Practical and Elite Key Management

Jacob Welsh
CTO, JWRD Computing
http://fixpoint.welshcomputing.com/
sales@jwrd.net

IRC: jfw

0CBC 0594 1D03 FD95 C3A4
7654 AE0D F306 0255 94B3

Overview

- Context
  - How to get rich with Bitcoin
    - The four simple steps!
  - Monsters under the bed
    - What you don’t know CAN hurt you!
  - How JWRD can help
- Demonstration of cryptographic concepts
- Demonstration of tools
- (Time permitting) Hashes and mining

How to get rich with Bitcoin

- “BTC is just a currency, it can’t generate me income like this alt-ether-ico-dao-nft-defi-du-jour”
  - Did you mean: “BTC won’t help me get rich quick by exploiting the accomplishments of others without having to lift a finger” ?

Get rich slow with Bitcoin

1. Buy BTC.
   - As much as you can!
2. Don’t lose your BTC.
3. Build & maintain trading relationships so you can cash in & out when you need to.
   - That means **people**. Public exchanges are subject to fiat “authorities” on top of their own deep reserves of idiocy.
4. Hold for 5+ years.

See also: http://trilema.com/2017/the-universal-plan-for-wealth/

Get rich slow with Bitcoin

2. Don’t lose your BTC...

Monsters under the bed

“...do not be afraid of all the things that are scary. The most they can do while under your gaze is make you stronger. Be instead afraid of the things you make no effort to understand, because from behind they can give you quite the sound trashing. And the worst part of it is... you'll likely never know.”

- Mircea Popescu

  http://trilema.com/2014/a-conceit-or-the-importance-of-blogging/

Well-known risks in bitcoin

- Counter-party risk (shady exchanges)
- “Hacking”
  - Buggy, insecure software
  - Weak passwords
  - Social engineering
- Data loss
- Physical theft
- Disinformation
- More?

“Minimize funds held on exchanges”

- But who are your *implicit* counter-parties?
- Are Apple, Microsoft, Google and Intel products fit to secure the world’s digital cash?
- In what power structure do these firms operate?
- How many people you don’t know can touch the code?
- How many people you *do* know are vetting the code?
- How much code *is* there?

Can you trust your software today?

CVE Details
The ultimate security vulnerability datasource

Search | View CVE (e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In | Register

Vulnerability Feeds & Widgets New | www.itsecdb.com

- Home
- **Browse :**
  - Vendors
  - Products
  - Vulnerabilities By Date
  - Vulnerabilities By Type
- **Reports :**
  - CVSS Score Report
  - CVSS Score Distribution
- **Search :**
  - Vendor Search
  - Product Search
  - Version Search
  - Vulnerability Search
  - By Microsoft References
- **Top 50 :**
  - Vendors
  - Vendor Cvss Scores
  - Products
  - Product Cvss Scores
  - Versions
- **Other :**
  - Microsoft Bulletins
  - Bugtraq Entries
  - CWE Definitions
  - About & Contact
  - Feedback
  - CVE Help
  - FAQ
  - Articles
- **External Links :**
  - NVD Website
  - CWE Web Site
- **View CVE :** Go (e.g.: CVE-2009-1234)

Google » Chrome : Vulnerability Statistics

Vulnerabilities (1858) | CVSS Scores Report | Browse all versions | Possible matches for this product | Related Metasploit Modules

Related OVAL Definitions : Vulnerabilities (971) | Patches (298) | Inventory Definitions (1) | Compliance Definitions (0)

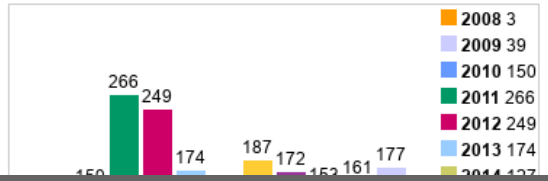
Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

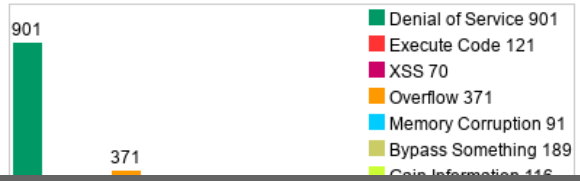
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2008	3	1	1				1								
2009	39	16	11	8	3		7			4	3		1		
2010	150	82	22	27	27		4			13	13		1		2
2011	266	188	11	62	12		3			21	8	1			
2012	249	195	13	60	9		8			14	8	2			
2013	174	120	5	41	12		3	4		9	8				
2014	127	86	4	19	4		8	2		14	6		1		
2015	187	124	8	37	13		5			31	5	2			
2016	172	83	2	31	3		7	1		37	16				
2017	153	5	10	30	5		13			11	16	1			
2018	161	1	15	33	2		8			10	17				
2019	177		19	23	1		3			25	16				
Total	1858	901	121	371	91		70	7		189	116	6	3		2
% Of All		48.5	6.5	20.0	4.9	0.0	3.8	0.4	0.0	10.2	6.2	0.3	0.2	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

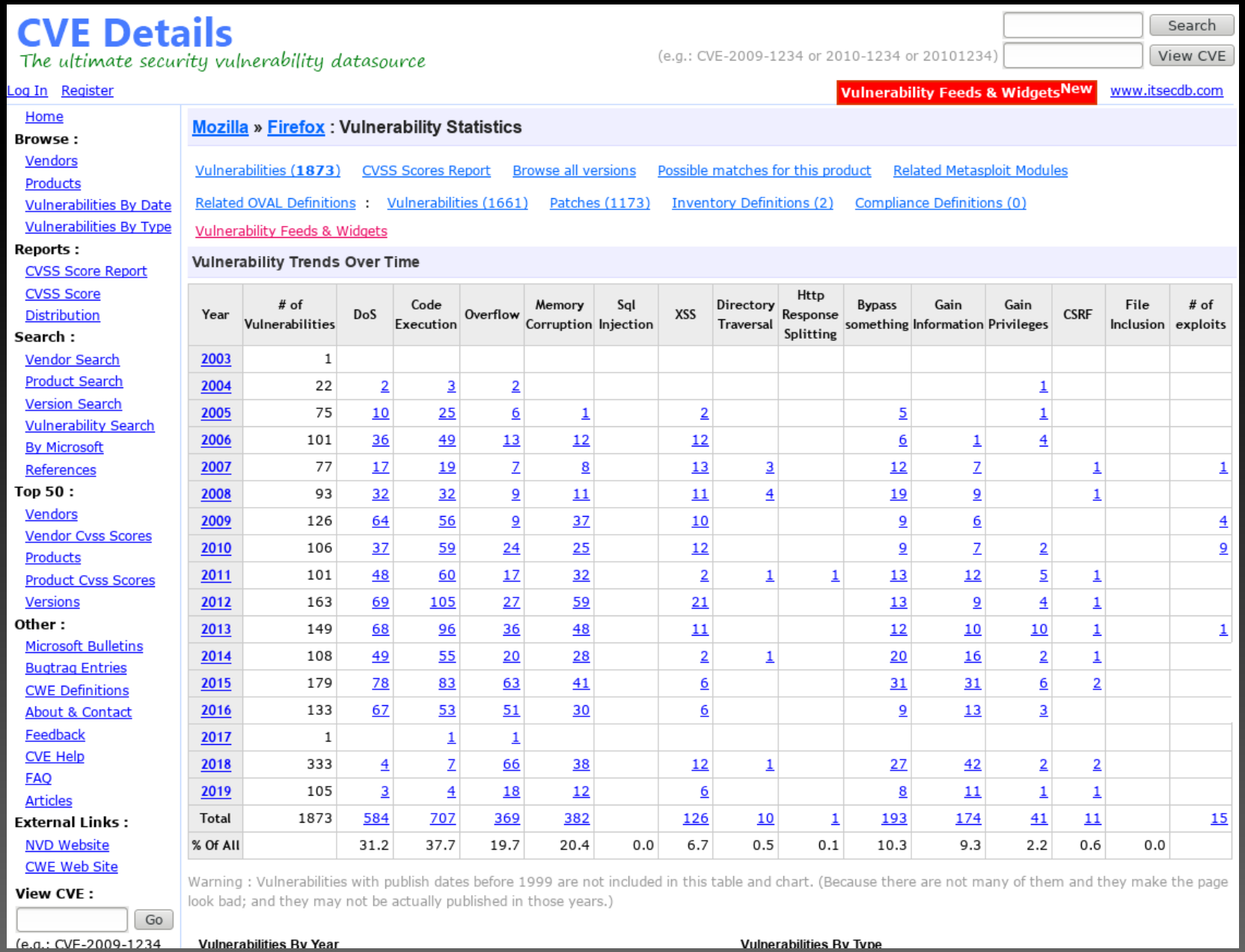
Vulnerabilities By Year



Vulnerabilities By Type



Can you trust your software today?



CVE Details
The ultimate security vulnerability datasource

Search
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)
View CVE

Log In Register

Vulnerability Feeds & Widgets New
www.itsecdb.com

Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
External Links :
NVD Website
CWE Web Site
View CVE :
Go
(e.g.: CVE-2009-1234

Mozilla » Firefox : Vulnerability Statistics

Vulnerabilities (1873) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules
Related OVAL Definitions : Vulnerabilities (1661) Patches (1173) Inventory Definitions (2) Compliance Definitions (0)
Vulnerability Feeds & Widgets

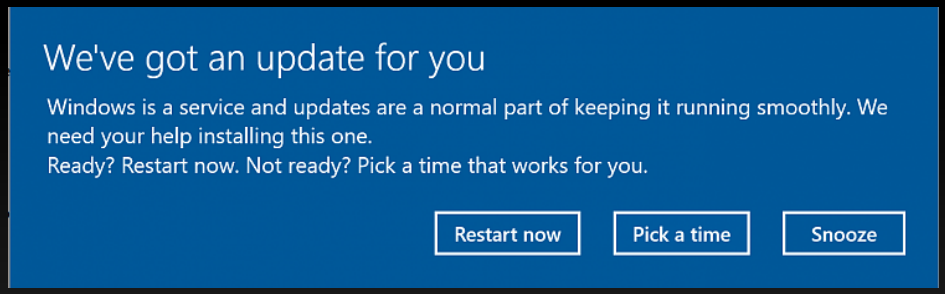
Vulnerability Trends Over Time

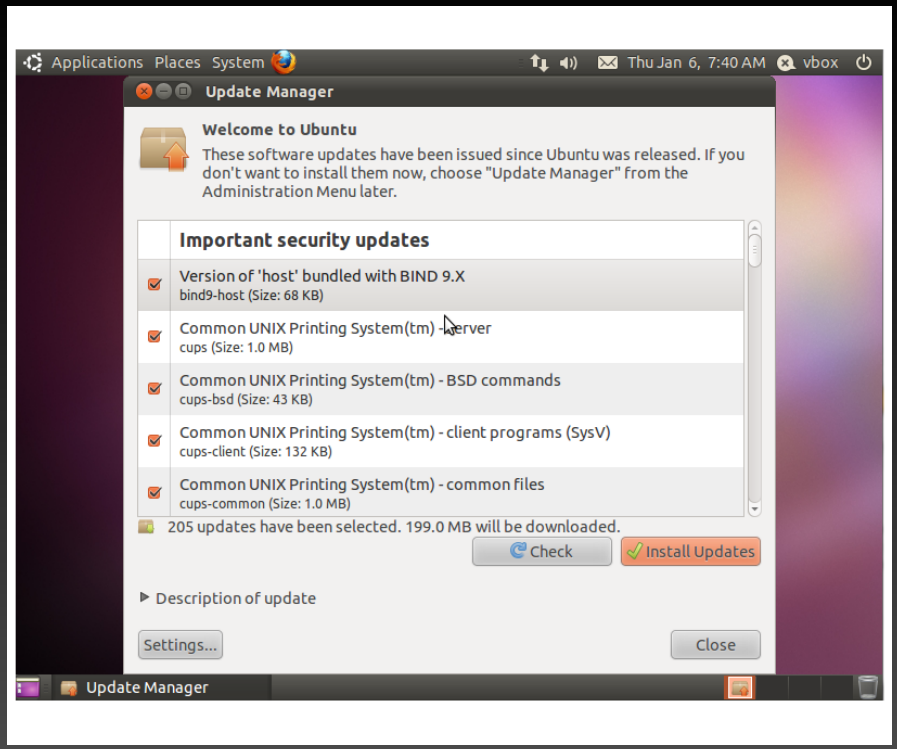
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2003	1														
2004	22	2	3	2								1			
2005	75	10	25	6	1		2			5		1			
2006	101	36	49	13	12		12			6	1	4			
2007	77	17	19	7	8		13	3		12	7		1		1
2008	93	32	32	9	11		11	4		19	9		1		
2009	126	64	56	9	37		10			9	6				4
2010	106	37	59	24	25		12			9	7	2			9
2011	101	48	60	17	32		2	1	1	13	12	5	1		
2012	163	69	105	27	59		21			13	9	4	1		
2013	149	68	96	36	48		11			12	10	10	1		1
2014	108	49	55	20	28		2	1		20	16	2	1		
2015	179	78	83	63	41		6			31	31	6	2		
2016	133	67	53	51	30		6			9	13	3			
2017	1		1	1											
2018	333	4	7	66	38		12	1		27	42	2	2		
2019	105	3	4	18	12		6			8	11	1	1		
Total	1873	584	707	369	382		126	10	1	193	174	41	11		15
% Of All		31.2	37.7	19.7	20.4	0.0	6.7	0.5	0.1	10.3	9.3	2.2	0.6	0.0	

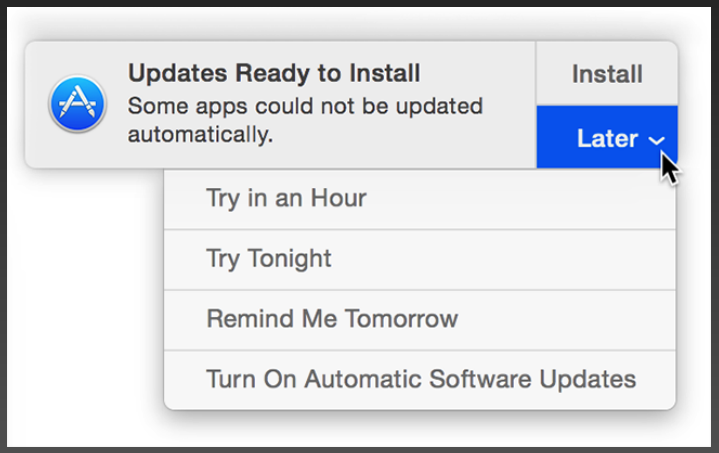
Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

Vulnerabilities By Year
Vulnerabilities By Type

Can you trust your software tomorrow?







Deliberately compromised hardware

- Intel Management Engine (2009)
- AMD Platform Security Processor (2013)
- UEFI firmware and “Secure Boot”
- ARM TrustZone, often opaque boot firmware
- Other architectures mostly confined to large-scale or low-power markets

Cold storage

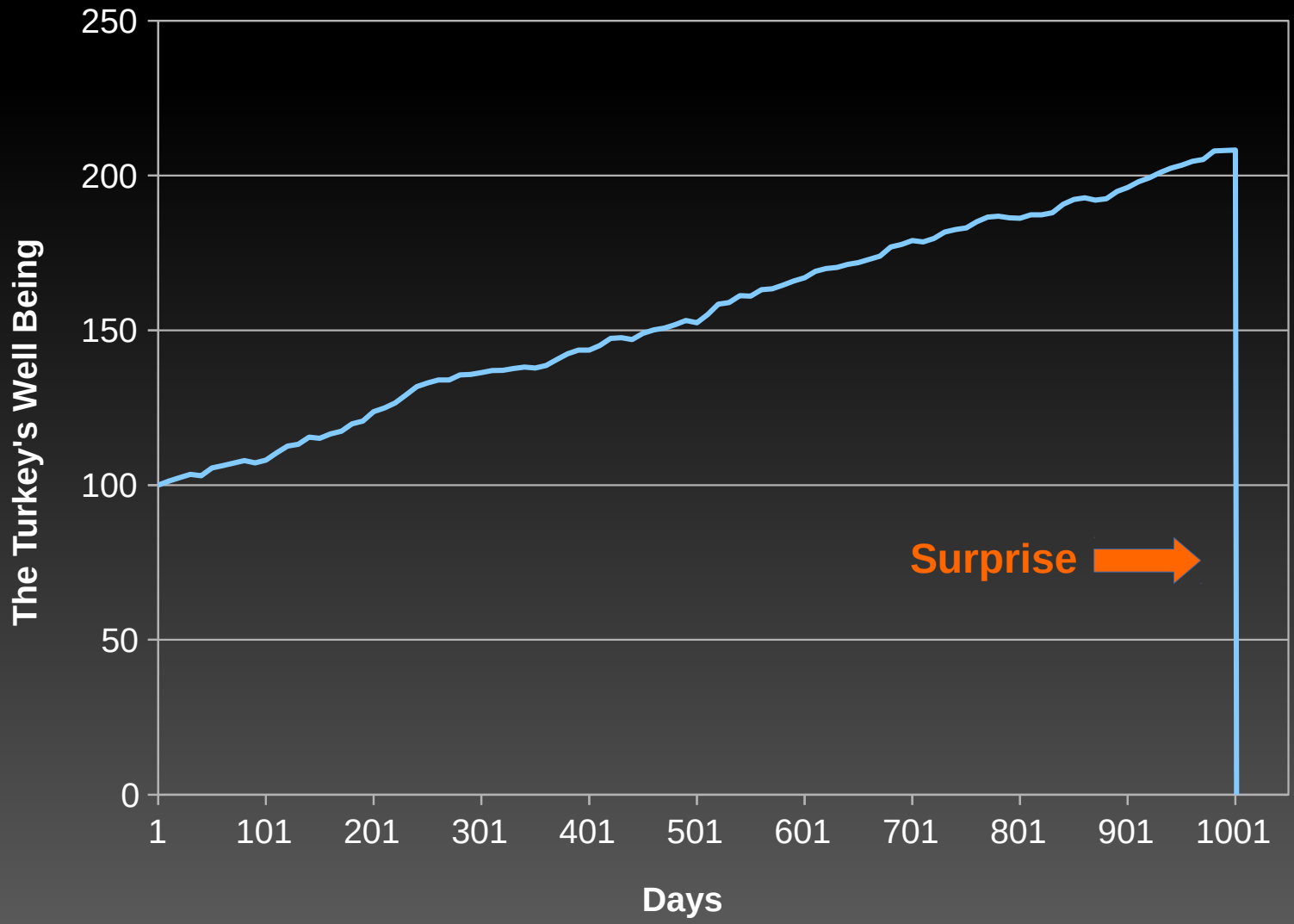
- “Paper” wallets?
  - Still need PC to generate keys
  - Still need *online* PC to spend the funds
- “Hardware” wallets?
  - Still need *online* PC to operate, exposing to bad **input** and **side-channel attacks** (power, timing)
  - Mass-market products with complex software stacks, security flaws and blind-trust **firmware updates**
  - Unverifiable **entropy sources**
- Not so cold after all...

A typical Bitcoin Hardware Wallet.

Do the risks matter?

- “What I’m doing has worked fine so far.”
- The problem of induction: can you predict the future based on past observations?
  - Who really owns “your” computer? Will it remain loyal in the hour of need ?
  - Illustrated through the worldview of a turkey (aka Russell’s chicken, adapted for a New World audience by Nassim Taleb)

1000 and 1 days in the life of a Thanksgiving turkey



Selected public Bitcoin losses

Year	Loser	Estimated amount
2014	MtGox	850`000 BTC
2015	Bitstamp	19`000 BTC
2016	Bitfinex	120`000 BTC
2017	NiceHash	4`700 BTC
2018	Zaif	6`000 BTC
2019	Binance	7`000 BTC

And earlier: http://trilema.com/2012/the-bitcoin-drama-timeline/

“So my friends : do not be afraid of all the things that are scary. The most they can do while under your gaze is make you stronger. Be instead afraid of the things you make no effort to understand, because from behind they can give you quite the sound trashing. And the worst part of it is... you'll likely never know.”

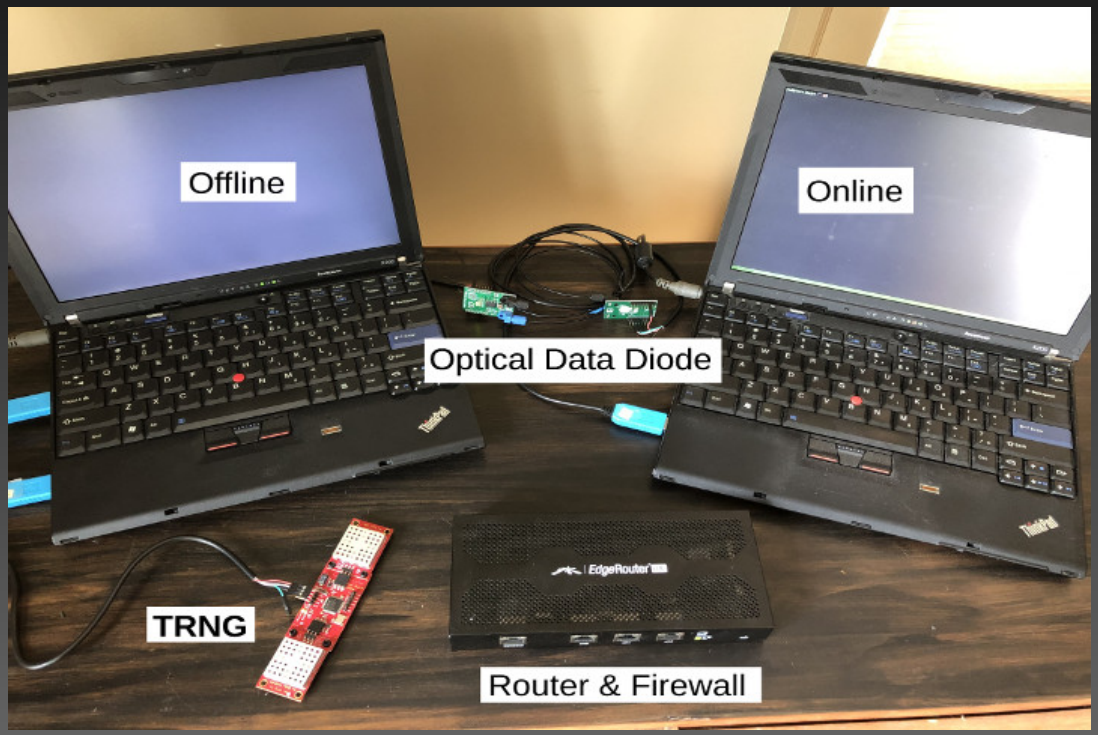
- Mircea Popescu

JWRD Computing

- On a mission to assist clients in realizing personal sovereignty through strengthening digital security.
- We provide a comprehensive solution to exclude many unnecessary risks and mitigate the necessary ones.
  - A tailored computing environment customized for the client’s needs
  - Full support including in-depth, one-on-one training in effective use of the tools
- Working since 2016 to develop, apply and refine our offerings.

Practical solutions at every layer

- Hardware
  - **Coreboot Thinkpads** with fully open-source firmware and OS
  - 3-port gigabit firewall **router** with custom OpenBSD install
  - Verifiable **random number generator**
  - Fiber-optic **data diode** for airgapping



Practical solutions at every layer

- 100% open-source software
  - Operating system
    - Original **Gales Linux** distribution, built fully from source code, tailored to the hardware and use case
  - Software development
    - **V** cryptographic version control system
    - **Gales Scheme** interpreter
  - Applications
    - **GPG** end-to-end communication security
    - Fully verifying **Bitcoin node**
    - Airgap-friendly **Gales Bitcoin Wallet** offering full control over transaction construction and signing
    - And much more... http://fixpoint.welshcomputing.com/category/software/

Recap

- When processing sensitive information, you implicitly trust a huge collection of hardware and software (and the small armies of coders churning it out).
- The industry is unaccountable, aligned with the socialist fiat system, and has continually proven untrustworthy.
- Most “security” products on the market are faking it to varying degrees.
- Solutions exist once you know where to look.

Overview

- Context
  - How to get rich with Bitcoin
    - Buy; don’t lose; develop trade; hold on for the ride
  - Monsters under the bed
    - Don’t be the turkey!
  - How JWRD can help
- Demonstration of cryptographic concepts
  - Entropy
  - Asymmetric keys
- Demonstration of tools
  - TRNG
  - gbw-signer
  - Data diode
- (Time permitting) Hashes and mining

Cryptographic entropy

- Numbers that can’t be predicted with any better odds than random guessing
- Required for cryptographic keys and strong passwords
- Cannot be obtained by algorithmic means; must come from **nature**
- **Statistical** randomness is implied but it alone is not sufficient
  - I.e., not enough to **look** random
  - Folly of RNG “whitening”
  - Rolling dice is likely better than whatever you’re doing now

Dice password generation

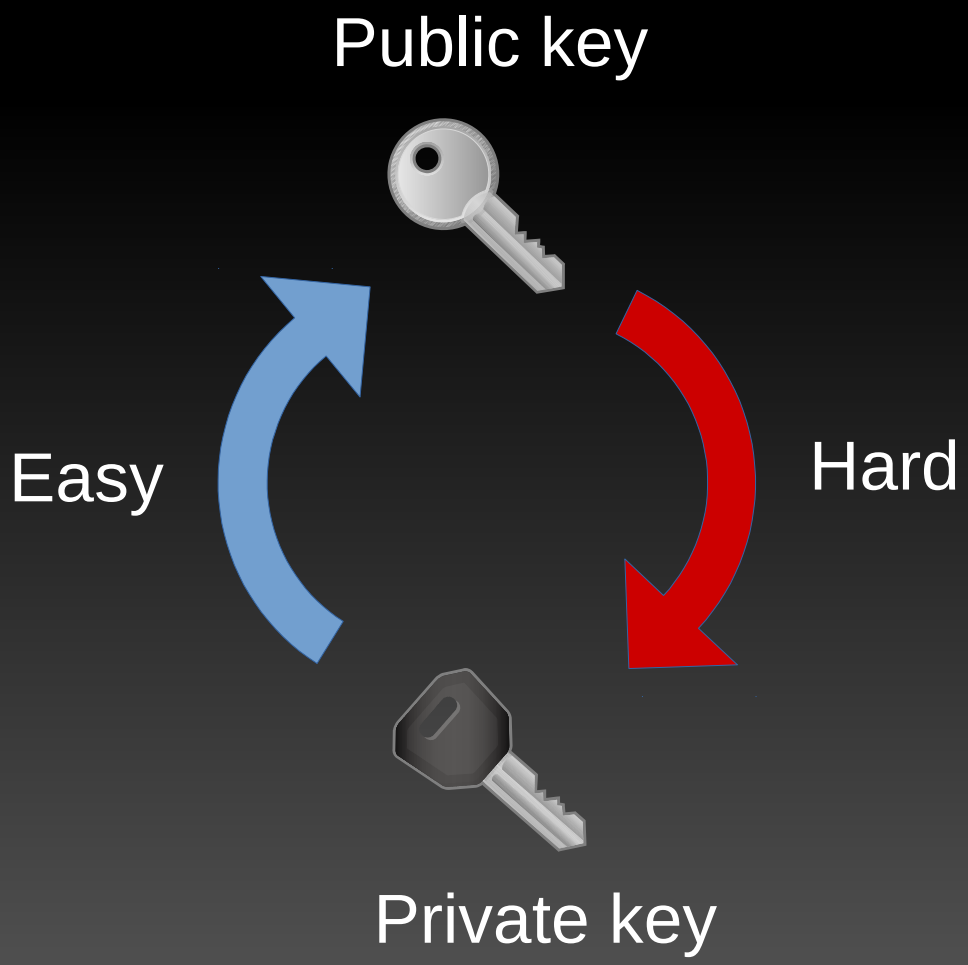
- 36 symbol alphabet ~ 5 bits per character (2^5 = 32)
- 25 characters > 128 bits

	1	2	3	4	5	6
1	a	b	c	d	e	f
2	g	h	i	j	k	l
3	m	n	o	p	q	r
4	s	t	u	v	w	x
5	y	z	0	1	2	3
6	4	5	6	7	8	9

The trouble with shared secrets...

- Passwords, credit card numbers, Social Security Numbers, birthdays, “security questions”, fingerprints and all other biometrics are examples of *shared secrets*
  - They can identify one party to another, but only as long as both keep the secret.
- “The best way for three people to keep a secret is...”
- They prove nothing to third parties who lack the secret; thus systems built on them inevitably demand ultimate trust be placed in a central authority.

Asymmetric key cryptography



Asymmetric key cryptography

- What are the prime factors of 13`843`867 ?

Asymmetric key cryptography

- What are the prime factors of 13`843`867 ?
  - hard...
- What is the product of 2`029 and 6`823 ?
  - even your phone can do it !!

Asymmetric key cryptography

- What are the prime factors of 13`843`867 ?
  - You could do a brute-force search (guess & check) with a computer
  - How does the work (expected guesses) scale with more digits ?