



# Announcements

- Programming Assignment #1
- Week 2 Discussion Forum
- Week 2 Labs

Week 2

May 2014



## 145 Million eBay Users Hacked

- Compromised name, encrypted password, email, home address, etc.
- Companywide password reset function was used in the attack.
- “The focus is on recovery,” CEO John Donahoe.



Week 2

Sept 2014



## Five Month Undetected Attack at Home Depot

- Compromised 56 million customer payment cards
- CEO apologized publicly after the cyber attack
- Famous security budget retort from ex-employee: "We sell hammers."

Week 2

Nov 2014



## Sony Destructively Hacked by North Korea

- Destructive malware attack ruined Sony compute infrastructure
- Revealed corporate emails including racist remarks about Pres. Obama
- "It was an attack on our freedom of expression." DHS Secretary Johnson

Week 2

Feb 2015

## The Details

- Company notified feds immediately
- No information compromised
- Massive database hacked

Anthem. 

JUST IN

**FBI INVESTIGATING LATEST DATA BREACH**  
ANTHEM INC. CREDITED FOR PROMPTLY NOTIFYING AUTHORITIES

#abc15

**abc 15**

10:06 65°

## 80 Million Medical Records Stolen from Anthem

- Two month process to notify astonished customers
- Abnormal system behavior went unnoticed for several months
- “I want to personally apologize to each of you.” *Joseph Swedish, CEO*



Week 2

June 2015



## Hackers Breach Harvard University Credentials

- Involved eight colleges (Arts & Sciences, Divinity, Radcliffe, etc.)
- University has no clear understanding of what happened or how
- FAQ suggests that everyone change their passwords

Week 2

Dec 2015



Plant supporting Stroganovka,  
outside Simferopol, Crimea

## Hackers Shut Power to 80,000 Ukrainian Citizens

- Hacked Power Company 1: Prykarpattiaoblenergo Electric Utility
- Hacked Power Company 2: Kyivoblenergo Electric Utility
- Affected Six More Companies with BlackEnergy Trojan Horse



Week 2

Jan 2016



## 191 Million US Voter Records Compromised

- NationBuilder collects information and provides as-a-service
- “We strongly believe in making voter information more accessible to political campaigns and advocacy groups,” NationBuilder's CEO Jim Gilliam

Week 2

Mar 2016

The Verizon logo is displayed in white on a red background. It features a large, stylized white checkmark above the word "verizon" in a bold, lowercase sans-serif font.

## Hackers Sell 1.5 Million Customer Records

- 1.5 million Verizon customer records stolen from the company
- Sale price: \$100,000 for the entire package on the Dark Web
- Verizon blamed an exploitable flaw in their Website

Week 2

Oct 2016

- 
- Airbnb<sup>[11]</sup>
  - Amazon.com<sup>[8]</sup>
  - Ancestry.com<sup>[12][13]</sup>
  - *The A.V. Club*<sup>[14]</sup>
  - BBC<sup>[13]</sup>
  - *The Boston Globe*<sup>[11]</sup>
  - Box<sup>[15]</sup>
  - *Business Insider*<sup>[13]</sup>
  - CNN<sup>[13]</sup>
  - Comcast<sup>[16]</sup>
  - CrunchBase<sup>[13]</sup>
  - DirecTV<sup>[13]</sup>
  - *The Elder Scrolls Online*<sup>[13][17]</sup>
  - Electronic Arts<sup>[16]</sup>
  - Etsy<sup>[11][18]</sup>
  - FiveThirtyEight<sup>[13]</sup>
  - Fox News<sup>[19]</sup>
  - *The Guardian*<sup>[19]</sup>
  - GitHub<sup>[11][16]</sup>
  - Grubhub<sup>[20]</sup>
  - HBO<sup>[13]</sup>
  - Heroku<sup>[21]</sup>
  - HostGator<sup>[13]</sup>
  - iHeartRadio<sup>[12][22]</sup>
  - Imgur<sup>[23]</sup>
  - Indiegogo<sup>[12]</sup>
  - Mashable<sup>[24]</sup>
  - National Hockey League<sup>[13]</sup>
  - Netflix<sup>[13][18]</sup>
  - *The New York Times*<sup>[11][16]</sup>
  - Overstock.com<sup>[13]</sup>
  - PayPal<sup>[18]</sup>
  - Pinterest<sup>[16][18]</sup>
  - Pixlr<sup>[13]</sup>
  - PlayStation Network<sup>[16]</sup>
  - Qualtrics<sup>[12]</sup>
  - Quora<sup>[13]</sup>
  - Reddit<sup>[12][16][18]</sup>
  - Roblox<sup>[25]</sup>
  - Ruby Lane<sup>[13]</sup>
  - *RuneScape*<sup>[12]</sup>
  - SaneBox<sup>[21]</sup>
  - Seamless<sup>[23]</sup>
  - *Second Life*<sup>[26]</sup>
  - Shopify<sup>[11]</sup>
  - Slack<sup>[23]</sup>
  - SoundCloud<sup>[11][18]</sup>
  - Squarespace<sup>[13]</sup>
  - Spotify<sup>[12][16][18]</sup>
  - Starbucks<sup>[12][22]</sup>
  - Storiify<sup>[15]</sup>
  - Swedish Civil Contingencies Agency<sup>[27]</sup>
  - Swedish Government<sup>[27]</sup>
  - Tumblr<sup>[12][16]</sup>
  - Twilio<sup>[12][13]</sup>
  - Twitter<sup>[11][12][16][18]</sup>
  - Verizon Communications<sup>[16]</sup>
  - Visa<sup>[28]</sup>
  - Vox Media<sup>[29]</sup>
  - Walgreens<sup>[13]</sup>
  - *The Wall Street Journal*<sup>[19]</sup>
  - Wikia<sup>[12]</sup>
  - *Wired*<sup>[15]</sup>
  - Wix.com<sup>[30]</sup>
  - WWE Network<sup>[31]</sup>
  - Xbox Live<sup>[32]</sup>
  - Yammer<sup>[23]</sup>
  - Yelp<sup>[13]</sup>
  - Zillow<sup>[13]</sup>

## DYN DDOS Attack

- Massive DDOS attack (possibly by Anonymous)
- Caused outages across major North American services
- Botnet: Cameras, gateways, baby monitor, and other IoT devices



Week 2

Nov 2016



## US Election “Information” Attacks

- Difference between “cyber superiority” and “information superiority”
- American Intelligence Community concludes Russian origin
- Social media manipulated using poorly monitored features

Week 2

May 2017



## WannaCry Ransomware Attack

- Hits 300,000 targets including National Institute of Health (NIH)
- Spread via worm using tools stolen from NSA
- Suggests weak disaster planning across most global business

Week 2

July 2017



## Equifax Breach Affects 143M US Citizens

- Vulnerabilities unpatched in Apache Struts in Equifax portal
- First vulnerability reported weeks before attack commenced
- Hackers created 39 undetected back doors into Equifax



Week 2

Nov 2017

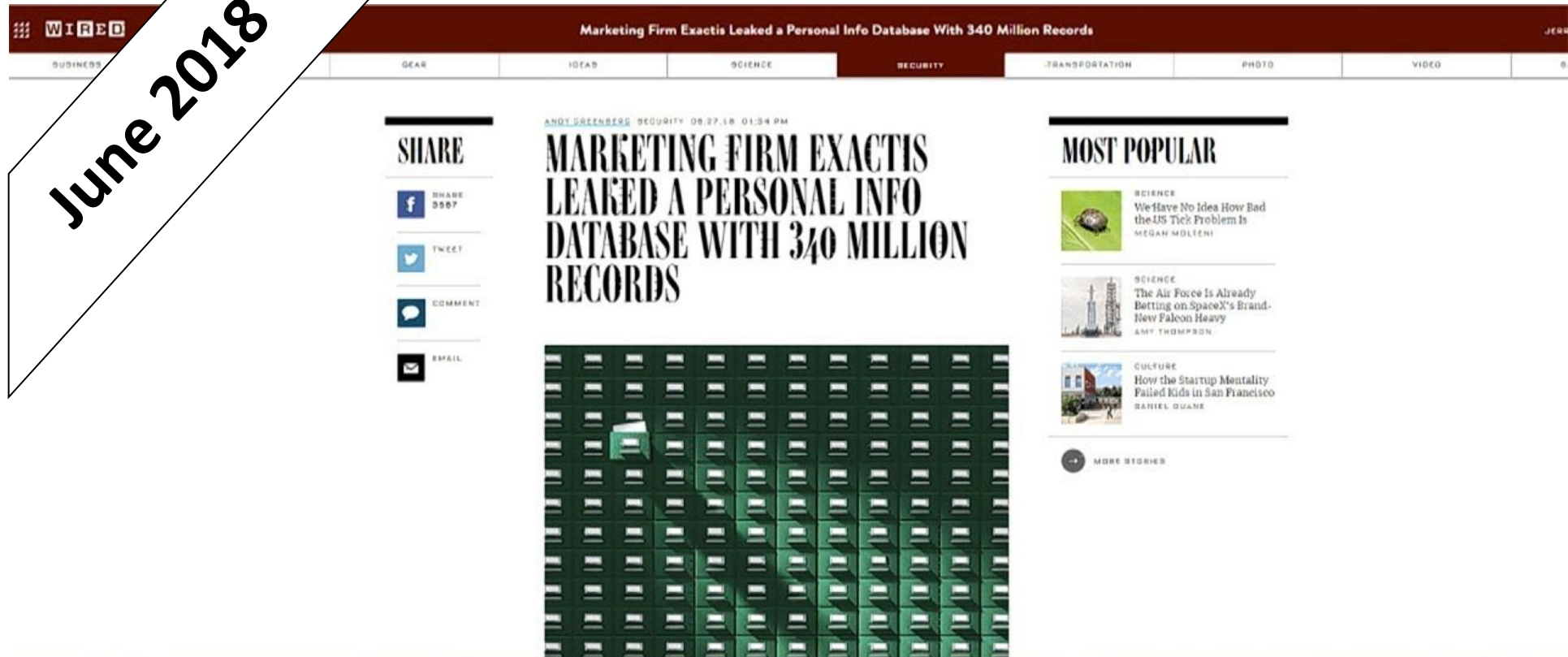


## Hackers Breach Personal Data for 45M Uber Riders

- Attack occurred in 2016 (GitHub account), but reported in 2017
- Hackers demanded \$100K for data and Uber paid the fee
- Cover-up causing considerable litigation on-going

Week 2

June 2018



## Exactis Exposes Data for 340M US Citizens

- Marketing firm had hacked data included name, address, email, etc.
- Security researcher noticed database openly accessible (via Shodan)
- Massive implications for citizen privacy

Week 2

**NBC NEWS**

gone ahead and fixed your Microsoft email server

SHARE THIS — f t e ...

**March 2021**

## The FBI might have gone ahead and fixed your Microsoft email server

The unusual operation highlights the severity of the Exchange vulnerability, which allowed scores of hackers to break into organizations since the beginning of the year.



## Microsoft Exchange, The FBI & A Lack Of Patching

- FBI has been quietly removing the web shells from infected systems
- Microsoft Exchange flaw that allowed hackers to install web shells to exfiltrate data and credentials
- Provides access and enables code execution. 120,000 systems had been infected and less than 10,000 remained unpatched as of March 22, 2021



## Under attack: California schools face ransomware threat



BY ZAYNA SYED , JULY 14, 2021 UPDATED JULY 15, 2021

Twitter

Facebook

WhatsApp



### University of California Schools Hit with Ransomware Attack

- Attack that targeted vulnerabilities in Accellion's legacy File Transfer Appliance
- Stolen data included the personal information of faculty and students
- A total of six vulnerabilities have been discovered and patched

# A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack

April 16, 2021 · 10:05 AM ET  
Heard on [All Things Considered](#)



DINA TEMPLE-RASTON



12-Minute Listen

+ PLAYLIST



March 2021



## SolarWinds attack reveals a hack launched by a sophisticated adversary

- Major US information technology firm, was the subject of a cyberattack that spread to its clients and went undetected for months
- Use the hack to spy on private companies like the elite cybersecurity firm FireEye and the upper echelons of the US Government
- The code created a backdoor to customer's information technology systems,

Week 2

## 533 million Facebook users' phone numbers and personal data have been leaked online

Aaron Holmes Apr 3, 2021, 10:41 AM



April 2021



## Facebook Data Leak Impacts 533 Million Users

- Data included account creation date, bio, birthdate, Facebook IT, full name, location, past location and relationship status, free to members of a hacking forum.
- Used deceptive disclosures and settings to undermine users' privacy preferences in violation of a FTC order with third-party



Week 2



May 2021

the Cyberattack

What to Know

Pipeline Resumes

\$5 Million Ransom

DarkSide Says Shutting Down

Weaknesses

## *Cyberattack Forces a Shutdown of a Top U.S. Pipeline*

The operator, Colonial Pipeline, said it had halted systems for its 5,500 miles of pipeline after being hit by a ransomware attack.



# Ransomware Attack Closes Colonial Pipeline

- Lack adequate physical and cyber security
- Corporate computer networks had been hit by a ransomware attack
- Hit by ransomware in a vivid demonstration of the vulnerability of energy infrastructure to cyberattacks

# Fundamental Design Principles

General Design Principles (not just security)

- Principle of Open Design
- Principle of Sweeping Simplifications
- Principle of Design for Iteration
- Principle of Least Astonishment

# Principle of open design

- Get others to comment on your design
- “given enough eyeballs, all bugs are shallow” -- Linus Torvalds
- Talk through your design with outsiders



# Principle of Sweeping Simplifications

- KISS principle (Keep It Simple Stupid!)
  - Makes design and interactions easy
  - Easy to prove its safety
  - Complexity  $\neq$  Security
- 
- If it is complicated, it will be hard to reason about.
  - Layering can help with this
  - Layers only communicate with adjacent layers, possibly forming a hierarchy
  - A layer may have a specific role / capability
  - OS kernel has unrestricted memory access

# Principle of design for iteration

- Ensure you can change pieces in the future
- Priorities evolve over time
- Attackers present new threats
- Make sure you can adapt
- Abstraction and modularity play into this

# Principle of least astonishment

- Do what the user should think would happen in each situation
- A system should behave how the user expects
- This is especially important for errors!
- Handle security in an understandable way



# Example 1

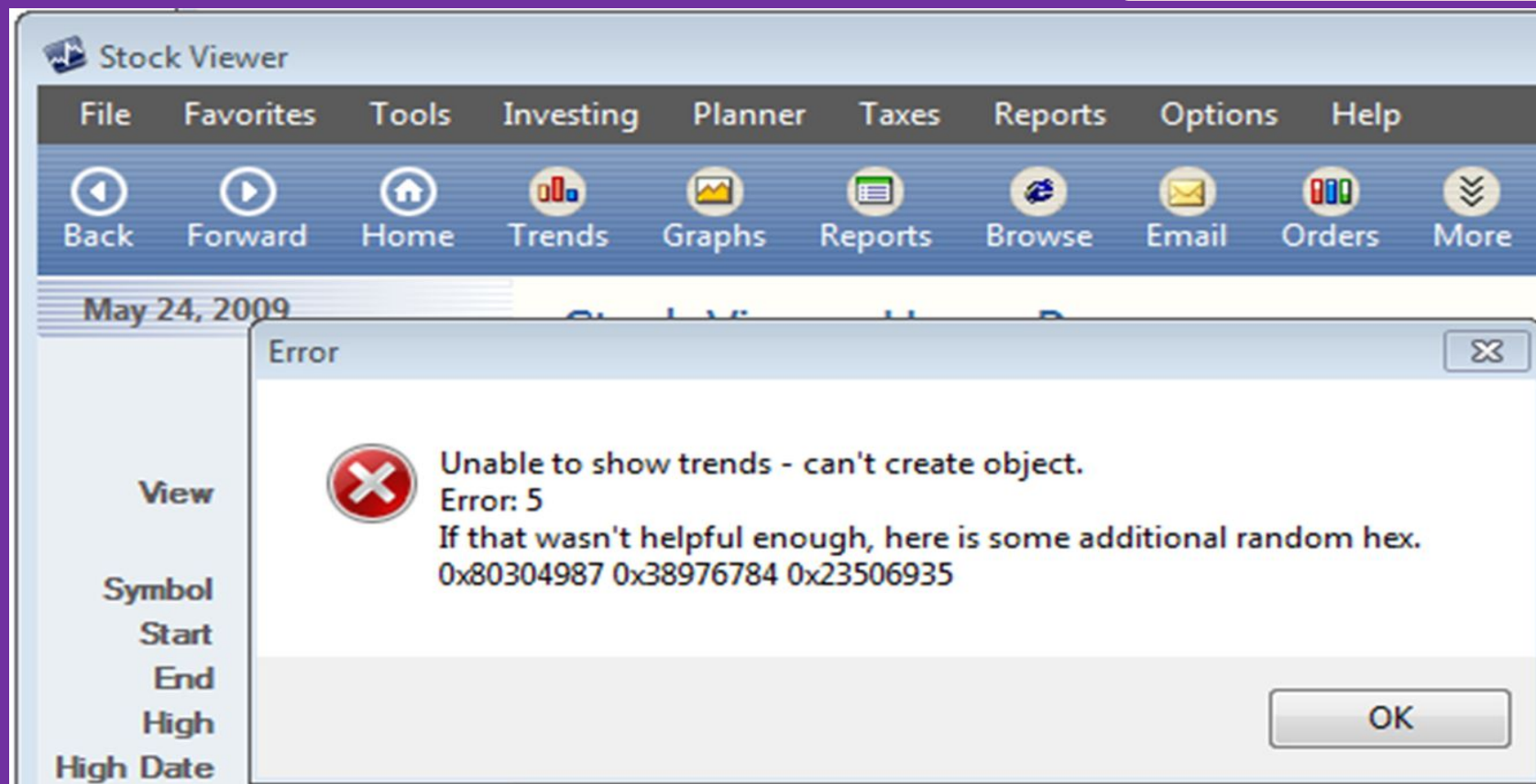
- Principle of Open Design
- Principle of Sweeping Simplifications
- Principle of Design for Iteration
- Principle of Least Astonishment

In the early days of electricity, someone would run a new wire from the electrical box to each new device. Eventually, the electrical plug / socket was invented (US version in 1904).

What principle does a plug and socket embody?

# Example 2

- Principle of Open Design
- Principle of Sweeping Simplifications
- Principle of Design for Iteration
- Principle of Least Astonishment



What principle is being ignored?



NYU

# Example 3

- Principle of Open Design
- Principle of Sweeping Simplifications
- Principle of Design for Iteration
- Principle of Least Astonishment



What principle is being followed?



# Example 4

- Principle of Open Design
- Principle of Sweeping Simplifications
- Principle of Design for Iteration
- Principle of Least Astonishment

Microsoft has begun downloading Windows 10 in the background even for users that do not request it. This results in GB of data being transferred.

<http://tech.slashdot.org/story/15/09/10/148238/microsoft-is-downloading-windows-10-without-asking>

Which principle is being violated?

## Example 5

- Principle of Open Design
- Principle of Sweeping Simplifications
- Principle of Design for Iteration
- Principle of Least Astonishment

Various cipher machines were developed and used during the two World Wars. For example, Enigma, Schlüsselzusatz, Purple, etc. It was believed that keeping secret the design of the machines will help boost the security.

Which principle is being violated?

Do you think this helped or harmed security?

# Example 6

- Principle of Open Design
- Principle of Sweeping Simplifications
- Principle of Design for Iteration
- Principle of Least Astonishment

## WTF? Microsoft now interrupting Chrome and Firefox installations to promote Edge in Windows 10



By [Wayne Williams](#)

Published 12 hours ago

[Follow @waynewill1](#)

[159 Comments](#)



Which principle is being violated?



NYU

# Principles of secure design

- Principle of minimizing secrets
- Principle of complete mediation
- Principle of fail-safe defaults
- Principle of least privilege
- Principle of simplicity (economy) of mechanism
- Principle of least common mechanism



## Principle of minimizing secrets

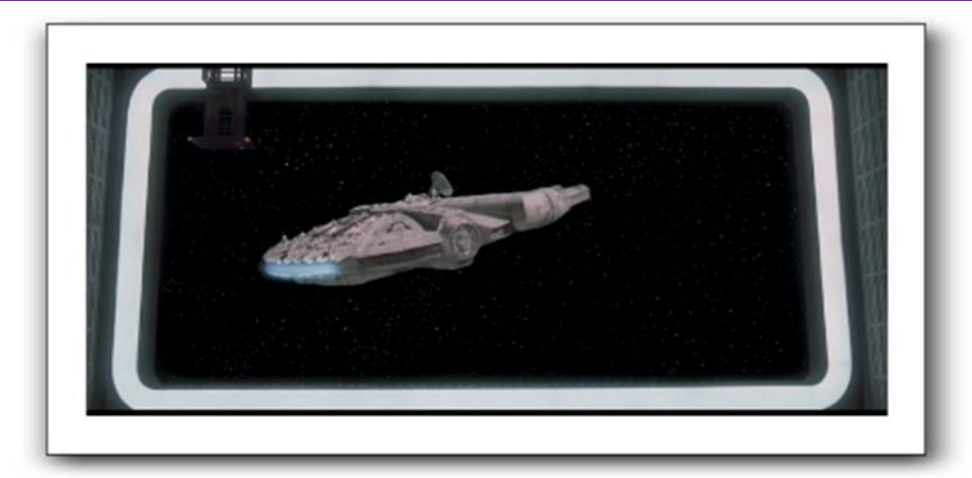
- Secrets should be few and changeable
- Do not assume that an attacker cannot see source code
- Security of a mechanism should not depend upon secrecy of its design or implementation (why not?)
- Secrecy  $\neq$  security
- “Security through obscurity”
- Cryptography and openness
- Related to principle of open design



Security of the Death Star should not have depended on the plans remaining secret!

# Principle of complete mediation

- All accesses to objects should be checked to ensure they are allowed.
- UNIX file descriptor
- DNS cache poisoning
- Check: authenticity, integrity, authorization
- No back doors!



Once the rebels returned to the Falcon, there is no access control check to leave, they simply fly away.



# Principle of fail-safe defaults

- Use sane defaults. The default should be secure.
- Default access to an object is none
- Access Control Lists (ACLs), firewall examples.
- Restricting privileges at the time of creation
- What if the attacker's goal is to cause denial-of-service?
- "Fail-closed" (as opposed to "fail-open")



OFFICER: Where are you taking this...thing?

LUKE: Prisoner transfer from Block one-one-three-eight.

OFFICER: I wasn't notified. I'll have to clear it.

HAN: Look out! He's loose!

LUKE: He's going to pull us all apart.

The officer is following fail-safe principles requiring a check rather than allowing the transfer.

# Principle of least privilege

- Temporary elevation of privilege should be relinquished immediately
- Entity should be given only the information / privileges needed to finish a task
- Granularity of privileges
- Append permission only for logging process.
- Strong privacy implications.

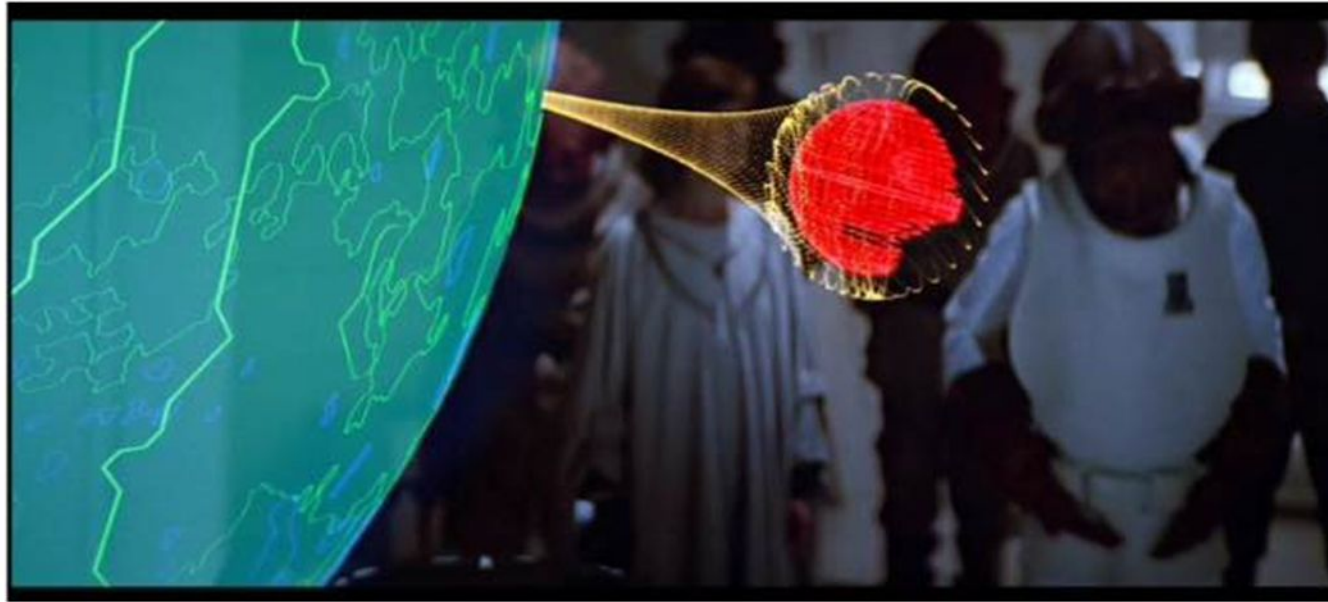


How about when on the Death Star, when R2D2 could not remotely deactivate the tractor beam over DeathNet(tm), Obi Wan had to go in person to do the job. This ultimately led to his detection by Darth Vader, and his death. Had R2D2 been able to hack the SCADA control for the tractor beam he would have lived. Unfortunately the designers of DeathNet employed the concept of least privilege, and forced Obi Wan to his demise.



# Principle of simplicity of mechanism

- Fewer errors
- Security mechanisms should be as simple as possible.
- Testing and verification is easy
- Assumptions are less
- "Minimizing the Trusted-Computing Base"
- (Also called “economy” of mechanism)



Why is the energy shield that protects the death star on the Forest Moon of Endor?  
(extra access paths and additional threats)

# Principle of least common mechanism

- Mechanisms used to access resources should not be shared
- Shared resources need resource isolation to prevent becoming a denial-of-service target
- Restrictive because it limits sharing
- Good Star Wars example?

# Example 1

- Principle of minimizing secrets
- Principle of complete mediation
- Principle of fail-safe defaults
- Principle of least privilege
- Principle of simplicity (economy) of mechanism
- Principle of least common mechanism

- Viruses cause havoc on PCs because, any program or script that is downloaded or received as email attachment, runs with the privileges of the user that runs them. Or worse the privileges of the administrator.
- What is the problem?
- What design principle is being exploited?



## Example 2

- Principle of minimizing secrets
- Principle of complete mediation
- Principle of fail-safe defaults
- Principle of least privilege
- Principle of simplicity (economy) of mechanism
- Principle of least common mechanism

- Criminals may take a check and forge portions of it to change the amount of money that is transferred.
- What design principle is being violated?
- What is this primarily failure of: authenticity, integrity, authorization

## Example 3

- Principle of minimizing secrets
- Principle of complete mediation
- Principle of fail-safe defaults
- Principle of least privilege
- Principle of simplicity (economy) of mechanism
- Principle of least common mechanism

- DVD players use encryption to prevent copying of movies.
- DRM (Digital Rights Management)
- The key listed by this flag:  
0x09F911029D74E35BD84156C5635688C0 is one such private key. If it is known, it is possible to pirate many movies.
- What principle is in play here?



## Example 4

- Principle of minimizing secrets
- Principle of complete mediation
- Principle of fail-safe defaults
- Principle of least privilege
- Principle of simplicity (economy) of mechanism
- Principle of least common mechanism

- In some versions of Python, if you use the default library to open an HTTPS connection, by default it does not check that the server certificate possesses a chain of signatures to a root-of-trust.
- What principle is being violated?

## Example 5

- Principle of minimizing secrets
- Principle of complete mediation
- Principle of fail-safe defaults
- Principle of least privilege
- Principle of simplicity (economy) of mechanism
- Principle of least common mechanism

- The TUF project protects the integrity and authenticity of software updates. TUF distributes the operation of signing software updates amongst multiple members of a project
- Given this functionality, what principle is TUF is trying to adhere to?

## Example 6

Principle of minimizing secrets  
Principle of complete mediation  
Principle of fail-safe defaults  
Principle of least privilege  
Principle of simplicity (economy) of mechanism  
Principle of least common mechanism

- The Stork package manager shares immutable copies of installed packages across OS VMs. It reduces duplicate package downloads between VMs and saves disk space, network bandwidth, and memory.
- Which of the above principles does Stork violate?



## Example 6

- Principle of minimizing secrets
- Principle of complete mediation
- Principle of fail-safe defaults
- Principle of least privilege
- Principle of simplicity (economy) of mechanism
- Principle of least common mechanism

- The Stork package manager shares immutable copies of installed packages across OS VMs. It reduces duplicate package downloads between VMs and saves disk space, network bandwidth, and memory.
- Which of the above principles does Stork violate?
- Stork violates the principles of least common mechanism and least privilege to prevent duplicate downloads. How would this impact the threat from a man-in-the-middle attacker?

## Example 7

- Principle of minimizing secrets
- Principle of complete mediation
- Principle of fail-safe defaults
- Principle of least privilege
- Principle of simplicity (economy) of mechanism
- Principle of least common mechanism

- Many people and businesses run open wireless networks. What principle is in play here?

## Example 8

- Principle of minimizing secrets
- Principle of complete mediation
- Principle of fail-safe defaults
- Principle of least privilege
- Principle of simplicity (economy) of mechanism
- Principle of least common mechanism

- A hacker found a flaw in Facebook that allowed him to post messages on user's walls that he was not friends with.

<http://www.cnn.com/2013/08/19/tech/social-media/zuckerberg-facebook-hack>

- This is due to a failure in which design principle?
- Was this primarily a failure of authentication, integrity, or authorization?

## Example 9

- Principle of minimizing secrets
- Principle of complete mediation
- Principle of fail-safe defaults
- Principle of least privilege
- Principle of simplicity (economy) of mechanism
- Principle of least common mechanism

- A recent Bluetooth bug enables attackers to take control of billions of devices. Almost any device in range that has Bluetooth enabled can be attacked.

<https://mobile.slashdot.org/story/17/09/12/2030213/blueborne-vulnerabilities-impact-over-5-billion-bluetooth-enabled-devices>

- Following which design principle may help to mitigate this?

# Example 10

- Principle of minimizing secrets
- Principle of complete mediation
- Principle of fail-safe defaults
- Principle of least privilege
- Principle of simplicity (economy) of mechanism
- Principle of least common mechanism

- Java has ~1 million lines of code in its standard libraries. All of this code is trusted in essentially the same way and may make privileged calls. This code is trusted, largely for performance reasons and to make the standard library programmers' lives easier.
- What design principles are in play?



# Example 11

- Principle of minimizing secrets
- Principle of complete mediation
- Principle of fail-safe defaults
- Principle of least privilege
- Principle of simplicity (economy) of mechanism
- Principle of least common mechanism

- Clickjacking - Google Docs page response doesn't have x-frame-options headers i.e; it can be embedded into any other webpage.
- An attacker can create a public google doc, embed it in an iframe into his webpage with allow microphone, then share the webpage with the victim and can record private conversations of the victim.

[https://medium.com/@raushanraj\\_65039/clickjacking-in-google-docs-and-voice-typing-feature-c481d00b020a](https://medium.com/@raushanraj_65039/clickjacking-in-google-docs-and-voice-typing-feature-c481d00b020a)

- Which principle is being violated ?

# Ethics

- Technology moves quickly
- Ethical issues become murky
- Is it ethical to rent a botnet to study it?

[http://www.nytimes.com/2013/07/28/magazine/bankrolling-the-botnets.html?\\_r=0](http://www.nytimes.com/2013/07/28/magazine/bankrolling-the-botnets.html?_r=0)

# Ethics (continued)

- Is it ethical to create a 'white worm' that breaks into systems to fix them?

<http://census2012.sourceforge.net/paper.html>

[http://www.schneier.com/blog/archives/2008/02/benevolent\\_worm\\_1.html](http://www.schneier.com/blog/archives/2008/02/benevolent_worm_1.html)

- A developer wrote a worm that patched 84 routines in IoT devices.
- He bricked ~2 million devices because he could not patch them.

<https://it.slashdot.org/story/17/04/21/2157251/developer-of-brickerbot-malware-claims-he-destroyed-over-two-million-devices>



# Ethics (continued)

- Is it ethical for FBI to hack Tor in order to arrest child porn suspects?

<http://rt.com/usa/fbi-suspected-hacking-child-porn-079/>

- Is it ethical for your ISP to insert ads into webpages?

<http://mobile.slashdot.org/story/14/09/08/2233235/comcast-using-javascript-injection-to-serve-ads-on-public-wi-fi-hotspots>

- Someone with “nothing to hide” gives away his passwords. He discloses private conversations w/ others.

[http://www.theatlantic.com/politics/archive/2014/08/this-man-has-nothing-to-hide/379041/?single\\_page=true](http://www.theatlantic.com/politics/archive/2014/08/this-man-has-nothing-to-hide/379041/?single_page=true)



# Legality

- Legal issues are murky
- Completely unsettled in many cases  
[http://www.youtube.com/watch?v=Qhfsg\\_ZBVRy](http://www.youtube.com/watch?v=Qhfsg_ZBVRy)  
<http://yro.slashdot.org/story/13/05/18/1417227/fed-appeals-court-says-police-need-warrant-to-search-phone>

- Discretion of (often oblivious) judge / prosecutor
- Odd rulings  
<http://yro.slashdot.org/story/12/12/20/2234257/japanese-police-charge-2channel-founder-over-forum-posts>  
<http://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email>





# Legality (continued)

- Legal 'solutions' help many problems though
- Revenge Porn
- Laws seem to be bringing down sites / punishing offenders  
[http://www.buzzfeed.com/ryanhatesthis/meet-the-women-you-call-w  
hen-your-most-intimate-photos-wind#4df6fot](http://www.buzzfeed.com/ryanhatesthis/meet-the-women-you-call-w<br/>hen-your-most-intimate-photos-wind#4df6fot)
- Swatting
- Legal penalties may help to curtail this  
[http://www.nbcnews.com/news/other/california-governor-signs-bill-cr  
ack-down-celebrity-swatting-f8C11126441](http://www.nbcnews.com/news/other/california-governor-signs-bill-cr<br/>ack-down-celebrity-swatting-f8C11126441)
- Botnet takedowns
- Trademark law brought down a botnet...  
[http://www.washingtonpost.com/blogs/wonkblog/wp/2013/07/24/ho  
w-microsoft-killed-off-a-massive-botnet-with-trademark-law/](http://www.washingtonpost.com/blogs/wonkblog/wp/2013/07/24/ho<br/>w-microsoft-killed-off-a-massive-botnet-with-trademark-law/)



# Legality (continued)

- Stingray devices allow police to intercept calls and track cellphone users
- In what circumstances should they be used?

# Legality (continued)

- Stingray devices allow police to intercept calls and track cellphone users
- In what circumstances should they be used?
- In 2011, detectives used a stingray to try to find a man who took his wife's cellphone during an argument, telling her, "If you won't talk to me, you're not going to talk to anyone," according to court records, a crime the surveillance team classified as a robbery. Police tracked the phone that day, but by then, it had already been returned to his wife, so they tracked it to her house.

<http://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/>

- Additional legal safeguards are now being added...

<http://yro.slashdot.org/story/15/09/04/031225/new-cellphone-surveillance-safeguards-imposed-on-federal-law-enforcement>




# Ethics / Legality Summary

My view:

- Be as legally unambiguous as possible
- Ask permission!
- Be willing to ethically justify to yourself / a higher power

# Passwords



**Authentication Required**

A username and password are being requested by  
<http://192.168.2.1>. The site says: "Default: admin/1234"

User Name:

Password:



# Passwords

The screenshot shows a web browser window with the Slashdot website. The browser's address bar displays the URL: <https://news.slashdot.org/story/17/09/13/1840258/equifax-has-new-data-breach-by-hackers-using-admin-as-password>. The Slashdot navigation bar includes links for Stories, Firehose, All, Popular, Polls, Deals, and a Submit button. A search bar and links for Login or Sign up are also present. Below the navigation bar, a banner promotes a deal for \$25 to add a second phone number to a smartphone using the promo code SLASHDOT25. The main article header reads "Equifax Has New Data Breach By Hackers Using 'Admin' As Password" with a source attribution to (bbc.com). The article is posted by msmash on Wednesday, September 13, 2017, at 02:50PM from the security-woes department. The article text states: "Reader [wired\\_parrot](#) writes: The credit report provider Equifax has been accused of a [fresh data security breach](#), this time affecting its Argentine operations. The breach was revealed after [security researchers discovered](#) that an online employee tool used by Equifax Argentina was accessible using the 'admin/admin' password combination." Social media sharing icons for Facebook, Twitter, LinkedIn, Google+, and Reddit are located below the article text. A "morons" button is visible on the right side of the article. At the bottom, there is a section titled "You may like to read:" with left and right navigation arrows.

Equifax Has New Data Breach

Secure | <https://news.slashdot.org/story/17/09/13/1840258/equifax-has-new-data-breach-by-hackers-using-admin-as-password>

**Slashdot** Stories Firehose > All Popular Polls Deals Submit

Topics: Devices Build Entertainment Technology Open Source Science YRO

Follow us: RSS Facebook Google+ Twitter Email

Want to read Slashdot from your mobile device? Point it at [m.slashdot.org](http://m.slashdot.org) and keep reading!

**DEAL:** For \$25 - Add A Second Phone Number To Your Smartphone for life! Use promo code **SLASHDOT25**. Check out the new SourceForge HTML5 Internet speed test!

**Equifax Has New Data Breach By Hackers Using 'Admin' As Password** (bbc.com)

Posted by msmash on Wednesday September 13, 2017 @02:50PM from the security-woes dept.

Reader [wired\\_parrot](#) writes:

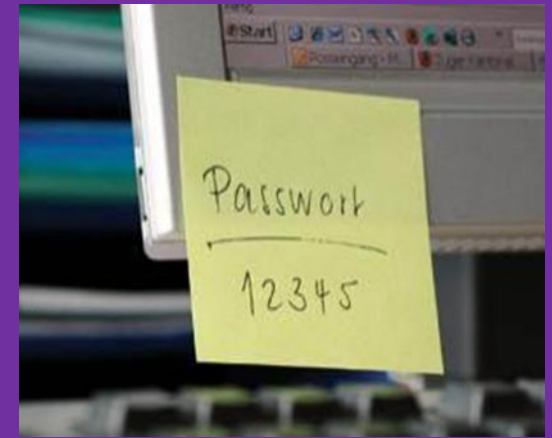
The credit report provider Equifax has been accused of a [fresh data security breach](#), this time affecting its Argentine operations. The breach was revealed after [security researchers discovered](#) that an online employee tool used by Equifax Argentina was accessible using the "admin/admin" password combination.

f t in g+ r

morons

← You may like to read: →

# Passwords



Site	#users	#pass	$\frac{\text{\#pass}}{\text{\#users}}$
hotmail	7300	6670	0.91
flirtlife	98930	43936	0.44
computerbits	1795	1656	0.92
rockyou	32603043	14344386	0.44

Rank	hotmail	#users	flirtlife	#users	computerbits	#users	rockyou	#users
1	123456	48	123456	1432	password	20	123456	290729
2	123456789	15	ficken	407	computerbits	10	12345	79076
3	111111	10	12345	365	123456	7	123456789	76789
4	12345678	9	hallo	348	dublin	6	password	59462
5	tequiero	8	123456789	258	letmein	5	iloveyou	49952
6	000000	7	schatz	230	qwerty	4	princess	33291
7	alejandro	7	12345678	223	ireland	4	1234567	21725
8	sebastian	6	daniel	185	1234567	3	rockyou	20901
9	estrella	6	1234	175	liverpool	3	12345678	20553
10	1234567	6	askim	171	munster	3	abc123	16648

# How Hard Is It To Crack Passwords?

6 lowercase characters: 308 million possible combinations

Cracking online using web app hitting a target site with one thousand guesses per second: 3.5 days.

Cracking offline using a laptop w/ GPU (one billion guesses/second): 0.28 seconds

Cracking offline, using cloud resources (one trillion guesses per second): 0.0000224 seconds

8 characters (letters, numbers, symbols, etc.): ~10 quadrillion possible combinations

Cracking online using web app hitting a target site with one thousand guesses per second: 317K years.

Cracking offline using a desktop w/ GPU (one billion guesses/second): 107 days

Cracking offline, using cloud resources (one trillion guesses per second): 2.58 hours


# Do compromises happen?

**USA TODAY** NEWS SPORTS LIFE MONEY TECH TRAVEL OPINION 55° INVESTIGATIONS SUBSCRIBE MORE

## Kanye, 000000 for your iPhone credentials is a really bad idea -- even without the cameras




Jefferson Graham, USA TODAY Published 6:15 p.m. ET Oct. 11, 2018 | Updated 9:20 a.m. ET Oct. 12, 2018

f t e m



During his White House Oval Office visit, Kanye West told President Donald Trump that his friends tried to scare him out of wearing his Make America Great Again hat. USA TODAY

### MOST POPULAR

-  Google Pixel 3: What we know about Google's next phones from all the rumors and leaks
-  Kanye, 000000 for your iPhone credentials is a really bad idea -- even without the cameras
-  All the useful, wacky and downright weird tech I saw on my recent trip to Japan

# Compromises Expose Passwords!

Companies with password breaches:

Hotmail, LastFM, Drupal, Formspring,  
ScribD, the New York Times, NVidia,  
Evernote, Billabong, Gawker, LinkedIn,  
Linode, ABC, Yahoo!, Ubuntu, eHarmony,  
LivingSocial, Nintendo, Ubisoft, Microsoft, ...

Yahoo: 600M accounts leaked!

# Passwords Get Re-used (bad!!!)

20 percent of compromised credentials, exposed via hacks other service providers, match Microsoft Account logins due to password reuse... The lists are circulated by organizations and hackers in the wake of attacks on third-party service providers."

<http://www.zdnet.com/one-in-five-hacked-logins-match-microsoft-accounts-7000000969/>





# Compromises Expose Passwords!

The screenshot shows a web browser displaying an article on the ComputerWorld website. The browser's address bar shows the URL: [www.computerworld.com/s/article/9227869/Hackers\\_crack\\_more\\_than\\_60\\_of\\_breached\\_LinkedIn\\_passwords](http://www.computerworld.com/s/article/9227869/Hackers_crack_more_than_60_of_breached_LinkedIn_passwords). The page features a yellow header with the 'COMPUTERWORLD' logo and navigation links for White Papers, Webcasts, Newsletters, Solution Centers, Events, Magazine, and social media icons. A search bar is also present. Below the header, a navigation menu includes 'Topics', 'News', 'In Depth', 'Reviews', 'Blogs', 'Opinion', 'Shark Tank', 'IT Jobs', 'More', and 'IT Verticals'. The 'Security' section is expanded, showing sub-topics like Application Security, Cybercrime and Hacking, Cyberwarfare, Data Security, Encryption, and Endpoint Security. The article itself is titled 'Hackers crack more than 60% of breached LinkedIn passwords' and is written by Jaikumar Vijayan. It discusses the speed of hackers in cracking passwords and the weakness of the security scheme used by LinkedIn. The article includes a byline, a date (June 7, 2012), and a comment count (45 Comments). Social media sharing buttons for LinkedIn, Twitter, Google+, and Facebook are visible. The article text states: 'More than 60% of the unique hashed passwords that were accessed by hackers from a LinkedIn password database and posted online this week have already been cracked, according to security firm Sophos.' and 'It's very likely the remaining passwords have also been cracked, said security researcher Chester Wisniewski late Wednesday.' On the right side of the page, there is a 'Top Stories' section with four items: 'Facebook and Twitter images show support for Boston following marathon explosions', 'CA Technologies buys Layer 7 for API smarts', 'Enterprise social software vendor Moxie goes freemium', and 'AV-TEST stands by Bing malware-link claim'. Below this is a 'Latest from CITE WORLD' section with three items: 'In today's workplace culture wars, IT and HR need to be on the same team', 'Return of the Start button may not be what you think', and 'Proof that all those Samsung ads are working'.

COMPUTERWORLD

White Papers Webcasts Newsletters Solution Centers Events Magazine

Google Custom Search

Topics News In Depth Reviews Blogs Opinion Shark Tank IT Jobs More IT Verticals

Security Application Security Cybercrime and Hacking Cyberwarfare Data Security Encryption Endpoint Security Malware and Vulnerabilities Mobile Security Privacy

Home > Security > Cybercrime and Hacking

News

## Hackers crack more than 60% of breached LinkedIn passwords

Speed of hackers to crack passwords shows weakness of security scheme used by LinkedIn, researchers say

By Jaikumar Vijayan  
June 7, 2012 10:45 AM ET 45 Comments

Share 0 Twitter +1 LinkedIn Like 468 More

More than 60% of the unique hashed passwords that were [accessed by hackers](#) from a LinkedIn password database and posted online this week have already been cracked, according to security firm Sophos.

It's very likely the remaining passwords have also been cracked, said security researcher Chester Wisniewski late Wednesday.

**Top Stories**

- Facebook and Twitter images show support for Boston following marathon explosions
- CA Technologies buys Layer 7 for API smarts
- Enterprise social software vendor Moxie goes freemium
- AV-TEST stands by Bing malware-link claim

**Latest from CITE WORLD**  
BY IDG ENTERPRISE

In today's workplace culture wars, IT and HR need to be on the same team

Return of the Start button may not be what you think

Proof that all those Samsung ads are working

## Readings for next week:

- Interesting article to read (think about ethics / legality)  
<https://www.infoworld.com/article/2203373/true-tales-of-mostly-white-hat-hacking-2.html>
- How changing requirements can drive odd designs  
<http://www.youtube.com/watch?v=aXQ2lO3ieBA>
- Optional video on lock picking  
<https://www.youtube.com/watch?v=ChbyaXBKNY8>