

Security Principles

CS 161: Computer Security
Prof. Vern Paxson

TAs: Paul Bramsen, Apoorva Dornadula,
David Fifield, Mia Gil Epner, David Hahn, Warren He,
Grant Ho, Frank Li, Nathan Malkin, Mitar Milutinovic,
Rishabh Poddar, Rebecca Portnoff, Nate Wang

<http://inst.eecs.berkeley.edu/~cs161/>

January 19, 2017



TL-15



TL-30



TRTL-30



TXTL-60

“Security is economics.”



utorrent mac



utorrent mac

utorrent mac **virus**

utorrent mac **free download**

utorrent mac **1.8.7**

[Mac and OSX Downloads - µTorrent® \(uTorrent\) - a \(very\) tiny ...](#)

www.utorrent.com/downloads/mac ▾

Download the official µTorrent® (uTorrent) torrent client for Windows, **Mac**, Android or Linux-- **uTorrent** ... For **Mac** (1.42 MB); English (US) - November 27, 2016.

[uTorrent \(Mac\)](#)

µtorrent estable(1.8.7 build 43001).

Para Mac (1.42 MB); Inglés ...

[More results from utorrent.com »](#)

[Download](#)

µTorrent Stable(1.8.7 build 43001).

Für Mac (1.42 MB); Englisch ...

[uTorrent \(Mac\) - Free download](#)

<https://utorrent.en.softonic.com/mac> ▾

★★★★★ Rating: 3 - 550 votes - Free - Mac OS - Utilities/Tools

uTorrent, free download. uTorrent 1.8.6: Super lightweight torrent client for **Mac**. **uTorrent for Mac** is a lightweight and efficient BitTorrent client that allows you to ...

IMPORTANT - Read this License Agreement carefully before clicking on the "Agree" button. By clicking on the "Agree" button, you agree to be bound by the terms of the License Agreement.

LICENSE AGREEMENT

Please review the license terms before installing μTorrent

μTorrent (also known as uTorrent) is a peer-to-peer file sharing application distributed by BitTorrent, Inc.

By accepting this agreement or by installing μTorrent, you agree to the following μTorrent-specific terms, notwithstanding anything to the contrary in this agreement.

License.

Subject to your compliance with these terms and conditions, BitTorrent, Inc. grants you a royalty-free, non-exclusive, non-transferable license to use μTorrent, solely for your personal, non-commercial purposes. BitTorrent, Inc. reserves all rights in μTorrent not expressly granted to you here.

Restrictions.

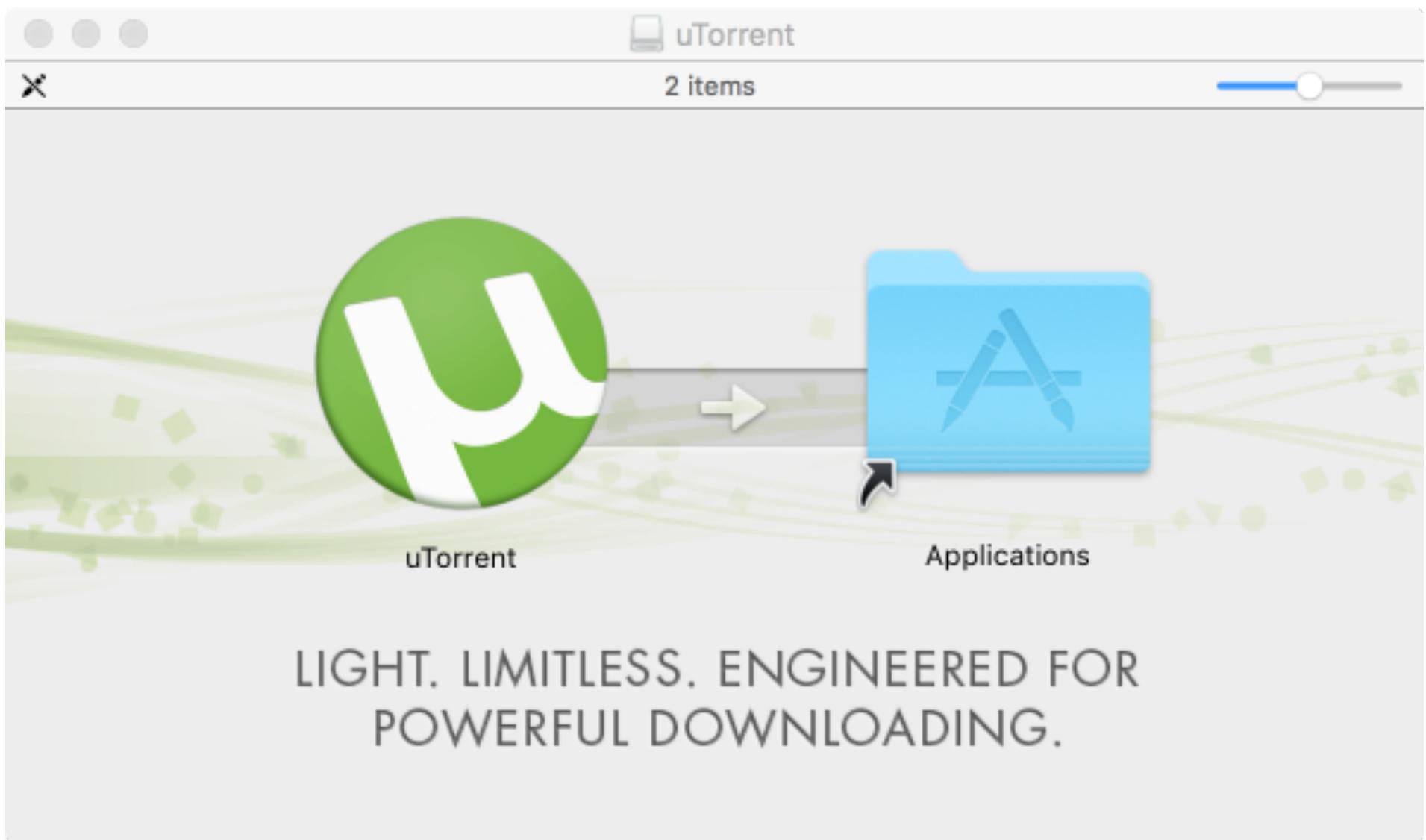
The source code, design, and structure of μTorrent are trade secrets. You will not disassemble, decompile, or reverse engineer it in whole or in part

Print

Save...

Disagree

Agree



LIGHT. LIMITLESS. ENGINEERED FOR
POWERFUL DOWNLOADING.

Advertisement ×

µTorrent

Add URL Add Feed

Start Stop Remove

Upgrade Now

Search piracy

TORRENTS

- All
- Downloading
- Completed
- Active
- Inactive

LABELS

No Label

FEEDS

All Feeds

Name # Size Done Status Seeds Peers ↓ Speed ↑ Speed ETA Uploaded

General Trackers Files Peers Speed

Downloaded: Availability:

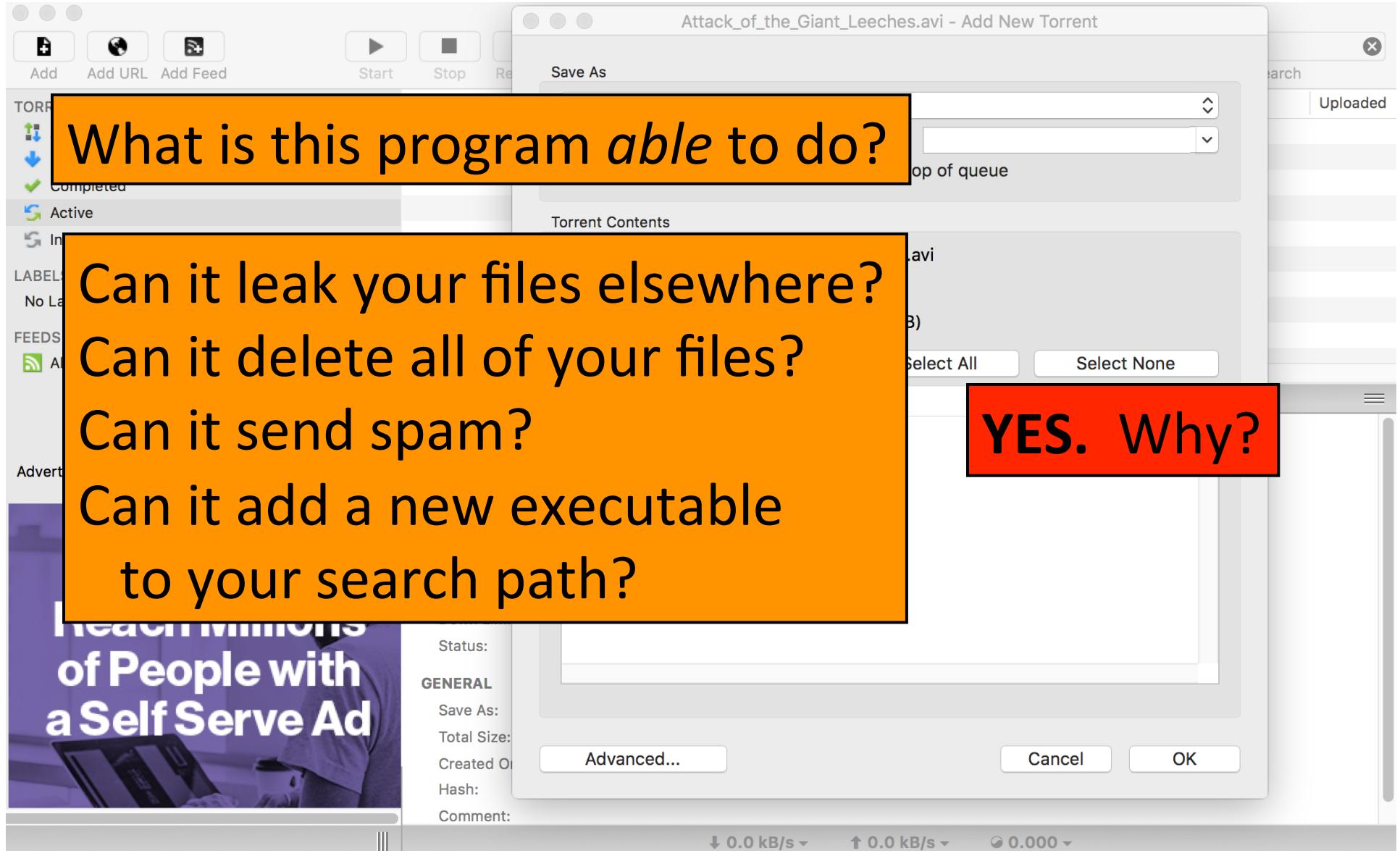
TRANSFER

Time Elapsed:	Remaining:	Wasted:
Downloaded:	Uploaded:	Seeds:
Download Speed:	Upload Speed:	Peers:
Down Limit:	Up Limit:	Share Ratio:
Status:		

GENERAL

Save As:	Pieces:
Total Size:	
Created On:	
Hash:	
Comment:	

↓ 0.0 kB/s ▾ ↑ 0.0 kB/s ▾ 0.000 ▾



What does this program *need* to be able to do?

Maybe:

- access screen
- manage a directory of downloaded files
- access config & documentation files
- open connections for a given set of protocols
- receive connections as a server

a Self Serve Ad

Attack_of_the_Giant_Leeches.avi - Add New Torrent

Save As

Torrent Contents

Labels: No Labels

Feeds: All

Advertisers

Save As:

Total Size:

Created On:

Hash:

Comment:

Advanced...

Cancel

OK

↓ 0.0 kB/s ▾ ↑ 0.0 kB/s ▾ ⏴ 0.000 ▾

A screenshot of a torrent client application. At the top, there's a toolbar with buttons for 'Add', 'Add URL', 'Add Feed', 'Start', 'Stop', and 'Re'. Below the toolbar, there's a sidebar with sections for 'TORRENTS' (Completed, Active, In Queue), 'LABELS' (No Labels), and 'FEEDS' (All). A purple sidebar on the left has a 'Self Serve Ad' section featuring a person at a computer. In the center, a modal dialog box titled 'Attack_of_the_Giant_Leeches.avi - Add New Torrent' is open, prompting the user to 'Save As'. The dialog includes fields for 'Save As:', 'Total Size:', 'Created On:', 'Hash:', and 'Comment:', along with 'Advanced...', 'Cancel', and 'OK' buttons. At the bottom of the main window, there are speed indicators: '↓ 0.0 kB/s', '↑ 0.0 kB/s', and '0.000'.

“Least privilege.”

Check for Understanding

- We've seen that laptop/desktop platforms grant applications a lot of privileges
- Quiz: Name a platform that does a better job of least privilege

**Allow “Adult Cat Finder” to
access your location while
you use the app?**

We use your location to find nearby
adorable cats.

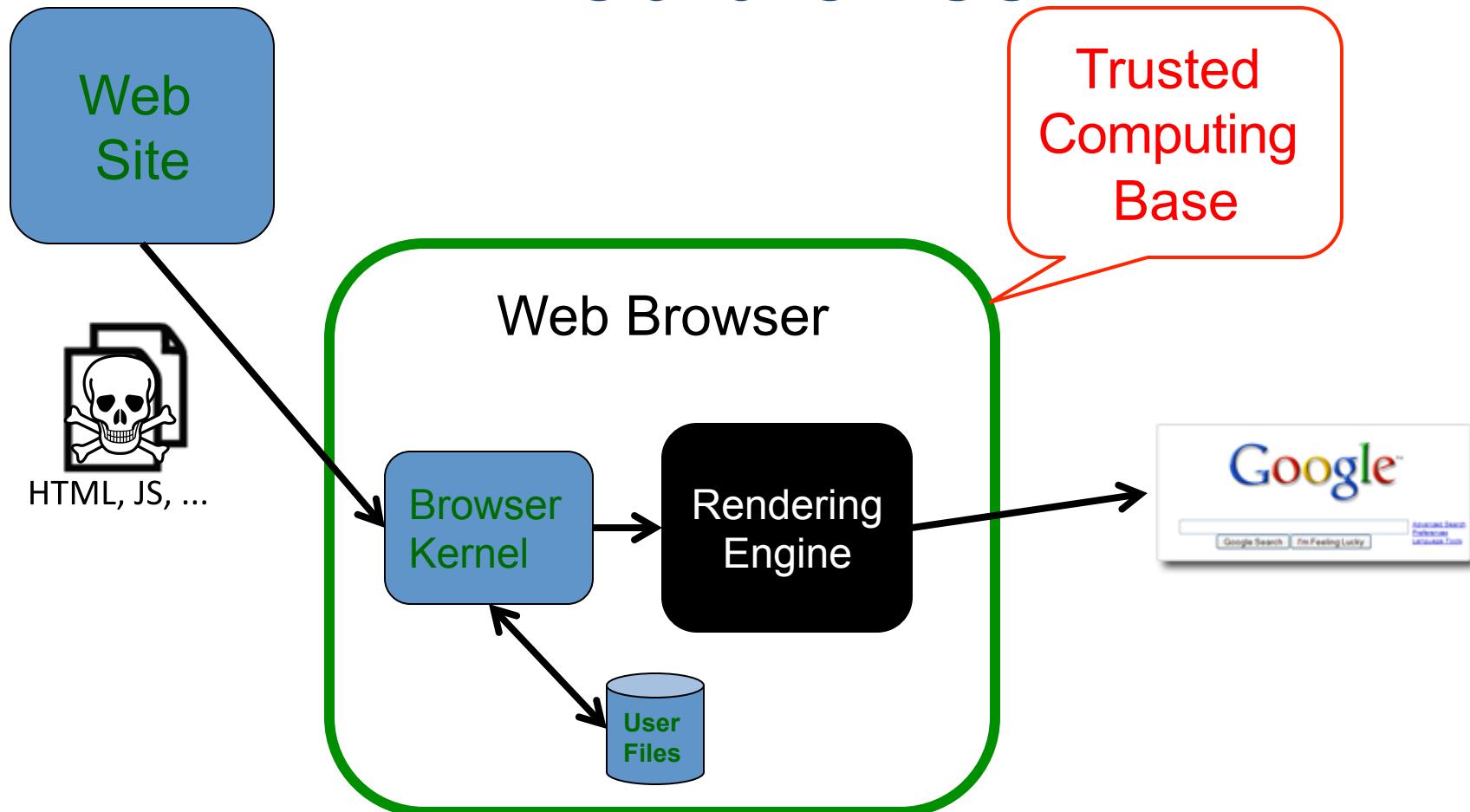
[Don't Allow](#)

[Allow](#)

Thinking About Least Privilege

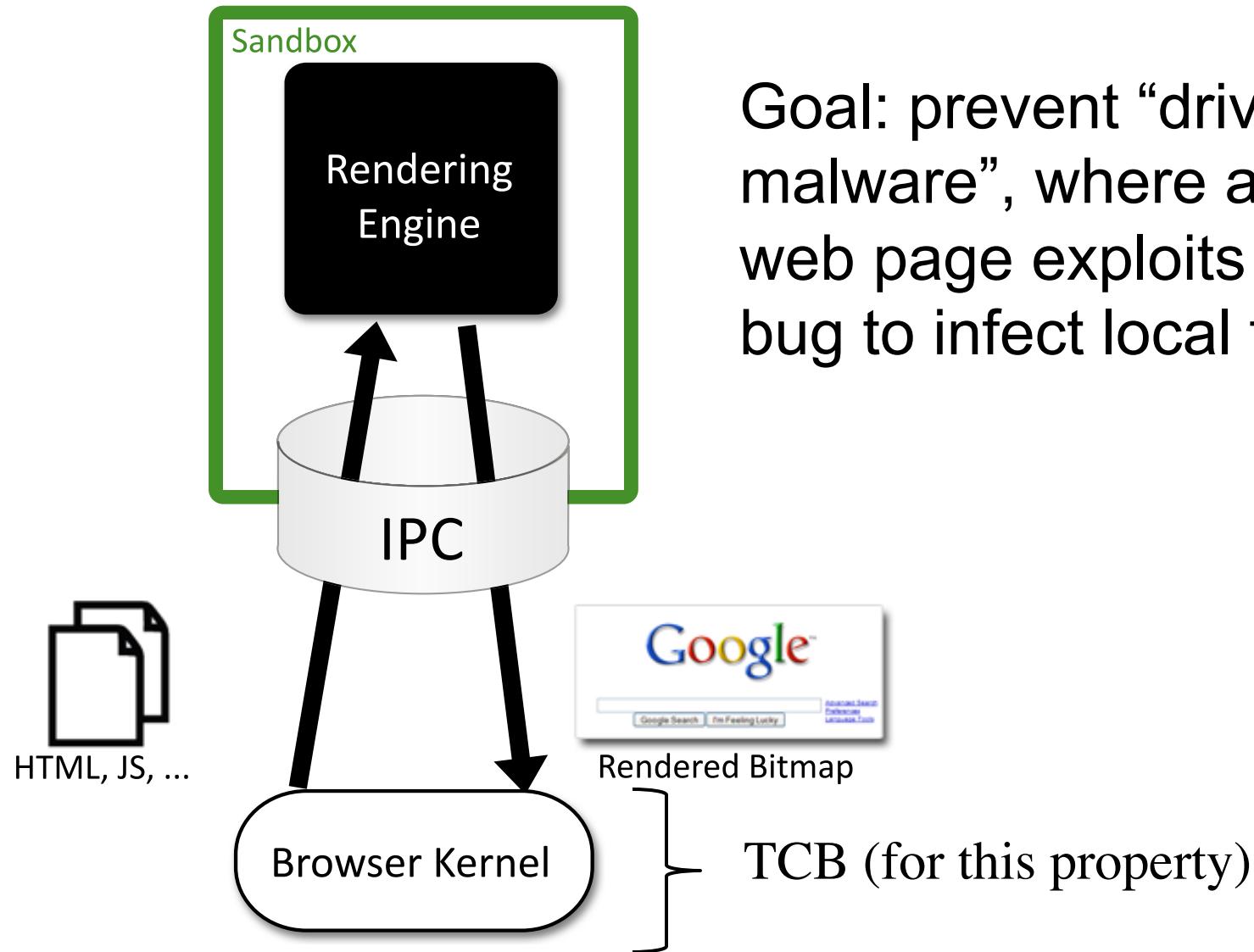
- When assessing the security of a system's design, identify the *Trusted Computing Base (TCB)*.
 - What components does security **rely upon?**
- Security requires that the TCB:
 - Is **correct**
 - Is **complete** (can't be bypassed)
 - Is itself **secure** (can't be tampered with)
- Best way to be assured of correctness and its security?
 - **KISS** = *Keep It Simple, Stupid!*
 - Generally, **Simple** = **Small**
- One powerful design approach: **privilege separation**
 - **Isolate** privileged operations to as small a component as possible

Web browser

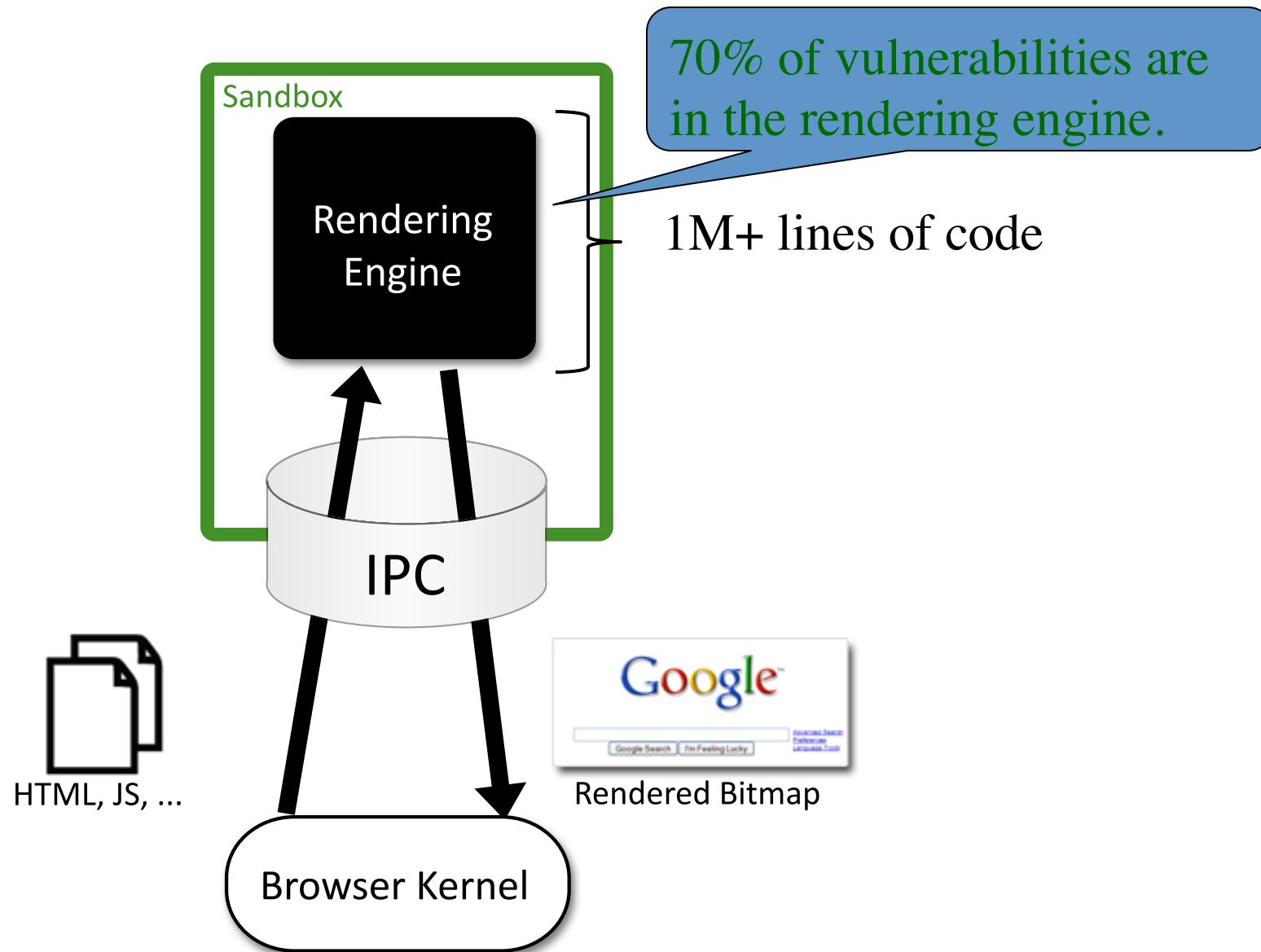


“Drive-by malware”: malicious web page
exploits browser bug to infect local files

The Chrome browser



The Chrome browser





“Ensure complete mediation.”

For every requested action,
check *authenticity, integrity,*
authorization

Ensuring Complete Mediation

- To secure access to some capability/resource, construct a *reference monitor*
- Single point through which all access must occur
 - E.g.: a network firewall
- Desired properties:
 - Un-bypassable (“complete mediation”)
 - Tamper-proof (is itself secure)
 - Verifiable (correct)
 - (Note, just restatements of what we want for TCBs)
- One subtle form of reference monitor flaw concerns *race conditions* ...

TOCTTOU Vulnerability

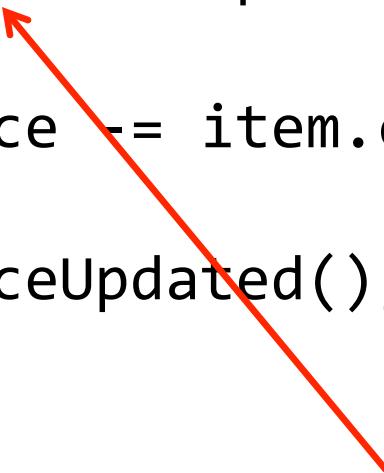
```
procedure withdrawal(w)
    // contact central server to get balance
    1. let b := balance
    2. if b < w, abort
    // contact server to set balance
    3. set balance := b - w
    4. dispense $w to user
```

Suppose that *here* an attacker arranges to suspend first call, and calls withdrawal again **concurrently**



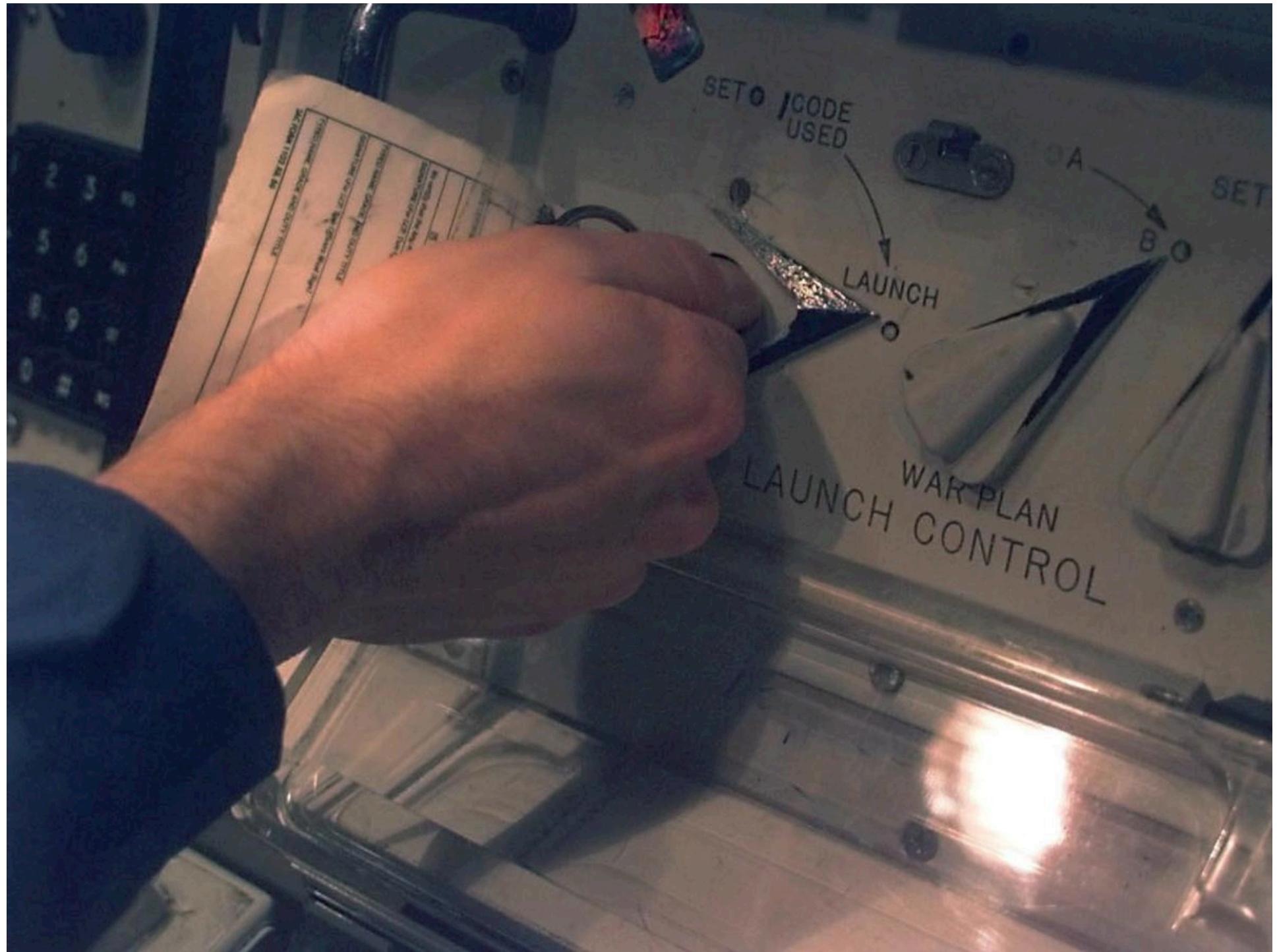
TOCTTOU = Time of Check To Time of Use

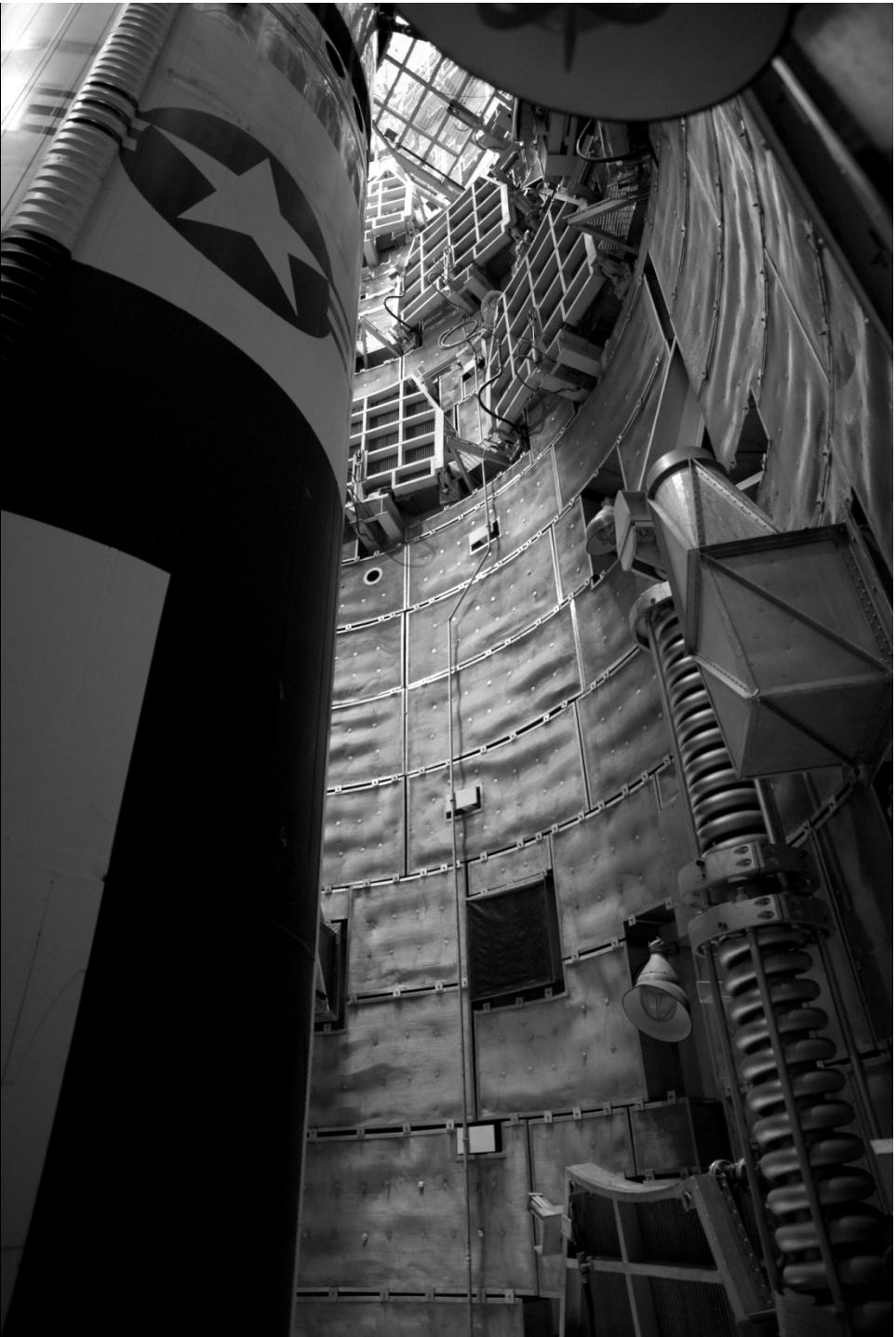
```
public void buyItem(Account buyer, Item item) {  
  
    if (item.cost > buyer.balance)  
        return; /* they can't afford it */  
  
    buyer.possessions.put(item); /* provide item */  
  
    buyer.possessionsUpdated(); /* freshen screen */  
    buyer.balance -= item.cost; /* deduct cost */  
  
    buyer.balanceUpdated(); /* freshen screen */  
}
```



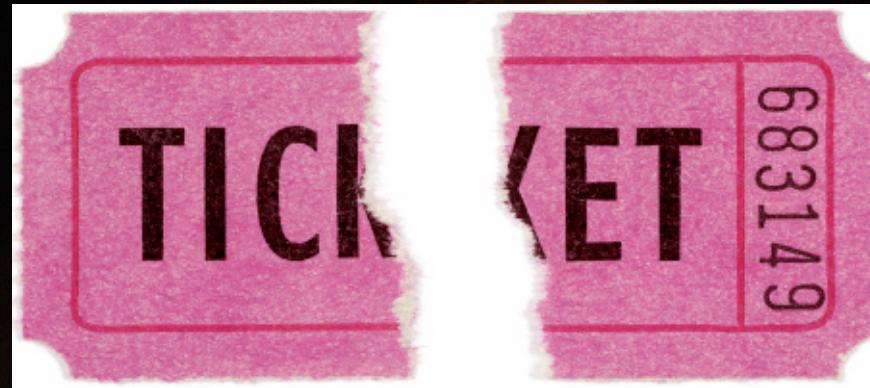
What if an **uncaught exception** happens *here*?







“Separation of responsibility.”

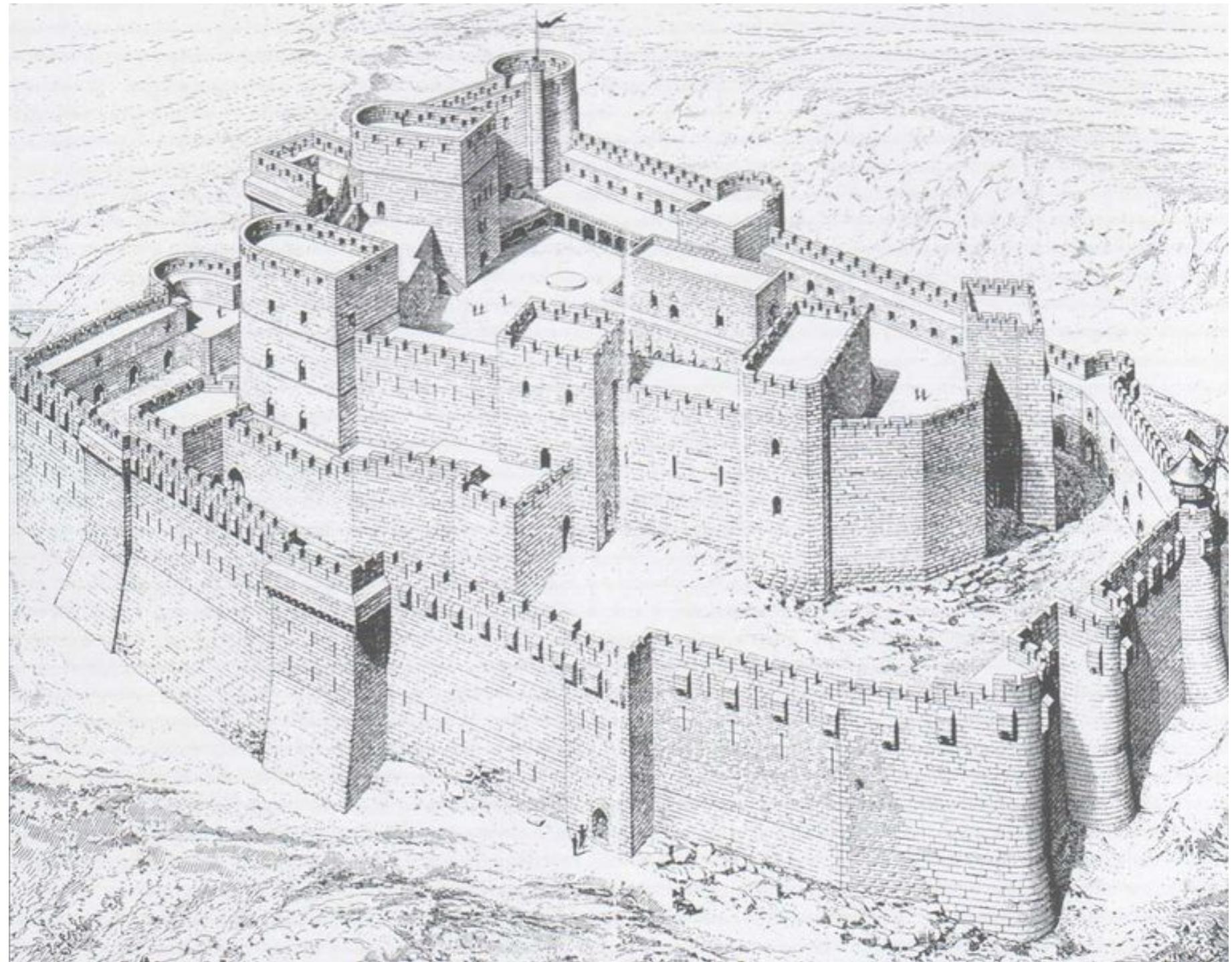


Independent audit



Summary: Notions Regarding Managing Privilege

- Least privilege
 - The notion of avoiding having unnecessary privileges
- Privilege separation
 - A way to achieve least privilege by isolating access to privileges to a small Trusted Computing Base (**TCB**)
- Separation of responsibility
 - If you need to have a privilege, consider requiring multiple parties to work together (collude) to exercise it



“Defense in depth.”

GSA Container Classes Defined:

GSA: General Services Administration (US Government)

GSA Class 1:
a GSA approved container meeting Federal Specification AA-F-357(canceled) with entry protection consisting of 10 Man-Minutes forced entry, 30 Man-Minutes surreptitious entry and 30 Man-Minutes covert entry



GSA Class 2:
a GSA approved container meeting Federal Specification AA-F-357(canceled) with entry protection consisting of 10 Man-Minutes forced entry, 20 Man-Minutes surreptitious entry and 20 Man-Minutes covert entry

GSA Class 3:
a GSA approved container meeting Federal Specification AA-F-358 with entry protection consisting of 10 Man-Minutes forced entry, 20 Man-Minutes surreptitious entry and 20 Man-Minutes covert entry

GSA Class 4:
a GSA approved container meeting Federal Specification AA-F-358 with entry protection consisting of 10 Man-Minutes forced entry, 20 Man-Minutes surreptitious entry and 20 Man-Minutes covert entry

Federal Specification AA-F-357(canceled)
Minutes forced entry
Minutes surreptitious entry

Federal Specification AA-F-358
Minutes forced entry
Minutes surreptitious entry

Federal Specification AA-F-357(canceled)
Minutes forced entry
Minutes surreptitious entry

Federal Specification AA-F-358
Minutes forced entry, 20 Man-Hours surreptitious entry and 30 Man-Minutes covert entry



Class 5 Four Drawer

GSA Class 5:

a GSA approved uninsulated container meeting Federal Specification AA-F-358 with entry protection consisting of 10 Man-Minutes forced entry, 20 Man-Hours surreptitious entry and 30 Man-Minutes Covert entry

358 with entry protection consisting of 20 Man-Hours surreptitious entry and 30 Man-Minutes covert entry



“Company policy: passwords must be at least 10 characters long, contain at least 2 digits, 1 uppercase character, 1 lowercase character, and 1 special character.”

COMPANY Portal
Password: 1secret

Bank
password:
goMets12

credit card:
bowser8

brokerage:
initial23

e-mail:
letmein

Log in to your message center.

Invalid log in or server error. Please try again.

[Forgot your password?](#)

Log in Address

example: joe234@jumbowidgetsco.com

Password

note: password is case-sensitive

Remember my Address and Password ([what is this?](#))

LOG IN

Done

login.postini.com

“Psychological acceptability.”

Internet Explorer



When you send information to the Internet, it might be possible for others to see that information. Do you want to continue?



In the future, do not show this message.

Yes

No

Internet Explorer



When you see a dialog box like this, click 'Yes' to make it go away. If available, click the checkbox first to avoid being bothered by it again.



In the future, do not show this message.

Yes

No

Website Certified by an Unknown Authority



Unable to verify the identity of svn.xiph.org as a trusted site.

Possible reasons for this error:

- Your browser does not recognise the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be svn.xiph.org, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to accept this certificate for the purpose of identifying the Web site svn.xiph.org?

[Examine Certificate...](#)

- Accept this certificate permanently
- Accept this certificate temporarily for this session
- Do not accept this certificate and do not connect to this Web site

OK

Cancel

Website Certified by an Unknown Authority



Unable to verify the identity of svn.xiph.org as a trusted site.

Blah blah geekspeak geekspeak geekspeak.

Before accepting this certificate, your browser can display a second dialog full of incomprehensible information. Do you want to view this dialog?

[View Incomprehensible Information](#)

- Make this message go away permanently
- Make this message go away temporarily for this session
- Stop doing what you were trying to do

OK

Cancel

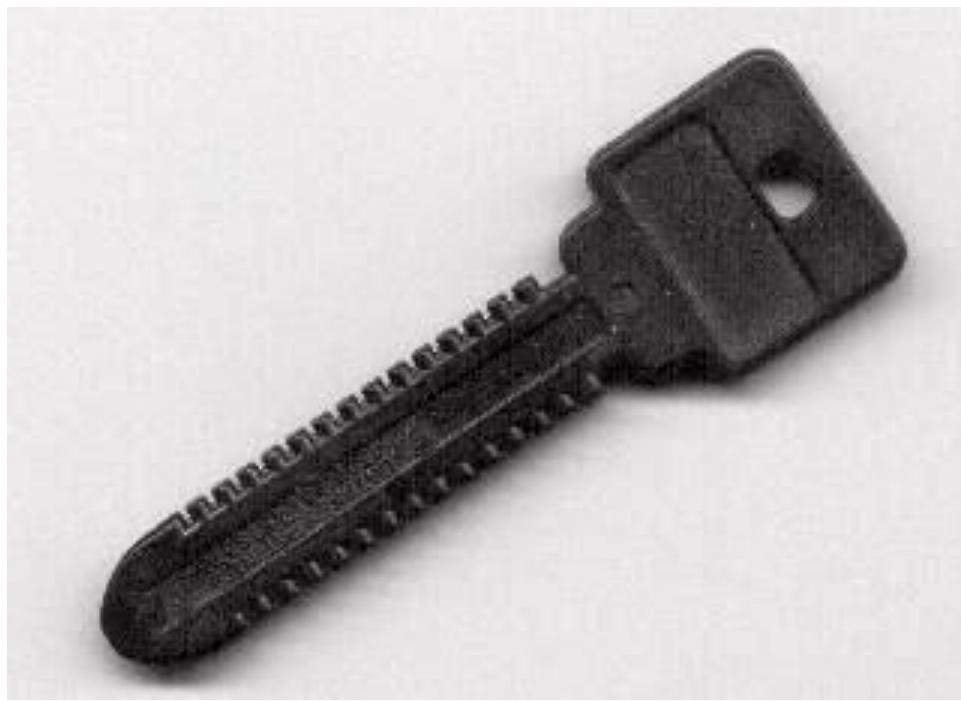
What a piece of work is a man! how Noble in Reason! how infinite in faculty! in form and moving how express and admirable! in Action, how like an Angel! in apprehension, how like a God!

-- *Hamlet* Act II, Scene II

“Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. (They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.)”

-- *Network Security: Private Communication in a Public World*,
Charlie Kaufman, Radia Perlman, & Mike Speciner, 1995

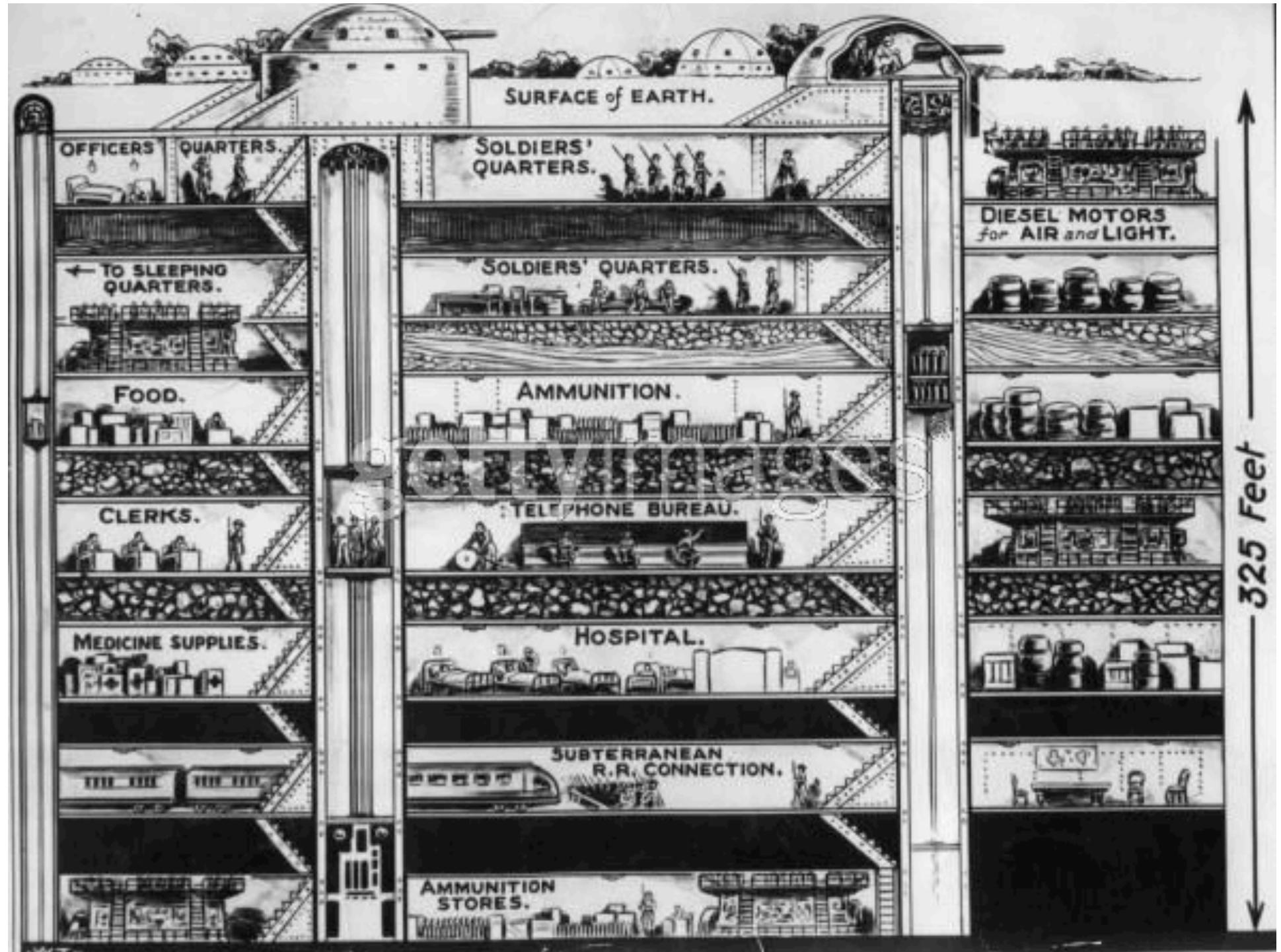
“Consider human factors.”



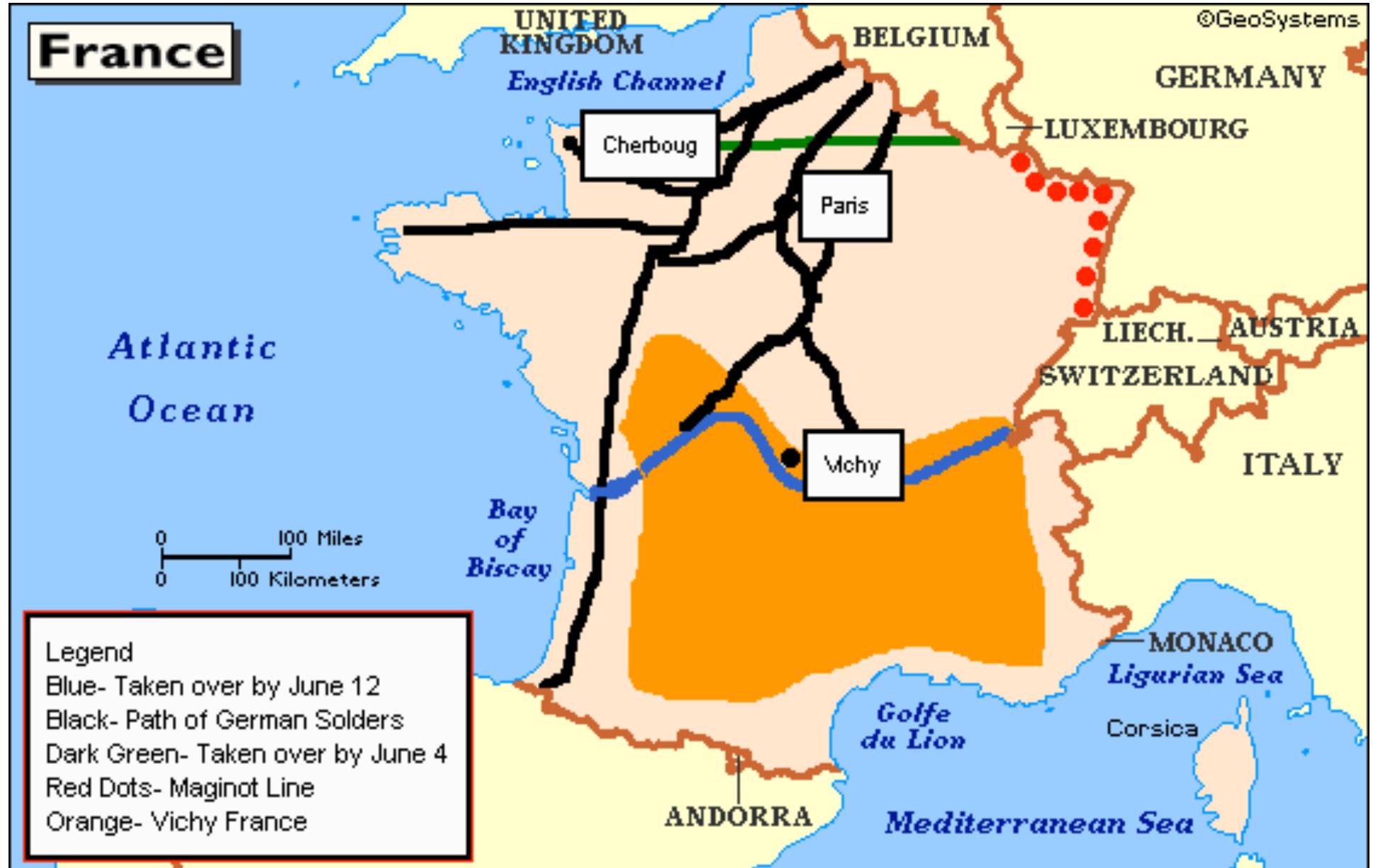
Summary: Dealing with Users

- Psychological acceptability
 - Will users abide a security mechanism, or *decide* to subvert it?
- Consider human factors
 - Does a security mechanism assume something about human behavior when interacting with the system that might not hold, even *in the absence* of conscious decisions by the users to subvert









“Only as secure as the weakest link.”

ACCIDENT
ON
MOTORWAY







RAPTORS
AHEAD
CAUTION

JANNA
MARCH
NUTTER
FRESH FISH
GROCERY
PETCO

TRAPPED
IN SIGN
FACTORY





SEND
HELP!

“Don’t **rely on security through
obscurity.”**

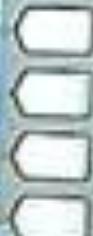


Selma's die traditionelle Brause
mit einem frischen Zitrusduft



Selma's die traditionelle Brause
mit einem frischen Zitrusduft
enthaltend 10% Bergamotte und 10% Zitrone
in einem frischen Zitrusduft

zum
Brausen



Abtropfdeckel abnehmen

1. Abtropfdeckel abnehmen



 Bradesco

Tarifas de
Servicios Bancarios

Atención Privada

www.bradescobancos.com

Multi Expresso

 Bradesco

Para sacar de su cuenta
dinero en efectivo o transferir
dinero a otra cuenta de su
banco o de otro banco.

Para pagar facturas.

Para pagar boletos de avión,

tren, ómnibus, taxi, etc.

Para pagar en comercios.

Para pagar en gasolineras.

Para pagar en estaciones de

servicio.

Para pagar en hoteles.

Para pagar en restaurantes.

Para pagar en supermercados.

Para pagar en farmacias.

Para pagar en clínicas.

Para pagar en hospitales.



Caixa

Teléfonos de
Serviços Bancários.

Bandeira

Cartão de Crédito





“Trusted path.”

User needs to know they’re talking w/ legit system.
System needs to know it’s talking w/ legit user.
These channels should be unspoofable & private.