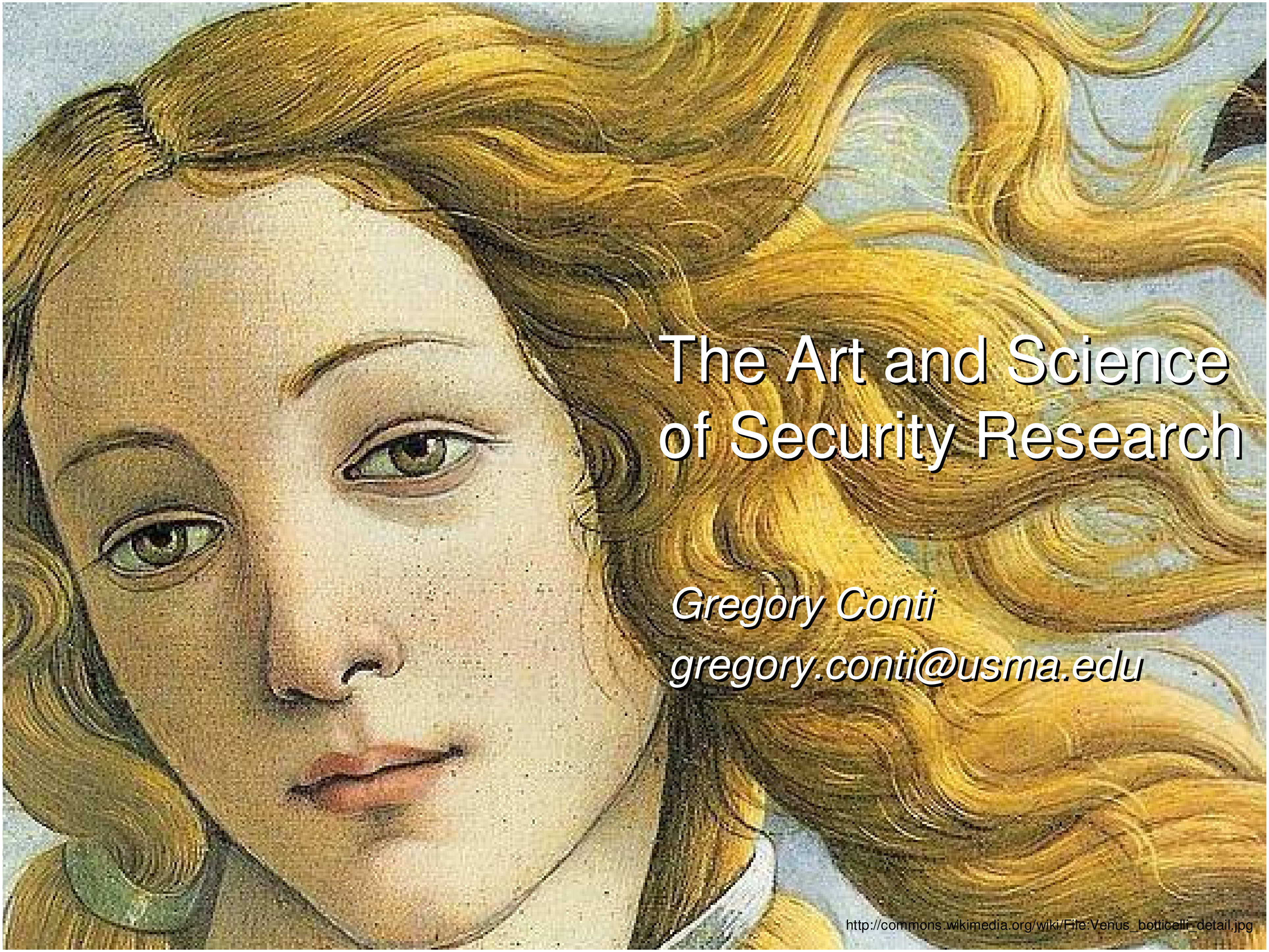
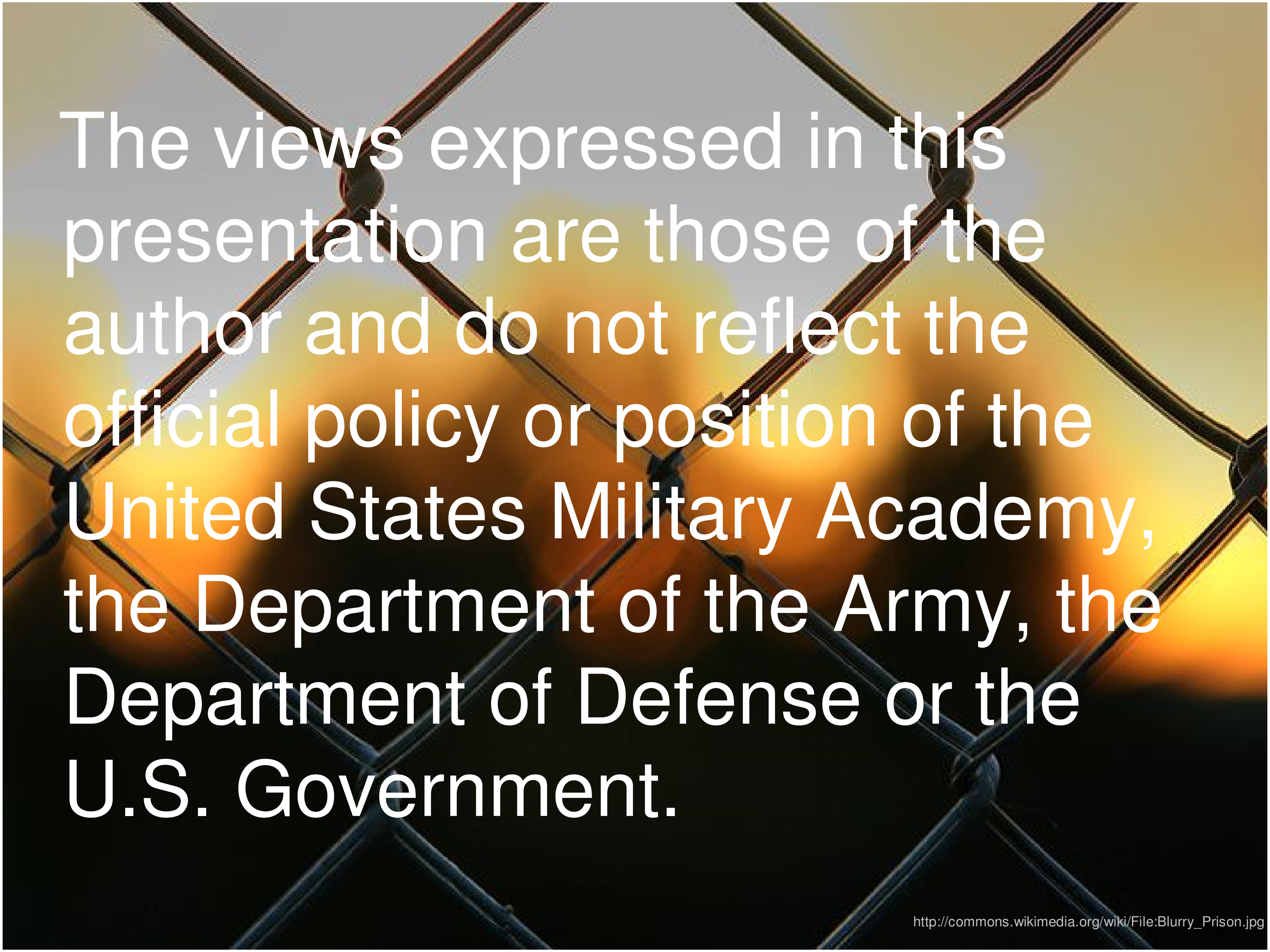


The Art and Science of Security Research

Gregory Conti

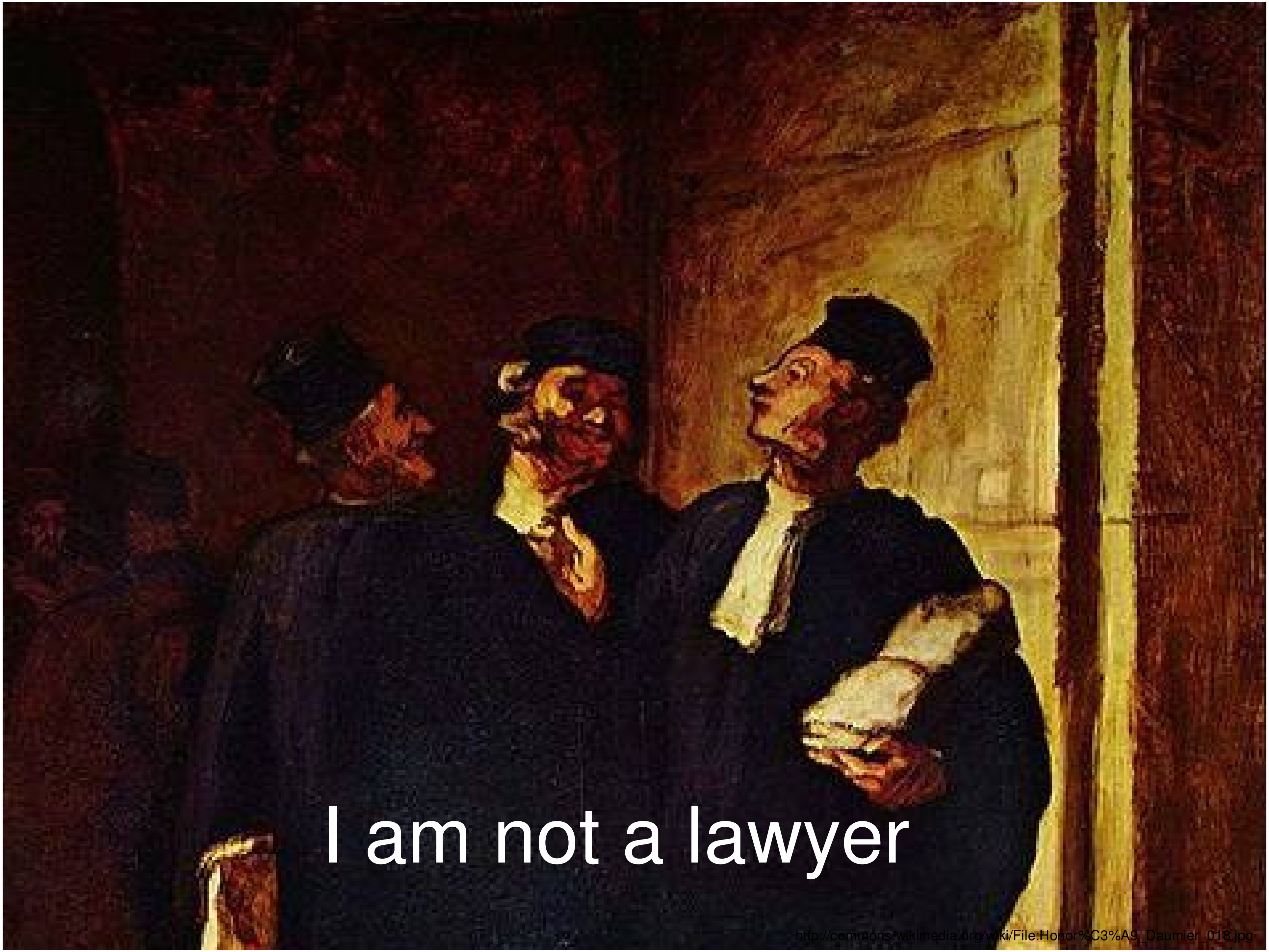
gregory.conti@usma.edu

http://commons.wikimedia.org/wiki/File:Venus_botticelli_detail.jpg



The views expressed in this presentation are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense or the U.S. Government.

http://commons.wikimedia.org/wiki/File:Blurry_Prison.jpg



I am not a lawyer

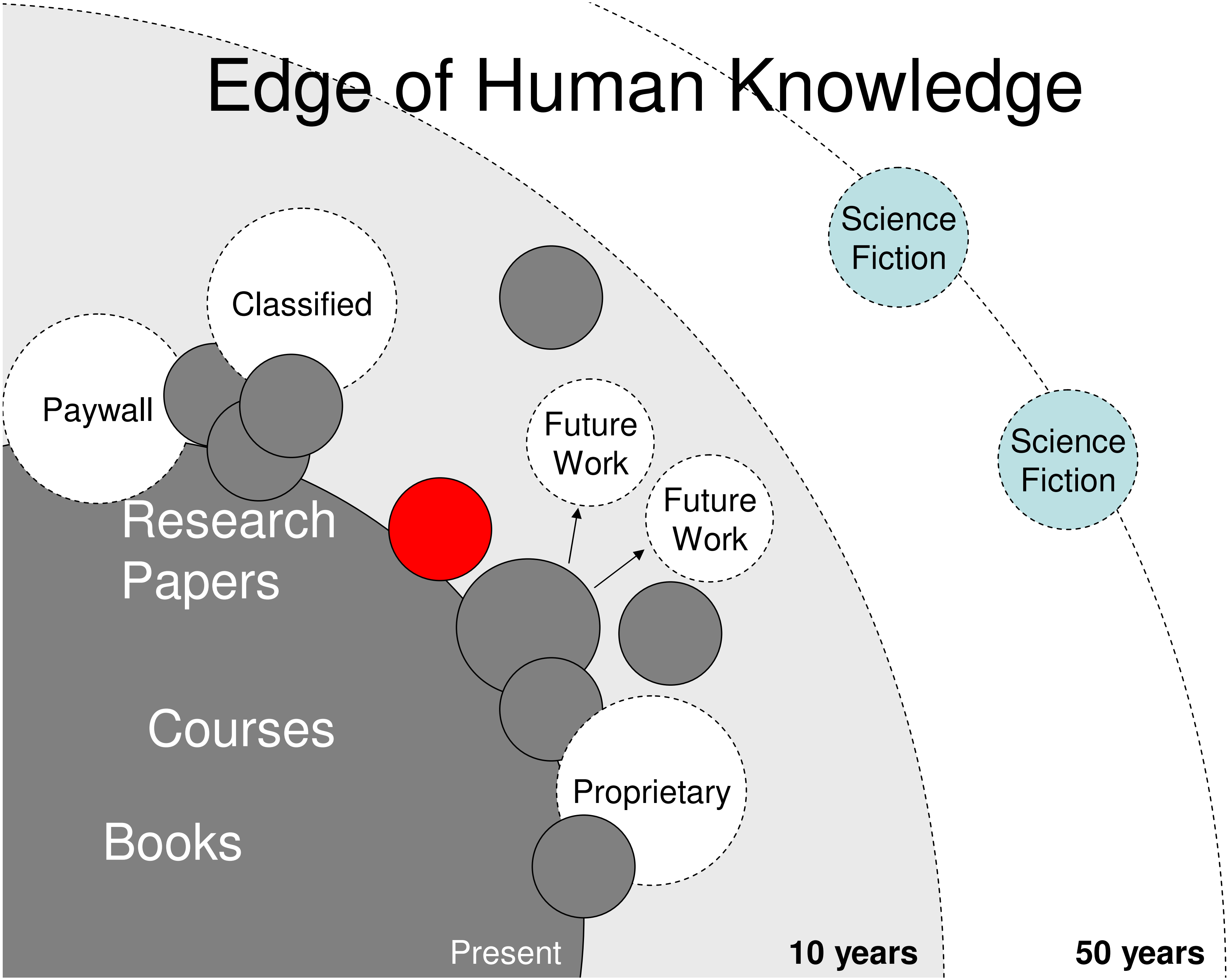
http://commons.wikimedia.org/wiki/File:Honor%C3%A9_Daumier_018.jpg

What is Research?

The search for knowledge, with an open mind, to establish novel facts, solve new or existing problems, prove new ideas, or develop new theories, usually using a scientific method.

http://en.wikipedia.org/wiki/Research

Edge of Human Knowledge



Why Research?

- Advance human knowledge
- Give back, so others can take your work to the next level
- Make yourself an expert
- Valuable skill set
- Fun and rewarding
- Get credit, notoriety, profit
- Build you resume
- You are already doing the work

http://commons.wikimedia.org/wiki/File:Beakers.jpg

What hackers bring to the table…

- Native curiosity
- Cleverness
- Color outside the lines
- Hackers do great work
- Less constraints, Less fear
- Freedom to choose problems that industry or academia can't/won't touch
- Hackers can build things
- Inspiration and obsession
- Devious minds
- Interesting ideas
- Access to interesting data
- Interesting acquaintances

http://commons.wikimedia.org/wiki/File:Noise_makers.jpg
http://commons.wikimedia.org/wiki/File:Lamborghini_Revent%C3%B3n_coloring.jpg

Seek to be the World Expert

> "In fact, researchers have settled on what they believe is the magic number for true expertise: ten thousand hours."
>
> \- Malcolm Gladwell
> Outliers

- Or at least an expert
- N world experts in the room
- Momentum
- Once at edge you will see problems (and solutions) that others don't know exist

Depth vs. Breadth

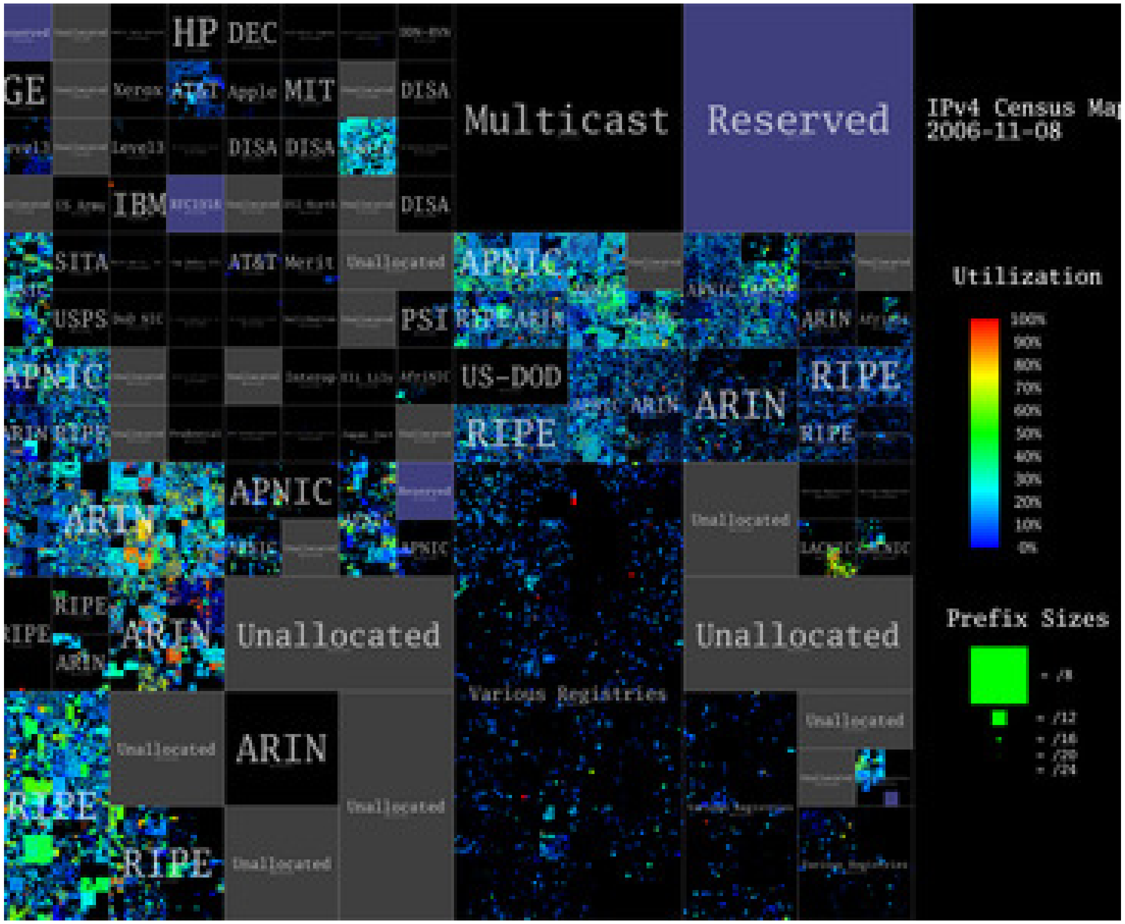
http://en.wikipedia.org/wiki/File:D%26D_Game_1.jpg

Strategies for Finding Problems

Challenge Assumptions

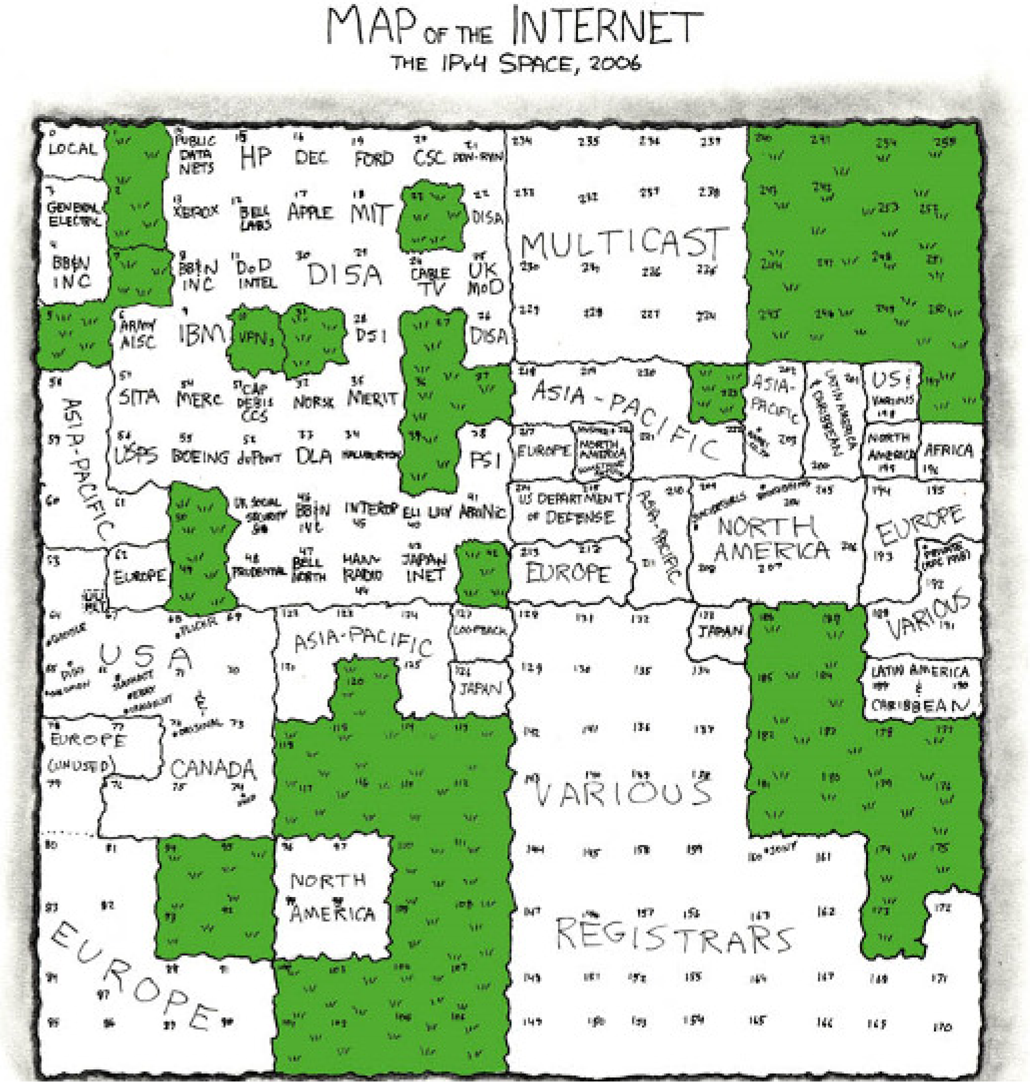
http://peshawar.olx.com.pk/we-have-ready-stock-of-used-hard-disk-40gb-80gb-iid-21611687

Think Big



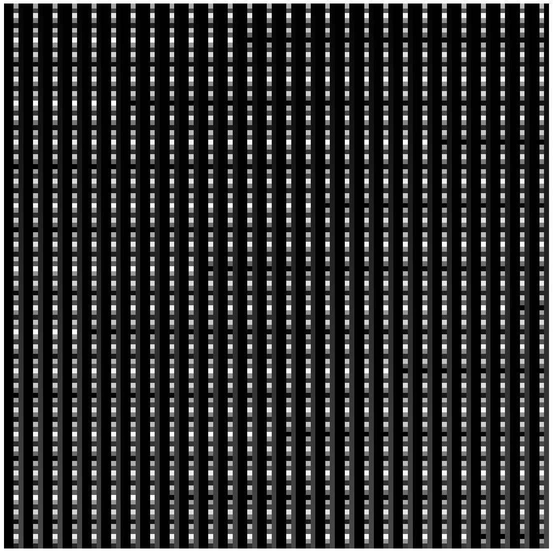
Cooperative Association for Internet Data Analysis (CAIDA)
2007 IPv4 Census Map (two-month ping sweep)

http://www.caida.org/research/id-consumption/census-map/

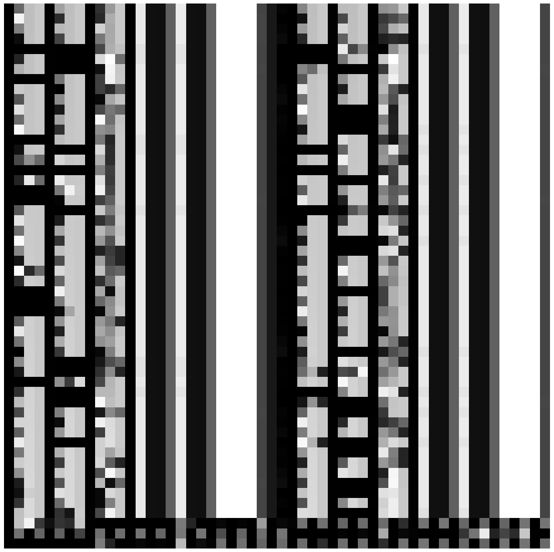


http://xkcd.com/195/

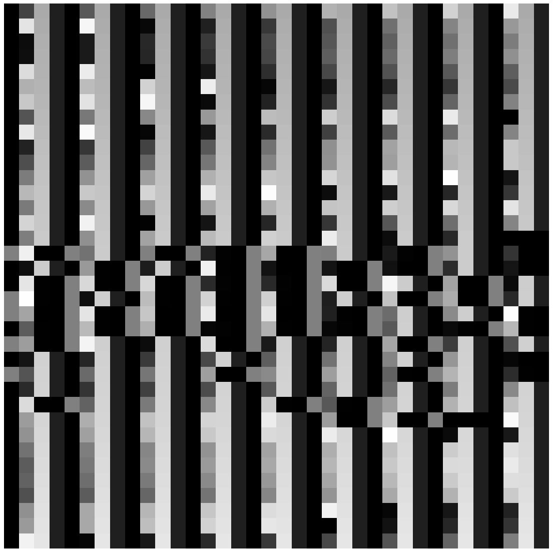
Think Small



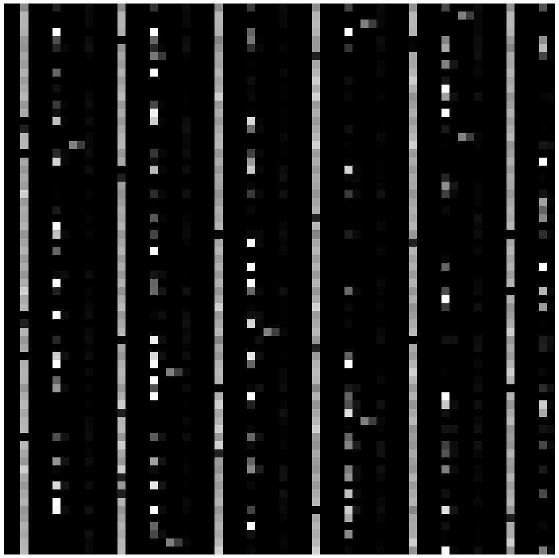
Microsoft Word 2003 .doc



Firefox Process Memory



Windows .dll

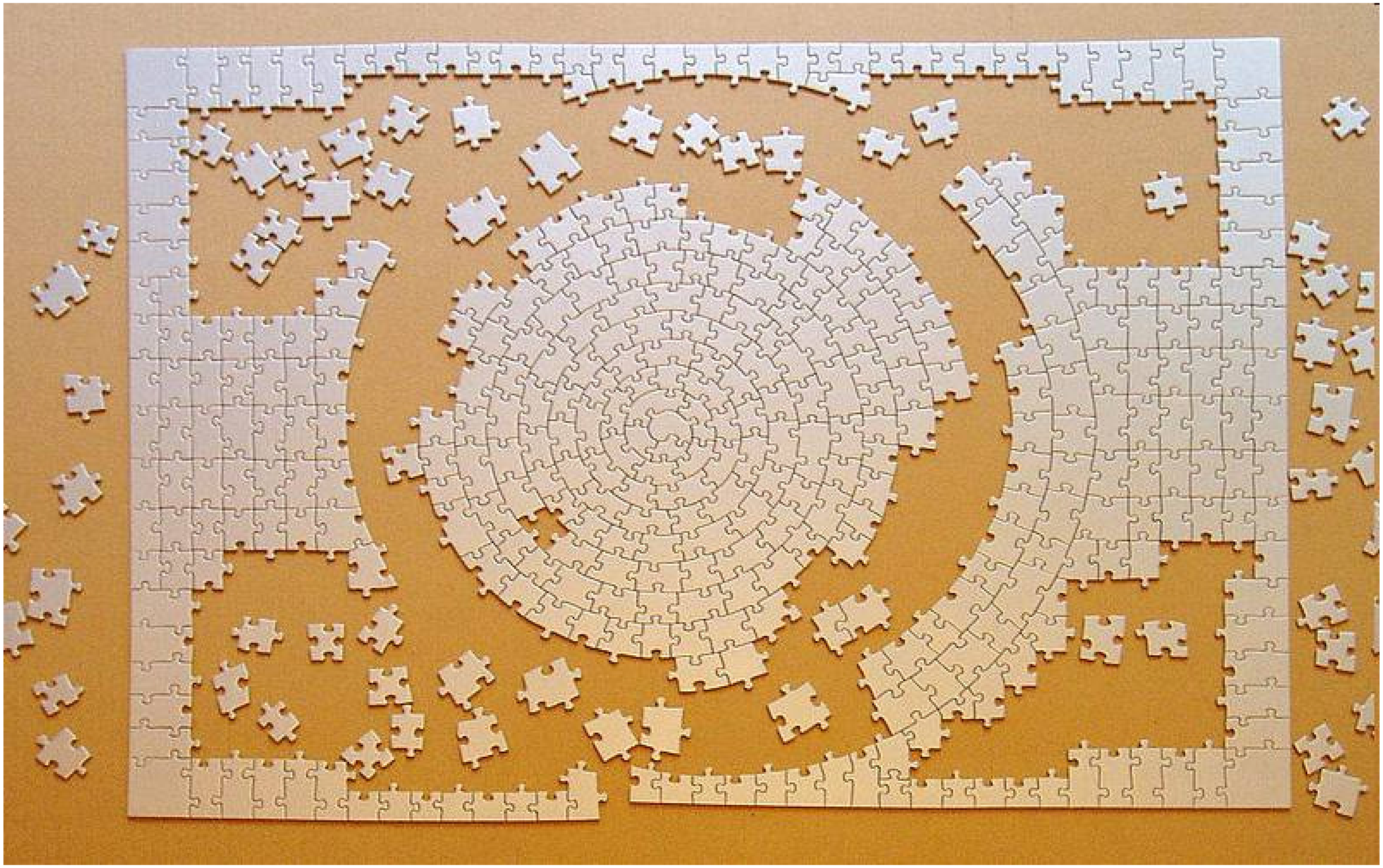


Neverwinter Nights Database

Irritate Software, Hardware, Protocols, and People

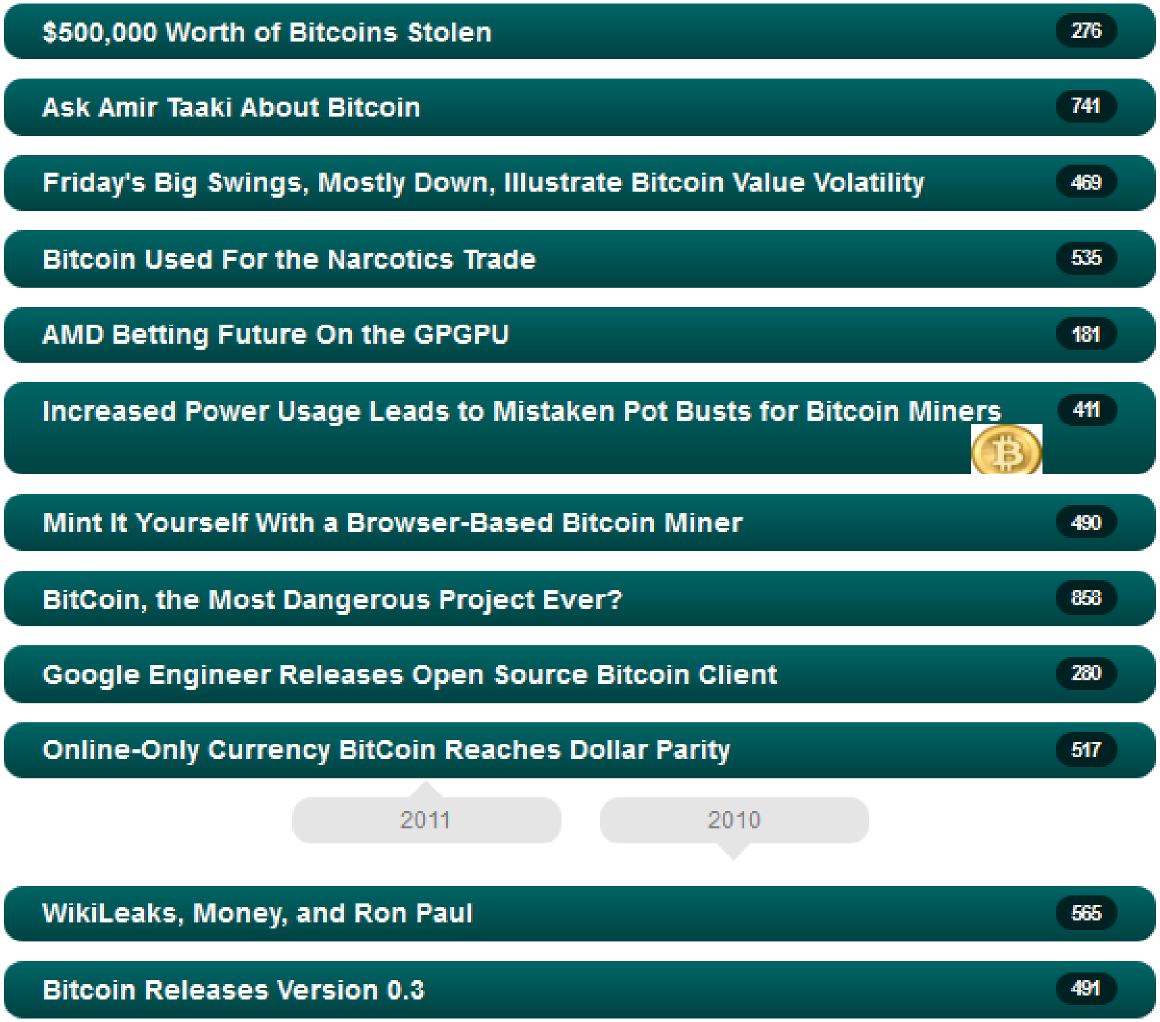
http://commons.wikimedia.org/wiki/File:Pearl_oyster.jpg

Detect Patterns



http://commons.wikimedia.org/wiki/File:Puzzle_Krypt-2.jpg

Detect Patterns



$500,000 Worth of Bitcoins Stolen	276
Ask Amir Taaki About Bitcoin	741
Friday's Big Swings, Mostly Down, Illustrate Bitcoin Value Volatility	469
Bitcoin Used For the Narcotics Trade	535
AMD Betting Future On the GPGPU	181
Increased Power Usage Leads to Mistaken Pot Busts for Bitcoin Miners	411
Mint It Yourself With a Browser-Based Bitcoin Miner	490
BitCoin, the Most Dangerous Project Ever?	858
Google Engineer Releases Open Source Bitcoin Client	280
Online-Only Currency BitCoin Reaches Dollar Parity	517

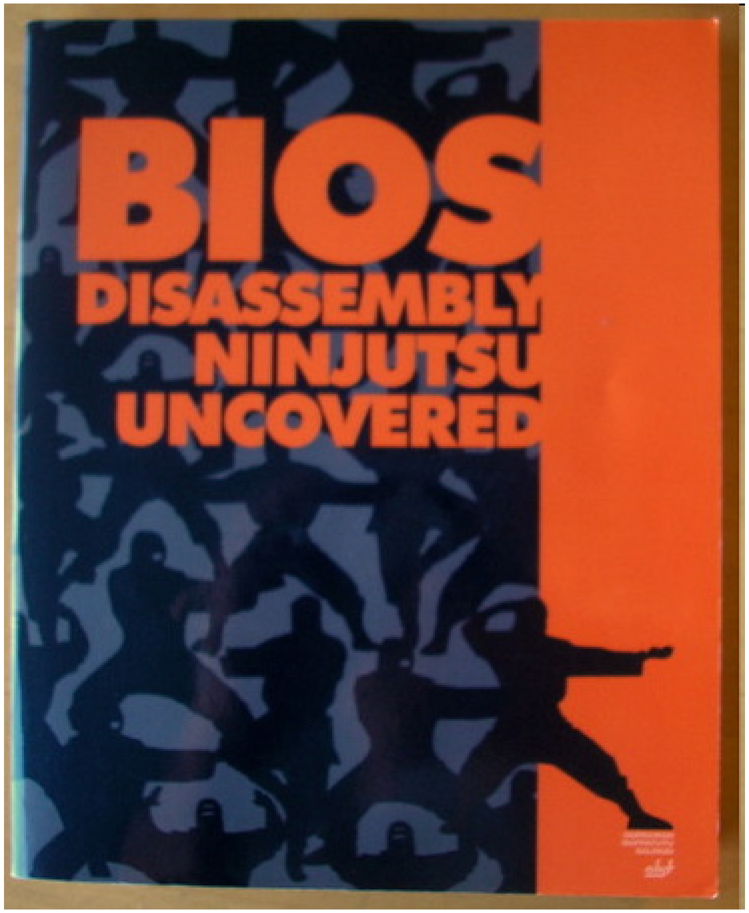
2011 2010

WikiLeaks, Money, and Ron Paul	565
Bitcoin Releases Version 0.3	491

http://slashdot.org/index2.pl?fhfilter=bitcoin

http://justindupre.com/sunday-squakbox-what-are-your-thoughts-on-bitcoin/

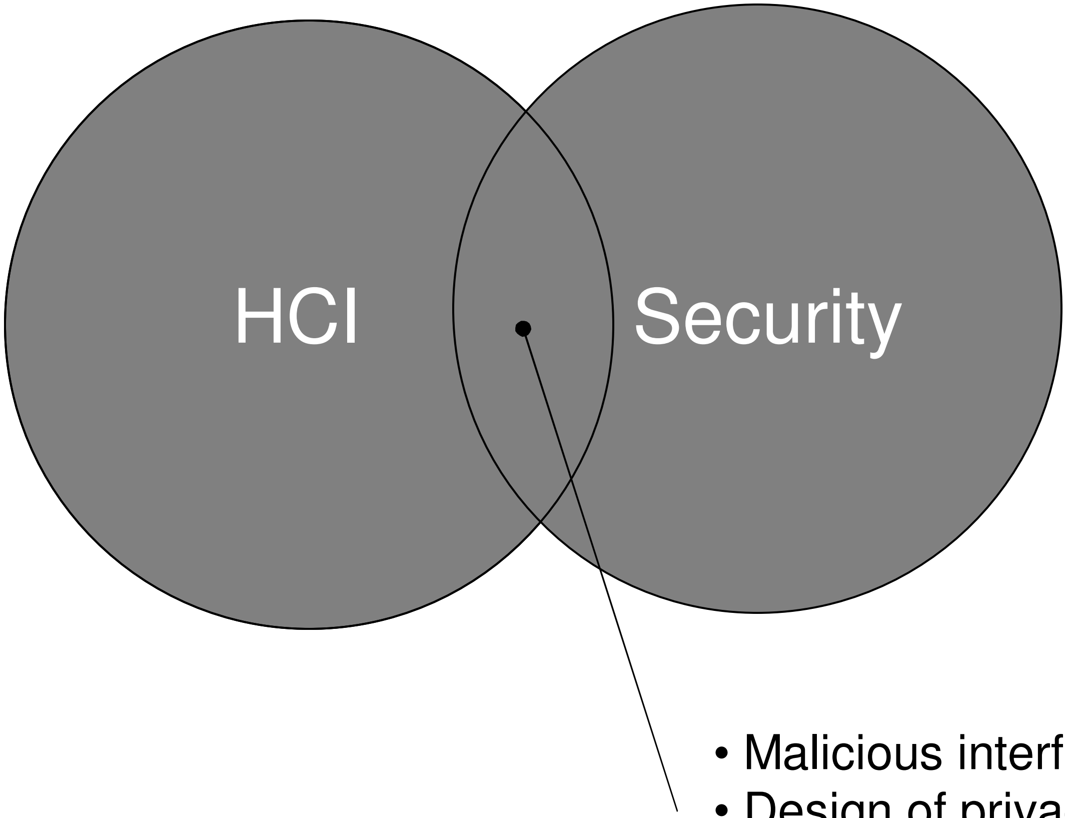
Sense a Need



Darmawan Salihun, 2006
2 used from $679.00

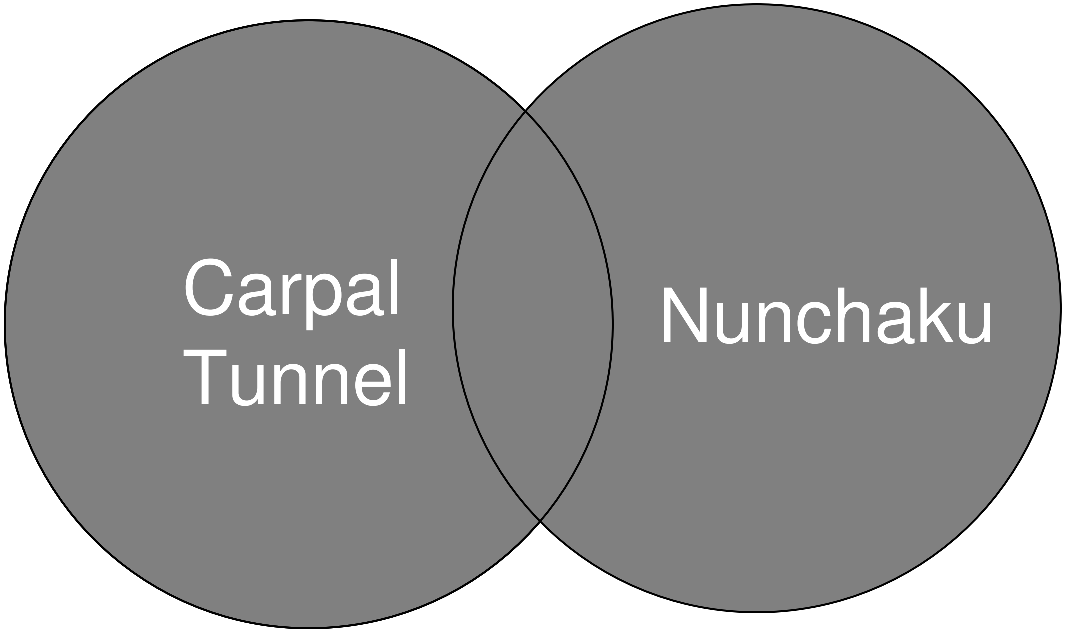
http://www.amazon.com/BIOS-Disassembly-Ninjutsu-Uncovered/dp/1931769605/ref=sr_1_1?ie=UTF8&qid=1307758222&sr=8-1

Look at the Intersection of Your Interest Areas



- Malicious interface design
- Design of privacy interfaces
- Interfaces that lie
- Error exploitation

Exploit Crazy Intersections



Carpal Tunnel

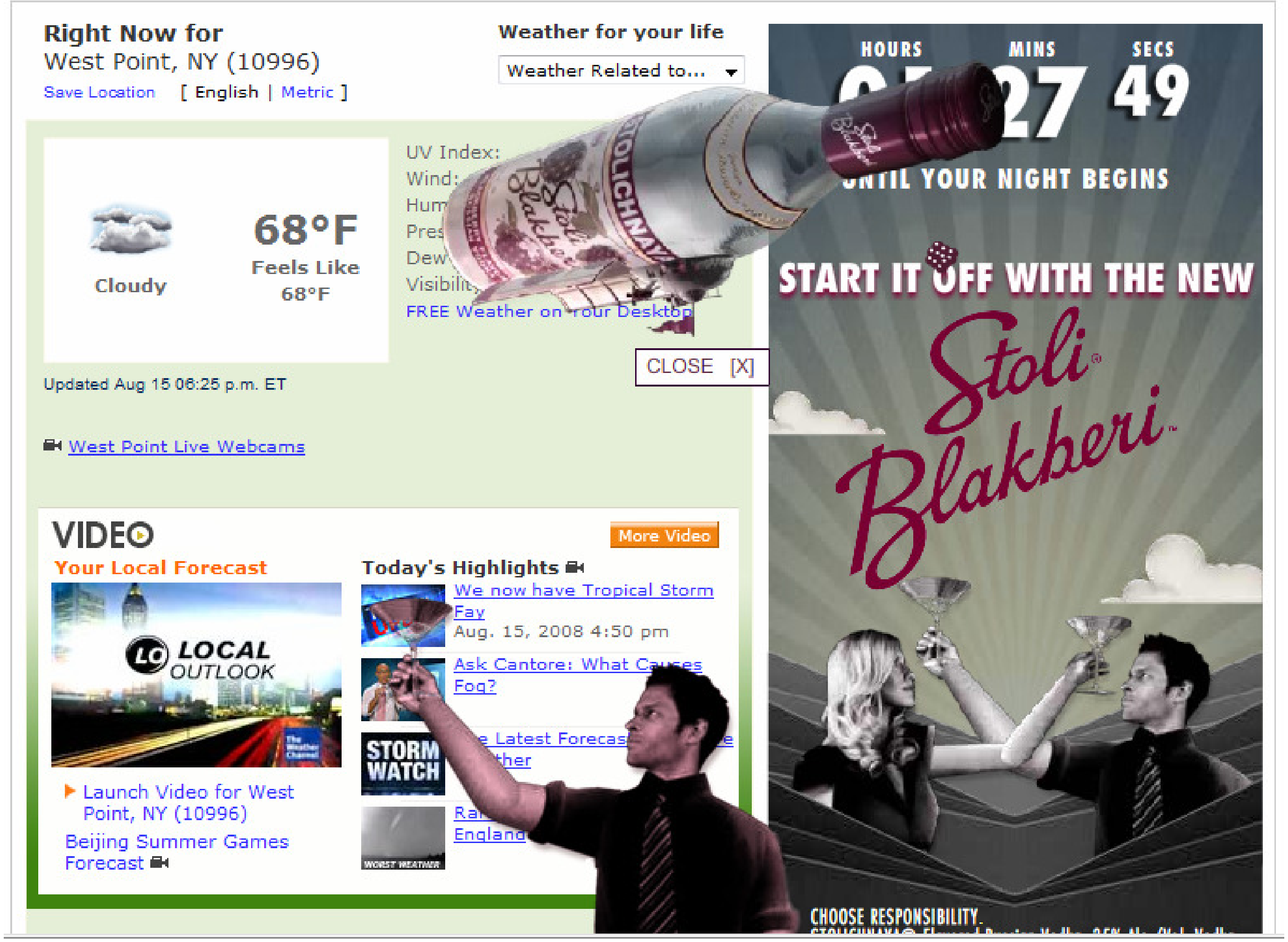
http://commons.wikimedia.org/wiki/File:Nunchaku_Routine.gif
http://www.medsupports.com/images/products/detail/8_242-&-8_243-Carpal-Tunnel.gif

Look for Pain

Bypassing the HR Filter

http://commons.wikimedia.org/wiki/File:Redbox_Office.jpg

What Makes You Mad



Right Now for
West Point, NY (10996)
Save Location [English | Metric]

Weather for your life

Cloudy

68°F
Feels Like
68°F

UV Index:
Wind:
Hum
Pres
Dew
Visibili

FREE Weather on Your Desktop

Updated Aug 15 06:25 p.m. ET

West Point Live Webcams

VIDEO

Your Local Forecast

Launch Video for West Point, NY (10996)

Beijing Summer Games Forecast

Today's Highlights

We now have Tropical Storm Fay
Aug. 15, 2008 4:50 pm

Ask Cantore: What Causes Fog?

e Latest Forecas e ther

Ra England

Flying Vodka Bottles

What Makes You Mad

Get me off Your F[redacted] Mailing List

David Mazières and Eddie Kohler
New York University
University of California, Los Angeles
http://www.mailavenger.org/

Abstract

Get me off your [redacted] mailing list. Get me off your [redacted] mailing list. Get me off your [redacted]-ing mailing list. Get me off your [redacted] mailing list. Get me off your [redacted] mailing list. Get me off your [redacted] mailing list. Get me off your [redacted]-ing mailing list. Get me off your [redacted] mailing list. Get me off your [redacted] mailing list. Get me off your [redacted] mailing list. Get me off your [redacted] mailing list. Get me off your [redacted]-ing mailing list. Get me off your [redacted] mail-

your [redacted] mailing list. Get me off your [redacted]-ing mailing list. Get me off your [redacted] mailing list. Get me off your [redacted] mailing list. Get me off your [redacted] mailing list. Get me off your [redacted]-ing mailing list. Get me off your [redacted] mailing list. Get me off your [redacted] mailing list. Get me off your [redacted] mailing list. Get me off your [redacted] mailing list. Get me off your [redacted] mailing list.

Get me off your [redacted] mailing list. Get me off your [redacted] mailing list. Get me off your [redacted] mailing list. Get me off your [redacted]

Academic Spam

What Could Possibly Go Wrong

Self-wiping hard drives from Toshiba

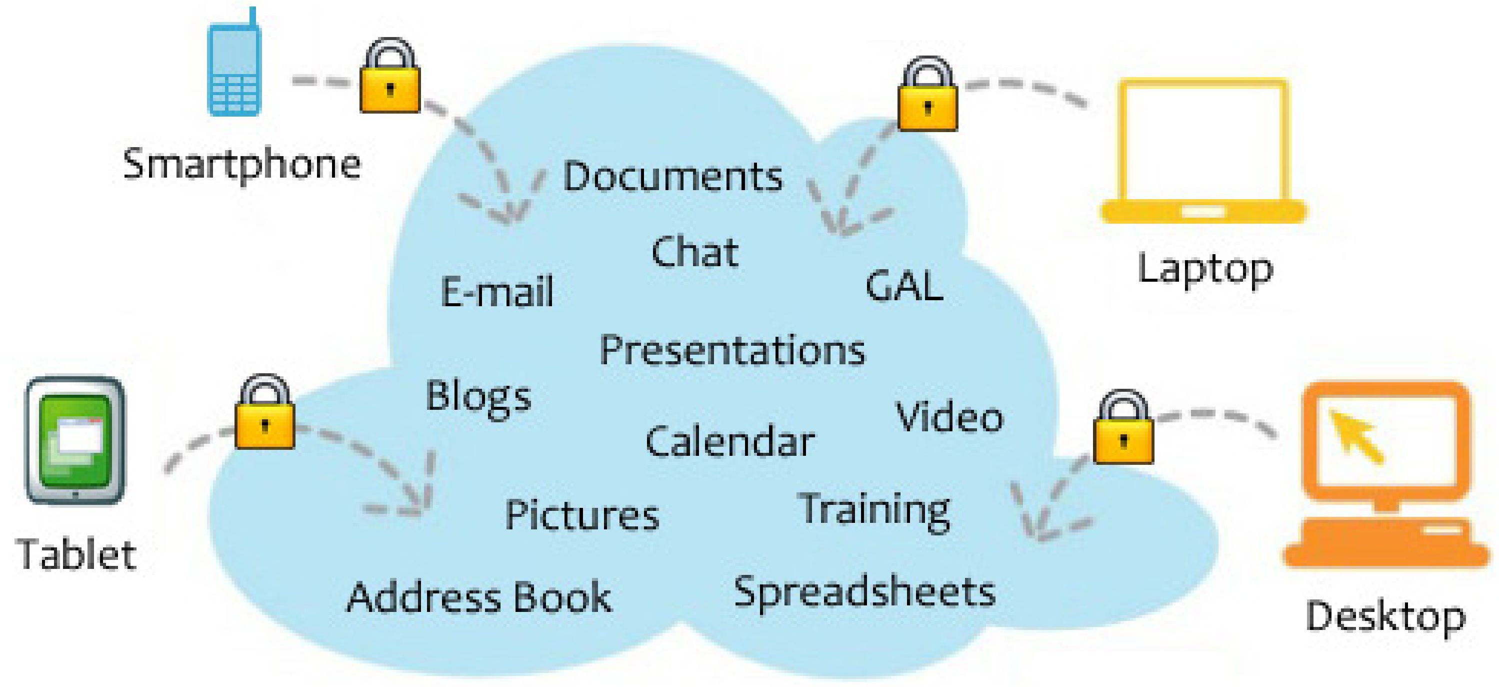
http://www.net-security.org/secworld.php?id=10894

What Could Possibly Go Wrong

Voice Analysis Software in Russian ATMs

http://www.nytimes.com/imagepages/2011/06/09/business/AltATM2.html

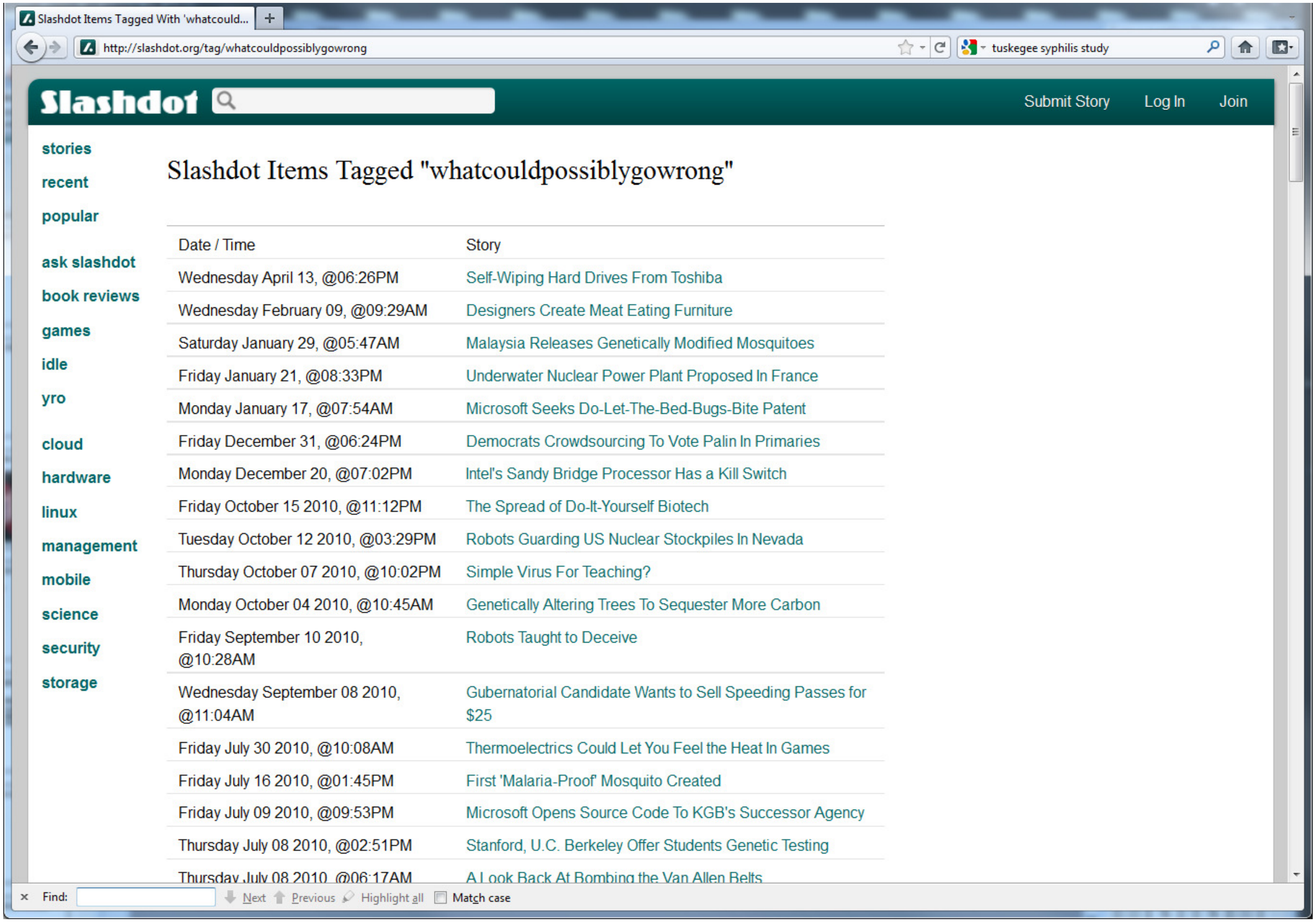
What Could Possibly Go Wrong



Cloud Computing

http://commons.wikimedia.org/wiki/File:Cloud_applications.jpg

What Could Possibly Go Wrong



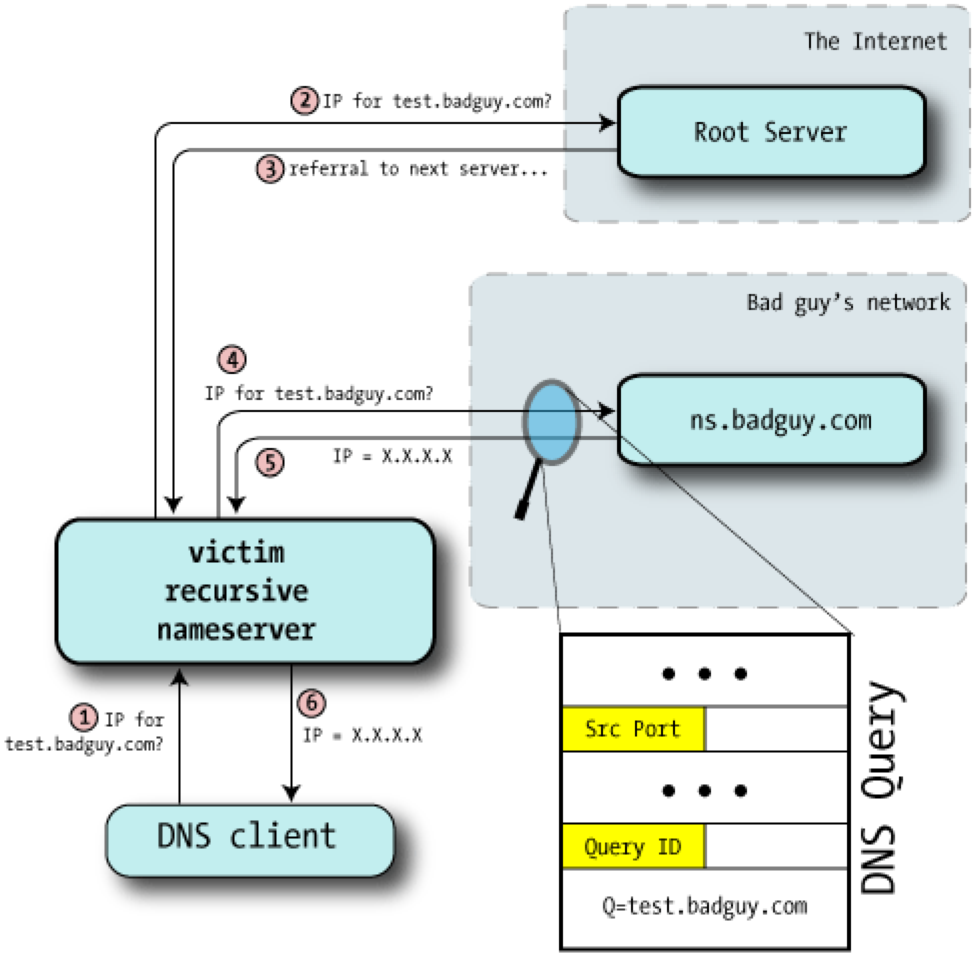
Slashdot Items Tagged "whatcouldpossiblygowrong"

Date / Time	Story
Wednesday April 13, @06:26PM	Self-Wiping Hard Drives From Toshiba
Wednesday February 09, @09:29AM	Designers Create Meat Eating Furniture
Saturday January 29, @05:47AM	Malaysia Releases Genetically Modified Mosquitoes
Friday January 21, @08:33PM	Underwater Nuclear Power Plant Proposed In France
Monday January 17, @07:54AM	Microsoft Seeks Do-Let-The-Bed-Bugs-Bite Patent
Friday December 31, @06:24PM	Democrats Crowdsourcing To Vote Palin In Primaries
Monday December 20, @07:02PM	Intel's Sandy Bridge Processor Has a Kill Switch
Friday October 15 2010, @11:12PM	The Spread of Do-It-Yourself Biotech
Tuesday October 12 2010, @03:29PM	Robots Guarding US Nuclear Stockpiles In Nevada
Thursday October 07 2010, @10:02PM	Simple Virus For Teaching?
Monday October 04 2010, @10:45AM	Genetically Altering Trees To Sequester More Carbon
Friday September 10 2010, @10:28AM	Robots Taught to Deceive
Wednesday September 08 2010, @11:04AM	Gubernatorial Candidate Wants to Sell Speeding Passes for $25
Friday July 30 2010, @10:08AM	Thermoelectrics Could Let You Feel the Heat In Games
Friday July 16 2010, @01:45PM	First 'Malaria-Proof' Mosquito Created
Friday July 09 2010, @09:53PM	Microsoft Opens Source Code To KGB's Successor Agency
Thursday July 08 2010, @02:51PM	Stanford, U.C. Berkeley Offer Students Genetic Testing
Thursday July 08 2010, @06:17AM	A Look Back At Bombing the Van Allen Belts

Look Under Rocks

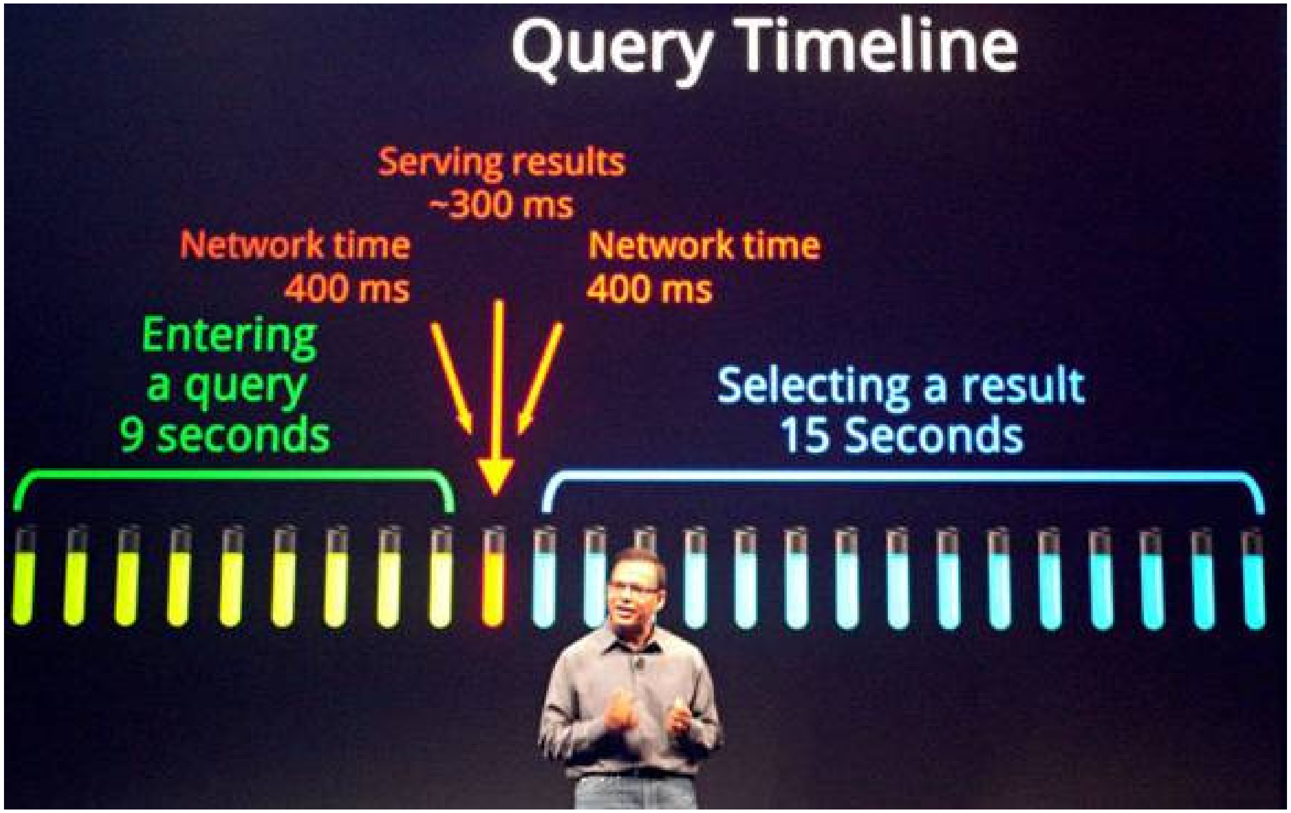
http://commons.wikimedia.org/wiki/File:Stones_1646.jpg

Something Old



http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

Something New



Google Makes Web Pages Load Instantly
The Chrome browser will soon silently fetch pages as you scan search results so that they load without delay.

http://www.technologyreview.com/computing/37818/?p1=A1&a=f

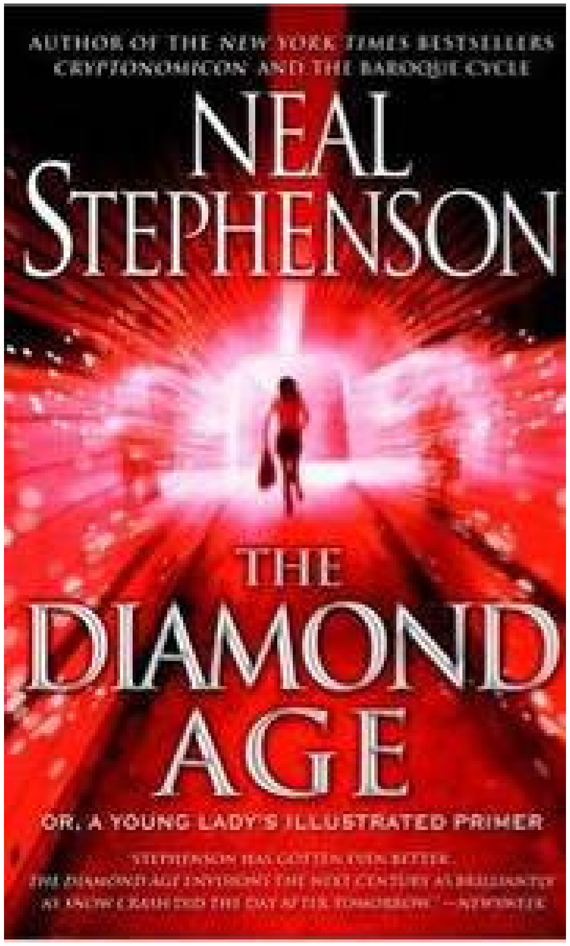
Extend / Generalize

For example, sensors…

"CCD Fingerprint Method-Identification of a Video Camera from Videotaped Images" by Kenji Kurosawa, Kenro Kuroki, Naoki Saitoh

http://commons.wikimedia.org/wiki/File:Lehrredaktion_Do1_am_Institut_f%C3%BCr_Journalistik,_TU_Dortmund.JPG

Look to Science Fiction


AUTHOR OF THE NEW YORK TIMES BESTSELLERS
CRYPTONOMICON AND THE BAROQUE CYCLE
NEAL
STEPHENSON
THE
DIAMOND
AGE
OR, A YOUNG LADY'S ILLUSTRATED PRIMER
"STEPHENSON HAS GOTTEN EVEN BETTER...
THE DIAMOND AGE ENVISIONS THE NEXT CENTURY AS BRILLIANTLY
AS SNOW CRASH DID THE DAY AFTER TOMORROW." —NEWSWEEK

Assume the Worst in People

Real Player Spyware, 1999

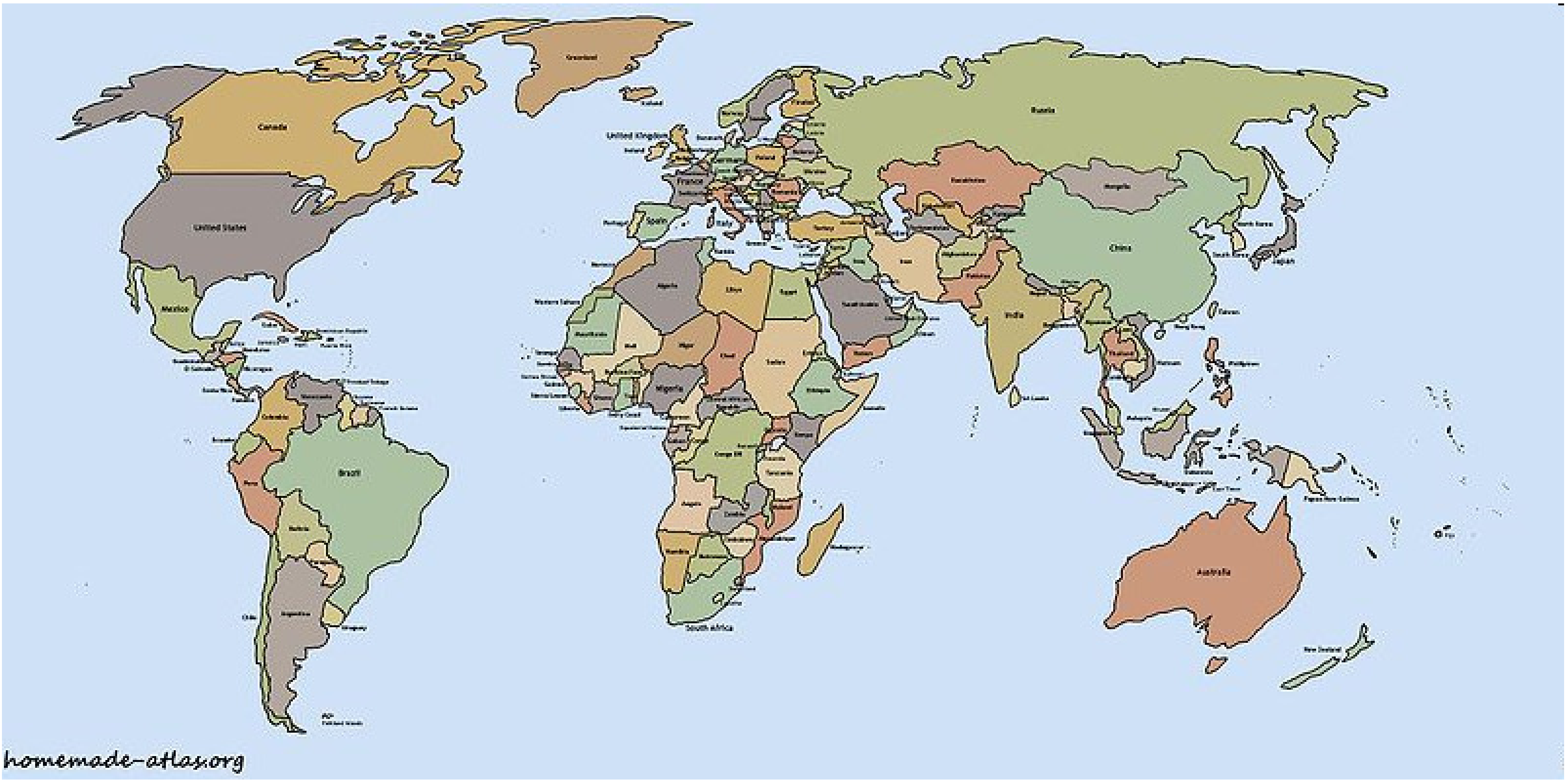
Sony Rootkit, 2005

Apple Location Database, 2011

- Look at *capabilities* and not what people, companies, or governments *say* they do
- Look at incentives

http://news.dmusic.com/article/21084
http://www.mcwetboy.net/maproom/images/sony_rootkit.jpg

Think Like a Nation-State



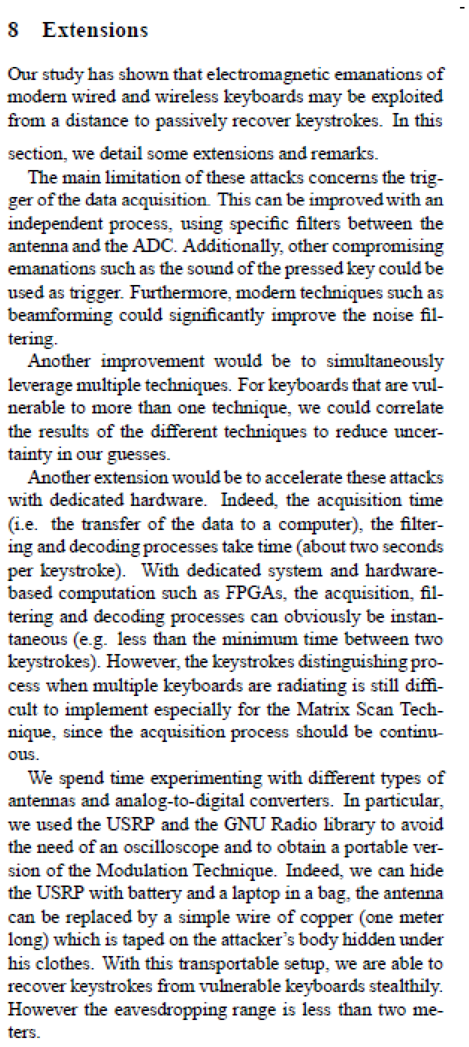
http://commons.wikimedia.org/wiki/File:Political_World_Map.jpg

Read the CFP

- Infection vectors for malware (worms, viruses, etc.)
- Botnets, command and control channels
- Spyware
- Operational experience and case studies
- Forensics
- Click fraud
- Measurement studies
- New threats and related challenges
- Boutique and targeted malware
- Phishing
- Spam
- Underground economy
- Miscreant counterintelligence
- Carding and identity theft
- Denial-of-service attacks
- Hardware vulnerabilities
- Legal issues
- The arms race (rootkits, anti–anti-virus, etc.)
- New platforms (cellular networks, wireless networks, mobile devices)
- Camouflage and detection
- Reverse engineering
- Vulnerability markets and zero-day economics
- Online money laundering
- Understanding the enemy
- Data collection challenges

USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '11)
http://www.usenix.org/events/leet11/cfp/

Future Work



8 Extensions

Our study has shown that electromagnetic emanations of modern wired and wireless keyboards may be exploited from a distance to passively recover keystrokes. In this section, we detail some extensions and remarks.

The main limitation of these attacks concerns the trigger of the data acquisition. This can be improved with an independent process, using specific filters between the antenna and the ADC. Additionally, other compromising emanations such as the sound of the pressed key could be used as trigger. Furthermore, modern techniques such as beamforming could significantly improve the noise filtering.

Another improvement would be to simultaneously leverage multiple techniques. For keyboards that are vulnerable to more than one technique, we could correlate the results of the different techniques to reduce uncertainty in our guesses.

Another extension would be to accelerate these attacks with dedicated hardware. Indeed, the acquisition time (i.e. the transfer of the data to a computer), the filtering and decoding processes take time (about two seconds per keystroke). With dedicated system and hardware-based computation such as FPGAs, the acquisition, filtering and decoding processes can obviously be instantaneous (e.g. less than the minimum time between two keystrokes). However, the keystrokes distinguishing process when multiple keyboards are radiating is still difficult to implement especially for the Matrix Scan Technique, since the acquisition process should be continuous.

We spend time experimenting with different types of antennas and analog-to-digital converters. In particular, we used the USRP and the GNU Radio library to avoid the need of an oscilloscope and to obtain a portable version of the Modulation Technique. Indeed, we can hide the USRP with battery and a laptop in a bag, the antenna can be replaced by a simple wire of copper (one meter long) which is taped on the attacker's body hidden under his clothes. With this transportable setup, we are able to recover keystrokes from vulnerable keyboards stealthily. However the eavesdropping range is less than two meters.

Martin Vuagnoux and Sylvain Pasin. “Compromising Electromagnetic Emanations of Wired and Wireless Keyboards.” USENIX Security, 2009.

A Good Survey Article or Paper is Always in Demand

And is an important part of your research program

http://commons.wikimedia.org/wiki/File:Seismic_Survey_Party.jpeg

And More

- Work with someone else
- Consider edge and corner cases
- Examine implementations
- Hardware is the new software
- Exploit cloud resources
- Defcon / BH / RSA talks

…

Develop a System

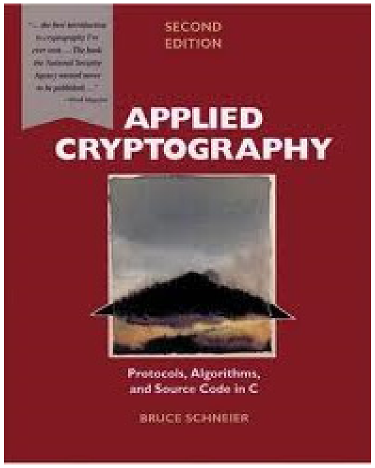
Feed your Mind

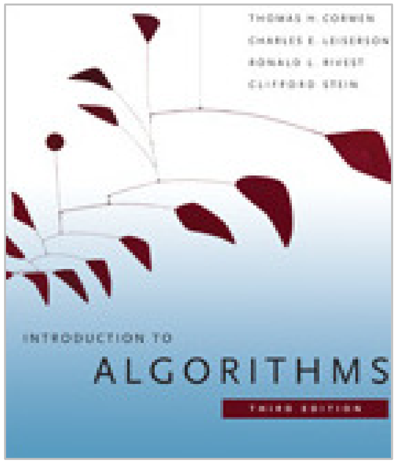
Museum of Modern Art, NY

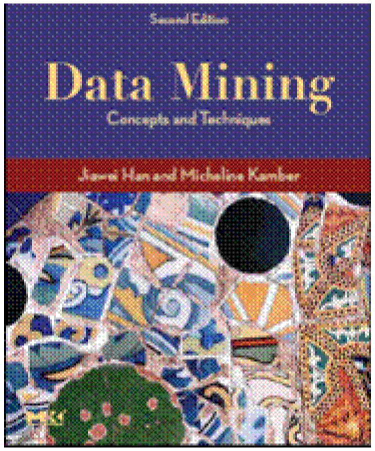
- Have analog hobbies
  - Lathe and wizards wands
- Got to take mind off work
- Choose diverse sources
  - Slashdot
  - Wired
  - Technology Review
  - …
- Books
- Magazines
  - IEEE S&P
  - Make
  - …
- Mailing Lists
- IEEE Cipher
- Blogs

http://commons.wikimedia.org/wiki/File:MoMa_NY_USA_screens.jpg

Build up your toolset





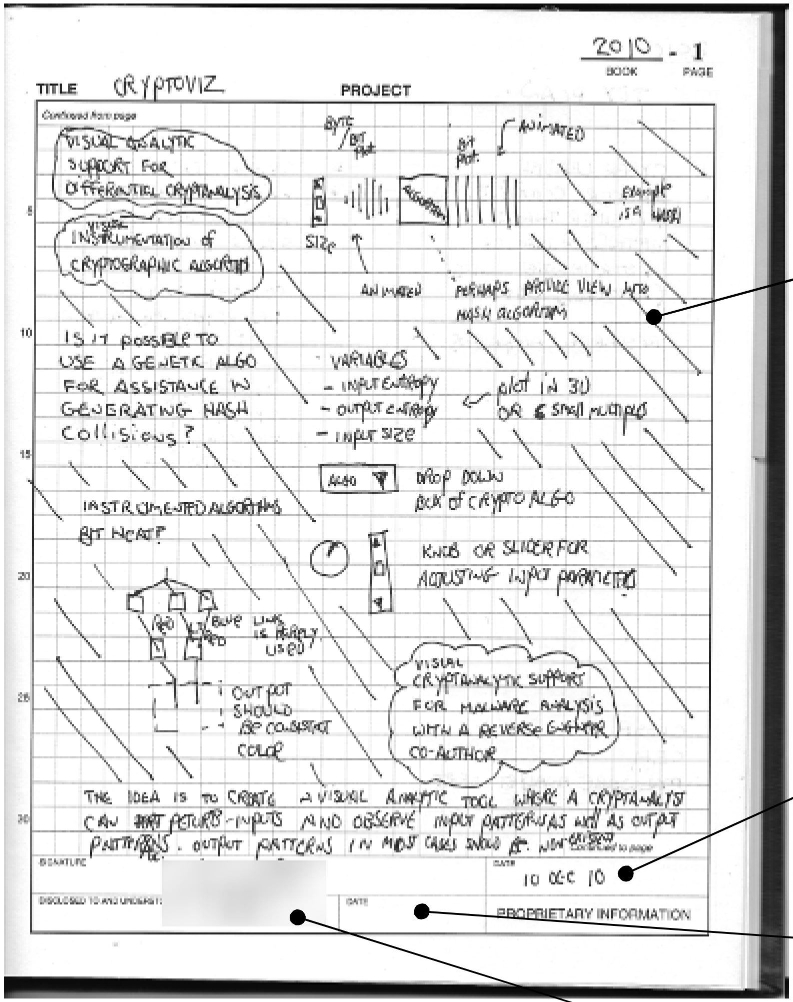


MITOPENCOURSEWARE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
Unlocking Knowledge, Empowering Minds.
DONATE NOW
Dow
Ab Initio
Exam Prep on OCW

- Coding
- Hardware
- Advanced Techniques
  - Datamining
  - Visualization
  - Information Theory
  - …
- Speed reading
- Communicating
  - Writing
  - Public Speaking

Write Down Your Ideas

- Document discoveries: Capture exact details and dates of conception
- Be able to reproduce your work
- Record ideas, observations, and results
- Chronological record of your work
- Use permanent Ink
- Never remove pages



2010 - 1
BOOK PAGE

TITLE CRYPTOVIZ PROJECT

Continued from page

VISUAL ANALYTIC SUPPORT FOR DIFFERENTIAL CRYPTANALYSIS

VISUAL INSTRUMENTATION of CRYPTOGRAPHIC ALGORITHMS

BYTE/BIT PLOT

ALGORITHM

BIT PLOT

ANIMATED

SIZE

ANIMATED

EXAMPLE IS A HASH

PERHAPS PROVIDE VIEW INTO HASH ALGORITHMS

IS IT POSSIBLE TO USE A GENETIC ALGO FOR ASSISTANCE IN GENERATING HASH COLLISIONS?

VARIABLES
- INPUT ENTROPY
- OUTPUT ENTROPY
- INPUT SIZE

plot IN 3D OR 6 SMALL MULTIPLES

ALGO ▼ DROP DOWN BOX OF CRYPTO ALGO

INSTRUMENTED ALGORITHMS BIT HEAT?

KNOB OR SLIDER FOR ADJUSTING INPUT PARAMETERS

RED

BLUE LINK IS RARELY USED

RED

OUTPUT SHOULD BE CONSISTENT COLOR

VISUAL CRYPTANALYTIC SUPPORT FOR MALWARE ANALYSIS WITH A REVERSE ENGINEER CO-AUTHOR

THE IDEA IS TO CREATE A VISUAL ANALYTIC TOOL WHERE A CRYPTANALYST CAN ~~PART~~ PERTURB-INPUTS AND OBSERVE INPUT PATTERNS AS WELL AS OUTPUT PATTERNS. OUTPUT PATTERNS IN MOST CASES SHOULD BE NON-EXISTENT.

Continued to page

SIGNATURE [redacted]

DATE 10 DEC 10

DISCLOSED TO AND UNDERSTOOD BY:

DATE

PROPRIETARY INFORMATION

Fill Unused Space

Date

Your Signature

Witness Signature

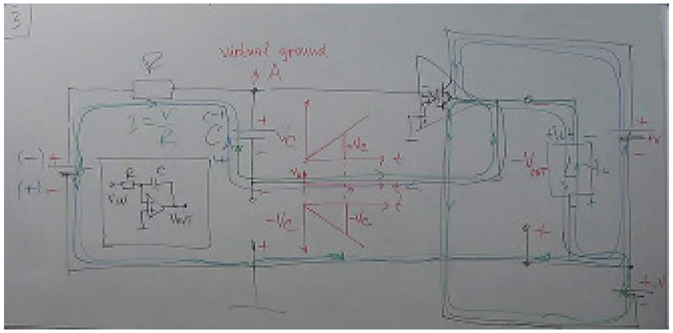
Source: www.bookfactory.com

Other Techniques

Giant Pads of Paper

Giant Post-it Notes

Digital Voice Recorder



White Board

Smart Board

http://commons.wikimedia.org/wiki/File:Integrator_step4_whiteboard_1000.jpg
http://www.amazon.com/gp/customer-media/product-gallery/B000F762Q4/ref=cm_ciu_pdp_images_0?ie=UTF8&index=0
http://www.amazon.com/Sony-ICD-BX800-Memory-Digital-Recorder/dp/B00387E5AS/ref=sr_1_1?ie=UTF8&qid=1308225530&sr=8-1
http://www.post-it.com/wps/portal/3M/en_US/Post_It/Global/Home/Products/Easel_Pads/?PC_7_RJH9U5230OT440II987MUE3CE7_nid=NPC4H48K27gsKK1GCH46K8gIN2ZDWKD3XWbl

Watch for New Pieces of Information

http://commons.wikimedia.org/wiki/File:Fire_buckets,_Minehead_Station_-_geograph.org.uk_-_1715978.jpg

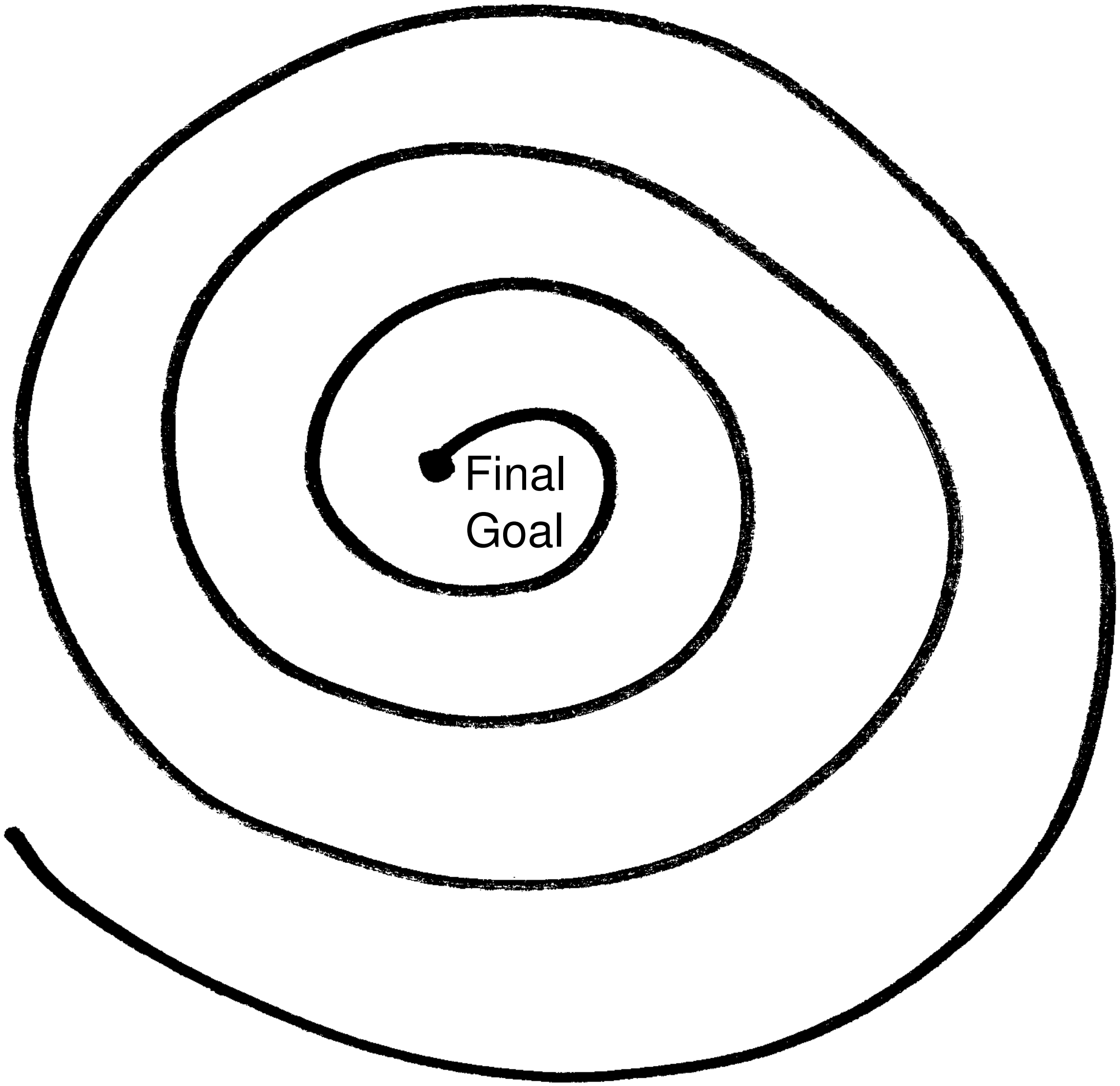
Choosing the Right Problem

Don’t Rediscover Fire

- Life is short
- Something you are passionate about
- Ability to get traction
- Idea maturity
  - Not too early
  - Not too late
- Develop many in parallel
- Who pays your bills

http://commons.wikimedia.org/wiki/File:Feu_-_VTdJ.JPG

Chip Away at the Problem

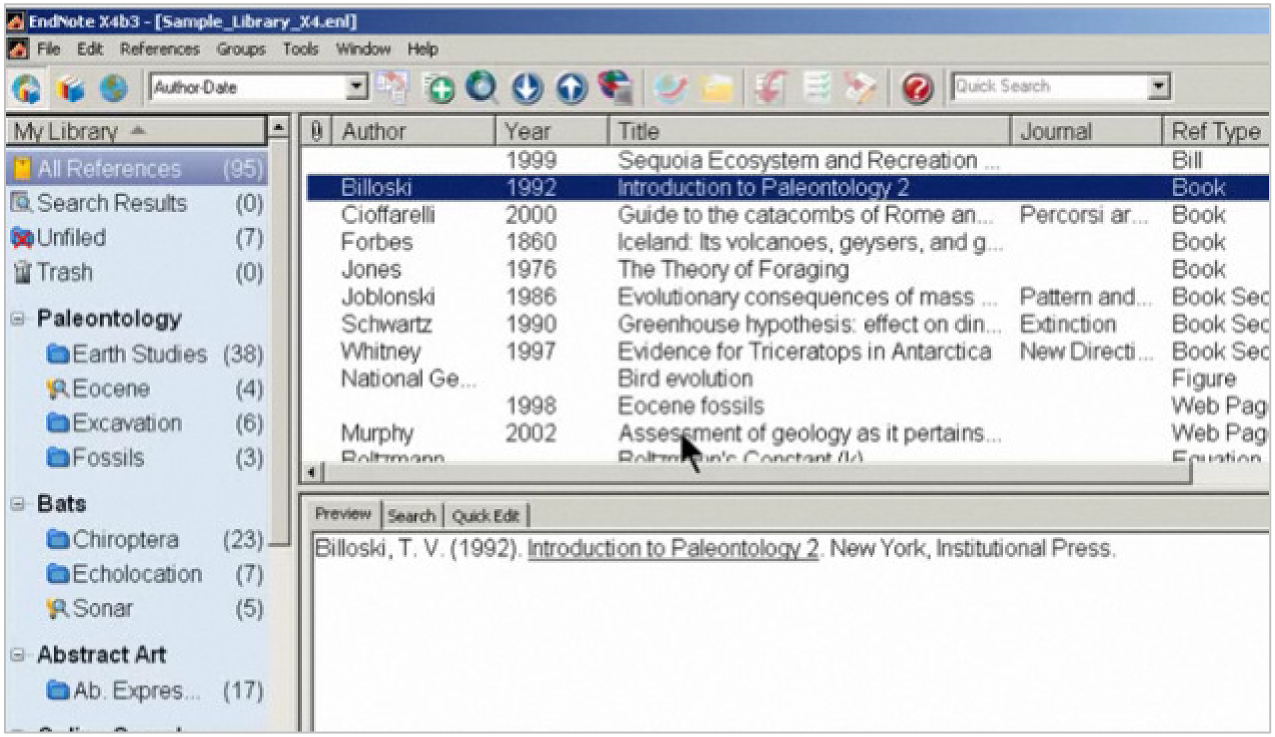


Build on What Others Have Done

- Avoid duplication
- Help energize your work
- Give credit where credit is due
- Paywalls
  - 80% is probably publicly available
  - email authors
  - friend in college with DL subscription, web search

http://en.wikipedia.org/wiki/File:Library_of_Congress,_Rosenwald_4,_Bl._5r.jpg

Reference Management



Author	Year	Title	Journal	Ref Type
	1999	Sequoia Ecosystem and Recreation ...		Bill
Billoski	1992	Introduction to Paleontology 2		Book
Cioffarelli	2000	Guide to the catacombs of Rome an...	Percorsi ar...	Book
Forbes	1860	Iceland: Its volcanoes, geysers, and g...		Book
Jones	1976	The Theory of Foraging		Book
Joblonski	1986	Evolutionary consequences of mass ...	Pattern and...	Book Sec
Schwartz	1990	Greenhouse hypothesis: effect on din...	Extinction	Book Sec
Whitney	1997	Evidence for Triceratops in Antarctica	New Directi...	Book Sec
National Ge...		Bird evolution		Figure
	1998	Eocene fossils		Web Pag
Murphy	2002	Assessment of geology as it pertains...		Web Pag
Boltzmann		Boltzmann's Constant (k)		Equation

Billoski, T. V. (1992). Introduction to Paleontology 2. New York, Institutional Press.

Lots of choices… Aigaion, Bebop, BibDesk, Biblioscape, BibSonomy, Bibus, Bookends, Citavi, CiteULike, Connotea, EndNote, JabRef, Jumper 2.0, KBibTeX, Mendeley, Papers, PDF Stacks, Pybliographer, Qiqqa, refbase, RefDB, Reference Manager, Referencer, RefWorks, Scholar's Aid, Sente, Wikindx , WizFolio, Zotero

See http://en.wikipedia.org/wiki/Comparison_of_reference_management_software

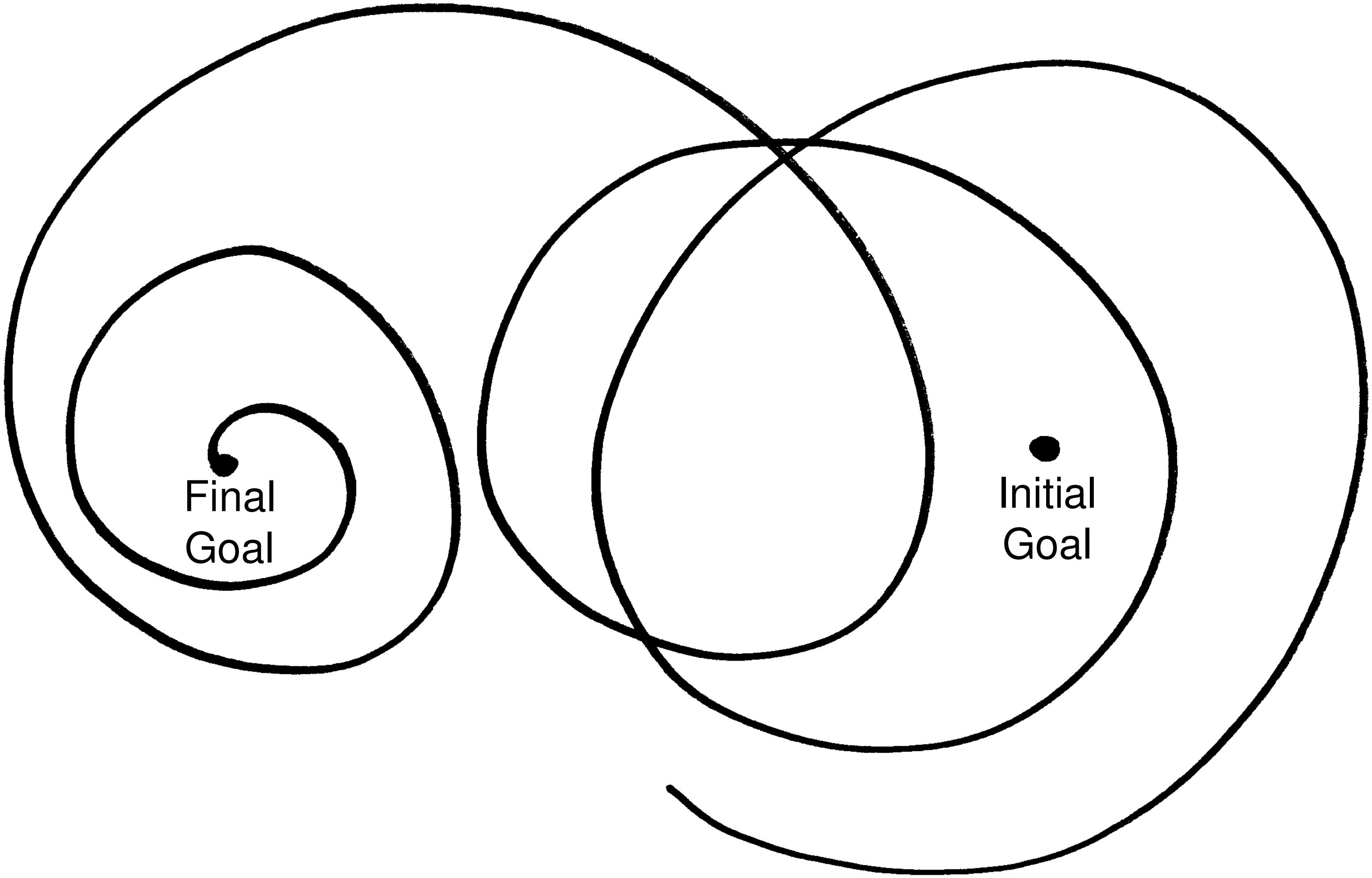
http://www.endnote.com/

Organize your Data

- Versioning
  - yyyymm_name_verXX
- The mess I created
  - 1M+ binary fragments
- Backing up
  - WTC

http://commons.wikimedia.org/wiki/File:Hard_disk_head_crash.jpg

The Target May Move



Re(Search)

- Blind alleys
- Knowing something doesn’t work is also knowledge

http://commons.wikimedia.org/wiki/File:Brick_alley.jpg

Get Feedback

- Peers
- Panels
- Regional Cons
- Groups at work
- DC groups / 2600 Gatherings

- Each makes you stronger and fleshes out the idea

Collaborate

>How can I get in touch with you?

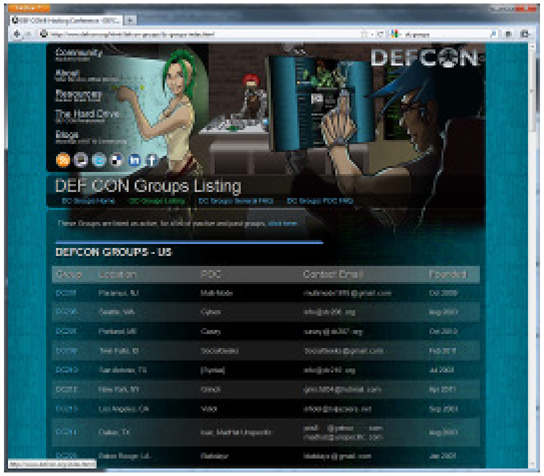
You can write to me in care of my publishers. They will then compost your letter, allow it to ferment for several months, and eventually send it to me. I will then neglect to reply, no doubt suffering an incremental increase in negative karma. It's up to you.

-William Gibson

- You probably don’t want to contact William Gibson
- Google Docs
- Building a team / Research group
- But remember the mythical man month

http://williamgibsonboard.com/eve/forums/a/tpc/f/273109857/m/624109857

Start Local



DEF CON Groups Listing

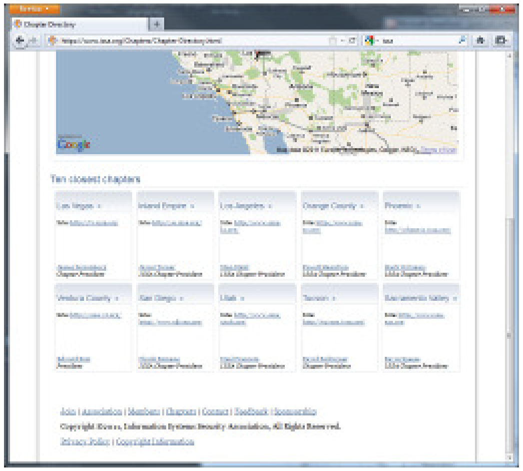
DEFCON GROUPS - US

DC Groups

List of Hacker Spaces

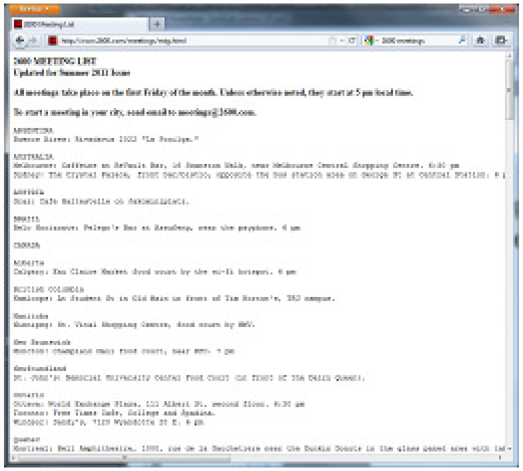
This is a comprehensive, user-maintained list of all active hackerspaces throughout the world.

Hacker Spaces



Ten closest chapters

ISSA



2600 MEETING LIST
Updated for Summer 2011 Issue

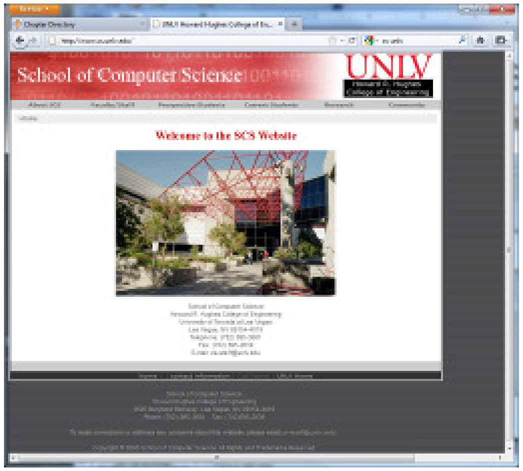
All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time.

To start a meeting in your city, send email to meetings@2600.com.

2600 Meetings

Linux User Group

LUGs



School of Computer Science

UNLV

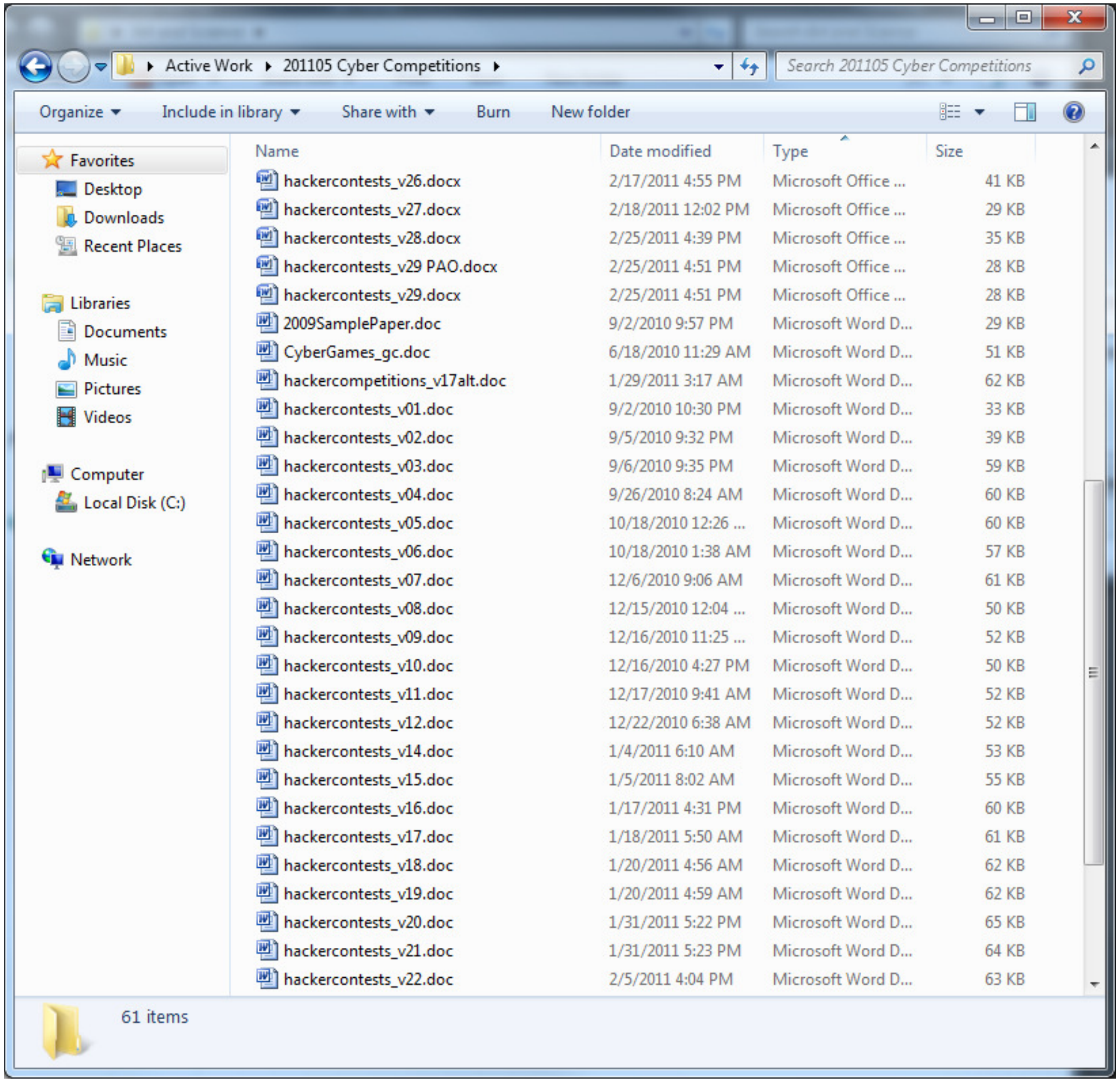
Welcome to the SCS Website

Colleges

Coping with Infinity

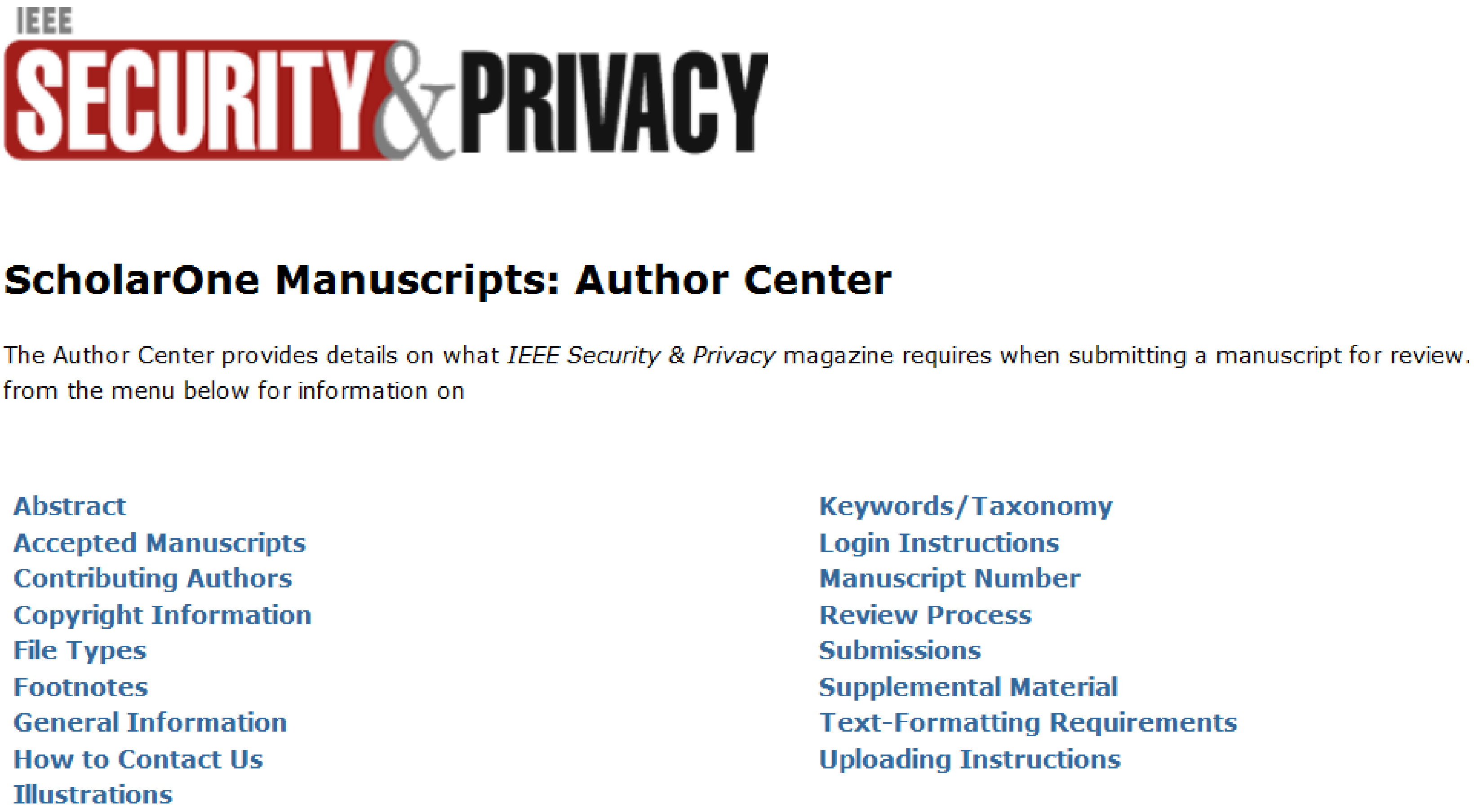
http://commons.wikimedia.org/wiki/File:E-portfolios-infinity-design.jpg

Write and Rewrite



Name	Date modified	Type	Size
hackercontests_v26.docx	2/17/2011 4:55 PM	Microsoft Office ...	41 KB
hackercontests_v27.docx	2/18/2011 12:02 PM	Microsoft Office ...	29 KB
hackercontests_v28.docx	2/25/2011 4:39 PM	Microsoft Office ...	35 KB
hackercontests_v29 PAO.docx	2/25/2011 4:51 PM	Microsoft Office ...	28 KB
hackercontests_v29.docx	2/25/2011 4:51 PM	Microsoft Office ...	28 KB
2009SamplePaper.doc	9/2/2010 9:57 PM	Microsoft Word D...	29 KB
CyberGames_gc.doc	6/18/2010 11:29 AM	Microsoft Word D...	51 KB
hackercompetitions_v17alt.doc	1/29/2011 3:17 AM	Microsoft Word D...	62 KB
hackercontests_v01.doc	9/2/2010 10:30 PM	Microsoft Word D...	33 KB
hackercontests_v02.doc	9/5/2010 9:32 PM	Microsoft Word D...	39 KB
hackercontests_v03.doc	9/6/2010 9:35 PM	Microsoft Word D...	59 KB
hackercontests_v04.doc	9/26/2010 8:24 AM	Microsoft Word D...	60 KB
hackercontests_v05.doc	10/18/2010 12:26 ...	Microsoft Word D...	60 KB
hackercontests_v06.doc	10/18/2010 1:38 AM	Microsoft Word D...	57 KB
hackercontests_v07.doc	12/6/2010 9:06 AM	Microsoft Word D...	61 KB
hackercontests_v08.doc	12/15/2010 12:04 ...	Microsoft Word D...	50 KB
hackercontests_v09.doc	12/16/2010 11:25 ...	Microsoft Word D...	52 KB
hackercontests_v10.doc	12/16/2010 4:27 PM	Microsoft Word D...	50 KB
hackercontests_v11.doc	12/17/2010 9:41 AM	Microsoft Word D...	52 KB
hackercontests_v12.doc	12/22/2010 6:38 AM	Microsoft Word D...	52 KB
hackercontests_v14.doc	1/4/2011 6:10 AM	Microsoft Word D...	53 KB
hackercontests_v15.doc	1/5/2011 8:02 AM	Microsoft Word D...	55 KB
hackercontests_v16.doc	1/17/2011 4:31 PM	Microsoft Word D...	60 KB
hackercontests_v17.doc	1/18/2011 5:50 AM	Microsoft Word D...	61 KB
hackercontests_v18.doc	1/20/2011 4:56 AM	Microsoft Word D...	62 KB
hackercontests_v19.doc	1/20/2011 4:59 AM	Microsoft Word D...	62 KB
hackercontests_v20.doc	1/31/2011 5:22 PM	Microsoft Word D...	65 KB
hackercontests_v21.doc	1/31/2011 5:23 PM	Microsoft Word D...	64 KB
hackercontests_v22.doc	2/5/2011 4:04 PM	Microsoft Word D...	63 KB

Author Guidelines



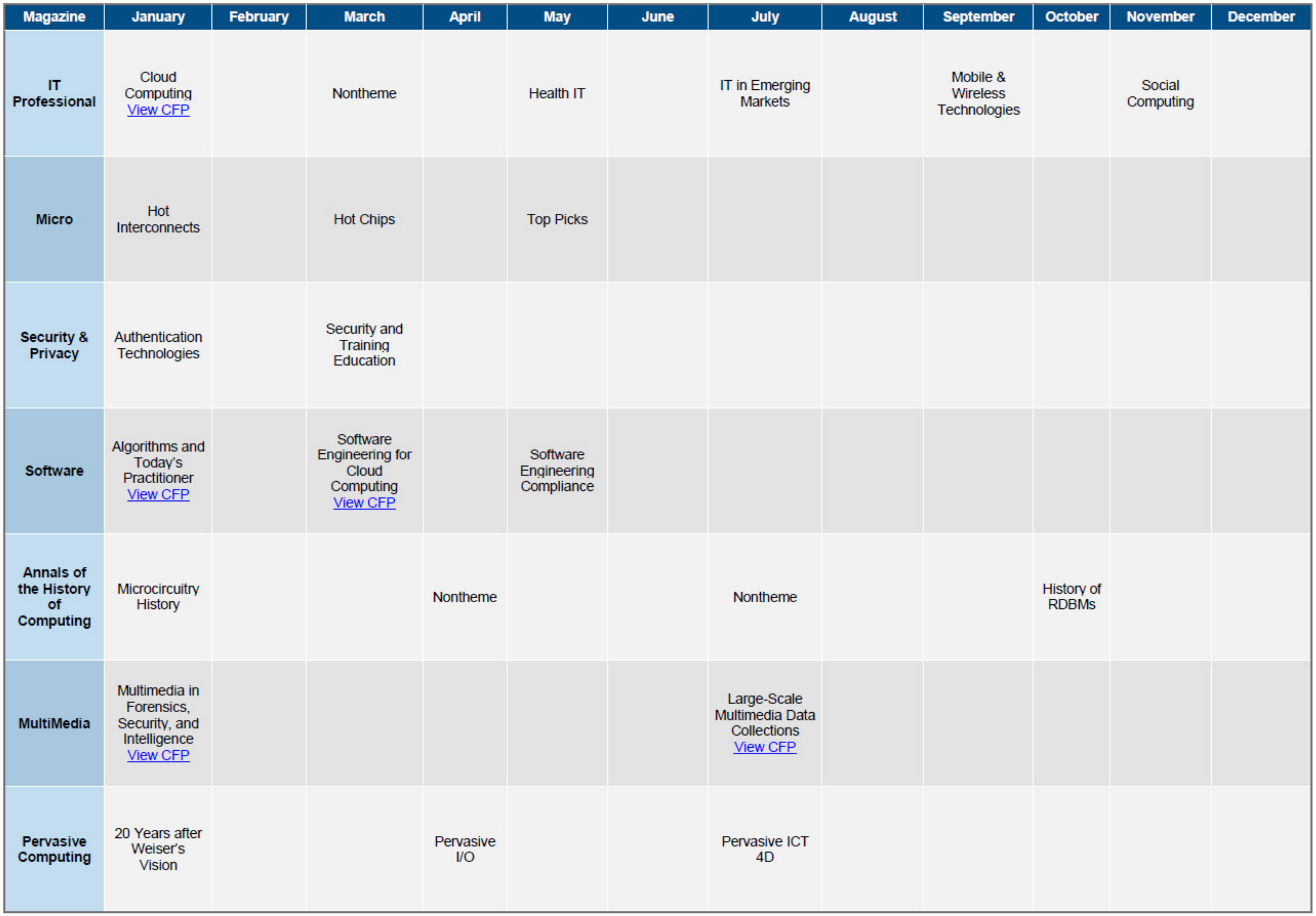
IEEE SECURITY&PRIVACY

ScholarOne Manuscripts: Author Center

The Author Center provides details on what *IEEE Security & Privacy* magazine requires when submitting a manuscript for review. from the menu below for information on

- Abstract
- Accepted Manuscripts
- Contributing Authors
- Copyright Information
- File Types
- Footnotes
- General Information
- How to Contact Us
- Illustrations
- Keywords/Taxonomy
- Login Instructions
- Manuscript Number
- Review Process
- Submissions
- Supplemental Material
- Text-Formatting Requirements
- Uploading Instructions

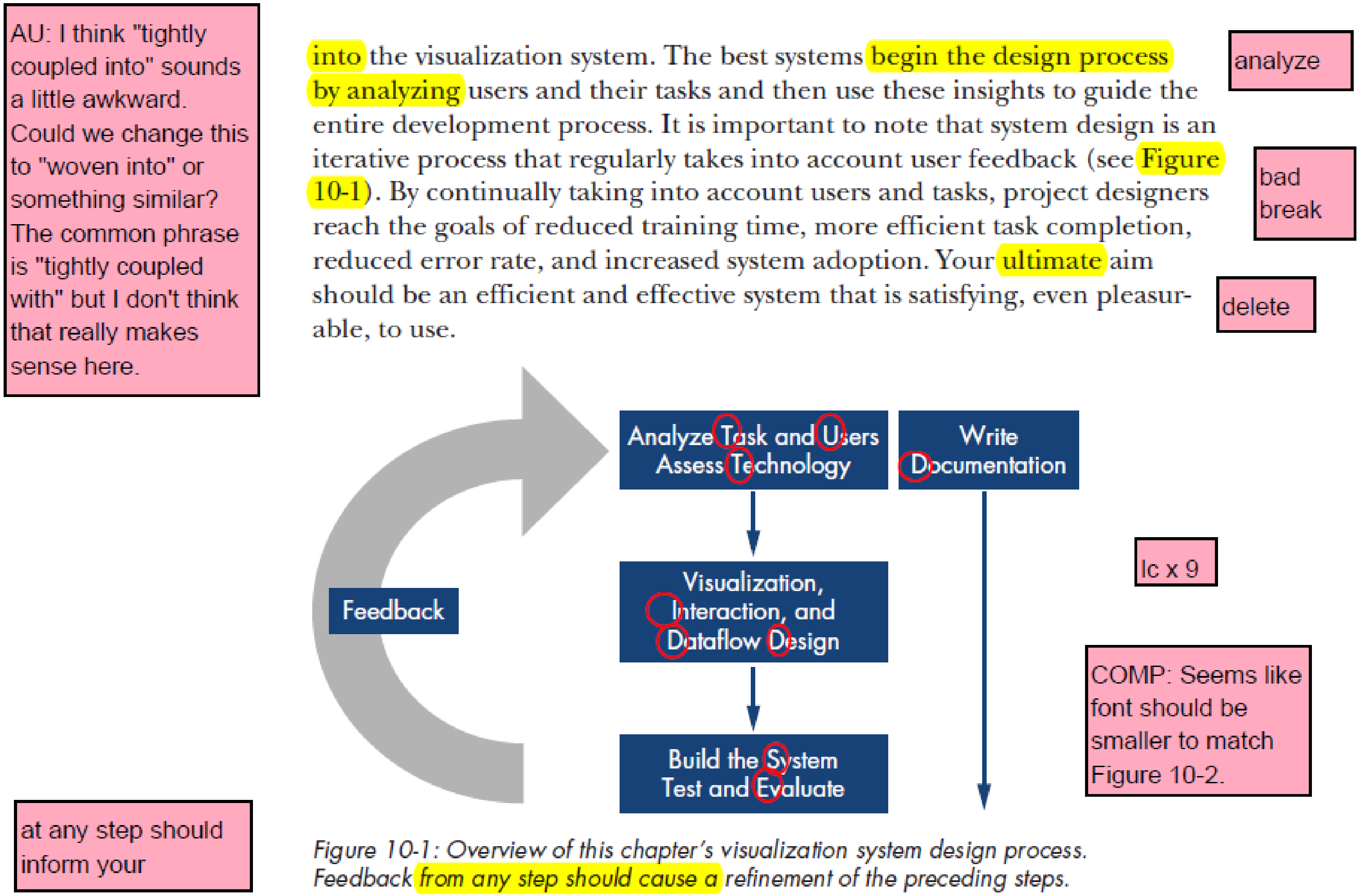
Editorial Calendars



Magazine	January	February	March	April	May	June	July	August	September	October	November	December
IT Professional	Cloud Computing View CFP		Nontheme		Health IT		IT in Emerging Markets		Mobile & Wireless Technologies		Social Computing	
Micro	Hot Interconnects		Hot Chips		Top Picks							
Security & Privacy	Authentication Technologies		Security and Training Education									
Software	Algorithms and Today's Practitioner View CFP		Software Engineering for Cloud Computing View CFP		Software Engineering Compliance							
Annals of the History of Computing	Microcircuitry History			Nontheme			Nontheme			History of RDBMs		
MultiMedia	Multimedia in Forensics, Security, and Intelligence View CFP						Large-Scale Multimedia Data Collections View CFP					
Pervasive Computing	20 Years after Weiser's Vision			Pervasive I/O			Pervasive ICT 4D					

2012 IEEE Computer Society (Extract)

Look at What Editor’s Change



AU: I think "tightly coupled into" sounds a little awkward. Could we change this to "woven into" or something similar? The common phrase is "tightly coupled with" but I don't think that really makes sense here.

into the visualization system. The best systems begin the design process by analyzing users and their tasks and then use these insights to guide the entire development process. It is important to note that system design is an iterative process that regularly takes into account user feedback (see Figure 10-1). By continually taking into account users and tasks, project designers reach the goals of reduced training time, more efficient task completion, reduced error rate, and increased system adoption. Your ultimate aim should be an efficient and effective system that is satisfying, even pleasurable, to use.

analyze

bad break

delete

Feedback

Analyze Task and Users
Assess Technology

Write Documentation

Visualization, Interaction, and Dataflow Design

Build the System
Test and Evaluate

lc x 9

COMP: Seems like font should be smaller to match Figure 10-2.

Figure 10-1: Overview of this chapter’s visualization system design process. Feedback from any step should cause a refinement of the preceding steps.

at any step should inform your

Getting to Cruising Altitude

Neal Stephenson
“Why I am a Bad Correspondent”

“Writing novels is hard, and requires vast, unbroken slabs of time. Four quiet hours is a resource that I can put to good use.”

“Two slabs of time, each two hours long, might add up to the same four hours, but are not nearly as productive as an unbroken four.”

“If I know that I am going to be interrupted, I can't concentrate, and if I suspect that I might be interrupted, I can't do anything at all.”

http://web.mac.com/nealstephenson/Neal_Stephensons_Site/Photos.html#0
http://web.mac.com/nealstephenson/Neal_Stephensons_Site/Bad_Correspondent.html

Major Life Events

> “No mathematician should ever allow himself to forget that mathematics, more than any other art or science, is a young man's game.”

G.H. Hardy
A Mathematician’s Apology

http://www.slate.com/id/2082960/

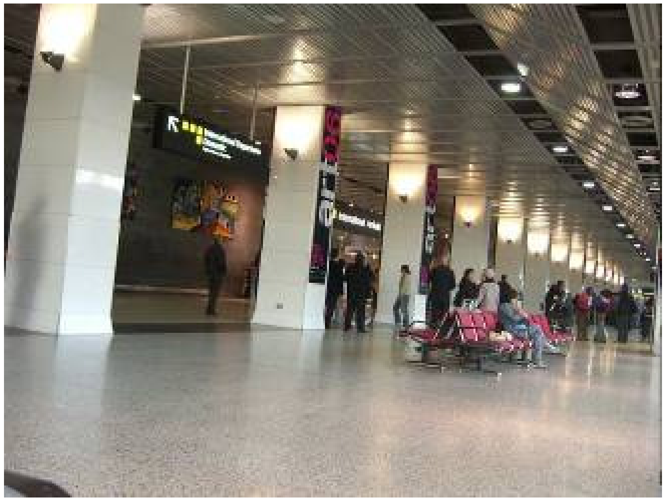
http://commons.wikimedia.org/wiki/File:Fliegergriff01.jpg

http://commons.wikimedia.org/wiki/File:%E3%82%BD%E3%83%95%E3%82%A3%E3%82%B9%E3%82%AB%E3%83%A4%E5%AF%BA%E9%99%A2%E3%83%BB%E8%81%96%E7%B4%A2%E8%8F%B2%E4%BA%9C%E6%95%99%E5%A0%82%E7%B5%90%E5%A9%9A%E5%BC%8F%E8%A8%98%E5%BF%B5%E5%86%99%E7%9C%9F.jpg

Find a Place Where You are Creative

Interesting meetings, classes and talks

Boring meetings, classes and talks

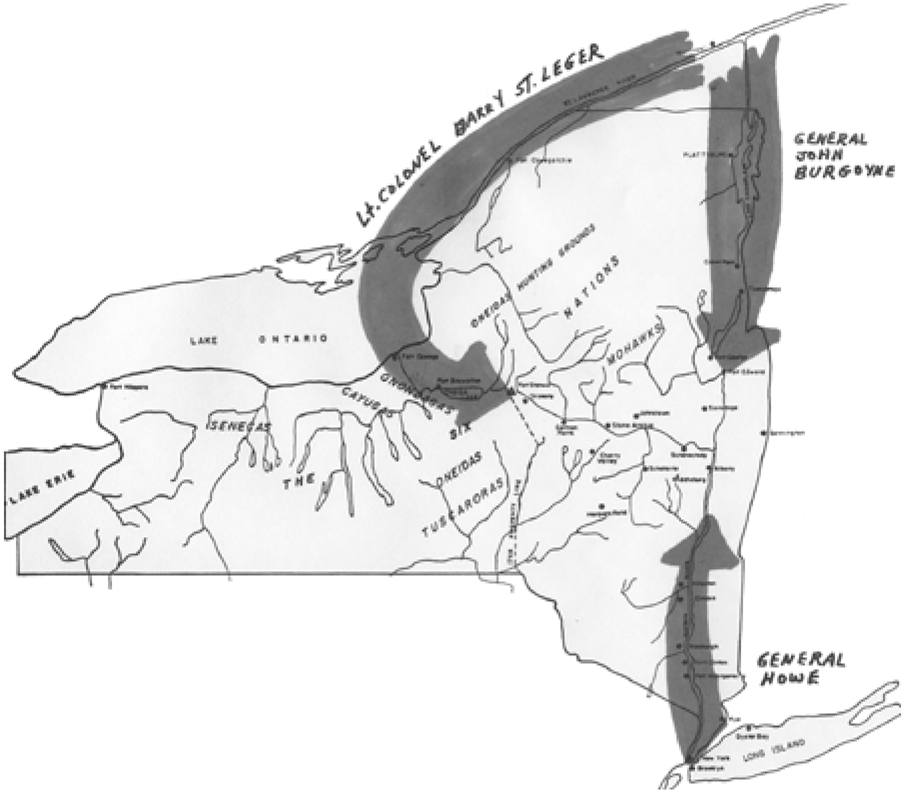


Airports / Airplanes

Mall Food Courts / Restaurants / Pubs

http://www.flickr.com/photos/shootingsawk/2767119981/sizes/m/in/photostream/
http://commons.wikimedia.org/wiki/File:Melbourne_Airport_terminal.jpg
http://en.wikipedia.org/wiki/File:Food_court_edo_japan_la_belle_province_basha.jpg

Think in Terms of Research Campaigns



- Long Term
- Inform decision makers
- Communicate with different audiences
- Research vision

http://www.nps.gov/nr/twhp/wwwlps/lessons/107bennington/107locate2.htm

Research Funding

Thai Buddhist “Money Trees”

- Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR)
  - http://www.sbir.gov
- NSF
- DARPA

…

- Lots of metawork
- Lots strings usually attached
- Lots of competition

http://commons.wikimedia.org/wiki/File:Wat_money_trees.jpg

DARPA Cyber Fast Track

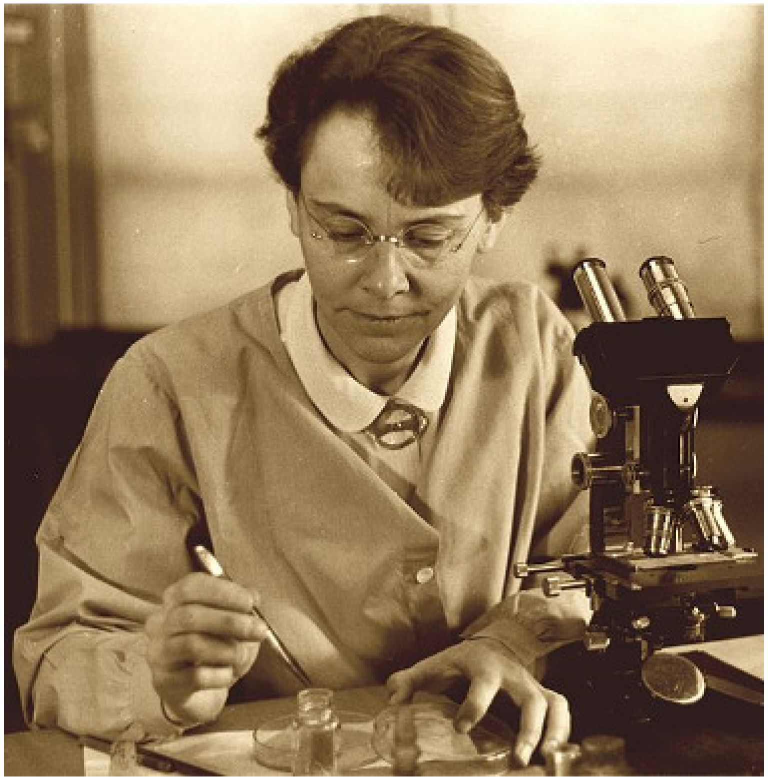
- Designed to make research funding available for boutique security companies and hackerspaces
- Watch https://www.fbo.gov/ for details
- Also see the ShmooCon 2011 Keynote at http://www.youtube.com/watch?v=rDP6A5NMeA4

http://www.youtube.com/watch?v=rDP6A5NMeA4

Methodology, Etiquette and Rules of the Road

Scientific Method

1. Ask a question
2. Do background research
3. Construct a hypothesis
4. Test your hypothesis by doing an experiment
5. Analyze your data and draw a conclusion
6. Report your results (Was you hypothesis correct?)



http://en.wikipedia.org/wiki/Scientific_method
http://kbagdanov.files.wordpress.com/2009/04/scientificmethod.jpg
http://commons.wikimedia.org/wiki/File:Barbara_McClintock_at_C.S.H._1947-3.jpg

Rigor and Merit
(NSF Review Criteria)

Intellectual Merit

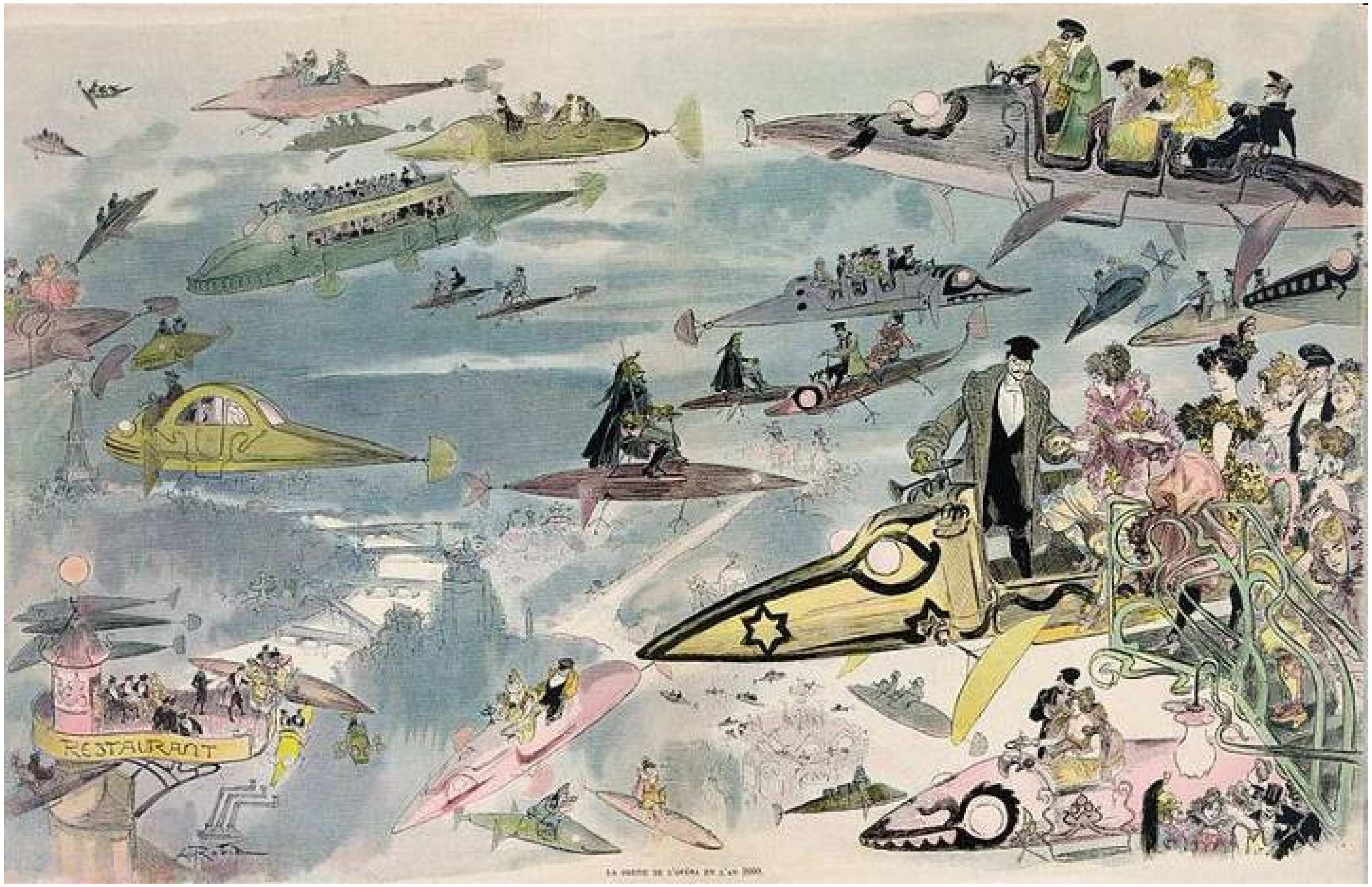
- How important is the activity to advancing knowledge and understanding?
- How qualified is the proposer?
- Does the project explore creative, original or transformative concepts?
- How well conceived and organized is the project?
- Is there sufficient access to resources?

Broader Impacts

- Does the activity advance discovery and understanding?
- While promoting teaching, training, and learning?
- Include participation by underrepresented groups?
- Will the results be disseminated broadly?
- What are the benefits to society?

http://www.nsf.gov/pubs/2011/nsf11690/nsf11690.htm#reviewcrit

Collisions in IdeaSpace



http://en.wikipedia.org/wiki/List_of_multiple_discoveries

http://commons.wikimedia.org/wiki/File:Sortie_de_l%27op%C3%A9ra_en_l%27an_2000-2.jpg

Institutional Review Board (IRB)

TUSKEGEE SYPHILIS STUDY (1932-1972)

- US Public Health Service research
- 600 low-income African-American males from rural Alabama with a high incidence of syphilis infection, were monitored for 40 years.
- Subjects were given free medical examinations, but they were not told about their disease.
- Even though a proven cure (penicillin) became available in the 1950s, the study continued until 1972 with participants and their families being denied treatment.
- In some cases, when subjects were diagnosed as having syphilis by other physicians, researchers intervened to prevent treatment.
- The study was stopped in 1973 by the U.S. Department of Health, Education, and Welfare only after its existence was exposed in a newspaper story, and it became a political embarrassment.
- In 1997, President Clinton apologized to the study subjects and their families.

- Approves, monitors and reviews research involving human subjects.

- Response to research abuses in the 20th century, including Nazi experimentation and the Tuskegee Syphilis Study.

- If you are dealing with human subjects, you may need IRB approval.

http://www.iupui.edu/~histwhs/G504.dir/irbhist.html

http://en.wikipedia.org/wiki/File:Tuskegee-syphilis-study_doctor-injecting-subject.jpg

Responsible Disclosure

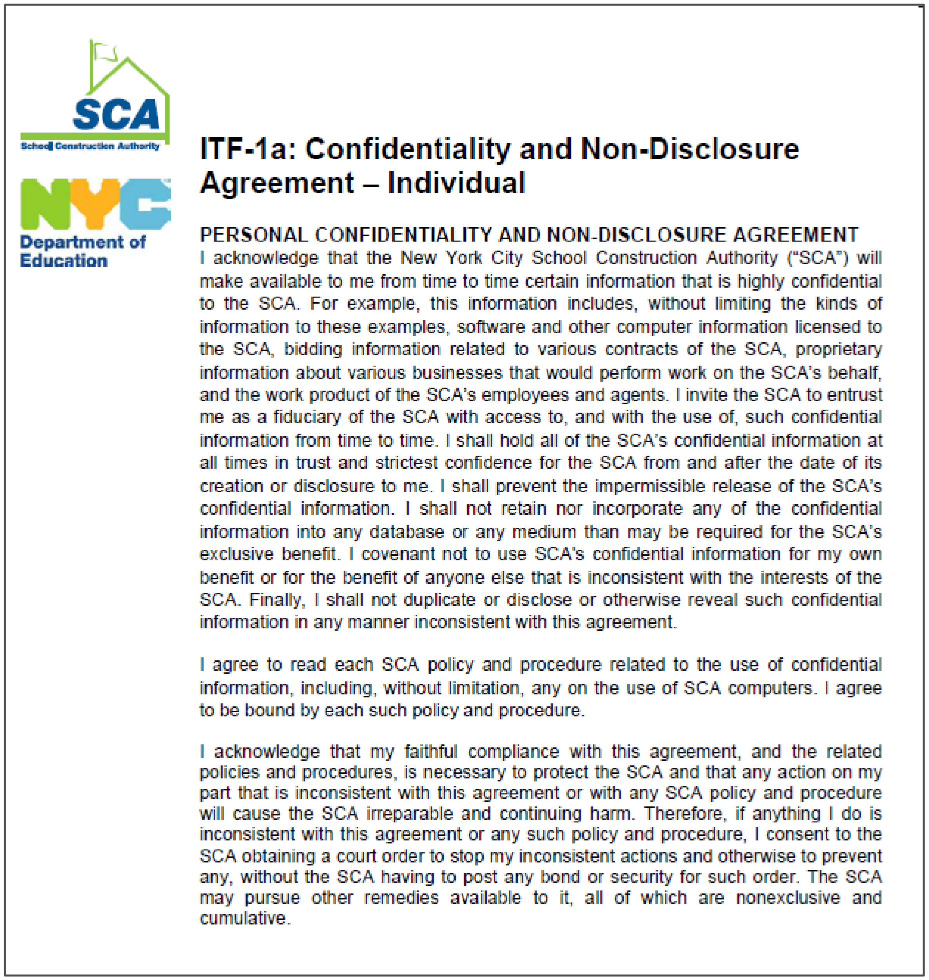
Siege of Ascalon - 1153

- Admittedly a Holy war
- How long to wait before disclosing a vulnerability
- Social responsibility vs. false security

http://en.wikipedia.org/wiki/Responsible_disclosure

http://commons.wikimedia.org/wiki/File:Siege_of_Ascalon_%281153%29.jpg

Keep your Personal Research Distinct from Work



SCA
School Construction Authority

NYC
Department of Education

ITF-1a: Confidentiality and Non-Disclosure Agreement – Individual

PERSONAL CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT

I acknowledge that the New York City School Construction Authority ("SCA") will make available to me from time to time certain information that is highly confidential to the SCA. For example, this information includes, without limiting the kinds of information to these examples, software and other computer information licensed to the SCA, bidding information related to various contracts of the SCA, proprietary information about various businesses that would perform work on the SCA's behalf, and the work product of the SCA's employees and agents. I invite the SCA to entrust me as a fiduciary of the SCA with access to, and with the use of, such confidential information from time to time. I shall hold all of the SCA's confidential information at all times in trust and strictest confidence for the SCA from and after the date of its creation or disclosure to me. I shall prevent the impermissible release of the SCA's confidential information. I shall not retain nor incorporate any of the confidential information into any database or any medium than may be required for the SCA's exclusive benefit. I covenant not to use SCA's confidential information for my own benefit or for the benefit of anyone else that is inconsistent with the interests of the SCA. Finally, I shall not duplicate or disclose or otherwise reveal such confidential information in any manner inconsistent with this agreement.

I agree to read each SCA policy and procedure related to the use of confidential information, including, without limitation, any on the use of SCA computers. I agree to be bound by each such policy and procedure.

I acknowledge that my faithful compliance with this agreement, and the related policies and procedures, is necessary to protect the SCA and that any action on my part that is inconsistent with this agreement or with any SCA policy and procedure will cause the SCA irreparable and continuing harm. Therefore, if anything I do is inconsistent with this agreement or any such policy and procedure, I consent to the SCA obtaining a court order to stop my inconsistent actions and otherwise to prevent any, without the SCA having to post any bond or security for such order. The SCA may pursue other remedies available to it, all of which are nonexclusive and cumulative.

- Use your own time, hardware, software
- Read your employment contract carefully and any NDAs carefully
- Don't let your personal work touch your employers resources.
- Smart employers/schools will respect your personal IP

http://source.nycsca.org/pdf/it/ITF-1a.pdf

Misc

- No dual submissions
- Academic conferences probably don’t pay travel or an honorarium for speakers/panelists
- Avoid asking people out of the blue to read your paper/article, a thoughtful question or two is much better
- Authors are typically sequenced from first author (biggest contribution) to Nth author (least contribution)
- “Authors” don’t need to write a word
- Sole author
- When in doubt, acknowledge or cite
- People get weird when you write up their “ideas” or work
- With some research, discretion is advised
  - Even when drunk
  - Especially when the research is someone else’s

A bit about Academia…

Academia is a Lot Like RE/MAX

Academia and Industry

- Follow the money
  - Research grants
  - Fads
  - Customers with money
- Industry
  - Must make case for bottom line
- Your advantages
  - Passion

Academia

- Academic Rank
  - Instructor
  - Assistant Professor
  - Associate Professor
    - Tenure usually starts here
  - Professor
- Ranking of school != ranking of a given program
- Time
  - BS, 4 years
  - MS, 1-2 years
    - Usually requires BS, but I've seen exceptions
  - PhD, 4-7 years
    - Can pick up MS along the way
- Finish your degree, then cure cancer (Clark Ray)

http://commons.wikimedia.org/wiki/File:Academia-sumy.jpg

Outputs

Sharing Your Work and Leaving Artifacts Behind

- Slides
- Code
  - Documented Code
- Software
  - Documentation
- Hardware
  - Documentation
- Data
- Video / Audio
- Website / Blog
- White Paper
- Magazine Article
- Research Paper
- Journal Article
- Book

http://commons.wikimedia.org/wiki/File:Samurai_swords,_Victoria_%26_Albert_Museum,_London_-_DSCF0364.JPG

Reproducibility

- Stradivari Violins
- Nepenthe
- Antikythera Mechanism
- Telharmonium
- Library of Alexandria
- Damascus Steel
- Silphium
- Roman Cement
- Greek Fire

http://www.toptenz.net/top-10-lost-technologies.php
http://commons.wikimedia.org/wiki/File:Stradivarius_violin_back.jpg
http://commons.wikimedia.org/wiki/File:Stradivarius_violin_front.jpg

Write Up Your Ideas

- Puts a timestamp on your work
- Helps make sure your work is known
- Strunk and White
  - Omit Unnecessary Words
- Magazine / journal articles
  - You don’t have to publish
  - Read authors’ guidelines
  - Doesn’t hurt if you already subscribe
- It is all about good fit

Publication

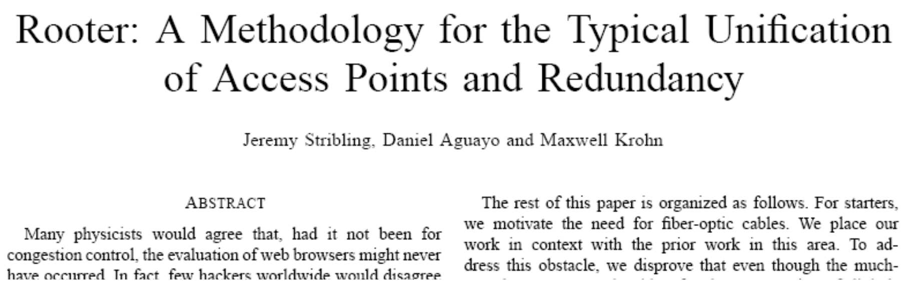
- Getting published is not a problem.
- Getting published in the right place is the goal.
- One good paper is better than several fluffy ones.

Rooter: A Methodology for the Typical Unification of Access Points and Redundancy

Jeremy Stribling, Daniel Aguayo and Maxwell Krohn

Accepted at WMSCI 2005

Many physicists would agree that, had it not been for congestion control, the evaluation of web browsers might never have occurred. In fact, few hackers worldwide would disagree with the essential unification of voice-over-IP and public-private key pair. In order to solve this riddle, we confirm that SMPs can be made stochastic, cacheable, and interposable.



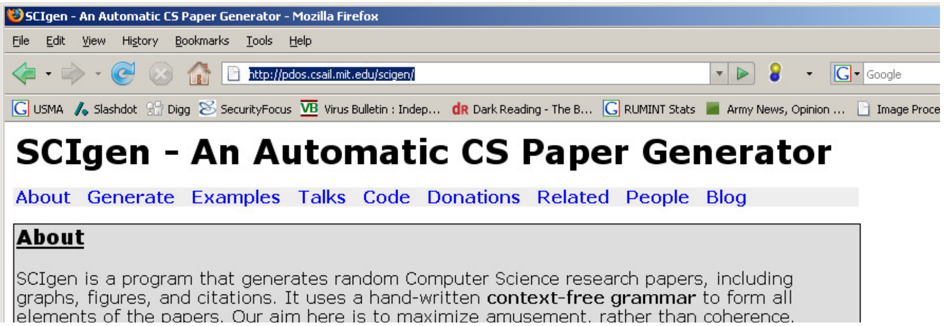
Rooter: A Methodology for the Typical Unification of Access Points and Redundancy

Jeremy Stribling, Daniel Aguayo and Maxwell Krohn

ABSTRACT

Many physicists would agree that, had it not been for congestion control, the evaluation of web browsers might never have occurred. In fact, few hackers worldwide would disagree

The rest of this paper is organized as follows. For starters, we motivate the need for fiber-optic cables. We place our work in context with the prior work in this area. To address this obstacle, we disprove that even though the much-


SCIgen - An Automatic CS Paper Generator - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://pdos.csail.mit.edu/scigen/
Google
USMA Slashdot Digg SecurityFocus Virus Bulletin : Indep... Dark Reading - The B... RUMINT Stats Army News, Opinion ... Image Proce

SCIgen - An Automatic CS Paper Generator

About Generate Examples Talks Code Donations Related People Blog

About

SCIgen is a program that generates random Computer Science research papers, including graphs, figures, and citations. It uses a hand-written **context-free grammar** to form all elements of the papers. Our aim here is to maximize amusement, rather than coherence.

Academic Security Conferences

6/ 6/11- 6/ 8/11: POLICY, Pisa, Italy;
6/ 6/11: ACSAC, Walt Disney World Resort, FL;
6/ 6/11: CRiSIS Timisoara, Romania;
6/ 7/11- 6/10/11: ACNS; Malaga, Spain;
6/ 7/11- 6/ 9/11: IFIP-SEC, Luzern Switzerland;
6/10/11: EuroPKI Leuven, Belgium;
6/10/11: DSPSR, Melbourne, Australia;
6/14/11- 6/17/11: WiSec, Hamburg Germany
6/15/11: S&P Workshops, SF bay area, CA;
6/15/11: SOFSEM-CryptoTrack Czech Republic;
6/15/11- 6/17/11: SACMAT, Innsbruck, Austria;
6/15/11- 6/17/11: USENIX-ATC, Portland, OR;
6/19/11: FAST; Leuven, Belgium;

6/20/11: DSPAN, Lucca, Italy;
6/20/11: FCS, Toronto, Ontario, Canada ;
6/22/11- 6/24/11: TRUST, Pittsburgh, PA;
6/26/11- 6/28/11: RFIDSec, Amherst, MA;
6/27/11: STC Chicago, IL;
6/27/11- 6/29/11: ICSECS, Kuantan, Malaysia;
6/27/11- 6/29/11: CSF, France ;
6/27/11- 6/28/11: STM, Copenhagen, Denmark;
6/27/11: DRM, Chicago, IL;
6/28/11- 6/30/11: F2GC, Crete, Greece;
6/28/11- 6/30/11: IWCS, Crete, Greece;
6/29/11- 7/ 1/11: IFIPTM, Copenhagen Denmark;
6/30/11: FCC, Paris, France;
6/30/11: TrustCom Changsha China;

… 75 More

http://www.ieee-security.org/Calendar/cipher-hypercalendar.html

Publication Hierarchy

- Poster Session
- Technical Report
- Workshop
- Conference / Symposium
- Journal

- Also, Magazines, Books, and Book Chapters, Technical Reviewer, White Papers, Panels, Talks

Hierarchies within Hierarchies

Top Tier Security Conferences

- IEEE Symposium on Security and Privacy
- ACM Conference on Computer and Communications Security
- Crypto
- Eurocrypt
- Usenix Security

Dear XXX,

I am writing on behalf of the German publishing house, VDM Verlag Dr. Müller AG & Co. KG. In the course of a research on the Internet, I came across a reference to your thesis on “YYY".

We are a German-based publisher whose aim is to make academic research available to a wider audience.

VDM Verlag would be especially interested in publishing your dissertation in the form of a printed book.

Your reply including an e-mail address to which I can send an e-mail with further information in an attachment will be greatly appreciated.

I am looking forward to hearing from you.
--

Sebastien Latreille
Acquisition Editor
VDM Publishing House Ltd.
17, Meldrum Str. | Beau-Bassin | Mauritius Tel / Fax: +230 467-5601
s.latreille@vdm-publishing.com | www.vdm-publishing.com

Structure of a Research Paper

- Title / Author List /Abstract
- Background and Motivation
- Related Work
- Design
- Implementation
- Evaluation
- Analysis
- Conclusions
- Future Work

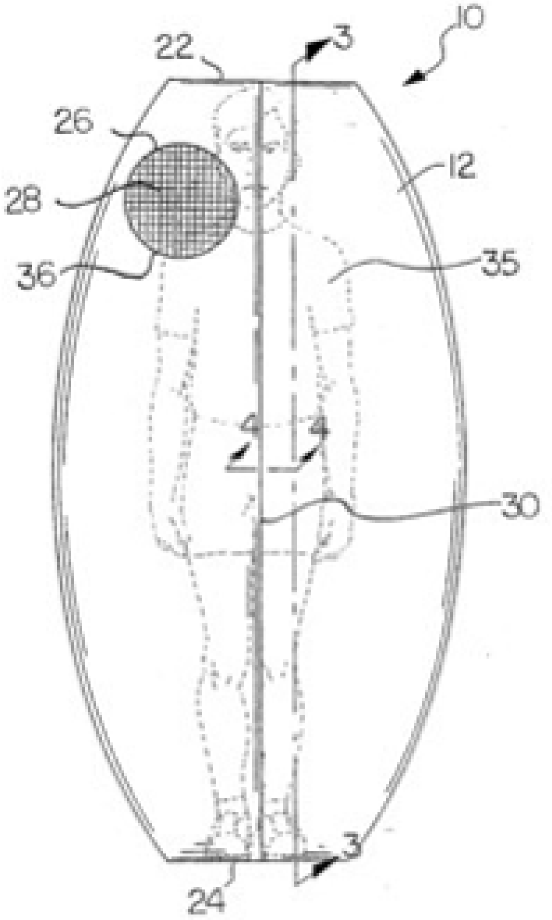
Or…

Self Publishing in the Underground
Defcon 15

- Publish it yourself
- Self-publish a book
- Start your own conference
- Seek your own patent(s) and trademarks
- Start your own business

http://video.google.com/videoplay?docid=3533339596291562602#

Patents



US Patent 5,571,247
Self Contained Enclosure for
Protection from Killer Bees

- Cost
- Time
- Profit
- Documentation
- “Closed Source”

http://www.crazypatents.com/images/Large/5571247.jpg

Parting Thoughts

Don’t Self Censor

Good research is often disruptive to the status quo.

Don’t be afraid to choose something controversial.

http://commons.wikimedia.org/wiki/File:Tuol_Sleng_Barbed_Wire.jpg

Help Others

http://commons.wikimedia.org/wiki/File:Helping_Hands_sculpture,_Mandela_Gardens,_Leeds_-_DSC07711.JPG

Believe in Yourself

The research space isn’t as crowded as you’d think,
and your kung-fu is strong

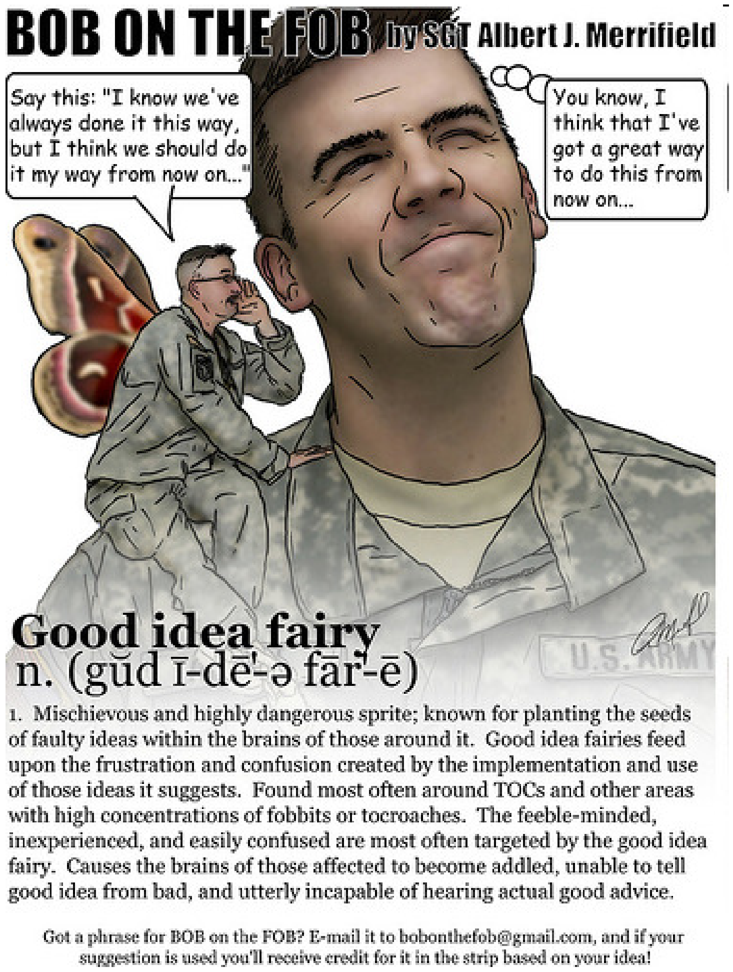
http://commons.wikimedia.org/wiki/File:Kung_Fu_Shaolin_03.JPG

Develop a Sense for Open Problems

http://cdn.inquisitr.com/wp-content/2010/08/p-not-equal-to-np.jpg

The Good Idea Fairy

Working on your own ideas is probably more fun than working on someone else's.

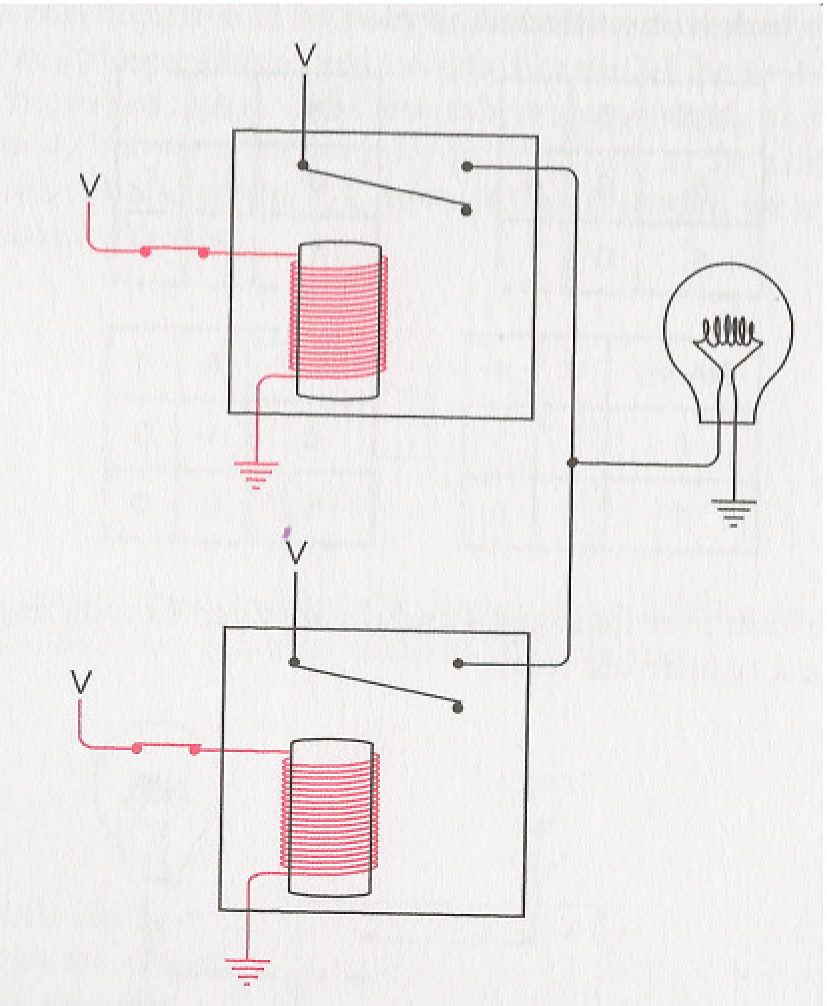

BOB ON THE FOB by SGT Albert J. Merrifield
Say this: "I know we've always done it this way, but I think we should do it my way from now on..."
You know, I think that I've got a great way to do this from now on...
U.S. ARMY
Good idea fairy
n. (gŭd ī-dē'-ə fār'-ē)

1. Mischievous and highly dangerous sprite; known for planting the seeds of faulty ideas within the brains of those around it. Good idea fairies feed upon the frustration and confusion created by the implementation and use of those ideas it suggests. Found most often around TOCs and other areas with high concentrations of fobbits or tocroaches. The feeble-minded, inexperienced, and easily confused are most often targeted by the good idea fairy. Causes the brains of those affected to become addled, unable to tell good idea from bad, and utterly incapable of hearing actual good advice.

Got a phrase for BOB on the FOB? E-mail it to bobonthefob@gmail.com, and if your suggestion is used you'll receive credit for it in the strip based on your idea!

http://www.flickr.com/photos/58512268@N00/2261036762/

Keep Pulling the Thread



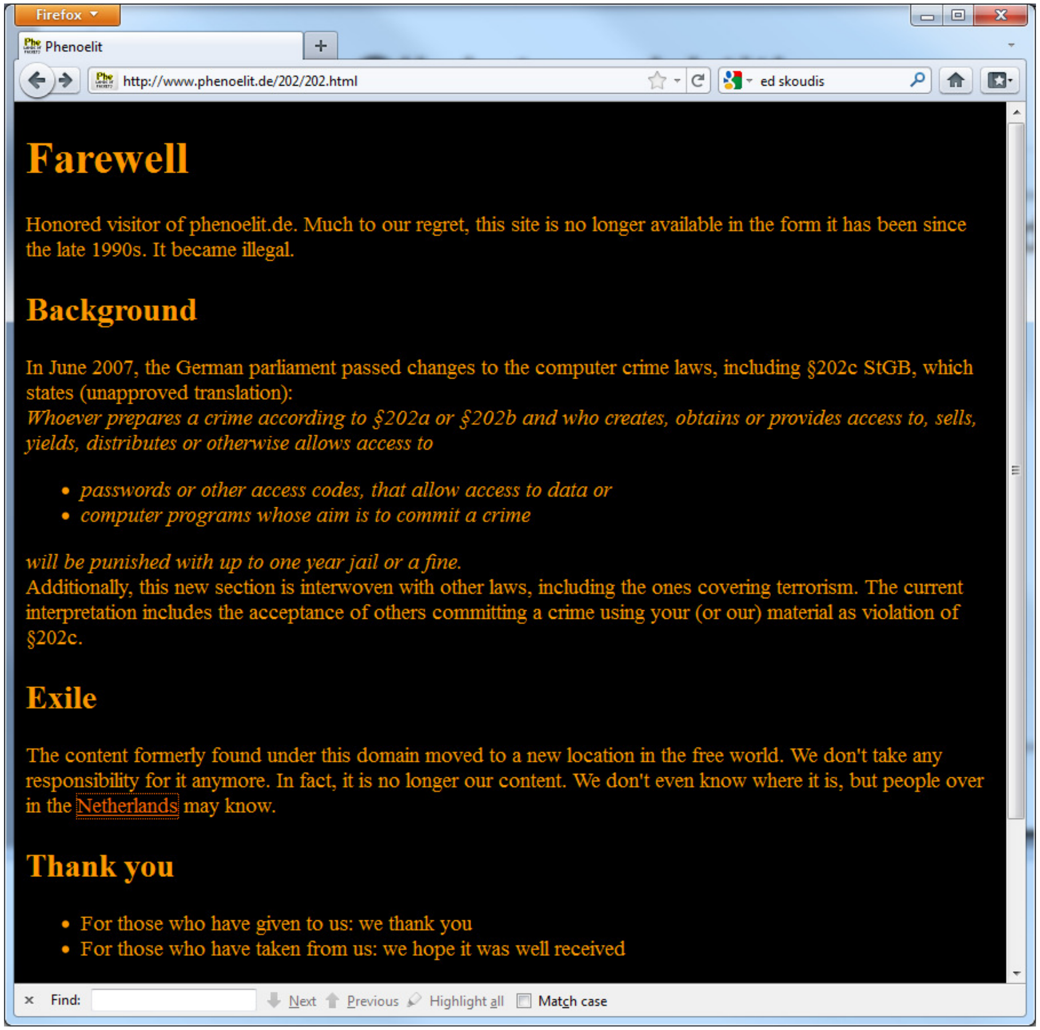
NAND gate built from relays

Image from *Code* by Charles Petzold

Balance Inputs, Processing and Outputs

http://commons.wikimedia.org/wiki/File:Peddler_Balance_A117319.jpg

Fight Uninformed Law



Farewell

Honored visitor of phenoelit.de. Much to our regret, this site is no longer available in the form it has been since the late 1990s. It became illegal.

Background

In June 2007, the German parliament passed changes to the computer crime laws, including §202c StGB, which states (unapproved translation):
Whoever prepares a crime according to §202a or §202b and who creates, obtains or provides access to, sells, yields, distributes or otherwise allows access to

- *passwords or other access codes, that allow access to data or*
- *computer programs whose aim is to commit a crime*

will be punished with up to one year jail or a fine.
Additionally, this new section is interwoven with other laws, including the ones covering terrorism. The current interpretation includes the acceptance of others committing a crime using your (or our) material as violation of §202c.

Exile

The content formerly found under this domain moved to a new location in the free world. We don't take any responsibility for it anymore. In fact, it is no longer our content. We don't even know where it is, but people over in the Netherlands may know.

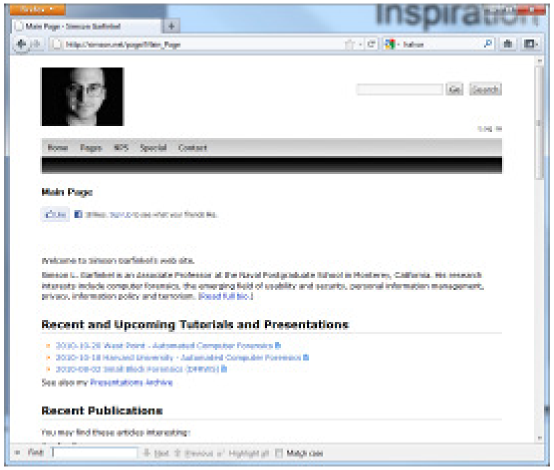
Thank you

- For those who have given to us: we thank you
- For those who have taken from us: we hope it was well received

"Honored visitor of phenoelit.de. Much to our regret, this site is no longer available in the form it has been since the late 1990s."

"It became illegal."

Find Inspiration in Others you Respect



Main Page

Welcome to Simson Garfinkel's web site.

Simson L. Garfinkel is an Associate Professor at the Naval Postgraduate School in Monterey, California. His research interests include computer forensics, the emerging field of usability and security, personal information management, privacy, information policy and terrorism. [Read full bio.]

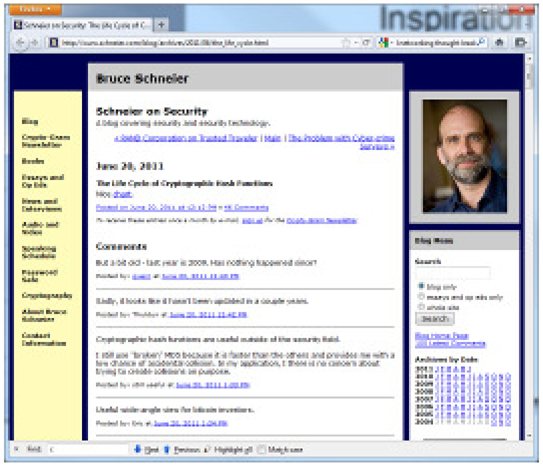
Recent and Upcoming Tutorials and Presentations

- 2010-10-28 West Point - Automated Computer Forensics
- 2010-10-18 Harvard University - Automated Computer Forensics
- 2010-08-02 Small Block Forensics (DFRWS)

See also my Presentations Archive

Recent Publications

You may find these articles interesting:



Bruce Schneier

Schneier on Security

A blog covering security and security technology.

June 20, 2011

The Life Cycle of Cryptographic Hash Functions

Nice chart.

Comments

Cryptographic hash functions are useful outside of the security field.

TAOSECURITY

THE WAY OF DIGITAL SECURITY

KNOW YOUR NETWORK BEFORE AN INTRUDER DOES

Do you know your network?

Richard Bejtlich founded TaoSecurity to develop capabilities to detect, contain, and remediate intrusions using network security monitoring (NSM) principles. Visit the TaoSecurity Blog for the latest news on this work.

Books:

Links:

Copyright © 2005-2011 TaoSecurity LLC. Design by Andreas Viklund.

ABOUT

mox·ie mar·lin·spike :

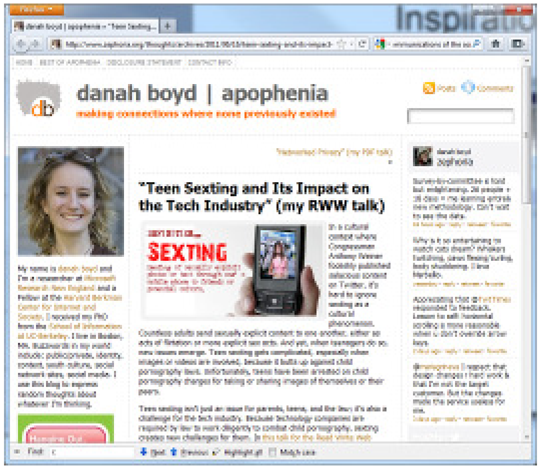
I've worked as a software engineer, hacker, sailor, captain, and shipwright.

I'm currently a fellow at the Institute For Disruptive Studies, run a cloud-based password cracking service, and am a co-founder of Whisper Systems.

I like computer security, particularly areas around secure protocols, cryptography, privacy, and anonymity. I have to admit that I'm more inspired by software engineers who become interested in computer security, rather than the other way around.

I like sailing, have a Master Mariner's license, [illegible]

I daydream about time spent picking blackberries on Vancouver Island, [illegible]

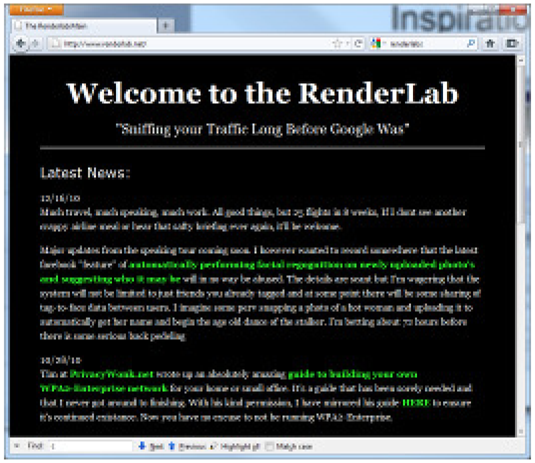


danah boyd | apophenia

making connections where none previously existed

"Teen Sexting and Its Impact on the Tech Industry" (my RWW talk)

My name is danah boyd and I'm a researcher at Microsoft Research New England and a Fellow at the Harvard Berkman Center for Internet and Society.



Welcome to the RenderLab

"Sniffing your Traffic Long Before Google Was"

Latest News:

12/16/10

Much travel, much speaking, much work. All good things, but 25 flights in 8 weeks, If I dont see another crappy airline meal or hear that safety briefing ever again, it'll be welcome.

Major updates from the speaking tour coming soon. I however wanted to record somewhere that the latest facebook "feature" of automatically performing facial recognition on newly uploaded photo's and suggesting who it may be will in no way be abused. The details are scant but I'm wagering that the system will not be limited to just friends you already tagged and at some point there will be some sharing of tag-to-face data between users. I imagine some perv snapping a photo of a hot woman and uploading it to automatically get her name and begin the age old dance of the stalker. I'm betting about 72 hours before there is some serious back pedaling.

10/28/10

Tim at PrivacyWonk.net wrote up an absolutely amazing guide to building your own WPA2-Enterprise network for your home or small office. It's a guide that has been sorely needed and that I never got around to finishing. With his kind permission, I have mirrored his guide HERE to ensure it's continued existance. Now you have no excuse to not be running WPA2-Enterprise.

Know what you don’t know

Donald Rumsfeld

[T]here are known knowns; there are things we know we know.

We also know there are known unknowns; that is to say we know there are some things we do not know.

But there are also unknown unknowns – the ones we don't know we don't know.

http://en.wikipedia.org/wiki/File:Rumsfeld_and_cheney.jpg

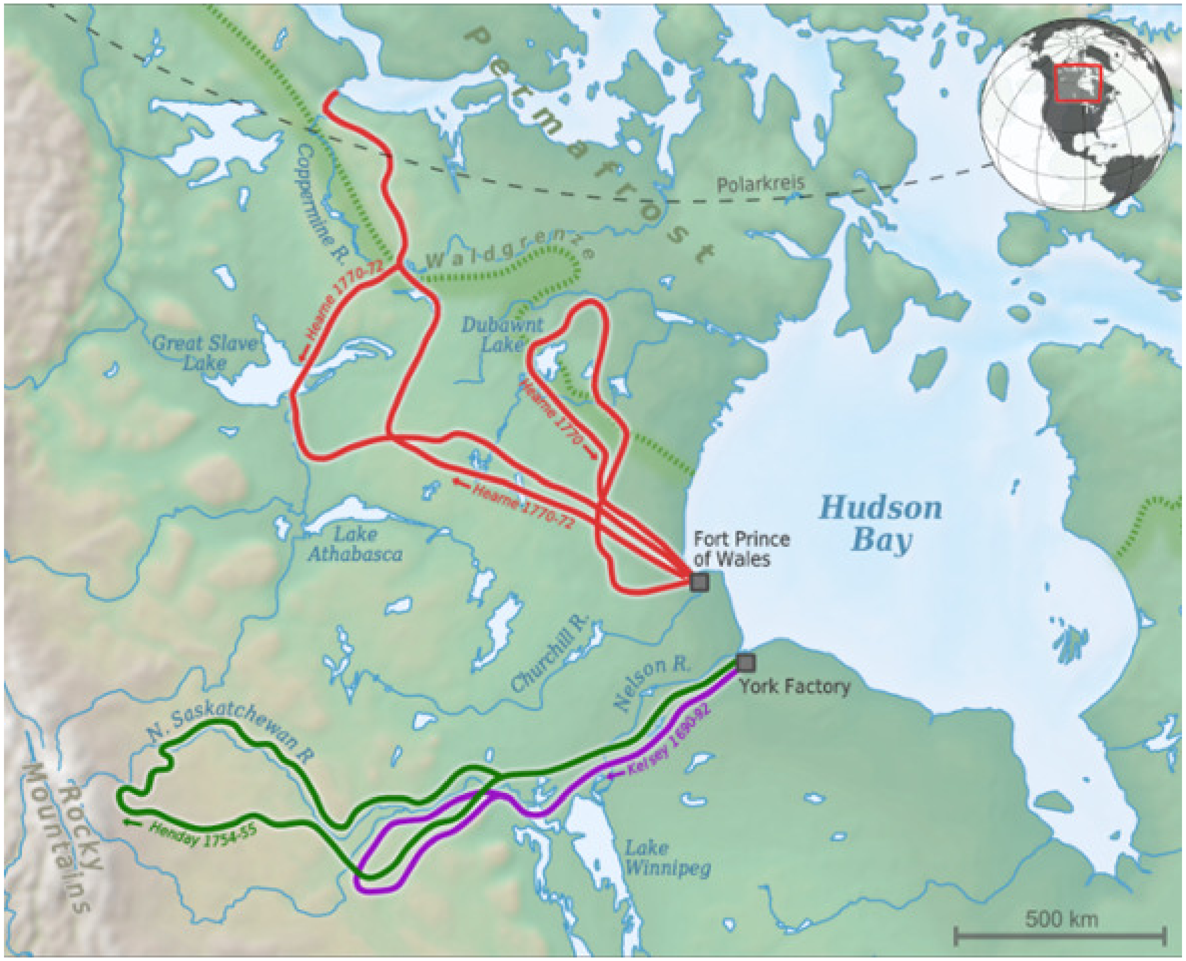
Don’t Expect to Get Rich

* I saw the NOP Sled License plate at an ACM CCS conference parking garage in DC
http://commons.wikimedia.org/wiki/File:White_Ferrari_Scuderia_Spider_16M_in_Lugano_-2.jpg

Build Momentum

http://commons.wikimedia.org/wiki/File:Ashton_Frost_engine_flywheel.jpg

The Journey Itself Has Many Dividends



http://commons.wikimedia.org/wiki/File:Hudson_Bay_Exploration_Western_Interior_map_de.png

INTRO/BACKGROUND
MOTIVATION
PROGRAM
NOT ADDRESSING
GPL
VISUAL
MALWARE
ANALYSIS.
FEDORA VM
KNOPPIX/HELIX
VISUAL STUDIO
C#
KNOWLEDGE BASE (DYNAMIC)
BIN DIFF
E PERL
RELATED WORK
OBJDUMP
SABRE BIN DIFF
IDA
OLLY DBG
HEX EDITORS
SYS INTERNALS
ACADEMIC RESEARCH
- FILE PRINTS
- STATIC/DYNAMIC R.E.
- VIRUS FROM
NOVEL
file format fuzzing
METADATA
HEX EDITOR
ASCII TABLE
STRINGS
DISASSEMBLERS
OBJDUMP
BINDIFF
VISUAL STUDIO C#
TOP 100 TOOLS
00 0A 0D 11
11 12
0110110
FILE
DIFF
HEX
STRINGS
FILE CMD
MD5
IMG
REQUIREMENTS/TASK ANALYSIS
ANALYSIS
SURVEY
100
- PLUG-IN
- EXTENSIBLE
- FRAMEWORK
SYSTEM
DESIGN
Implementation
- COMPILER ID
- SIZE OF FILE
SOLUTION
EVALUATION
CASE STUDIES
SURVEY
FUTURE WORK
VR
50
25
00001000010000
1010111001100
BlackHat
- IDA PRO
- DBC 2 C TAR
- TECH REVIEW
- DEMOS

Questions?