



UNCERTAINTY OF ATTRIBUTION

Finding the Needle
in the Needlestack

Davi Ottenheimer
@daviottenheimer
Vienna, April 2014


WHOAMI



2014 Breach Analysis: flyingpenguin

"While high flying speeds can be detrimental to landing on tree perches for flying birds, there is little consequence to high impact landing in water."

@daviottenheimer

- 🔒 Anthropology of Language / Music / Math
"Shintiri: the secret language"
- 🔒 Bike / Sailboat Racing
- 🔒 Ethics of "Humanitarian Intervention"
- 🔒 International History
- 🔒 ...&  20 Years InfoSec



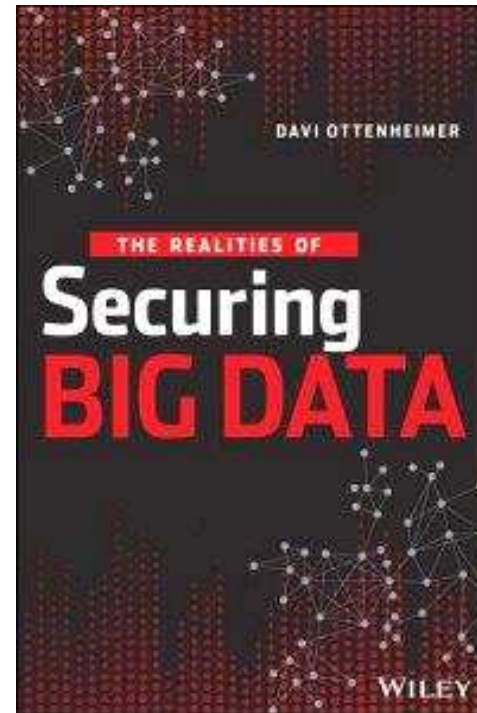
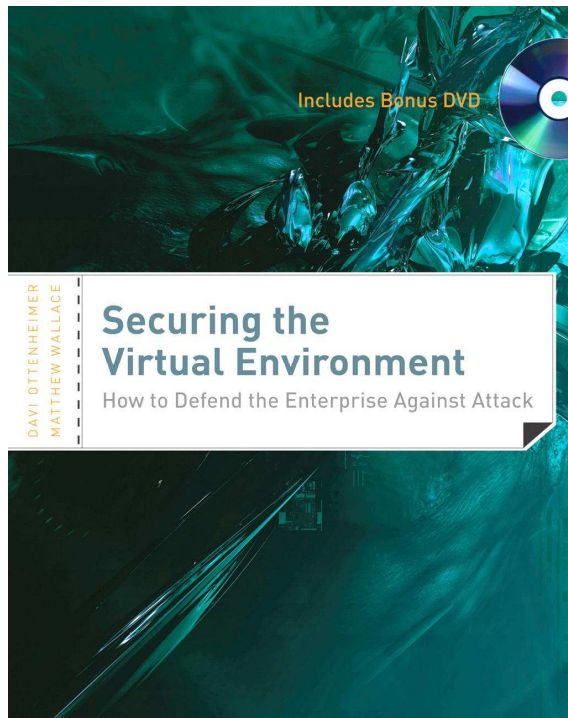
EMC²

Pivotal



vmware

GROWING **BODY** OF DATA OBESITY RESEARCH



DEFINITION

at·tri·bu·tion

noun \,a-trə-'byü-shən\
The act of saying the origin or cause of something

The act of saying the origin or cause of something

Ascribing an event to a particular agent or action



EMC²

Pivotal

RSA

vmware

DEFINITION

hack·er

noun /'hakər/

A person who attempts rough or short cuts

Someone whose curiosity or method leads to access via new or unexpected means



EMC²

Pivotal

RSA

vmware

ATTRIBUTION CAT-EGORIES

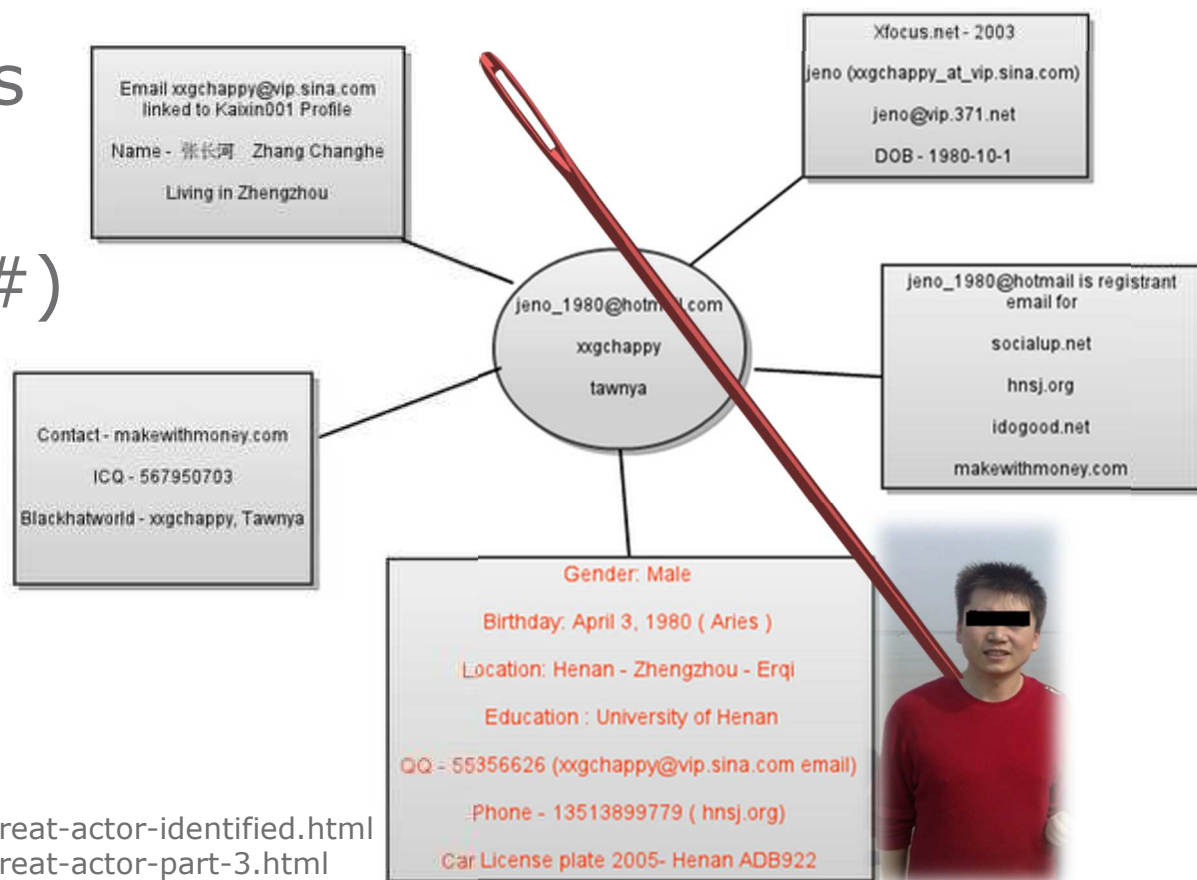
HACKER?

SITUATION
(ENVIRONMENT)

DISPOSITION
(INDIVIDUAL)

WYCORES EXAMPLE

1. Traced Attacks
2. Profiled IDs
3. Dumped (QQ#)
4. Remedied...
 - Situation
 - Disposition
 - Both?



<http://cyb3rsleuth.blogspot.com/2011/08/chinese-threat-actor-identified.html>
<http://cyb3rsleuth.blogspot.com/2012/03/chinese-threat-actor-part-3.html>

FLAKE POWER THEORY?

Effects

Hackers are addicted to the power of controlling machines.

!= sysadmins because?

Almost every time they compromise a new machine, their “compromise boundary” grows.

The drug gets better the more you take - unlike “regular” drugs.

!= power because?

What does this mean?

An out-of-control hacker will only stop expanding the network of compromised machines once every machine is either compromised by him, or on his compromise boundary.

“19% of UK senior roles go to women compared to 51% in China”

https://docs.google.com/presentation/d/1Sv8IHkbtBEXjSW7WktEYg4EbAUHtVyXIZBrAGD3WR5Y/edit?pli=1#slide=id.g268c10cab_0267
<https://www.theguardian.com/women-in-leadership/2013/sep/25/china-uk-female-senior-managers-study>



EMC²

Pivotal



vmware

"WHAT DOES [POWER ADDICTION] MEAN?"

Science, technology and innovation participation: tertiary science and engineering enrollment

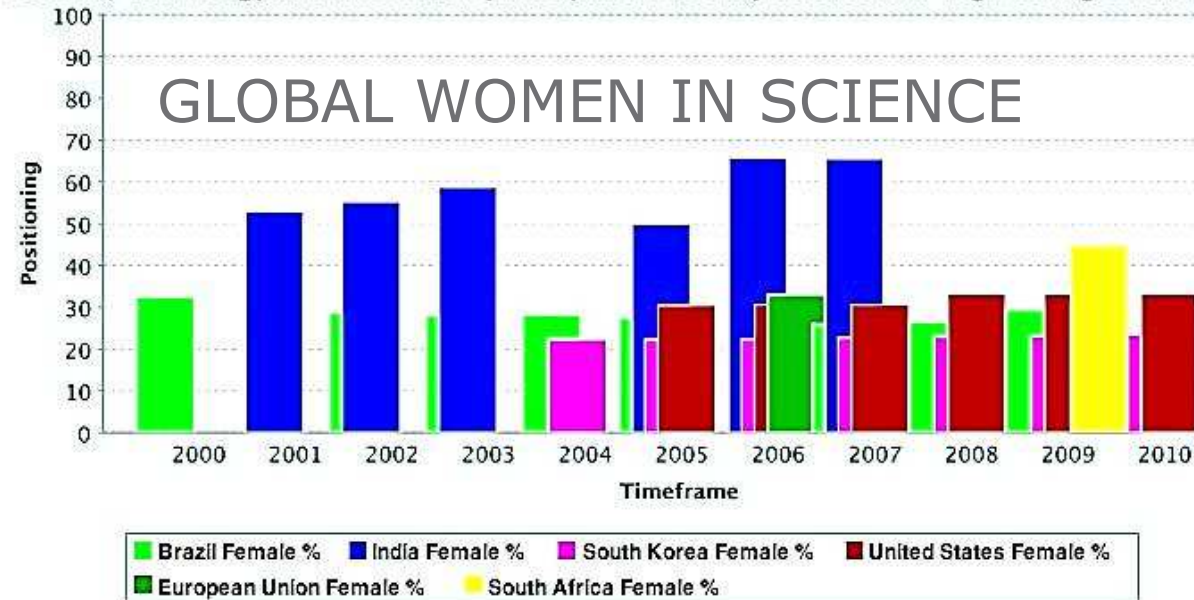
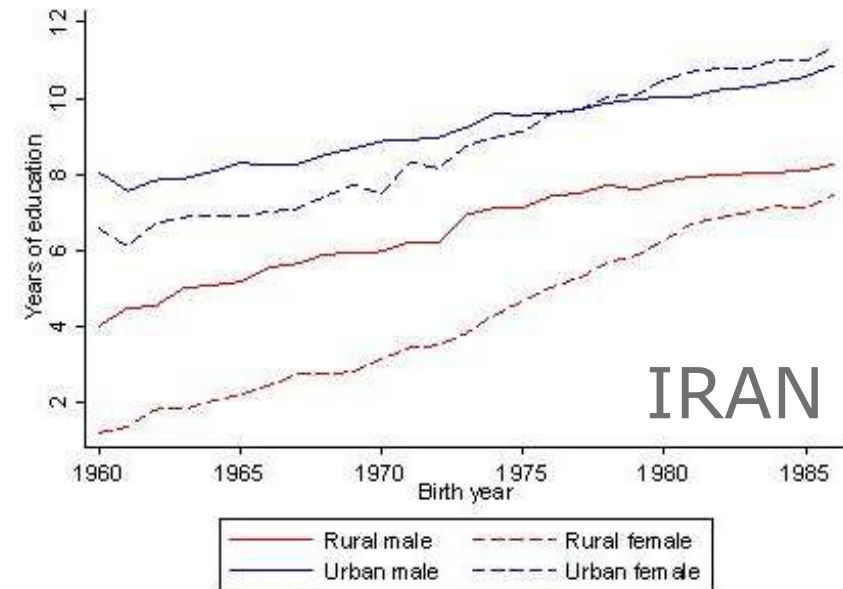


Figure 4. Average years of schooling by birth cohort



Source: Author's calculations using HEIS data files.

<http://wisat.org/what-we-do/sti1/>
<http://www.brookings.edu/research/opinions/2009/01/29-iran-salehi-isfahani>



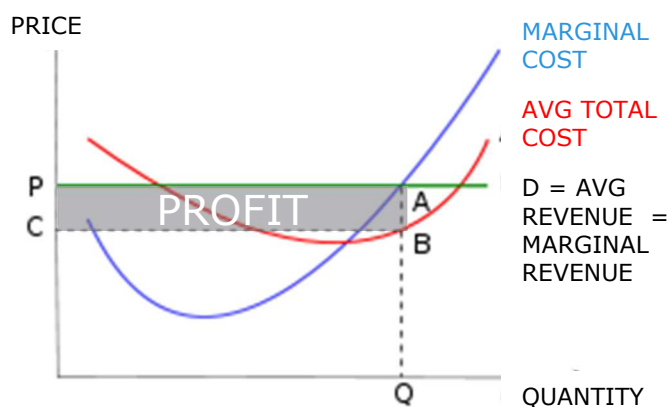
OF MICE AND MEECES

Money

Ideology

Compromise or Coercion

Ego or Extortion



Money

Entertainment

Ego

Cause

Enter Social Groups

Status

1. Anti-Collaborative...SHHHH!
2. Collaborative
3. Hyper-Collaborative



<http://www.sparknotes.com/economics/micro/supplydemand/equilibrium/section3.rhtml>

<http://www.aic.gov.au/documents/1/B/A/%7B1BA0F612-613A-494D-B6C5-06938FE8BB53%7Dhtcb006.pdf>



EMC²

Pivotal



vmware

HOW TO LOSE A FIGHT



the grugq
@thegrugq

Slides for my talk on mobile phone operational security and hardening Android: slideshare.net/grugq/mobile-o... + source code: github.com/grugq/darkmatt...

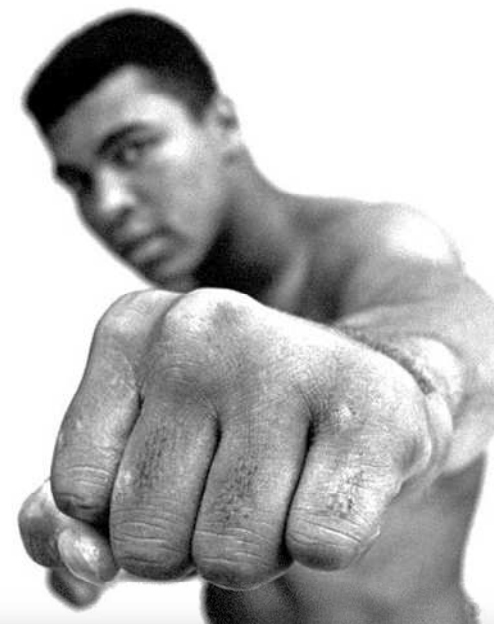
Reply Retweeted Favorite More

RETWEETS
139

FAVORITES
177



2:23 AM - 4 Apr 2014



“If you want to lose a fight, talk about it first”

–Quellcrist Falconer

<http://www.twitter.com/thegrugq/status/452013704632991745>



EMC²

Pivotal

RSA

vmware

HOW TO LOSE A CITE

"If you want to lose a fight, talk about it first"

-Quellcrist Falconer

W http://en.wikipedia.org/wiki/Quellcrist_Falcoi

If you want to lose a fight, talk about it first.

Furies



g+1 5



45 Reviews
Write review

Woken Furies

By Richard K. Morgan

If you want to lose a figl

Go

No results found in this book for **If you want to lose a fight, talk about it first** - [Search all books »](#)

http://books.google.com/books?id=RvJMkL8cuw0C&lpg=PA138&ots=9_MMVQdOcP&dq=quellcrist%20falconer%20%20woken%20furies&pg=PA138#v=snippet&q=If%20you%20want%20to%20lose%20a%20fight,%20talk%20about%20it%20first&f=false



EMC²

Pivotal



vmware

GANGSTER CONFESSION

“Nobody could pay me for this work. It was my **patriotic duty**. There ain't **no amount of money** to buy them kind of things”

- Meyer Harris "Mickey" Cohen



[http://books.google.com/books?id=TXOnqtNJWWEc&q=nobody could pay me for this work](http://books.google.com/books?id=TXOnqtNJWWEc&q=nobody+could+pay+me+for+this+work)
<http://life.time.com/crime/mickey-cohen-photos-of-a-legendary-los-angeles-mobster-1949/>

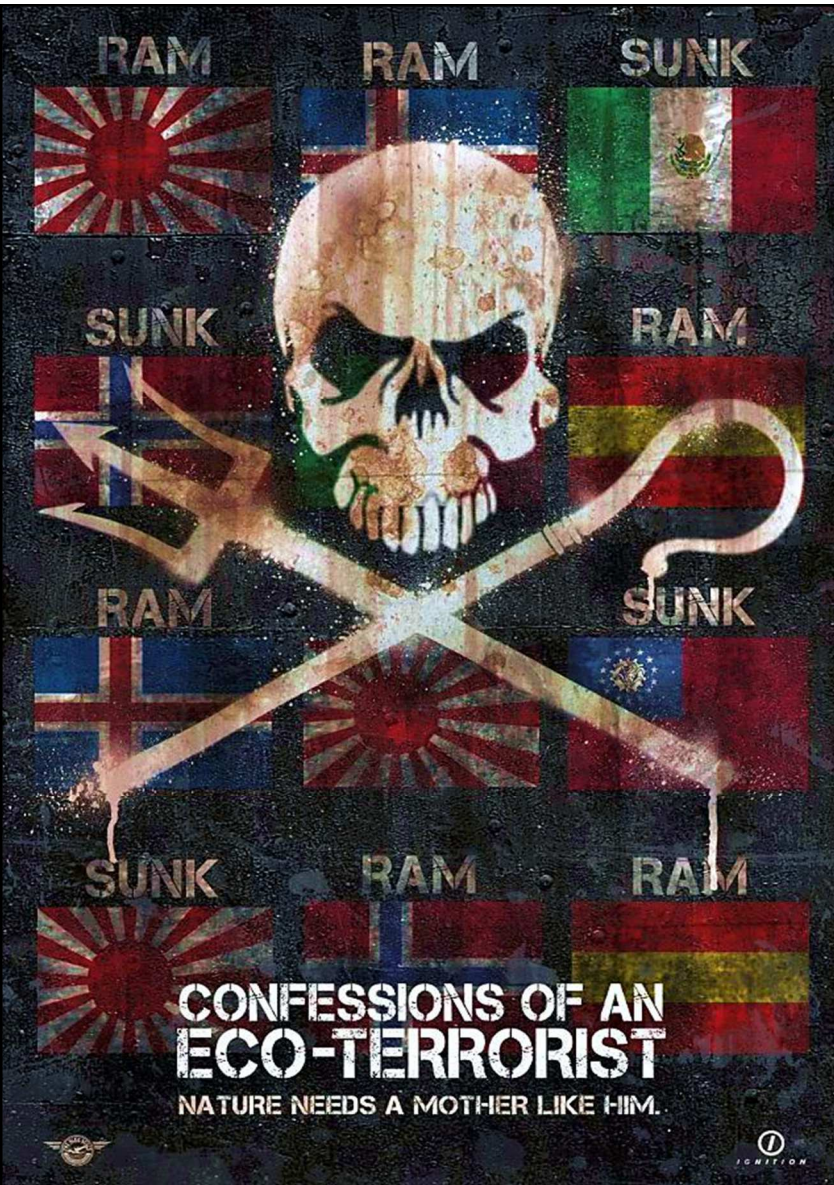


EMC²

Pivotal



vmware



ACTIVIST CONFESSION

1. Seek attention

2. To win...talk. A lot

“Hey, seal is no big deal,
I’ve eaten elephant...”





3. Leverage motive triggers
(Humor, Fear, Despair)

BEKENNTNISSE EINES ÖKO-TERRORISTEN
http://www.youtube.com/watch?v=KOSo_LHZeTw

MAPTNDIANT1 EXAMPLE

1. 99.8% HTRAN connections:
Redirected to **Shanghai addresses**
2. 97% monitored RDP sessions:
Simplified Chinese systems
3. **Chinese government**: only one
with motive, means, and
opportunity

Resident foreigners in Shanghai (1%)

Country of Origin	Population (2009)	Population (2010)
 Japan	31,490	35 075
 United States	21,284	24 358
 South Korea	20,700	21 073
 France	7,437	8 238
 Germany	7,253	8 023
 Singapore	7,209	7 545
 Canada	6,121	7 306
 Australia	5,257	6 165
 United Kingdom	5,137	5 591

“...trading houses from the **United Kingdom, France, the United States, Italy, Russia, Germany, Japan, the Netherlands and Belgium**”

- Wikipedia



EMC²

Pivotal

RSA

vmware

SIMPLIFIED CHINESE SYSTEMS

Microsoft MS 00-069

IME for Simplified Chinese does not correctly recognize the machine state, and exposes inappropriate functions as part of the logon screen. As a result, a malicious user who had access to either a physical keyboard or a terminal server session on an affected machine could gain **LocalSystem privilege even without logging onto the machine.**

Sun CVE-2008-0730

(1) Simplified Chinese, (2) Traditional Chinese, (3) Korean, and (4) Thai language input methods in Sun Solaris 10 **create files and directories with weak permissions...**

Microsoft MS 13-075

The vulnerability could allow elevation of privilege if a logged on attacker launches Internet Explorer from the toolbar in Microsoft Pinyin IME for Simplified Chinese. An attacker who successfully exploited this vulnerability could **run arbitrary code in kernel mode.**

<http://www.cvedetails.com/cve/CVE-2008-0730/>

<http://technet.microsoft.com/en-us/security/bulletin/ms00-069>

<http://technet.microsoft.com/en-us/security/bulletin/ms13-075>



EMC²

Pivotal



vmware

SIMPLIFIED CHINESE SYSTEMS

March 2, 2014



感谢大家对微软 XP 退休的关注。针对大家关心的问题，我们在这里做四点进一步的说明：

首先，已经安装 XP 的电脑仍然可以在 4 月 8 日以后使用。

第二，微软中国已经采取特别行动，与包括腾讯在内的国内领先互联网安全及防病毒厂商密切合作，为中国全部使用 XP 的用户，在用户选择升级到新一代操作系统之前，继续提供独有的安全保护。

第三，数据显示，70% 的中国 XP 用户，在过去 13 年中没有选择使用微软定期推送的安全保护服务。对于大部分用户来说，XP 退休带来的影响有限。尽管如此，微软与众多国内厂商即将推出的这一系列安全措施，仍将在这些用户选择升级到新一代操作系统之前提供保护。

第四，这款长达 13 年的产品已经不能满足互联网时代的需求，不足以应对层出不穷且变化多端的网络安全威胁。新一代的操作系统在网络环境下，其安全程度大幅提升。

感谢大家一直以来对 XP 的喜爱和不离不弃。说再见总是很难，但千里相送终须一别。在大家选择升级到新一代操作系统之前，我们与包括腾讯等在内的国内领先互联网安全厂商，仍将对你不离不弃，护你左右。

@微软中国

“Microsoft will work with Chinese security firms to issue patches for XP for an indefinite period”

70% Chinese XP users never installed **any** security update

- 195m PCs
- 55% Run XP = **107m**
- 90% Pirated = 10.7m Patchable
- 30% Patched Once = 3m
- 3m of 107m Systems =

3% Patched

<http://www.neowin.net/news/statcounter-windows-xp-is-the-most-used-os-in-eight-countries-including-china>

<http://www.neowin.net/news/ballmer-9-out-of-10-copies-of-windows-in-china-is-pirated>

<http://www.tomsguide.com/us/windows-xpocalypse-china,news-18403.html>



EMC²

Pivotal

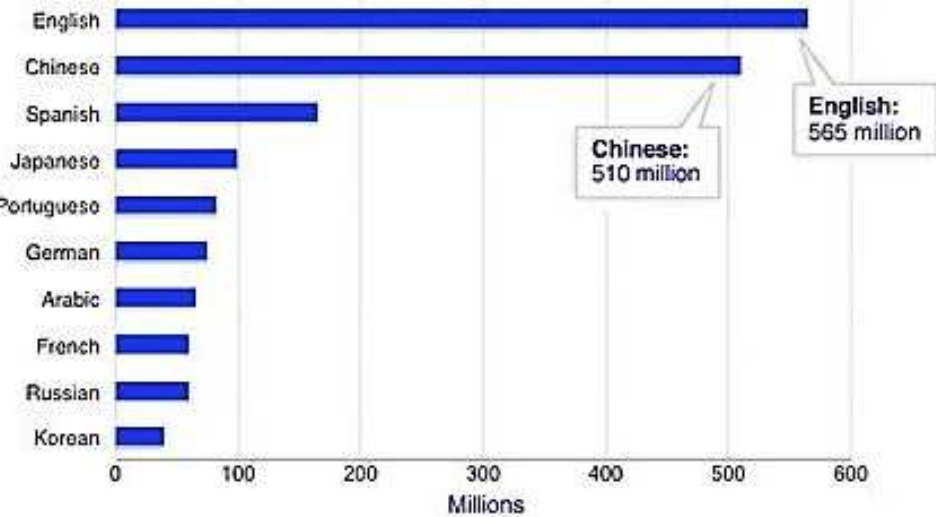


vmware

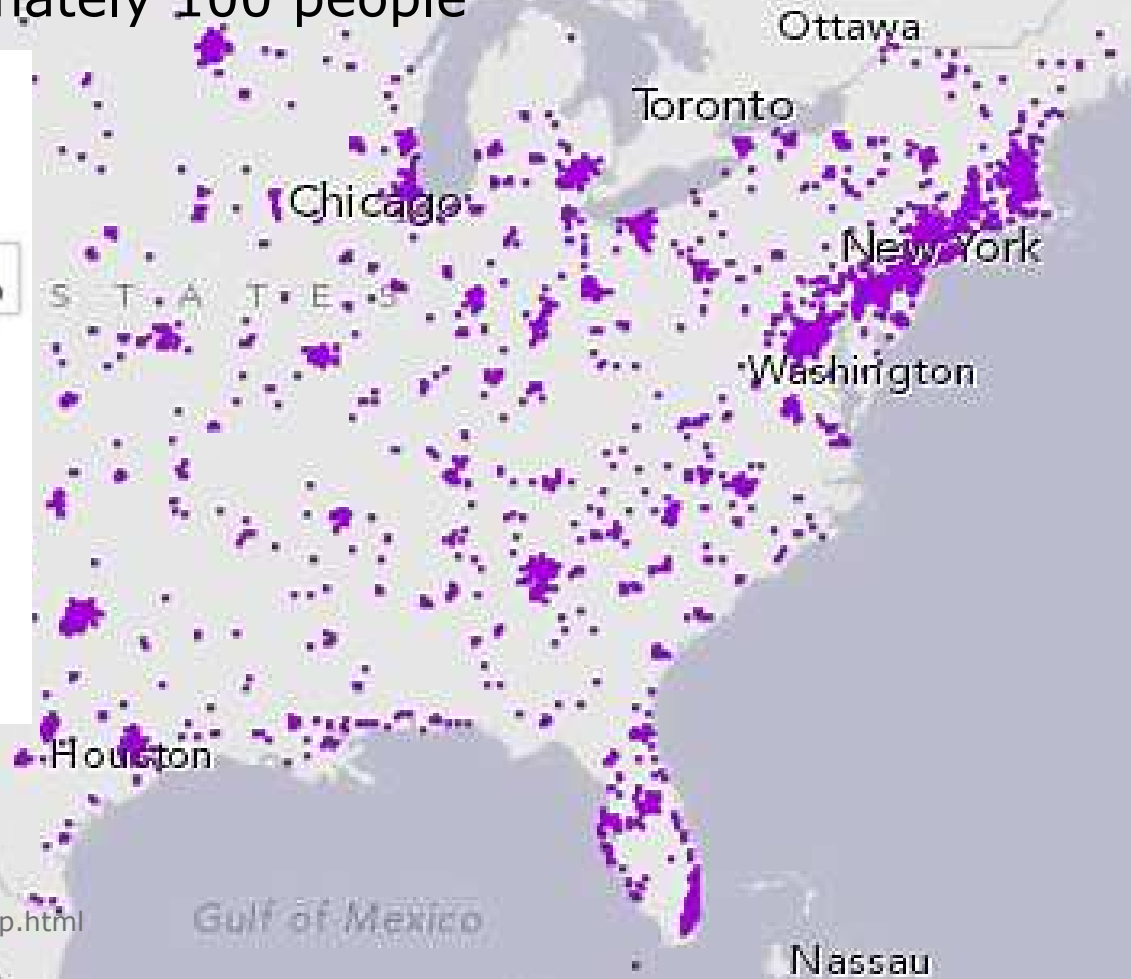
NATIVE CHINESE SPEAKERS

Each dot = approximately 100 people

Top Ten Languages on the Internet, May 2011



Source: Broadband Commission



SOCIAL ENGINEERING LINGUISTICS

419 Linguistic Attack Analysis: *Phonology*

Punctuation and spacing errors

- "I am elder son of . Maj.General Gwazo former Military chief Security officer"
- "send me a letter of **ofn**invitation, in other for me to get my Visa to join you up"

Capitalization errors

- "Dear **sir**, Before **i** start, **i** must first apologize"
- "I was oppertune and pleased to have come across your **C**ontact though this satellite media"

31

RSACONFERENCE 2010

419 Linguistic Attack Analysis: *Morphology*

Fancy words carefully spelled

- "my family has been subjected to all sorts of harassment and intimidation"
- "This money is now floating in the NPA domiciliary account"
- "Modalities have been worked out at the highest level"

De-contractions

- "Our status as refugees **does not** permit us to run an account here"
- "We **do not** know whom exactly to blame"
- "we **can not** leave the country"
- "my need to get **some one** to assist me"

32

RSACONFERENCE 2010

419 Linguistic Attack Analysis: *Syntax*

Insertion of infinitives

- "that made me **to** contact you"

Unusual word order

- "money **of which** I am in possession"
- "**Since after** the death of the Head of State"
- "we shall be **coming over** to your country"

Incorrect agreement

- "things **gets** better"
- "until my father is release"
- "The Federal Government **have** seized all our properties"

33

RSACONFERENCE 2010

419 Linguistic Attack Analysis: *Discourse*

Florid style

"I am glad to say that with the introduction of Internet and website, I was oppertune and pleased to have come across your Contact though this satellite media"

"I therefore personally, appeal to you seriously and religiously for your urgent assistance to move this money into your country where I believe it will be safe since we can not leave the country due to the restriction of movement imposed on my father and the members of our family by the Nigerian Government."

34

RSACONFERENCE 2010

AFF Language-Based Detection Rules

Linguistic Analysis	Real	Fraud
Misspellings	Frequent	Few
Contractions	Frequent	Few
Syntax	Correct	Incorrect
Florid Discourse	Some	Very

RSAC 2010

39

RSACONFERENCE 2010



EMC²

Pivotal



vmware



IF ATTRIBUTION
TO LANGUAGE
HARD (2)

THEN ATTRIBUTION
TO A NATIONAL
"SITUATION" (3)...



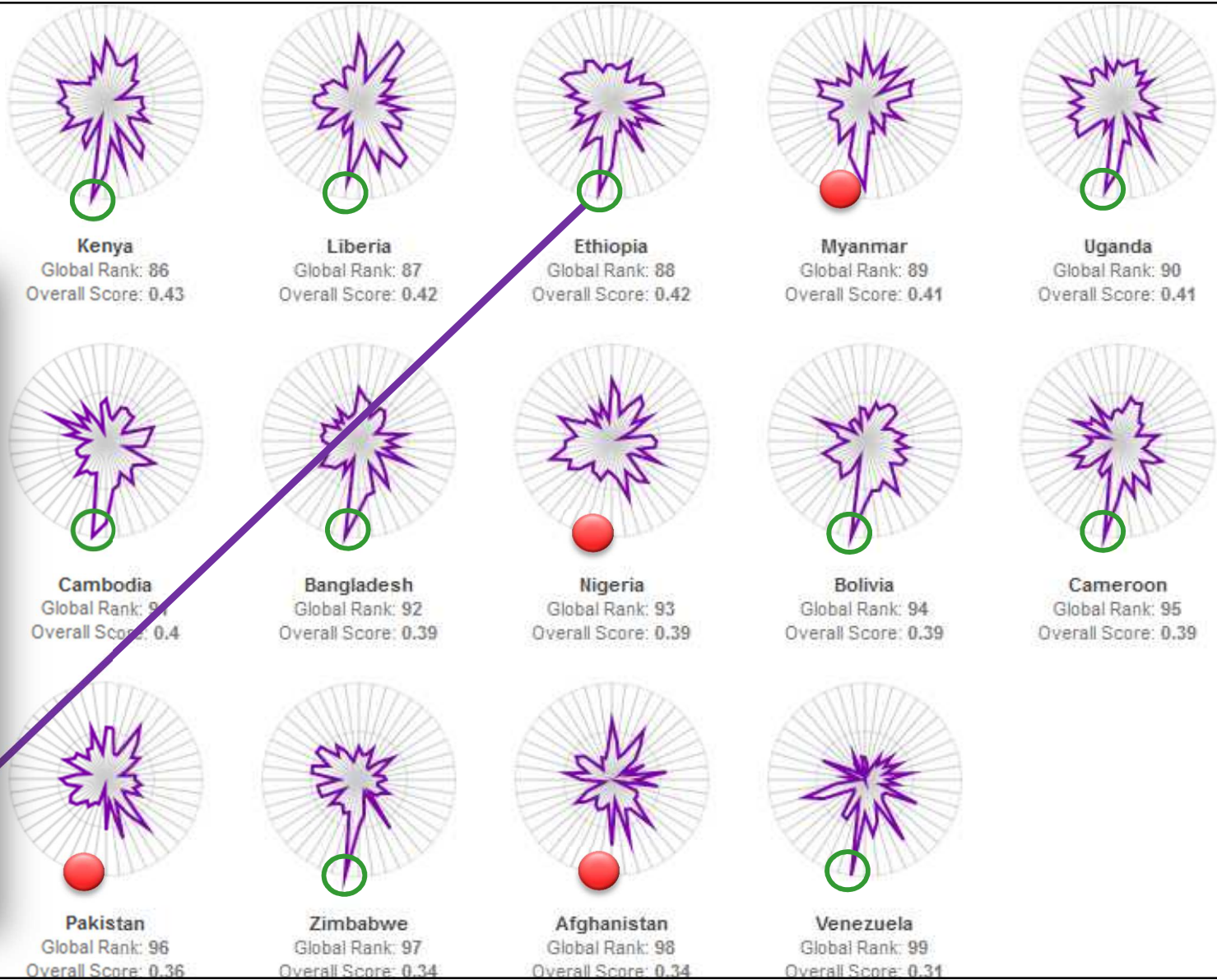
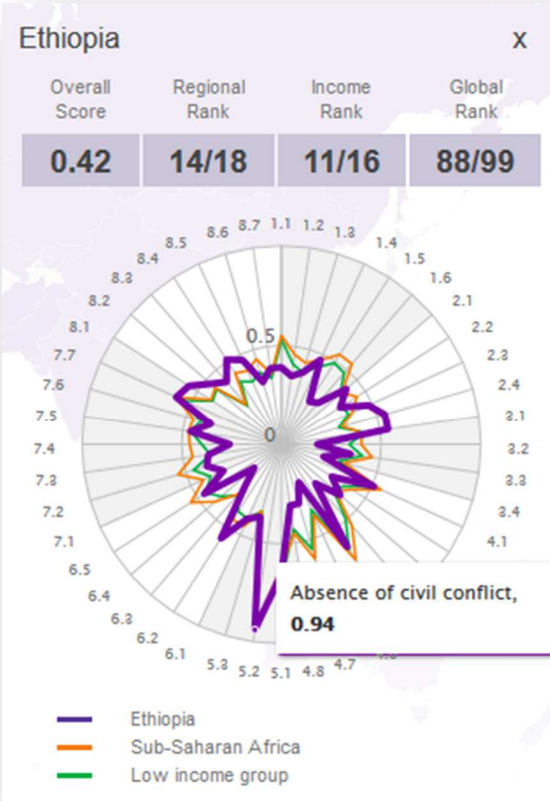
EMC²

Pivotal



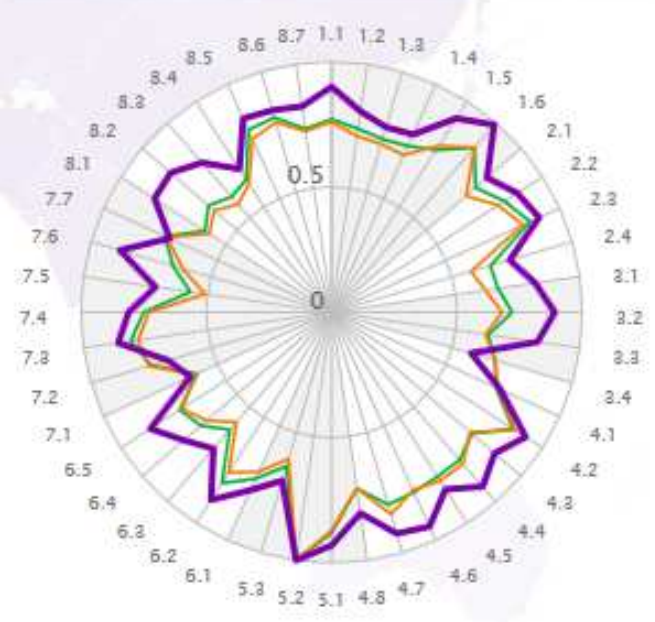
vmware[™]

SIUTATION ACCORDING TO worldjusticeproject



Austria x

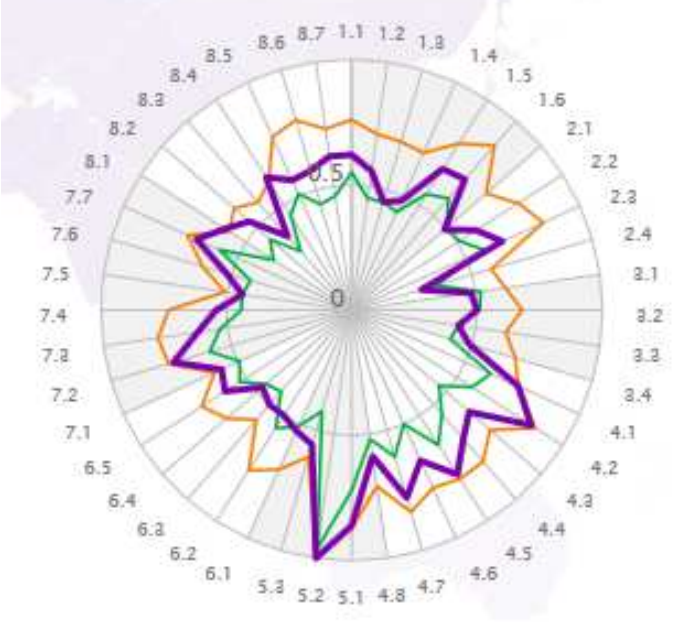
Overall Score	Regional Rank	Income Rank	Global Rank
0.82	6/24	7/30	7/99



- Austria
- Western Europe & North America
- High income group

Romania x

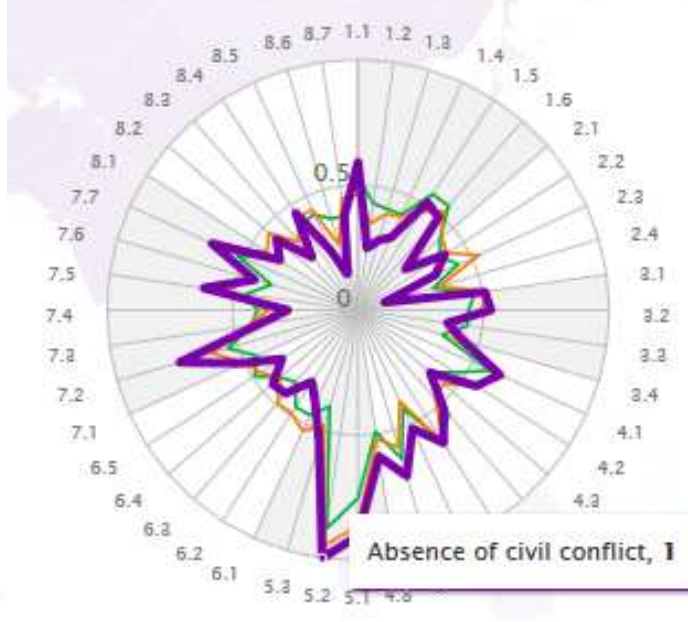
Overall Score	Regional Rank	Income Rank	Global Rank
0.59	22/24	3/29	33/99



- Romania
- Western Europe & North America
- Upper middle income group

Ukraine x

Overall Score	Regional Rank	Income Rank	Global Rank
0.47	8/13	13/24	68/99



- Ukraine
- Eastern Europe & Central Asia
- Lower middle income group



OOPS, UH, WE MEANT KOREAN...

“**CHINESE** Espionage Attacks Against Ruskies”

Dec 12, 11:12 am: ...**clues point to Chinese design and operation.** The malicious Word document sample that kicked this off was authored from a Microsoft Windows system that was set to use the **language pack** “Windows Simplified Chinese (PRC, Singapore). The researchers also say they were able to gain access to the control server used in the attack, which revealed **systems logging in from China** to check on new victims.

Update, 1:05 pm: FireEye just published a blog post about this research, which indicates they now believe the **likely source of this attack was Korea**, not China. The headline to this story has been modified.

<http://krebsonsecurity.com/2012/12/chinese-espionage-attacks-against-ruskies/#more-17850>



OOOPS, UH, WE MEANT...

China **Dragon** UAV

ANDIANT

This is what the pterodactyl looks like

“WHAT **PTERODACTYL** LOOKS LIKE”



2006 DRAGON

<http://www.flyingpenguin.com/?p=14880>



“Well, that is what it was bloody well designed to do, wasn't it?”

- Sir Frank Whittle
Inventor of the Jet Engine

1930 – Whittle UK patent

1935 – Nazi gov builds working model

http://www.eaa.org/warbirdsbriefing/articles/1211_frank-whittle-1942-jet-pioneer.asp



EMC²

Pivotal

RSA

vmware[®]

DEFENSE RESEARCH

DETECTION

AVOIDANCE



EMC²

Pivotal



vmware[™]

A person wearing a black balaclava and a red jacket is standing in a garage. The person is looking towards the camera. The background shows a white garage door, a bicycle, and various tools and equipment hanging from the ceiling. The word "DETECTION" is overlaid in large white letters with a black outline.

DETECTION

CAUGHT ON TAPE

VACATIONING COUPLE THWART BURGLAR

PHONE APP HELPS CATCH CROOK



EMC²

Pivotal



vmware[™]

CONTINUOUS AVAILABILITY & DATA PROTECTION

AVOIDANCE

<http://www.emc.com/collateral/demos/microsites/mediaplayer-video/continuous-operations-oracle-rac-emc-vplex.htm>



EMC² Pivotal RSA vmware

DEFENSE RESEARCH

KNOWLEDGE

PRIVACY



EMC²

Pivotal



vmware[®]

KNOWLEDGE



EMC²

Pivotal

RSA

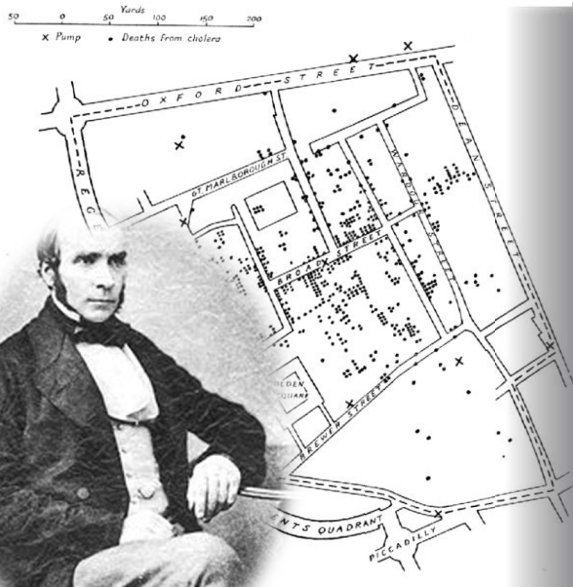
vmware[™]

A close-up photograph of a squirrel sitting on a grassy surface. The squirrel is holding three large walnuts in its mouth and paws. The squirrel has brown and tan fur with dark stripes on its back. The background is a soft, out-of-focus green. The word "GNAWLEDGE" is written in white, bold, sans-serif capital letters across the right side of the image.

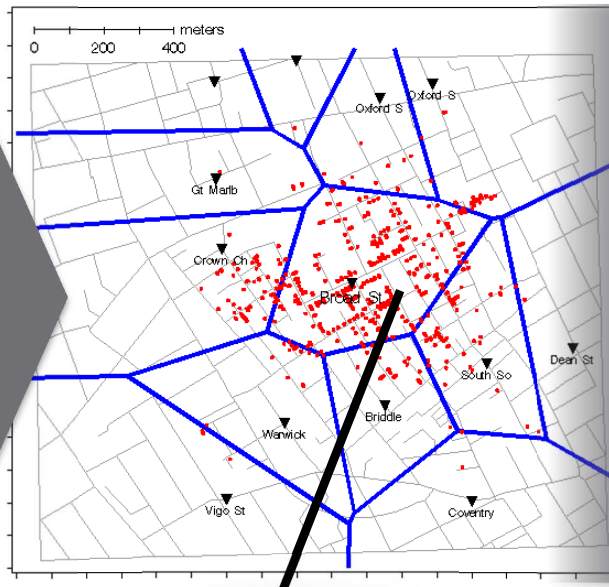
GNAWLEDGE

LESSONS FROM THE SNOW DEN

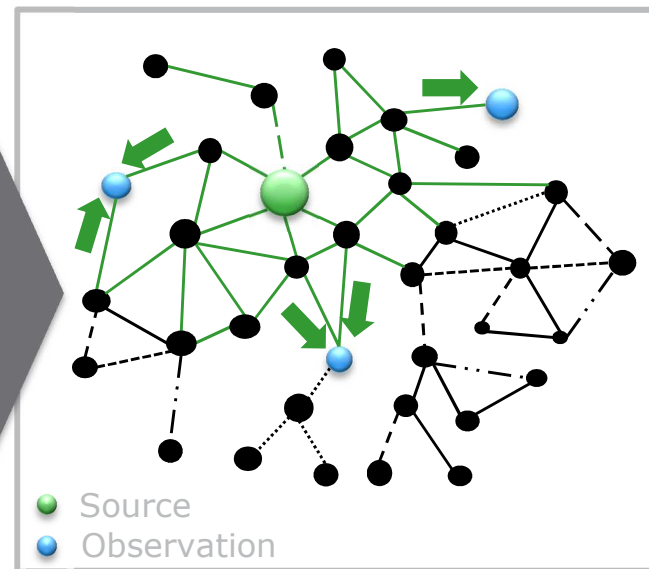
1854: GHOST MAP OF LONDON



1854: CHOLERA VORONOI



RSAC 2012: BREACH DATA



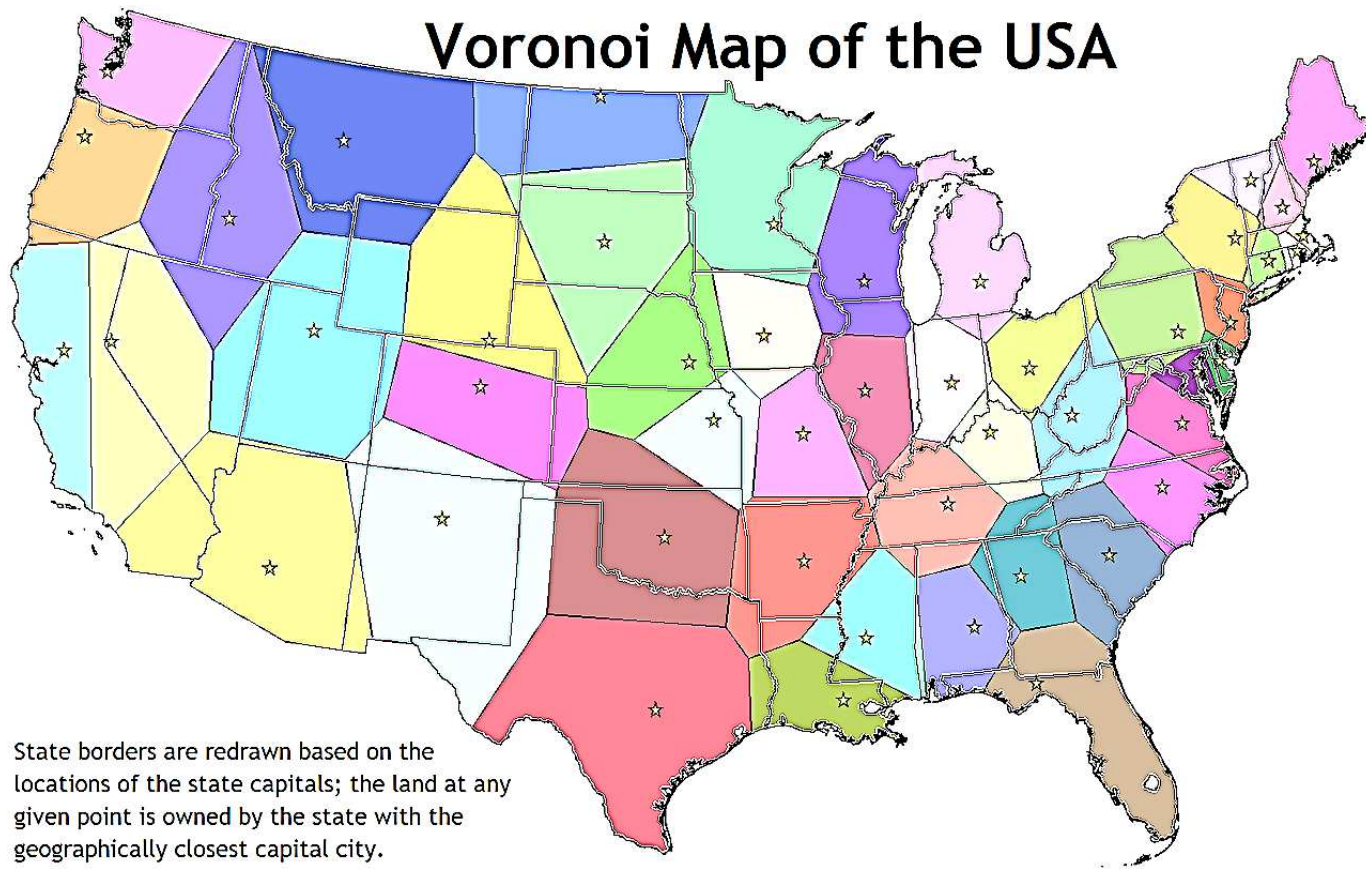
<http://www.flyingpenguin.com/?p=18259>

Dr. John Snow
1813-1858



FURTHEST POINT FROM POLITICIANS

Voronoi Map of the USA



State borders are redrawn based on the locations of the state capitals; the land at any given point is owned by the state with the geographically closest capital city.

<http://vizual-statistix.tumblr.com/post/48625446909/these-are-voronoi-maps-of-the-contiguous-usa>



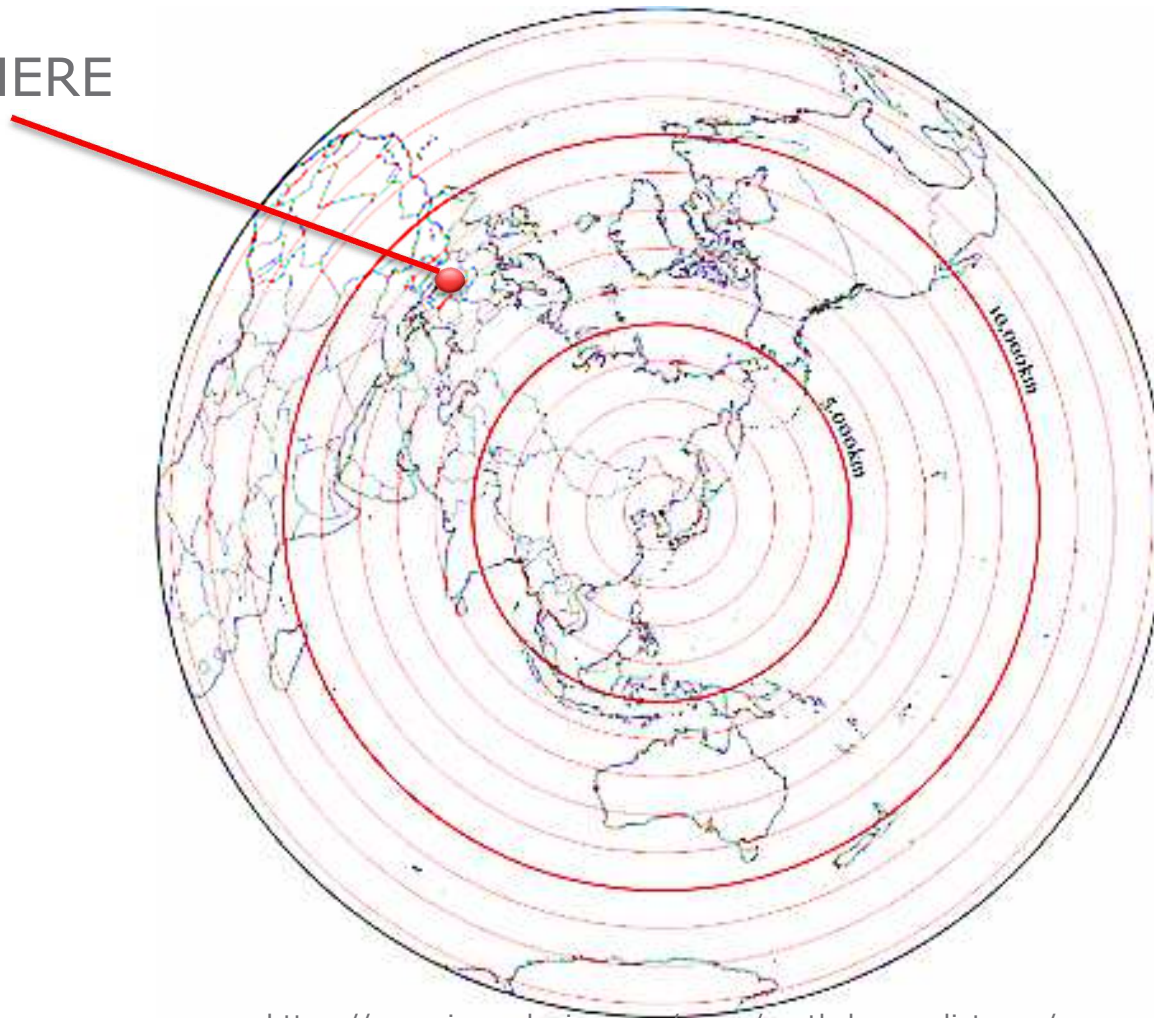
EMC²

Pivotal



vmware

YOU ARE HERE



<https://www.jasondavies.com/maps/north-korea-distance/>



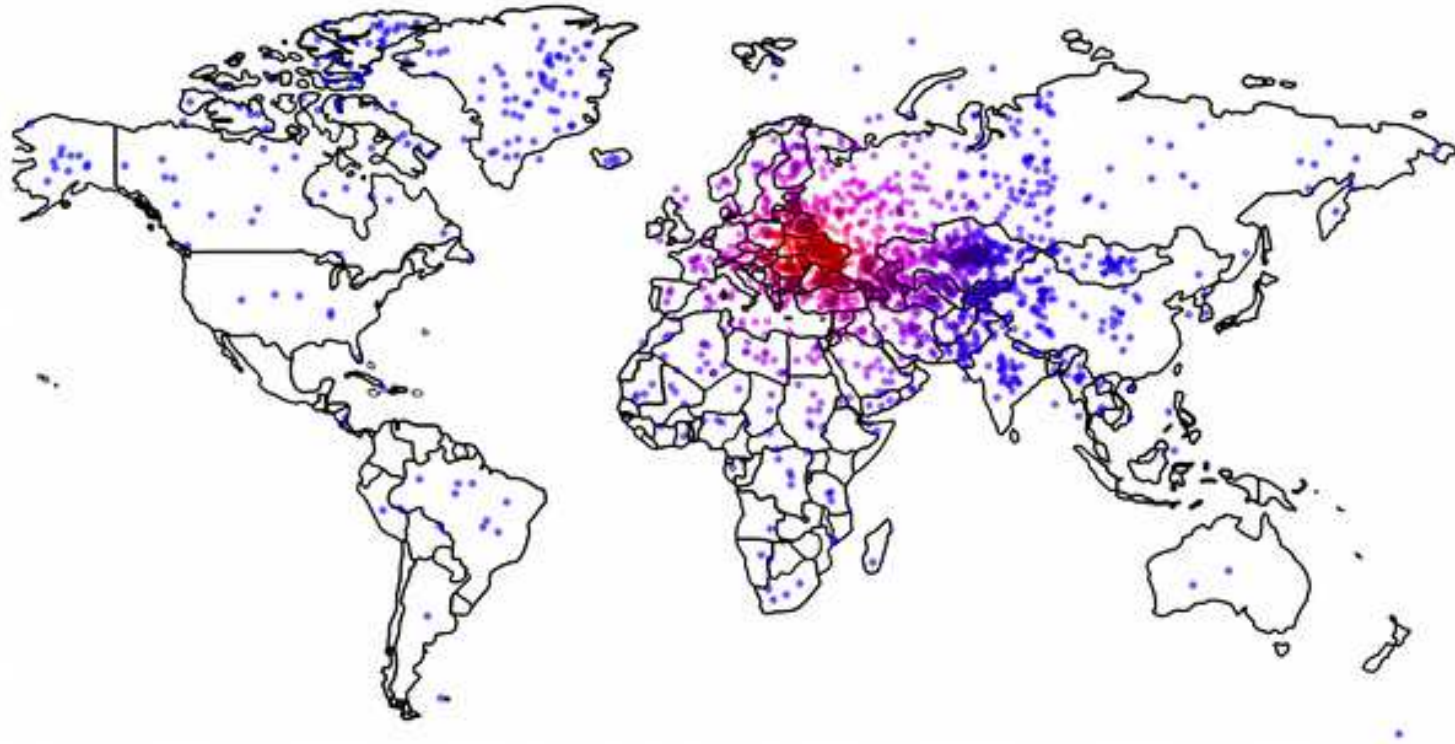
EMC²

Pivotal



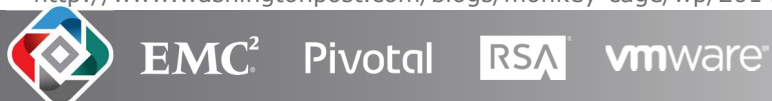
vmware


"THE LESS AMERICANS KNOW...THE MORE THEY WANT TO INTERVENE"



Where's Ukraine? Each dot depicts the location where a U.S. survey respondent situated Ukraine; the dots are colored based on how far removed they are from the actual country, with the most accurate responses in red and the least accurate ones in blue. (Data: Survey Sampling International; Figure: Thomas Zeitzoff/The Monkey Cage)

<http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/04/07/the-less-americans-know-about-ukraines-location-the-more-they-want-u-s-to-intervene/>



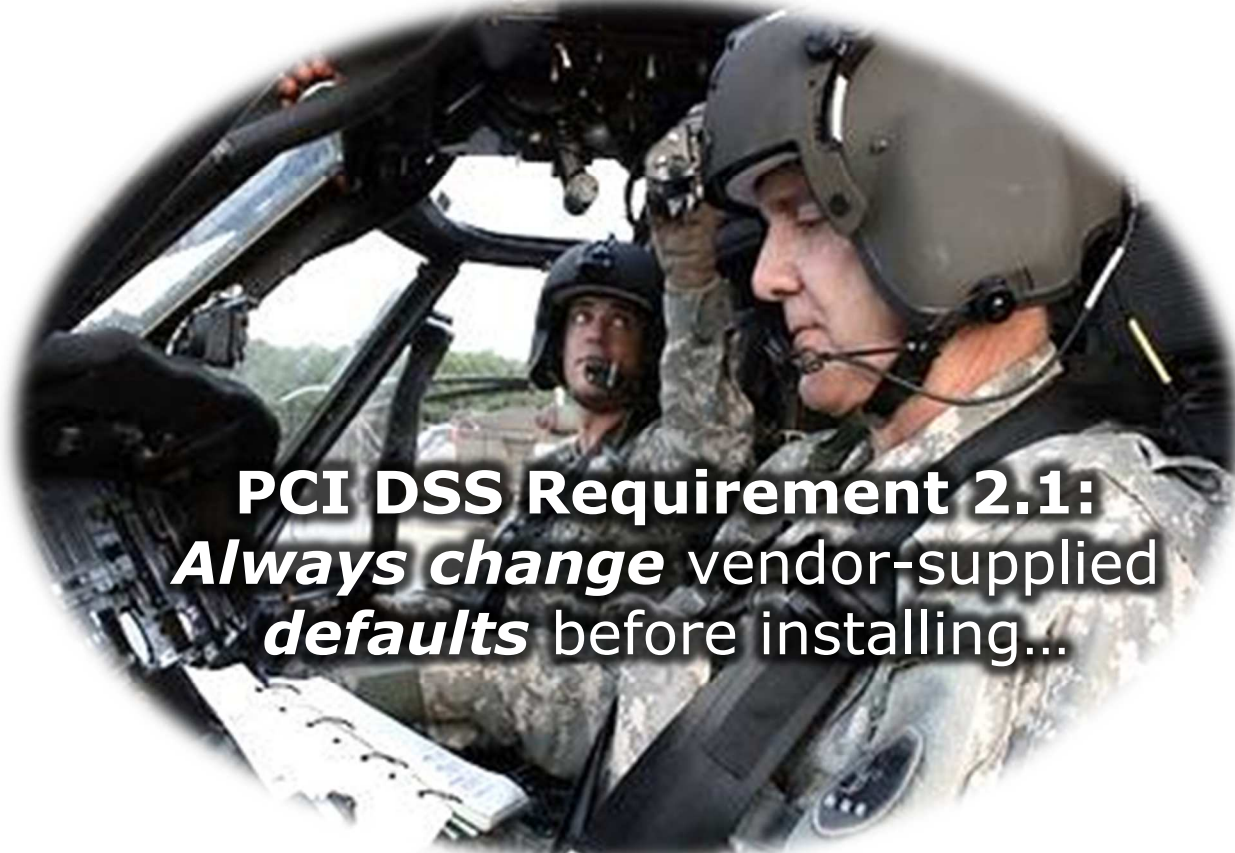


Give me six hours to chop
down a tree and I will
spend the first four
sharpening the axe.

Quellcrist Falconer

GNAWLEDGE

"SIMPLE" CHECKLISTS



PCI DSS Requirement 2.1:
Always change vendor-supplied
defaults before installing...

INTELLIGENT ANALYSIS



http://www.mdjonline.com/view/full_story/9738998/article-Father-trains-son--to-fly-helicopters-with-night-vision
<http://www.dvidshub.net/image/962244/oklahoma-national-guard-pilots-train-war-time-standard>



EMC²

Pivotal



vmware[®]

INTELLIGENT ANALYSIS AT SCALE

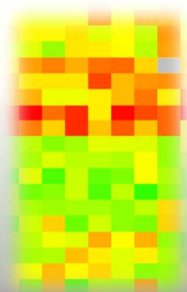
BINARY



RANKED



MEANING



ZERO
POINT



EXACT



ERROR MARGIN

INTELLIGENCE

CAVEAT: "NO FISH IN TOO CLEAR WATER"



EMC²

Pivotal



vmware[™]

NYC FIRE ATTRIBUTION

3,000 Major Fires / Year
1,000,000 Buildings (330K Inspected)

2013

- Random Inspections
- **60 Factors**

2014

- Inspections by Rank
- **2400 Factors**

“Low-income neighborhoods are correlated with fires”

- Jeff Chen, NYFD Director of Analytics

<http://blogs.wsj.com/digits/2014/01/24/how-new-yorks-fire-department-uses-data-mining/>



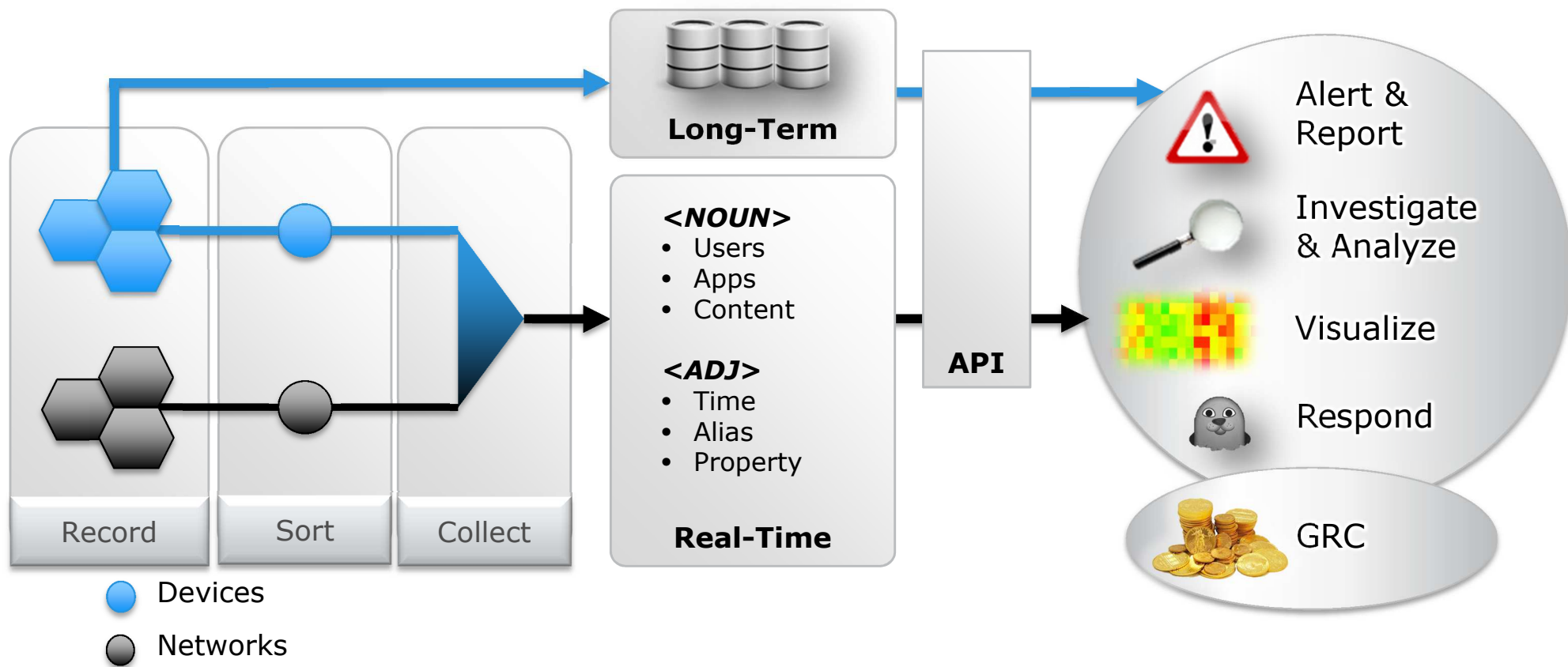
EMC²

Pivotal

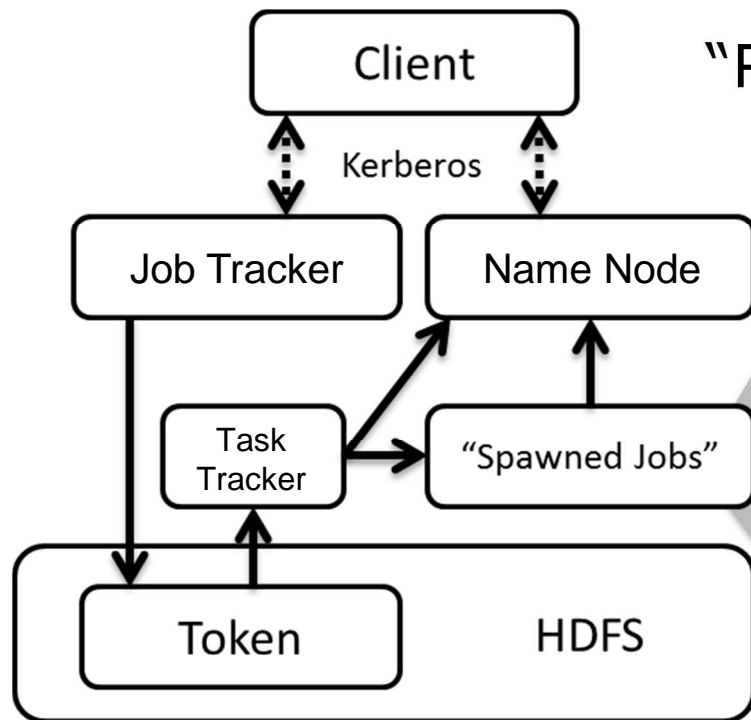
RSA

vmware

INTELLIGENCE REDEFINES KNOWLEDGE



EVEN KNOWLEDGE OF REPLICANTS



“Runaway Job! Kill -9”



EMC²

Pivotal

RSA

vmware

PRIVACY



EMC²

Pivotal



vmware[™]

THE FAR SIDE® BY GARY LARSON



The Far Side® by Gary Larson © 1994 FarWorks, Inc. All Rights Reserved. Used with permission

Anthropologists!
Anthropologists!



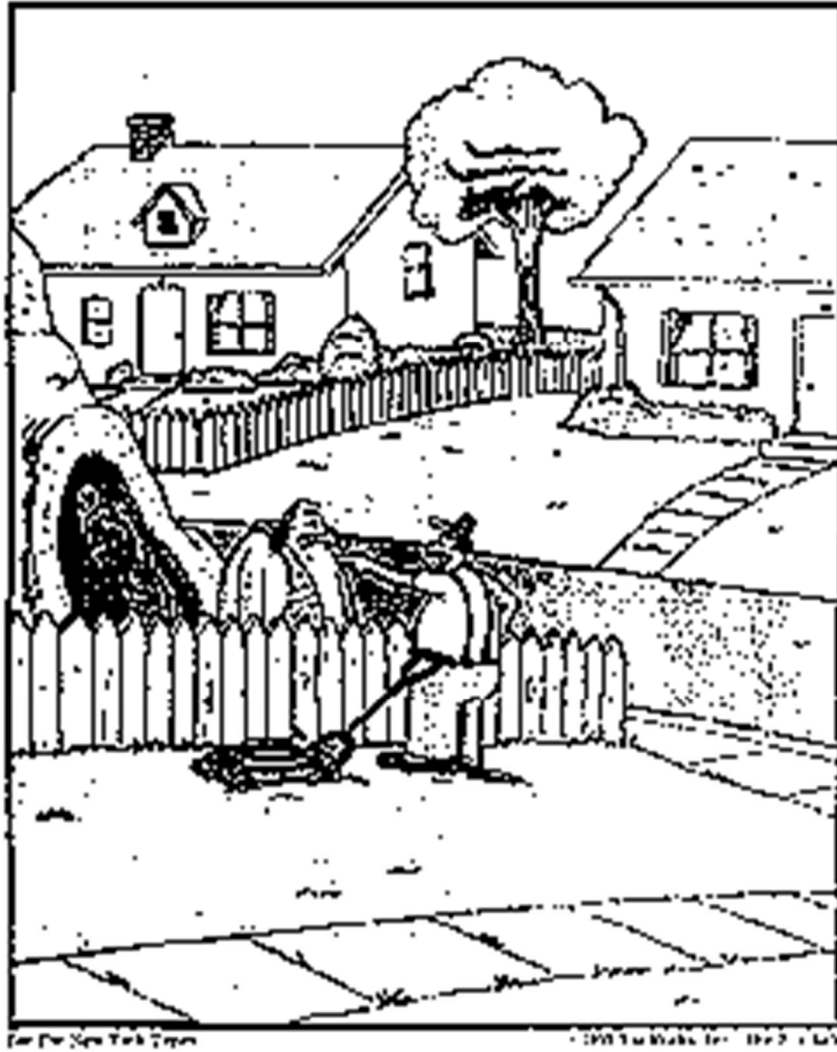
EMC²

Pivotal



vmware

THE FAR SIDE® BY GARY LARSON



Don't threaten me,
Thagerson!

My cousin's an
anthropologist
and she can make
your life hell!

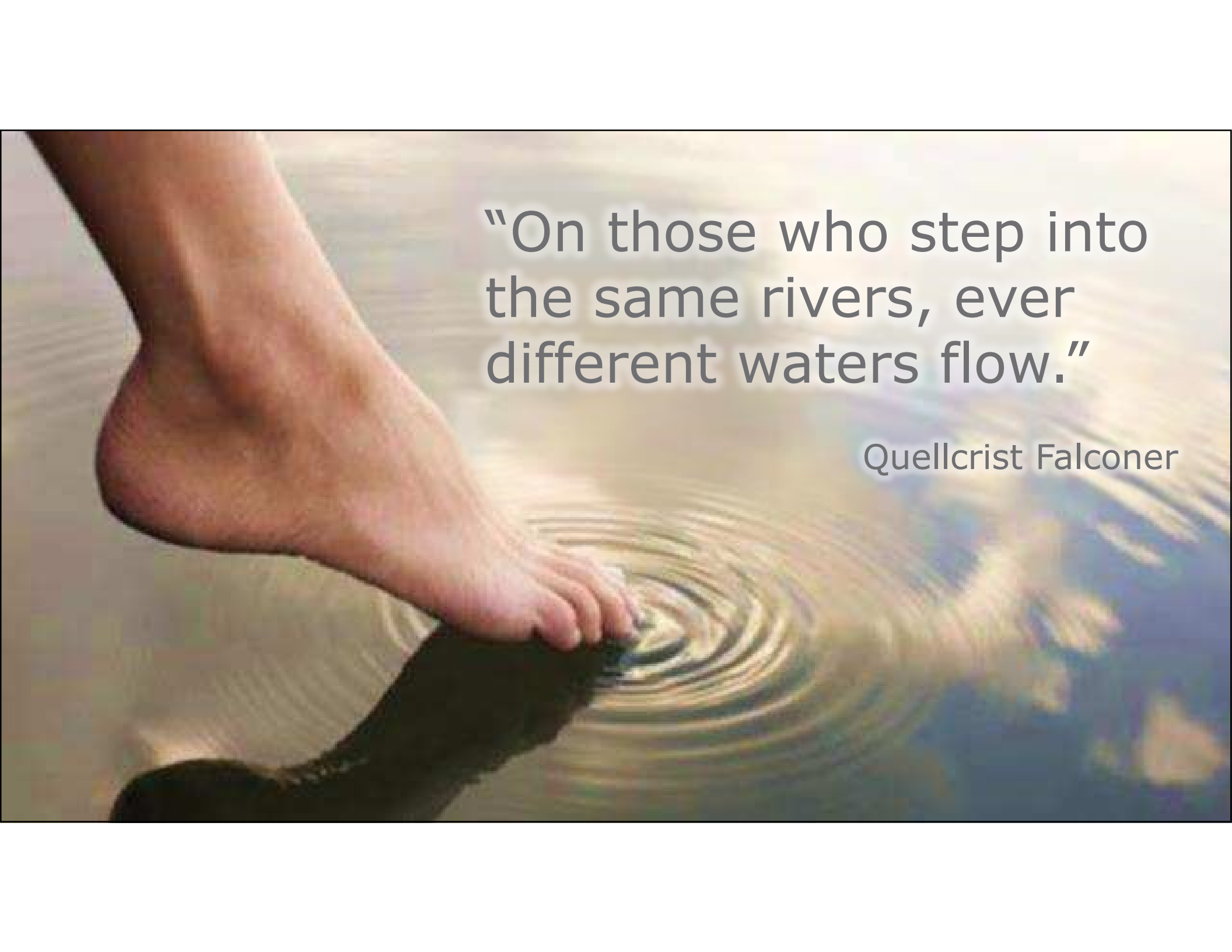


EMC²

Pivotal



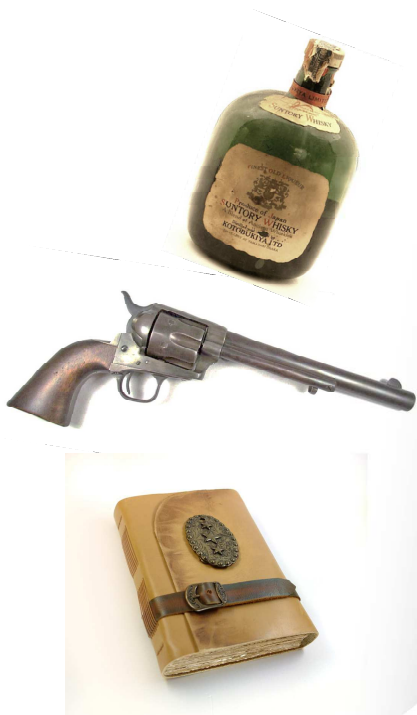
vmware



“On those who step into
the same rivers, ever
different waters flow.”

Quellcrist Falconer

KONZA WASTE ARCHAEOLOGY



<http://www.imagekind.com/art/stunning/flint-hills/artwork-on/fine-art-prints>



EMC²

Pivotal

RSA

vmware

© Copyright 2014 EMC Corporation. All rights reserved.

REAL-TIME WASTE ARCHAEOLOGY



<http://gizmodo.com/meth-in-london-heroin-in-zagreb-the-answer-is-found-i-1508209127>



EMC²

Pivotal

RSA

vmware

“ONE CLICK”

“**Ad blocking** to me is so fundamentally wrong, it just boils my blood...fundamental **threat** that it is.”

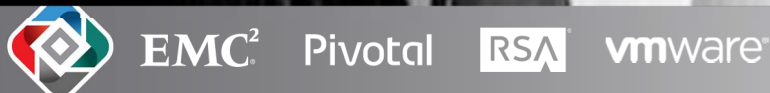
General Counsel and EVP Public Policy

Interactive Advertising Bureau

“We Googled my name, and up popped an ad suggesting I had an arrest record. I do not.”

<http://phys.org/news/2013-05-fairness-ads-outlines-bias-score.html>

<http://www.cnet.com/news/ad-blockers-get-ad-group-execs-blood-boiling-q-a/>



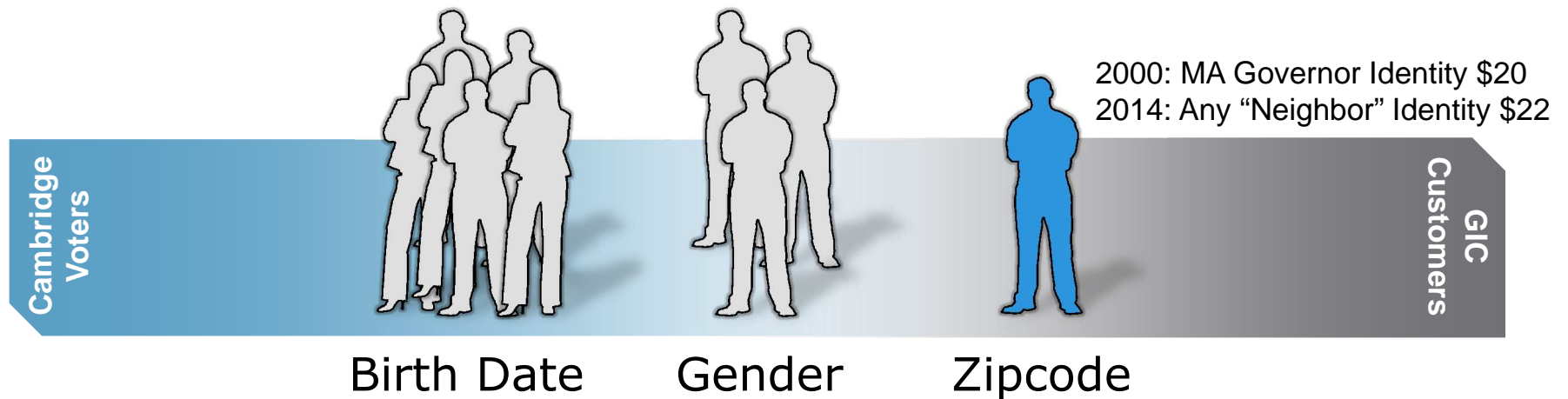
RE-IDENTIFICATION

- 53% IDs Unique
DOB + Sex + City
- 87% IDs Unique
DOB + Sex + Zip
- Minimums Advised:
State, Year

“Few Characteristics Needed”

Latanya Sweeney, 2000

THE AGE OF "RE-IDENTIFICATION"



Voter Registration / Group Insurance Commission (GIC) Data

<http://dataprivacylab.org/projects/identifiability/index.html>

<http://www.uclalawreview.org/?p=1353>

<http://www.zeit.de/2014/07/harald-martenstein-datenschutz>



EMC²

Pivotal

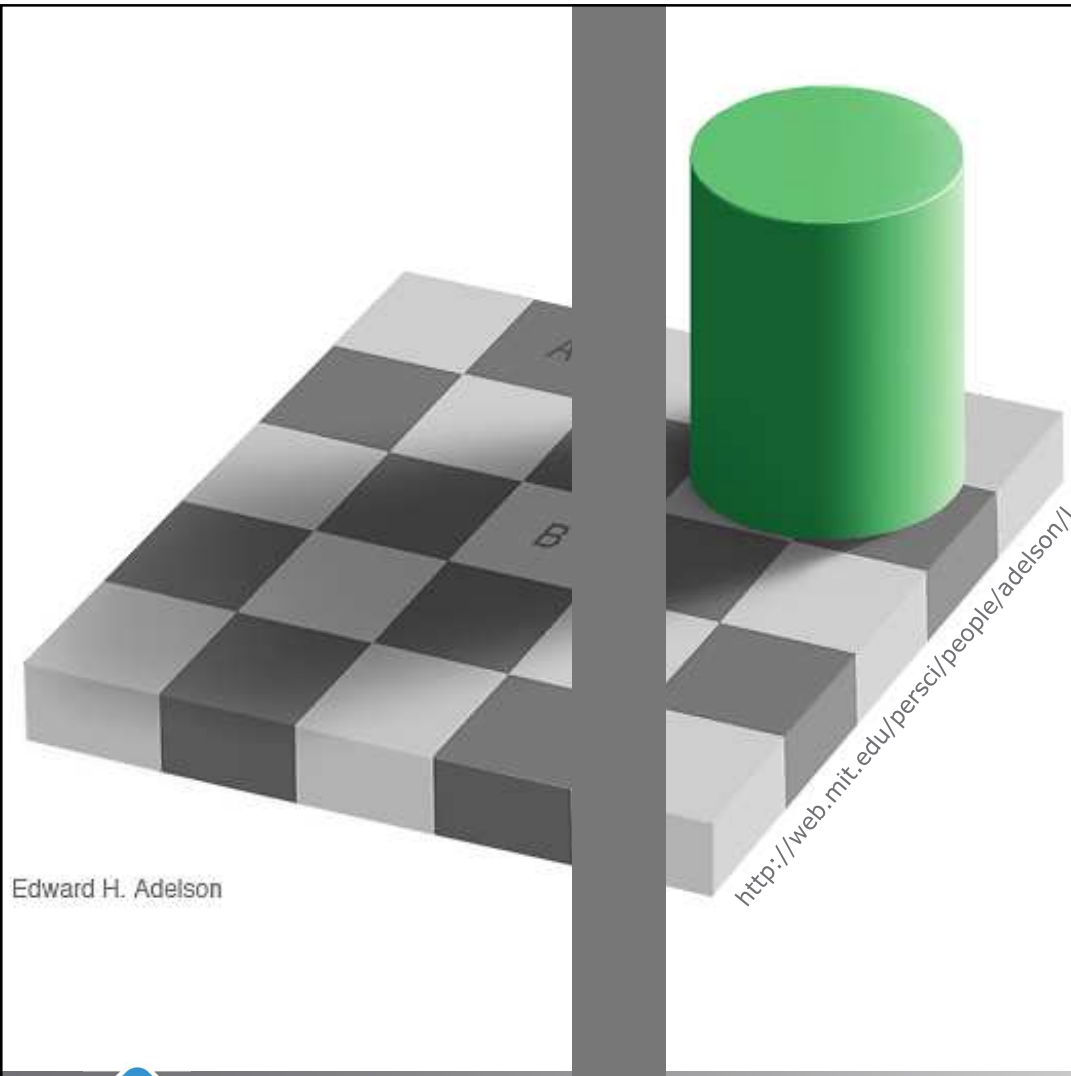
RSA

vmware

UNCERTAINTY OF ATTRIBUTION

Finding the Needle
in the Needlestack

Davi Ottenheimer
@daviottenheimer
Vienna, April 2014



Edward H. Adelson



EMC²

Pivotal



vmware



EMC²

Pivotal

RSA[®]

vmware[®]

Thank you!