Flying Linux

Picture Copyright © Berke Breathed,
from *"A Wish for Wings that Work"*;
used without permission

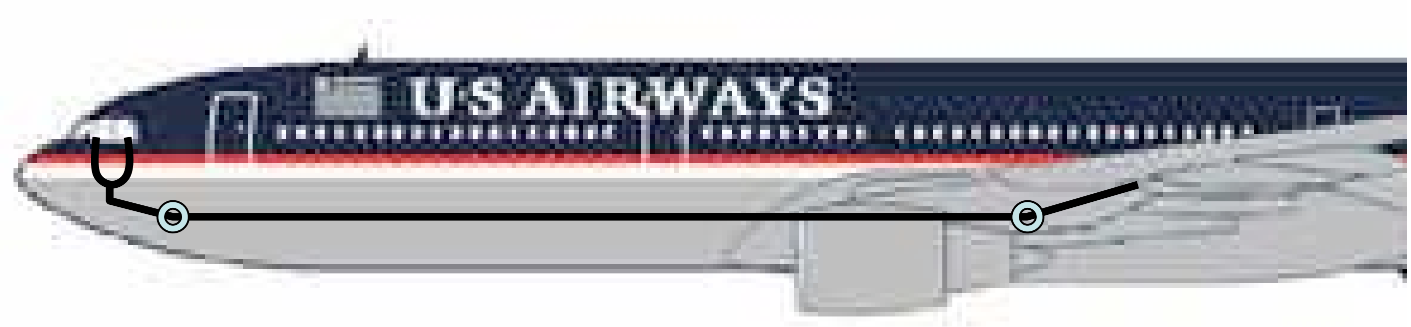
Daniel V. Klein

dan@klein.com

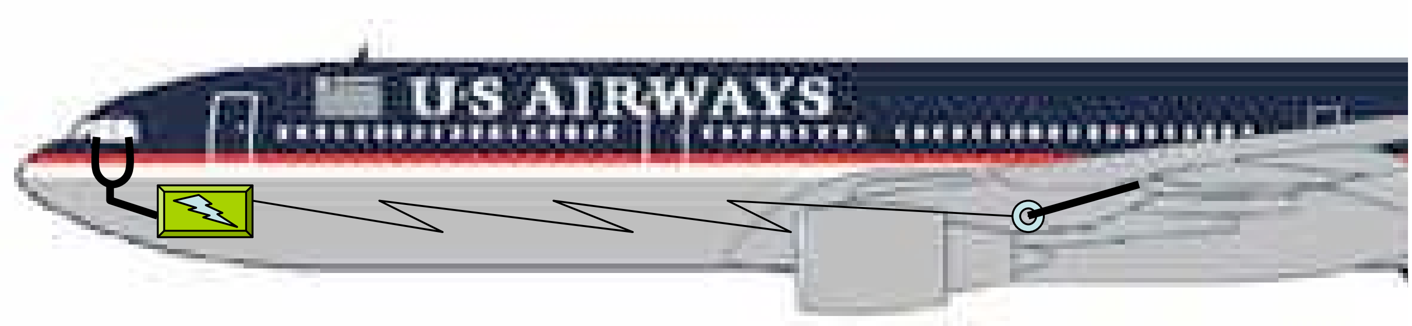
Airbus A330

"Digital fly-by-wire" aircraft

Linkage Flying



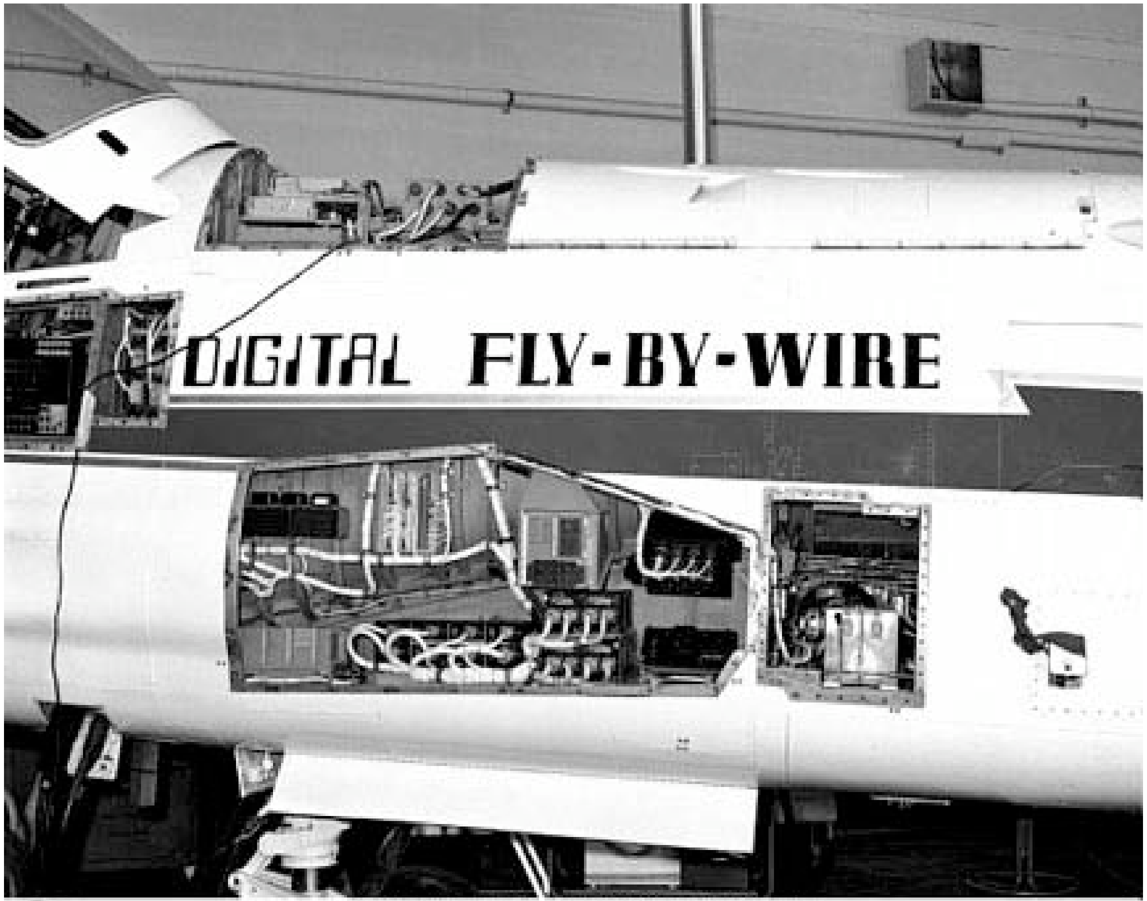
Digital Fly by Wire



Early DFBW

- Mercury
  - Glorified Missle Guidance System
- Gemini
  - Computer-based controls
- Apollo
  - Computer based, better UI

NASA 802 - F8-C



NASA Dryden Flight Research Center Photo Collection
http://www.dfrc.nasa.gov/gallery/photo/index.html
NASA Photo: E-24741 Date: 1971 Photo by: NASA photo

F-8 DFBW on-board electronics

Cool Things about DFBW

- On “old” aircraft, 1:1 linkage
  - Scaled Composite’s X-Prize winner
- On DFBW, pilot action expresses *intent*
  - DFBW translates into action – DWIM
    - Account for environment
    - Correction of errors (pilot induced oscillation)
  - Behaviorial Emulation
    - Space Shuttle Simulator

"This is so cool! I'm flying this thing completely on my Palm pilot!"

Unstable aircraft – F117A

- Faceted aircraft
  - Highly unstable in all 3 axes
- Cannot be flown without computer aid!
- Four pitot tubes out the front that sample air pressure

REDUNDANCY!

- Many DFBW are triple-redundant
  - Voting systems
  - Purpose-built systems
- F117A is quadruply redundant
  - So unstable that if computer crashes they break apart

Cars are becoming DDBW

- ABS
- Traction control
- Mercedez-Benz F200

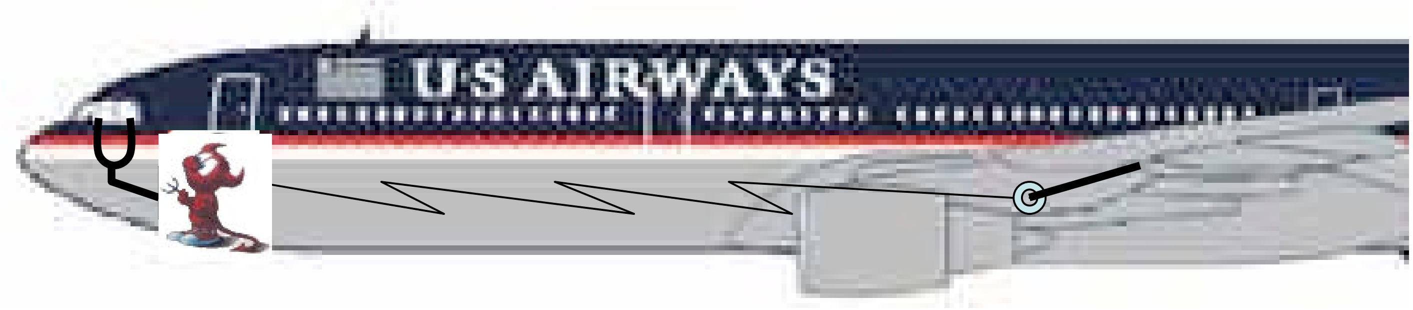
Digital Walk by Wire

Proprioception

- Short-loop reflexes

- Fly-by-wire implements reflexes
- Pilot (driver, walker) asserts intent

Would you fly if… ?



Where do you want to go today?

Not a Gamble I Want to Take!

It’s easy to make fun of Microsoft

- Ping of Death
- MyDoom
- “Crazy uptimes” with new IIS
  - 3 whole days!
- Blue screen of Death

CNN

You can’t test everything!

- Combinatorial testing
  - Odd interrelations
- Stress testing
  - Circuit breakers
  - Arkansas School plumbing
  - Golden Gate Bridge
- Correlative debugging
  - Temporal separation
  - Food allergies

Remember Y2K?

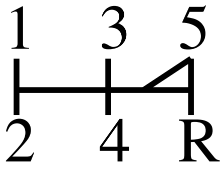
- No big deal
  - According to the media :-)
  - We always have backups!
- What about critical systems?
  - In US, extra staffing
  - In China, interesting solution…
- Perspective changes when it is *your* life!

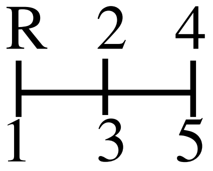
Do it by the book!

- Because it works!
- If everything else fails…
  - …try something new.
- If you survive…
  - …it goes in the book!

Interesting additions to the book

- Software Coding/Testing
  - Mariner 1: Missing hyphen in navigation code
  - Bug in X/Y/Z-axis code: `DO 100 I=1.3`
- Control systems
  - Wheels up while on ground
- Fighter plane autopilot
  - Invert aircraft after crossing equator
- Stick shift patterns





Failing to Do It By The Book

- June 4, 1996: Arianne 5 Crash
  - Software works in Arianne 4
  - Management: “No need to test in Arianne 5”
  - Integer overflow at 39 seconds halts processor
    - Float -> Int conversion
    - Code written in Ada
    - Program halt is *specified*
  - Subsequent test proved this
- Ada™ is *smart* – it knows better!
- C would have just corrupted memory and flown

Glenford J. Meyers

- We try to solve the problem by rushing through the design process so that enough time is left at the end of the project to uncover the errors that were made because we rushed through the design process.

Interesting Problems

- Timezones
- GMT
  - conventions change ca. 1927 (GMAstronomicTime)
- Feb 29
- `cal 9 1752`

```
   September 1752
Su Mo Tu We Th Fr Sa
       1  2 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
```

The Gimli Glider

- Air Canada 143 – July 23, 1983
  - B767 ran out of fuel at 41,000ft
  - FQIS (Fuel Quality Information System) busted
    - bad sensor, bad circuit breaking, no fuel gauges
  - Manually drip tanks at origin
  - Use specific gravity of jet fuel in calculation
- 1.77 lbs/liter *vs*. 0.9 kg/liter
  - 11,430 liters != 20,400 kg
  - 11,430 liters == 9,144 kg

Gimli Glider *(contd.)*

- Flying from Montreal to Vancouver
- Diverts to Winnipeg on first flameout
- Diverts to Gimli on second flameout
  - 132 ton glider, sink rate of 2,000 fpm
  - No fuel, no engines, no APU
- RAT
  - Powers ailerons, elevator, and rudder
  - Not flaps, slats, or landing gear!

Gimli Glider *(final)*

- Pilot does a “sideslip” to slow down
- Discovers that it is “Family Day” at Gimli
  - Runway 32L is a racetrack
- Nosegear collapses on landing
  - Stops safely, but fire in nose
  - Evacuation slides

- Repair crew from Winnipeg…
  - …runs out of gas

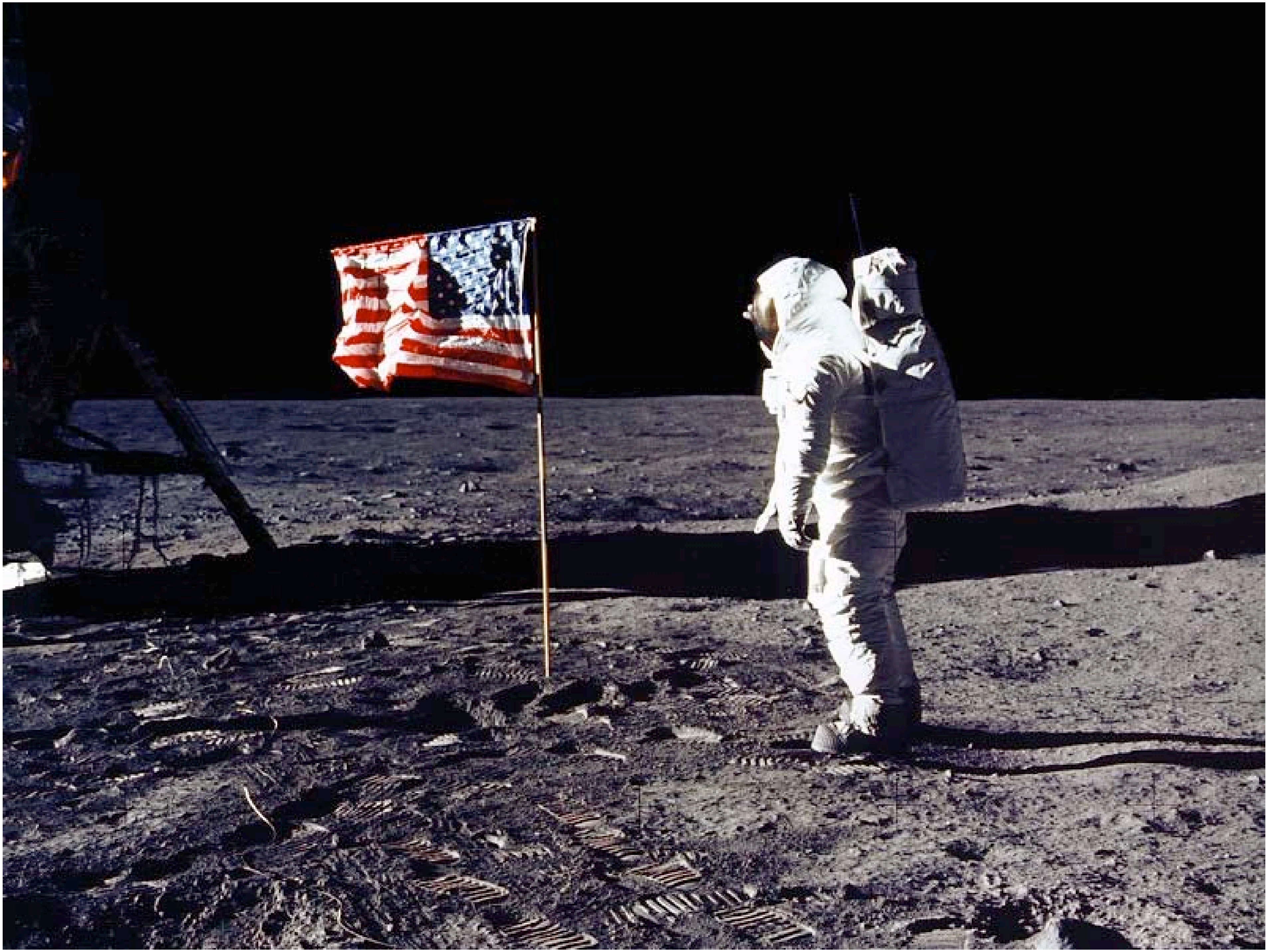
More Interesting Problems

- Marsmission crews
  - No TCP to Mars
- Epoch throughout kernel
  - 64-bit `time_t`
- Rebuilding my desktop
  - From BSDI to FreeBSD

In DxBW, *no room for error*

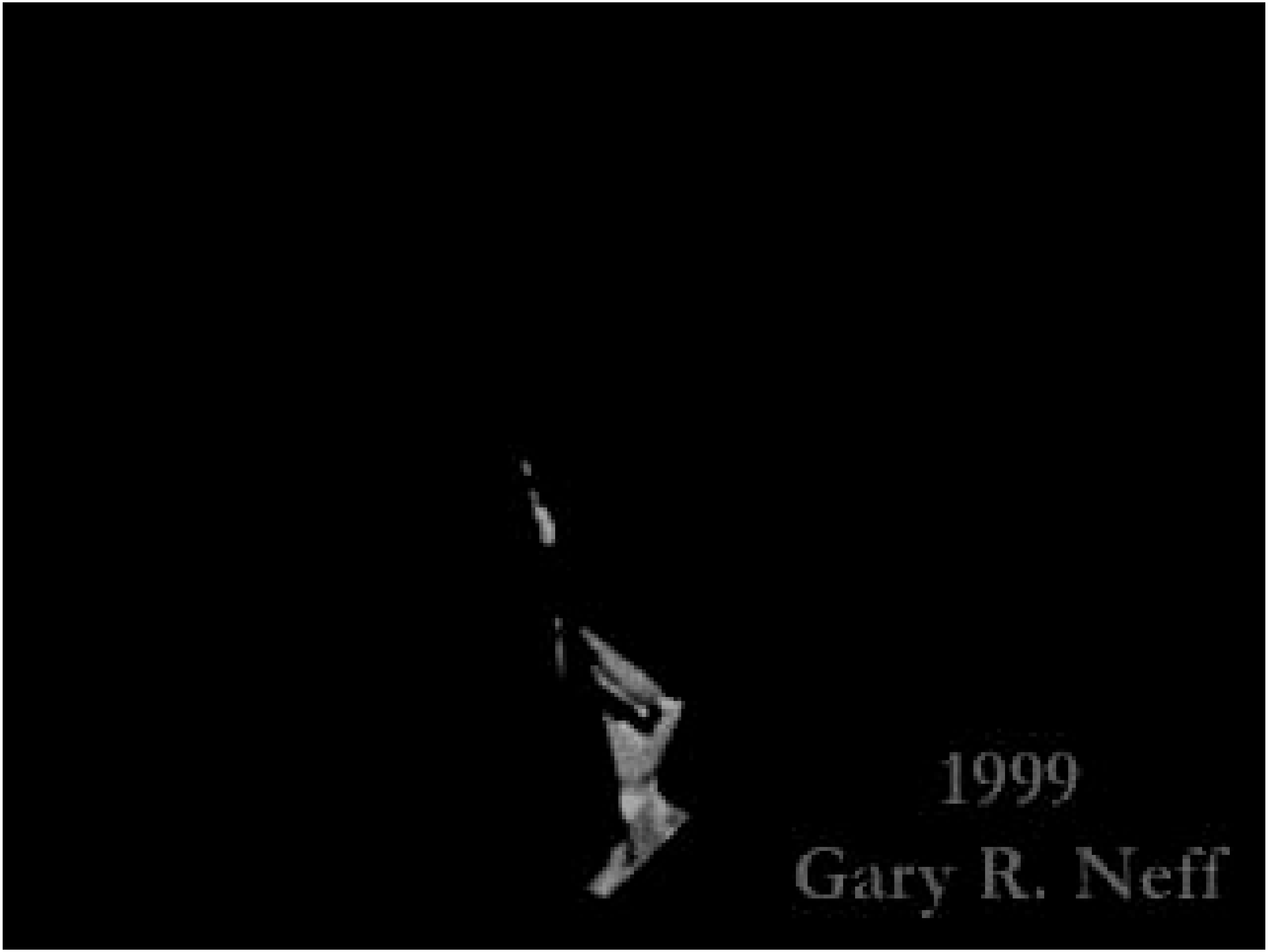
- Everything must be known
  - Timing, size, power
- No `#ifdef`
- No loadable modules
- No games :-)

- My phone sometimes hangs…



Landing was slightly “off”

- Flew until only 30 seconds of fuel remained
  - Looking for a parking space
- Landing was 3 miles downrange
  - Tunnel venting
- More interesting problems…



1999

Gary R. Neff

102:38:20 Aldrin: Got the Earth straight out our front window.

102:38:21 Armstrong: Houston, you're looking at our Delta-H.

102:38:25 Duke: That’s affirmative.

102:38:26 Armstrong: Program Alarm.

102:38:28 Duke: It’s looking good to us. Over.

102:38:30 Armstrong: (To Houston) It's a 1202.

102:38:32 Aldrin: 1202.

[Good radar data. Altitude now 33,500 feet.]

102:38:42 Armstrong (To Buzz) What is it? Let's incorporate…
(To Houston) Give us a reading on the 1202 Program Alarm.

102:38:53 Duke: Roger. We got you... We're Go on that alarm.

102:38:59 Armstrong: Roger. (To Buzz) *(Garbled)* 30.

102:39:01 Duke: 6 plus 25. Throttle down...

102:39:02 Aldrin: Okay. Looks like about 820...

102:39:03 Duke: ...6 plus 25, throttle down.

Real-time debugging

- 400,000 km from Earth to moon
- 10 km to go
- 99.9975% of the way there
- Uh oh!
  - The computer signaled “overloaded executive job queues”
  - Potential loss of execution of certain tasks
  - Potential life-hazard to crew

On-Star™

- GPS-based radio assistance for cars
  - They call you when there is a crash
  - Call from Ferry in Lake Michigan
- Apollo MOCR had software experts on-site
  - Steve Bales (26 years old) made on-the-spot “go” call
  - 10 seconds after landing, MOCR called MIT…
- No On-Star™ for commercial flights
  - No time to explain the problem!

Problem never seen in simulation!

- “Cycle stealing” – I/O system keeps looking for data.
- Rendezvous Radar Switch was “on”
  - Computer was looking for radar data
  - “Why is it on for *Descent*? Its meant for ***Ascent***!”
- The book said to do it that way…
  - …in simulation the radar switch was not connected!

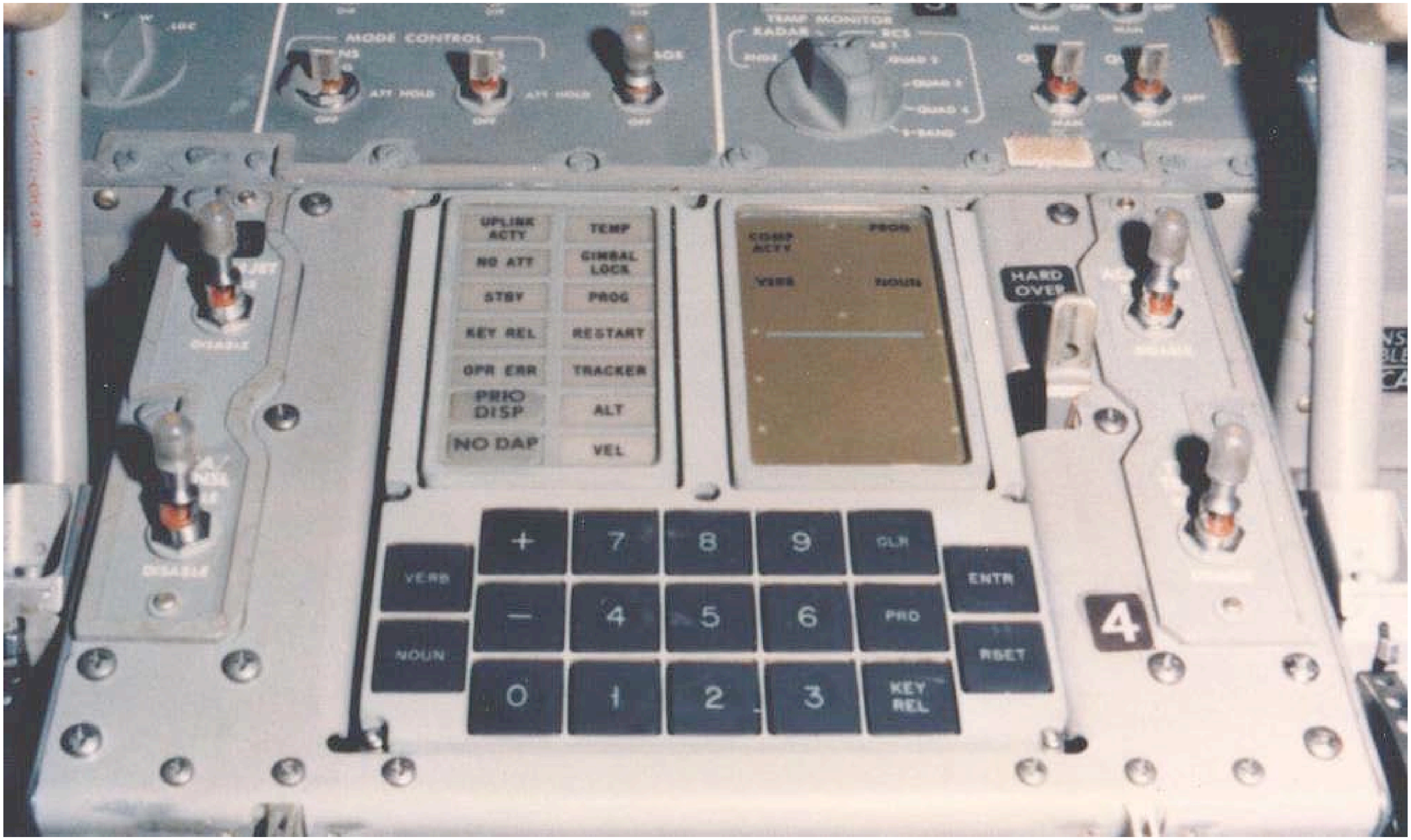
Apollo Computer

- The on-board Apollo Guidance Computer (AGC) was about 1 cubic foot
- 2K of 16-bit RAM
- 36K of hard-wired core-rope memory
  - Copper wires threaded or not threaded through tiny magnetic cores
- The 16-bit words were generally 14 bits of data (or two op-codes), 1 sign bit, and 1 parity bit.
- The cycle time was 11.7 micro-seconds.

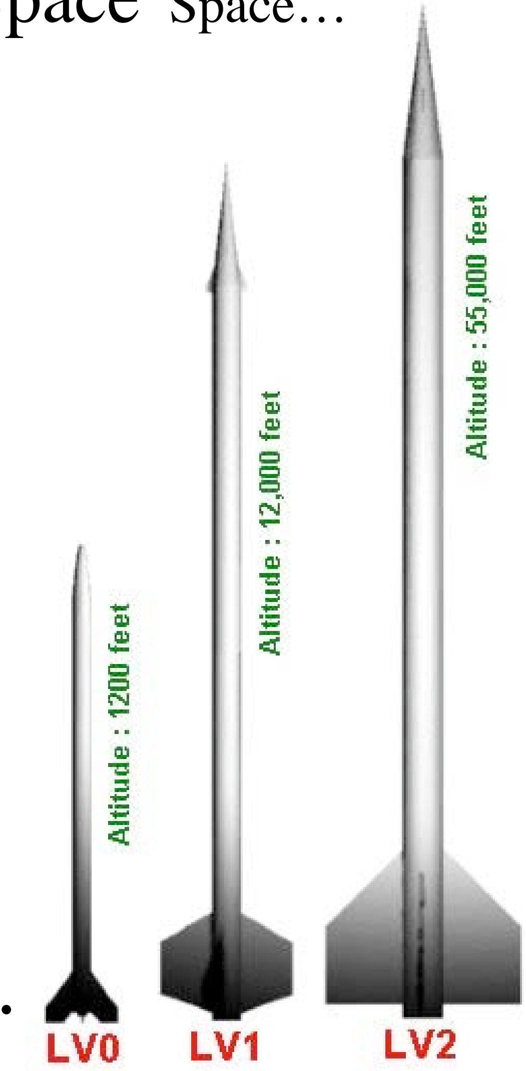
Programming

- Assembly language
- Interpretive reverse Polish language
- Scaling was fixed point fractional
- An ADD took about 23.4 μsec.
- The OS featured a multi-programmed, priority/event driven asynchronous executive packed into 2K of memory.

DSKY- Display and Keyboard Assembly



Linux in Space Space Space Space…



- Okay, atmospheric, sub orbital…

PSAS: Linux off the ground?

- June 2, 2003: “From 5:00pm - 2:30am we worked on the software and firmware for the avionics system, trying desperately to get it to work for USENIX [June 9]. We even got pretty close!”
- “There’s nothing like getting 25 people out to a desert in the middle of nowhere for a launch and knowing if you screw up your rocket will become a giant lawn dart.”
- October 15, 2004 launch cancelled

Two Quotes from Perkins [USENIX03]

- Real-time Operating Systems (RTOS's) hand-built in assembly language are not a good idea for a complex, multi-volunteer effort. An off-the-shelf RTOS with better networking and free, easily learned development tools is much more appropriate.
- The navigation software needs serious computational power: a CPU with hardware floating point support is highly desirable.

Modern OS's

- FreeBSD Kernel ≈2,000,000 LOC
- Linux Kernel ≈5,500,000 LOC

```
find . -name \*\[chsS] | xargs wc | egrep total
```

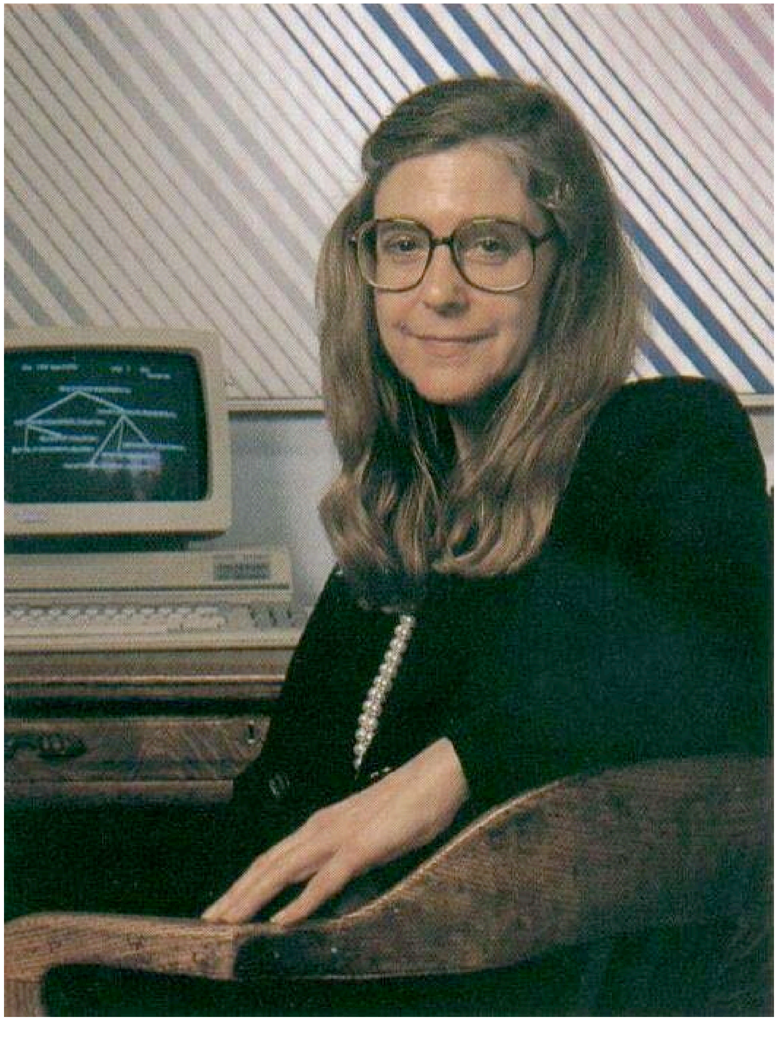
Linux: Babettes Gaestebud

Linux: Babette's Feast

- Filled with wonderful things!
  - Do you recognize them all?
  - Do you understand them all?
  - Are they safe to use?
- Simple question:
  - How many switches to `ls` do you know?
  - *There are 33 of them!*

The Right Stuff

Margaret Hamilton - The Right Stuff



The Hard Stuff

The Boring Stuff

- Writing cool code is fun!
- Writing documentation is not fun
  - Especially in English
- Writing test code is not fun
  - And it is hard, too!
- Many bugs are merely an annoyance
  - The BUGS section in the man pages…

Andrew System @ CMU

- Mail

  Send pictures, sounds, signatures…

  …but delivery was unreliable…

  …even for plain text!

- Multi-threaded system

  `printf` was not thread safe!

Who do you trust?

- *Volunteers* wrote Linux
  - They do what they want!
- Companies invest in Linux
  - IBM, Novell
  - They tell *employees* what to do
- And then who owns it?
  - SCO

SCO vs. IBM (& Linux)

- Linus is Martin Luther
- SCO is the Catholic Church
  - – IBM is Henry VIII & the Episcopal Church
  - – Dual Papacy – a Disputed Primacy
    - Novell is in Rome
    - SCO is in Avignon
    - The people are in the middle
- Microsoft is Islam and the Ottoman Empire

Two of the 95 Theses

“Disputation on the Power and Efficacy of Indulgences”

#5 The pope has neither the will nor the power to remit any penalties beyond those imposed either at his own discretion or by canon law.

No Licensing Fees!

#88 Surely a greater good could be done to the church if the pope were to bestow these remissions and dispensations, not once, as now, but a hundred times a day, for the benefit of any believer whatever.

Open Source is Good!

Who do you trust?

- February 24, 2004
- SELinux
- “Linux Gets Security Boost from NSA”
  - Not the CIA, but…

http://www.internetnews.com/dev-news/article.php/3317331

The Farewell Dossier

http://www.ranum.com/security/homeland_security/
http://www.nytimes.com/2004/02/02/opinion/02SAFI.html

- 1970’s – The cold war
- Col. Vladimir “Farewell” Vetrov
- Soviets covertly buys/steals hardware and software from US
  - US in arms race with itself
- Soviets want control software for trans-Siberian gas pipeline
  - US arranges Trojaned software

All your base are belong to us!

- Soviets test code, hardware
  - Passes test
- In real operation though:
  - Reset pump speeds, valve settings
  - Pressures exceed pipe and weld capacity
  - June 1982: Kaboom!
  - 3 Kiloton explosion, detected from space
- No casualties, but all software now suspect!

CIA Declassified Farewell

- But I didn’t see how the Trojan was triggered…

- Spooks don’t tell *all* their secrets!

- Am I paranoid?

Hypothetical Terrorism

- Passengers board in LHR
- “Unrelated actions” on board
- Plane lands in JFK
- Plane takes off from JFK
- All your ~~base~~ plane are belong to us

- Am I paranoid?

Open Source == Safe ?

- “Farewell” code checked by Soviets
  - Proprietary source
  - Possibly only binary available
- Linux truly open source
  - See code
  - Test it thoroughly…
  - …but not rigorously!

- Am I paranoid?

Linux Attacked the Most

- MI2G Security Group (London)
- Successful **Manual** Attacks in:

	January ’04	Nov’03-Oct’04
– BSD/Mac OS-X	555	11,370
– Windows	2,005	59,419
– Linux	13,654	154,846

http://www.macworld.co.uk/news/top_news_item.cfm?NewsID=7980

http://www.mi2g.com/cgi/mi2g/press/021104.php

Red Hat Phishing

- October 24, 2004

  Email from secalert@redhat.com says:

  “Go to http://www.fedora-redhat.com/ and download & install security patch”

- Am I paranoid?

Who contributes to the Kernel?

- I personally know:

  `phk@freebsd.org`

  `tytso@mit.edu`

  `sct@redhat.com`

- But who is:

  `sux@loplof.de`

  `kuznet@ms2.inr.ac.ru`

  `rzsfl@rz.uni-sb.de`

Who do you trust?

"On the Internet, nobody knows you're a dog."

Login Backdoor

- Ken Thompson alleges backdoor in `login`
  - Backdoor not visible in public code
- Compiler knows when it is compiling login
  - Inserts backdoor code
- Compiler knows when it is compiling itself
  - Inserts backdoor code
    - http://www.acm.org/classics/sep95/

- Am I paranoid?

Open Source == Safe ?

- Many eyes look at the code
  - Few (no?) eyes look at binary
  - Unified audit? Test harness?
- Is *all* the code examined?
  - Does *anyone* ***understand*** all the code?

Nobody Wants to Audit Code!

- Sardonix project

http://developers.slashdot.org/developers/04/02/01/2048217.shtml?tid=106&tid=126&tid=172&tid=185

http://www.securityfocus.com/news/7947

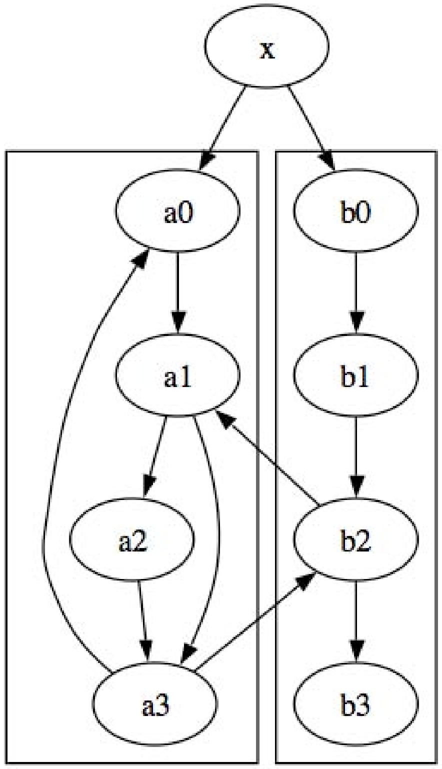
- A few good guys report vulnerabilities
  - Bad guys exploit them
- Would you want Diebold to use Linux?

Open Source Mistakes

- Servers that announce their version
  - *Hi, I’m SSH version 1.99, OpenSSH 2.1.1*
- Every initial connection should be a challenge
  - **Hi, I think I’m talking to SSH**
  - *Why yes, that’s right*

Graphviz

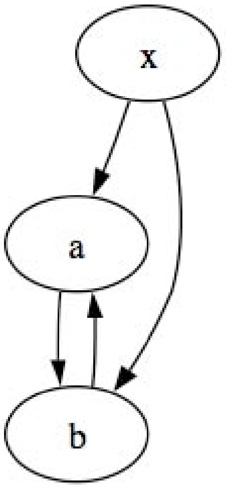
```
digraph G {
   subgraph cluster_c0 {a0 -> a1 -> a2 -> a3;}
   subgraph cluster_c1 {b0 -> b1 -> b2 -> b3;}
   x -> a0;
   x -> b0;
   a1 -> a3;
   a3 -> a0;
   a3 -> b2;
   b2 -> a1;
}
```



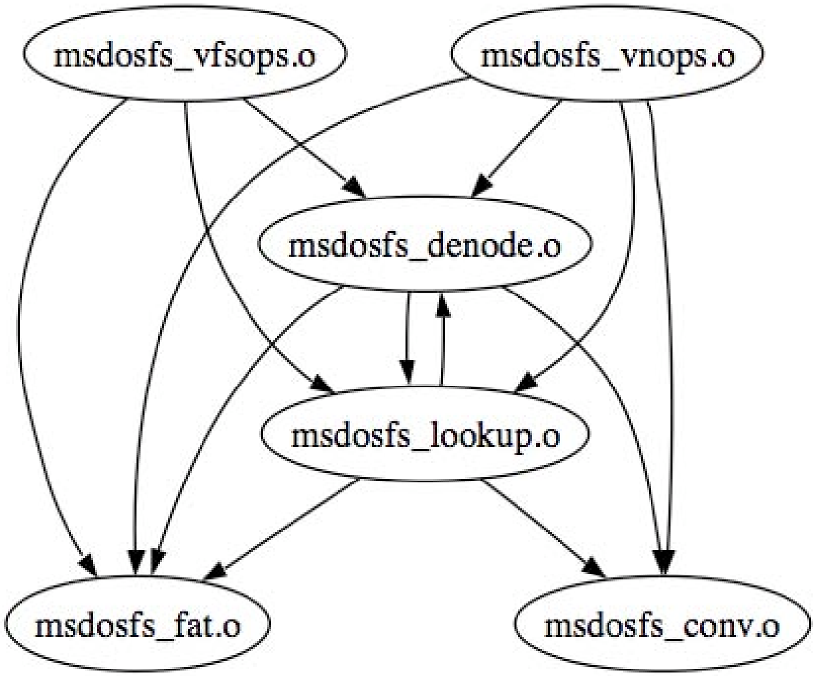
Graphviz

- Simplification for sanity

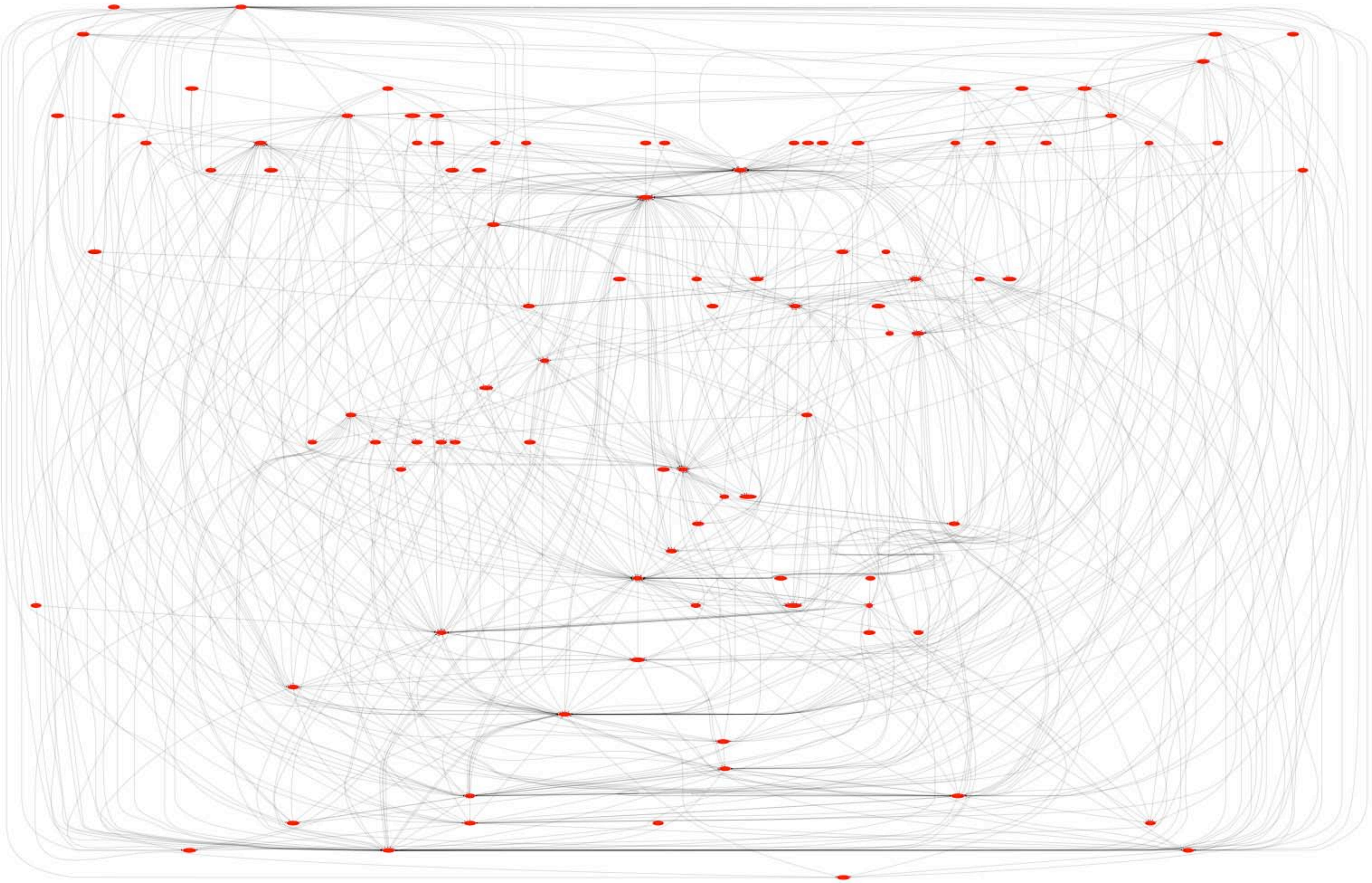
```
digraph G {
   x -> a;
   x -> b;
   a -> b;
   b -> a;
}
```



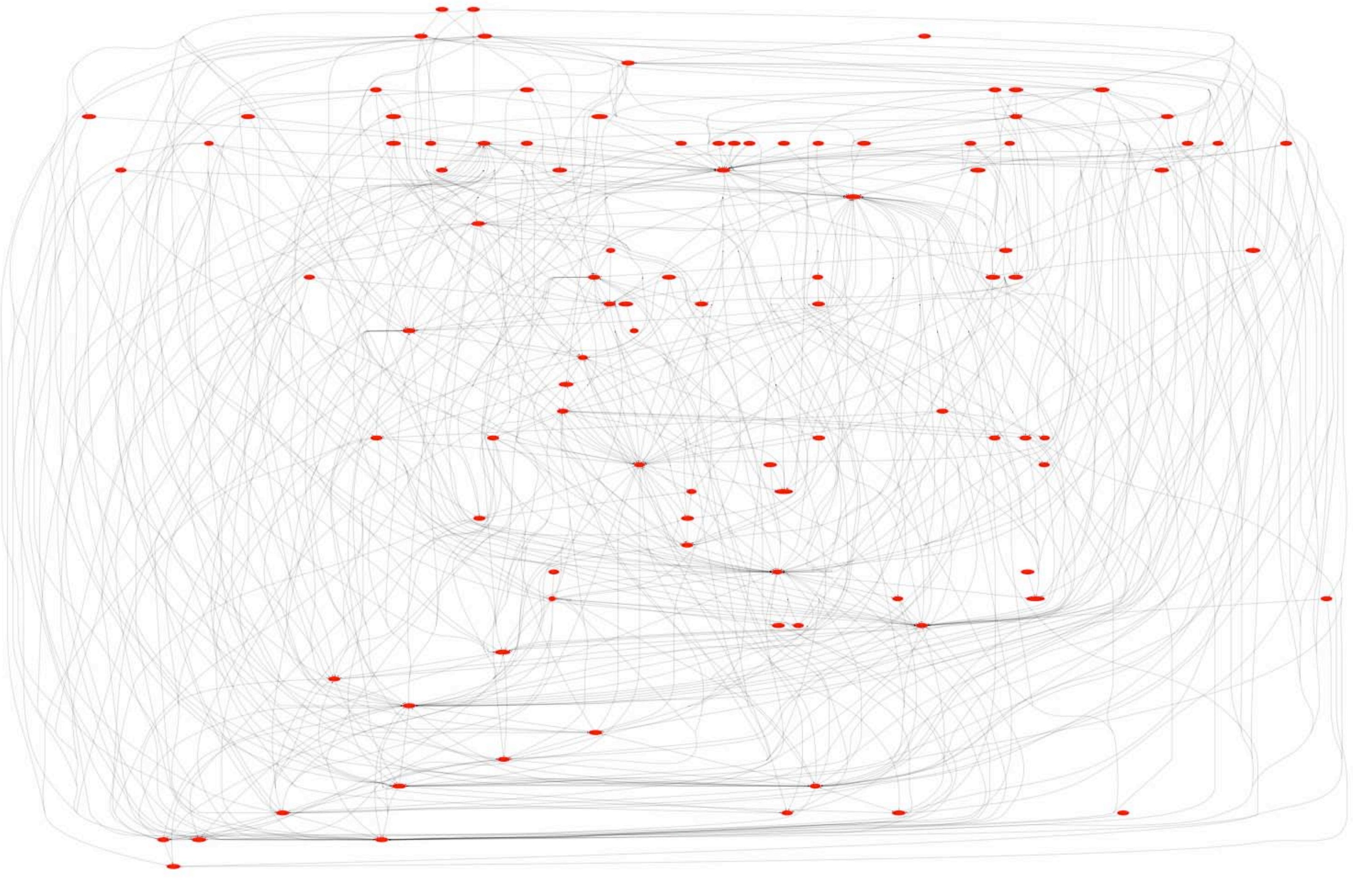
FreeBSD's MSDOS FileSystem



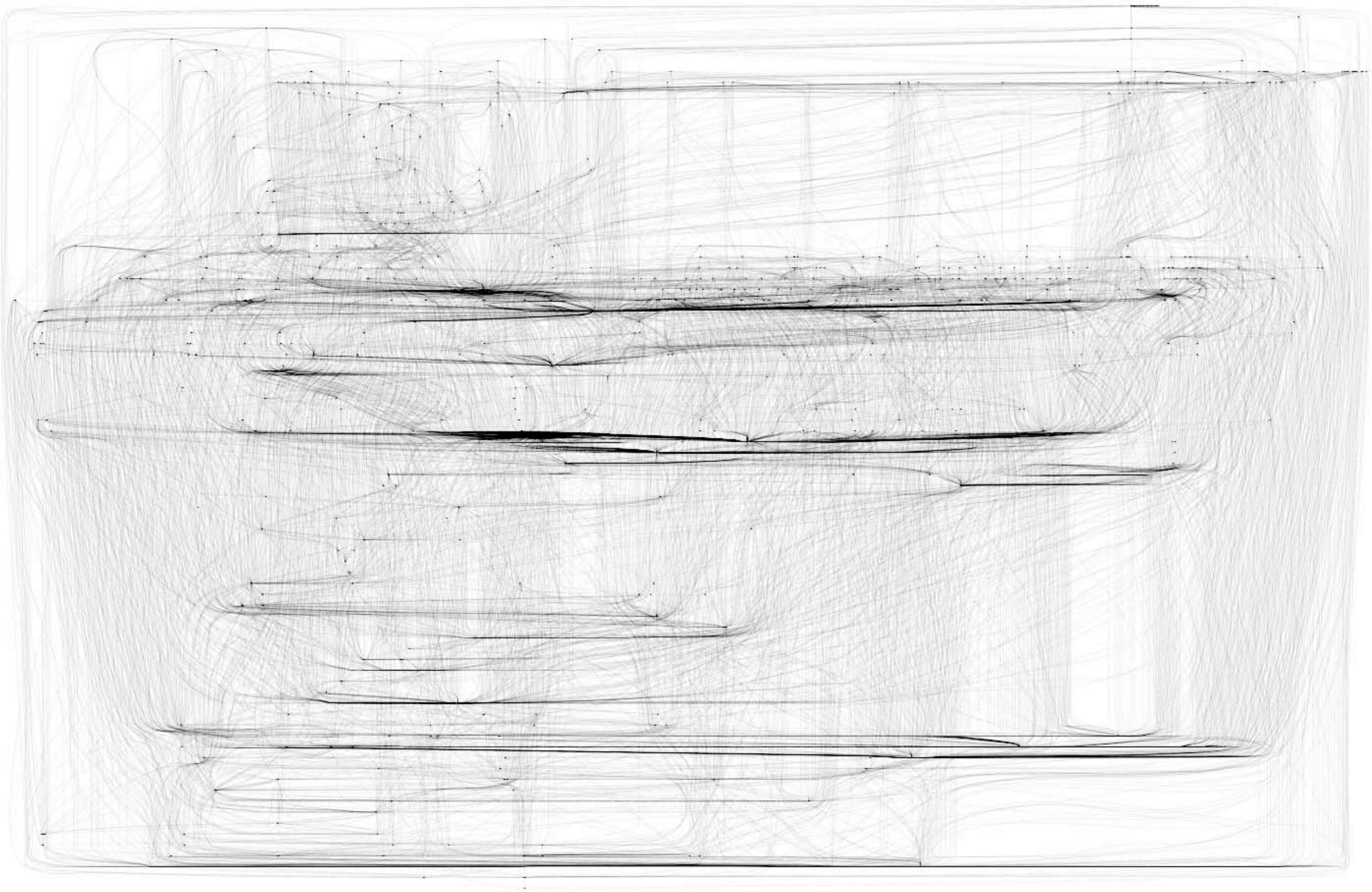
GraphViz of FreeBSD kern/



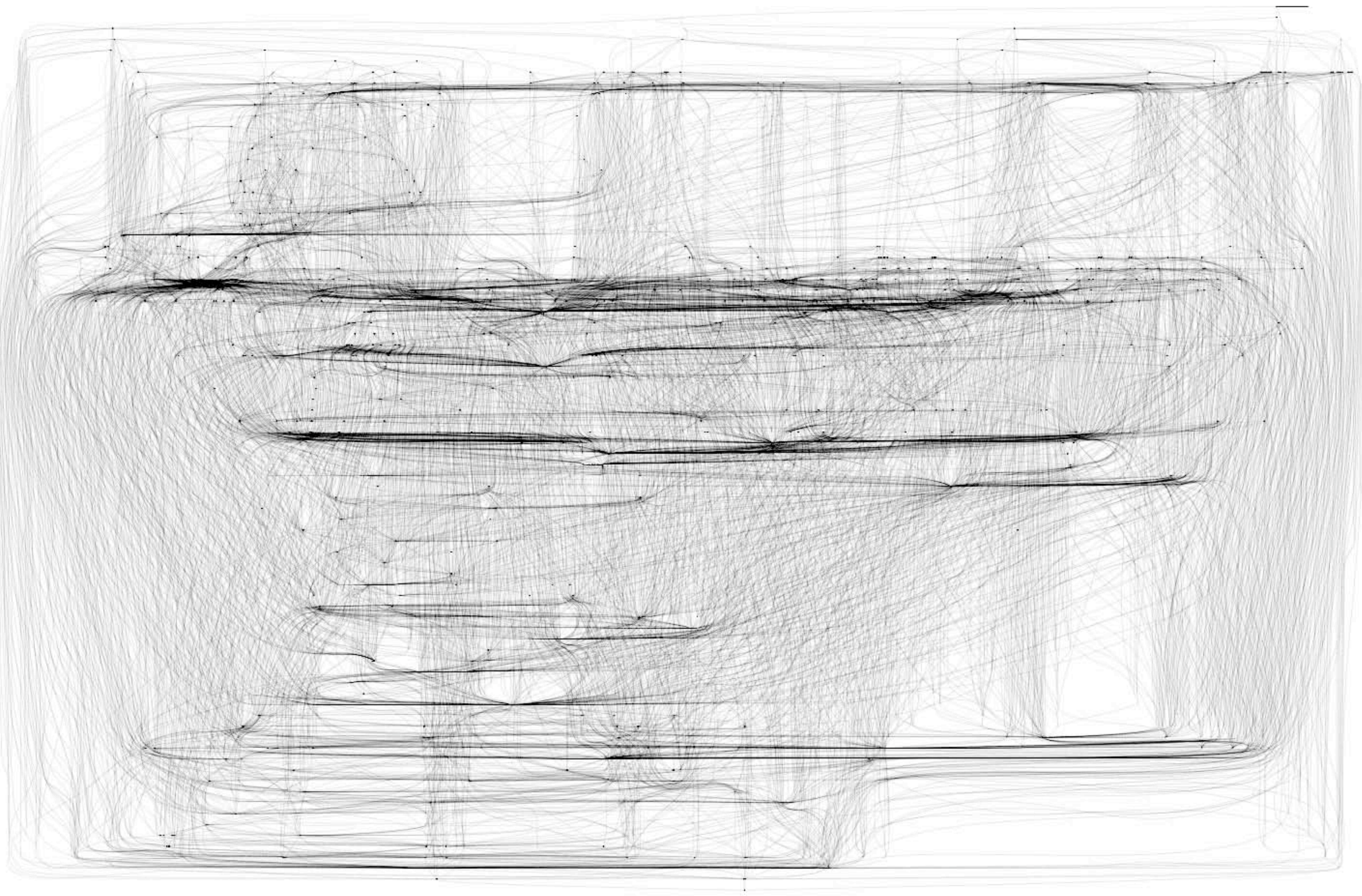
GraphViz of kern/ *(compressed)*



GraphViz of full FreeBSD Kernel



FreeBSD Kernel *(compressed)*



Scale

- FreeBSD Kernel ≈2,000,000 LOC

- Linux Kernel ≈5,500,000 LOC

Linux – Under Solen

Finnish Films

The
Man
without a past
"THE FUNNIEST FILM KAURISMAKI HAS EVER MADE!"
"A DELICIOUS BLEND OF INSANITY AND HEARTBREAK."

- Mies Vailla Menneisyyttä
  - The Man Without a Past
- Perkele! Kuvia Suomesta
  - Fuck Off! - Images of Finland
- Populäärimusiikkia Vittulanjänkältä
  - Populärmusik från Vittula
- Night on Earth
  - Final scene shot in Helsinki…

Wikipedia
Finnish Actors & Actresses

- No entries

Finnish Directors: Jouko Turkka

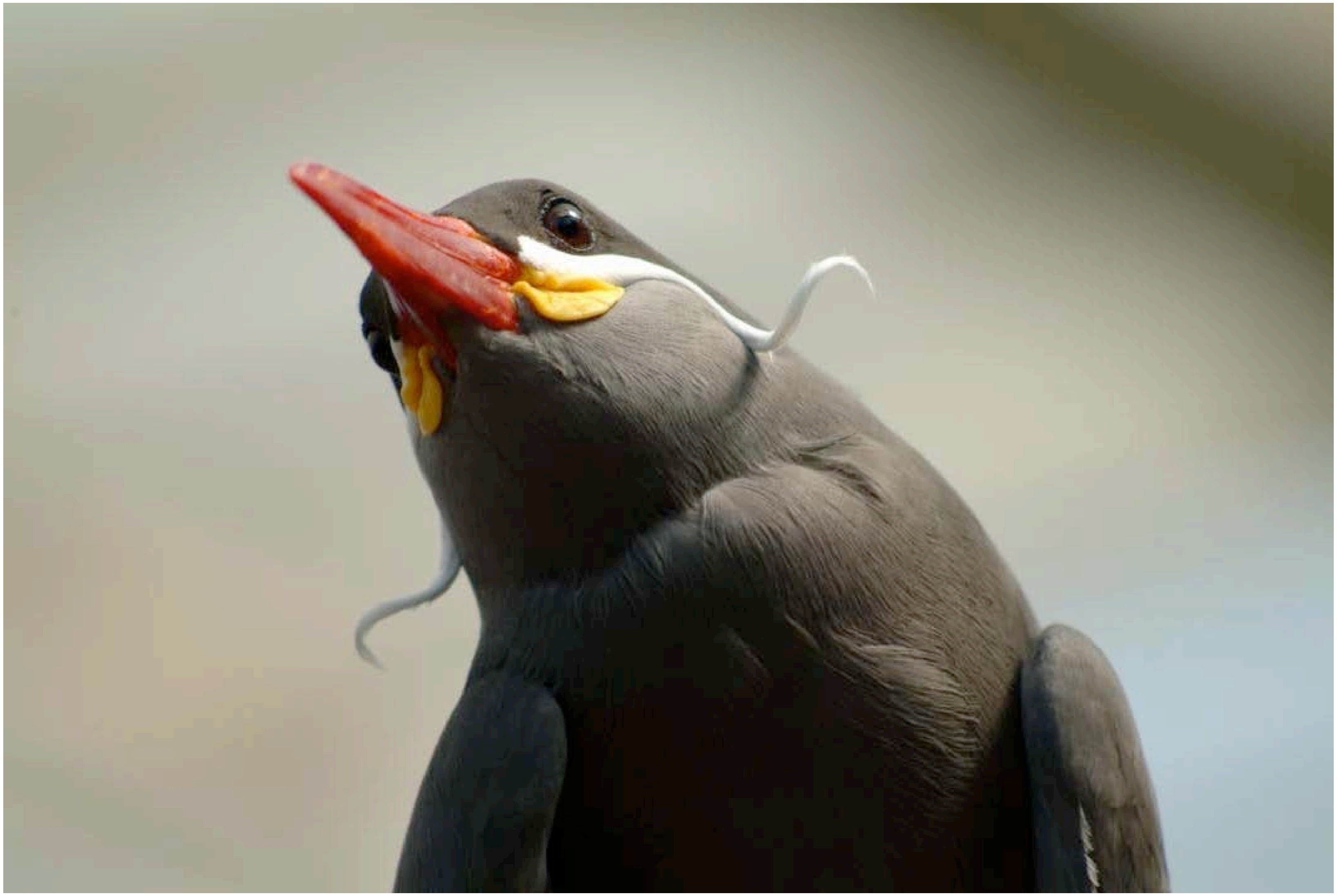
- Finnish theatrical director and controversialist
  - Created a generation of Finnish actors
  - Recognizable style of acting
- Progressively search for a mental borderline state
  - Psychic and physical exertion
  - Performance characterized by actors shaking uncontrollably, spewing spit and snot and other bodily fluids around them
  - Likened to brainwashing, religious cults
- Renowned for his sadistic directorial style
  - Numerous instances of reducing actors to tears and/or nervous breakdown
- Very few people doubt his genius

`http://www.fact-index.com/j/jo/jouko_turkka.html`

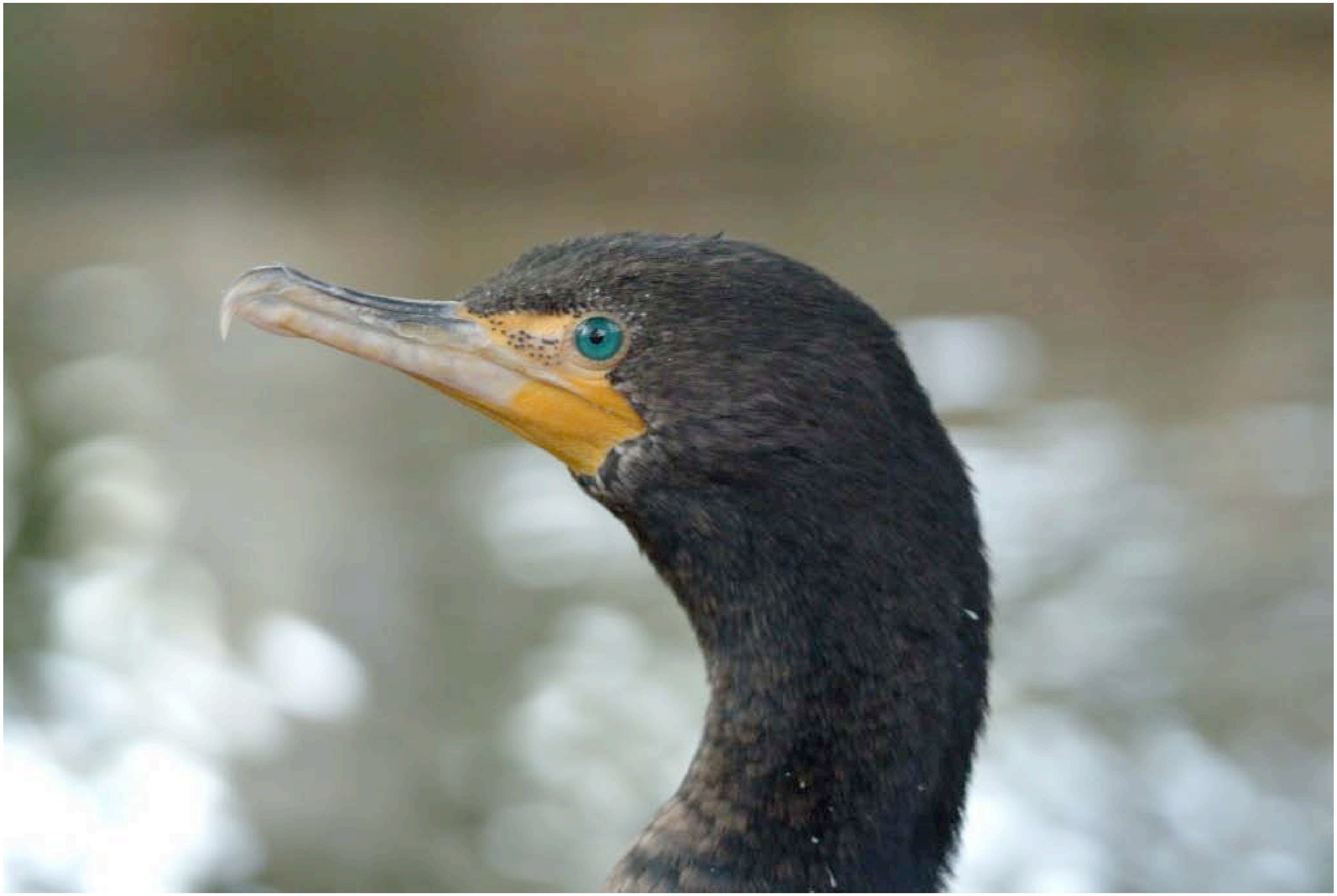
Tradeoffs

- “Security is about Tradeoffs” *—Bruce Schneier*
- “Risk is about tradeoffs” *—Me*
- “Evolution is about tradeoffs” *—Me too!*
  - Humans
    - Big heads, so childbirth is “challenging”
    - No fur, but clothes
    - No claws, but tools
  - Birds…

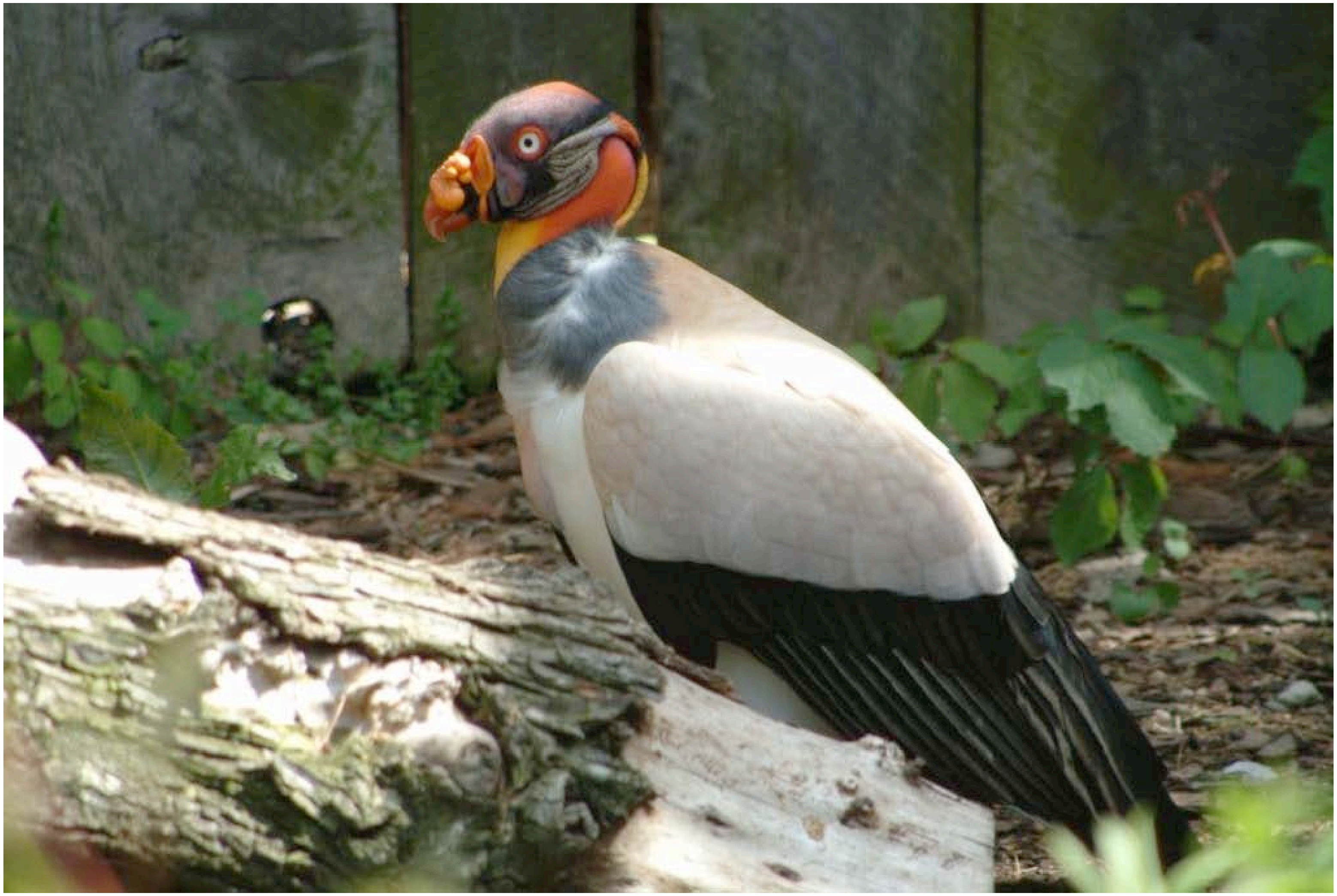
Inca Tern



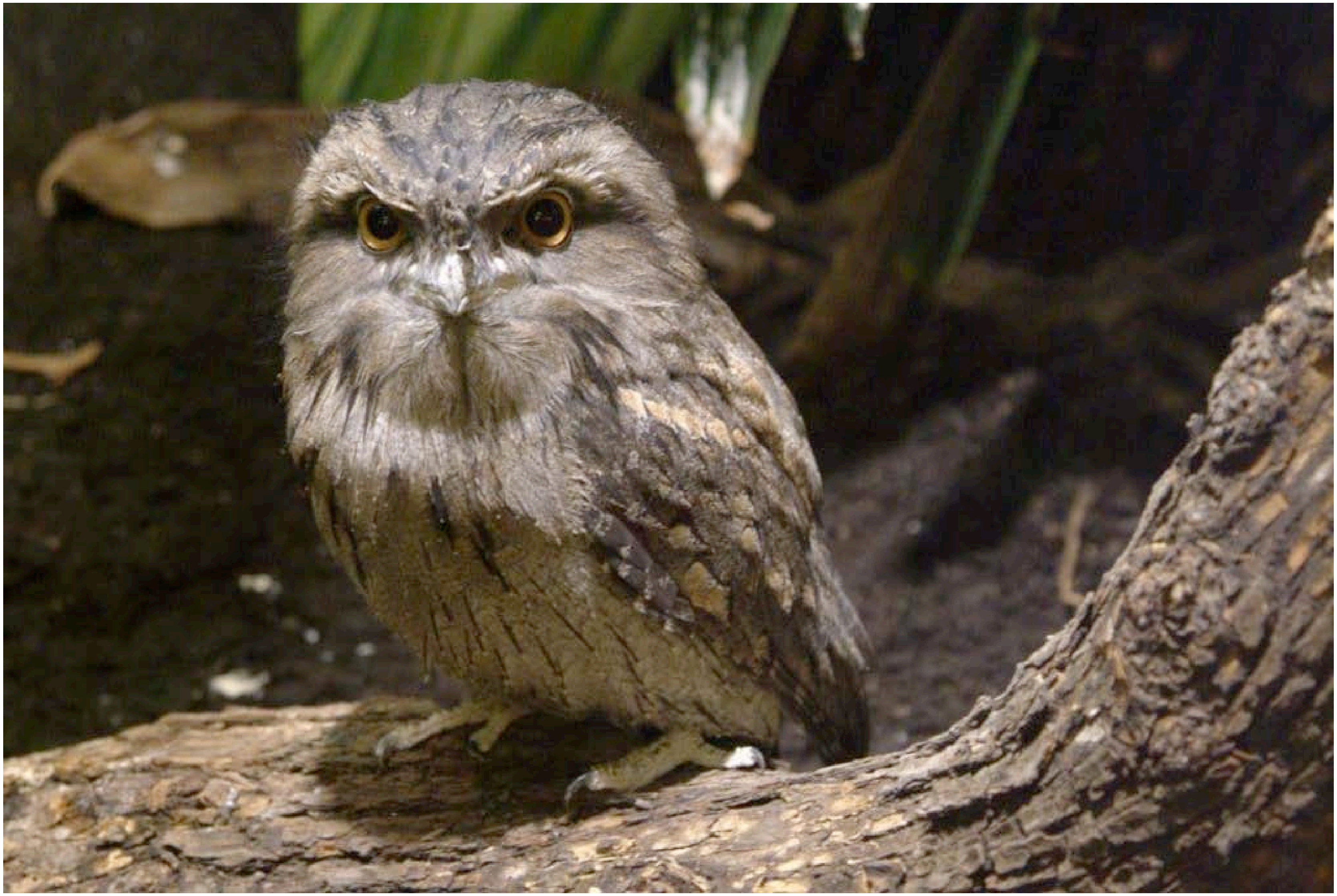
Double Crested Cormorant



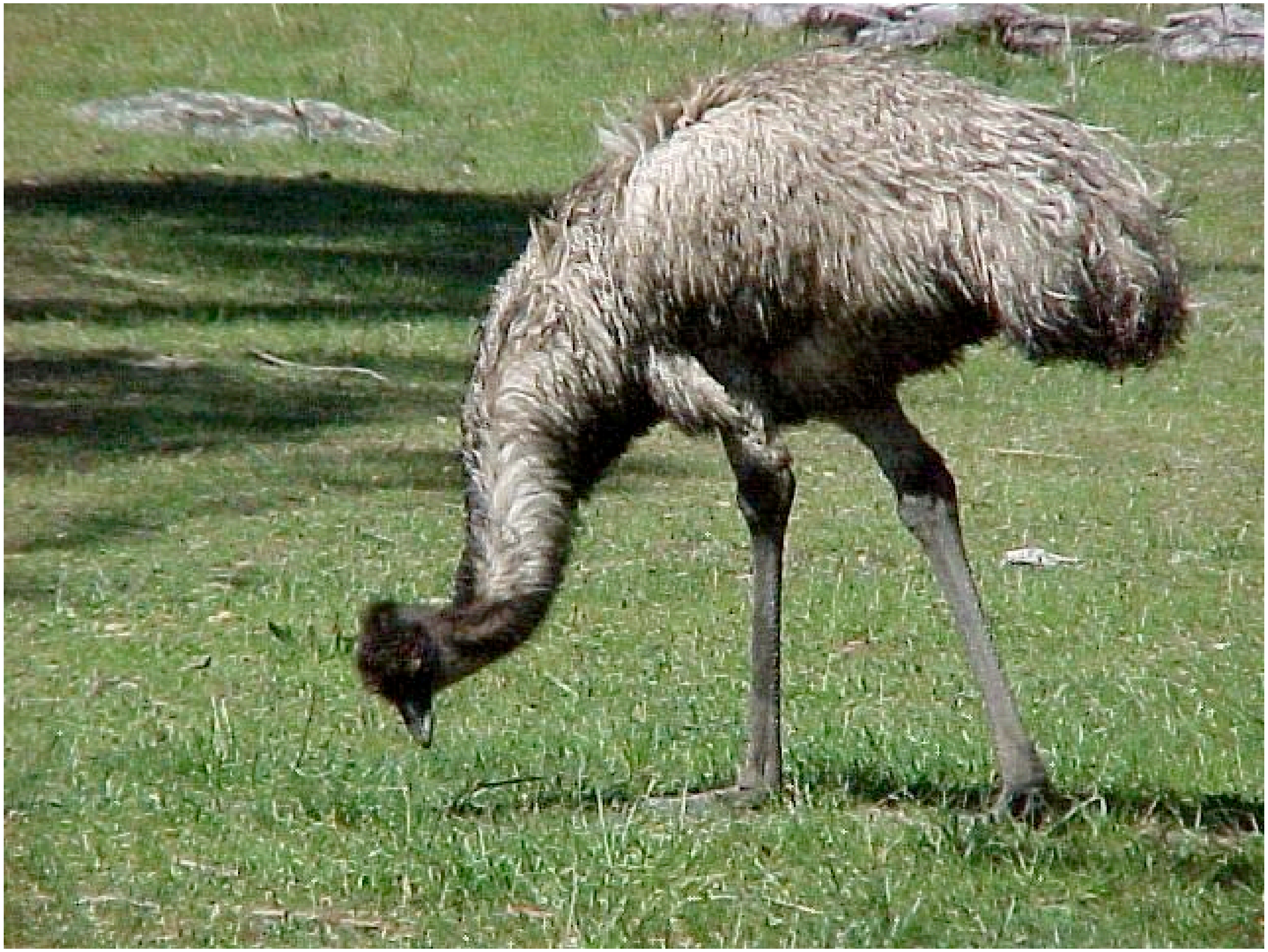
King Vulture



Tawny Frogmouth



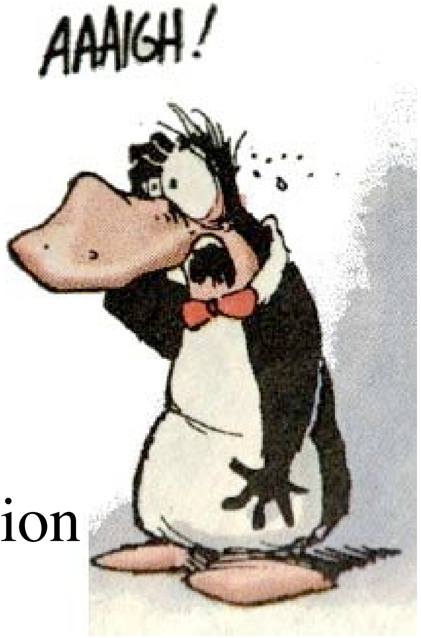
Emu



Bird Tradeoffs

- Poor manipulation skills
  - But most fly!
- If they fly…
  - Usually lousy runners
  - Compare robin, sparrow, pigeon
- Penguins don’t walk well
- Penguins don’t fly at all

Maybe Linux will never fly…



- But that’s okay!
- It’s all about tradeoffs…
  - What you get is Babettes Gaestebud
  - What you get is everything Under Solen
  - What you get is Martin Luther/Linus reformation
  - What you *don’t* get is Det Sjunde Inseglet
- Manageable risk, manageable security
- Someone else flies the plane

But it’s Okay to Dream!

Flying Linux (or not)

Picture Copyright © Berke Breathed, from *"A Wish for Wings that Work"*; used without permission

Daniel V. Klein

dan@klein.com

Assorted Links

- Apollo 11
  - http://www.hq.nasa.gov/alsj/a11/a11.landing.html
  - http://www.hq.nasa.gov/alsj/a11/a11.1201-fm.html
  - http://www.hq.nasa.gov/alsj/a11/a11.1201-pa.html
  - http://www.hq.nasa.gov/alsj/a11/a11Hamilton.html
- Digital Fly By Wire
  - http://www.dfrc.nasa.gov/History/Publications/PDF/DFBW.pdf
  - http://www.disenchanted.com/dis/technology/fly-by-wire.html
- Gimli Glider
  - http://www.wadenelson.com/gimli.html
- Open Source and Potential for Foul Play
  - http://www.devx.com/opensource/Article/20111
  - http://www.devx.com/opensource/Article/20135