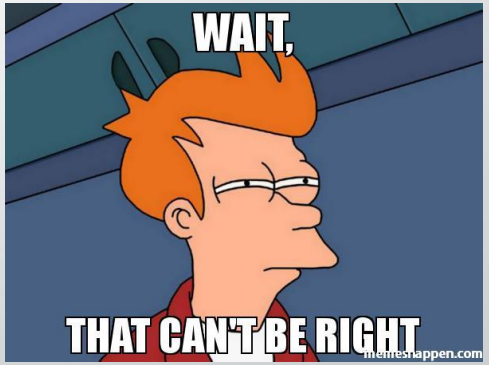
10 Digital Privacy Controls

Greg Sternberg
March 5, 2020

Things You Won't Find In My Bio

- Can't make my mind up about a career – Geo-Physicist, Chemical Engineer, Hacker, Red/Blue/Purple/Mauve teamer, Programmer, Lead, Manager, Architect, CISO, Teacher, Privacy Advocate, …
- Like to say "Just one more thing" in architecture/security reviews and open doors that say "Do Not Open" and push buttons that say "Do Not Push"

- Have gotten 'the look' from significant others when asked, "What are you thinking about?" and I reply "Wondering how one might rob this movie theater."



OWASP Top 10 Lists

- OWASP Top 10 Proactive Controls for 2018
  - C1: Define Security Requirements
  - C2: Leverage Security Frameworks and Libraries
  - C3: Secure Database Access
  - C4: Encode and Escape Data
  - C5: Validate All Inputs
  - C6: Implement Digital Identity
  - C7: Enforce Access Controls
  - C8: Protect Data Everywhere
  - C9: Implement Security Logging and Monitoring
  - C10: Handle All Errors and Exceptions
- OWASP Top 10 Privacy Risks for 2014
  - P1: Web Application Vulnerabilities
  - P2: Operator-sided Data Leakage
  - P3: Insufficient Data Breach Response
  - P4: Insufficient Deletion of personal data
  - P5: Non-transparent Policies, Terms and Conditions
  - P6: Collection of data not required for the primary purpose
  - P7: Sharing of data with third party
  - P8: Outdated personal data
  - P9: Missing or Insufficient Session Expiration
  - P10: Insecure Data Transfer

(My) Top 10 Proactive Privacy Controls

- PC1: Define Privacy Requirements
- PC2: Secure Data
- PC3: Safeguard Data Quality
- PC4: Enforce Access Controls
- PC5: Give User Control Of Their Data
- PC6: Transparency Over Confusion
- PC7: Avoid PII Transitivity
- PC8: Practice Data Minimization
- PC9: Implement Logging and Monitoring
- PC10: Handle All Errors and Exceptions

PC2: Secure Data

```
FUNCT=() { ignore; }; echo shellshock
...
echo shellshock
```

```
<?php
print("Please specify the name of the file to delete");
print("<p>");
$file=$_GET['filename'];
system("rm $file");
?>
```

```
sql = "SELECT * FROM customers WHERE address ='" + sys.argv[1] + "'"
mycursor.execute(sql)
myresult = mycursor.fetchall()
```

- Without security there is no privacy
- Without privacy security is meaningless

```
UserId,BillToDate,ProjectName,Description,DurationMinutes
1,2017-07-25,Test Project,Flipped the jibbet,60
2,2017-07-25,Important Client,"Bop, dop, and giglip", 240
2,2017-07-25,Important Client,"=2+5+cmd|' /C calc'!A0", 240
```

```
int main(char* argc, char** argv) {
        char cmd[CMD_MAX] = "/usr/bin/cat ";
        strcat(cmd, argv[1]);
        system(cmd);
}
```

PC3: Safeguard the Quality of Personal Data

- "Quality is everyone's responsibility." - W. Edwards Deming
- "Quality is never an accident. It is always the result of intelligent effort." - John Ruskin

PC4: Enforce Access Controls

- Choose ‘No’ over ‘Yes’

PC5: Give User Control Of Their Data

- "User knows best"
- "It's my data and I'll say no if I want to"

PC6: Transparency Over Confusion

- Confusion is to privacy as obfuscation is to security
- "By placing an order via this web site on the first day of the fourth month of the year 2010 Anno Domini, you agree to **grant Us a non transferable option to claim, for now and for ever more, your immortal soul**. Should We wish to exercise this option, you agree to surrender your immortal soul, and any claim you may have on it, within 5 (five) working days of receiving written notification from gamesation.co.uk or one of its duly authorised minions. We reserve the right to serve such notice in 6 (six) foot high letters of fire, however we can accept no liability for any loss or damage caused by such an act. If you a) do not believe you have an immortal soul, b) have already given it to another party, or c) do not wish to grant Us such a license, please click the link below to nullify this sub-clause and proceed with your transaction."


I'm bored
I'm ready
Oooo!
Squirrel!

Only The 'Big Boys' Need To Worry About Privacy

- Size does *not* matter

PC7: Avoid PII Transitivity

Transitive:

If b=a and b=c

then a = c

PC8: Practice Data Minimization/ Avoidance

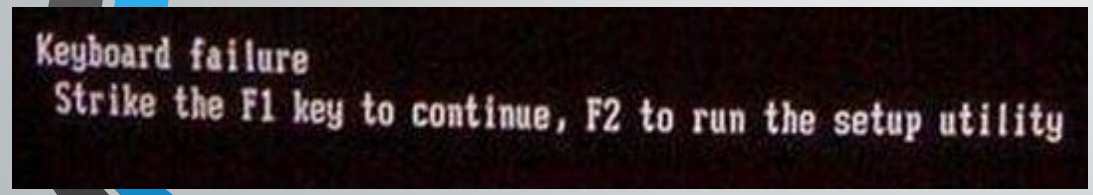
- Just cuze you can doesn't mean you should

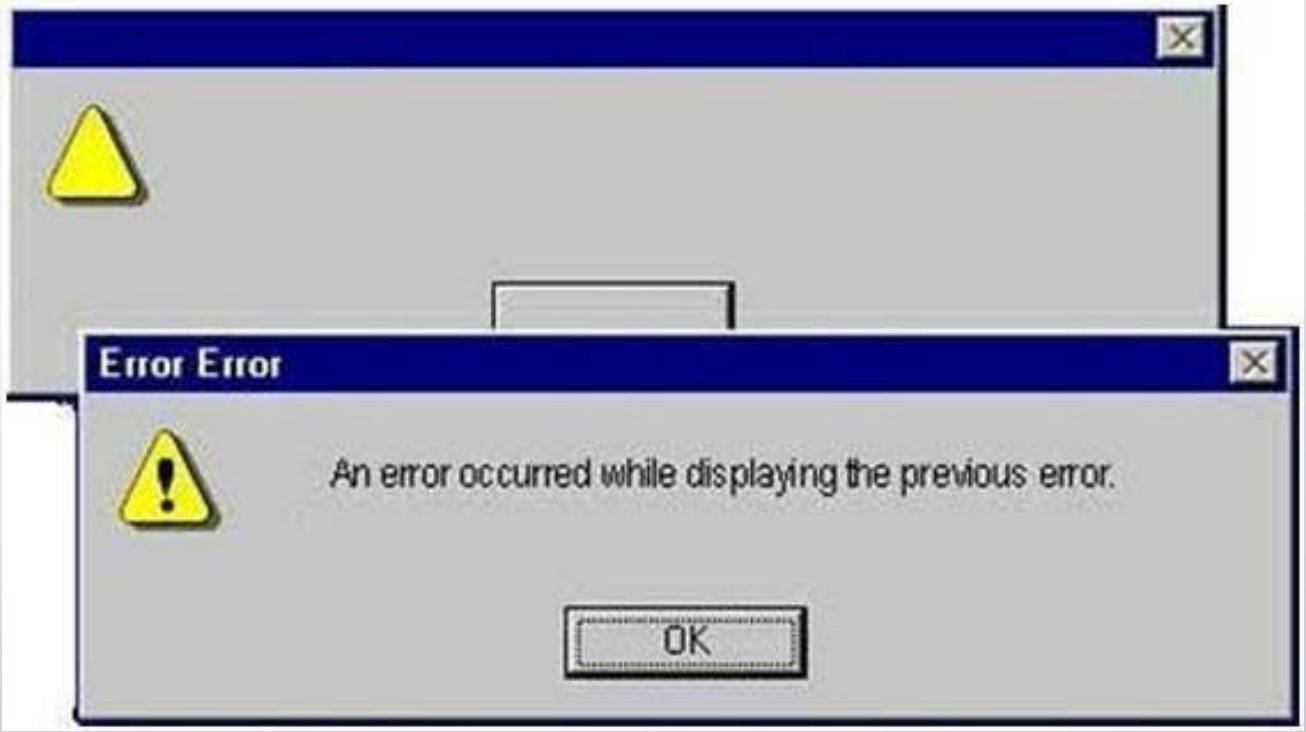
PC9: Implement Logging and Monitoring

- If you don't know they are there you can't kick them out

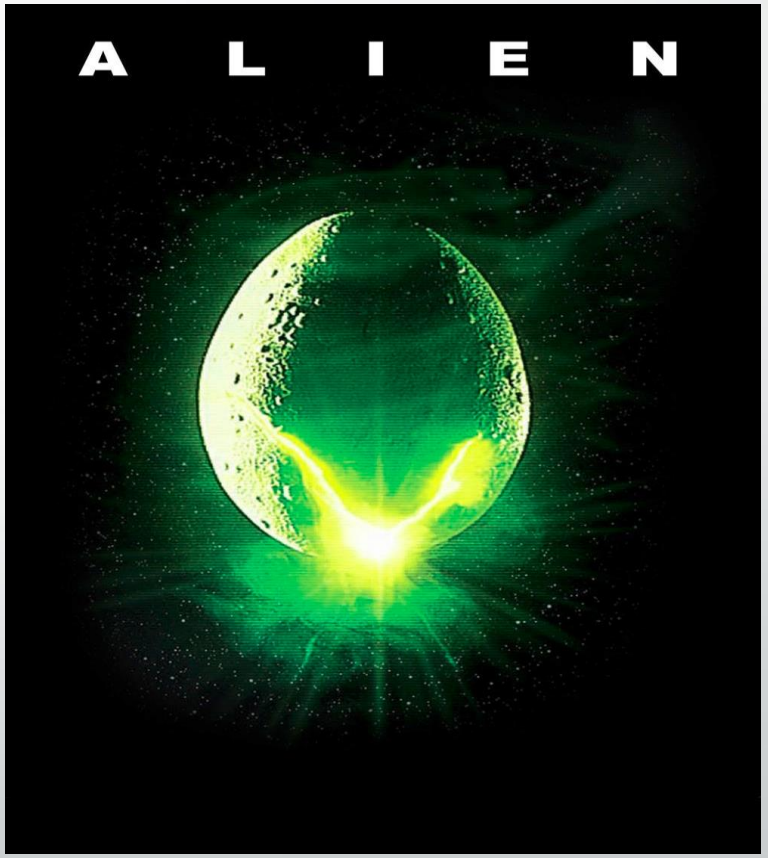
PC10: Handle All Errors and Exceptions

- "It's not for us to decide if/when but what to do when it happens"





Yes, Privacy* is Emergent…



* security, architecture, DR, [insert nonfunctional]

PC1: Define Privacy Requirements

- "Only you can prevent privacy fires"


SHINY THINGS

First Amendment

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances

- “Clearview AI says the First Amendment lets it scrape the internet”: https://www.cnet.com/news/clearview-says-first-amendment-lets-it-scrape-the-internet-lawyers-disagree/
- “Big Telecon Say It Has First Amendment Right to Sell Your Private Data”: https://www.vice.com/en_us/article/qjdza5/big-telecom-say-it-has-first-amendment-right-to-sell-your-private-data


Questions
?
?
Answers
?

Supporting Slides

References (1/4)

- OWASP Secure Coding Practices and Quick Reference - https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf
- OWASP Top 10 Privacy Risks - https://owasp.org/www-project-top-10-privacy-risks/
- International Association of Privacy Professionals (IAPP) - https://iapp.org/about/
- Electronic Privacy Information Center (EPCI) - https://epic.org/
- Privacy Program from NIST - https://www.nist.gov/privacy
- “Websites Can Probably Guess Your Identity With Three Basic Data Points” - https://observer.com/2015/09/http-injection-browser-fingerprinting-w3c-access-mark-nottingham/
- “*k*-Anonymity: A Model for Protecting Privacy,” *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems* 10, no. 5 (2002): 557–570.
- “How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did” - https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/
- Cookiebot (GDPR, ePrivacy and CCPA compliant cookies) - https://www.cookiebot.com/en/

References (2/4)

- “U.S. soldiers are revealing sensitive and dangerous information by jogging” - https://www.chicagotribune.com/nation-world/ct-soldiers-sensitive-information-fitbits-20180128-story.html
- “Fitness tracking app Strava gives away location of secret US army bases” - https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases
- “Reports raise video privacy concerns for Amazon-owned Ring” - https://techcrunch.com/2019/01/10/amazon-ring-privacy-concerns/
- Privacy pattern - https://www.privacypatterns.org/. In its infancy but promising
- Must have a warrant to get cellphone tower data - https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf
- darkpatterns.org – the scary things websites do to influence you
- The Privacy Project. An effort by the NY times to explore technology and privacy - https://www.nytimes.com/series/new-york-times-privacy-project

References (3/4)

- Colorado Digital ID - https://www.colorado.gov/pacific/dmv/mycolorado-and-colorado-digital-id
- Privacy Enhancing Technologies: https://www.privacyswan.com/blog/why-pets-are-so-important
- “Google keeps a scary amount of data on you. Here’s how to find and delete it”: https://www.cnet.com/how-to/google-keeps-a-scary-amount-of-data-on-you-heres-how-to-find-and-delete-it/
- “The Secretive Company That Might End Privacy as We Know It”: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html
- “Protecting privacy in an AI-driven world”: https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/
- “Unity Technologies Reaches Settlement of Children’s Privacy Lawsuit”: https://www.mediapost.com/publications/article/346866/unity-technologies-reaches-settlement-of-children.html
- “The 10 Generally Accepted Privacy Principles”: https://linfordco.com/blog/the-10-generally-accepted-privacy-principles/

References (4/4)

- “NIST Privacy Framework”: https://www.nist.gov/privacy-framework
- “Privacy By Design”: https://en.wikipedia.org/wiki/Privacy_by_design
- “Privacy By Design Cheat sheet”: https://www.varonis.com/blog/privacy-design-cheat-sheet/

Programmer (Privacy) Ethics

- From the Code of Ethics and Professional Conduct from the Association for Computing Machinery:
  - **Respect the privacy of others.** Computer systems are wrongly used by some people to violate the privacy of others. Software developers should write programs that can protect users' private information and that can avoid other undesired people to have unauthorized access to it (Code of Ethics and Professional Conduct).
- Modified Hippocratic Oath:
  - I will use programming to help according to my ability and judgment, but never with a view to injury and wrong-doing. Neither will I create software with the intent to harm when asked to do so, nor will I suggest such a course. But I will keep pure and holy both my life and my art.
  - Into whatsoever establishment I enter, I will enter to help my customers, and I will abstain from all intentional wrong-doing and harm, especially from abusing man or woman. And whatsoever I shall see or hear in the course of my profession, as well as outside my profession in my interactions with people, if it be what should not be published abroad, I will never divulge, holding such things to be involatile secrets.

Privacy Principles

- Do no harm (to the user)
- Data must have a neutral owner who is responsible for ensuring there are no adverse or unfair usages to the individuals the data relates to
- Notice and clear rational must be given if data is used, collected, or aggregated
- Individuals must have complete rights to and control over all data that pertains to them
- Choose no data over data aggregation and over data storage
- For data to be private there must be security
- Opt-in must not be all or nothing
- Not opting in must not mean striking out
- Data must have a life cycle
- There must be a legitimate purpose to gather the data and explicit boundaries and limits on the usage of that data

"If You Have Something You Don't Want Anyone To Know, Maybe You Shouldn't Be Doing It"

- Why the "Nothing to Hide" argument is deeply flawed:
  - Privacy is about protecting and having control over your information
  - Fundamental right
  - Not protecting your privacy gives *everyone* carte blanche to you

OWASP Top 10 Privacy Risks for 2019 (under consideration)

- Collection of data not required for the user-consented purpose
- Data Aggregation and Profiling
- Insufficient Data Quality
- Inability of users to access and modify data
- Problems with getting Consent
- Misleading Content
- Non-transparent Policies, Agreements, Terms and Conditions
- Inappropriate Policies, Terms and Conditions
- Form field design issues
- Secondary use
- Operator-sided Data Leakage
- Collection without consent
- Transfer or processing through 3rd party
- Sharing of data with 3rd party
- Insufficient deletion of personal data
- Web Application Vulnerabilities
- Insufficient Data Breach Response
- Insecure data transfer
- Missing or Insufficient Session Expiration
- Consent on Everything *NEW*
- Insufficient data structure model to handle user rights
- Changes in legislation [local / Global] or legal requirements that affect Data Subject rights