IN SEARCH OF EVIDENCE-BASED IT-SECURITY

Hanno Böck
https://hboeck.de

INTRODUCTION

Hanno Böck, freelance journalist and hacker.

Writing for Golem.de and others.

Fuzzing Project, funded by Linux Foundation's Core Infrastructure Initiative.

Author of monthly Bulletproof TLS Newsletter.

IT SECURITY PRODUCTS

Picture: Hanno Böck, Black Hat USA 2016

Picture: Hanno Böck, Black Hat USA 2016

Picture: Hanno Böck, Black Hat USA 2016

Picture: Hanno Böck, Black Hat USA 2016

I'M A BIT SKEPTICAL

Tavis Ormandy
@taviso · 14 Dec 2015
271 221

A stack buffer overflow in Avast! because strncpy() was replaced with strcpy() in some open source code. code.google.com/p/google-secur… ¯_(ツ)_/¯

Tavis Ormandy
@taviso · Mar 30
902 545

TrendMicro accidentally left a remote debugging server running on all customer machines ¯_(ツ)_/¯ #oops

Issue 773 - project-zero - TrendMicro: A remote debugger stub is listening in default…
bugs.chromium.org

Tavis Ormandy
@taviso · Nov 18
346 319

Here's a remote memory corruption in Palo Alto Networks bugs.chromium.org/p/project-zero…. They ship an EOL web server ¯_(ツ)_/¯

908 - Palo Alto Networks PanOS: appweb3 stack buffer overflow - project-zero - Monorail
bugs.chromium.org

Tavis Ormandy
@taviso · 15 Dec 2015
148 124

If you work for AVG, please email me - I'm about to give up trying to find an address to report vulns to. Also, your code makes zero sense.

Source: Twitter / Tavis Ormandy ([1], [2], [3], [4])

PCWorld FROM IDG

SUBSCRIBE

NEWS | REVIEWS | HOW-TO | VIDEO | BUSINESS | LAPTOPS | TABLETS | PHONES | HARDWARE | SECURITY | SOFTWARE | GADGETS

Privacy | Encryption | Antivirus

Home / Security

NEWS

Antivirus software could make your company more vulnerable

Security researchers are worried that critical vulnerabilities in antivirus products are too easy to find and exploit

The Register® Biting the hand that feeds IT

DATA CENTRE | SOFTWARE | SECURITY | TRANSFORMATION | DEVOPS | BUSINESS | PERSONAL TECH | SCI

Security

Antivirus tools are a useless box-ticking exercise says Google security chap

Advocates whitelists and other tools that 'genuinely help' security

April King
@aprilmpls

Following

@justinschuh @VessOnSecurity @codelancer @taviso Not speaking for my employer (@mozilla) but AV causes piles of security issues for Firefox.

RETWEETS 26 LIKES 67

5:28 PM - 1 Dec 2016

4 26 67 •••

Justin Schuh
@justinschuh

Following

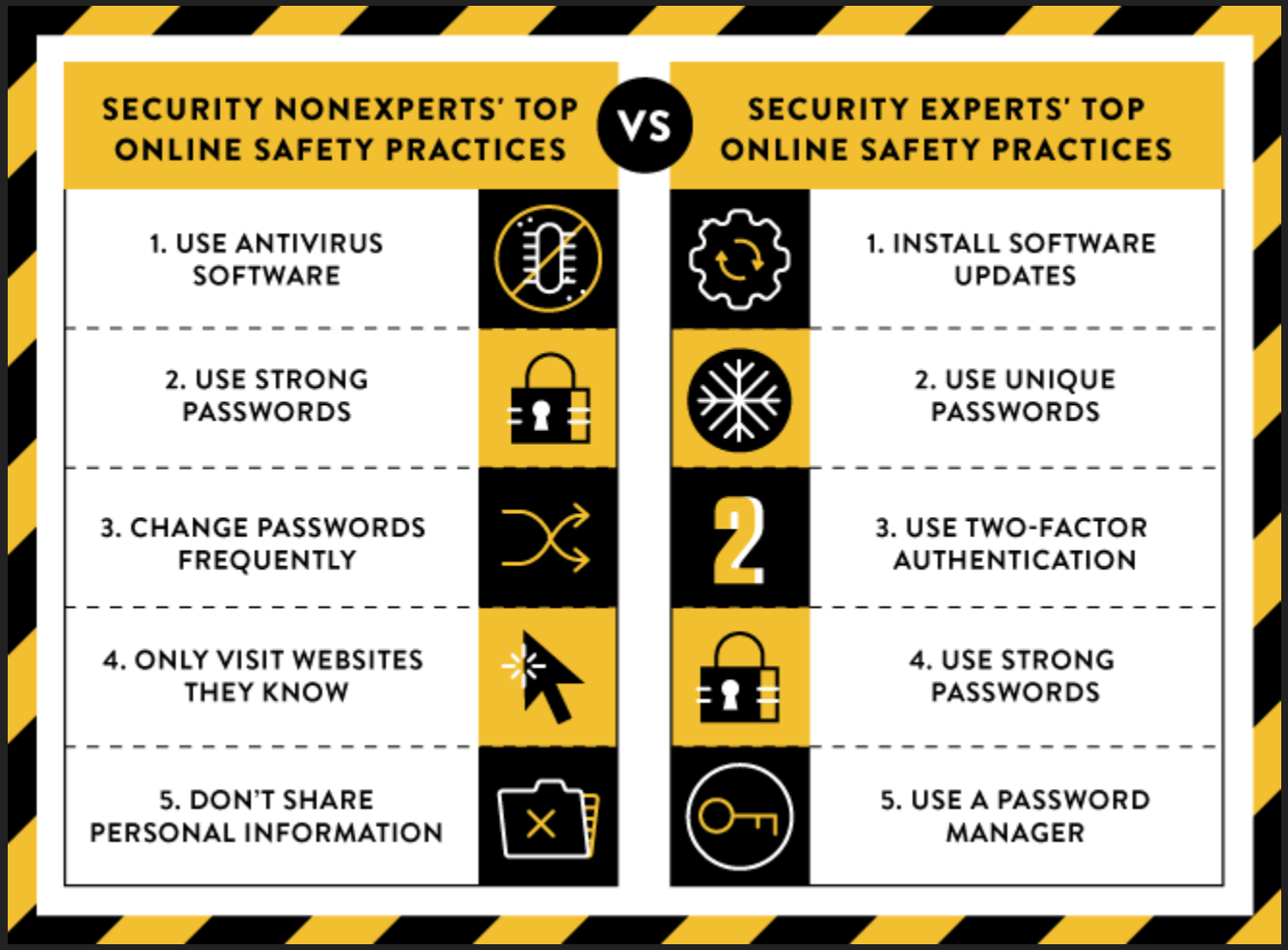
@taviso @VessOnSecurity @CarlGottlieb @ecbftw @ygjb Or keeping the medical analogy, AV is to security what homeopathy is to medicine.

RETWEETS 20 LIKES 42

9:20 PM - 3 Dec 2016

5 20 42 •••

Sources: PCWorld, The Register, April King/Twitter, Justin Schuh/Twitter.



New research: Comparing how security experts and non-experts stay safe online (Google Security)

THERE IS CONSIDERABLE DISAGREEMENT WHETHER MANY IT SECURITY AND ESPECIALLY ANTIVIRUS PRODUCTS ARE A GOOD IDEA.

HOW DO WE KNOW IF THESE THINGS WORK?

LET'S LOOK AT SOMETHING COMPLETELY DIFFERENT

ANOTHER ANTI-VIRUS

Pictures: CDC/Wikimedia Commons, Hanno Böck

VITAMIN C AGAINST THE COMMON COLD

It's probably not very useful.

Why do we know that?

SCIENCE!

VITAMIN C

Regular ingestion of vitamin C had no effect on common cold incidence in the ordinary population [...]. However, regular supplementation had a modest but consistent effect in reducing the duration of common cold symptoms [...].

Trials of high doses of vitamin C administered therapeutically, starting after the onset of symptoms, showed no consistent effect on the duration or severity of common cold symptoms.

Vitamin C for preventing and treating the common cold, H. Hemilä, E. Chalker, Cochrane Library (2013)

RANDOMIZED CONTROLLED TRIAL (RCT)

Randomly split patients in groups.

Simple: Group A gets medication, Group B gets placebo

More complex: Group A gets new medication, Group B gets best old medication, Group C does alternative to medication, e.g. exercise.

See who gets better.

META ANALYIS

We don't care about single studies. We care about all the evidence we have.

Meta analysis: Pool results from all available studies.

EVIDENCE-BASED MEDICINE

Ideally all decisions in medicine should be based on high quality scientific evidence.

SCIENCE HAS PROBLEMS

PLOS | MEDICINE

ESSAY

Why Most Published Research Findings Are False

John P. A. Ioannidis

NATURE | NEWS

Over half of psychology studies fail reproducibility test

Largest replication study to date casts doubt on many published positive results.

STAT

Newsletters | Log In / Subscribe

THE WATCHDOGS

Many clinical trials' findings never get published. Here's why that's bad

Sources: PLOS One, Nature News, STAT

SPOTTING BAD SCIENCE (1)

Small number of research subject (underpowered studies).

Making causal claims although the data only supports a correlation (too many results purely rely on observational data).

Single or few studies. Good science needs to be replicated.

SPOTTING BAD SCIENCE (2)

Publication bias - only studies with "postive" results get published.

Fishing for results and outcome switching. (If we don't find X in our data, maybe we find something else.)

Ideally all empirical studies should be preregistered (but we're very far from that).

NOW LET'S GET BACK TO IT SECURITY

This was an empty slide.

It was also the complete list of all randomized controlled trials ever done on the effectiveness of Antivirus applications or other IT security products.

QUESTIONABLE ANTIVIRUS TESTS

There are some tests that compare Antivirus prudcts against each other (AV-Test, AV comparatives), but the methodology is extremely flawed.

PROBLEMS WITH NAIVE ANTIVIRUS TESTS

If a software detects a malware it does not mean it would've caused harm if undetected.

Alternatives to Antivirus software are not considered.

Antivirus software as a security risk is not considered.

None of these tests are with real users.

QUESTIONABLE STATISTICS

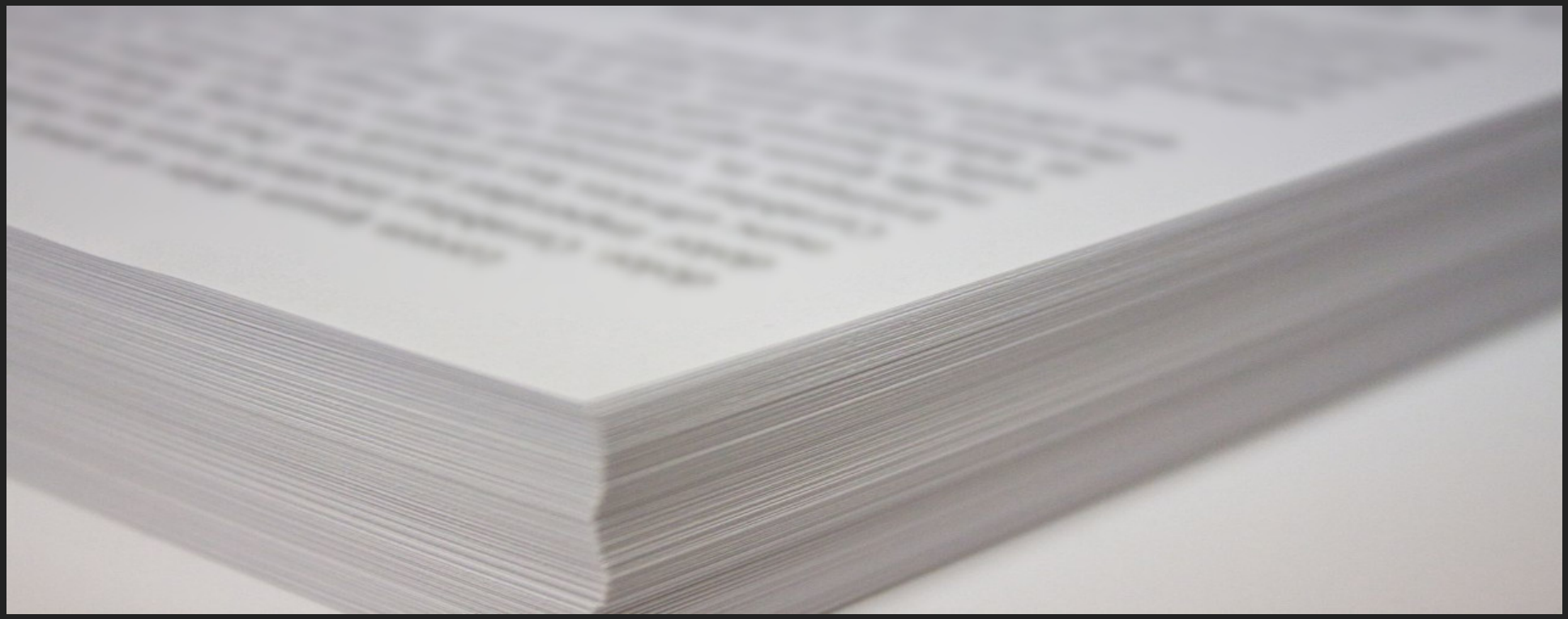
Bad statistics about IT security are common.

The most notorious example is probably CVE counting.

(see also Black Hat USA 2013 - Buying into the Bias: Why Vulnerability Statistics Suck)

IT SECURITY IS LARGELY NOT BASED ON SCIENTIFIC EVIDENCE

WAIT, AREN'T THERE PLENTY OF SCIENTIFIC PAPERS AND CONFERENCES ON IT SECURITY?



MOST CITED ACADEMIC SECURITY & CRYPTO PAPERS

1. Candidate Indistinguishability Obfuscation and Functional Encryption for all Circuits
   S Garg, C Gentry, S Halevi, M Raykova, A Sahai, B Waters, FOCS, 2013
2. Candidate Multilinear Maps from Ideal Lattices.
   S Garg, C Gentry, S Halevi, Eurocrypt, 2013
3. FRESCO: Modular Composable Security Services for Software-Defined Networks.
   S Shin, PA Porras, V Yegneswaran, MW Fong, G Gu, M Tyson, NDSS, 2013
4. Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based.
   C Gentry, A Sahai, B Waters, Crypto, 2013

Google Scholar Metrics 2013/2014

PAPERS THAT AFFECT REAL SOFTWARE

11. DREBIN: Effective and Explainable Detection of Android Malware in Your Pocket.
    D Arp, M Spreitzenbarth, M Hubner, H Gascon, K Rieck, NDSS, 2014
20. Lucky Thirteen: Breaking the TLS and DTLS Record Protocols
    NJ Al Fardan, KG Paterson, IEEE S&P, 2013

NOT A SINGLE PAPER THAT TESTS WITH REAL USERS.

IT SECURITY AND SCIENCE

Most academic research in IT security is comparable to basic research.

Practical research tends to investigate interesting, but probably not very relevant parts of the problem.

PROPOSAL FOR A RANDOMIZED CONTROLLED TRIAL ON SECURITY SOFTWARE

Get a large group of users, randomly split them in groups:

- n groups using Security products.
- 1 group using "alternative treatment", e. g. automatic regular updates / application whitelisting.
- 1 group gets a user training ("Don't click on that attachment").
- Placebo (let them do whatever they did before).

RANDOMIZED CONTROLLED TRIAL FOR SECURITY SOFTWARE

- Measure security incidents.
- Measure "side effects" (performance slowdowns, costs, downtimes, ...).
- Compare result after some amount of time.

"BUT THIS IS REALLY HARD!"

YES, IT IS. SORRY, SCIENCE IS HARD.

PROBLEMS

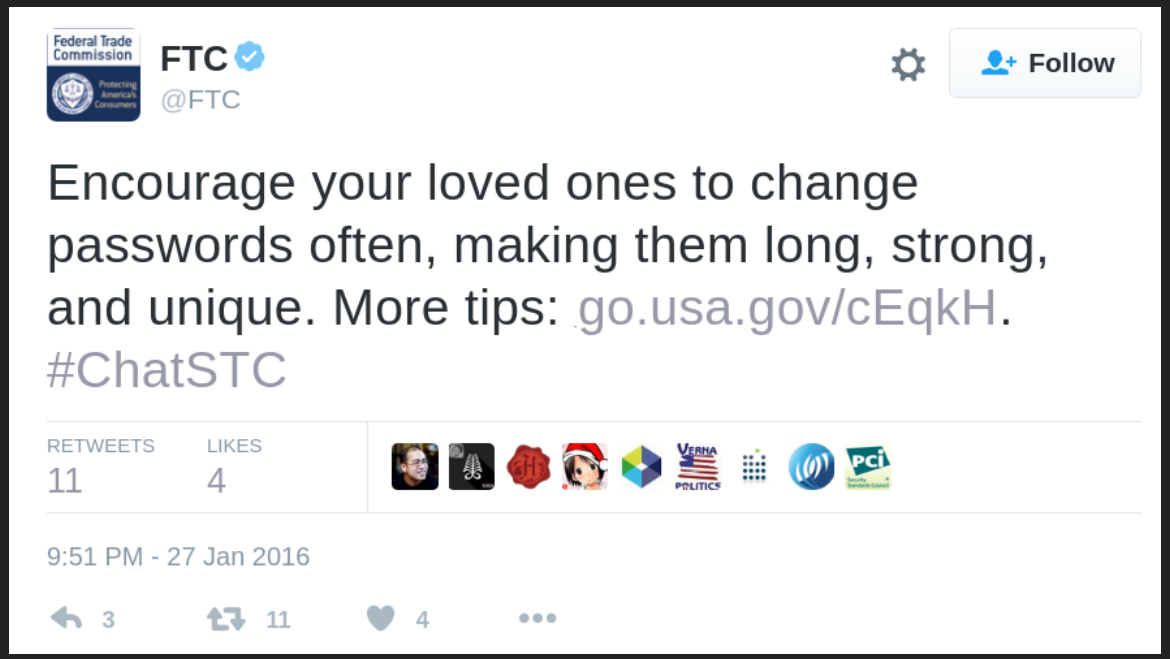
- Ethics (situation comparable to medicine).
- How to measure incidents?
- Standard attacks versus targetted attacks?

OTHER THINGS THAT COULD BE TESTED

Safety of programming languages (e. g. Rust versus C++).

Application security (e. g. different browser brands).

AN EXAMPLE THAT IS BOTH GOOD AND BAD



FTC on Twitter

FTC AND PASSWORDS

The Federal Trade Commission (FTC) found out they had no scientific evidence for their recommendation to change passwords often.

FTC RECOMMENDS THE OPPOSITE

Regular mandatory password changes are probably not a good idea.

We have studies that say so.

HOWEVER...

All of the studies are based on observational data, no intervention studies (Correlation != Causation). Nothing that comes close to a randomized controlled trial.

The studies measure things like password entropy, not real incidents (in medicine you would call that a surrogate endpoint).

FTC AND PASSWORDS

Good: The FTC looked at the scientific evidence.

Not so good: The quality of the evidence was relatively low.

CAVEATS OF EVIDENCE-BASED IT-SECURITY

FUTURE OR VERY RARE THREATS

Post-Quantum Cryptography: We want to protect against future attacks on cryptography.

Reproducible Builds: Protect against rare, but powerful attack scenario.

THERE ARE THINGS YOU SHOULDN'T STUDY

Some IT security products make impossible claims.

"Full protection from malware" - that violates the halting problem.

Related debate in medicine: Should you study claims that violate the laws of physics? (Homeopathy)

EVIDENCE-BASED IT-SECURITY

Today IT security is largely not based on scientific evidence - instead we rely on experience, expert advice or - even worse - marketing.

We should use Evidence-based IT-Security based on high-quality science. However the science largely doesn't exist.