Ultraparanoid Computing for the Consumer

David Pruett

June 27, 2018

Abstract

Fear sucks the joy out of life, hence joy requires security. A review of famous security failures distills into the **ultraparanoid assumptions**. There are security principles that have worked since before computers existed, that are in no danger of being suddenly *cracked*. A life without fear can only be constructed using the latter to address the former. Handling even the ultraparanoid fears permits joy to exist.

A practical step recommended by every security talk includes using a password system. Most are 4 part systems, with all mechanics hidden from the user, requiring no more than selecting a password. The similarities unravel when the ultraparanoind assumptions are put to the test. Reconstruction after a loss or disaster is usually sufficient to highlight the differences. The key to success involves separated parts, safe media, and safe places.

Ultra Paranoid Assumptions

A1. Your foes are better at math.
A2. Every Black Box and Network is corrupt.
A3. Anything stored on any physical medium will be lost or destroyed.
A4. Every person or corporation you trust will betray you.
A5. There will be leaks.
A6. You will lose your keys.

Bibliography

- TEDx Midwest Talk by Pablo Holman
- Information Theory - Shannon
- Applied Cryptography - Schneiderman
- The Code Book – Singh
- Code Breakers: Bletchley Park’s Lost Hero’s - BBC 2011
- Alan Turing: The Enigma - Hodges
- Disappearing Cryptography - Wayner
- How to Disappear - Ahearn and Horon
- The Constitution, that delicate balance - Friendly and Elliot
- IEEE Austin CTCN Talk by Larry Moore (July 26, 2017)

Standard Conclusions from almost All Security Talks

- Use a password system - and not your browswer
    - Do not share passwords with anyone (A4)
    - Do not re-use passwords (A5)
    - Use longer passwords (A1)
- Use backups (preferably offsite) (A3)
- Do not respond to *anything* unsolicited
- Do not use your (real) email as an ID
- Do not use Facebook, Alexa, Hey Google, ... (A4)

Rules from the Big Dogs (Security, Military, IT, Accounting)

- If you don’t have physical security, you don’t have security. (A1)
- Success is knowing you have been compromised (A1)
- Reduce the attack surfaces (no GUI) (A1)
- Do not use your intuition (A1)
- Restrictions on passwords weaken them (A1)
- Use Separation (“Air Gaps”) (A1,A2)
- Cut the wires (especially the wireless ones) (A2)
- Destroy the machine (A2)
- Any system can be defeated with enough conspirators (A4)
- Need to Know Basis (Compartmentalize Knowledge) (A5)
- Don’t leave a key under the doormat (A6)

Refined or Dissenting Opinions

- Use separated parts stored on safe media and in safe places (A1)
- Do not use black boxes (A2)
- Never update the password system (A3)
- Strongly avoid the man in the middle (clouds) (A2,A4)
- Address the compartmentalization problem (A5)
- Special characters do not help
- Changing passwords arbitrarily does not help, but …
- Do not *ever* use passwords you can not change (A5)
    - Social Security Number
    - Body parts
    - “Something you *are*”
- Reduce the attack window (turn it off, remove it, download and delete it)

Guess Rate x Guess Time

Rate in guesses/sec, Time in seconds	$Q = 2^{bits}$	chr6(pw)
All The Computers in the Universe	2^{60}	10
GPU (4 TeraFlops)	2^{42}	7
Laptop (4 Core, 8 Gigaf bps)	2^{33}	5.5
Throttled (3 Wrong Guesses/Day)	2^{-15}	-2.5
The Age of the Universe	2^{60}	10
Human Lifetime	2^{32}	5.5
1 Year	2^{25}	4
1 Week	2^{19}	3
1 Day	$2^{16.4}$	2.75
1 Hour	2^{12}	2
Dictionary Word (Q = 4-100K words)	$2^{12\text{-}17}$	2-2.75

Code	Length 2^x	Rate 2^x/sec	Time 2^x sec	Time in English
Enigma (1940)	14	1	13	2 Hours
DES (1998)	56	39	17	2 Days

Brief History of Failed Crypography/Security (A1)

- 1586 Mary Queen of Scotts, Babington Plot. Phelippes
- 1854 Vigenere Cipher cracked. Babbage
- 1917 Zimmerman Telegram causes US entry into WWI. Montgomery, de Grey
- 1918 German ADFGVX cipher. Painvin
- 1940 Enigma Machine (3 wheeled). Schmidt,Rejewski,Turing/Bombe
- 1944 Lorenz SZ40/42 Cipher (12 wheel). Tutte,Flowers/Colossus
- 1998 DES cracked. EFF/Deep Crack
- 2001 WEP (Wireless Security) cracked.
- 2008 Transport Layer Security (MD5) cracked
- 2011 Apple code signing cracked
- 2011 SSL cracked (BEAST)
- 2013 SSL cracked (BREACH)
- 2013 Silk Road (Dark Web using Bit Coin) cracked, operation Onymous
- 2014 Jennifer Lawrence, Kate Upton, etc. pictures stolen
- 2015 Diffe Helman cracked (LOGJAM)
- 2015 RSA, Certificates cracked. Shamir declares cryptography “over within 3 years.”
- 2016 US Elections hacked
- 2017 Speculative Branching attacks (SPECTRE and MELTDOWN)
- 2018 Golden State Killer found through family DNA using geneology web site.

Pristine Machines and Networks (A2)

- 2015 Superfish (Lenovo, Dell, Toshiba)
- Stuxnet
- SSL Cracks (2011+)
- Signing Cracks (2011+)
- Certificate Cracks (2015)
- Cell Tower Spoofing
- Autojoin networks by name (ATT)

Physical Media Failures (A3)

Brief History of Famous Trust Failures (A4)

- Byzantine Kings
- Hans-Thilo Schmidt. Sold Enigma plans to French → Polish → British
- John Cairncross. Blechley park. Russian Battle of Kursk (1943) changed WWII
- Klaus Fuchs. One of the top 4 scientists at Los Alamos
- Julius and Ethel Rosenberg, proximity fuse that shot down Gary Powers
- David Greenglass (Courier related to Rosenberg and Fuchs)
- John Anthony Walker. 1968 Pueblo capture to modern Soviet Subs
- Edward Snowden
- Spear Fishing / Whaling (Friend/Foe Mistake)
- Facebook, Google, Divorce, etc.

Major Database Breaches (A5. Tom's Guide, Huffington Post)

* 2016 FBI (Kene Gamble) 20000 Employees
* 2014 Sony 6800 Employees

* 2013 Yahoo 3000M
* 2016 Friend Finder 412M (SHA-1)
* 2016 MySpace 360M
* 2011 Epsilon 250M
* 2012 Linked In 165M
* 2017 Equifax 145M
* 2014 eBay 145M
* 2009 Heartland Payment 130M
* 2013 Target 110M
* 2011 Sony Play Station 102M
* 2014 Rambler 98M
* 2003 TJMax 94M
* 2006 TJMax 46M
* 2015 Anthem Health 80M
* 2014 JP Morgan Chase 76M
* 2008 Natl Archives 76M Veterans
* 2012 Drop Box 68M
* 2013 Tumblr Blogging 64M
* 2014 Home Depot 56M
* 2013 Evernote 50M
* 2013 Living Social 50M
* 2015 Ashley Madison 40M
* 2008 GE Money (7-11, JCPenney, NASDAQ)

Major Ransomware Attacks (A5)

* 2015 Cryptolocker 500K Machines
* 2014-6 Teslacrypt
* 2015-6 SimpleLocker Android (150K Machines)
* 2017 WannaCry SMB Hole from Eternal Blue NSA Kit.
* 2016-7 NotPetya Russian Attack on Ukraine?
* 2018 City of Atlanta

Things that were NOT cracked (maybe sort of)

- 1800BC Linear A and several lost languages
- 1586 Vigenere Cipher (cracked in 1854 by Charles Babbage)
- 1820 Beale pamphlet (probably fake. A Vigenere Cipher)
- 1918 One Time Pad. Uncrackable. Still used for Washington-Moscow. Mauborgne
- 1918 Chaocipher (method not keys, violating Kerckhoffs rule from 1883)
- 1935 United States Bullion Depository (Fort Knox)
- 1942 Naval Version of Enigma (Off and On. June 1941 – June 1942)
- 1942 Siemens T43 Encryption Machine
- 1942 Navaho Wind Talkers
- 1966 -74 Zodiac letters, and Zodiac Killer
- 1978 Unabomber (Turned in by family after over 15 years)
- 1984 Quantum Key Distribution (BB84 Bennet, Brassard)
- 1987 Feynman Challenge Ciphers
- 1990 Kryptos Sculpture Ciphers (3rd challenge). Scheit, Sanborn
- 2001 Osama Bin Laden (escaped for nearly 10 years)
- –---- Banking, Military, Block and other Chains
- —-- See Elonka's List of Famous Unsolved Codes and Ciphers

Safe Media for Separated Key Parts

```
  * Public    immune to:  disaster, loss,  theft,          capacity limit,
  * Mental    immune to:  disaster, loss,  theft, spying,
.
  * Paper     immune to:                           spying, capacity limit,
  * CD-Rom    immune to:                           spying, capacity limit,
```

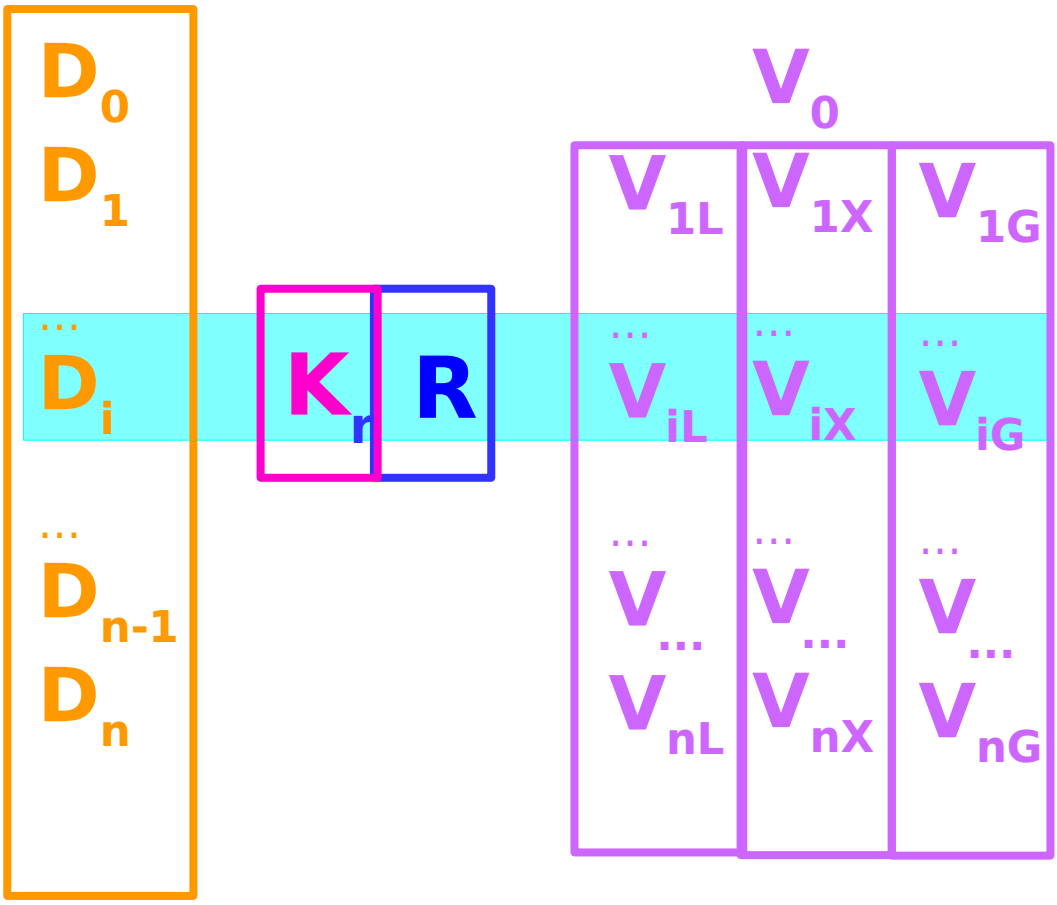
- Immune to modification and remote attack (no wires).
- Primary parts immune to disaster.
- Secondary parts re-creatable from the Primary parts.

Safe Places for Separated Vault Parts

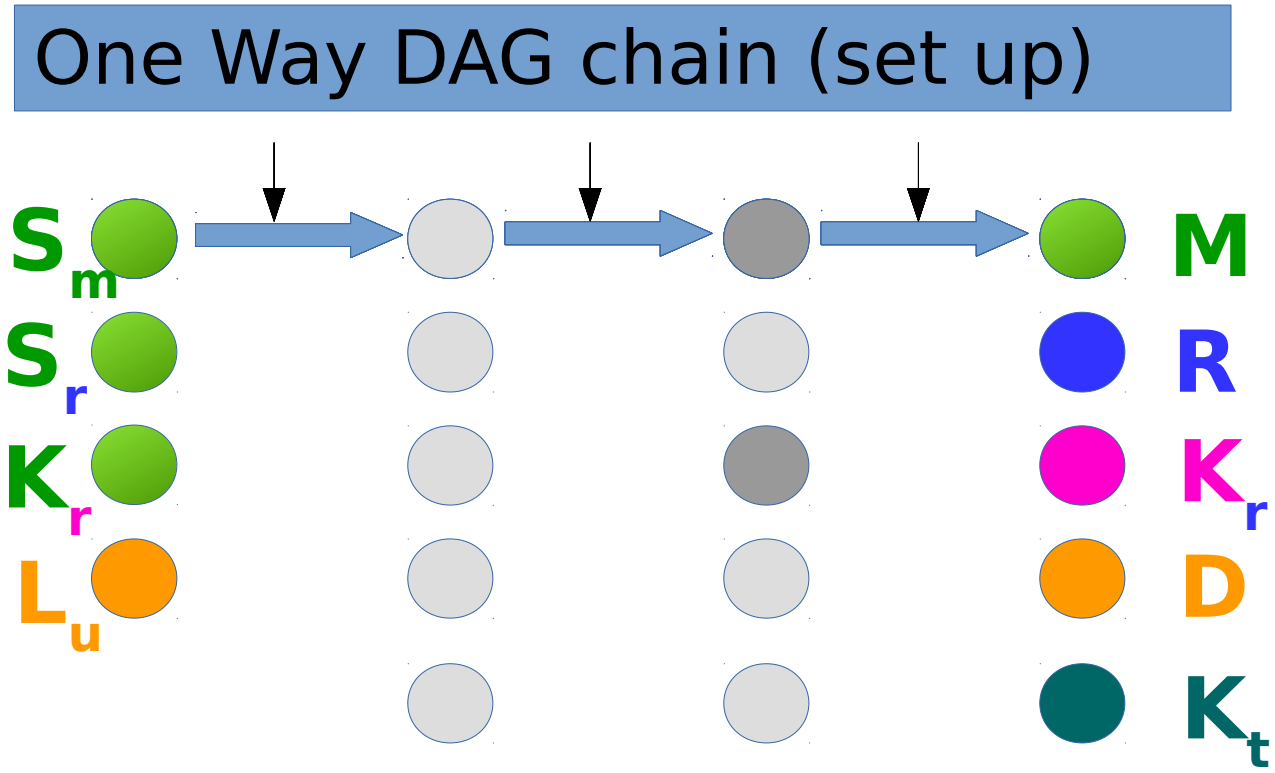
```
  * Local     (susceptible to: local attack,
  * Remote    (susceptible to:               remote attack,
  * Guarded   (susceptible to:                                disaster
```

- Using a 2 out of 3 system removes any single catastrophe susceptibility.
- Single duplication by type gives an 80% chance of recovery even if 4 out of 6 are destroyed.

4 Part System (Subst-Head)



$K_i = d(R, K_r, D_i)$ *Perfect Sharing revisited*



The Ultra Paranoid Assumptions Revisited

A1. Your foes are better at math.
See "Perfect Secret Sharing" in Disappearing Cryptography.

A2. Every Black Box and Network is corrupt.
All mental path keys can be created entirely without black boxes.

A3. Anything stored on any physical medium will be lost or destroyed.
The system is disaster immune.

A4. Every person or corporation you trust will betray you.
There are no entities in posession of the required mental keys.

A5. There will be leaks.
All keys are reviseable to handle leaks - no body parts are used.

A6. You will lose your keys.
System reconstruction is disaster immune.

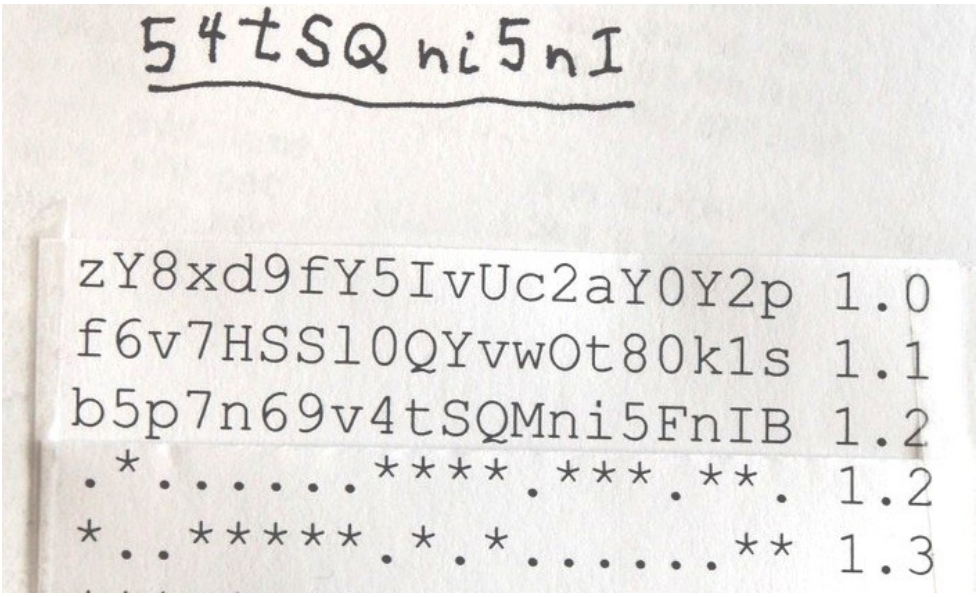
Wallet Cards

Password cards contain a list of passwords (K_i), each encoded using its corresponding mask card key (K_{ti}).

$W_i = e_t(K_i, K_{ti})$ *machine (or hand written)*

$K_i = e_t^{-1}(W_i, K_{ti})$ *mental + paper*

The transpositions are very easy to perform. Familiar passwords jump out at you even without a mask card (K_{ti}).



Extensions to Atoms

- Compartmentalize assets as well as data.
- Design of physical access is a directed cyclic graph problem.
- All resource locations must be reachable from any potential disaster (lost key) condition.
- Entry points into the cyclic graph must be reachable by you, but not by foes.
- Critical resource locations must not be reachable by custodian keys (i.e., the neighbors)

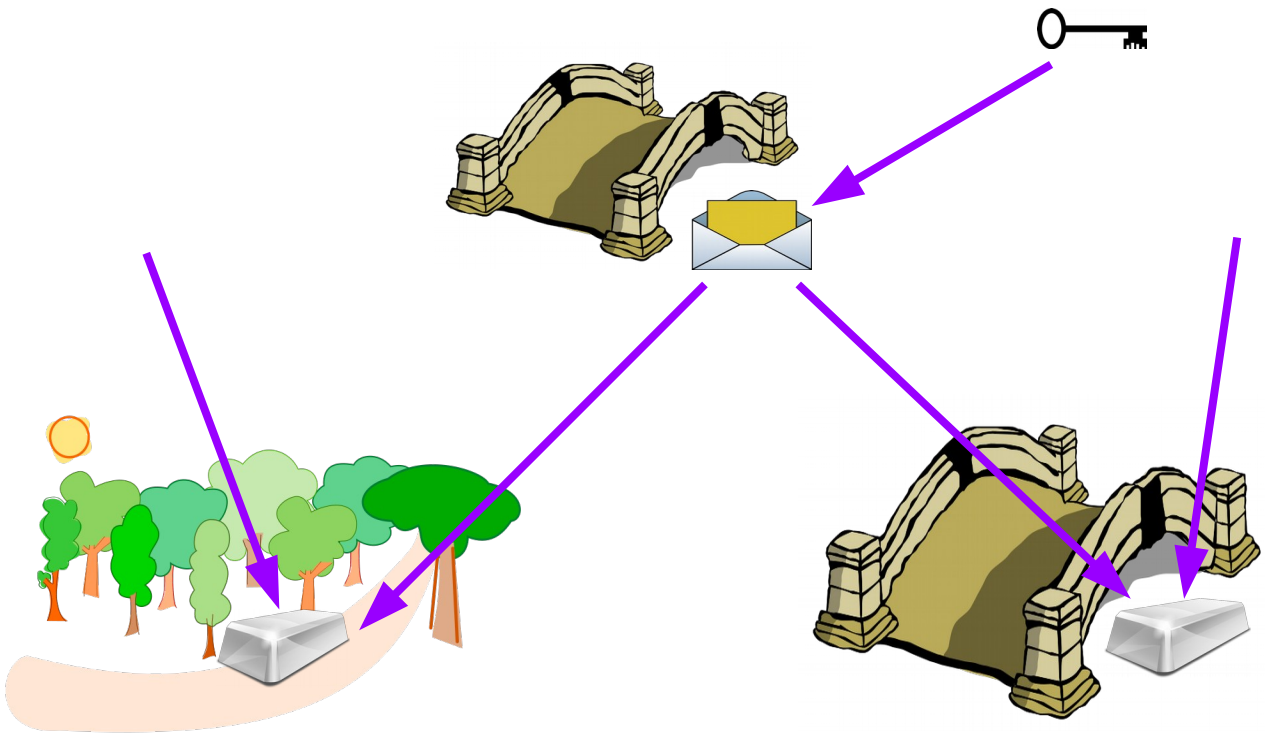
Extensions to Banking

- Do not bank online
- Use **only** bank property
- Use gift cards, not bank cards for online purchases
- Do not fail over checking to life savings or credit
- Compartmentalize banks in an Acyclic Graph
- freeze your credit scores

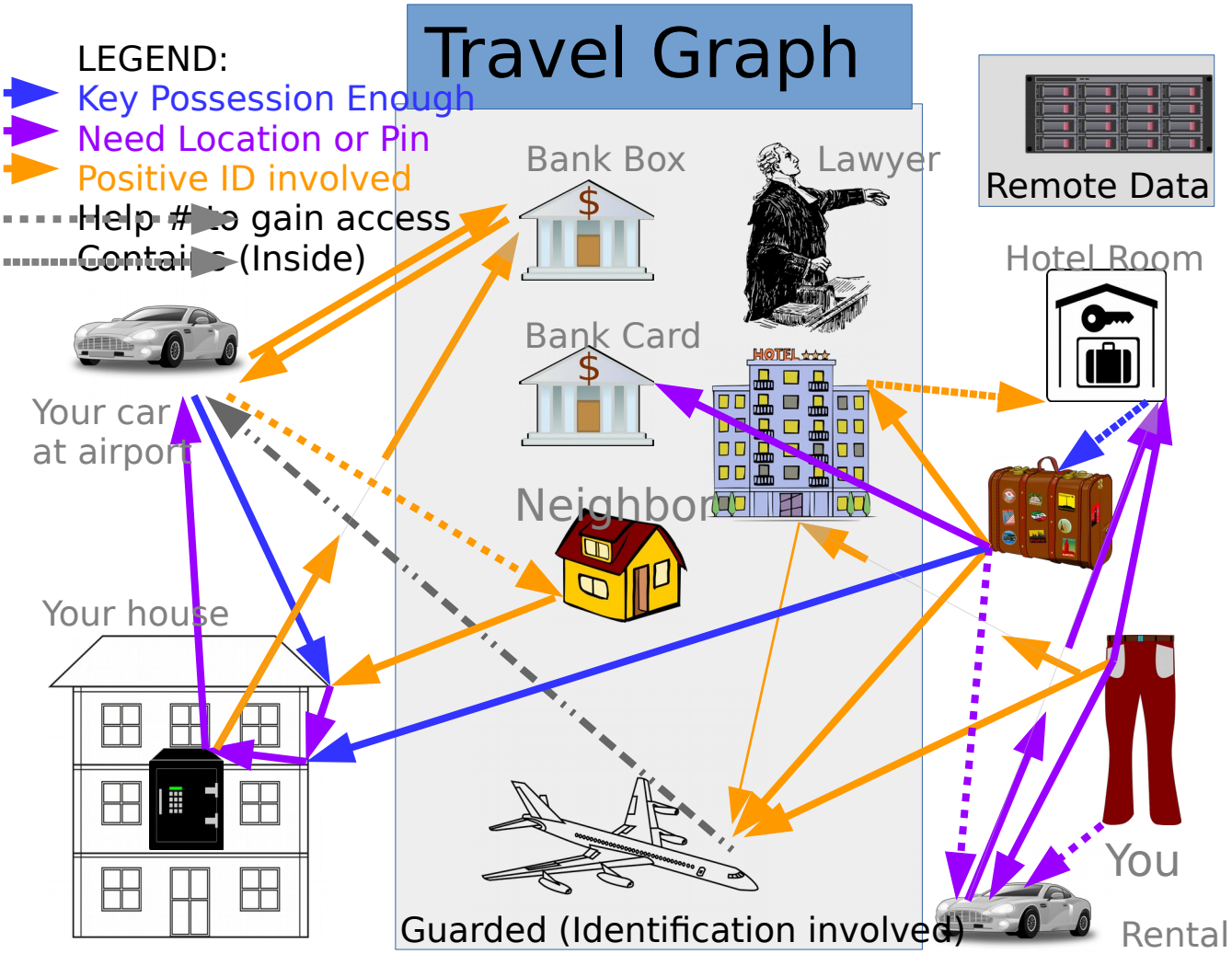
Extensions to Travel

- The Separated Safe Places concept applies to critical resources: Money, Medicine, ID.
- Which places are safe is not an absolute: Hotel rooms, cars, luggage, etc.
- On person separation using fake wallets and interior pockets (pick pocket situations).
- A passport and drivers licence are the only two separable ID’s that can get you on an airplane.
- Card and Folder passports are the only separable ID’s that will get you back in the country.
- Separable copy or photo of main passport page will get you a new one at US consulate.

Graph of Alan Turing's “Atoms”



Two buried silver bars, hidden encrypted instructions



Graph Failure Analysis

Examine effect of each node being destroyed
Examine “Brick through Window” on unguarded nodes
(If you don't have physical security, you don't have ...)
Excessive fan-out from any node is generally bad
Single entry nodes are lost if source node destroyed

→ becomes → upon guard failure at source end
→ becomes → if “secret” owner present (by coercion)
Blue paths are a failure mode (simple key possession)

Extensions to Safety: Partial List of US Serial Killers

year	day	dead/inj	Killer	Description
1966,	Jul 14	8/0	Richard Speck	Chicago Nurses
1966,	Aug 01	16/31	Charles Whitman	UT Tower, Houston McCoy
1966,	-1974	9/2	- Zodiac Killer	Never caught
1974,	Dec 30	3/11	Antony Barbaro	Olean High, Earl Metcalf
1976,	-1977	6/7	David Berkowitz	Son of Sam
1976,	-1986	12/45	Joseph DeAngelo	Golden State Killer
1978,	-1995	3/23	Ted Kacynski	Unabomber
1994,	Jun	3/?	Roger Fain	Darlene Anderson
1995,	Apr 19	168/680	McVeigh & Nichols	Murrah Bldg (OKC Bombing)
1996,	Jul 27	1/111	Eric Rudolf	Atlanta, (+3 other bomgings)
1999,	Apr 20	13/21	Harris & Klebold	Columbine High School
2001,	Sep 11	3000/?	Osama Bin Ladin	Twin Towers
2012,	Jul 12	12/70	James Holmes	Aurora, Colorado Movie Theater
2012,	Dec 14	27/0	Adam Lanza	Sandy Hook Elementary
2013,	Apr 13	3/264	Tsarnaev brothers	Boston Marathon
2016,	Jun 12	49/58	Omar Mateen	Pulse Night Club
2017,	Oct 01	58/851	Stephen Paddock	Las Vegas
2017,	Nov 05	26/20	Devin Kelley	Sutherland Springs Babtist
2018,	Feb 14	17/17	Nikolas Cruz	Parkland (Stoneman Douglas High)
2018,	Mar	2/5	Mark Conditt	Austin Bomber
2018,	May 18	10/13	Dimit. Pagourtais	Santa Fe High School

- See **How to Disappear** for guidelines on dating and other applicable social situations.
- Always make sure someone knows where you are.
- If necessary, write a note and put it in your desk, rip it up when you get back.
- An available turniquette kit greatly increases chances of surviving a shooting.