

A Talk about Talks



{haroon | marco}@thinkst.com

Introduction

- Who we are
- What we do
- Why this talk ?

T+0 YEARS



Job Title: Programmer

Publications: None

Motivation: Get a job,
figure out what's going on

Hair: Brown, Sassy, Side-Part

VERACODE

T+0 YEARS

T+5 YEARS



Job Title: Hacker

Publications: Advisories,
password auditing tools, etc.

Motivation: Get in the
media as much as possible.

Hair: Unix Sysadmin

VERACODE

T+0 YEARS

T+5 YEARS

T+10 YEARS



Job Title: Security Researcher

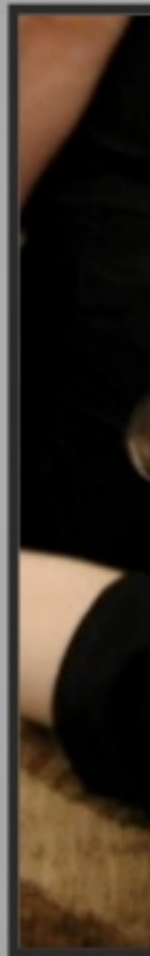
Publications: Binary analysis software

Motivation: Do something impossible

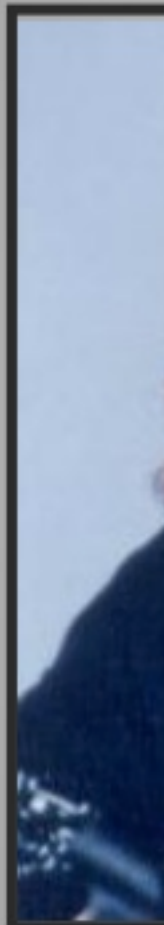
Hair: Receding Muppet Blue

VERACODE

T+0 YEARS



T+5 YEARS



T+10 YEARS



T+15 YEARS



Job Title: Chief Scientist

Publications: Mobile software analyzer, speaking, the occasional O-day

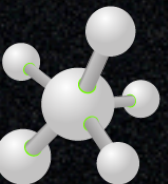
Motivation: Improve the state of the industry

Hair: Migrating to ears/nose

Improve the State of the Industry

- ITWeb Security Summit (Fig Leaf Security)
- 44Con (Penetration Testing Considered Harmful)
- Brucon (You & Your Research)

Security Conferences



Why talk about Conferences?

Why talk about Conferences?

- We thought it could be interesting

So..

We started collecting
conferences...

<http://cc.thinkst.com/>

Why talk about Conferences?

Why talk about Conferences?

- We thought it could be interesting, &

Why talk about Conferences?

- We thought it could be interesting, &
- You are (kinda) a captive audience

Why talk about Conferences?

- We thought it could be interesting, &
- You are (kinda) a captive audience
- They make an excellent proxy for the industry in general..

Why talk about Conferences?

- We thought it could be interesting, &
- You are (kinda) a captive audience
- They make an excellent proxy for the industry in general..

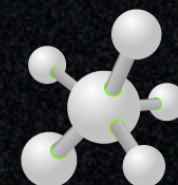
"Fig Leaf Security"

@haroonmeer - 2011



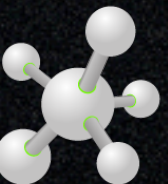
<http://thinkst.com/stuff/zacon2/itweb-2011-sb.pdf>

thinkst
applied research



"Fic

InfoSec: We Suck



"Fid

In

and it's our fault

Why talk about Conferences?

- We thought it could be interesting, &
- You are (kinda) a captive audience
- They make an excellent proxy for the industry in general..

Why talk about Conferences?

- We thought it could be interesting, &
- You are (kinda) a captive audience
- They make an excellent proxy for the industry in general..
- There are lots of complaints about them

Complaining is what we do

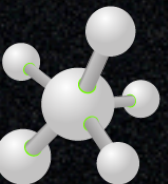
Need to distinguish:

- What needs fixing
- What needs acceptance
- What is just bike-shedding!

Stuff we won't cover

- Booth Babes
- Did X Sell-out / Jump the Shark ?
- Conference {Food;Venue;Prices}
- Conference Wifi

Start Simple..



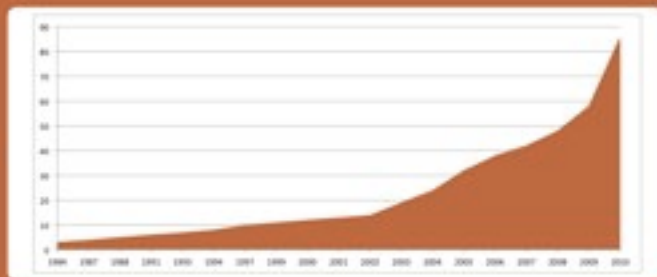
there are lots of them..

~~Setec Astronomy~~ Setec Confer Moan (yo!)



Number of Industry Related
InfoSec conferences in 1997
vs.
Number of Industry Related
Infosec conferences in 2010

Number of
Conferences
per year
(1984-2010)



The Established
Conferences keep
getting bigger...

Speakers
(BlackHat 1997)

Speakers
(BlackHat 2010)

At Least one InfoSec Conference is going on in any
given month (with 19 in October alone!)



That means an Infosec
conference is taking
place for 205/365 days
of the year

<http://blog.thinkst.com>

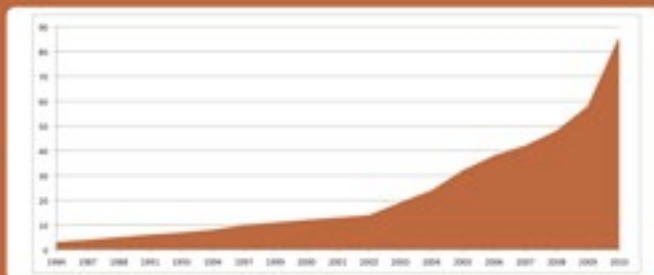
Lots & Lots of them..

~~Setec Astronomy~~ Setec Confer Moan (yo!)



Number of Industry Related
InfoSec conferences in 1997
vs.
Number of Industry Related
Infosec conferences in 2010

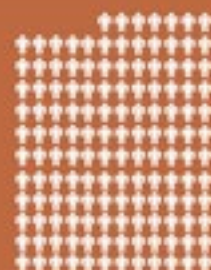
Number of
Conferences
per year
(1984-2010)



The Established
Conferences keep
getting bigger...



Speakers
(BlackHat 1997)



Speakers
(BlackHat 2010)

At Least one InfoSec Conference is going on in any
given month (with 19 in October alone!)



That means an Infosec
conference is taking
place for 205/365 days
of the year

<http://blog.thinkst.com>

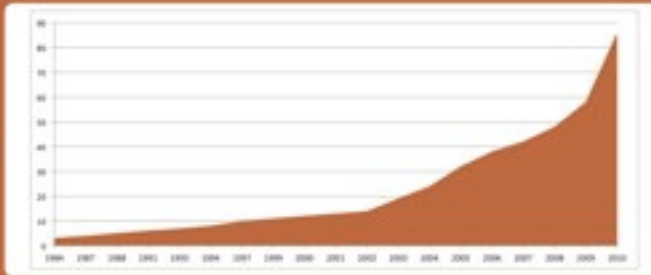


Setec Astronomy Setec Confer Moan (yo!..)

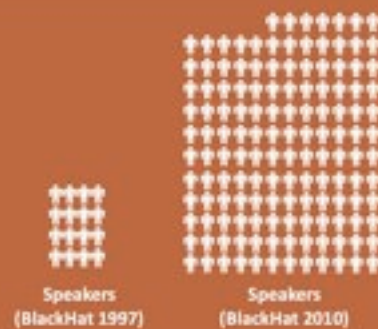


Number of Industry Related
InfoSec conferences in 1997
vs.
Number of Industry Related
Infosec conferences in 2010

Number of
Conferences
per year
(1984-2010)



The Established
Conferences keep
getting bigger...

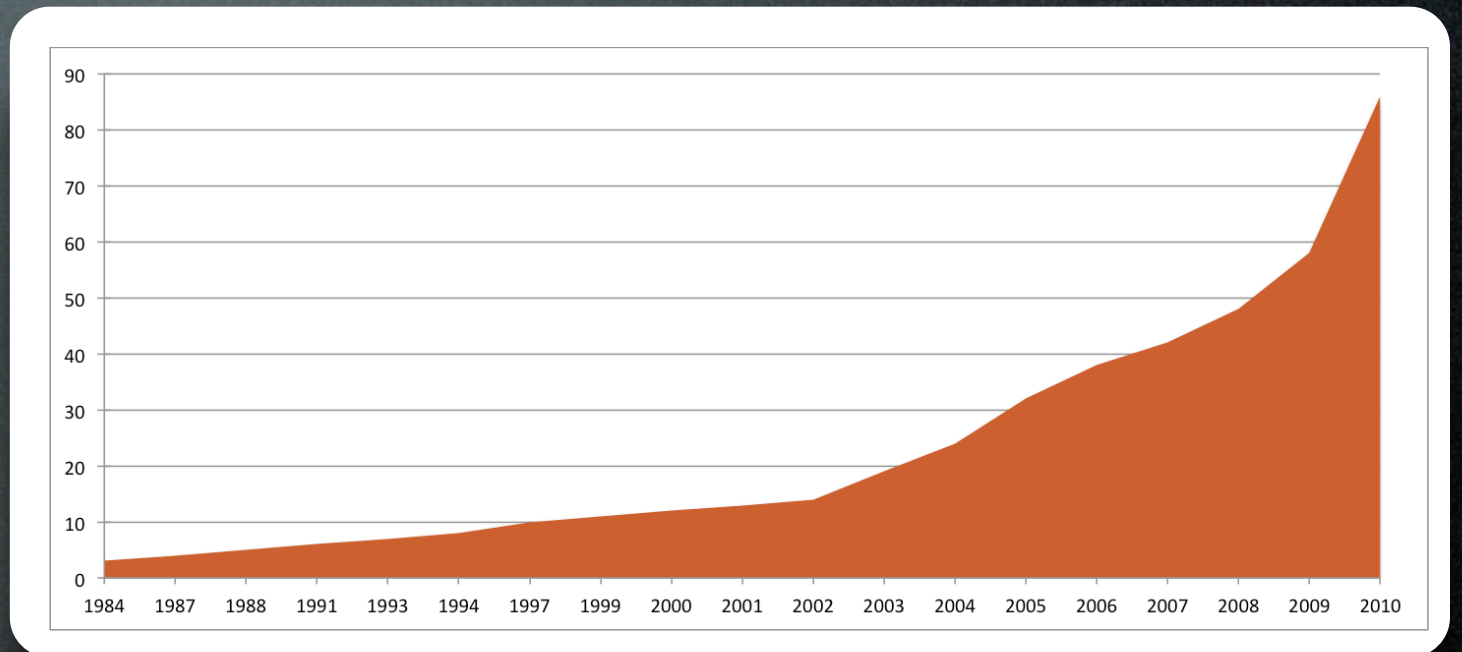


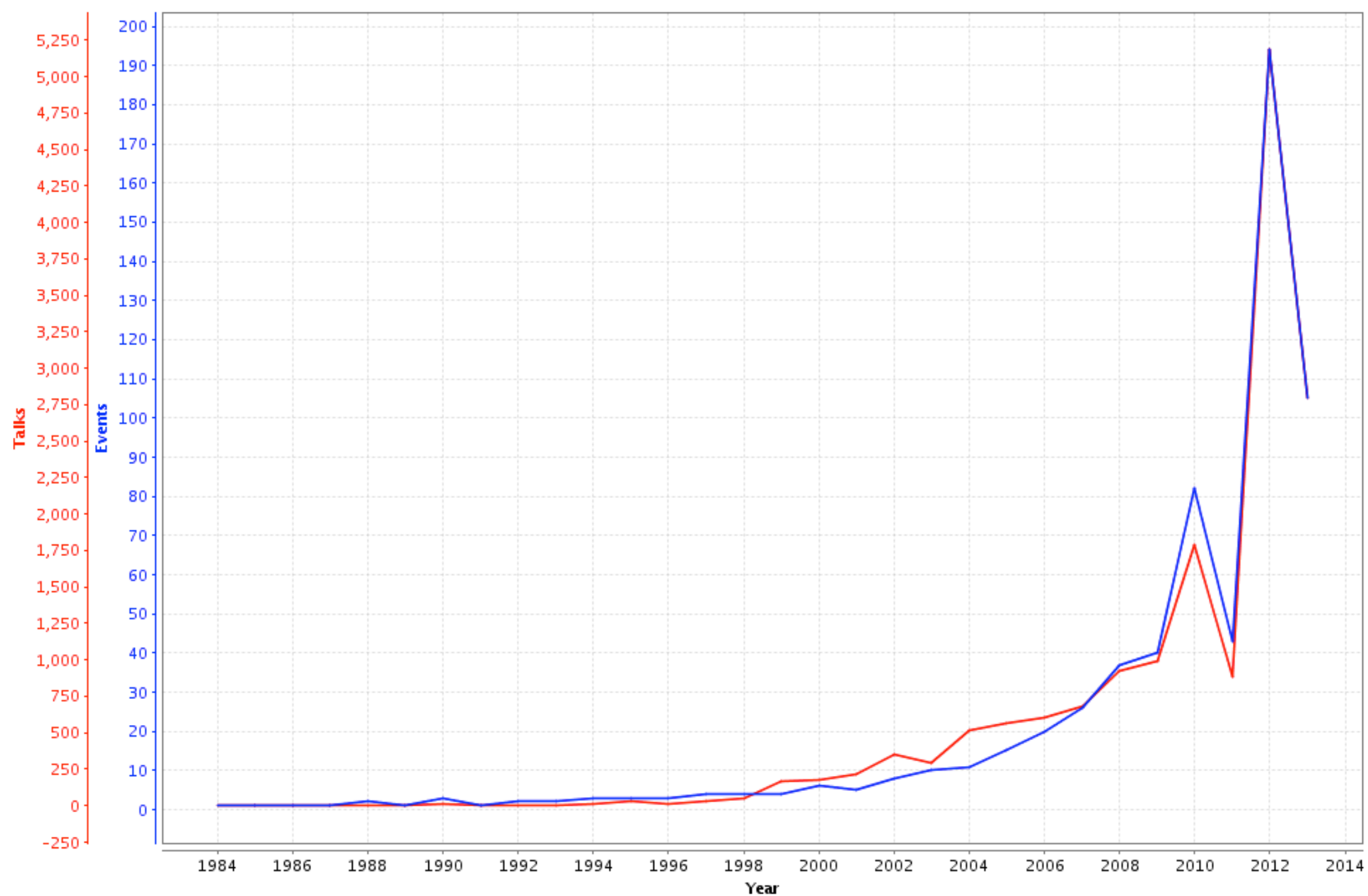
At Least one InfoSec Conference is going on in any
given month (with 19 in October alone!)



That means an infosec
conference is taking
place for 205/365 days
of the year

<http://blog.thinkst.com>



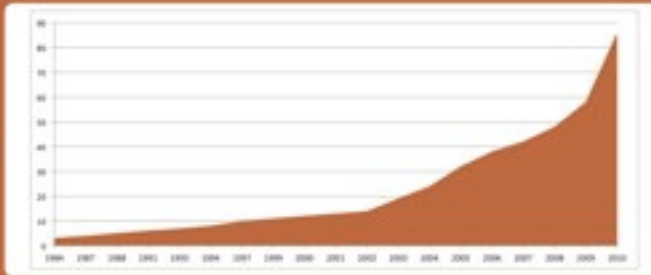


~~Setec Astronomy~~ Setec Confer Moan (yo!..)



Number of Industry Related
InfoSec conferences in 1997
vs.
Number of Industry Related
Infosec conferences in 2010

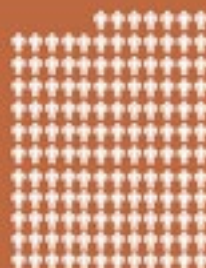
Number of
Conferences
per year
(1984-2010)



The Established
Conferences keep
getting bigger...



Speakers
(BlackHat 1997)



Speakers
(BlackHat 2010)

At Least one InfoSec Conference is going on in any
given month (with 19 in October alone!)



That means an infosec
conference is taking
place for 205/365 days
of the year

<http://blog.thinkst.com>



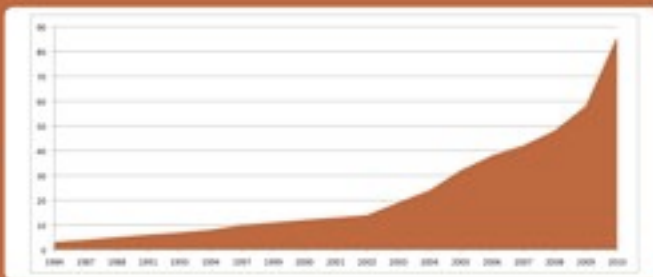
Speakers (BlackHat 1997)

~~Setec Astronomy~~
Setec Confer Moan (yo!..)

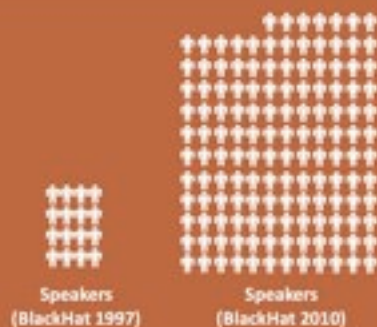


Number of Industry Related
InfoSec conferences in 1997
vs.
Number of Industry Related
Infosec conferences in 2010

Number of
Conferences
per year
(1984-2010)



The Established
Conferences keep
getting bigger...



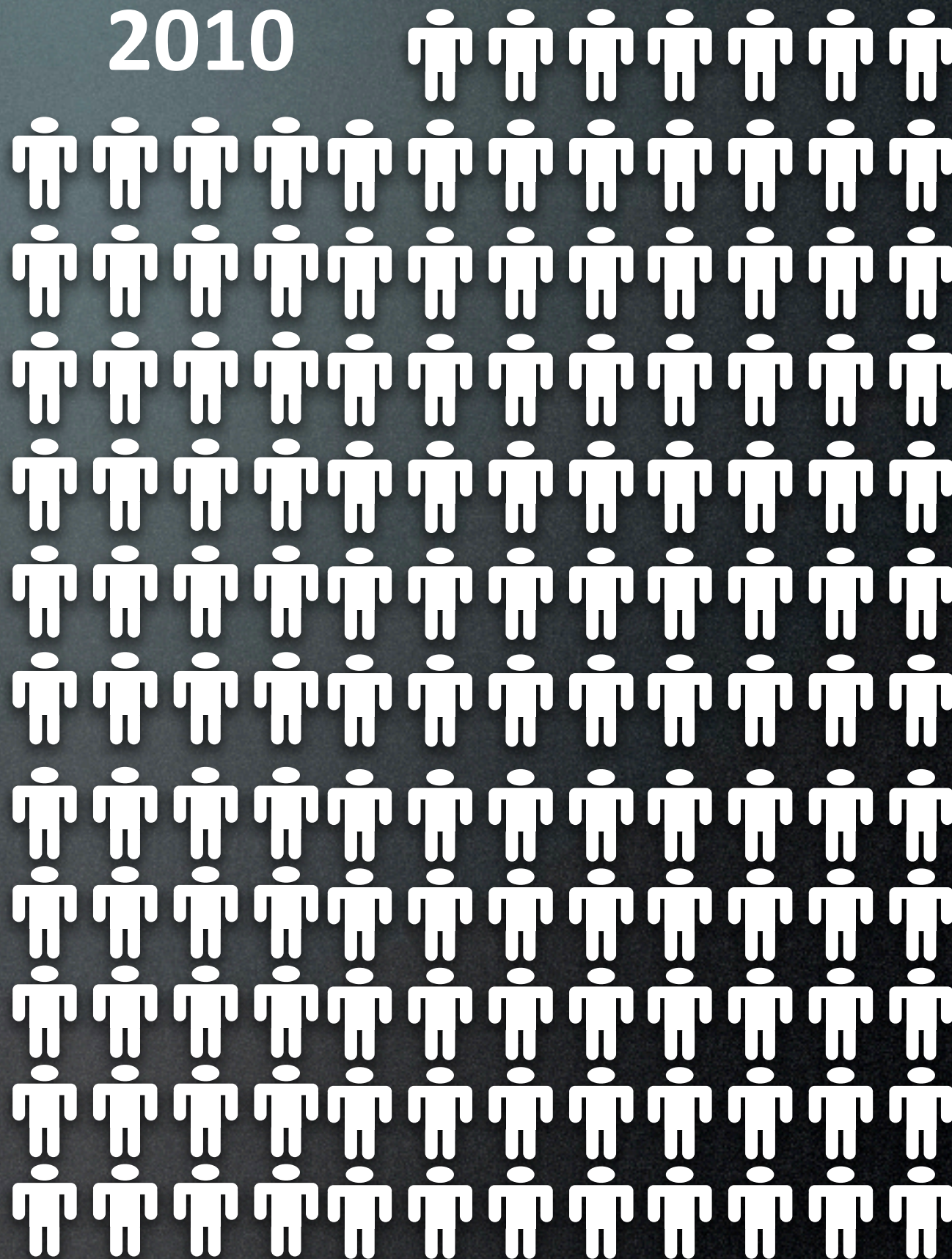
At Least one InfoSec Conference is going on in any
given month (with 19 in October alone!)



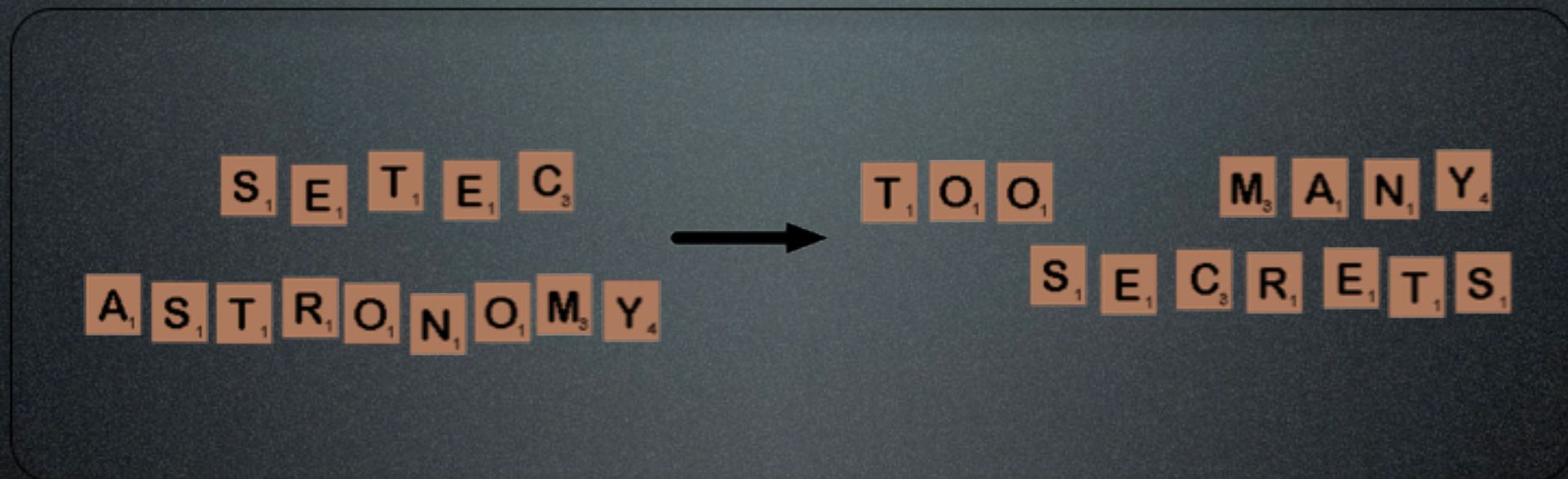
That means an infosec
conference is taking
place for 205/365 days
of the year

<http://blog.thinkst.com>

2010



Naming things is hard



Setec Confer Moan (yo!_{+n})

Too Many Conferences

Is this unique to us?

Random bits

Random thoughts about random things...by Jonathan Katz



About

Does crypto have too many conferences?

Posted by: **jonkatz** | August 7, 2009

Does crypto have too many conferences?

Posted by: **jonkatz** | August 7, 2009

<http://jonkatz.wordpress.com/2009/08/07/does-crypto-have-too-many-conferences/>

WSJ Do Doctors Attend Too Ma X

blogs.wsj.com/informedreader/2007/06/08/do-doctors-attend-too-many-conferences/

WSJ EUROPE WSJ LIVE MARKETWATCH BARRON'S ALLTHINGS DJX MORE

News, Quotes, Companies, Videos SEARCH

THE WALL STREET JOURNAL.

EUROPE EDITION Tuesday, September 10, 2013 As of 11:47 PM AST

Subscribe Log In

Home World Europe U.K. U.S. Business Markets Market Data Tech Life & Culture Opinion Heard on the Street Property

TOP STORIES IN U.S. 1 of 12 2 of 12 3 of 12

White House, Senators Weigh Syria Options

Republican Lawmakers Cool on House Spending Plan

Michigan Governor to Be Deposed in Detroit Bankruptcy Case

NRC Chief Says Yucca Mountain Review Uncertain

WSJ BLOGS

The Informed Reader

A survey of insights from media around the world.

June 8, 2007, 4:03 PM

Do Doctors Attend Too Many Conferences?

Article

THE INFORMED READER HOME PAGE »

Email Print

f t g+ in

A A

Doctors attend far too many conventions, and the constant meetings have brought a false sense of urgency to medical issues that should be dealt with in a more methodical way, writes New York physician [Kent Sepkowitz in Slate](#).

With the rare exception of true calamities such as AIDS, there is rarely enough to talk about at medical conferences, Dr. Sepkowitz says, especially now that new information can be communicated so effectively in other ways. Diseases like tuberculosis and avian flu are frightening, but other than AIDS, no infectious diseases present a "grand-scale" public-health crisis. Doctors should diagnose and manage non-crisis infections in a way that "respects the natural pace of science — its fits and starts, in which a step forward is followed by two steps back when the 'breakthrough' is reconsidered."

THE NEW NYPOST.COM

Articles Comments

<http://blogs.wsj.com/informedreader/2007/06/08/do-doctors-attend-too-many-conferences/>



Doctors attend far too many conventions, and the constant meetings have brought a false sense of urgency to medical issues that should be dealt with in a more methodical way, writes New York physician

<http://blogs.wsj.com/informedreader/2007/06/08/do-doctors-attend-too-many-conferences/>

Do we have too many philo x
www.newappsblog.com/2012/11/do-we-have-too-many-philosophy-conferences.html

New APPS: Art, Politics, Philosophy, Science

A group blog with people from all over the map.

Subscribe to this blog's feed

RECENT COMMENTS

Irem Kurtul Steen on Not Forwarding Referee Comments

NRM Rao on We need MOOTs, not MOOCs!

Bill Wringe on Not Forwarding Referee Comments

ABC on Not Forwarding Referee Comments

Bill Wringe on Not Forwarding Referee Comments

Aaron Lercher on Not Forwarding Referee Comments

ABC on Not Forwarding Referee Comments

Mark van Rooijen on Not Forwarding Referee Comments

Bill Wringe on Not Forwarding Referee Comments

adamcarter on Not Forwarding Referee Comments

ARCHIVES

September 2013

August 2013

July 2013

June 2013

May 2013

April 2013

March 2013

February 2013

January 2013

December 2012

BLOGROLL

« [14N: European Day of Action and Solidarity -- against austerity](#) | [Main](#) | [Why Husserl? Ask Gödel](#) »

14 November 2012

Do we have too many philosophy conferences?

A thought-provoking [comment](#) at Feminist Philosophers deserves discussion:

Why not kill a bunch of birds with one stone and just have fewer conferences? They're terrible for the environment and a completely decadent use of money that should be going towards financial aid for students or helping lower-income people heat their homes. Even at prestigious conferences, I find the papers are often lackluster, and at any rate, I consistently find that I could have learned just as much by staying at home, reading papers from authors' websites, and Skyping or e-mailing them.

As to the present point — a gajillion conferences all across the globe, on hyper-specialized topics, often by invitation, with sketchy review procedures when not, and the prospect of being the only woman at quasi-party full of dudes in a faraway land — of COURSE you're going to get gender disparities. So yay to the [GCC](#), but I'd like to see an Anti-Conference Campaign (ACC) as well!

Posted by [John Protevi](#) on 14 November 2012 at 14:28 in [Improving the philosophy profession](#), [Political Economy of higher education](#) | [Permalink](#)

Reblog (0)
 Digg This
 Save to del.icio.us
 Tweet

TrackBack

TrackBack URL for this entry:

<http://www.typepad.com/services/trackback/6a00d8341ef41d53ef017c337b6864970b>

Listed below are links to weblogs that reference [Do we have too many philosophy conferences?](#):

Comments

1

Helen De Cruz said...

I don't think this is a bad idea. I love conferences, and love to learn about things I would normally not learn about, but I also realize that they unfairly advantage people with (1) a large travel credit, who are typically (2) from more prestigious, richer universities, and who are also typically (3) from better networks, which help them get invited as plenary speakers, commentators etc.

[Reply](#)
14 November 2012 at 14:36

MORE

Authors

Comments Policy

Signatories to the petition in support of the Gendered Conference Campaign (22 Sept 2012; 835 names)

RECENT POSTS

Not Forwarding Referee Comments

Courtney Love - Pacific Coast Highway

Precarious HE labor and health care

Endangered Orcas and the Concept of "Population"

guest starring SIR STEWART WALLACE as HIMSELF

Sports fandom as a practice of subjectivation

Lefty Prof Cites Goldwater Institute in Blog Link Shocker!

Brazilian music on Fridays: Repentistas

Further thoughts on reductio proofs

Open Syllabus Project

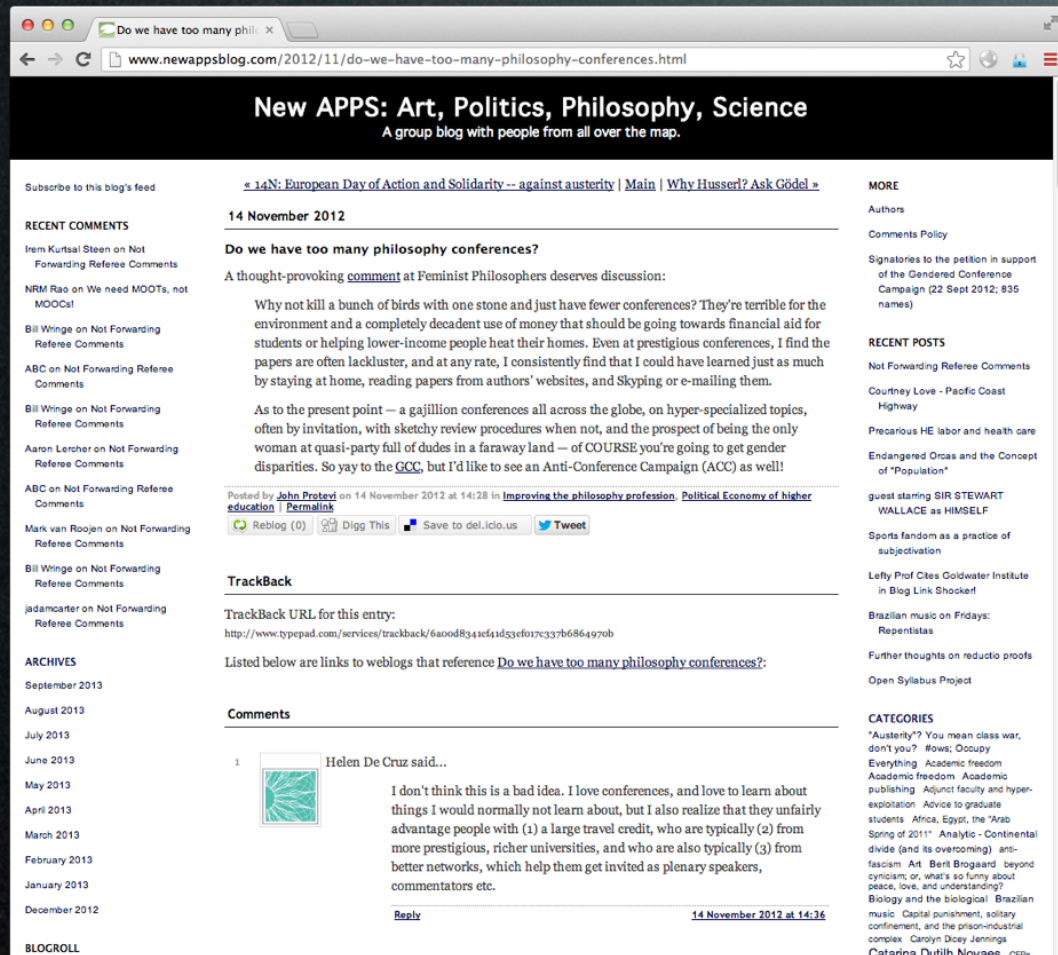
CATEGORIES

"Austerity"? You mean class war, don't you? #ows; Occupy

Everything Academic freedom

Academic freedom Academic publishing Adjunct faculty and hyper-exploitation Advice to graduate students Africa, Egypt, the "Arab Spring of 2011" Analytic - Continental divide (and its overcoming) anti-fascism Art Berit Brogaard beyond cynicism; or, what's so funny about peace, love, and understanding? Biology and the biological Brazilian music Capital punishment, solitary confinement, and the prison-industrial complex Carolyn Dicey Jennings Catarina Dutilh Novaes CFPs,

<http://www.newappsblog.com/2012/11/do-we-have-too-many-philosophy-conferences.html>



— a gajillion conferences all across the globe,
on hyper-specialized topics, often by
invitation, with sketchy review procedures
when not, and the prospect of being the only
woman at quasi-party full of dudes in a
faraway land

STATE OF CONS

- TOO MANY CONS
- TOO FEW GOOD SPEAKERS
- TOO MANY REPEAT PRESENTATIONS



These factors bring down the quality of
all conferences

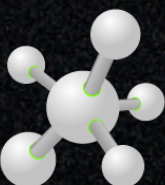
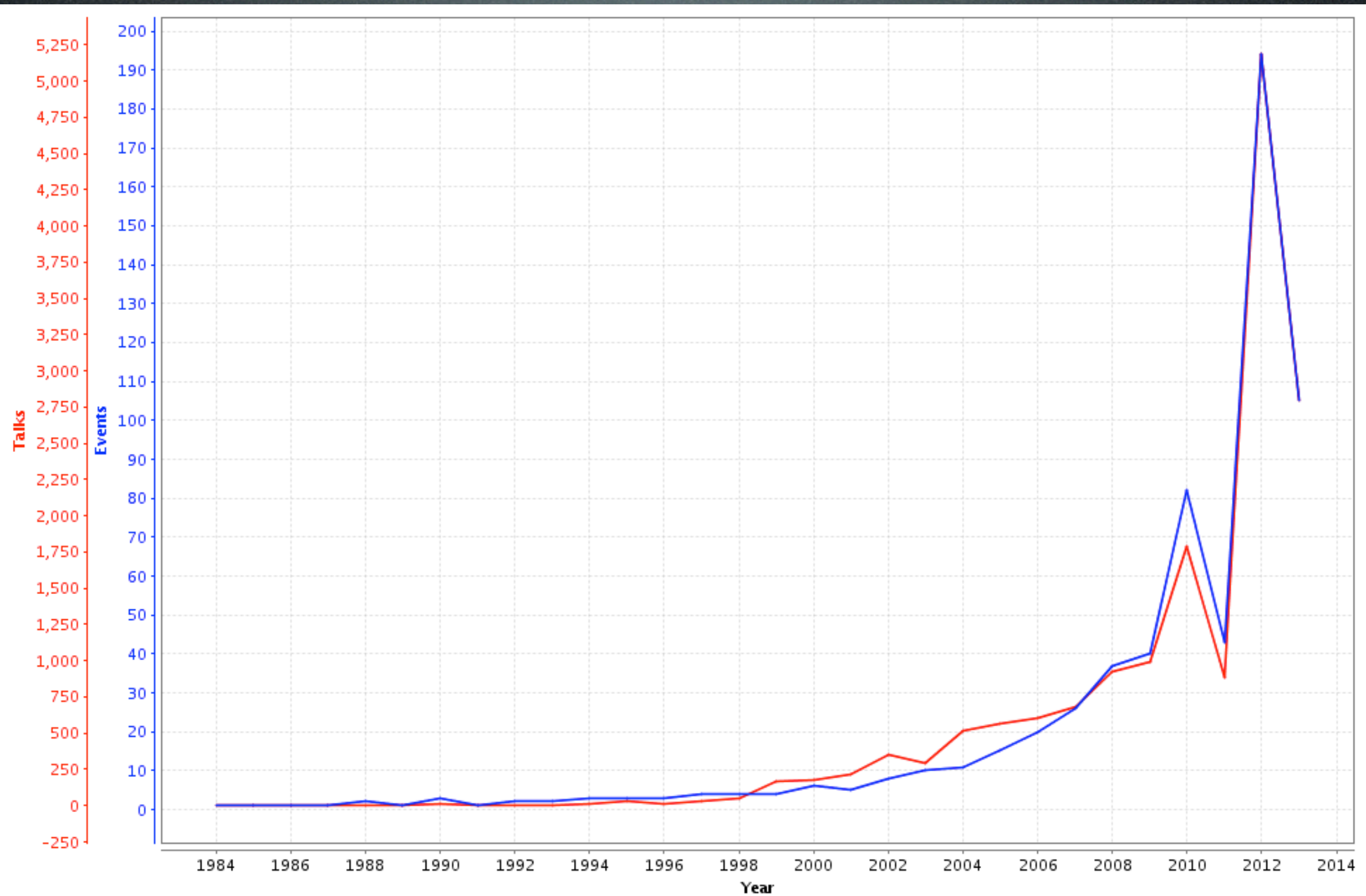
Is it true ?

repeat presentations

- 1998 - 2%
- 1998 - 2007 - $6\% < x < 13\%$
- 2007 - 2013 - $\sim 10\%$

actually a conference
organizer problem

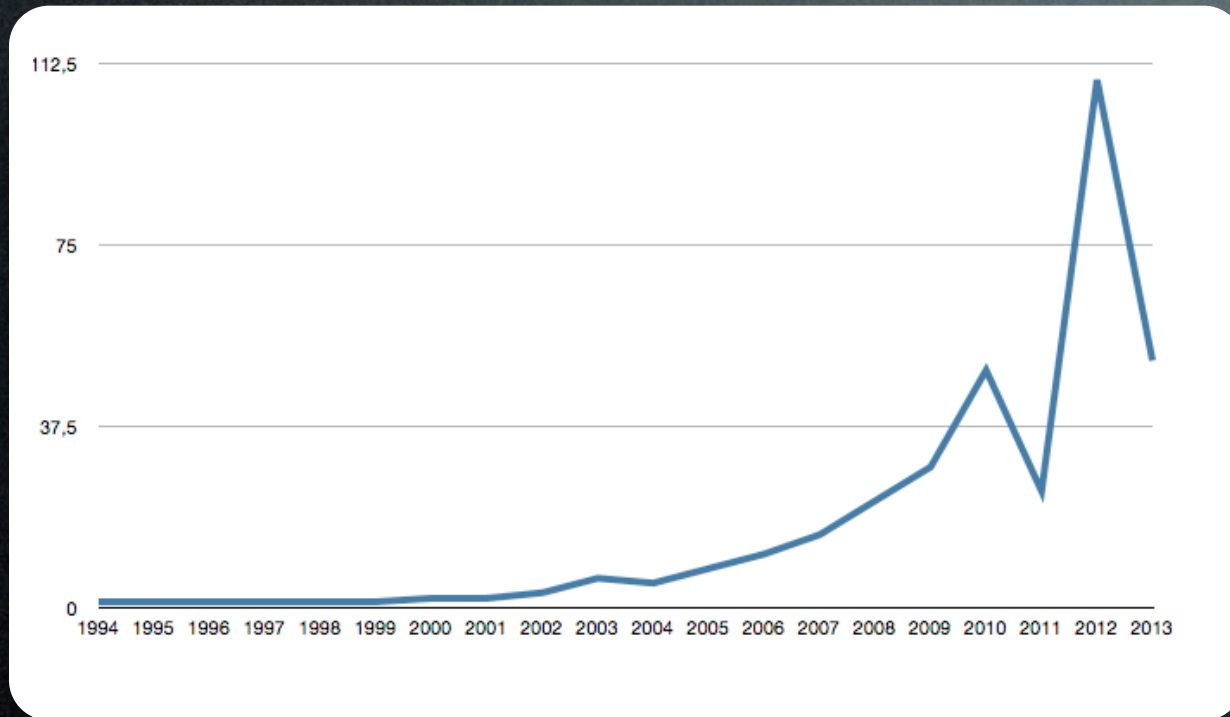
Growth



Why the crazy increase?

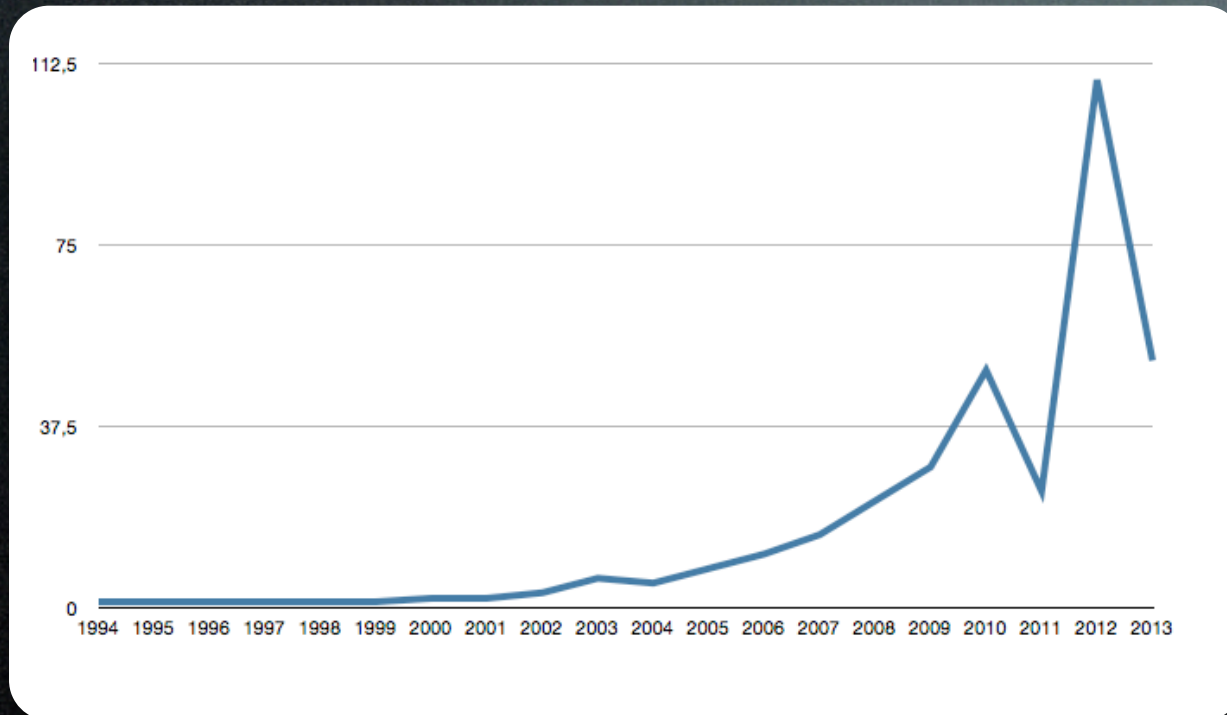
Industry Growth

Globalization

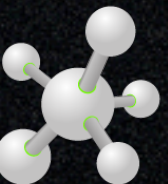


Non-USA Talks

Globalization



Non-USA Talks



The birth of smaller cons

Positive

- Cons without flight / accom charges
- More opportunities for up & comers
- SVC

Positive

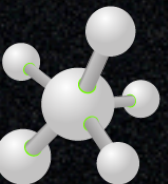
- Cons without flight / accom charges
- More opportunities for up & comers
- SVC

Positive

- Cons without flight / accom charges
- More opportunities for up & comers
- SVC



Negative



Negative

- Signal to Noise Ratio drops

Negative

- Signal to Noise Ratio drops
- “Conference Speaker” as a high quality marker

Why are so many people
running conferences?

Why are so many people running conferences?

- Many noble reasons..
- Money
- Influence

Is it Profitable ?

Is it Profitable ?



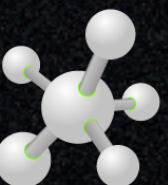
thomas lim @thomas_coseinc

7 Aug

..... - BH is
for the community. then why charge so much and profit so much?

 Retweeted by Ben Nagy

[Expand](#)



But lots of conferences
are not for profit

Why are so many people running conferences?

- Many noble reasons..
- Money
- Influence

[Dailydave] Paid-for Vendor talk seems legit?

Moxie Marlinspike [moxie at thoughtcrime.org](mailto:moxie@thoughtcrime.org)

Thu Mar 22 17:20:08 EDT 2012

> On 21.3.2012 15:26, Dave Aitel wrote:
>> Why is it that every conference has gone the full hog and decided
>> that you must sell keynotes?

As odious as paid keynotes might be, I wonder if this is just a more direct representation of how all conferences work. Running a security conference comes with a certain amount of power; even if they're not paid, the ability to choose which submitted talks will be given allows the organizers to define the narrative for what people think is happening and what's important.

Paid keynotes exemplify an obvious microcosm of how this can play out. Even when there are no paid keynotes, however, most security conferences today are put together by organizations or individuals who have a business stake in the security industry. So while Immunity might not accept paid keynotes, it should be no surprise that the types of talks at Infiltrate are what they are. That is to say, Infiltrate doesn't need to accept paid keynotes, because the unpaid talks are already selected to contribute to Immunity's business.

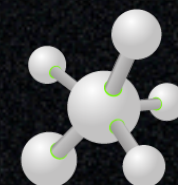
I fully believe that, within the context that Immunity has identified as contributing to its success, they will select talks based on technical content, speaking ability, and prevalence of buffy quotes. But while BHEU had a 30 minute commercial for Fortigate, let's not forget that Infiltrate is in some sense one really big commercial for Immunity.

This isn't to say that I dislike watching the Immunity commercial, or that I don't appreciate its subtlety, but I think we should be wary of suggesting that these things are somehow "vendor neutral" or devoid of vendor influence when the organizers themselves are very often vendors and yield considerably more influence than a single paid talk ever could.

- moxie

--

<http://www.thoughtcrime.org>



[Dailydave] Paid-for Vendor talk seems legit?

Moxie Marlinspike [moxie at thoughtcrime.org](mailto:moxie@thoughtcrime.org)

Thu Mar 22 17:20:08 EDT 2012

> On 21.3.2012 15:26, Dave Aitel wrote:
>> Why is it that every conference has gone the full hog and decided
>> that you must sell keynotes?

As odious as paid keynotes might be, I wonder if this is just a more direct representation of how all conferences work. Running a security conference comes with a certain amount of power; even if they're not paid, the ability to choose which submitted talks will be given allows the organizers to define the narrative for what people think is happening and what's important.

Paid keynotes exemplify an obvious microcosm of how this can play out. Even when there are no paid keynotes, however, most security conferences today are put together by organizations or individuals who have a business stake in the security industry. So while Immunity might not accept paid keynotes, it should be no surprise that the types of talks at Infiltrate are what they are. That is to say, Infiltrate doesn't need to accept paid keynotes, because the unpaid talks are already selected to contribute to Immunity's business.

I fully believe that, within the context that Immunity has identified as contributing to its success, they will select talks based on technical content, speaking ability, and prevalence of buffy quotes. But while BHEU had a 30 minute commercial for Fortigate, let's not forget that Infiltrate is in some sense one really big commercial for Immunity.

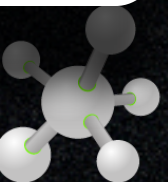
This isn't to say that I dislike watching the Immunity commercial, or that I don't appreciate its subtlety, but I think we should be wary of suggesting that these things are somehow "vendor neutral" or devoid of vendor influence when the organizers themselves are very often vendors and yield considerably more influence than a single paid talk ever could.

- moxie

--

<http://www.thoughtcrime.org>

Running a security conference comes with a certain amount of power; even if they're not paid, the ability to choose which submitted talks will be given allows the organizers to define the narrative for what people think is happening and what's important.



[Dailydave] Paid-for Vendor talk seems legit?

Moxie Marlinspike moxie@thoughtcrime.org

Thu Mar 22 17:20:08 EDT 2012

> On 21.3.2012 15:26, Dave Aitel wrote:
>> Why is it that every conference has gone the full hog and decided
>> that you must sell keynotes?

As odious as paid keynotes might be, I wonder if this is just a more direct representation of how all conferences work. Running a security conference comes with a certain amount of power; even if they're not paid, the ability to choose which submitted talks will be given allows the organizers to define the narrative for what people think is happening and what's important.

Paid keynotes exemplify an obvious microcosm of how this can play out. Even when there are no paid keynotes, however, most security conferences today are put together by organizations or individuals who have a business stake in the security industry. So while Immunity might not accept paid keynotes, it should be no surprise that the types of talks at Infiltrate are what they are. That is to say, Infiltrate doesn't need to accept paid keynotes, because the unpaid talks are already selected to contribute to Immunity's business.

I fully believe that, within the context that Immunity has identified as contributing to its success, they will select talks based on technical content, speaking ability, and prevalence of buffy quotes. But while BHEU had a 30 minute commercial for Fortigate, let's not forget that Infiltrate is in some sense one really big commercial for Immunity.

This isn't to say that I dislike watching the Immunity commercial, or that I don't appreciate its subtlety, but I think we should be wary of suggesting that these things are somehow "vendor neutral" or devoid of vendor influence when the organizers themselves are very often vendors and yield considerably more influence than a single paid talk ever could.

- moxie

--
<http://www.thoughtcrime.org>

So while Immunity might not accept paid keynotes, it should be no surprise that the types of talks at Infiltrate are what they are. That is to say, Infiltrate doesn't need to accept paid keynotes, because the unpaid talks are already selected to contribute to Immunity's business.

[Dailydave] Paid-for Vendor talk seems legit?

Moxie Marlinspike [moxie at thoughtcrime.org](mailto:moxie@thoughtcrime.org)
Thu Mar 22 17:20:08 EDT 2012

> On 21.3.2012 15:26, Dave Aitel wrote:
>> Why is it that every conference has gone the full hog and decided
>> that you must sell keynotes?

As odious as paid keynotes might be, I wonder if this is just a more direct representation of how all conferences work. Running a security conference comes with a certain amount of power; even if they're not paid, the ability to choose which submitted talks will be given allows the organizers to define the narrative for what people think is happening and what's important.

Paid keynotes exemplify an obvious microcosm of how this can play out. Even when there are no paid keynotes, however, most security conferences today are put together by organizations or individuals who have a business stake in the security industry. So while Immunity might not accept paid keynotes, it should be no surprise that the types of talks at Infiltrate are what they are. That is to say, Infiltrate doesn't need to accept paid keynotes, because the unpaid talks are already selected to contribute to Immunity's business.

I fully believe that, within the context that Immunity has identified as contributing to its success, they will select talks based on technical content, speaking ability, and prevalence of buffy quotes. But while BHEU had a 30 minute commercial for Fortigate, let's not forget that Infiltrate is in some sense one really big commercial for Immunity.

This isn't to say that I dislike watching the Immunity commercial, or that I don't appreciate its subtlety, but I think we should be wary of suggesting that these things are somehow "vendor neutral" or devoid of vendor influence when the organizers themselves are very often vendors and yield considerably more influence than a single paid talk ever could.

- moxie

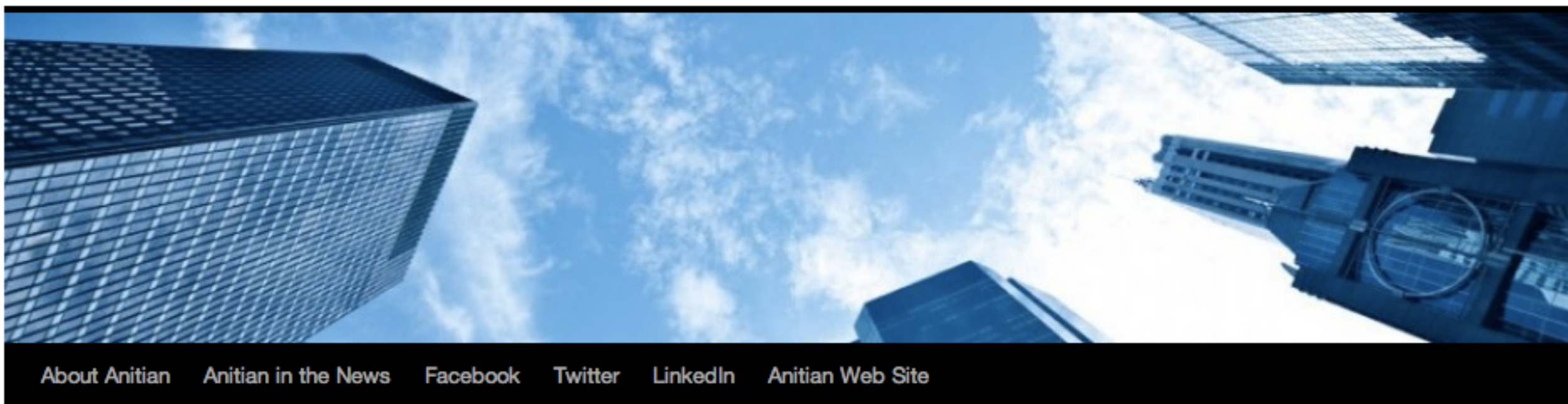
--
<http://www.thoughtcrime.org>

..while BHEU had a 30 minute commercial for Fortigate, let's not forget that Infiltrate is in some sense one really big commercial for Immunity.

...the organizers themselves are very often vendors and yield considerably more influence than a single paid talk ever could.

Conference organizers
have a different set of
incentives to
researchers

Offense vs Defense Bias



[About Anitian](#) [Anitian in the News](#) [Facebook](#) [Twitter](#) [LinkedIn](#) [Anitian Web Site](#)

Deprecated Defense – The Diminishing Value of the Big Security Conferences

Posted on [March 19, 2013](#) by [Andrew Plato](#)

Reflecting upon RSA2013, there is a lingering wanting. Like a meal that fills you up, but leaves you unsatisfied. There is a quiet battle being waged at the big security conferences like RSA, BlackHat, Defcon and such. This is not a battle of exploits or force, but one of attention. It is the battle to dismiss defense as irrelevant.

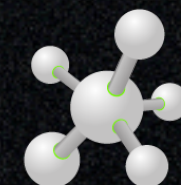
Top Posts & Pages

- [The Cult of Palo Alto Networks](#)
- [UTM v NGFW - A Single Shade of Gray](#)
- [PCI: I Find Your Lack of Scope Disturbing](#)

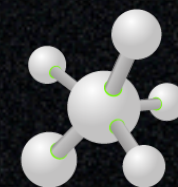
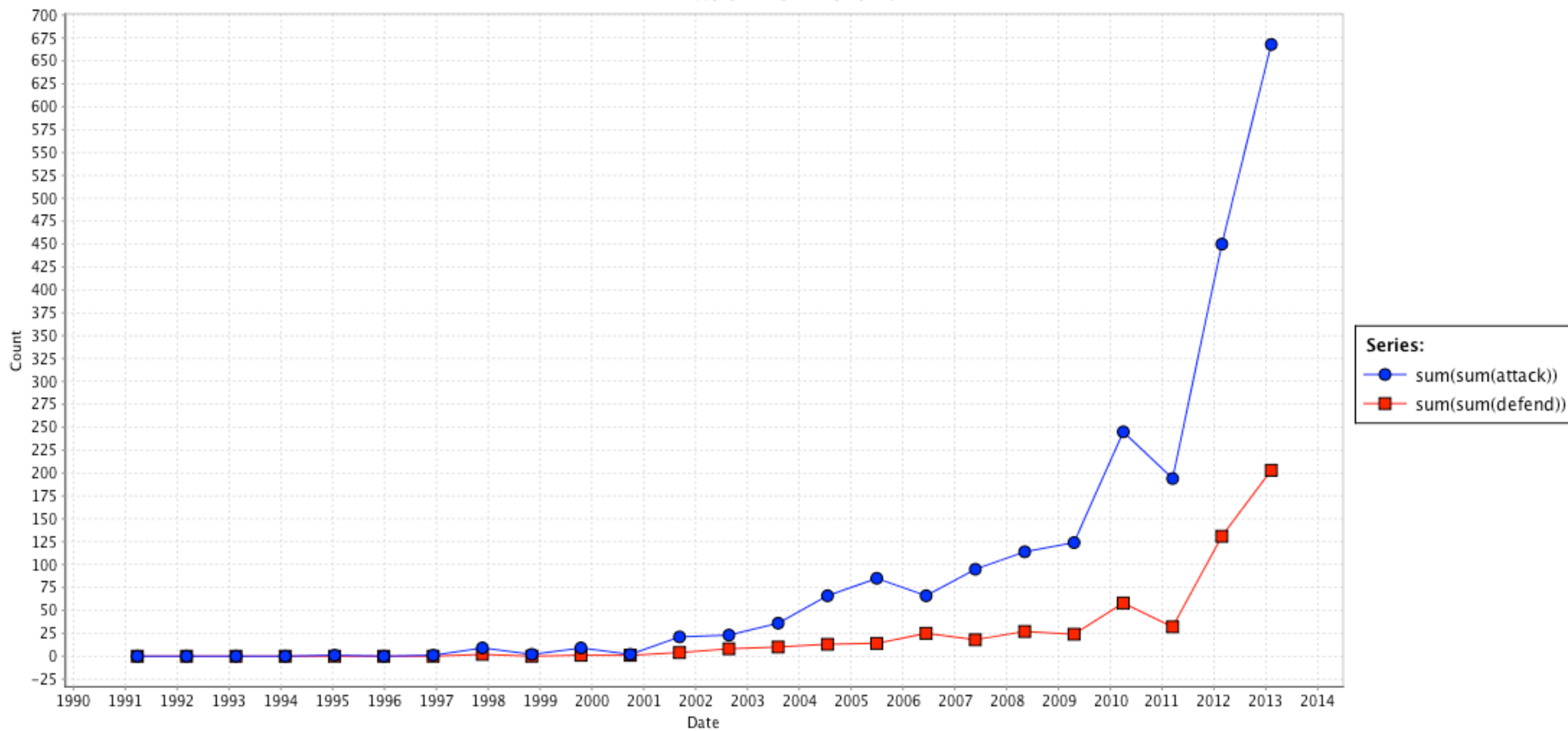
Recent Posts

- [How to Get a Meaningful Security Assessment](#)

<http://blog.anitian.com/deprecated-defense-the-diminishing-value-of-the-big-security-conferences/>



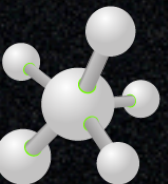
Attack vs. Defend



Why ?

Offense is Sexy?

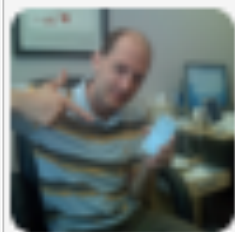
because, Economics..



Broken Review Panels!

Every year there are
some complaints

Some years more than
others



Charlie Miller @0xcharlie

30 May

Dam, me and @nudehaberdasher's excellent car hacking talk got rejected from blackhat youtube.com/watch?v=ws8lSo... Needed more cyber-APT presumably

 [View media](#)

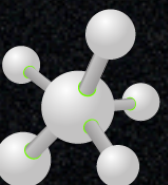
 [Reply](#)

 [Retweet](#)

 [Favorite](#)

 [More](#)

Some years more than
others

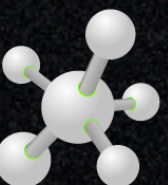


Hmm @ seeing #BlackHat and #Defcon talks with less content than my rejected abstract.

Expand

← Reply ↕ Retweet ★ Favorite ... More

Some years more than
others



Some mistakes are more
visible than others



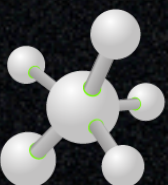
Ben Nagy @rantyben

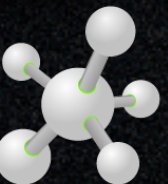
30 May

The level of head-in-assery that would lead to a con "committee" passing on @0xcharlie and @nudehaberdasher HACKING CARS defies physics.

Expand

← Reply ↕ Retweet ★ Favorite ... More







BBC

News Sport Weather Capital Culture Auto

NEWS TECHNOLOGY

Home UK Africa Asia Europe Latin America Mid-East US & Canada Business Health Sci/Envir

25 July 2013 Last updated at 23:04 GMT

Share f t e

Car hackers use laptop to control standard car

By Zoe Kleinman
Technology reporter, BBC News



IOACTIVE

The researchers managed to stop, start and steer a car with an old Nintendo handset


Next time you have a passenger in the back seat of your car offering infuriatingly "helpful" advice about your driving skills, count yourself lucky that they aren't doing anything more sinister in their attempts to guide your vehicle.

Related Stories

Car control systems 'vulnerable'

charlie miller chris valasek x

← → ↺ <https://www.google.co.za/search?q=charlie+miller+chris+valasek&source=Inms...> ☆ 🔒 ☰



[Hackers crack car systems wide open](#)

[Independent Online](#) - 04 Sep 2013


Charlie Miller, a security engineer for Twitter, and fellow hacker **Chris Valasek** said: "We could control steering, braking, acceleration to a ..."

[+ Show more](#)

[Duo hacks cars with '80s Nintendo controller](#)

[Vancouver Sun](#) - 03 Sep 2013


In front of a room of some of the brightest hackers on the planet, security researchers **Charlie Miller** and **Chris Valasek** will show the world how ...



[How Hackers Can Grab Your Car](#)

[ABC News](#) - by [Adam Levin](#) - 31 Aug 2013


... the brakes, which caused researcher **Charlie Miller** to drive the SUV ... convention for hackers, Miller and his co-researcher **Chris Valasek** ...



[Scientist BANNED from revealing secret codes used to start luxury ...](#)

[Birmingham Mail](#) - 31 Aug 2013

Charlie Miller, a security engineer at Twitter, and **Chris Valasek**, the Director of Security Intelligence at IOActive, had received an 80,000 dollar ...



[Taking over cars, and homes, remotely](#)

[NDTV](#) - 12 Aug 2013

Charlie Miller, a security researcher at Twitter, and **Chris Valasek**, director of security intelligence at IOActive, a security research company, ...

[+ Show more](#)

[The Car Hacks That Could Cost You Big Time](#)

[Huffington Post](#) - by [Adam Levin](#) - 29 Aug 2013

... the brakes, which caused researcher **Charlie Miller** to drive the SUV ... convention for hackers, Miller and his co-researcher **Chris Valasek** ...

Capital Culture Auto

Business Health Sci/Envir

Share f t e p

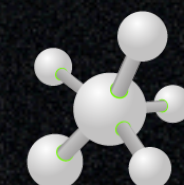
standard

ACTIVE

set

Related Stories

[Car control systems 'vulnerable'](#)



How should acceptance
be done ?



Andrew @no_structure

2 Aug

@0xabad1dea @aaronportnoy you know what's hilarious? how security cons don't do blind review

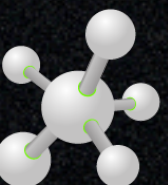
 [View conversation](#)

 [Reply](#)

 [Retweet](#)

 [Favorite](#)

 [More](#)





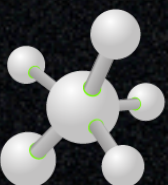
sergey bratus @sergeybratus

3 Aug

@haroonmeer @no_structure @aaronportnoy Review by specialists is hardly ever blind: even if name's removed, school of origin is often clear.

[Expand](#)

[← Reply](#) [↕ Retweet](#) [★ Favorite](#) [⋮ More](#)





Ben Nagy @rantyben

3 Aug

You guys run a blind review where selectors don't know the speakers. I'll do one where I don't read the submissions. See who sells more tix.

[Collapse](#)

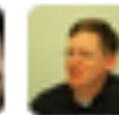
[← Reply](#) [↕ Retweet](#) [★ Favorite](#) [... More](#)

10

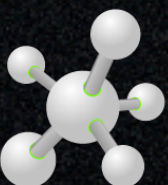
RETWEETS

2

FAVORITES



2:10 AM - 3 Aug 13 · [Details](#)





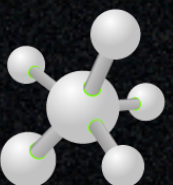
Nico Waisman @nicowaisman

3 Aug

The best cfp review should be a 15m webex with a 5m q&a after.

[Expand](#)

[← Reply](#) [↕ Retweet](#) [★ Favorite](#) [⋮ More](#)

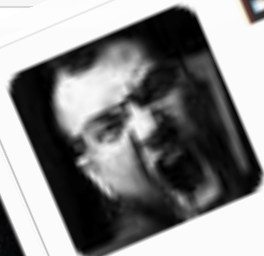




Nico Waisman @nicowaisman

The best cfp re

Expand



Ben Nagy @rantyben

@nicowaisman BH had like 800 submissions ;)

Hide conversation

2:26 AM - 3 Aug 13 · Details

Reply

Retweet

Favorite

More

3 Aug

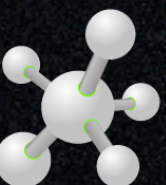
in a 5m q&a after.

Retweet

Favorite

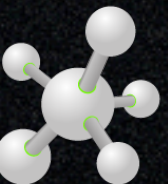
More

3 Aug



Economics (again)

Rock-Star Speakers



Stunt Hacking

Michal Zalewski [lcamtuf at coredump.cx](mailto:lcamtuf@coredump.cx)

Thu Mar 22 21:48:11 EDT 2012

- Previous message: [\[Dailydave\] Paid-for Vendor talk seems legit?](#)
- Next message: [\[Dailydave\] Paid-for Vendor talk seems legit?](#)
- Messages sorted by: [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#)

Researchers have no intrinsic, "noble" reason to present their findings at a conference. They withhold interesting findings for months, and travel to a distant location, to do a slideshow in front of several hundred people. Hoping to capitalize on the profile of the event, and the PR attention that comes with it, is a huge part of the incentive. Events such as Pwn2own are the pinnacle of this trend.

Organizers... well, they often start for noble reasons, but are subject to perverse incentives: conferences don't get successful and profitable unless you allow the merits of the content to take a back seat. You need to seek presenters who are known to the journalists, and offer them high five-figure compensation for even the most trivial talks and keynotes.

Vendors treat the conferences as trade shows (fair enough), or more insidiously, hope to befriend researchers and strategically score brownie points in ways that have no objective merits. They throw lavish "invitation-only" vendor parties (complete with escorts / strippers), or have entire teams seemingly dedicated to just shaking hands, taking photos with researchers, and blogging about how much they like responsible disclosure.

I don't think it's necessarily a bad thing, but I also think there's no point in getting too worked up about paid keynotes. There are more troubling trends.

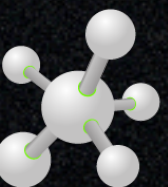
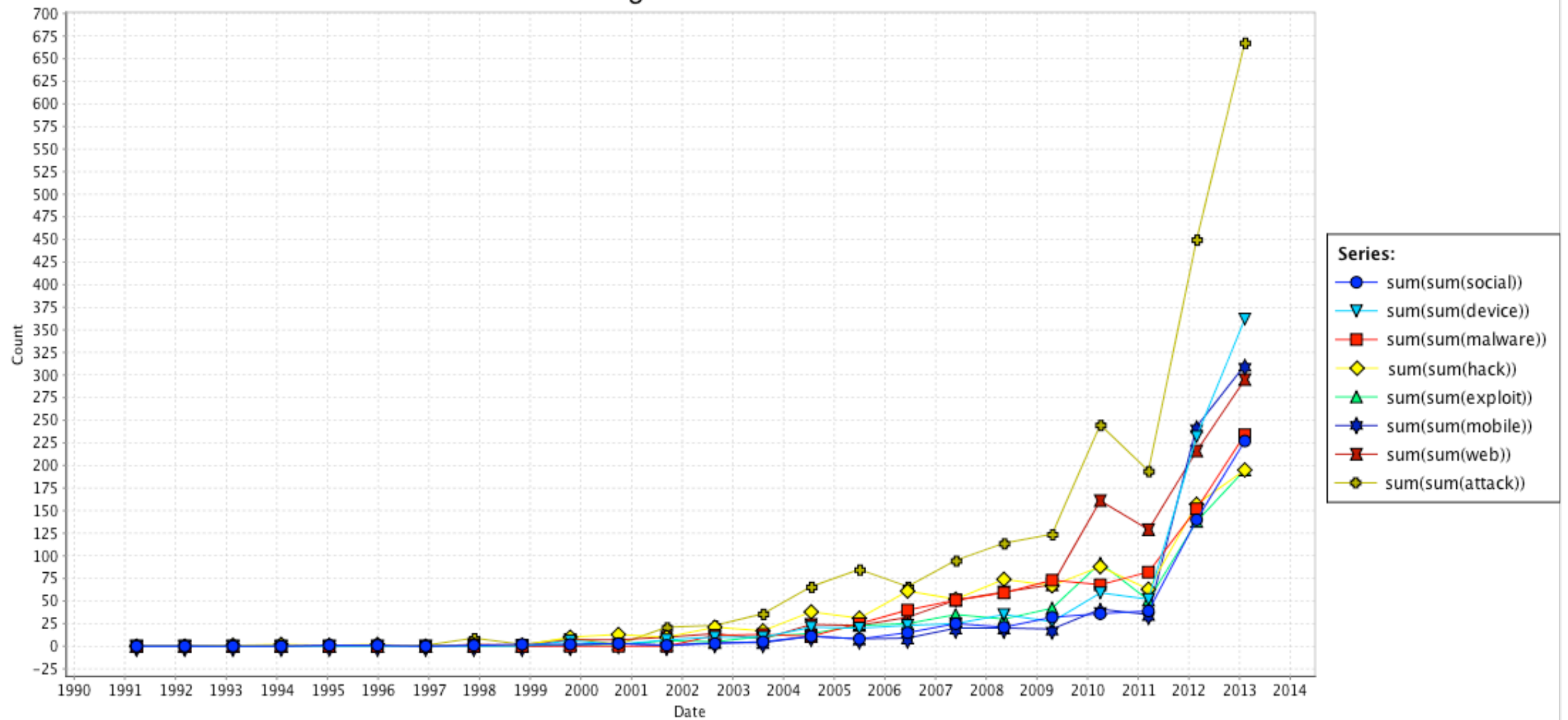
/mz

Understand what they are

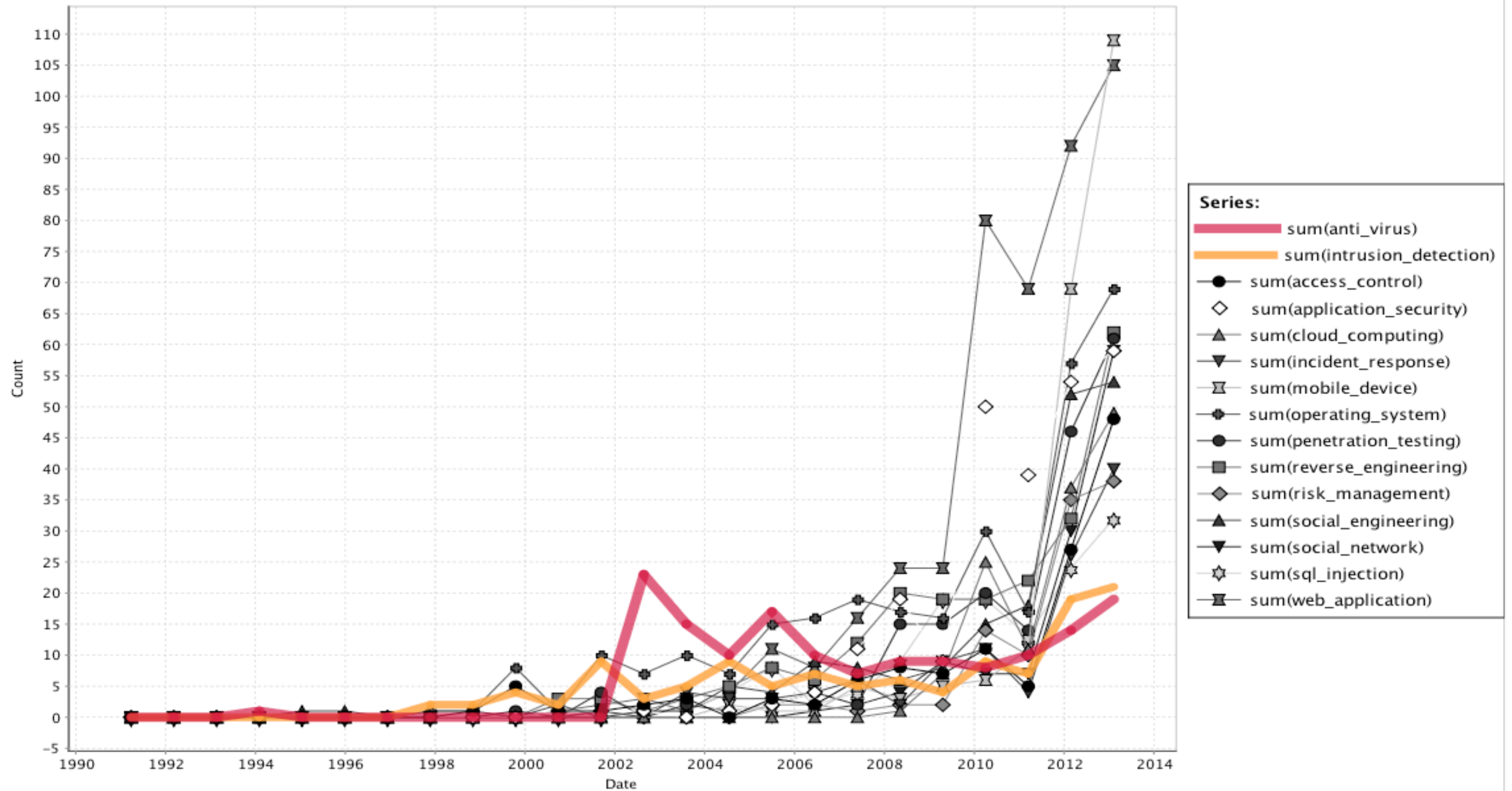
It's might be ok, as long as we still cover the
right topics,
and we are still learning..

Are we aiming at the
right topics?

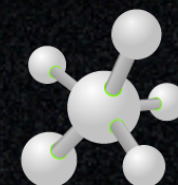
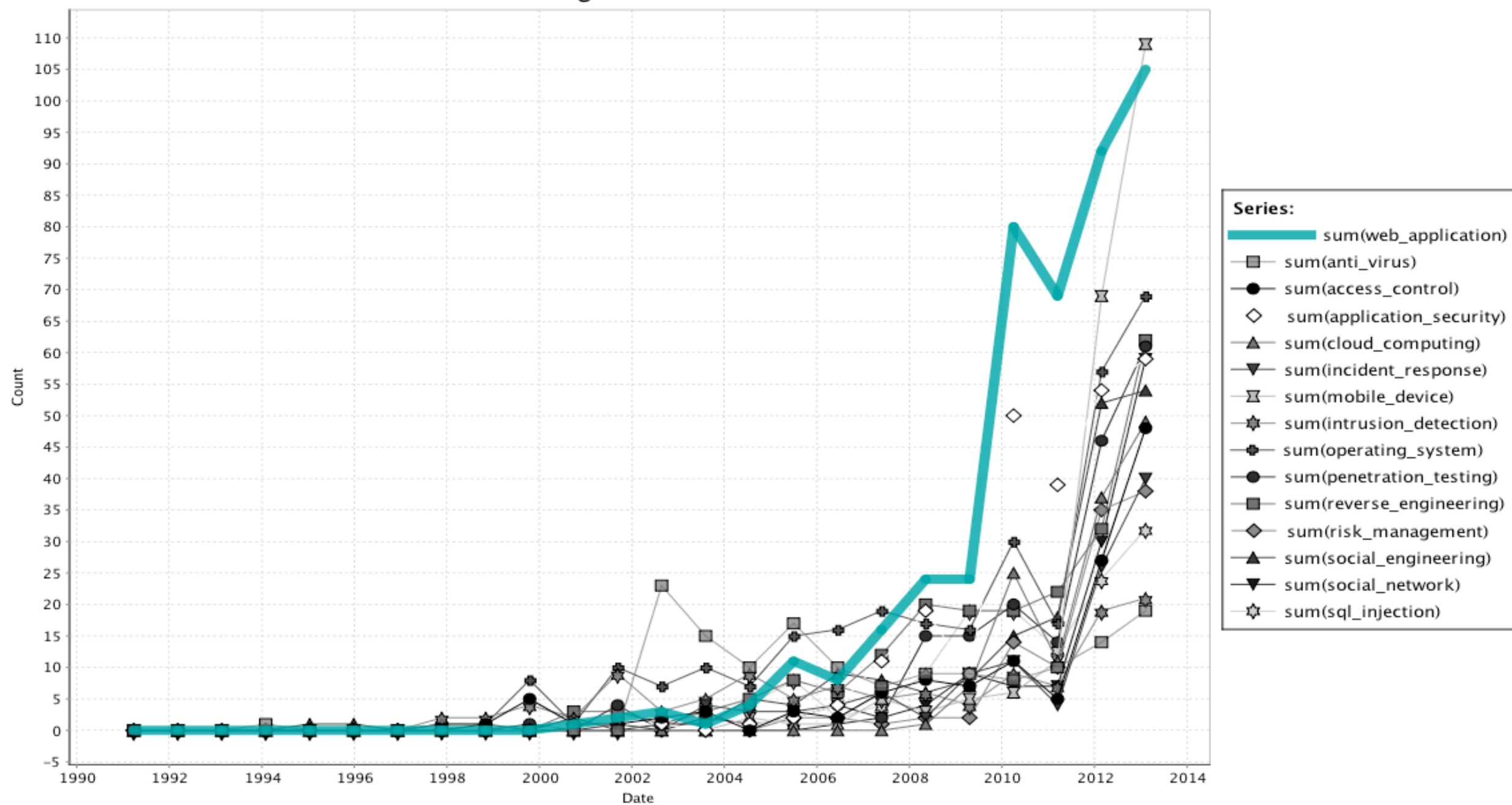
1-gram Abstracts and Titles



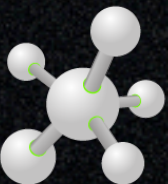
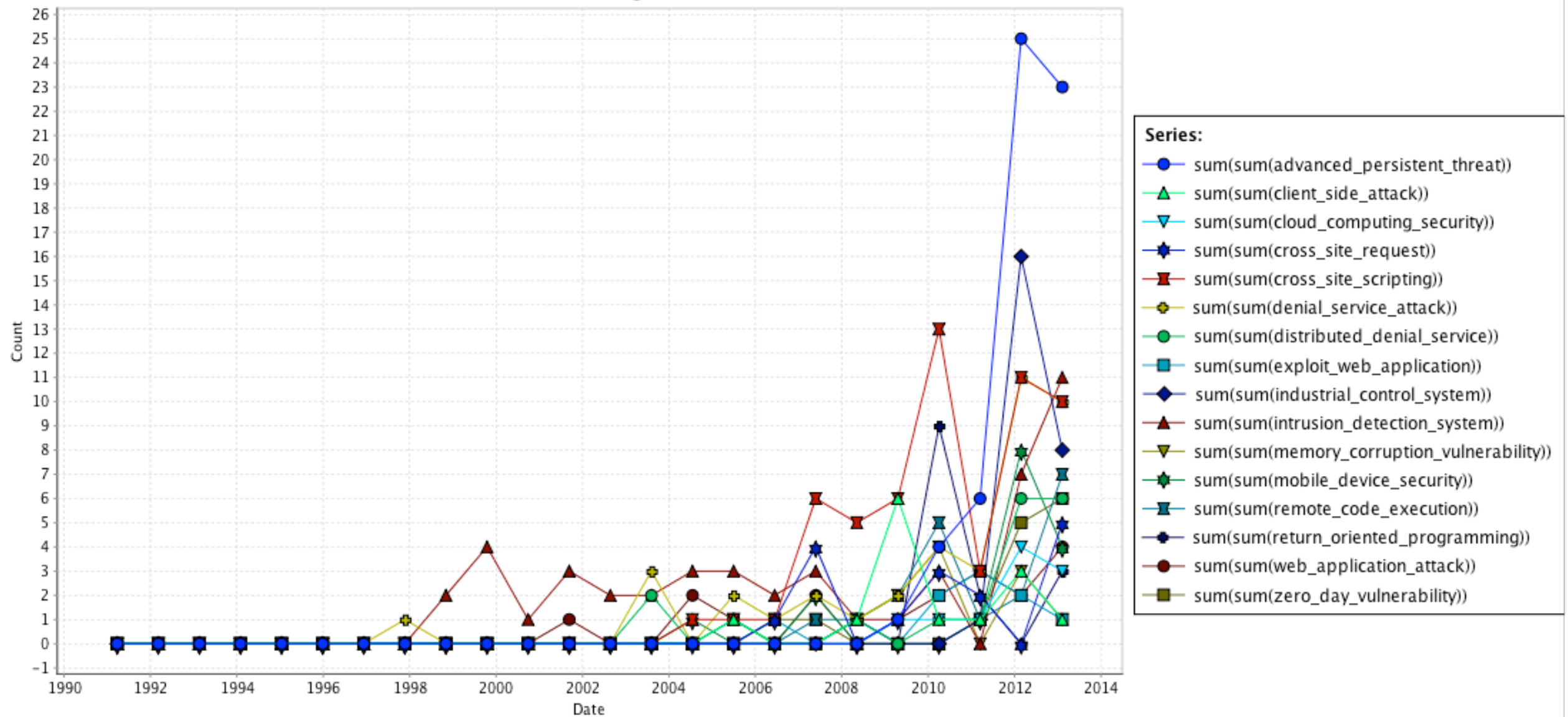
2-grams in Titles and Abstracts



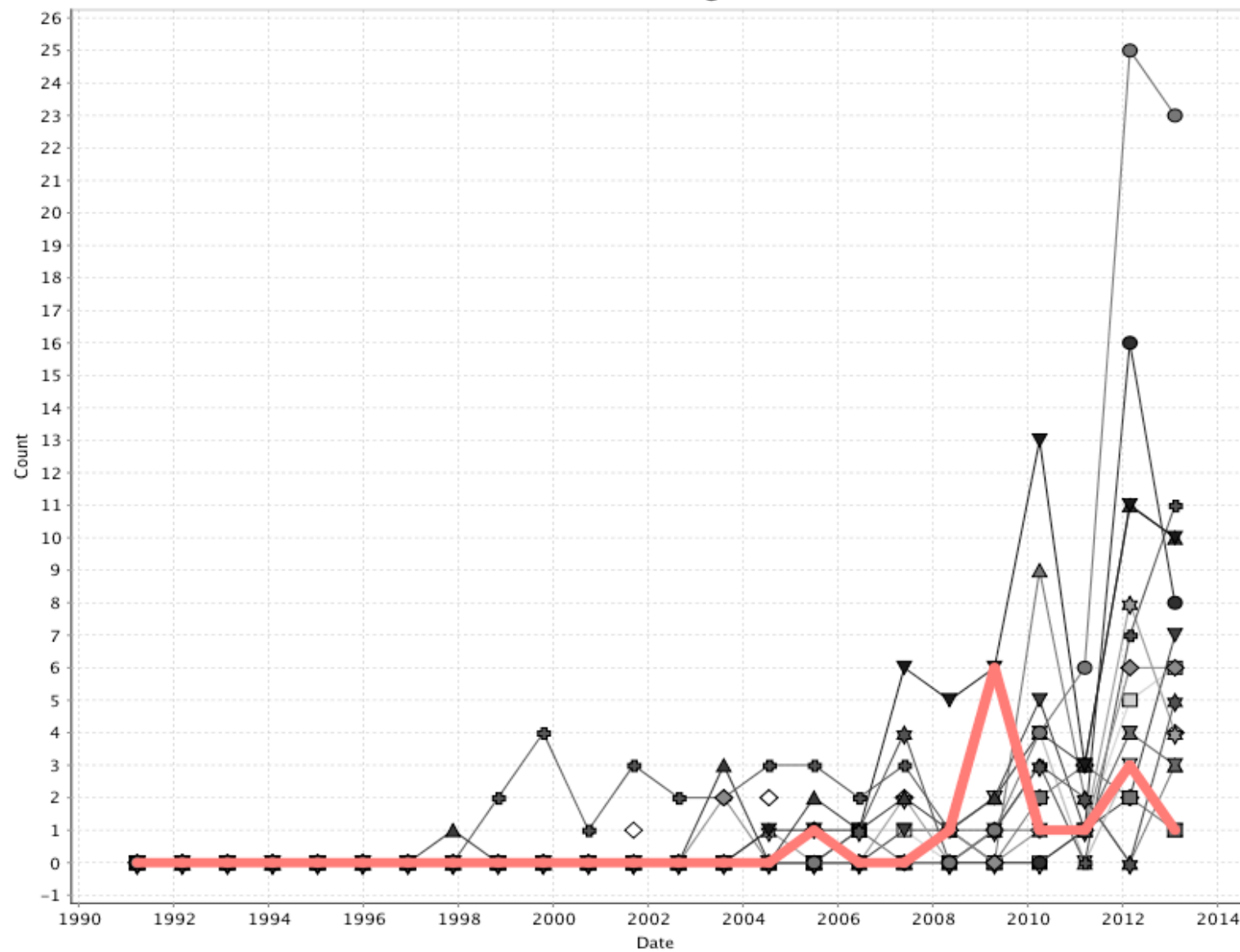
2-grams in Titles and Abstracts



3-gram Abstracts and Titles

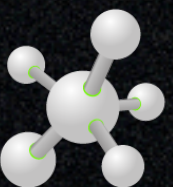


3-gram Abstracts and Titles

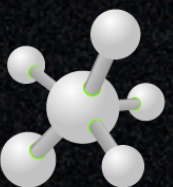
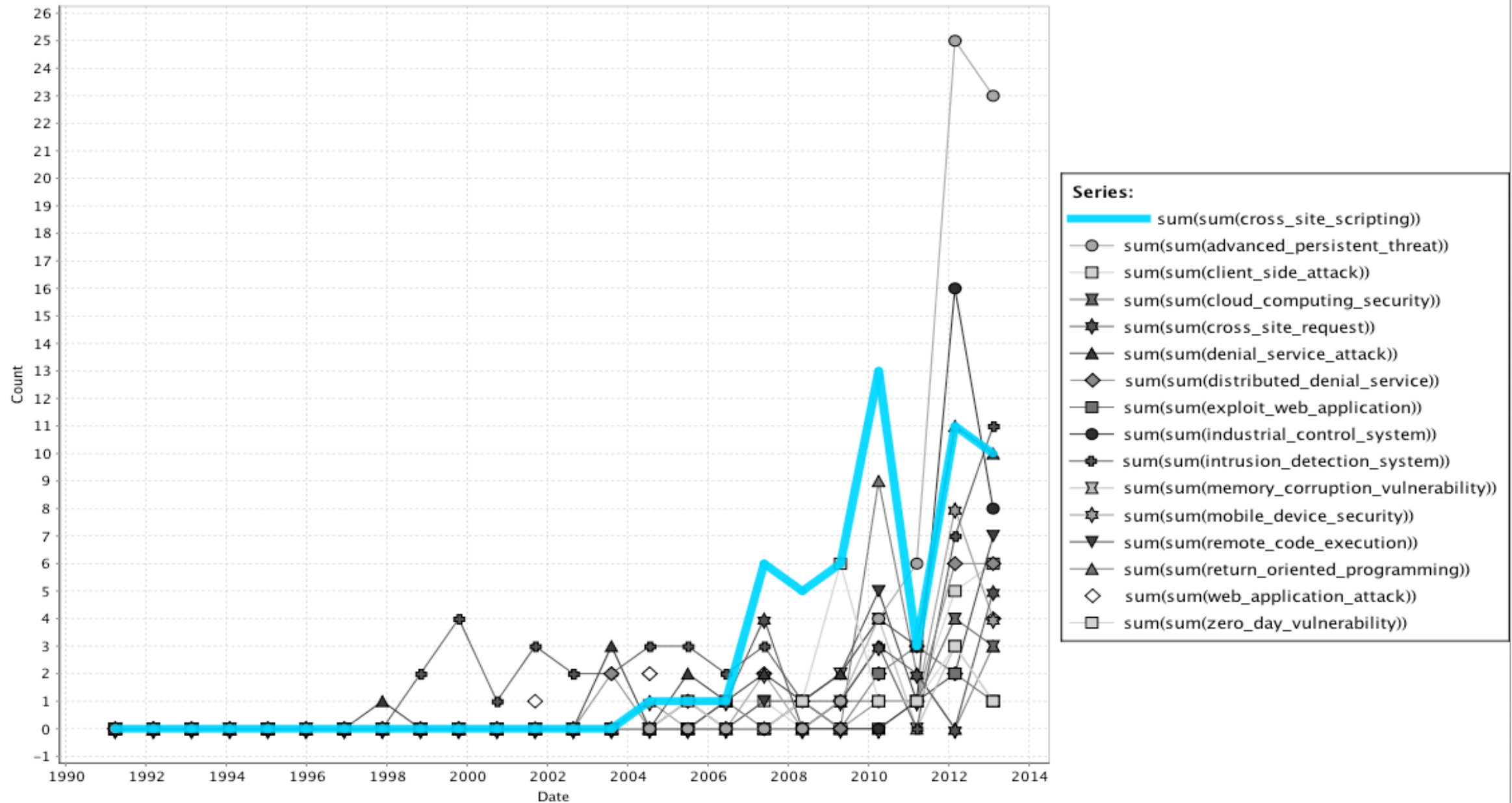


Series:

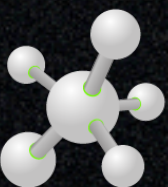
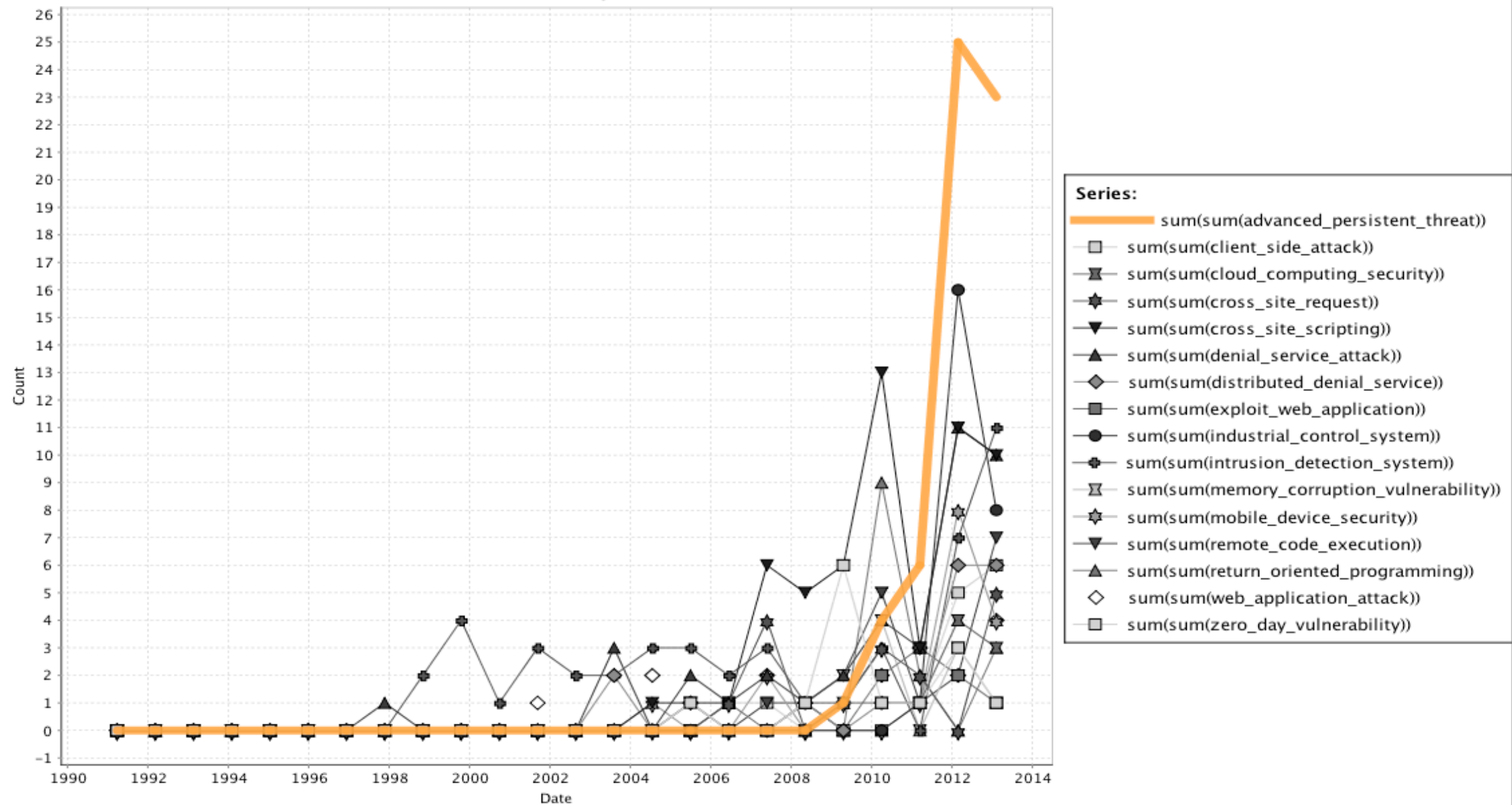
- sum(sum(client_side_attack))
- sum(sum(advanced_persistent_threat))
- sum(sum(cloud_computing_security))
- sum(sum(cross_site_request))
- sum(sum(cross_site_scripting))
- sum(sum(denial_service_attack))
- sum(sum(distributed_denial_service))
- sum(sum(exploit_web_application))
- sum(sum(industrial_control_system))
- sum(sum(intrusion_detection_system))
- sum(sum(memory_corruption_vulnerability))
- sum(sum(mobile_device_security))
- sum(sum(remote_code_execution))
- sum(sum(return_oriented_programming))
- sum(sum(web_application_attack))
- sum(sum(zero_day_vulnerability))



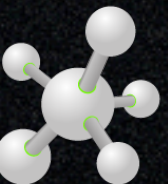
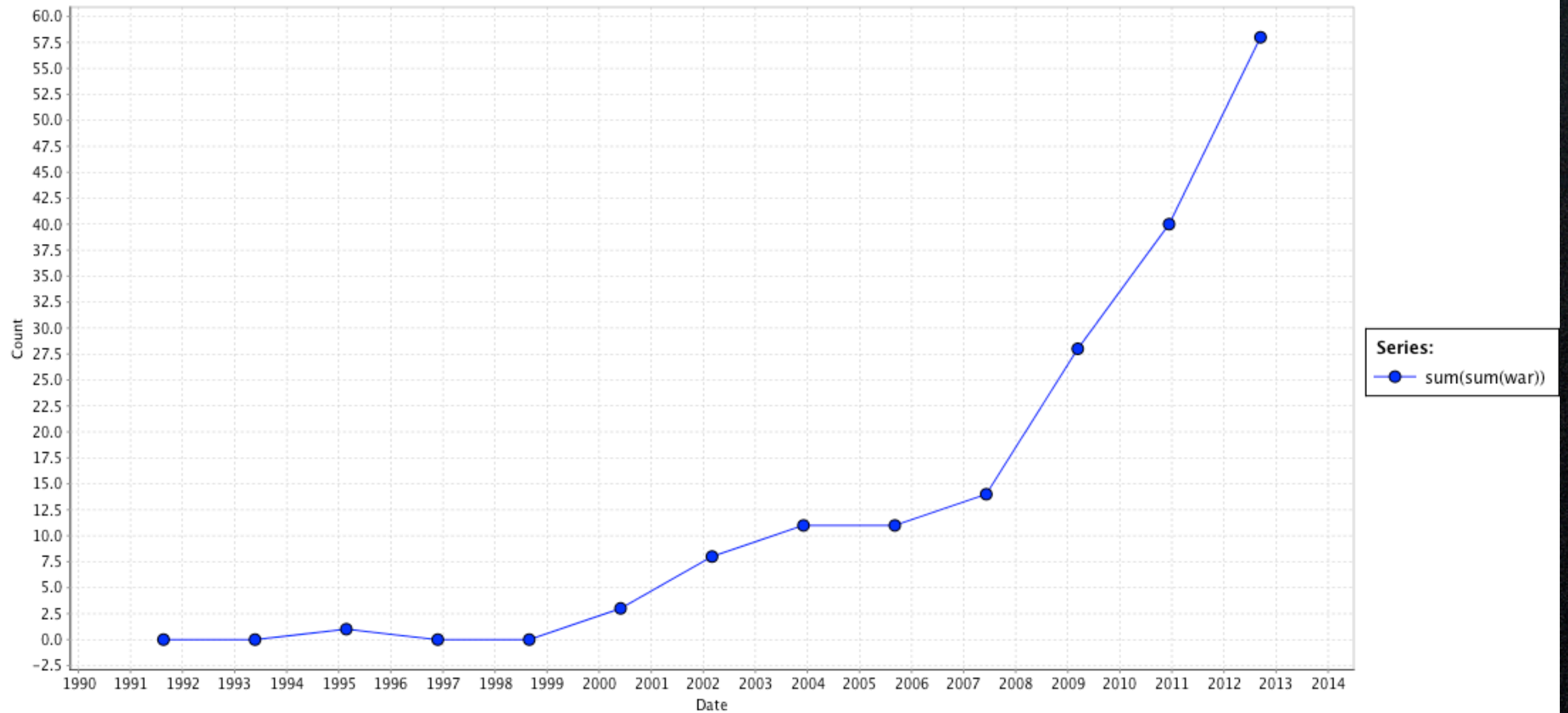
3-gram Abstracts and Titles



3-gram Abstracts and Titles



Prevalence of 'war'



We certainly are not forward leaning..
We are being led by the nose, by topics
of the day

It's might be ok, as long as we still cover the
right topics,
and we are still learning..

Are we learning ?

Quora

Anonymous

Votes by Michał Strojnowski, Anirudh Joshi, Ming Law, and 193 more.



I think it's because a good deal of TED enthusiasts (the ones who post talks to Facebook) seem to think that listening to a 20-minute talk is an intellectual endeavor, when it really isn't.

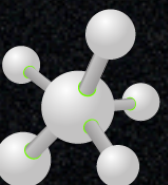
There's nothing special about these talks -- in fact, they're surprisingly devoid of substance. Even if the presenter talks in rapid spurts, there really isn't a lot of information that can be covered in such a short amount of time. And each lecture is a one-way discussion; only one side of an argument is presented, so it can be made as compelling as the speaker desires without standing up to rigorous inspection.

It annoys me when people post a lecture and say, "Listen to this! This guy/girl is so right!" when they can't possibly know anything about a topic that is still hotly debated among Economics PhD's, for instance. The talks are simply a form of entertainment -- the contrarian arguments give listeners the good feeling that they know something that other people don't. This is what creates the urge to "share".

So I think the TED haters are reacting to the over-enthusiasm of the TED lovers who mistakenly believe that listening constitutes some kind of intellectual pursuit.

I think it's because a good deal of TED enthusiasts (the ones who post talks to Facebook) seem to think that listening to a 20-minute talk is an intellectual endeavor, when it really isn't.

<http://www.quora.com/TED/Why-do-some-people-hate-TED>



Quora

Anonymous

Answered by Michał Strojnowski, Anirudh Joshi, Ming Law, and 193 more.



I think it's because a good deal of TED enthusiasts (the ones who post talks to Facebook) seem to think that listening to a 20-minute talk is an intellectual endeavor, when it really isn't.

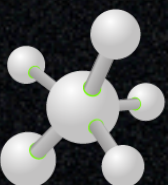
There's nothing special about these talks -- in fact, they're surprisingly devoid of substance. Even if the presenter talks in rapid spurts, there really isn't a lot of information that can be covered in such a short amount of time. And each lecture is a one-way discussion; only one side of an argument is presented, so it can be made as compelling as the speaker desires without standing up to rigorous inspection.

It annoys me when people post a lecture and say, "Listen to this! This guy/girl is so right!" when they can't possibly know anything about a topic that is still hotly debated among Economics PhD's, for instance. The talks are simply a form of entertainment -- the contrarian arguments give listeners the good feeling that they know something that other people don't. This is what creates the urge to "share".

So I think the TED haters are reacting to the over-enthusiasm of the TED lovers who mistakenly believe that listening constitutes some kind of intellectual pursuit.

there really isn't a lot of information that can be covered in such a short amount of time. And each lecture is a one-way discussion

<http://www.quora.com/TED/Why-do-some-people-hate-TED>



Quora

Anonymous

Answered by Michał Strojnowski, Anirudh Joshi, Ming Law, and 193 more.



I think it's because a good deal of TED enthusiasts (the ones who post talks to Facebook) seem to think that listening to a 20-minute talk is an intellectual endeavor, when it really isn't.

There's nothing special about these talks -- in fact, they're surprisingly devoid of substance. Even if the presenter talks in rapid spurts, there really isn't a lot of information that can be covered in such a short amount of time. And each lecture is a one-way discussion; only one side of an argument is presented, so it can be made as compelling as the speaker desires without standing up to rigorous inspection.

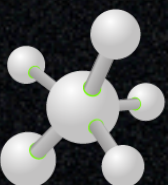
It annoys me when people post a lecture and say, "Listen to this! This guy/girl is so right!" when they can't possibly know anything about a topic that is still hotly debated among Economics PhD's, for instance. The talks are simply a form of entertainment -- the contrarian arguments give listeners the good feeling that they know something that other people don't. This is what creates the urge to "share".

So I think the TED haters are reacting to the over-enthusiasm of the TED lovers who mistakenly believe that listening constitutes some kind of intellectual pursuit.

TED makes you think you've learned a lot in 18 minutes, when you really haven't. It offers the illusion of an easier alternative to good old-fashioned hard work when it comes to learning or knowing something. And that's why it's dangerous.

<http://www.quora.com/TED/Why-do-some-people-hate-TED>

thinkst
applied research



Lets make this tangible

- Don't tell Joanna the virtualized Rootkit is Dead;
- Charlie Miller vs Macbook Batteries;

*Don't Tell Joanna, The
Virtualized Rootkit Is Dead*

Obvious Proxy Moment

Are we Winning?

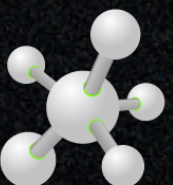
Anecdotaly...



haroon meer @haroonmeer

7 Sep

Lulzsec hacks embarrassed the sec community by showing we were outclassed as defenders. NSA leaks show we were outclassed as attackers too

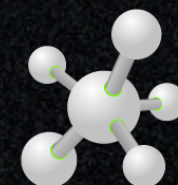


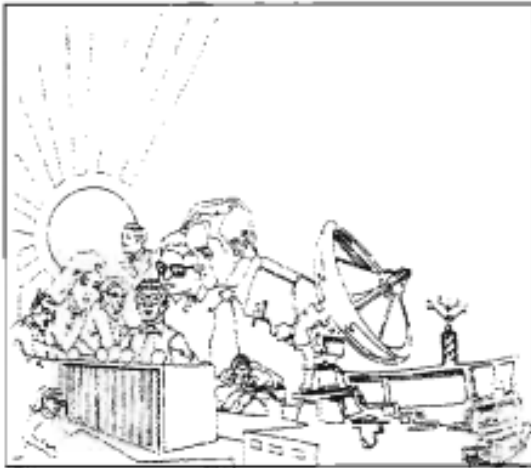


Vincenzo Iozzo @_snagg

7 Sep

[@haroonmeer](#) Or to be a tad more direct: however you slice it, the InfoSec industry has failed badly





NATIONAL SECURITY AGENCY

CRYPTOLOG

This Issue:

The Director's Summer Program

Page 2

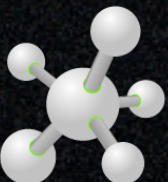
The Closing of NSGA Philippines

Page 9

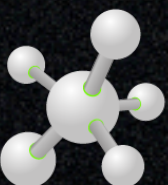
An Agnostic Look at TQM

Page 20

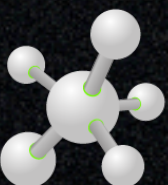
... AND MORE (Table of Contents, page i)



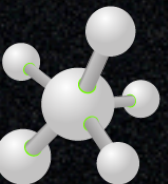
(U) Three of the last four sessions were of no value whatever, and indeed there was almost nothing at Eurocrypt to interest us (this is good news!). The scholarship was actually extremely good; it's just that the directions which external cryptologic researchers have taken are remarkably far from our own lines of interest.



(U) I think I have hammered home my point often enough that I shall regard it as proved (by emphatic enunciation): the tendency at IACR meetings is for academic scientists (mathematicians, computer scientists, engineers, and philosophers masquerading as theoretical computer scientists) to present commendable research papers (in their own areas) which might affect cryptology at some future time or (more likely) in some other world. Naturally this is not anathema to us.

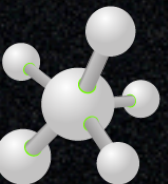


why are we sucking?



- format that discourages interaction
- audience that's increasingly passive
- more slots to fill world-wide
- push toward cons as entertainment

Containment



Containment

- Insidious
- Constantly Creeping
- Wears many masks..

Why we should fight it
(as attendees)

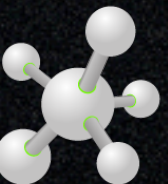
Why we should fight it
(as researchers)

Why we should fight it (as researchers)

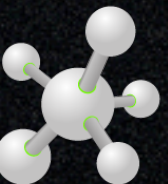
ARE YOU NOT ENTERTAINED?



IS THIS NOT WHY YOU ARE HERE?



It's a fine line..



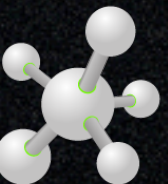
Take some stuff more
seriously



Charlie Miller @0xcharlie

3 Jun

It's driving me crazy reading the academic papers submitted to WOOT. They NEVER **cite** non academic work.



how often do you see us
reference anyone?

Over Last 3 Years

- Talks X
- Talks with Actual Accompanying Papers $X/2$
- Papers with Actual Acceptable References $X/4$

- confs skew towards entertainment
- confs skew towards stuff digestible in an hour

Why do we want to
present ?

Career Progression

Fame & Fortune

Share our Research

Conferences have probably
become the wrong vehicle for
that

Computational Complexity x

blog.computationalcomplexity.org/2009/07/time-for-computer-science-to-grow-up.html

إنشاء مدونة إلكترونية تسجيل الدخول

المزيد المشاركة 0

Computational Complexity

Computational Complexity and other fun stuff in math and computer science from Lance Fortnow and Bill Gasarch



Friday, July 24, 2009

Time for Computer Science to Grow Up

The August CACM has my viewpoint article Time for Computer Science to Grow Up about the urgent need for conference reform.

Our conference system forces researchers to focus too heavily on quick, technical, and safe papers instead of considering broader and newer ideas. Meanwhile, we have devoted much of our time and money to conferences where we can present our research that we can rarely attend conferences and workshops to work and socialize with our colleagues.

Computer science has grown to become a mature field where no major university can survive without a strong CS department. It is time for computer science to grow up and publish in a way that represents the major discipline it has become.

I argue that computer science uses conferences to play the role of reputation that journals play in other fields for reputation but then conferences no longer focus on the more important role of bringing out community together.

You can also download the pre-publication PDF.

Update 8/3: The editors of CACM have made the full text of the CACM article publicly accessible.

8/7: Collection of related blog posts and other links. Feel free to send me others.

Posted by Lance Fortnow at 5:18 AM






Recommend this on Google

119 comments:

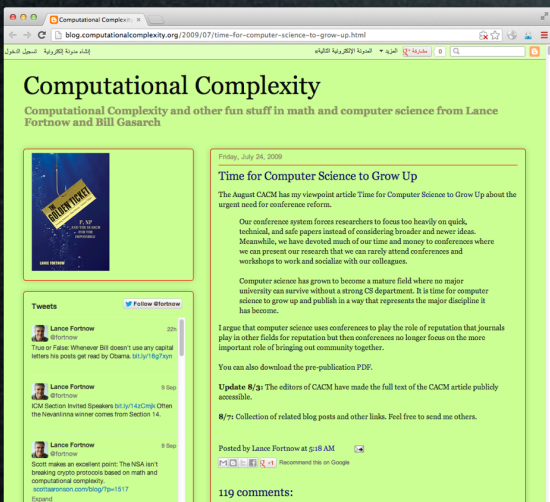
Tweets Follow @fortnow

Lance Fortnow @fortnow 22h
True or False: Whenever Bill doesn't use any capital letters his posts get read by Obama. bit.ly/16g7xyn

Lance Fortnow @fortnow 9 Sep
ICM Section Invited Speakers bit.ly/14zCmjk Often the Nevanlinna winner comes from Section 14.

Lance Fortnow @fortnow 9 Sep
Scott makes an excellent point: The NSA isn't breaking crypto protocols based on math and computational complexity. scottaaronson.com/blog/?p=1517

Expand



Unlike every other academic field, computer science uses conferences rather than journals as the main publication venue. While this made sense for a young discipline, our field has matured and the conference model has fractured the discipline and skewered it toward short-term, deadline-driven research. Computer science should refocus the conference system on its primary purpose of bringing researchers together. We should use archive sites as the main method of quick paper dissemination and the journal system as the vehicle for advancing researchers' reputations.

Were they ever the right
vehicle for that?

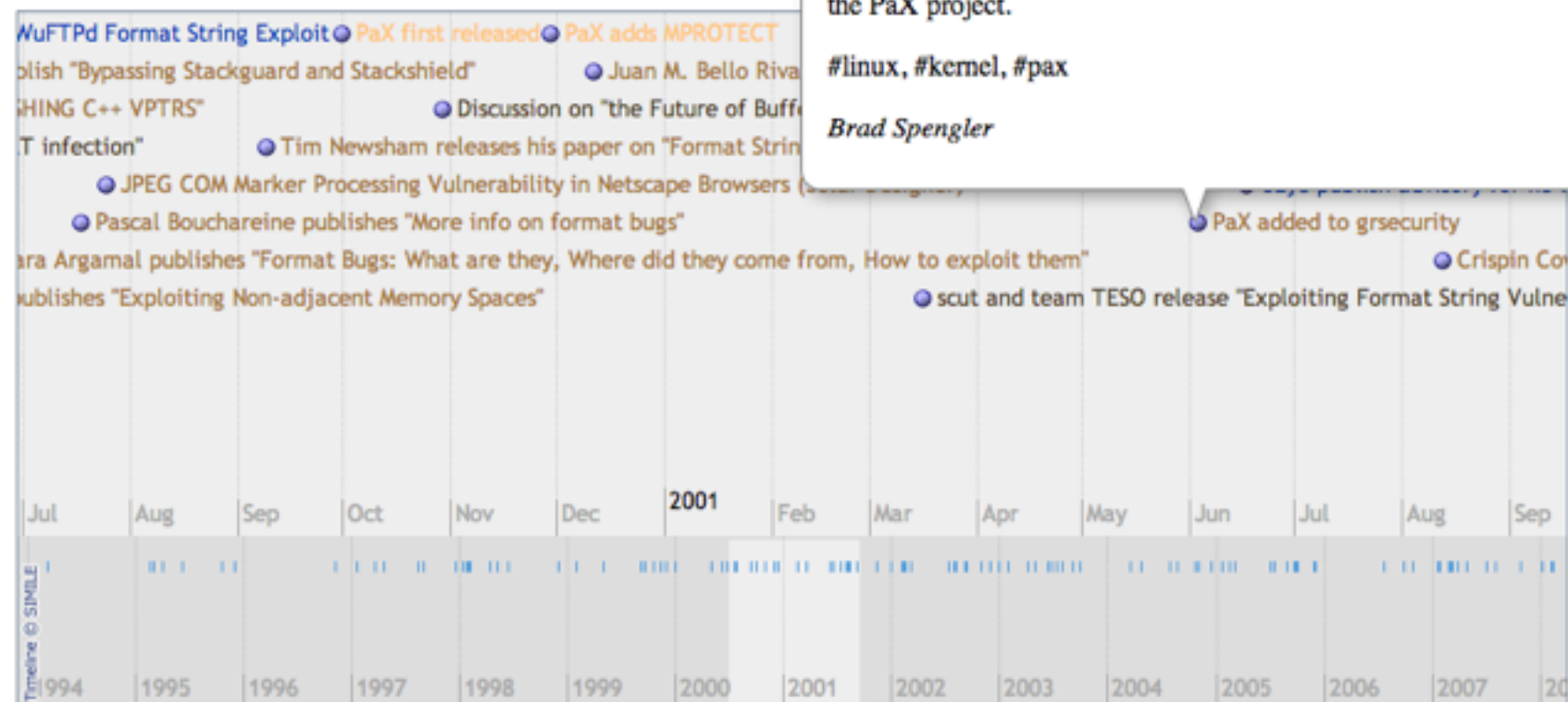


Combo-Action!

The timeline on top is courtesy of the uber [simile project](#) from MIT. It allows us to filter on events and even to search on them with pretty output per event too. The google interactive visualization underneath maps the same events alongside with the number of reported memory corruption bugs (crawled from OSVDB) over the same periods.

You can add to the timeline by filling in the form [\[here\]](#)

1 result out of 157



Search

Event Type

- 12 #Publication
- 14 Exploit
- 5 Incident
- 5 Organization
- 3 Patch
- 96 Publication
- 6 Release

#Publication Exploit Incident Organization Patch Publication Release Tool



Of all the events considered impactful
to memory corruption attacks

23% Papers

17% Mail List

14% Paper (at Conference)

5% PPT (at Conference)

Are we doing more than
complaining?

Wrapping Up..

Huxley vs Orwell



ALDOUS HUXLEY

Author: "Brave New World"

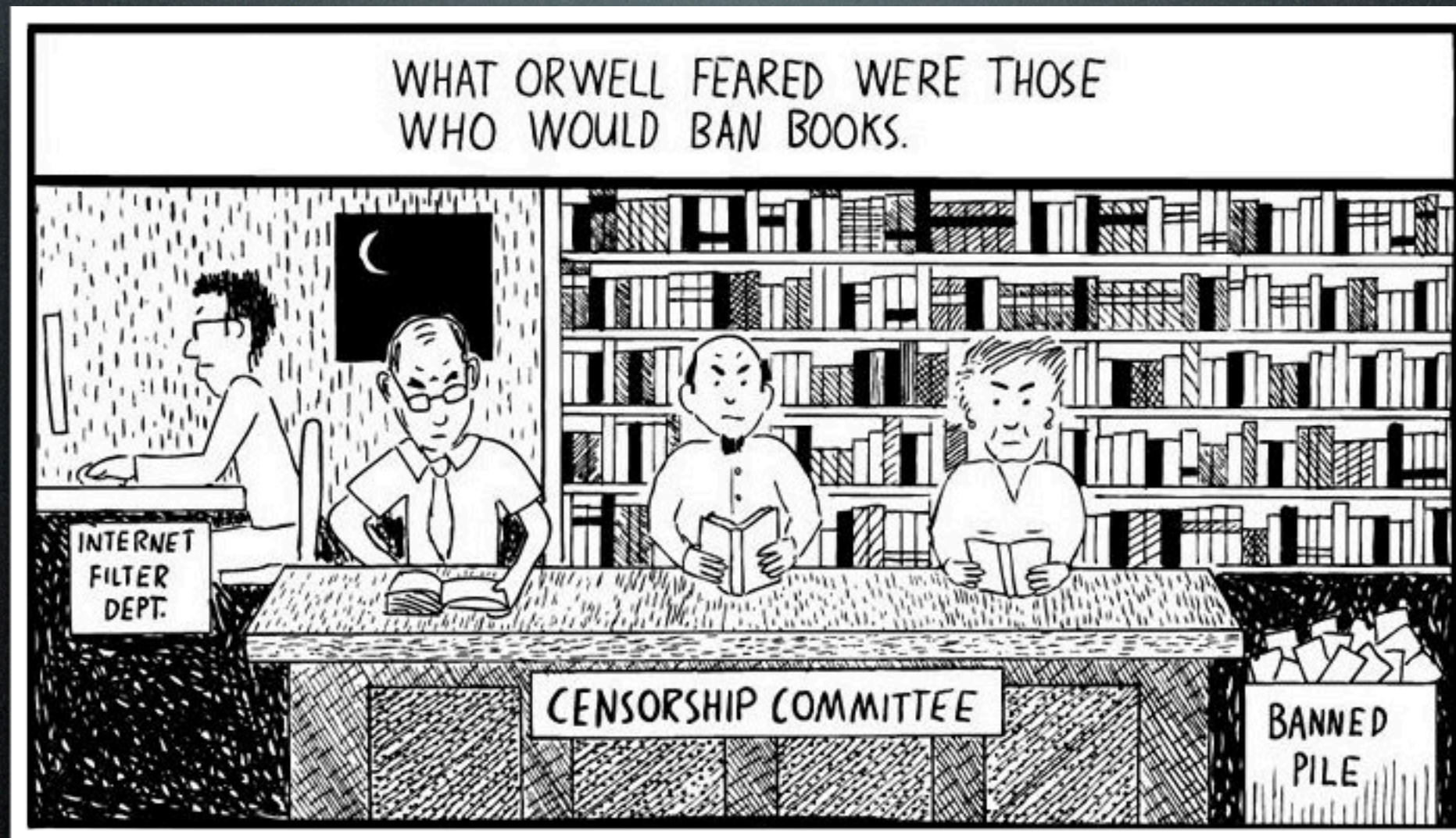
vs.



GEORGE ORWELL

Author: "Nineteen Eighty-Four"

<http://www.highexistence.com/amusing-ourselves-to-death-huxley-vs-orwell/>



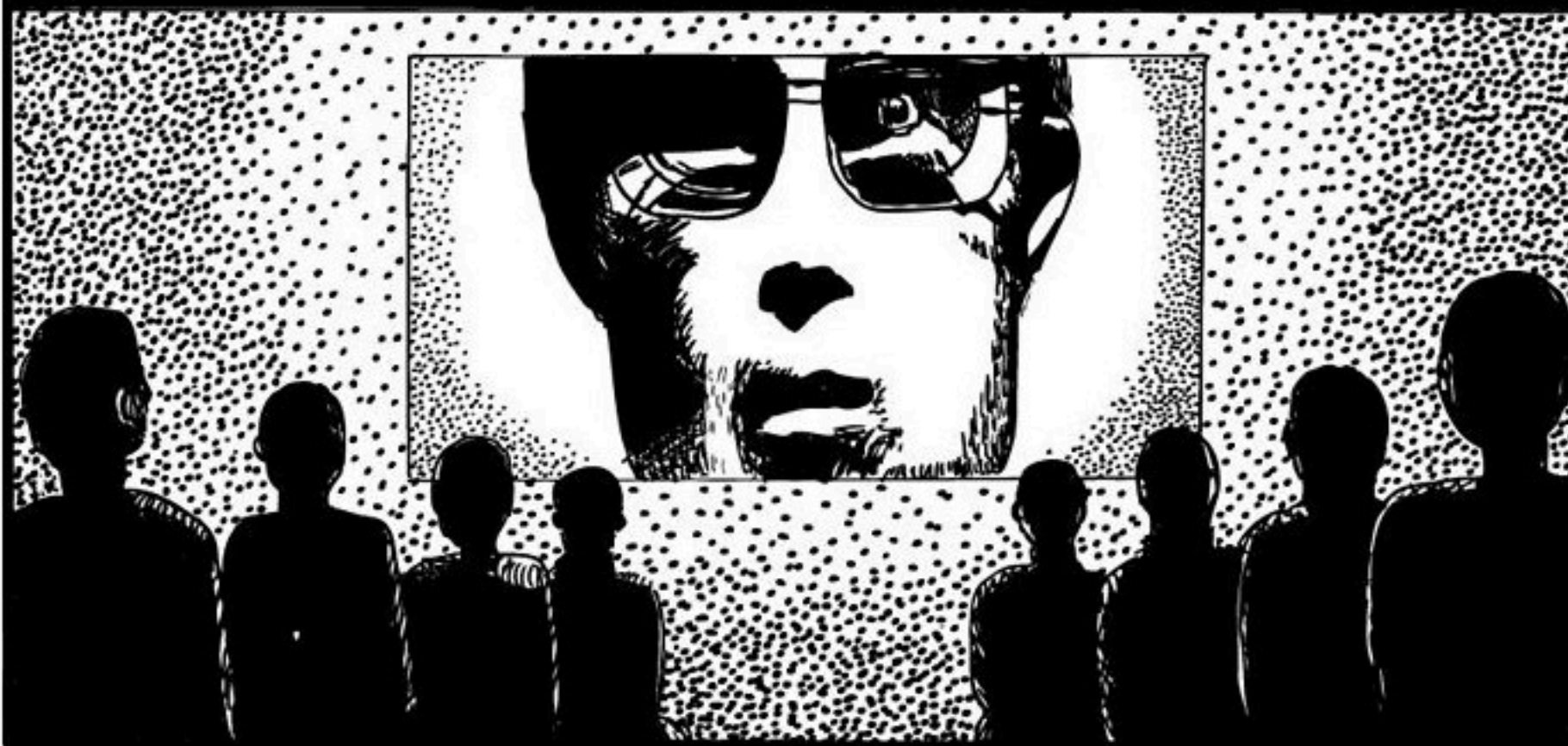
<http://www.highexistence.com/amusing-ourselves-to-death-huxley-vs-orwell/>

WHAT HUXLEY FEARED WAS THAT THERE WOULD BE
NO REASON TO BAN A BOOK, FOR THERE WOULD BE
NO ONE WHO WOULD WANT TO READ ONE.



<http://www.highexistence.com/amusing-ourselves-to-death-huxley-vs-orwell/>

ORWELL FEARED THOSE WHO WOULD
DEPRIVE US OF INFORMATION.



<http://www.highexistence.com/amusing-ourselves-to-death-huxley-vs-orwell/>

HUXLEY FEARED THOSE WHO WOULD GIVE US SO MUCH
THAT WE WOULD BE REDUCED TO PASSIVITY AND EGOTISM.



IN "NINETEEN EIGHTY-FOUR",
PEOPLE ARE CONTROLLED
BY INFLICTING PAIN.



IN "BRAVE NEW WORLD",
PEOPLE ARE CONTROLLED
BY INFLICTING PLEASURE.

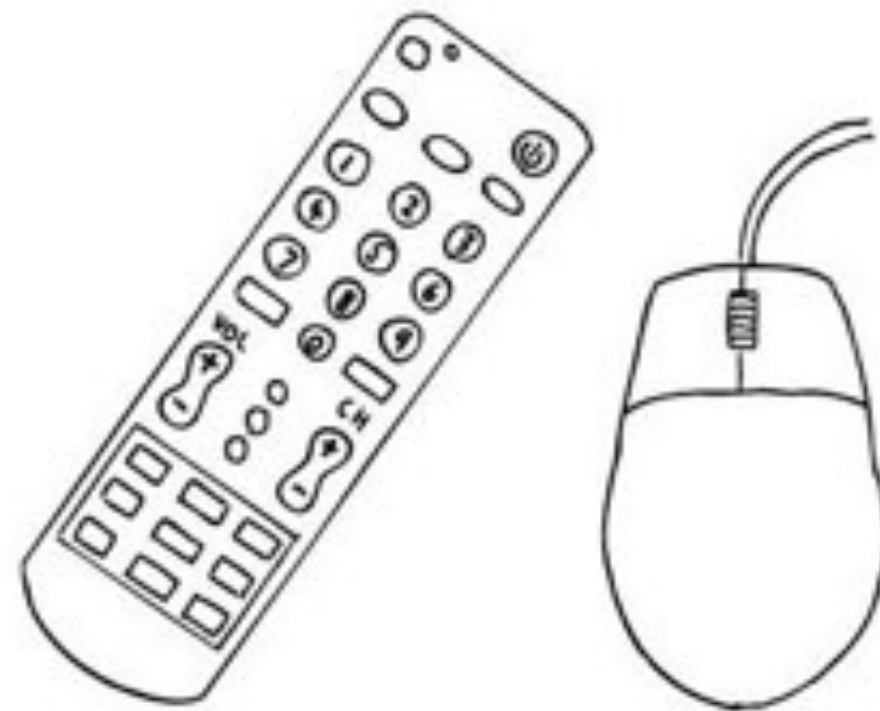


<http://www.highexistence.com/amusing-ourselves-to-death-huxley-vs-orwell/>

IN SHORT, ORWELL FEARED
THAT WHAT WE HATE
WILL RUIN US.



HUXLEY FEARED THAT WHAT
WE LOVE WILL RUIN US.



Tim O'Reilly



"What we choose to fight is so tiny!
What fights us is so great!
When we win it's with small things,
and the triumph itself makes us small

- Our industry is at an important inflection point
- We simultaneously face a crisis of relevance & confidence
- We have important problems to solve
- Our best, and brightest shouldn't be burning their time creating sideshows to distract / entertain the rest..

- Researchers:

Lets work on stuff that matters

- Attendees:

Lets demand a little more

- Organizers:

Lets give people more of what they need (instead of just what they think they want)

Questions ?

@marcoslaviero | @haroonmeer

