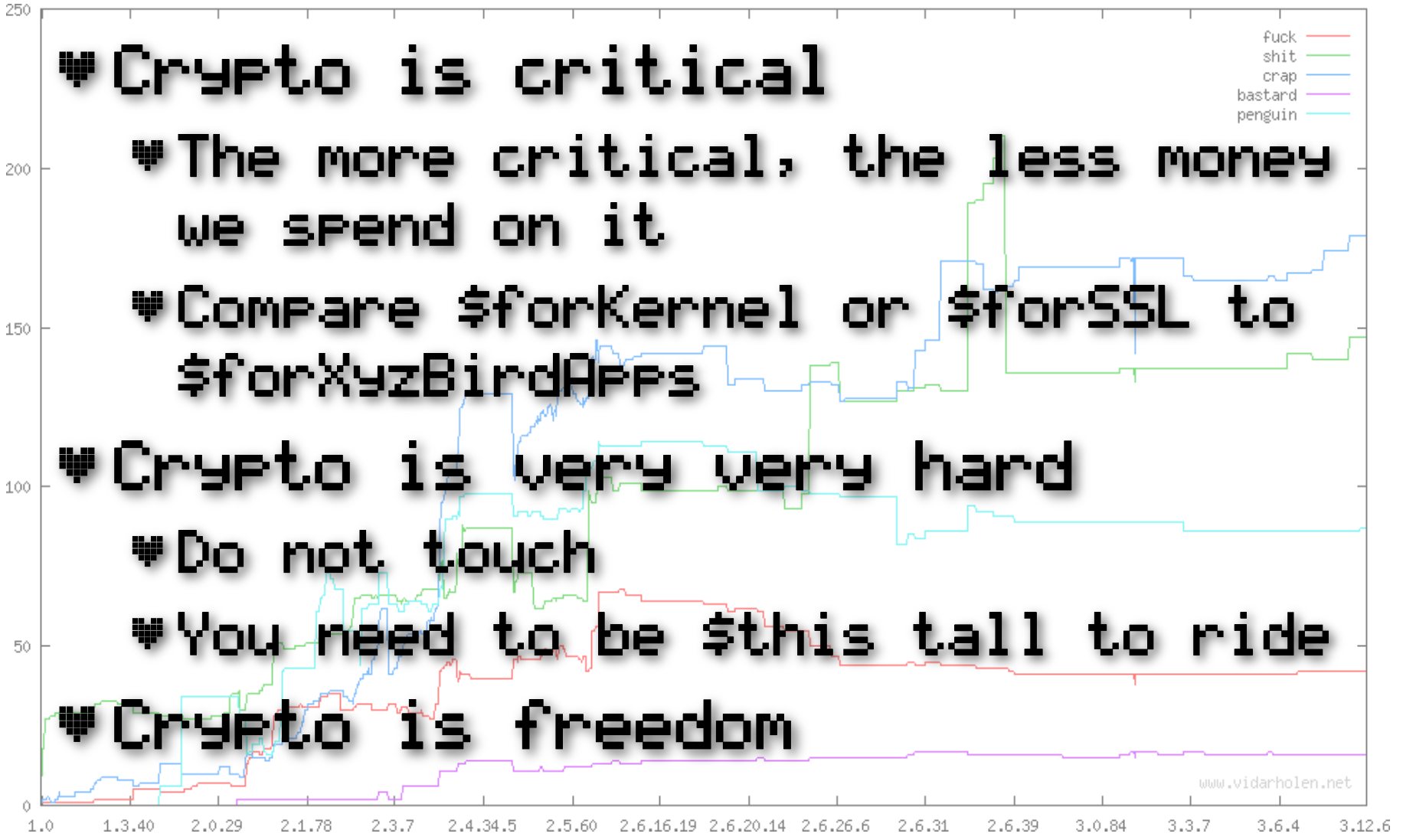
GOTO KLARKOMMEN

DAS IST NICHT LUSTIG
(AUCH WENN'S SO AUSSIEHT)
DAS IST CRYPTO !!!
DIE BRAUCHEN WIR NOCH

INTRO SONST NITRO

- Crypto is critical
  - The more critical, the less money we spend on it
  - Compare $forKernel or $forSSL to $forXyzBirdApps
- Crypto is very very hard
  - Do not touch
  - You need to be $this tall to ride
- Crypto is freedom



Das sicherste Daten Verschlüsselungs Programm der Welt !

VOLLBIT

One of the rare cases that allow evaluation of the encryption by visual inspection of the UI.

THE POSER

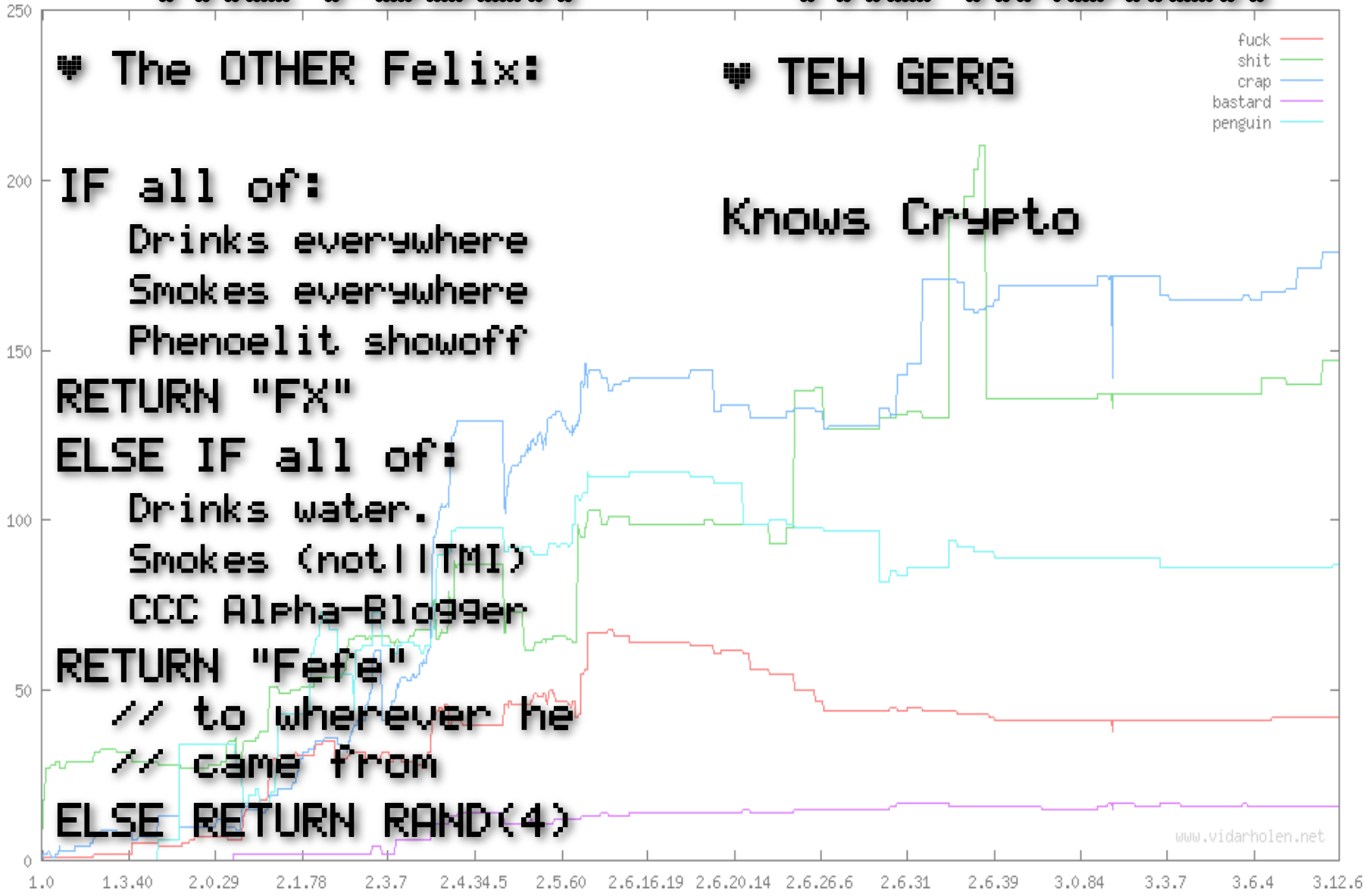
- The OTHER Felix:

```
IF all of:
    Drinks everywhere
    Smokes everywhere
    Phenoelit showoff
RETURN "FX"
ELSE IF all of:
    Drinks water.
    Smokes (not||TMI)
    CCC Alpha-Blogger
RETURN "Fefe"
   // to wherever he
   // came from
ELSE RETURN RAND(4)
```

THE KNOWER

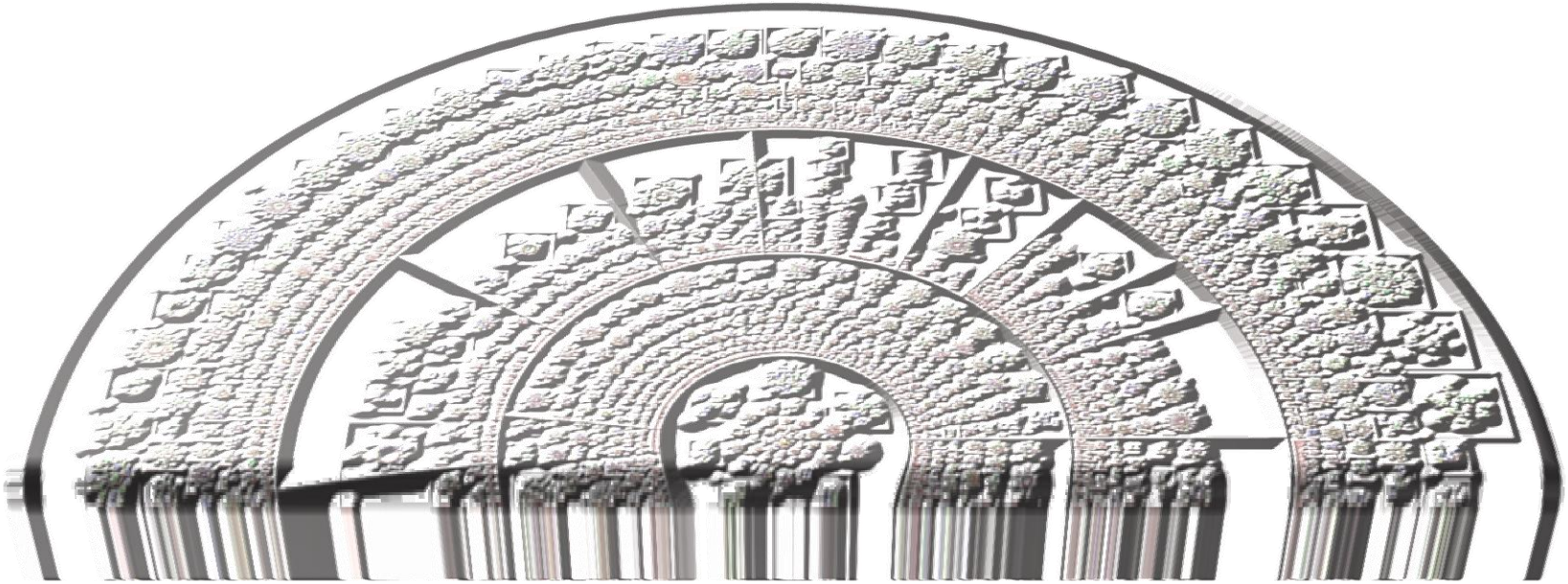
- TEH GERG

Knows Crypto



KEY ACCOUNT MANAGER

REGENT CRYPTO FAIL

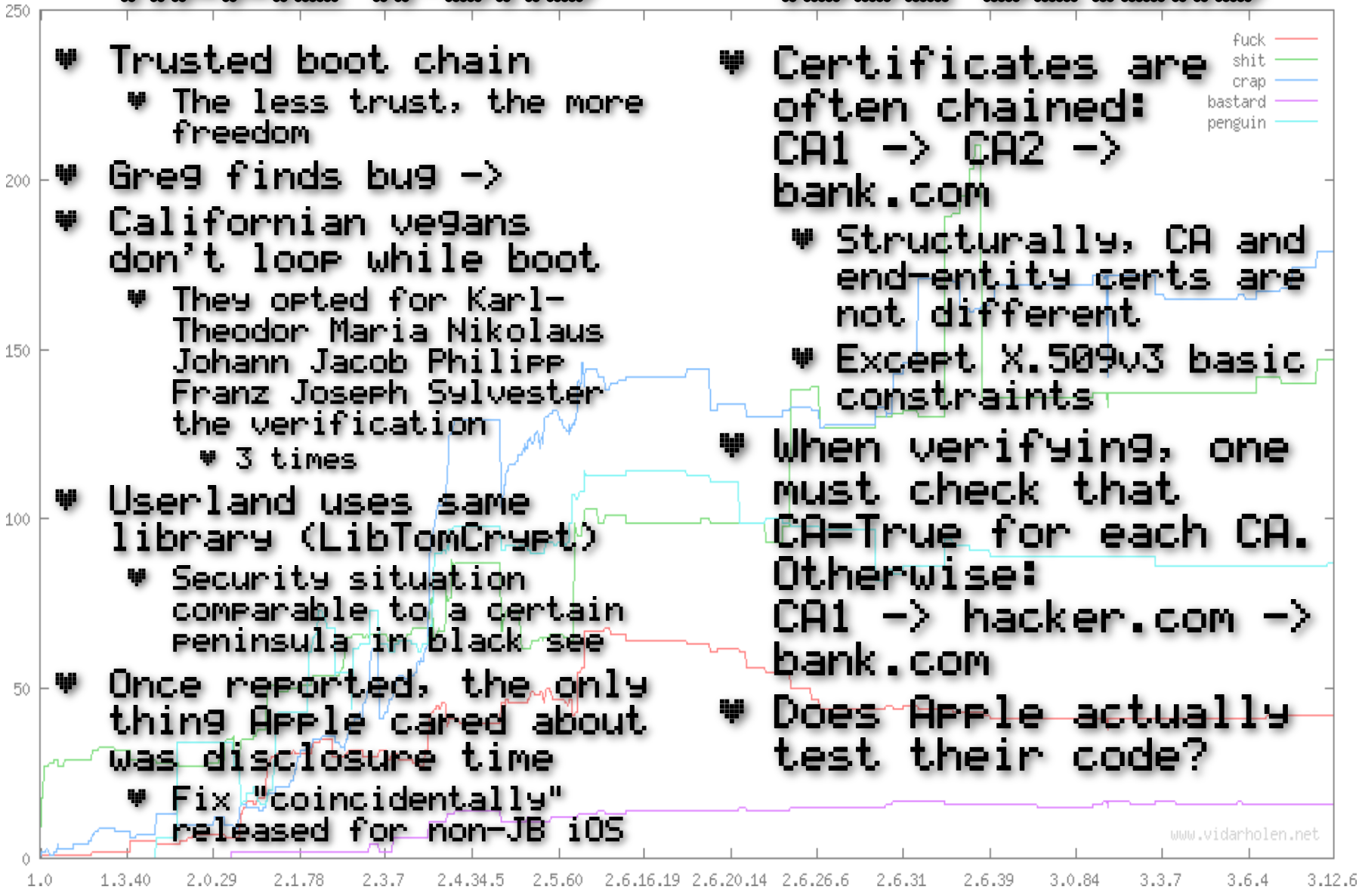


Apple iPony

- Trusted boot chain
  - The less trust, the more freedom
- Greg finds bug ->
- Californian vegans don't loop while boot
  - They opted for Karl-Theodor Maria Nikolaus Johann Jacob Philipp Franz Joseph Sylvester the verification
    - 3 times
- Userland uses same library (LibTomCrypt)
  - Security situation comparable to a certain peninsula in black see
- Once reported, the only thing Apple cared about was disclosure time
  - Fix "coincidentally" released for non-JB iOS

iSSL Details

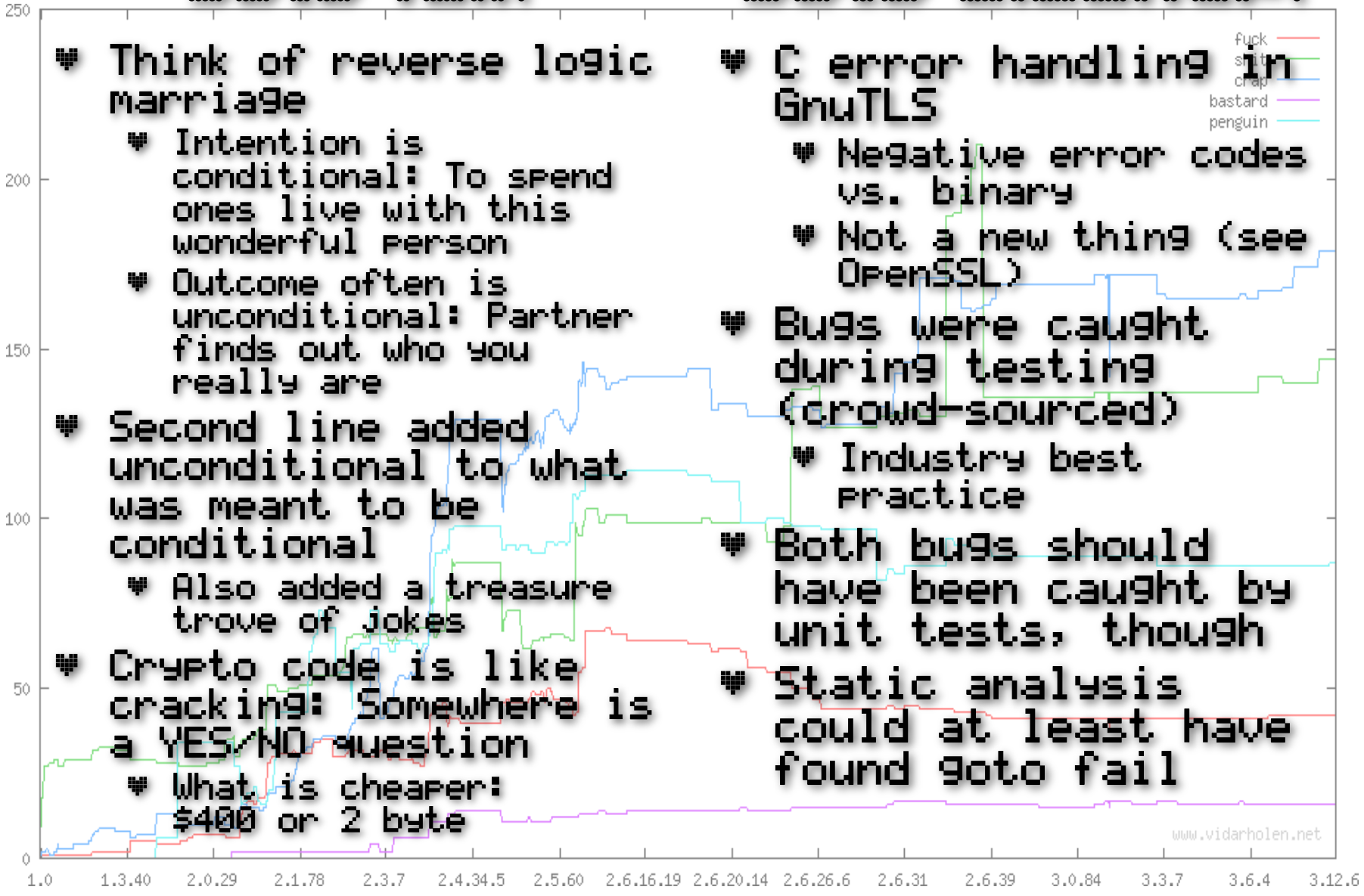
- Certificates are often chained: CA1 -> CA2 -> bank.com
  - Structurally, CA and end-entity certs are not different
  - Except X.509v3 basic constraints
- When verifying, one must check that CA=True for each CA. Otherwise: CA1 -> hacker.com -> bank.com
- Does Apple actually test their code?



goto fail;
goto fail;

goto cleanup;

- Think of reverse logic marriage
  - Intention is conditional: To spend ones live with this wonderful person
  - Outcome often is unconditional: Partner finds out who you really are
- Second line added unconditional to what was meant to be conditional
  - Also added a treasure trove of jokes
- Crypto code is like cracking: Somewhere is a YES/NO question
  - What is cheaper: $400 or 2 byte
- C error handling in GnuTLS
  - Negative error codes vs. binary
  - Not a new thing (see OpenSSL)
- Bugs were caught during testing (crowd-sourced)
  - Industry best practice
- Both bugs should have been caught by unit tests, though
- Static analysis could at least have found goto fail



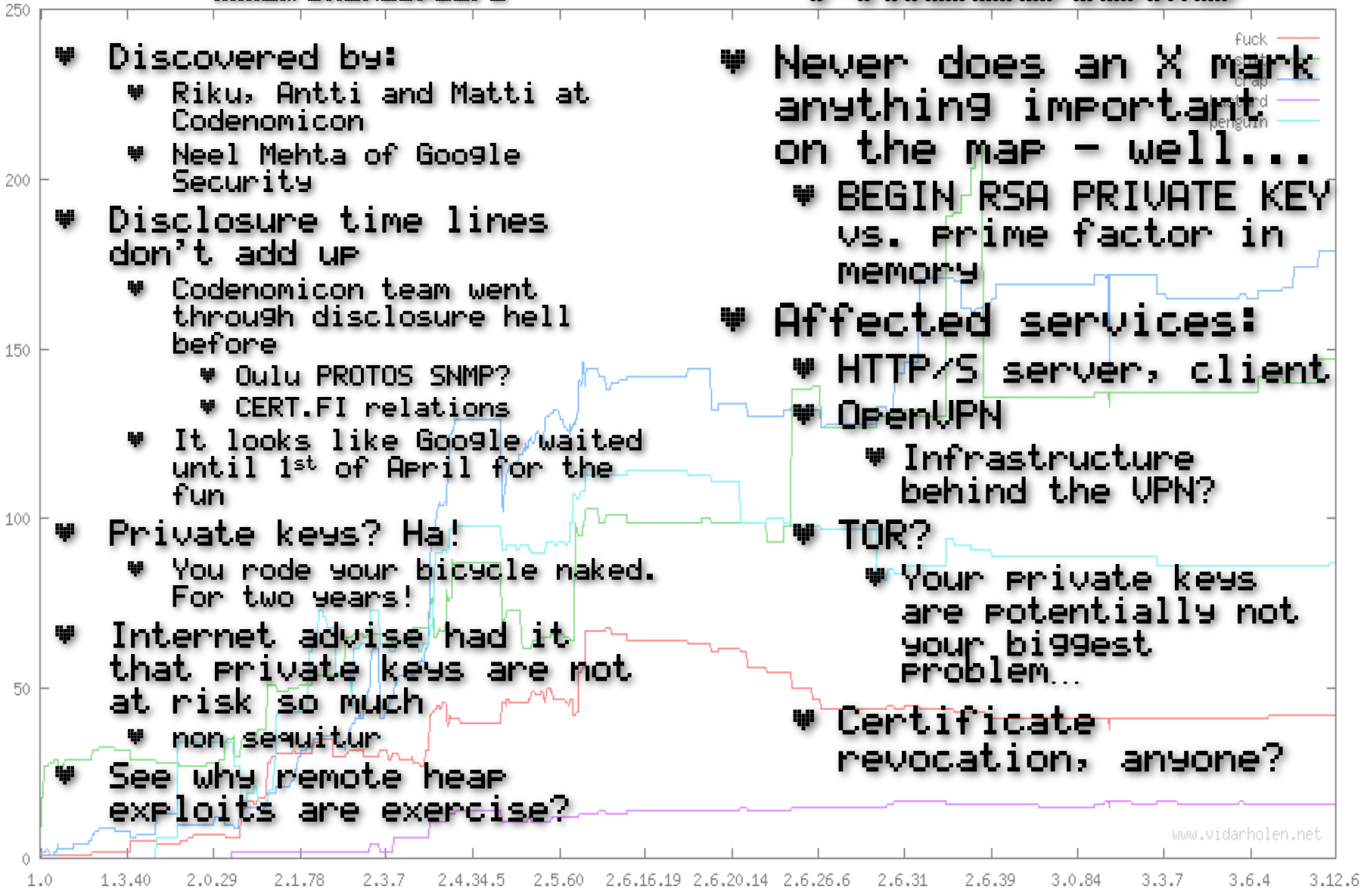
Weep I cannot. But my heart bleeds

William Shakespeare

Applied phlebotomy

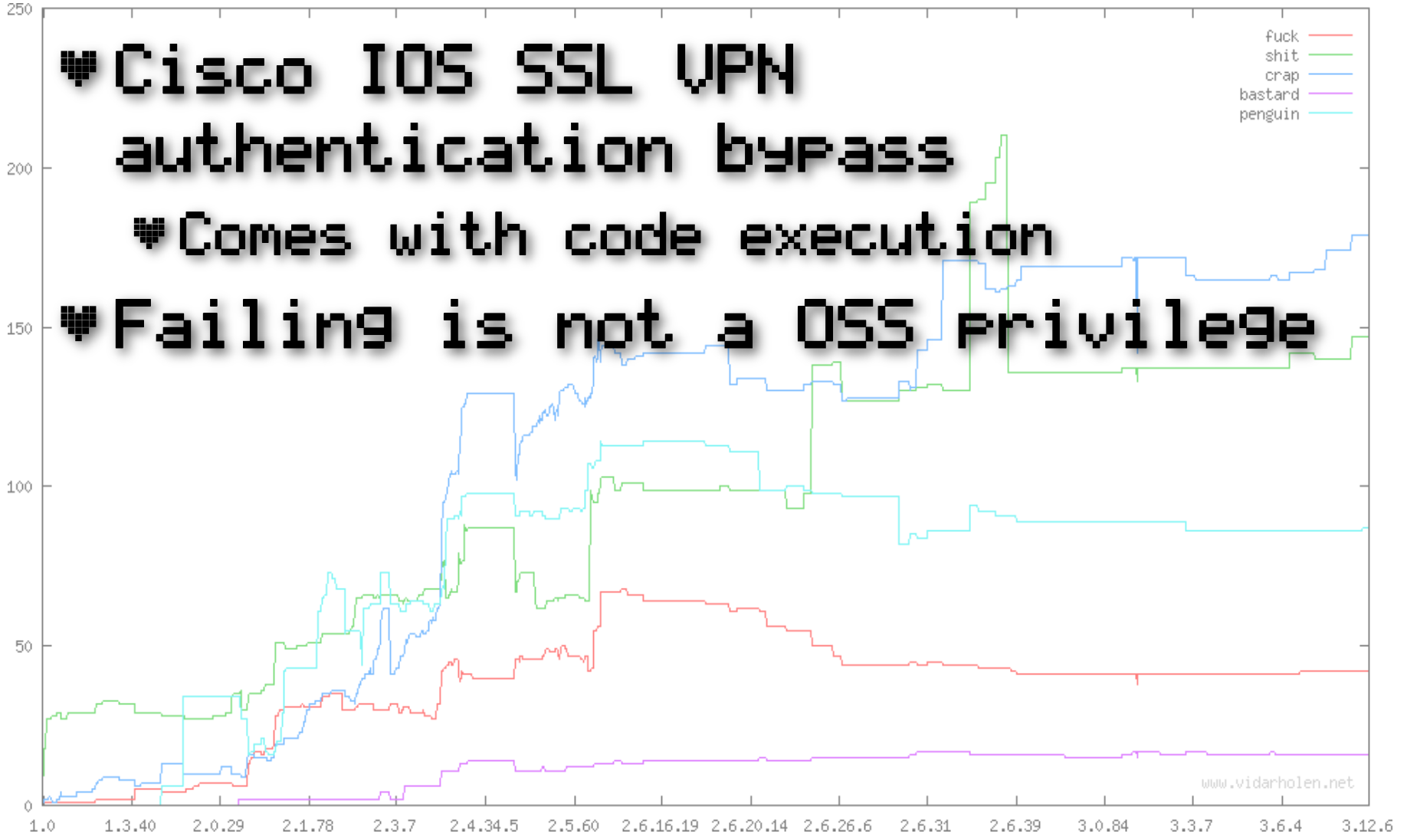
- Discovered by:
  - Riku, Antti and Matti at Codenomicon
  - Neel Mehta of Google Security
- Disclosure time lines don't add up
  - Codenomicon team went through disclosure hell before
    - Oulu PROTOS SNMP?
    - CERT.FI relations
  - It looks like Google waited until 1st of April for the fun
- Private keys? Ha!
  - You rode your bicycle naked. For two years!
- Internet advise had it that private keys are not at risk so much
  - non sequitur
- See why remote heap exploits are exercise?

- Never does an X mark anything important on the map - well...
  - BEGIN RSA PRIVATE KEY vs. prime factor in memory
- Affected services:
  - HTTP/S server, client
  - OpenVPN
    - Infrastructure behind the VPN?
  - TOR?
    - Your private keys are potentially not your biggest problem...
  - Certificate revocation, anyone?



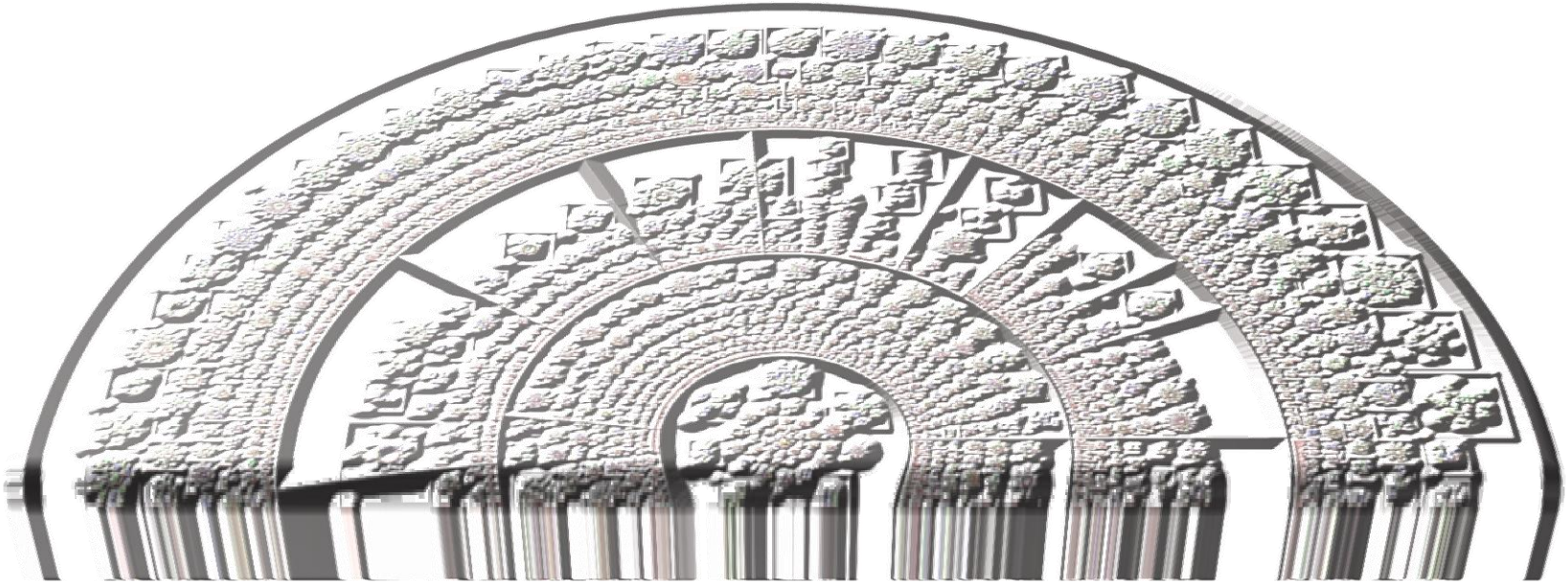
UND WAS IST MIT CISCOMFG?

- Cisco IOS SSL VPN authentication bypass
  - Comes with code execution
- Failing is not a OSS privilege



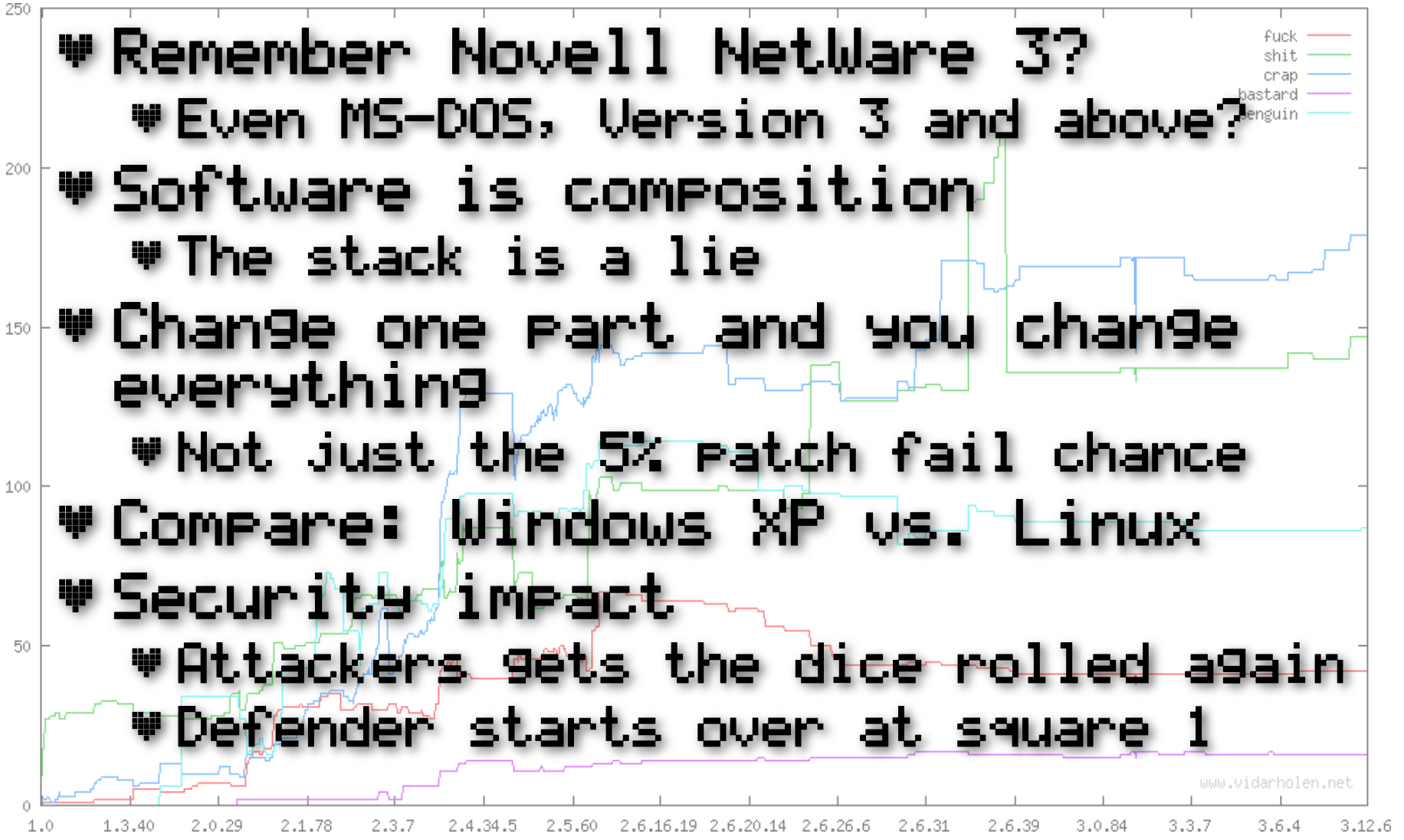
TERRION UNTERM ARGEN WEGZIEHEN

UPDATING AND PATCH



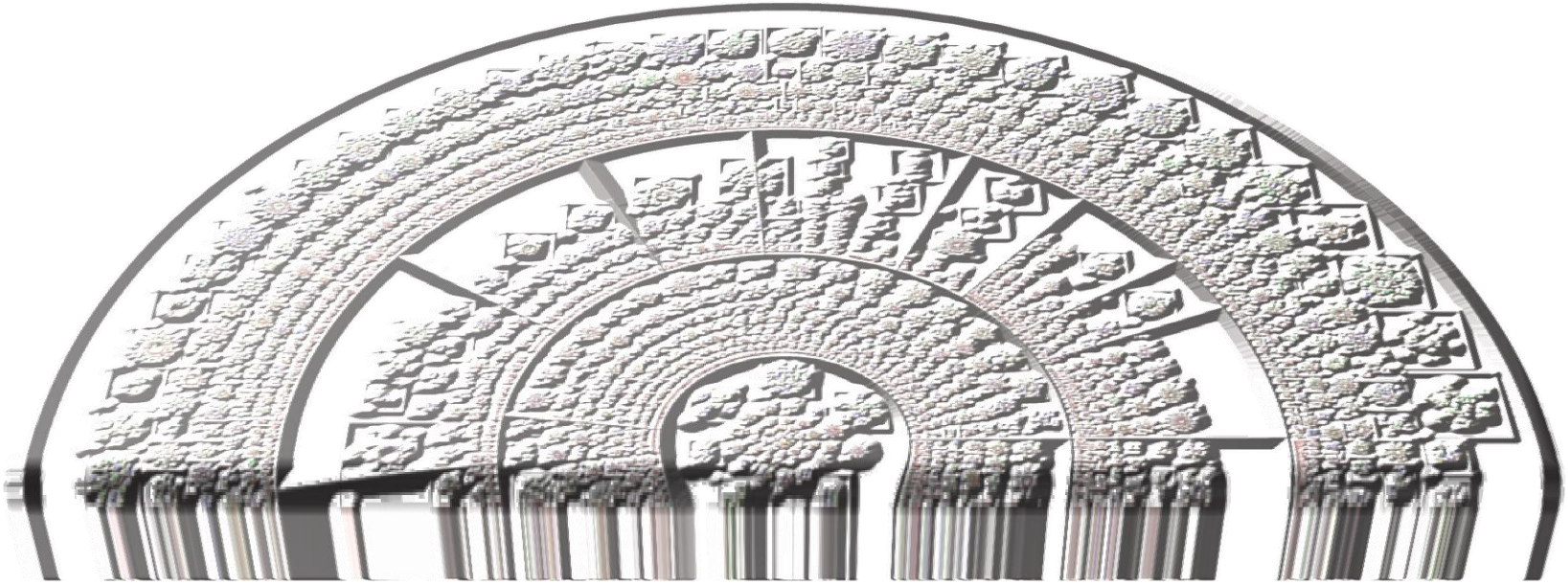
IF YOU SEE CYBER UPDATE AND AV!!

- Remember Novell NetWare 3?
  - Even MS-DOS, Version 3 and above?
- Software is composition
  - The stack is a lie
- Change one part and you change everything
  - Not just the 5% patch fail chance
- Compare: Windows XP vs. Linux
- Security impact
  - Attackers gets the dice rolled again
  - Defender starts over at square 1



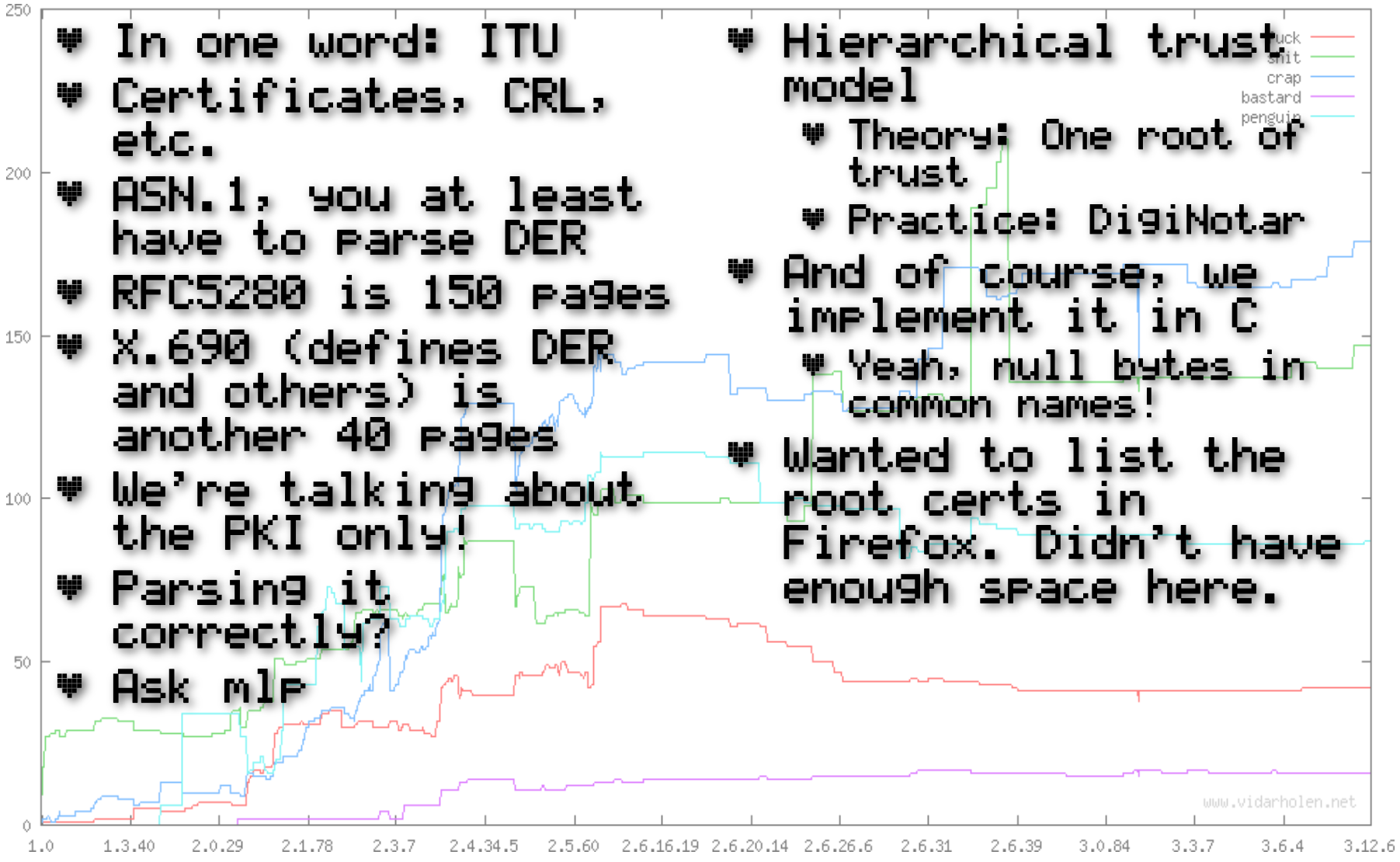
SOZIALVERSICHERUNGSPFLICHTIGES
BESCHAEFTIGUNGSVERHAELTNIS

WRITE. READ. AUDIT. FIX. REPEAT

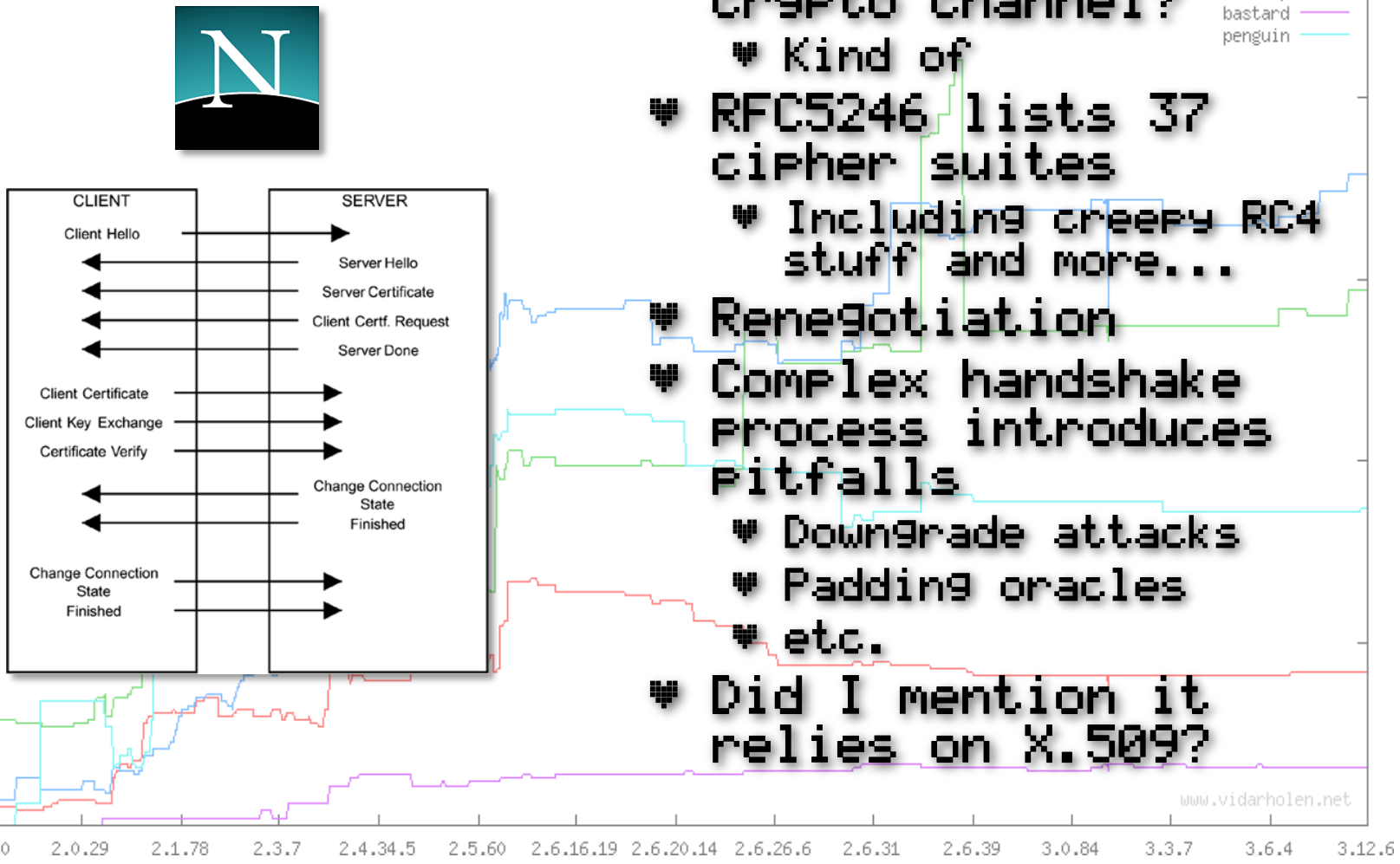


X.509

- In one word: ITU
- Certificates, CRL, etc.
- ASN.1, you at least have to parse DER
- RFC5280 is 150 pages
- X.690 (defines DER and others) is another 40 pages
- We're talking about the PKI only!
- Parsing it correctly?
- Ask mlp
- Hierarchical trust model
  - Theory: One root of trust
  - Practice: DigiNotar
- And of course, we implement it in C
  - Yeah, null bytes in common names!
- Wanted to list the root certs in Firefox. Didn't have enough space here.



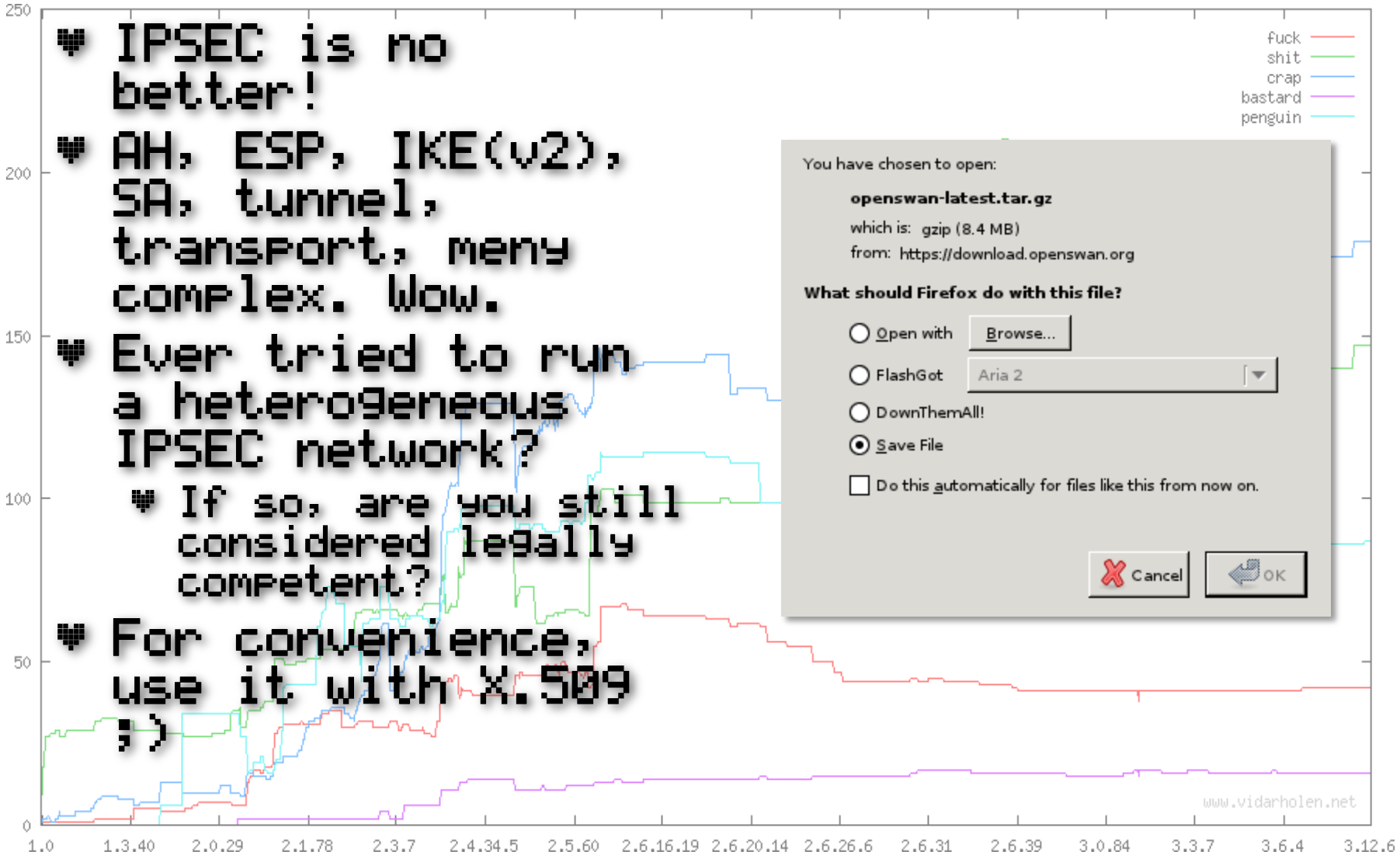
TLS



- Simply wrap TCP in a crypto channel?
  - Kind of
- RFC5246 lists 37 cipher suites
  - Including creepy RC4 stuff and more...
- Renegotiation
- Complex handshake process introduces pitfalls
  - Downgrade attacks
  - Padding oracles
  - etc.
- Did I mention it relies on X.509?

IPSEC

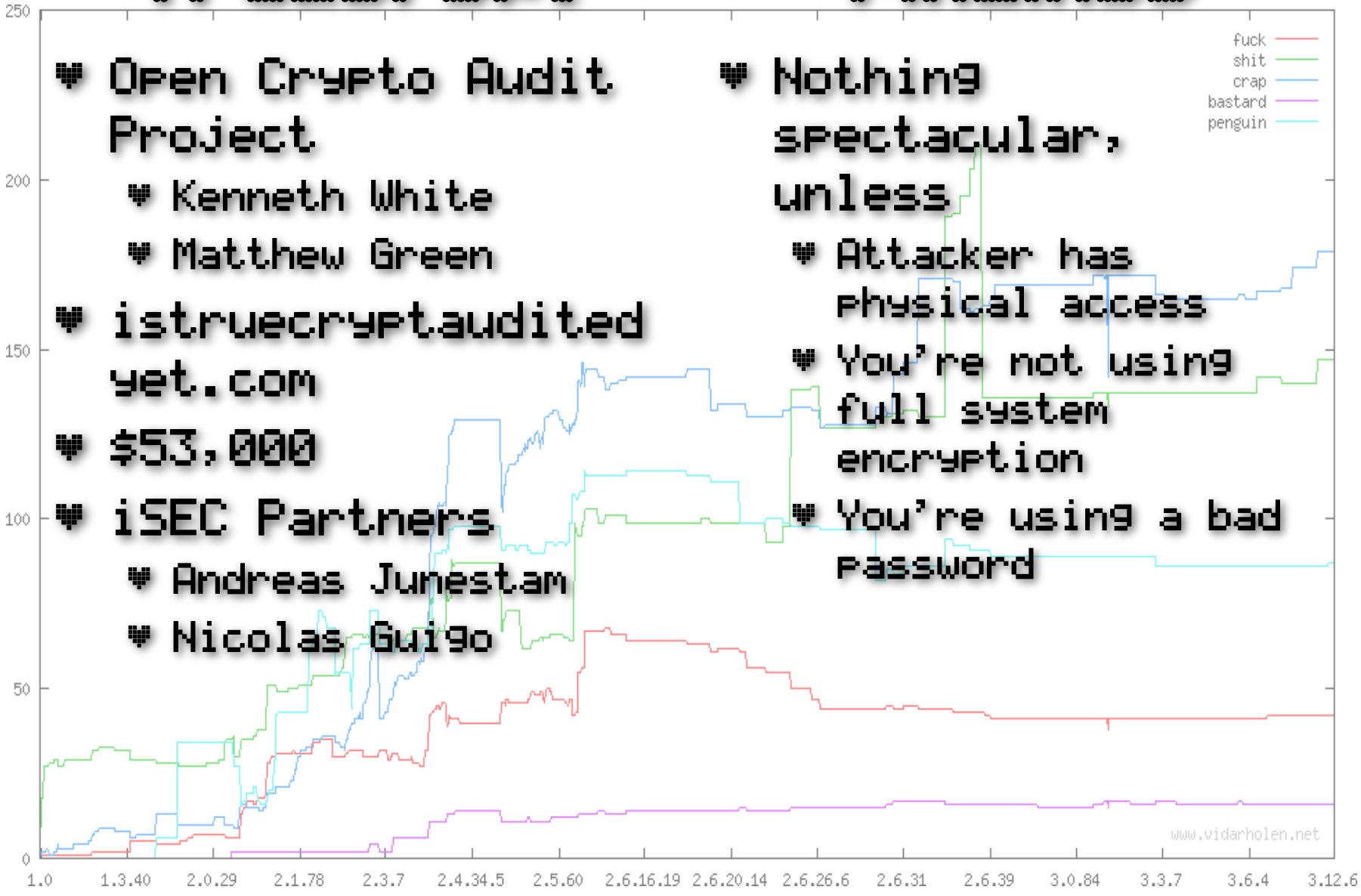
- IPSEC is no better!
- AH, ESP, IKE(v2), SA, tunnel, transport, meny complex. Wow.
- Ever tried to run a heterogeneous IPSEC network?
  - If so, are you still considered legally competent?
- For convenience, use it with X.509 ;)



TrueCrypt Findings

- Open Crypto Audit Project
  - Kenneth White
  - Matthew Green
- istruecryptaudited yet.com
- $53,000
- iSEC Partners
  - Andreas Junestam
  - Nicolas Guigo

- Nothing spectacular, unless
  - Attacker has physical access
  - You're not using full system encryption
  - You're using a bad password

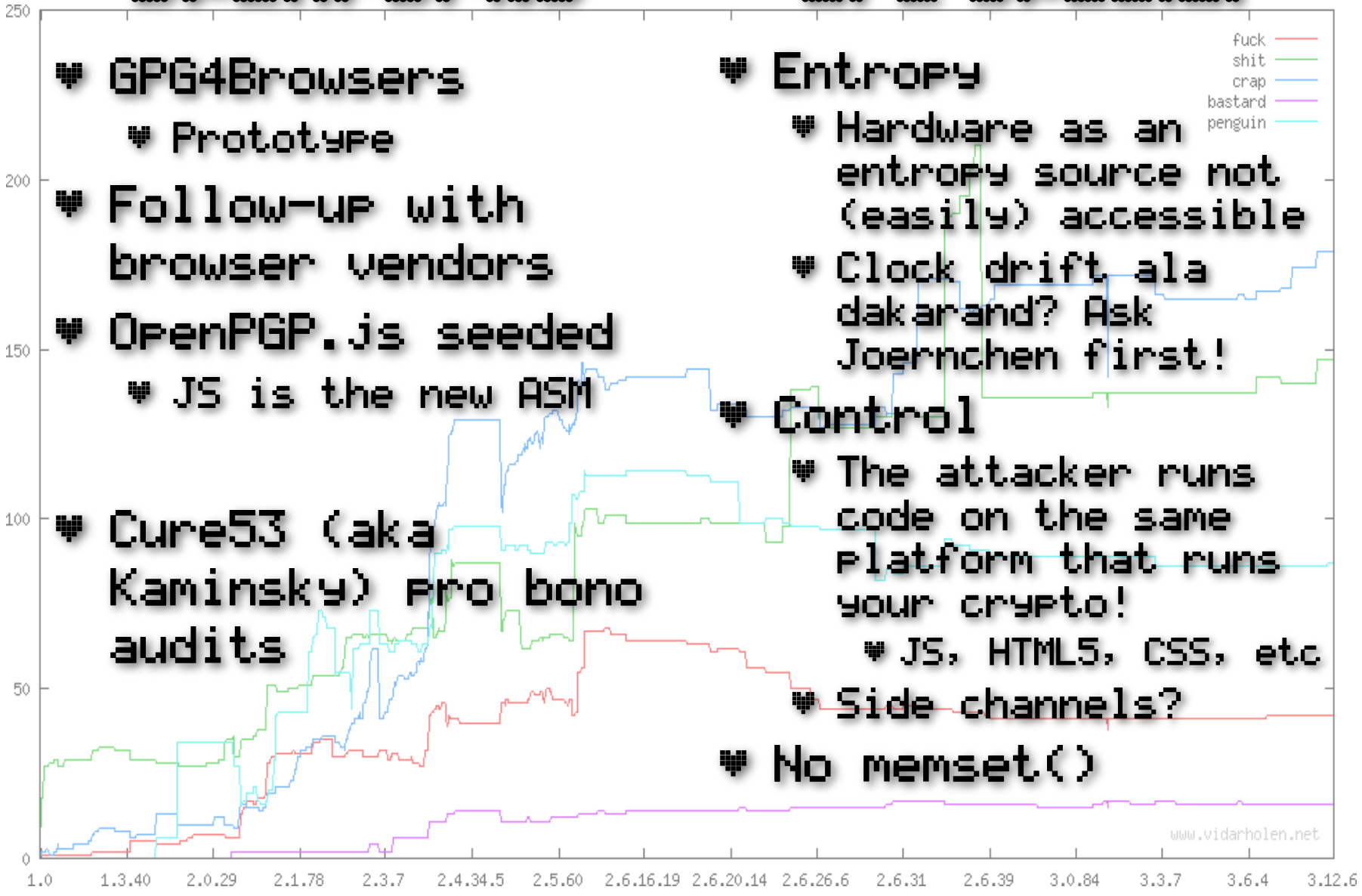


OpenPGP.js

Browser are special

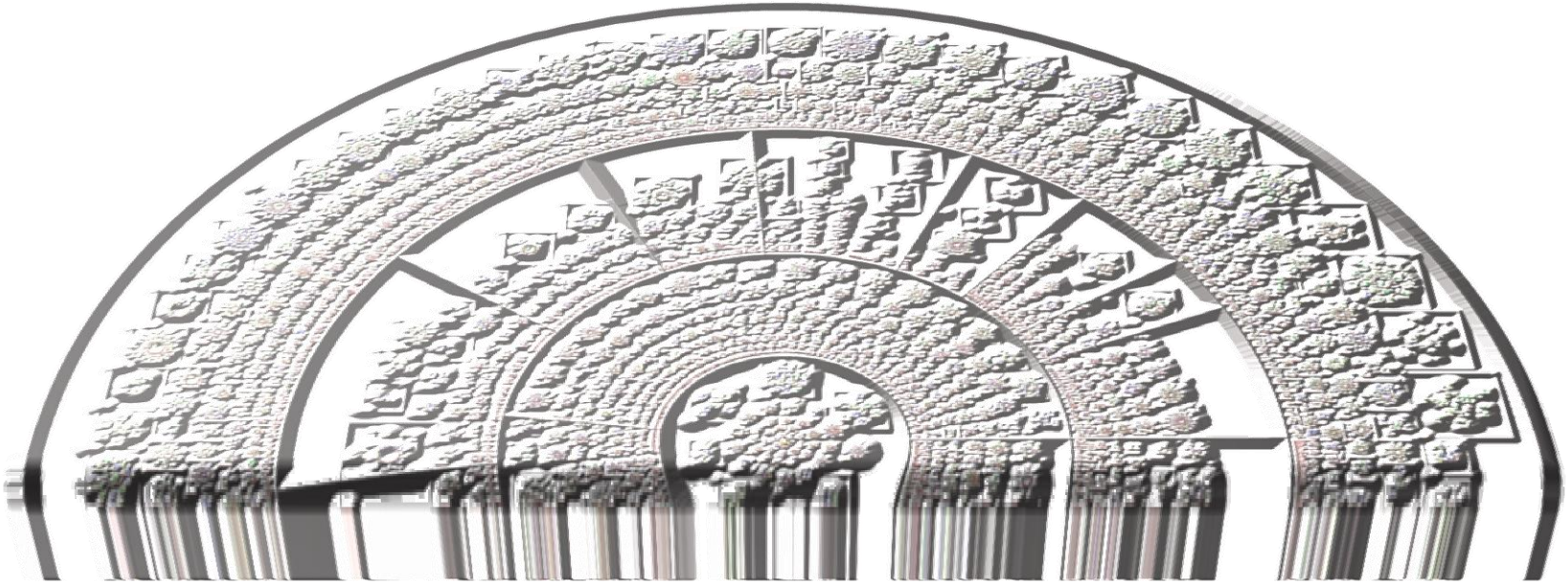
- GPG4Browsers
  - Prototype
- Follow-up with browser vendors
- OpenPGP.js seeded
  - JS is the new ASM
- Cure53 (aka Kaminsky) pro bono audits

- Entropy
  - Hardware as an entropy source not (easily) accessible
  - Clock drift ala dakarand? Ask Joernchen first!
- Control
  - The attacker runs code on the same platform that runs your crypto!
    - JS, HTML5, CSS, etc
  - Side channels?
- No memset()



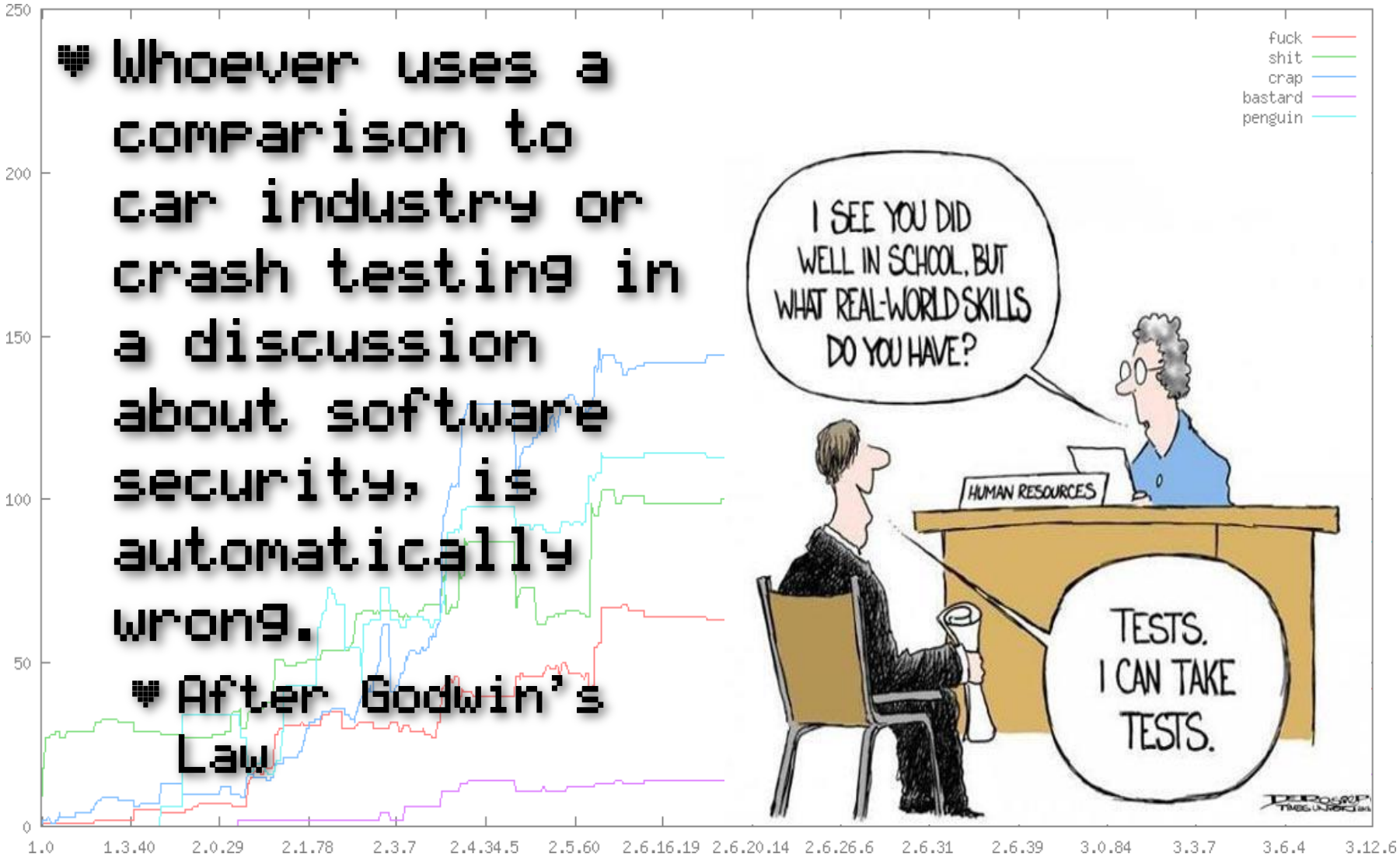
JAHRESLOHNSTEUERAUSGLEICHSFORMULAR

TESTING CRYPTO



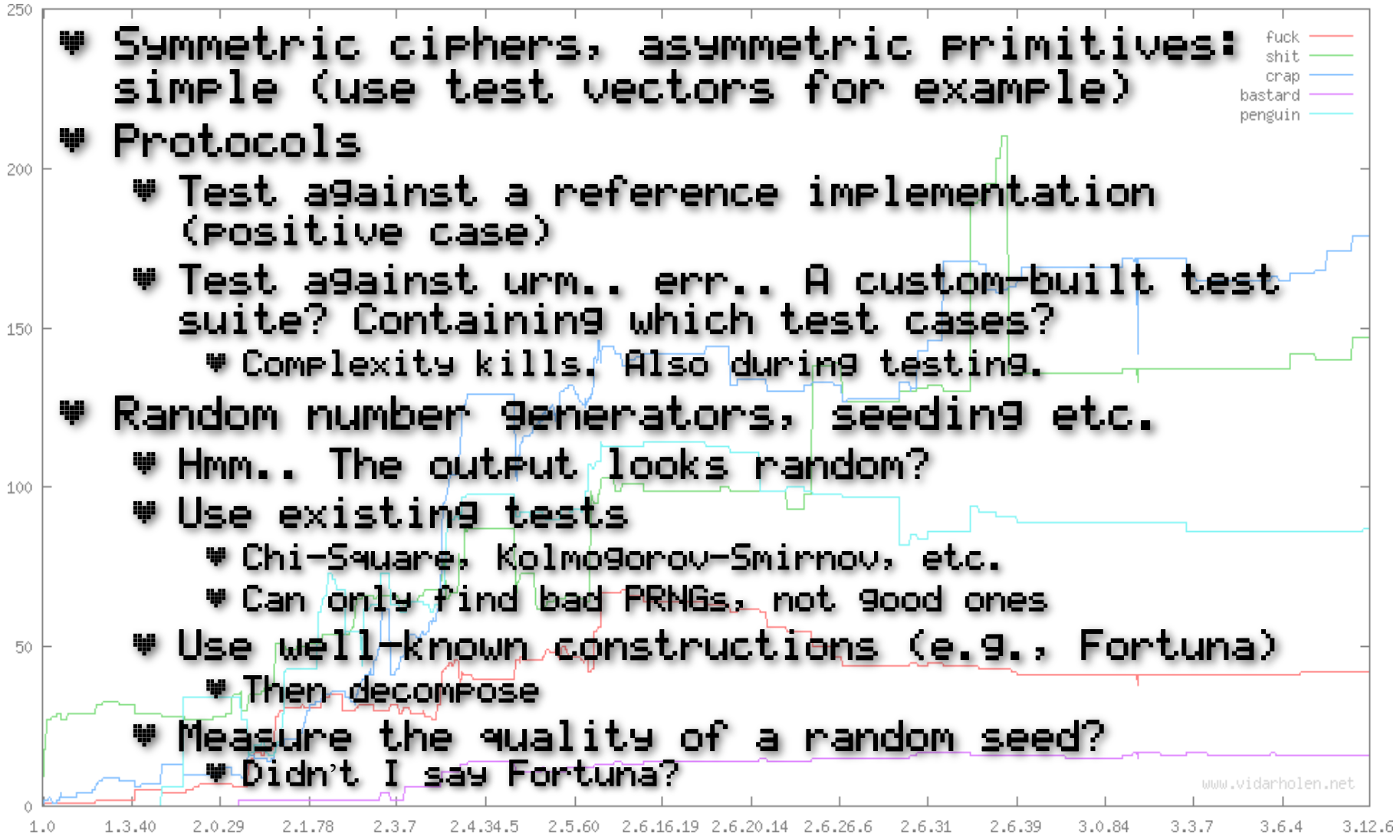
HELMBRECHT'S LAW

- Whoever uses a comparison to car industry or crash testing in a discussion about software security, is automatically wrong.
  - After Godwin's Law



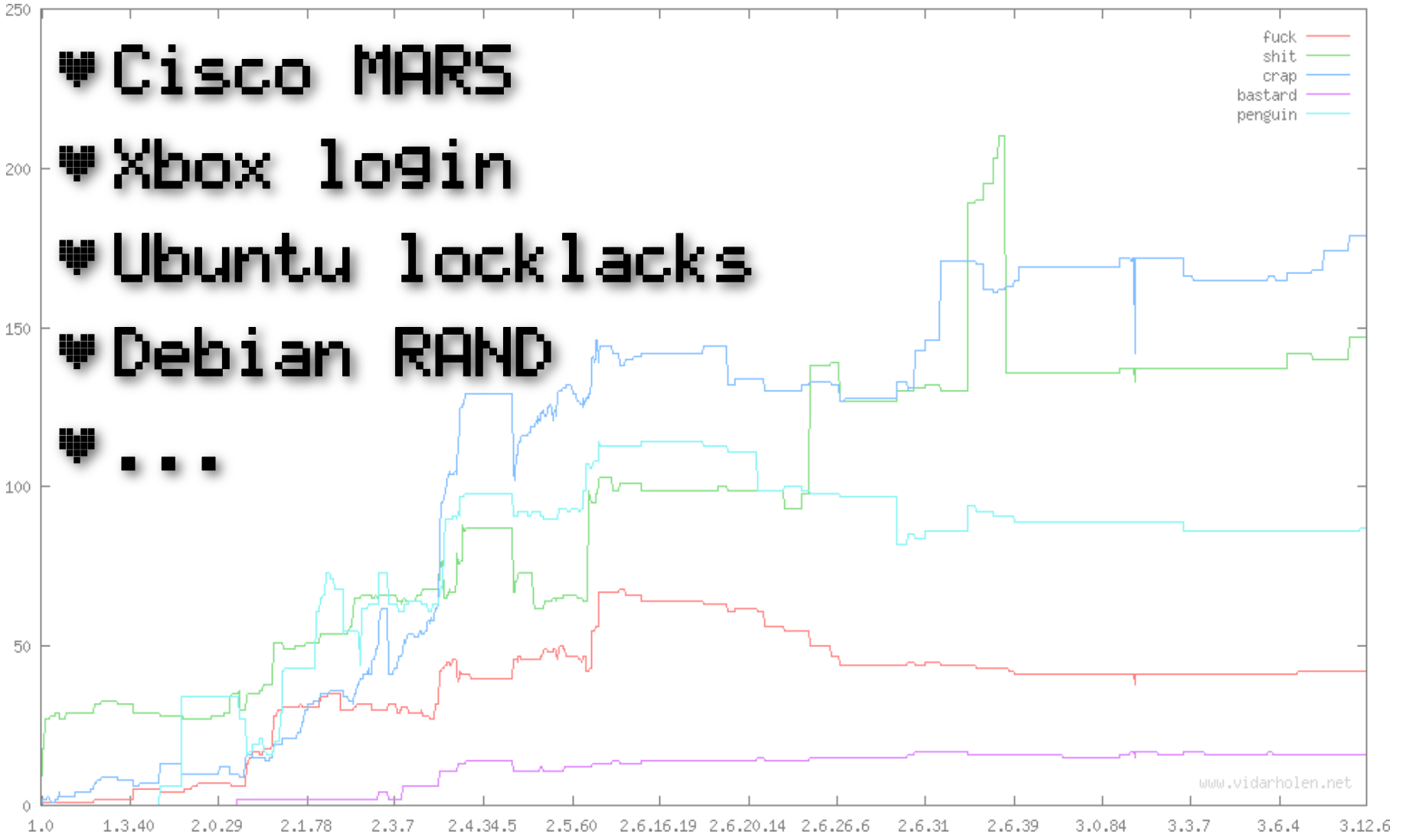
CHALLENGES AND HOWTO

- Symmetric ciphers, asymmetric primitives: simple (use test vectors for example)
- Protocols
  - Test against a reference implementation (positive case)
  - Test against urm.. err.. A custom-built test suite? Containing which test cases?
    - Complexity kills. Also during testing.
- Random number generators, seeding etc.
  - Hmm.. The output looks random?
  - Use existing tests
    - Chi-Square, Kolmogorov-Smirnov, etc.
    - Can only find bad PRNGs, not good ones
  - Use well-known constructions (e.g., Fortuna)
    - Then decompose
  - Measure the quality of a random seed?
    - Didn't I say Fortuna?



MINIMUM TESTING

- Cisco MARS
- Xbox login
- Ubuntu locklacks
- Debian RAND
- ...



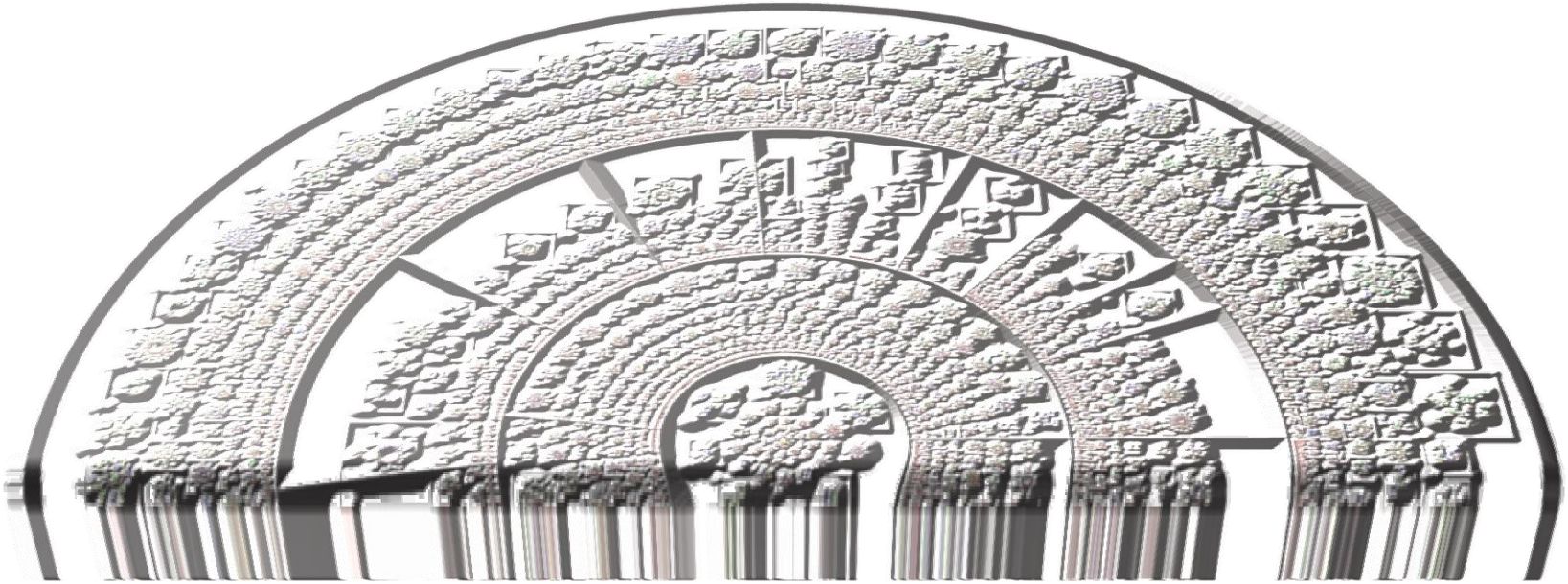
WELCHE SPRACHEN SPRECHEN SIE?

3, 3+ LANGUAGES: MULTILINGUAL

2 LANGUAGES: BILINGUAL

1 LANGUAGE: AMERICAN

LANGUAGES MATTER



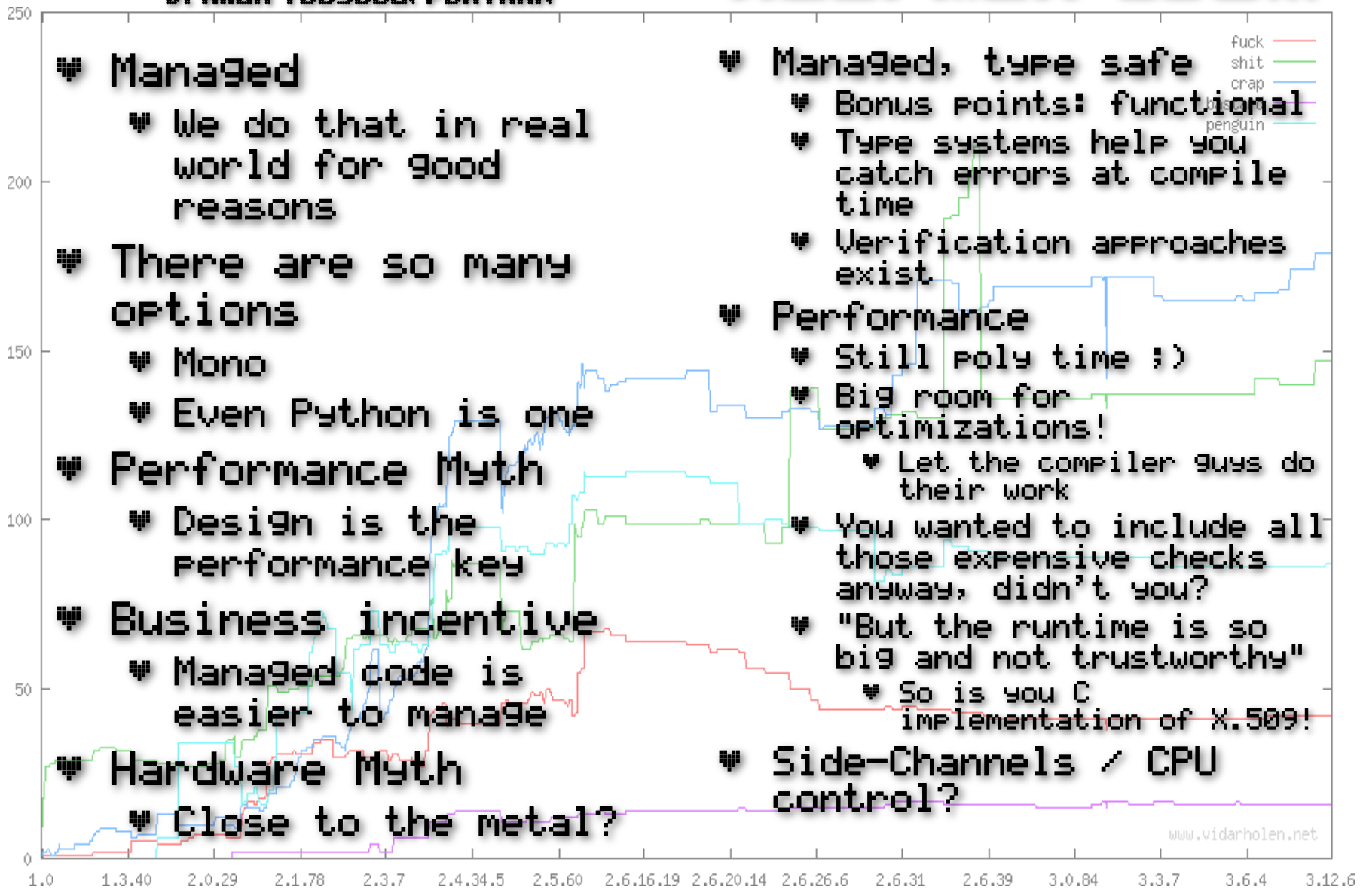
God is Real, unless declared Integer

J. Allan Toogood, FORTRAN

Real men use...

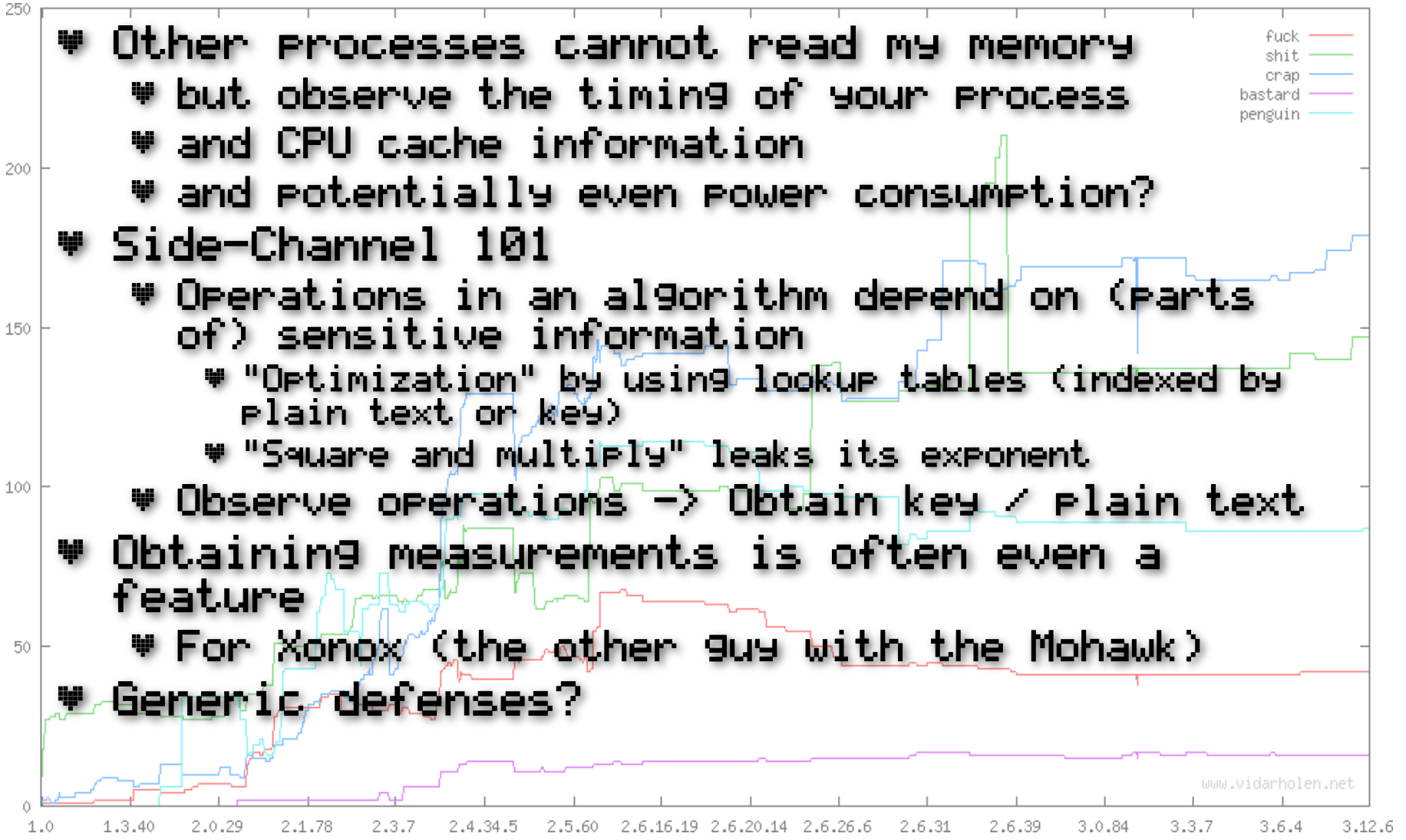
- Managed
  - We do that in real world for good reasons
- There are so many options
  - Mono
  - Even Python is one
- Performance Myth
  - Design is the performance key
- Business incentive
  - Managed code is easier to manage
- Hardware Myth
  - Close to the metal?

- Managed, type safe
  - Bonus points: functional
  - Type systems help you catch errors at compile time
  - Verification approaches exist
- Performance
  - Still poly time ;)
  - Big room for optimizations!
    - Let the compiler guys do their work
  - You wanted to include all those expensive checks anyway, didn't you?
  - "But the runtime is so big and not trustworthy"
    - So is you C implementation of X.509!
- Side-Channels / CPU control?

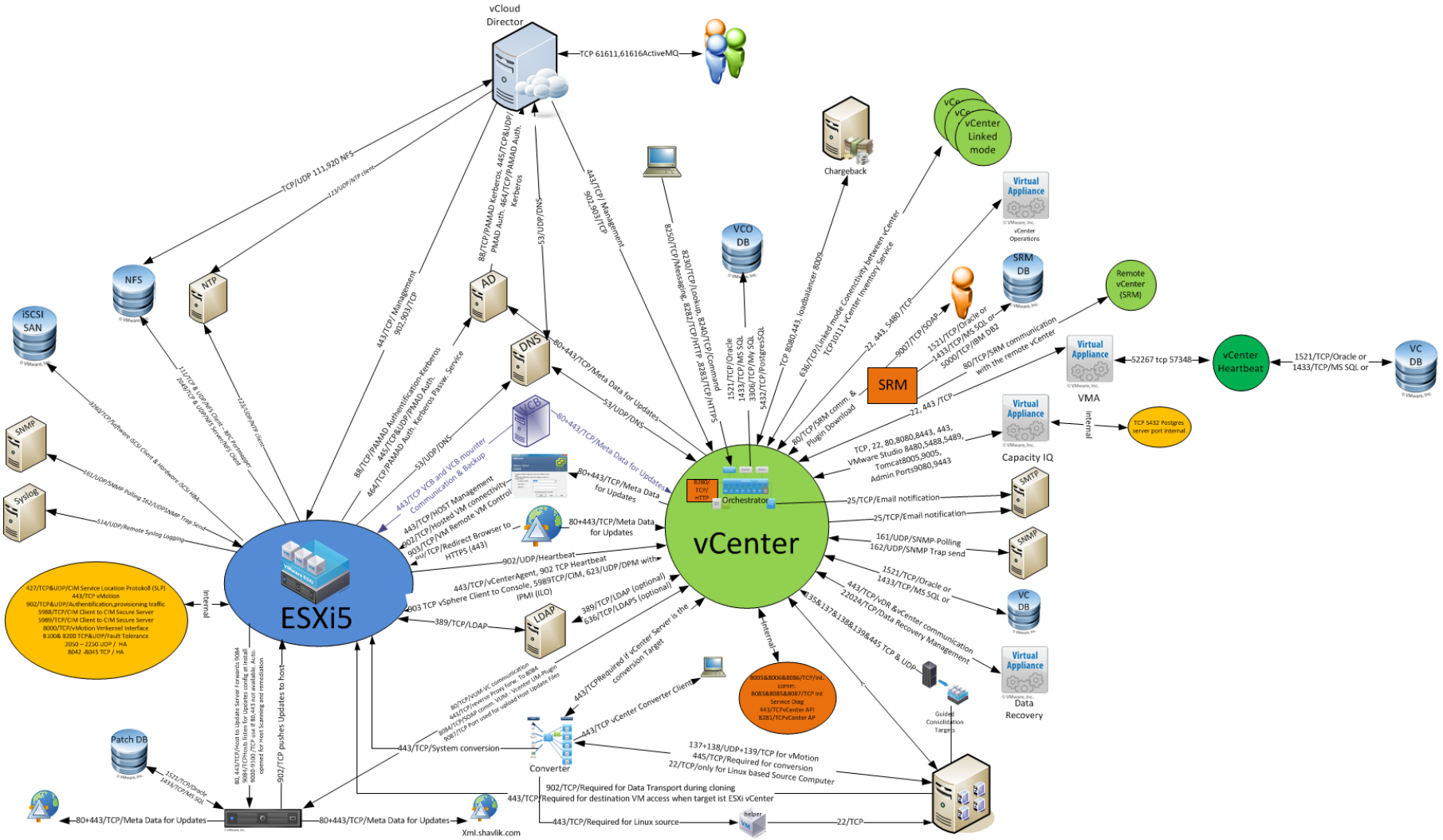


YOU ARE NOT ALONE (ON THE CPU)

- Other processes cannot read my memory
  - but observe the timing of your process
  - and CPU cache information
  - and potentially even power consumption?
- Side-Channel 101
  - Operations in an algorithm depend on (parts of) sensitive information
    - "Optimization" by using lookup tables (indexed by plain text or key)
    - "Square and multiply" leaks its exponent
  - Observe operations -> Obtain key / plain text
- Obtaining measurements is often even a feature
  - For Xonox (the other guy with the Mohawk)
- Generic defenses?

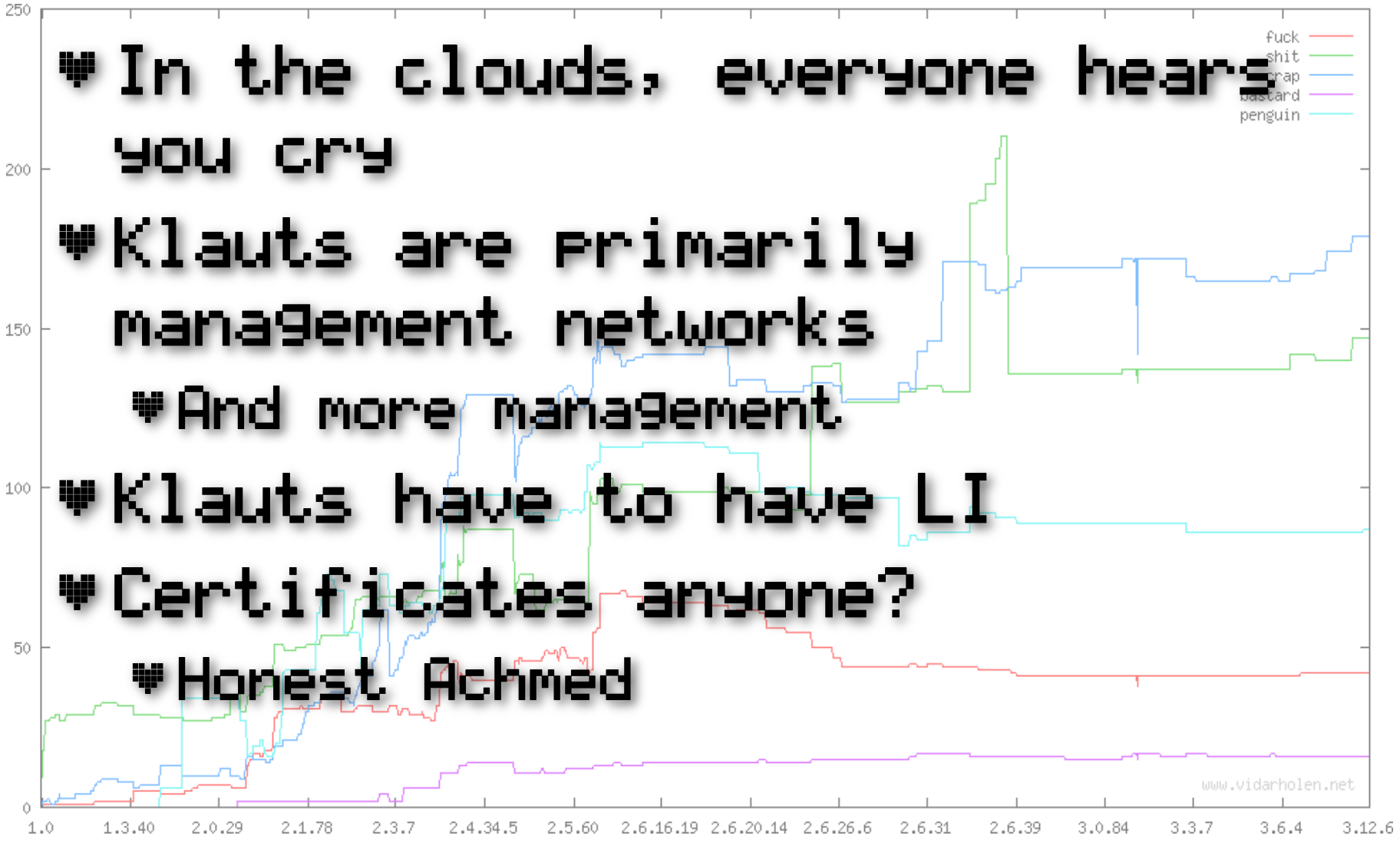


CRYPTO IN THE KLAUTS



CRYPTO IN THE KLAUTS

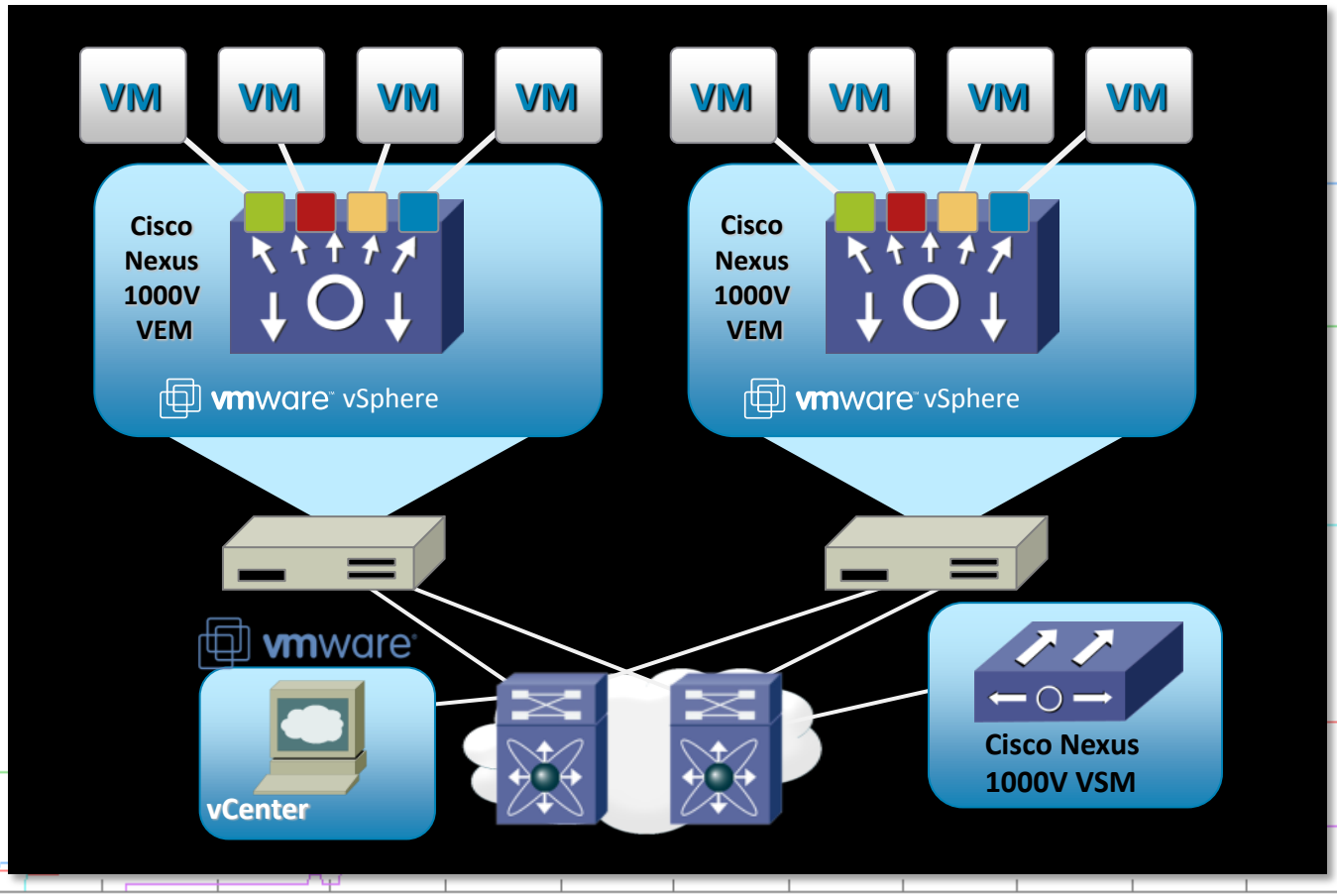
- In the clouds, everyone hears you cry
- Klauts are primarily management networks
  - And more management
- Klauts have to have LI
- Certificates anyone?
  - Honest Achmed




CISCO
In The Sky
With Diamonds

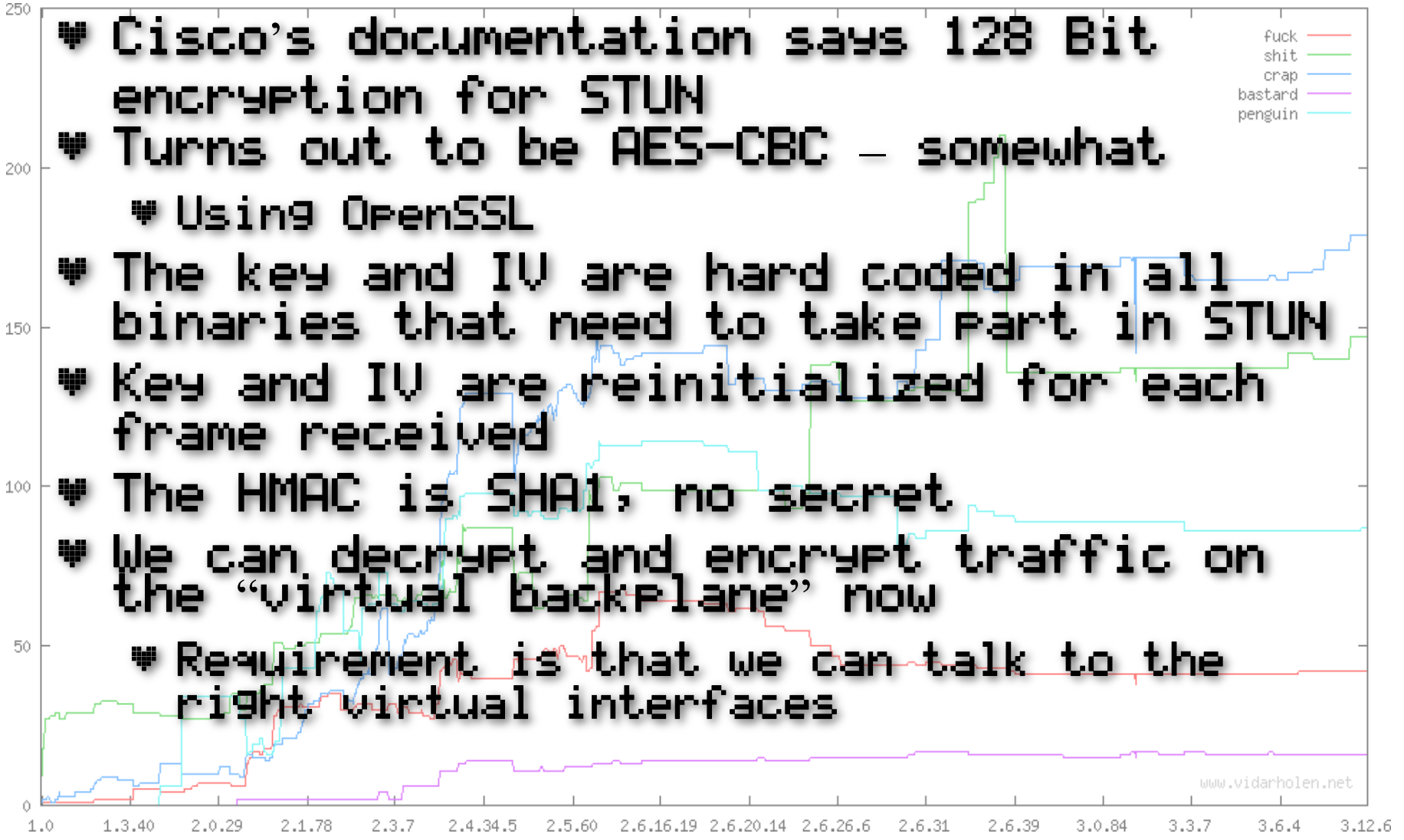
UND WAS IST MIT CISCOMFG?

- Cisco Nexus 1000V



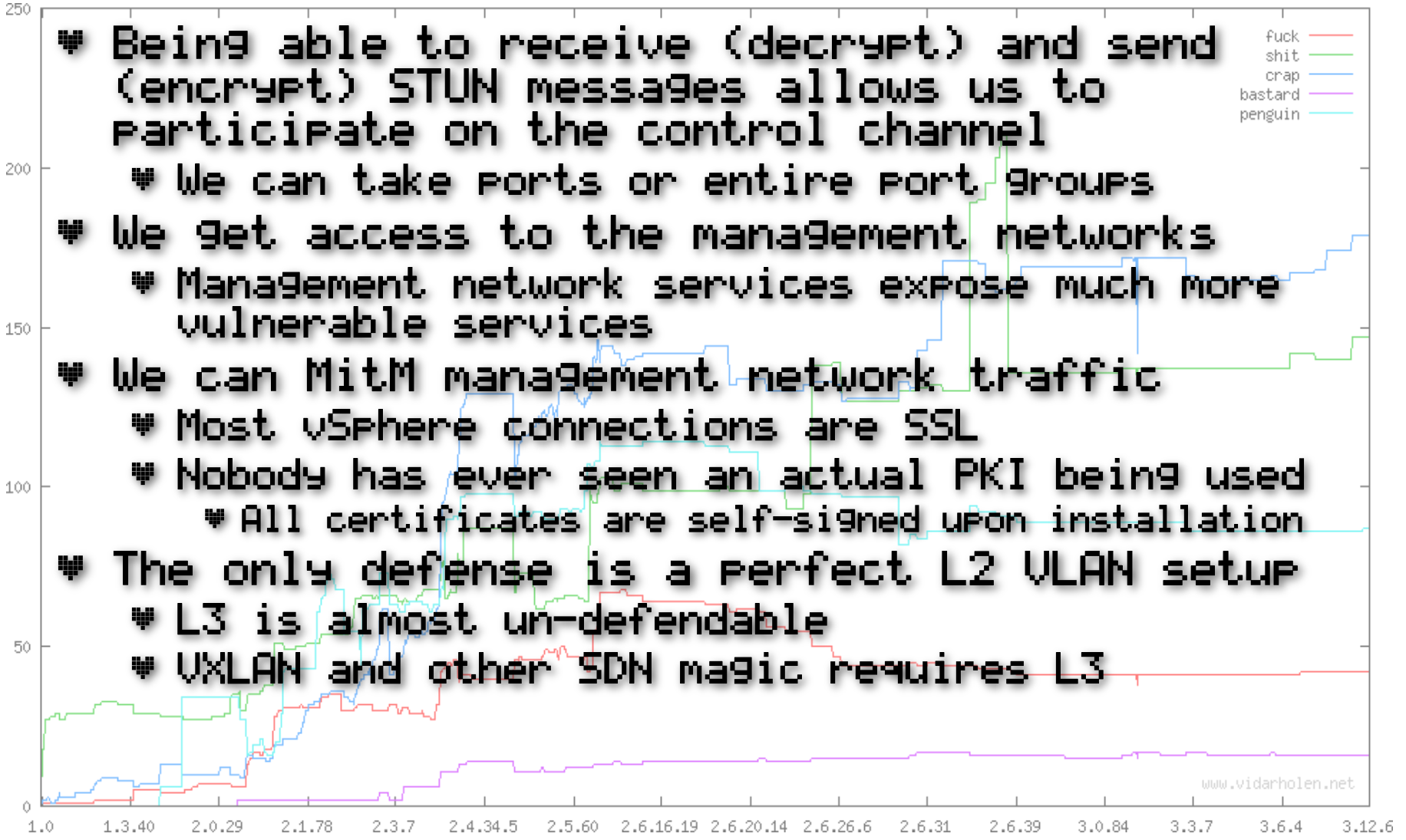
UND WAS IST MIT CISCOMFG?

- Cisco's documentation says 128 Bit encryption for STUN
- Turns out to be AES-CBC – somewhat
  - Using OpenSSL
- The key and IV are hard coded in all binaries that need to take part in STUN
- Key and IV are reinitialized for each frame received
- The HMAC is SHA1, no secret
- We can decrypt and encrypt traffic on the "virtual backplane" now
  - Requirement is that we can talk to the right virtual interfaces



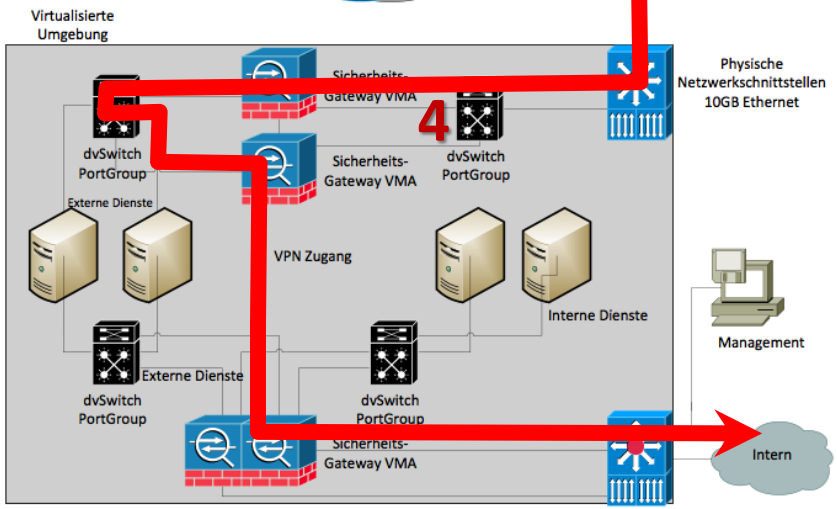
WHO WAS IST MIT CISCONFG?

- Being able to receive (decrypt) and send (encrypt) STUN messages allows us to participate on the control channel
  - We can take ports or entire port groups
- We get access to the management networks
  - Management network services expose much more vulnerable services
- We can MitM management network traffic
  - Most vSphere connections are SSL
  - Nobody has ever seen an actual PKI being used
    - All certificates are self-signed upon installation
- The only defense is a perfect L2 VLAN setup
  - L3 is almost un-defendable
  - VXLAN and other SDN magic requires L3



UND WAS IST MIT CISCONFG?

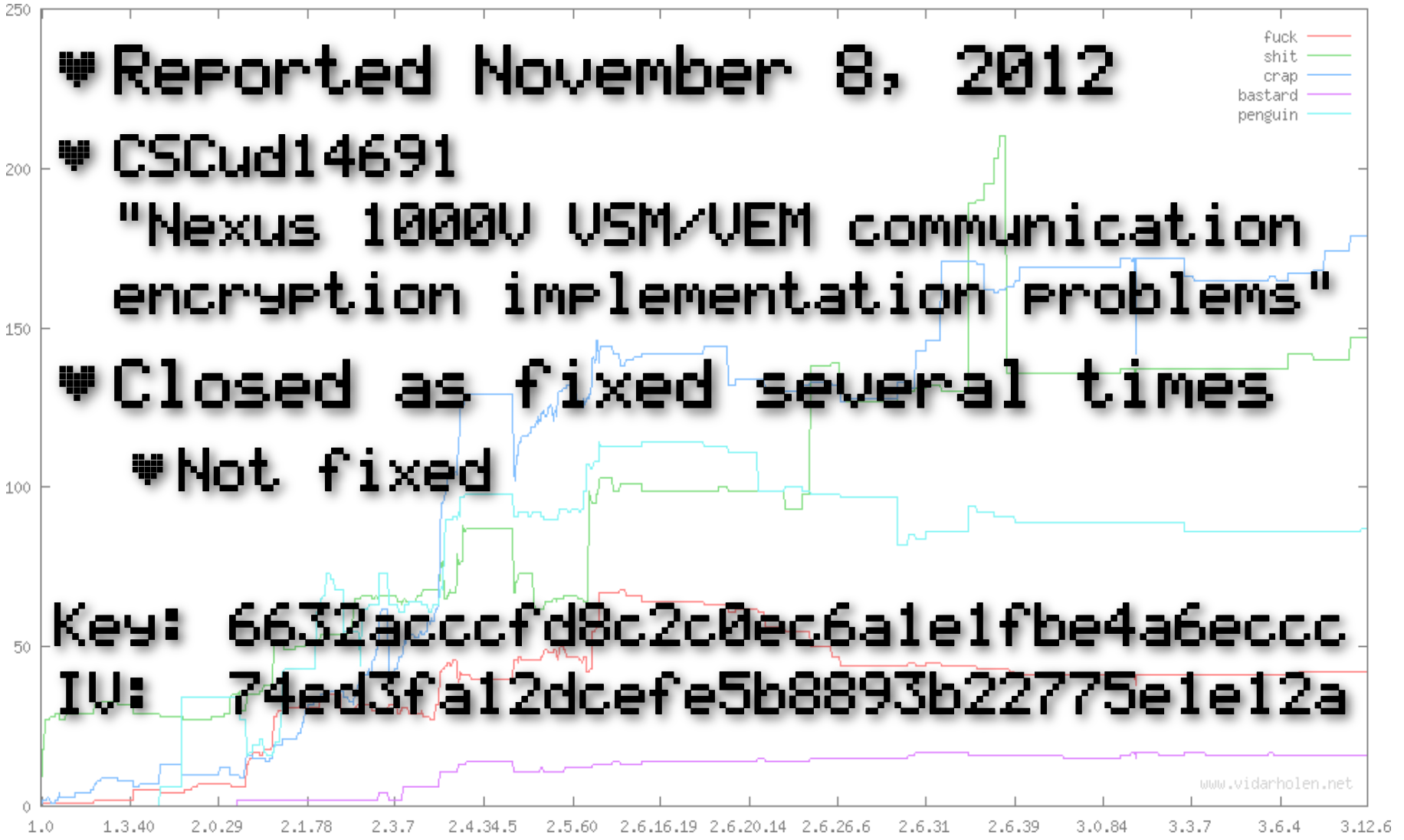
1. Compromise a web server in a virtual DMZ
   - ➔ Non-administrative shell
2. Upload a script (e.g. PHP) for STUN L3 communication
3. Run VEM STUN L3 attack to VSM
   - ➔ Takeover of port groups
   - ➔ Configure new mappings
4. Configuration and use of a direct tunnel to internal or management network



UND WAS IST MIT CISCONFG?

- Reported November 8, 2012
- CSCud14691
  "Nexus 1000V VSM/VEM communication encryption implementation problems"
- Closed as fixed several times
  - Not fixed

Key: 6632acccfd8c2c0ec6a1e1fbe4a6eccc
IV: 74ed3fa12dcefe5b8893b22775e1e12a

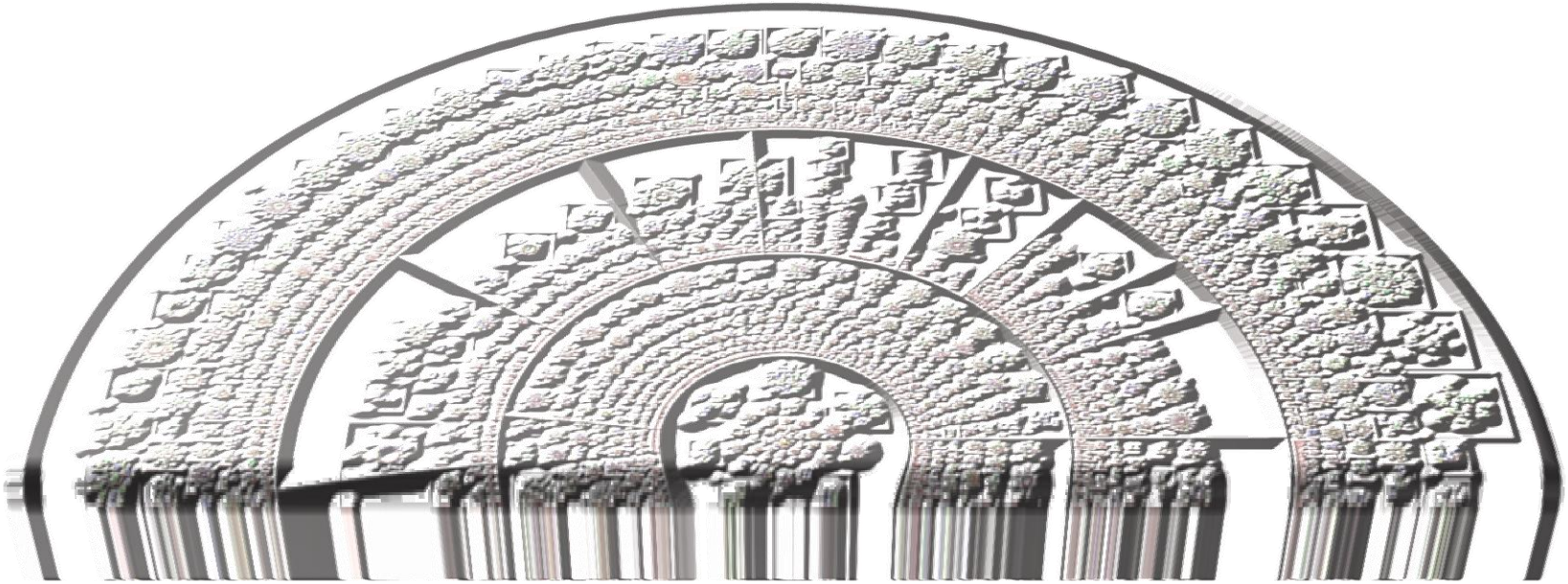


SCHLUESSELPOSITION:

ENTWEDER MAN KANN ES ODER MAN

TRAEGT DIE VERANTWORTUNG

KEYS TO THE CRYPTO



```
        $index_page = $this->hide_index?'':'index.php';
        $this->change_config($file_name, "index_page", $index_page, $key_prefix, $key_suffix,
-       $this->change_config($file_name, "encryption_key", 'namidanoregret', $key_prefix, $key
+       $encryption_key = md5(time() . rand());
+       $this->change_config($file_name, "encryption_key", $encryption_key, $key_prefix, $key_
        $table_name = 'ci_sessions';
        if(!trim($this->db_table_prefix) == ''){
            $table_name = $this->db_table_prefix.'_'.$table_name;
```

THE BIGGEST ISSUE

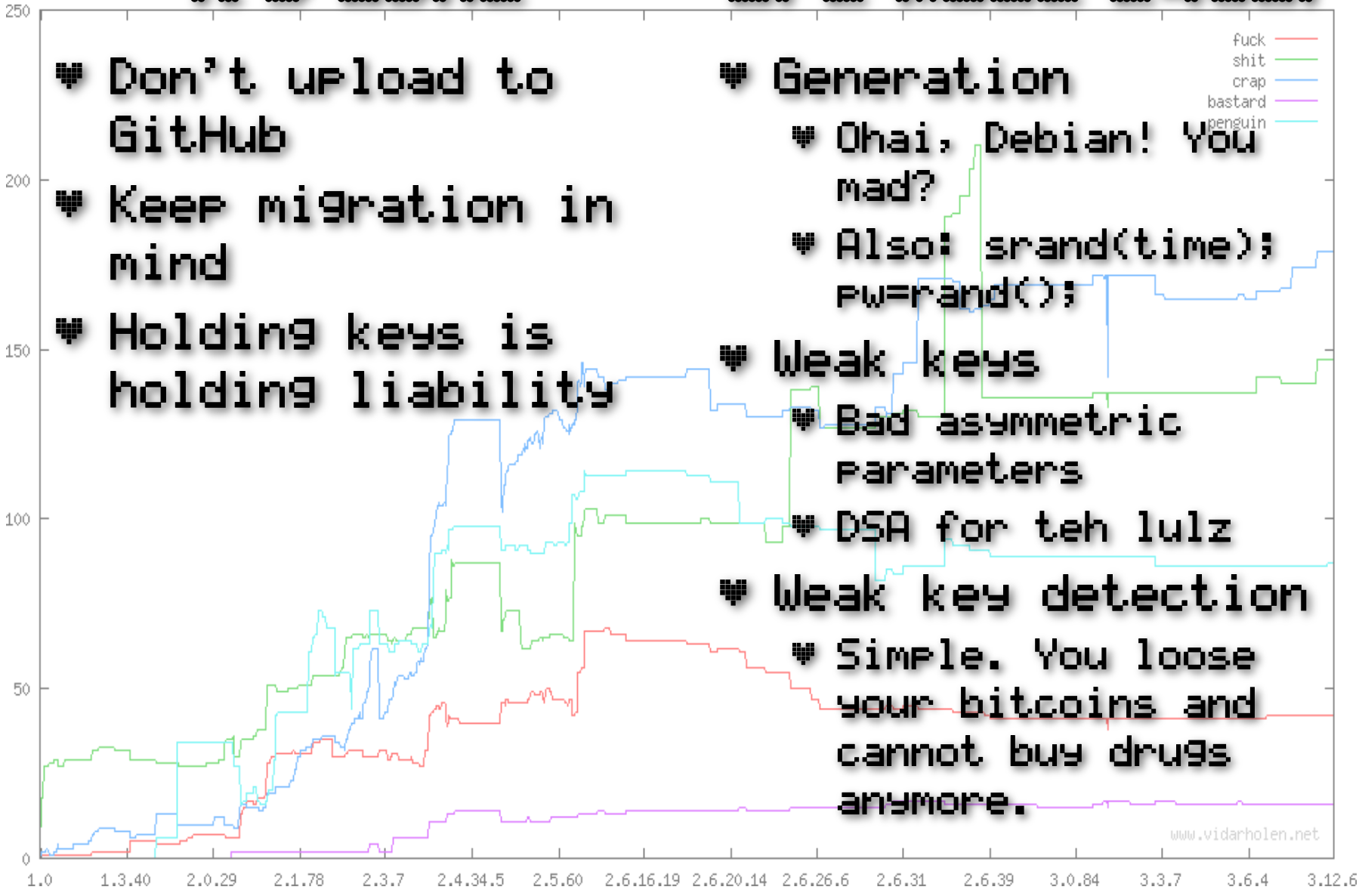
Keys are hard

When it's gone it's done

- Don't upload to GitHub
- Keep migration in mind
- Holding keys is holding liability

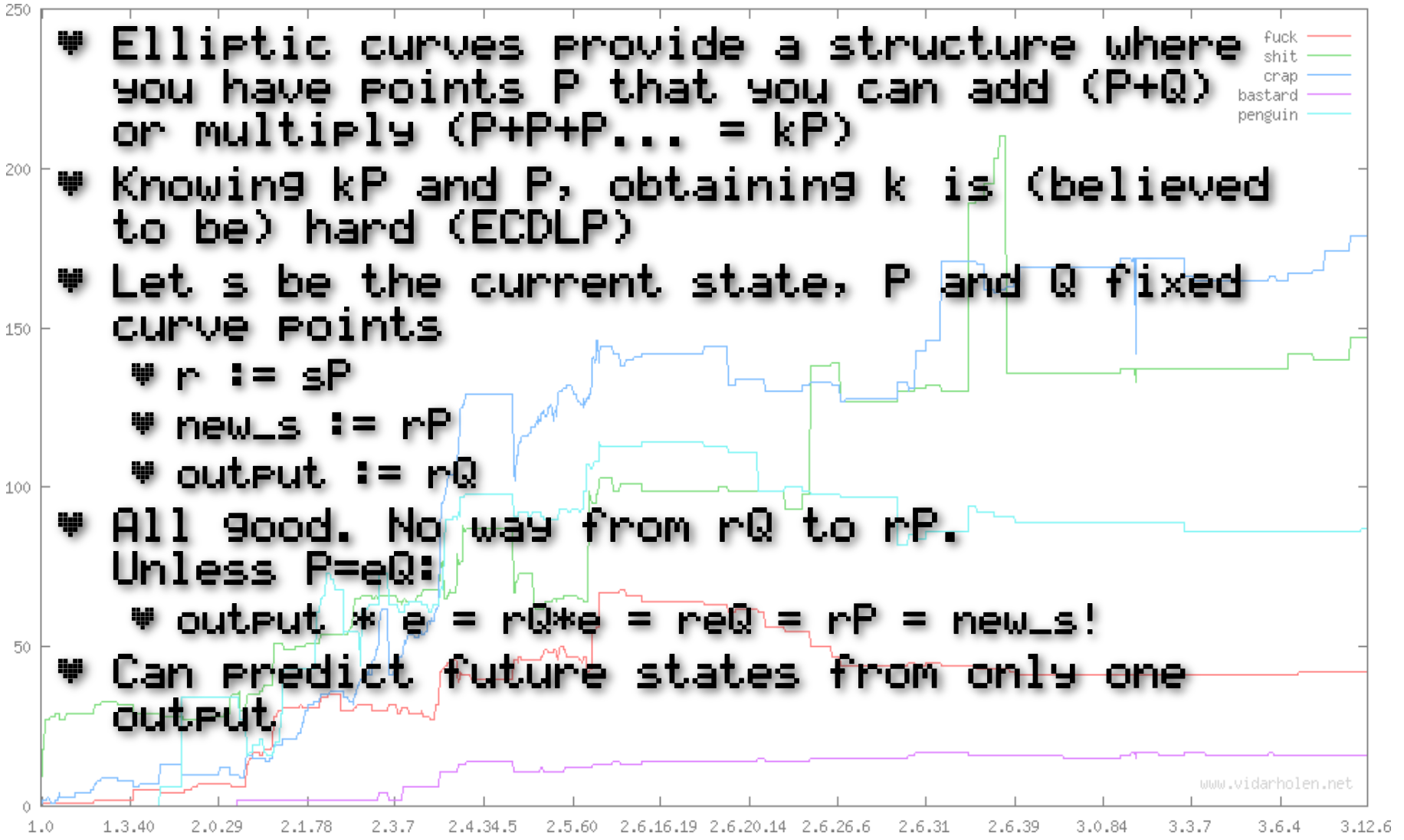
Not all keys are made equal

- Generation
  - Ohai, Debian! You mad?
  - Also: srand(time); pw=rand();
- Weak keys
  - Bad asymmetric parameters
  - DSA for teh lulz
- Weak key detection
  - Simple. You loose your bitcoins and cannot buy drugs anymore.



NIST SP800-90

- Elliptic curves provide a structure where you have points P that you can add (P+Q) or multiply (P+P+P... = kP)
- Knowing kP and P, obtaining k is (believed to be) hard (ECDLP)
- Let s be the current state, P and Q fixed curve points
  - r := sP
  - new_s := rP
  - output := rQ
- All good. No way from rQ to rP. Unless P=eQ:
  - output * e = rQ*e = reQ = rP = new_s!
- Can predict future states from only one output



RECHNUNG
CVE-2014-0160

- OpenSSL versions on all machines
- Again for creative .so names/dirs
- Compile OpenSSL
- Compile OpenSSL #Please?
- Compile OpenSSL DAMN IT!
- Deploy
- Search binaries hard linked ^U
- Download IDS signature from ^W
- HTTP BLOCK "heartbleed" WHERE
  $SRC IN NET (VORSTAND || BUND)
- PORN & BEER Time!!! ^D
  - Mist! Frau Zuhause :(^Z^Z^Z^Z

♥lichen Dank auch!

ES BEDIENTE SIE
4817504D069B4C5082161B02A22116AD75F822B1
PAUERT BEI TEH-SYSTEMZ