Frank Lloyd Wright was Right

Reflections on Architecture,
Computer Security,
Risk and Investments

Frank Lloyd Wright (1867-1959)

• Architect
• Curmudgeon
  – BAFH
• High School Dropout
• University Dropout
• Art Dealer, Philanderer, Fraud
• Genius
Le Corbusier
Florida Southern College (1938)

Fallingwater (1934)
Early in life I had to choose between honest arrogance and hypocritical humility. I chose the former and have seen no reason to change.

Johnson Wax Headquarters (1939)
Hell With The Lid Off

Louisa St.
Harding Way

Orion St.
Toboggan St. & Rising Main St.

Vinecliffe St.
Sycamore St.

Interstate 376
Interstate 376
Topography

City Fathers: What do you think?

Frank: I liked it better when I couldn’t see it.

City: Okaaaay… What should we do?

Frank: Raze it and start over!
Raze It and Start Over?

- Never gonna happen
- Too expensive
- Too inconvenient
- They’ll find a way to fix it

- We’ll never be unemployed
History

- Frank Lloyd Wright died 50 years ago [1959]
History

• Frank Lloyd Wright died 50 years ago [1959]
• ARPANet was born 40 years ago [1969]
• Unix created 40 years ago [1969]
History

• Frank Lloyd Wright died 50 years ago [1959]
• ARPANet was born 40 years ago [1969]
• Unix was born 40 years ago [1969]
• I start using Unix [1976]
• Macintosh released 25 years ago [1984]
• Morris Worm released 21 years ago [1988]
• Windows 3.0 released 20 years ago [1989]
• First WWW Conference 15 years ago [1994]
• Linux 1.0 released 15 years ago [1994]
History

- Frank Lloyd Wright died 50 years ago [1959]
- ARPANet was born 40 years ago [1969]
- Unix was born 40 years ago [1969]
- I start using Unix [1976]
- Macintosh released 25 years ago [1984]
- Morris Worm released 21 years ago [1988]
- Windows 3.0 released 20 years ago [1989]
- First WWW Conference 15 years ago [1994]
- Linux 1.0 released 15 years ago [1994]
- Thompson & Ritchie: National Medal of Technology [1999]
- Google [1999]
- My mother embraces email 10 years ago [1999]

We’re In Deep Kimchee

- Viruses
- Worms
- Trojans
- Keyloggers
- Botnets
- Phishing
- Phlashing
- Spam
- SQL Injection
- Phone viruses!
- Internet
- Intranet
- LAN
- WAN
- PAN
- Bluetooth
- RFID
- GPRS
- Pacemakers!
- Active Infiltration
- Cyberterrorism
RFID as a Malware Vector

• RFID can spread viruses & worms
  http://www.rfidvirus.org/
• Classic attacks
  – Buffer overflow
  – SQL injection
• My cats have an RFID chip…

Well, that’s hard to do, right?
Best Company Name Ever!

RBAC

Where Am I?

- I have an HTML page
- that was built using SSI
- that has a `<FORM>`
- the invokes a CGI Query
- that runs a Perl script
- (that uses `Template::Toolkit`)
- to create an Ajax response
- (in a frameset)
- that updates a `<DIV>`
- that invokes some Javascript
- (with `onLoad`, of course)
- that triggers an asynchronous timeout event
- that redraws the page by changing the CSS

20 developers

15 timezones

Apache Sandboxes
Auto-recompile

Session Keys
MVC
MySQL
Class DBI

Caching
Selective JS Upload

jQuery
Dynamically generated
We have technological ADD

This is “normal” coding practice

Yahoo 1999
Yahoo 2009

Lycos 1999
“Form Follows Function”… that has been misunderstood. Form and function should be one, joined in a spiritual union.

*Frank Lloyd Wright*
Google 1999

Google 2009
K.I.S.S.

- The United States Internal Revenue Service code is codified in 26 USC
- Tax Exempt Status is defined in Subtitle A, Chapter 1, Subchapter F, Part I, §501, ¶(a)
  - Also called 501(a)
- 501(b) discusses taxation of tax-exempt groups
- 501©1 through 501©28 lists specific criteria
- 501® discusses non-exemption of Communist Controlled organizations

How Can I Fix That?

- Preferences, of course!
Okay, How Can I Fix That?

No, Really, I Want to Fix That!
Fifth Ave & Penn Ave

Beechwood Blvd & Monitor St
K.I.S.S.

• Keep It Simple, Stupid
• Keep it Simple for **Security**
• Keep it Simple for **Safety**
• Keep it Simple for **Sanity**

Less is only more when more is no good.

*Frank Lloyd Wright*
It’ll only get worse: Moore’s Law

Why does this happen?
Why does this happen?

Autorun

- Microsoft will (theoretically) disable it in
  - Windows 7
  - Future versions of Vista and XP
    [http://tech slashdot org/article.pl?id=09/04/29/2110241](http://tech.slashdot.org/article.pl?id=09/04/29/2110241)
- About time!
  - Conficker, etc
Beauty is skin deep. Ugly goes clear to the bone.

unknown
Installing Our Software...

Click "Yes" if prompted.

Get to your meetings faster! When prompted, click the "Show Certificate" button, check the "Always trust these certificates" checkbox, then click the "Yes" button.

This applet was signed by "Citrix Online," but Java cannot verify the authenticity of the signature's certificate. Do you trust this certificate?

Click Trust to run this applet and allow it unrestricted access to your computer. Click Don't Trust to run this applet with standard Java restrictions.

Always trust "Citrix Online"

Citis Online

Issued by: VeriSign Class 3 Code Signing 2004 CA
Expires: 07/01/09
This certificate is valid

Trust
Details

Hide Certificate
Don't Trust
Trust
Most Users are Idiots


Proceedings of the Human Factors and Ergonomics Society

So why…

• Do we expect them to understand
  – Authentication?
  – Authorization?
  – Certificates?
  – Certificate Authorities?
• They cannot make informed decisions…
  – But we require them to!
• WE are the problem!
The page at http://etalon-en-chaaleur.over-blog.com says:

ATTENTION : SITE / BLOG POUR ADULTES, STRICTEMENT RESERVE A UN PUBLIC MAJEUR

Ce site / blog est reserve a un public majeur et averti. Il contient des textes, des liens, des images, des videos qui peuvent etre choquants pour des personnes mineures.

Pour acceder a ce site je certifie sur l'honneur :
- etre majeur selon la loi en vigueur dans mon pays et que les lois de mon etat ou mon pays m'autorisent a acceder a ce site / blog
- admettre que ce site / blog a le droit de me transmettre des donnees a caracterise pornographique :
- ne pas etre choque par aucun type de sexualite et m'interdit de poursuivre la societe editrice de toute action judiciaire sur le type de sexualite :
- ne pas faire etat de l'existence de ce site / blog et a ne pas en diffuser le contenu a des mineurs :
- etre en la possibility d'empacher l'acces de etalon-en-chaaleur.over-blog.com a toutes personnes mineures :
- assumer ma responsabilite, si un mineur accede a ce site / blog a cause de negligeance de ma part : absence de protection de l'ordinateur personnel, absence de logiciel de censure, divulgation ou perte du mot de passe de securite :

Si toutefois ce site / blog presente un contenu litigieux, veuillez contacter l'auteur du blog et la societe editrice de ce site / blog.

J'ai lu attentivement les conditions d'acces ci-dessus de ce site / blog ayant un contenu strictement reserve aux adultes et accepte electroniquement mon accord avec ce qui precede en cliquant sur le bouton OK.
Spam

- 94% (at least) of all email is spam!
- 97% of my email is spam!

![Graph of Spam to Ham % over months]

- 62,000,000,000,000
  - 62 x $10^{12}$ spam emails/year
  - 33 x $10^9$ KWh
- What will it take to fix?
- Microsoft, Apple, and Unix/Linux to agree on a new protocol
NEWS FLASH!
Microsoft/Apple/Linux Agree!

The Sorrow and the Pity

• We get crap because there is no market pressure for the good stuff
  – IPv6
  – DNSSEC
  – Tagged packet support (IPSO vs. 802.1Q)
  – Secure wireless
• Market shortsightedness
  – Cheap / fast / good
• We can provide openness and security!
  – Have the design account for topography
If I have seen further it is only by standing on the shoulders of giants

—Sir Isaac Newton

Mathematicians stand on each other’s shoulders while computer scientists stand on each other’s toes

—Richard Hamming

Users Don’t See As Far…

…because they stand in the footprints of giants!
Date: Mon, 08 Sep 2008 14:02:50 +0100
From: ROBERT SWAN MUELLER III <online12135@earthlink.net>
Subject: FEDERAL BUREAU OF INVESTIGATION FBI.

WASHINGTON D.C. ROOM, 7367
J. EDGAR HOOVER FBI BUILDING
935 PENNSYLVANIA AVENUE,
NW WASHINGTON, DC 20535,

RE: FEDERAL BUREAU OF INVESTIGATION SEEKING TO WIRETAP THE INTERNET

We believe this notification meets you in a very good state of mind and health. We the Federal bureau of investigation (FBI) Washington, DC in conjunction with Internet Crime Complaint Center (IC3), National White Collar Crime Center (NW 3C), Bureau of Justice Assistance (BJA) and some other relevant Investigation Agencies here in the United States of America have recently been informed through our Global intelligence monitoring network that you presently have a transaction going on with the Central Bank of Nigeria (CBN) as regards your over-due contract payment which was fully endorsed in your favour accordingly.

It might interest you to know that we have taken out time in screening through this project as stipulated on our protocol of operation and have finally confirmed that your contract payment is 100% genuine and hitch free from all facet and of which you have the lawful right to claim your payment without further delay. Having said all these we will further advise that you go ahead in dealing with the Central Bank office accordingly as we will be monitoring all their activities with you as well as your correspondence at all level. Also be informed that we recently had a meeting with the Executive Governor of the Central Bank of Nigeria, in the person of Prof. Chukwuma Soludo along with some of the top officials of the Ministry regarding your case and they made us understand that your file has been held in abase depending on when you personally come for the claim.

They also told us that the only problem they are facing right now is that some unscrupulous elements are using this project as an avenue to Scam innocent people off their hard earned money by impersonating the Executive Governor and the Central Bank office.

We were also made to understand that a lady with name Mrs. Joan C.Bailey from OHIO has already contacted them and also presented to them all the necessary documentations evidencing your claim purported to have been signed personally by you prior to the release of your contract fund valued at about US$10,700,000.00 (Ten million Seven Hundred Thousand United States Dollars), but the Central Bank office did the wise thing by insisting on hearing from you personally before they go ahead on wiring your fund to the Bank's information which was forwarded to them by the above named Lady, so that was the main reason why they contacted us so as to assist them in making the investigations.
http://www.upi.com/News_Photos/Features/Nuclear_Power_Plant_in_Iran/1581/2/
Missing the obvious…

Easy targets, sacred cows

- **Windows 7**
  - Vulnerable to first 8/10 wild viruses
- **Null pointer dereference bug grants root**
  - Fixed this week in 2.6.32rc
  - RHEL doesn’t have mmap_min_addr quick fix
    [http://www.theregister.co.uk/2009/11/03/linux_kernel_vulnerability](http://www.theregister.co.uk/2009/11/03/linux_kernel_vulnerability)
Why Is This *Still* Happening?

- Why are there wireless routers with default SSID and password?
- Why are there administrative accounts with no password?
- Why are people on the net using Windows 98?
- Why are we the burial society?
- Why aren’t we like the CDC?
GPS Enabled Asthma Inhalers

• Great Idea!
  – Prevent asthma attacks through correlation
  – http://i.gizmodo.com/5207511/
• Can be used maliciously, too…

We have FAILED at our job…

…by misinterpreting what our job is!
We Can See The Problem!

Are We Willing to See the Solution?

Or do we just want Security Job Security?
A physician can bury his mistakes, but the architect can only advise his clients to plant vines.

Frank Lloyd Wright
We Are Planting Ivy

- Patches
- Hacks
- Backwards compatibility
- Revisions
- Bug-for-bug compliance
- Pretty graphics!
- Flash animation!
- Clippy!

Pictures deface walls oftener than they decorate them.

--Frank Lloyd Wright
Raze It and Start Over?

• Never gonna happen
• Too expensive
• Too inconvenient
• They’ll find a way to fix it

• We’ll never be unemployed

Y Gwir yn Erbyn y Byd

The Truth Against the World
Or we can change jobs…

• Switch from reactive…
  – to proactive

• From neutral…
  – to advocatory

• Or it will all fall down…
  – it is already happening!

CitiGroup Center (NYC)
Hacks are Bad

• Replace welded joints with bolts
  – Cheaper
  – Quicker
• Building might collapse in hurricane winds
  – Every 55 years on average
  – Every 16 years, if tuned mass damper failed
• Newspaper strikes are “good”
  – Repair work done in secret
  – Hurricane Ella veered away with hours to spare
Examples

• Write it right!
  – *NASA does it*…

• Apolitical improvements to email
  – *Refuse to interface w/old protocol after 3-5 years*

• Proper security decisions by software
  – *Take the stupid human out of the loop*
  – *Quarantine infected machines*
Examples

• Refuse to allow users to be stupid
  – *No bad passwords*
  – *Start with good configurations*

• Alter the market pressure
  – *Embarrass the purveyors of crap*
  – *Tout (or push for!) the good solutions*

There *are* precedents!

• The Big Stink ➞ London Sewers (1850’s)
• B&W ➞ Color TV in Europe
• Analog ➞ Digital TV in US/Australia
• NCP ➞ TCP (ARPAnet ➞ Internet)
• A big mess ➞ The Big Dig (Boston)
• Sydney Harbor Bridge

• Problems/solutions are not purely technical
The thing always happens that you really believe in; and the belief in a thing makes it happen

--Frank Lloyd Wright

Frank Lloyd Wright was Right

Reflections on Architecture,
Computer Security,
Risk and Investments