Twitter
About Us
Contact
Blog
Status
Goodies
API
Business
Help
Jobs
Terms
Privacy
Language: English

TECHNISCHE UNIVERSITÄT DRESDEN

Not yet Web 2.0





Native code execution

- Faster than interpreted code
- Make use of platform-specific assembly (e.g., SSE)
- Arbitrary code → Security threat
- **NaCl:** framework to support safe execution of x86 machine code in a sandbox

Recap: Software Fault Isolation

- Robert Wahbe, 1993
- Plugins in sub-address spaces (segments)
  - Segment matching: check that plugin stays within sandbox
    - Mostly static checks
    - Additionally insert runtime checks
  - Address sandboxing
    - For each memory access fix upper bits of address to segment idx
  - System calls & system resource accesses → cross-domain RPC
- Limitations
  - RISC (extended to CISC: XFI, Erlingson 2006)
  - x86 register scarcity

Native client

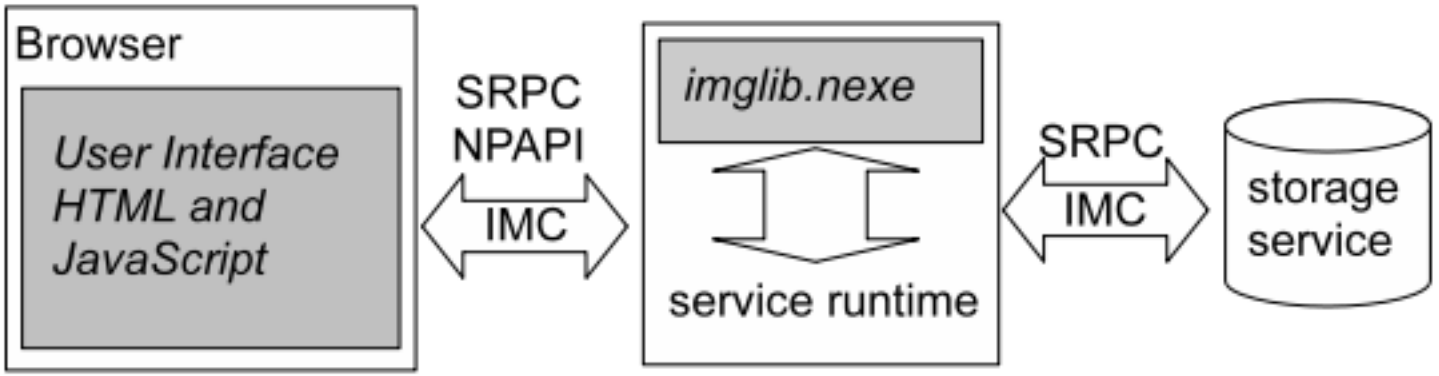


Figure 2: The hypothetical photo application of Figure 1 with a trusted storage service.

Sandboxing native code

- Outer sandbox:
  - System-call monitoring
- Inner sandbox
  - Static checking at load-time
  - Dynamic runtime checks
- Service runtime
  - System-level interface

Static checking

- Reliable disassembly
  - All valid code within text segment
  - No self-modifying code
- No unsafe instructions
  - SYSENTER, INT, segment-related instructions, RET
  - Ring 0 instructions
- Control-flow integrity
  - Ensure each jmp goes to a valid instruction

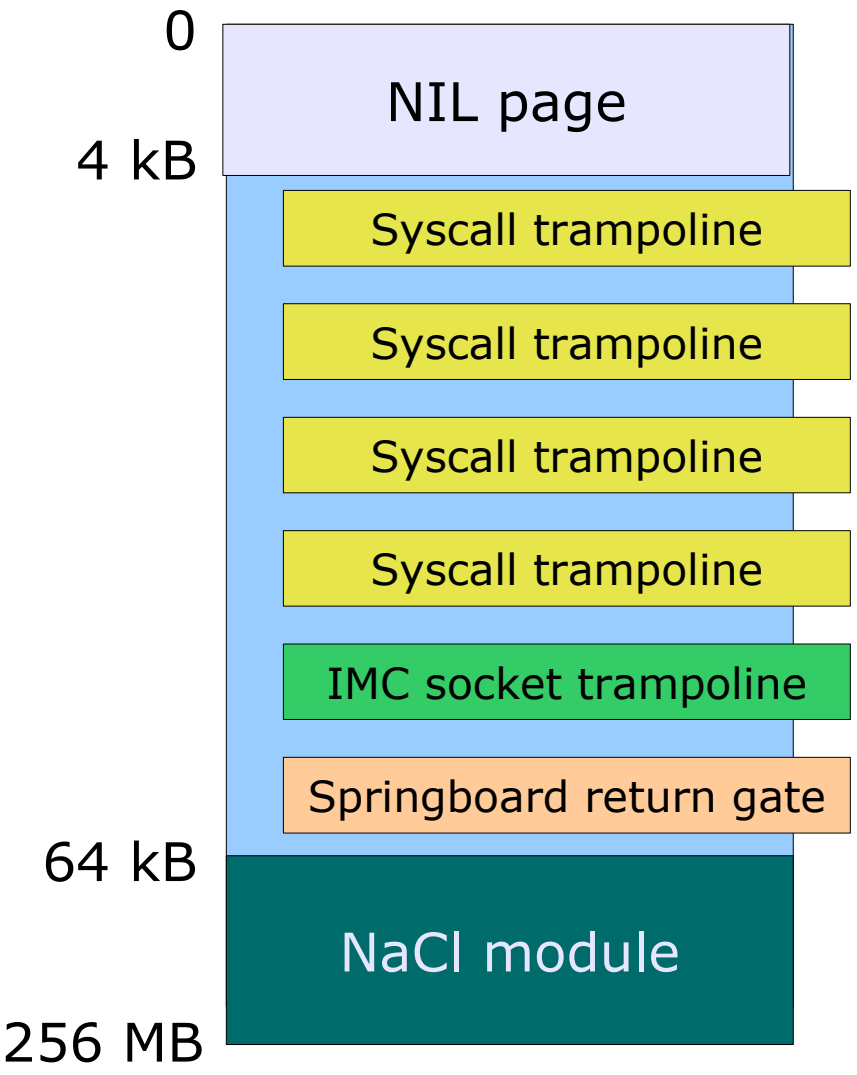
Runtime checks

- Indirect jumps: nacl_jump

  ```
  and %eax, 0xFFFFFFe0
  jmp *%eax
  ```

- Use x86 segmentation to enforce sandbox
  - Restriction: x86/32bit
- Disallow (asynchronous) hardware exceptions
  - Would need to copy with stack segment, which is invalidated during NaCl execution

Service runtime



- Unrestricted code
- System call trampolines
  - save/restore segments
  - 32-byte aligned
  - one per system call
- Springboard
  - Allow calls into NaCl modules
  - Potentially unrestricted
  - Start with HLT
- IMC sockets
  - Datagram-based
  - Higher-level protocols on top

Evaluation

- Modified GCC 4.2.2 + Binutils 2.18
- SPEC2000: average 5%., top 12% overhead in NaCl mode
- Near-native performance for
  - Computer graphics
  - H.264 decoding
  - Quake (yeah!)
- Going into Google Chrome

Ben Hawks @ HAR 2009

"This is my tentative endorsement, that, yes, Native Client could actually win

…

but only if they lock Tavis Ormandy in a room for a year or two

…

and I'm worried about the outer sandbox, so you should be too."

Discussion

- Hack it?
  - Return-oriented programming works for fixed-length RISC instruction sets.
  - Doing harm depends on configuration of outer sandbox.