Privacy Security and Functionality

Privacy

- Privacy is the ability for someone to seclude themselves, information about themselves, and to express information selectively

- (That means you don’t want people looking in your window, you don’t want random people knowing your social insurance number, and you don’t want random criminals to see you posting vacation pictures so they know when to rob your house).

Security

- You want your services (website, billing etc.) to be resistant to attacks
- People shouldn’t be able to steal your money
- Third parties shouldn’t get your personal data through hacking

Observation 1

- Generally users want security and privacy (or at least, control over those things)

Observation 2

- Users will try and make secure choices if they can understand those options

Observation 3

- Users usually do not know enough to make secure choices

KIM ZETTER SECURITY 07.27.12 6:00 AM

KIDS CAN OPEN GUN SAFES WITH STRAWS AND PAPER CLIPS, RESEARCHERS SAY

LAS VEGAS — Is a plastic drinking straw from McDonald's the only thing keeping a thief — or worse, a child — from accessing the loaded weapon in your closet safe?

That's apparently the case with one model of personal safes that a team of researchers will be cracking at DefCon on Friday.

But the researchers found similar problems with several brands of personal safes that are marketed for securing guns and other valuables. Toby Bluzmanis, Marc Weber Tobias, and Matt Fiddler demonstrated in videos that they were able to swiftly open seven models of safes, using household items like paper clips, a wire hanger and a drinking straw. In one case, they opened a safe simply by lightly bouncing it on a floor once.

It's estimated that about a fifth of all households own a handgun, according to a study by the American Journal of Preventive Medicine. About 500 teens and children are killed accidentally each year with guns, some of them by handguns stored in their homes.

Unsafe Gun Safes Can Be Opened By A Three-Year Old

Marc Weber Tobias Contributor ⓘ
I am an investigative attorney and physical security specialist.

Americans love their guns, and every day someone in the U.S. is either shopping for or buying a gun safe. Small gun safes have become popular as an alternative security system for protecting both weapons and valuables, even though Federal law requires some sort of lock to be provided with every gun sale.

The author and his team used a variety of simple implements to open these safes, including paperclips, strips of thin brass, drinking straws and wires. All of these safes shown can be easily and quickly opened.

You should know how unsafe these gun safes are. Both small and large gun safes are sold at all major sporting goods stores and on-line retailers, including Walmart, Cabelas (37 stores), Scheels (24 stores), and Dicks Sporting Goods (450 stores). These safes typically cost $75-$200 depending upon manufacturer, retail outlet, container size and alleged "sophistication and method of locking." There are three leading brands that are sold by these retail outlets: Stack-on, GunVault, and Bulldog.

Continuation of Previous Slide

- https://www.youtube.com/watch?v=erGOJxQIf5c

- Even in physical security you need to be able to trust that products you buy won't be laughably bad

- As it turns out, without government oversight and regulation selling garbage is a great way to make money and leave consumers with no recourse

Human Interpretation vs Technical Correctness

- At the core of most of UX is the difference between *Technical Correctness* and how people understand things

- Ultimately it's up to you as a user of tech to try and develop an understanding of the technical correctness, and it's up to designers to help educate you.

- Realistically though, most users will never understand what the tech does or why

Recommendation Algorithms

- Amazon has something like 600 million unique products for sale in the US (and close to 3 billion globally, though probably there is overlap there)
- Netflix has about 6600 combined TV + Movies in the US (Canada has roughly half of that)
- Spotify has ~ 30 million songs in its catalog

- Same basic problem with Internet search (finding something the user will click on)

Recommendation Concepts

- (The details of how to build this is more big data + machine learning, which for now is largely grad school)

- Cluster users based on past activity
- Base recommendations on past activity (single user or cluster)
- Build models of topics (categories) users are interested in
- Model similarity of products to each other

Online Dating

- As discussed previously, online dating started out really simplistic. Basically a screen name and a forum
- It evolved into pictures, profiles a searches based on various criteria
- Then it started to include basically glorified psychological profiles on people with literally hundreds of questions, and tried to use Science™ to match people

Table 1. Types of U.S. Online Dating Sites and Their Distinctive Features

Row	Type of site	Distinctive feature	Example sites
	Site types within the purview of the present article		
1	General self-selection sites	Users browse profiles of a wide range of partners	Match, PlentyOfFish, OkCupid
2	Niche self-selection sites	Users browse profiles of partners from a specific population	JDate, Gay, SugarDaddie
3	Family/friend participation sites	Users' family/friends can use the site to play matchmaker for them	Kizmeet, HeartBroker
4	Video-dating sites	Users interact with partners via webcam	SpeedDate, Video dating, WooMe
5	Virtual dating sites	Users create an avatar and go on virtual dates in an online setting	OmniDate, Weopia, VirtualDateSpace
6	Matching sites using self-reports	Sites use algorithms to create matches based on users' self-report data	eHarmony, Chemistry, PerfectMatch
7	Matching sites not using self-report	Sites use algorithms to create matches based on non-self-report data	GenePartner, ScientificMatch, FindYourFaceMate
8	Smartphone apps	GPS-enabled apps inform users of partners in the vicinity	Zoosk, Badoo, Grindr
	Site types beyond the scope of the present article		
9	General personal advertisement sites	Users can advertise for diverse goods and services, including partners	Craigslist, most newspaper sites
10	Sex or hookup sites	Users meet partners for casual sexual encounters	OnlineBootyCall, AdultFriendFinder, GetItOn
11	Infidelity sites	Users or partners (or both) pursue extrarelationship affairs	AshleyMadison, IllicitEncounters, WaitingRoom
12	Sites for arranging group dates	Users propose get-togethers with a group of strangers	Ignighter, Meetcha, GrubWithUs
13	Social networking sites	Users can meet friends of friends	Facebook, MySpace, Friendster
14	Massively multiplayer online games	Users can meet partners using avatars in a complex online environment	SecondLife, TheSims, WorldOfWarcraft

Note: The content in this table is illustrative, not comprehensive. The distinctive feature of a particular type of site does not imply that it is the sole purpose or method the site uses; many sites have multiple features or use multiple methods to help users access potential partners. In addition, due to the rapid pace of technological and entrepreneurial innovation, the methods that people use to meet potential romantic partners online are constantly changing. This table represents a snapshot from 2011. GPS = global positioning system.

From 2012

Getty Images/iStockphoto

The man never thought he'd be blackmailed just a couple of weeks after signing up to the site

RACHEL HOSIE
@rachel_hosie
Monday 16 January 2017 13:25

Back in August 2015, the 'dating' site Ashley Madison was hacked, exposing married cheaters the world over.

We found out 86 per cent of the site's users were men, São Paulo had the most registered users of any city and it's mainly used by rich, powerful men.

But what became of the marriages of the guilty parties, whose secret infidelity was suddenly not-so-secret at all?

One man who was exposed in the hacking has now spoken out about what happened to him in an article for the LA Times.

- Ashley Madison is/was(?) a dating site for married people to cheat on their spouses

- They got hacked

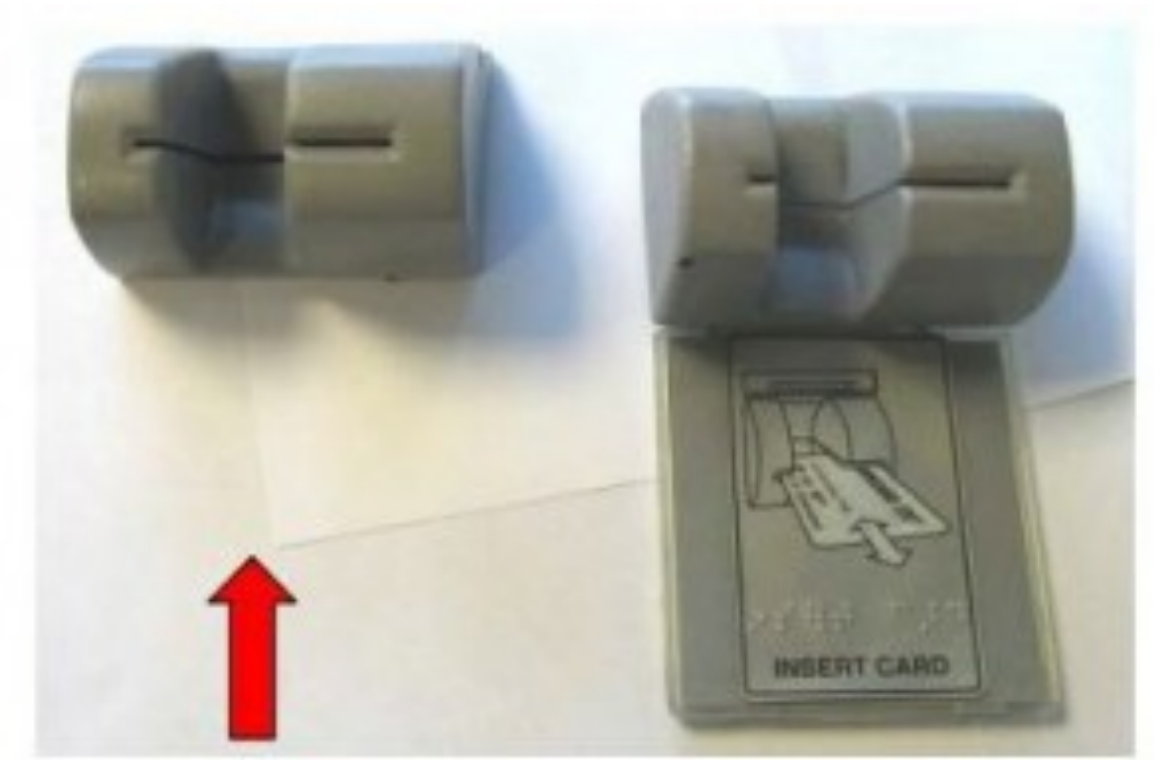
Facebook said to test new dating feature in Colombia with safeguards to prevent stalking

- Facebook announced that it is testing its new dating feature in Colombia.
- The dating feature will focus on details and creating meaningful connections and relationships.
- The dating feature has incorporated a few features to prohibit stalking and steer clear of quick hookups.

- That is as of sept 20 2018

- (N.B. Facebook employees tested the feature before that got some confused press, they did so on a sort of internal fake facebook with fake profiles.)

Card Skimmers

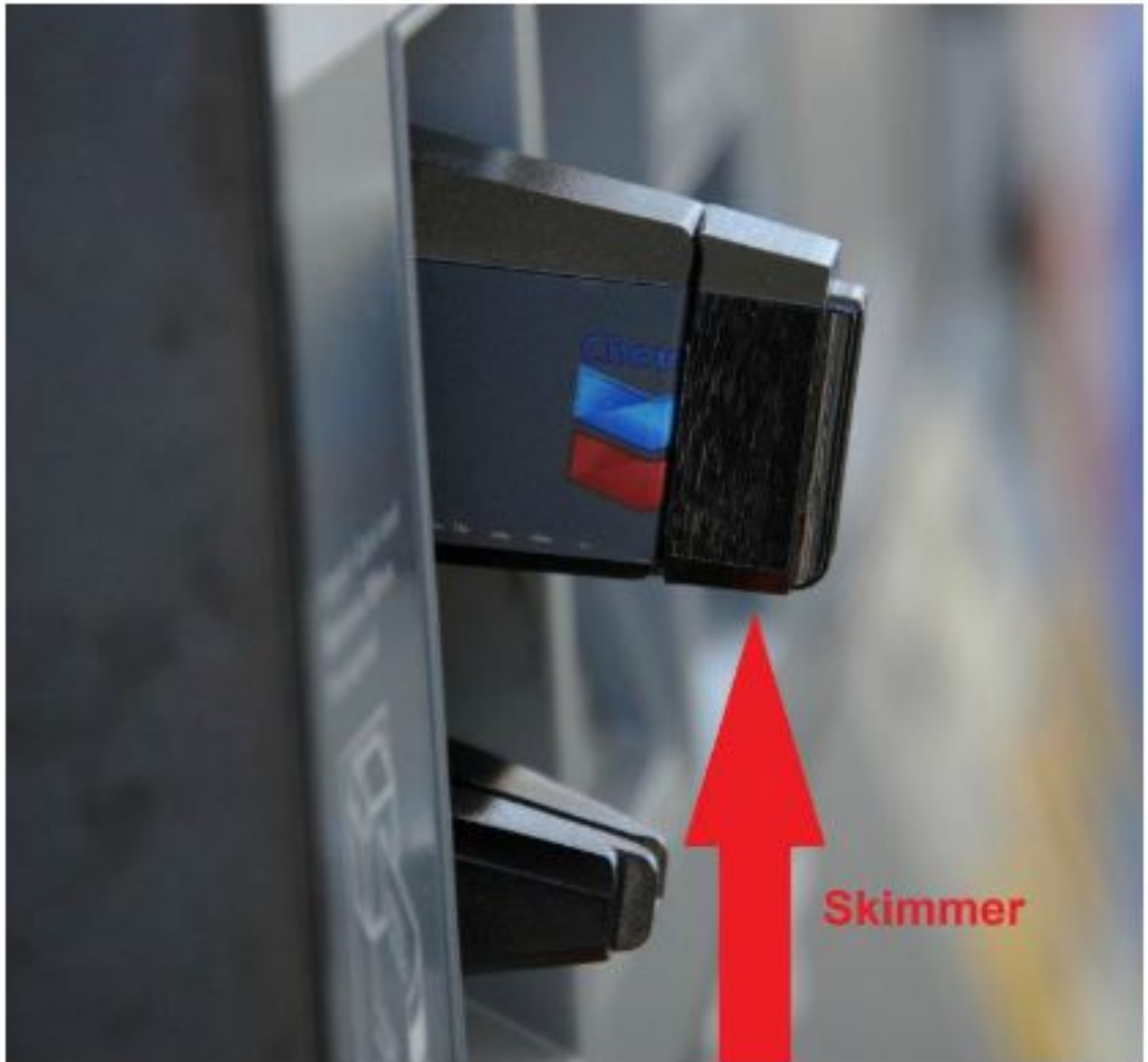


The real card reader slot.

The capture device


AIB

- Tape as a “security” measure


Skimmer

Design Challenges

- The more diverse the machines the harder it is to build skimmers for each type but the harder it is to know which ones are legitimate
- Tiny Cameras make keypads vulnerable
- In theory tap can be more secure (but then boosted signals)

Common Consumer Advice

1. Look for signs of a skimmer.
2. Pull on the card reader.
3. Use a smartphone app to scan for skimmers with Bluetooth radios.
4. Use an EMV (Chip) card.
5. Use cash.

- To quote the paper I am citing (see comments): “While seemingly helpful on their surface, many of these tips offer little in terms of specific steps. Beyond common sense, Tips 1 and 2 suggest that users know how payment devices should look and feel.”
- N.B. This is of course advice for the US. Chip cards are more common in Europe and Canada (though insecure in other ways)

Passwords

1. Maintain an 8-character minimum length requirement (and longer is not necessarily better).
2. Eliminate character-composition requirements.
3. Eliminate mandatory periodic password resets for user accounts.
4. Ban common passwords, to keep the most vulnerable passwords out of your system.
5. Educate your users not to re-use their password for non-work-related purposes.

~~6. Enforce registration for multi-factor authentication.~~

~~7. Enable risk based multi-factor authentication challenges~~

- Source: R.Hicock (former student of Sri's from UWO) Microsoft identity protection team. Crossed out stuff aren't actual passwords

Anti Pattern 1: Requiring long passwords

- (Rhetorical) How many services still mandate those sorts of rules?

- Long passwords, mathematically, are stronger… in practice, users use repeating or easy to remember passwords. It’s also a nightmare for typo’s and entry using non keyboard devices

Anti-Pattern #2: Requiring the use of multiple character sets

- Common advice:
- Passwords need characters from all three of the following categories:
  - Uppercase characters
  - Lowercase characters
  - Non-alphanumeric characters

- Reality: People use similar patterns for this, and Cyber criminals build their dictionary attacks around this (Most people use similar patterns (i.e. capital letter in the first position, a symbol in the last, and a number in the last 2)

Anti-Pattern #3: Password expiry for users

- Password expiration policies do more harm than good, because these policies drive users to very predictable passwords composed of sequential words and numbers which are closely related to each other

- That is, the next password can be predicted based on the previous password. Password change offers no containment benefits cyber criminals almost always use credentials as soon as they compromise them.

Successful: Banning common passwords

- 123456
- 123456789
- qwerty
- 12345678
- 111111
- 1234567890
- 1234567
- password
- 123123
- 987654321
- qwertyuiop
- mynoob
- 123321
- 666666
- 18atcskd2w
- 7777777
- 1q2w3e4r
- 654321
- 555555
- 3rjs1la7qe

Successful: Banning common passwords

- The list is MUCH longer than that (that’s just the top 20) and you can ban stuff that meets common bad password patterns

- You can also ban all known passwords

Password Reuse

- Sri has 124 passwords in his password manager (and probably has more passwords than that)
- It’s not possible to remember all of those
- There’s also the practical problem of what happens if you forget the password to your password manager or die, and someone else needs to access it (e.g. only one party in a married couple manages all the bills… and then dies, or someone manages their parents stuff)

Two Factor Authentication

- By now you should all know what two-factor authentication is even if you don’t have much that uses it

- It’s where you for example, have a random number device/app or get a text message in addition to using a password

WoW versus a Bank

- Your world of Warcraft account, if you have an authenticator is significantly more secure than your bank account
- Blizzard has support costs associated with fixing it
- Banks have insurance
- There are legal mandates banks have to follow… and usually they do a terrible job of it.

WoW authenticator

- Synchronized clocks with a pre-determined Random number generation
- If the authenticator system fails everything Protected by it goes to hell fast
- If WoW security fails it costs Blizzard money
- Keyloggers can compromise the system, but Users need to have gotten a keylogger somehow

RSA token

- RSA took a 10 million dollar payout from the NSA to deliberately weaken their Random number generator in their tokens
- (technically it was to use the NIST standard RNG that the NSA was on a standards committee for, and deliberately weakened).

Got here fall 2019

- https://arstechnica.com/tech-policy/2019/09/facebook-confirms-its-standards-dont-apply-to-politicians/

- News for 2020

- Aren’t politicians the people we should be fact checking the most?


I ♥ VMware
GoPro
ecobee
D. tech
INFORMATION SYSTEMS
COMPUTING SYSTEMS
ENGINEERING

Resilient Procedures

- A big issue in the news lately has been the idea of ‘government back doors’ in messaging systems
- The idea being that governments should be able to spy on and wiretap communications… notably to catch spies
- The problem is that a backdoor for good guys, is backdoor for bad ones too

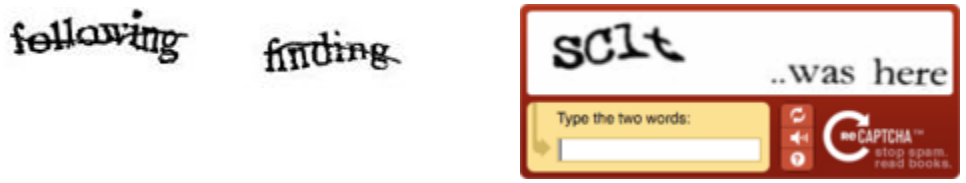
Identifying Bots

- One of the challenges in security is to prevent malicious attempts at access by bots
- Bots might try millions of passwords per second
- DDOS a website
- Scan your page or grab data from it
- Snipe purchases that you are considering (to drive the price up or to sell to you later at a markup)

- (Bots do other stuff but in our context for now this is what we're worried about)

CAPTCHA

- Completely Automated Public Turing test to tell Computers and Humans Apart



- Primary use in security is to prevent automated attacks

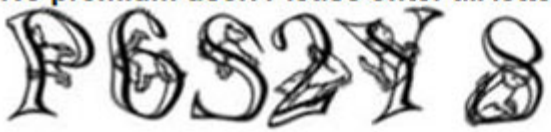
CAPTCHA

- Do I even need to explain what is wrong with CAPTCHAs from a UX perspective?

Download via TeliaSonera

Download via GlobalCrossing #2

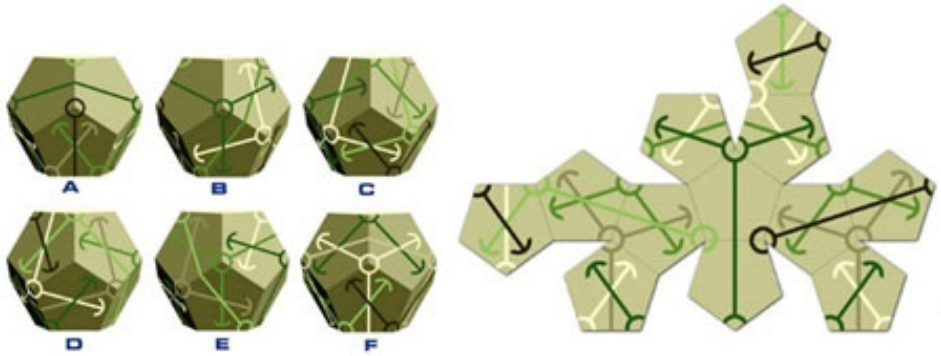
No premium user. Please enter all letters having a  **below.**



Four letters with a  **:** [ ] Download via Cogent

onus	Valid for	Payment-possibilities

No premium user. Please enter the one that can NOT be created from the unfolded pattern. 29 seconds remain.



[ ] Download via Cogent #2

Add Comment:

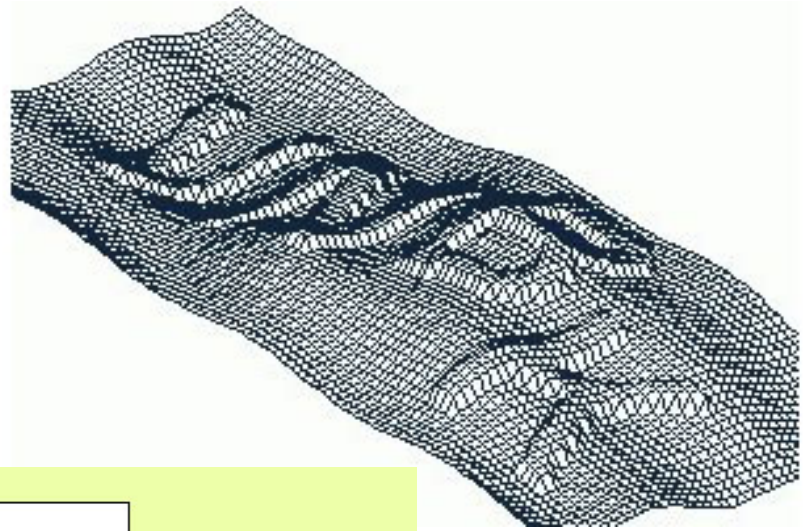
Your Name:

Comments:

Hidden Code:

Submit Query

Hidden code:



Password (required)

****

Birthday (required)

March | 31 | 1981

Human test (required)

Type in the text you see in the box below.

Sorry, your text and the image didn't match. Please try again.

Read (really!)

☑ I have read and agree to the **Terms of Use** and **Privacy Policy**.

CAPTCHA

- What about people who have low vision or hearing loss or just plain cannot figure the damn things out?

- What happens when machines get better at this than people (as has happened with some simple tests)

CAPTCHA

- Sort of aside from the security stuff, CAPTCHA's have proven interesting in other ways.
- Google can use them to train or identify information (e.g. street signs it cannot read automatically)
- And complex problems like text and object recognition have gotten a lot of research to address and solve these issues

Software Updates

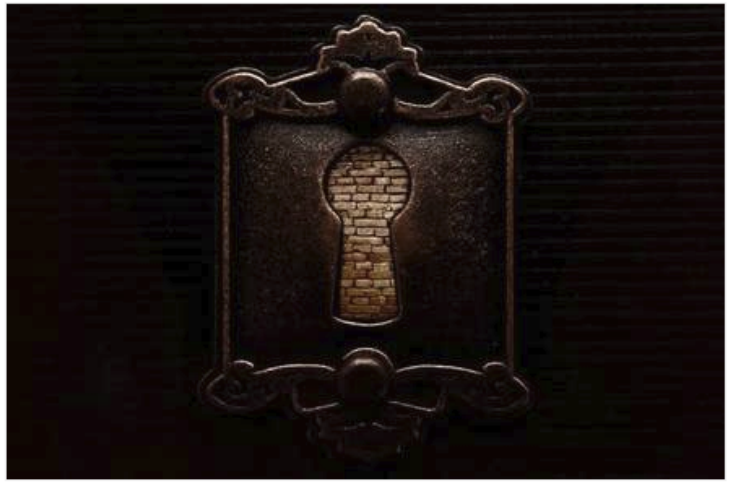
- Mandatory Software Updates
- Optional
- 3rd Party Software

Emergent Tech ▸ Internet of Things

Firmware update blunder bricks hundreds of home 'smart' locks

Automatic over-the-air upgrade will knacker front-door gear for at least five days

By Iain Thomson in San Francisco 11 Aug 2017 at 23:06 118 SHARE ▼



Hardware biz Lockstate has managed to brick hundreds of internet-connected so-called smart locks on people's front doors with a bad firmware update.

The upshot is you can't use the builtin keypad on the devices to unlock the door. Lockstate's smart locks are popular among Airbnb hosts as it allows them to give guests an entry code to get into properties without having to share physical keys. Lockstate is even a partner with Airbnb.

Earlier this week, though, new software was automatically sent out to folks' $469 Lockstate 6000i locks – one of the upstart's top residential smart locks – which left the keypad entirely useless. The crashed locks – which connect to your home Wi-Fi for remote control and monitoring as well as firmware updates – are now going to be out of action for at least a week.

Samsung's bad software update bricks smart TVs

Customers are angry over Samsung's bad update followed by terrible communications.

By Liam Tung | August 25, 2017 -- 12:56 GMT (05:56 PDT) | Topic: Internet of Things

12

Some owners are reporting their smart TV becoming stuck on a channel and unresponsive after the update.

Image: Samsung

Samsung smart TV customers are complaining that a software update has rendered their TVs unusable.

Exasperated customers are also furious at the lack of support and poor communication from Samsung after the bad update rolled-out last Thursday.

FEATURED STORIES

Meet Amazon's new hardware: Prices, features, release dates

MORE FROM LIAM TU

Mobility
Windows 10 Mobile's
Wileyfox revives its c
phone

Security
Google to lawmakers
data is still open to a

Enterprise Software
Windows 10 1803 log
Microsoft has finally

Mobility
iPhone XS, XS Max, X
size, RAM details rev
filings

NEWSLETTERS

ZDNet Innovation

This week in emerging te
innovative ideas from around
digital business transfo

Your email address

SEE ALL

RELATED STORIES

1 of 3

Nokia
safety
Nokia's
energy,
public
global
segme
in on o
involvin
LTE sol

In June 2016, a California woman won $10,000 (£8,000) after her PC was disabled when she installed a Windows 10 update. *(REUTERS/Shannon Stapleton)*

Lawyers representing three complainants allege hundreds of thousands of people have been affected by problems with upgrade

LUCY PASHA-ROBINSON
@lucypasha
Sunday 26 March 2017 22:06

Microsoft is being sued by three people who claim a Windows 10 update destroyed their data and damaged their computers.

The company "failed to exercise reasonable care in designing, formulating, and manufacturing the Windows 10 upgrade and placing it into the stream of commerce," the complaint filed in Chicago's District Court alleges.

The complainants argue the software is defective and that any potential risks about installing it were not made clear by the manufacturer.

His ISP has agreed to cut the charges in half and has warned all of its customers if they want Windows 10, the ISP will offer them a copy on a returnable USB memory device for free.

Nacef thinks the huge multiple download attempts to receive Windows 10 itself was responsible for most of the extra usage, but he is wary about the frequent software updates and the fact they are shared with other users by default.

That is what may have tripped up Rob DuGrenier who paid an exorbitant $150 this month for 1.5Mbps Internet service just to get a 75GB usage allowance for his immediate family in far northern Québec. The alternative was an overlimit fee of $20 for each 5GB allotment of usage over the usual 30GB allowance granted to "Power" users.

"Internet is not an option for our family for medical reasons, but this hurts," DuGrenier writes. "It is definitely Windows 10 and there is something wrong with it because our ISP reports we are sending a lot more data than we are receiving, and there are no viruses or malware on the computers."

His ISP now suspects Microsoft is using his connection to distribute software updates to a number of other users across northern Canada. When DuGrenier's family disabled the option that opted them in to distributing Microsoft updates to other customers, upstream traffic dropped 98%.

"Were we sending Windows 10 itself all over northern Quebec and Nunavut? We just don't know and Microsoft has not responded," DuGrenier reports. "They have billions, I do not. They should be paying my Internet bill this month."

- Software updates on a metered (notably satellite) connection can be disastrously expensive
- MS tried to use a P2P network to distribute updates

	Vendor Name	Number of Products	Number of Vulnerabilities	#Vulnerabilities/#Products
1	Microsoft	484	5879	12
2	Oracle	533	5292	10
3	Apple	116	4272	37
4	IBM	972	4067	4
5	Google	69	3598	52
6	Cisco	2666	3568	1
7	Adobe	124	2723	22
8	Linux	17	2157	127
9	Mozilla	23	2048	89
10	Redhat	269	1957	7

- That #vul/#products is crazy
- Note that this chart is cumulative to 1998

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Linux Kernel	Linux	OS	2142
2	Mac Os X	Apple	OS	2084
3	Android	Google	OS	1926
4	Firefox	Mozilla	Application	1742
5	Debian Linux	Debian	OS	1723
6	Chrome	Google	Application	1546
7	Iphone Os	Apple	OS	1495
8	Ubuntu Linux	Canonical	OS	1145
9	Windows Server 2008	Microsoft	OS	1116
10	Flash Player	Adobe	Application	1062
11	Safari	Apple	Application	984
12	Windows 7	Microsoft	OS	974
13	Internet Explorer	Microsoft	Application	952
14	Acrobat	Adobe	Application	951

- Again, cumulative so don’t read too much into it
- But that’s a LOT of bugs over 20 years

Home/Car Automation

- Google/Nest and Amazon (and a few others) are pushing hard into homes and cars

- What happens if your automation data gets compromised/accessed (someone shuts down your home heating system in the winter, or turns on your AC or something, which has both power cost and potential structural implications for your house)

Child locks mother's iPhone for 48 YEARS after repeatedly entering the wrong passcode and it could happen to YOU

- **A toddler from Shanghai was left with his mother's iPhone to play games**
- **The two-year old boy repeatedly entered the wrong code to unlock the phone**
- **When the mother returned it was locked for more than 25 million minutes**
- **Locked mobile phones can be returned to normal through a factory reset**

By JOE PINKSTONE FOR MAILONLINE

PUBLISHED: 10:43 EDT, 6 March 2018 | **UPDATED:** 17:27 EDT, 6 March 2018

A two-year-old boy has locked his mother's **iPhone** for 48 years after repeatedly entering the wrong passcode.

A mother in Shanghai left her son to watch 'educational videos' on her smartphone but returned to find it had been locked for 25 million minutes.

Apple's iPhones can be set to lock out anyone trying to use them if a wrong passcode is entered with the lockout period increasing with each failed attempt, but it is not clear how many times the child typed in the wrong numbers.

Scroll down for video

Social Engineering Attacks

- Familiarity - (Act like you belong)
- Hostile situation – (Act Angry)
- Gather information – (Trust/threaten)
- Learn body Language – (Be attractive, learn to read signs)
- Become an employee – (real or fake)

Sad Reality: Social Engineering

- No matter how much technical work you do, users will still give up passwords for chocolate bars
- And click on phishing links
- Etc.

Other things we can talk about if we have time

- Third party data gathering
- Data Retention
- Digital Estate assets

Third Party Data Gathering

- How do you know what third parties are getting data wise?

Data Retention

- See NCIX breach

- And toys R us apparently

Digital Estate assets

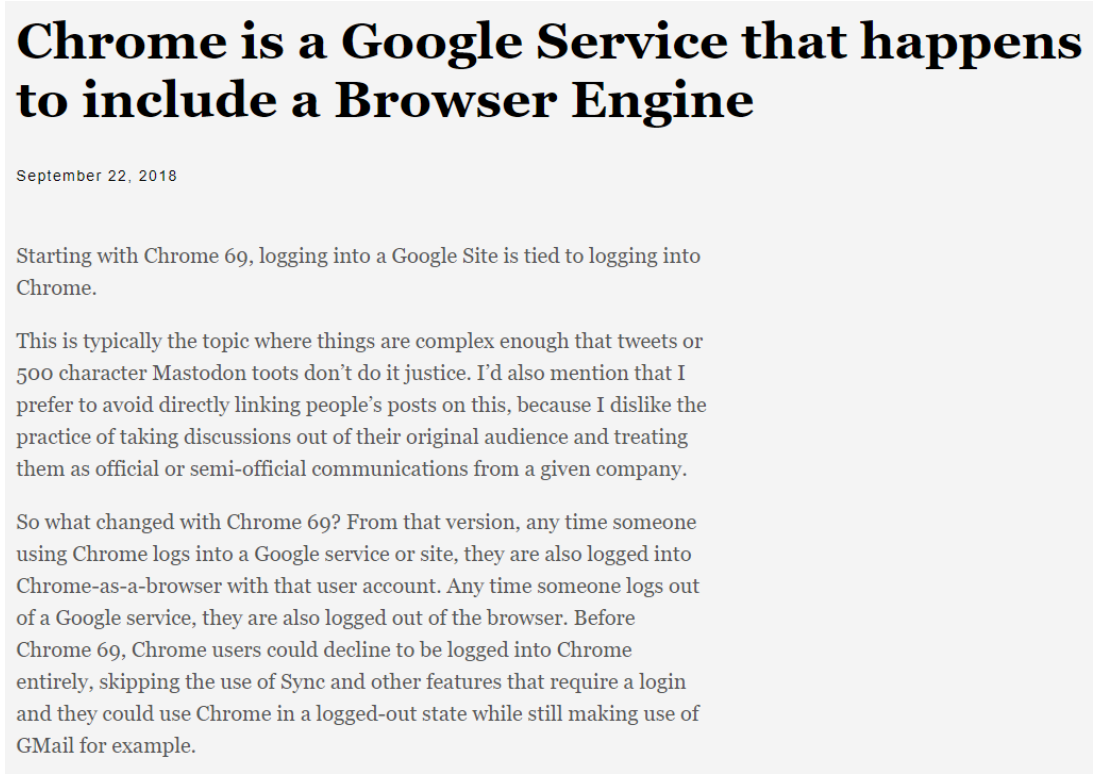
- Who owns your iTunes or Google play library if you die? (Are they even transferable)

- What about children attached to accounts?

Terms of Service

- Can you even know what you are agreeing to give up?
- That’s standard A4 sized paper

What does it mean to be logged in?



Chrome is a Google Service that happens to include a Browser Engine

September 22, 2018

Starting with Chrome 69, logging into a Google Site is tied to logging into Chrome.

This is typically the topic where things are complex enough that tweets or 500 character Mastodon toots don't do it justice. I'd also mention that I prefer to avoid directly linking people's posts on this, because I dislike the practice of taking discussions out of their original audience and treating them as official or semi-official communications from a given company.

So what changed with Chrome 69? From that version, any time someone using Chrome logs into a Google service or site, they are also logged into Chrome-as-a-browser with that user account. Any time someone logs out of a Google service, they are also logged out of the browser. Before Chrome 69, Chrome users could decline to be logged into Chrome entirely, skipping the use of Sync and other features that require a login and they could use Chrome in a logged-out state while still making use of GMail for example.

- Google is tying logging into chrome to logging in to Google services
- Or at least thinking about it

Google Amp, Opera Mobile Accelerator

- The idea is that all of your traffic is fed through their servers
- They (Google or Opera) in some way compress the result and send that to you

- This cuts bandwidth costs for mobile users and speeds up page loads

- But it means all of your content (including encrypted content) runs through their services

Next Week

- UI building blocks and some HTML