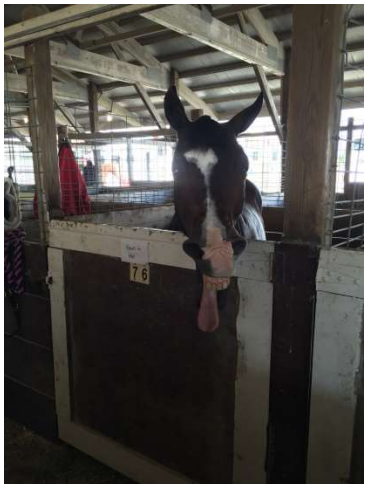

Personal and Application Security
Scott Goodwin

About me

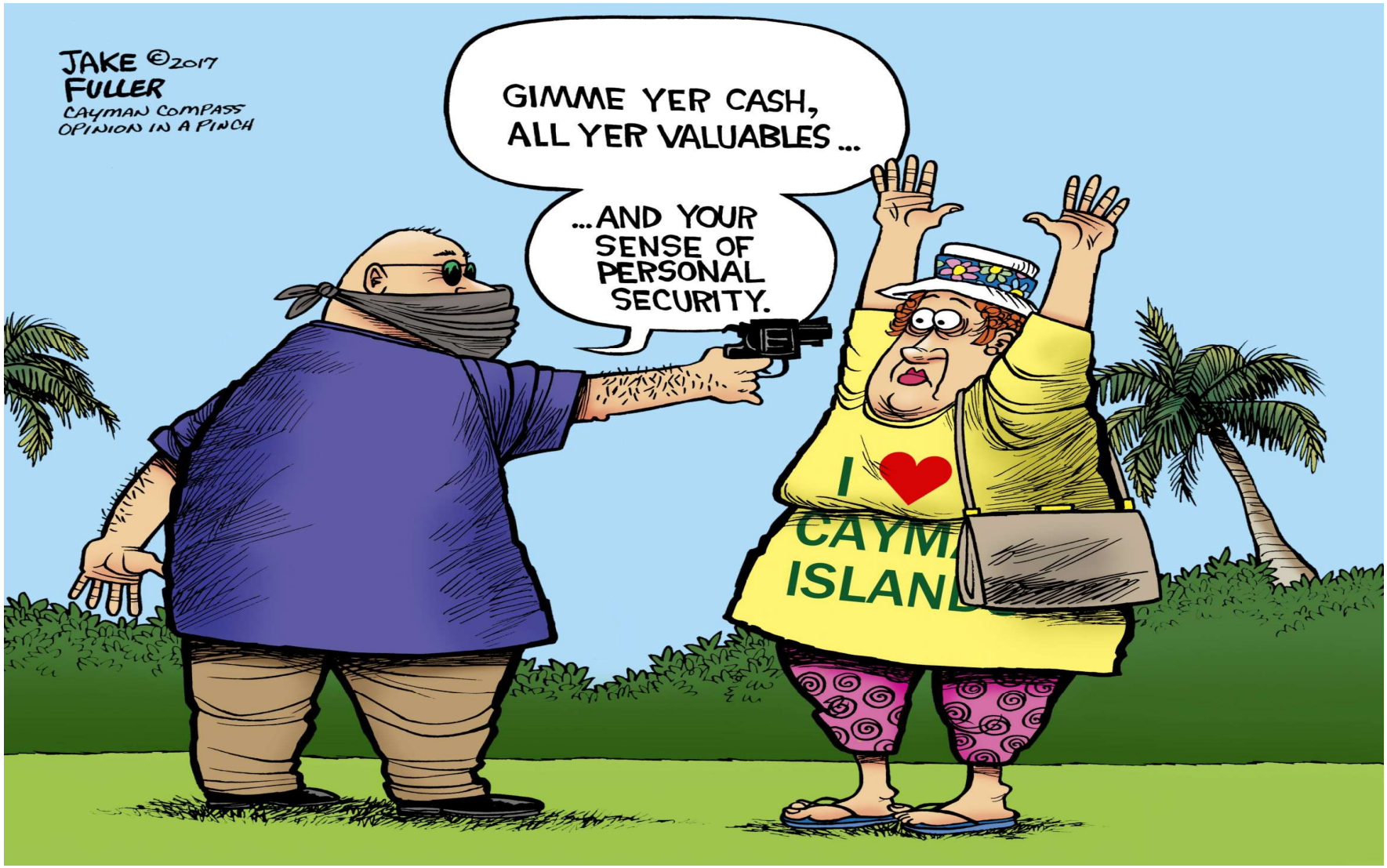
- Bachelor of Electrical Engineering
- Master of Science in Accounting
- CISSP, CEH, CDPSE



Agenda

- Passwords
- Click here or not
- Currency
- Application Development
- OWASP
- Helpful Links
- Get involved
- Give back

Personal Security



Passwords

- What you know
- What you are
- What you have
- Combined with user IDs

Passwords

- Longer is better
  - Each character increases the complexity exponentially. This is why passwords typically have a minimum requirement of 8 characters
    - 26 lower case letters
    - 26 upper case letters
    - 10 digits
    - ~30 special characters
    - 92 options per character
- Password keepers

The Math Behind Long Passwords

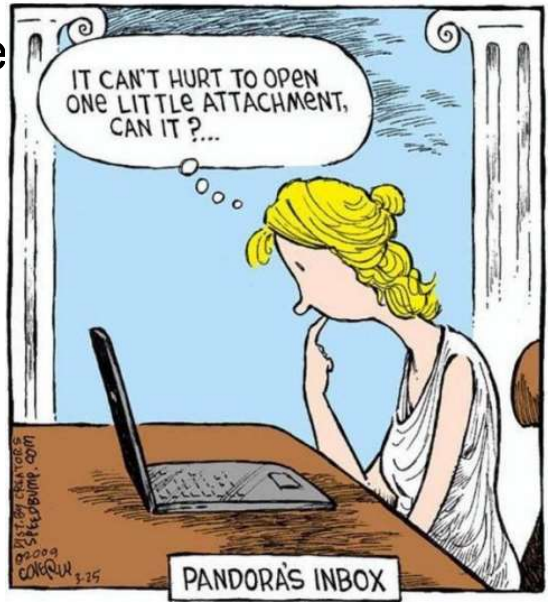
- Modern GPUs can guess about 700 million passwords per second
- Number of possible characters to the power of the password length
  - 8 character single case password = 26^8 =
    - 208.8 billion possible passwords
    - ~ 5 minutes to try every combination
  - 8 character using all combinations = 92^8 =
    - 5,132 trillion possible passwords
    - ~ 85 days to try every combination
    - Increase to 12 characters, ~16.5 million years to try every combination

Multi-Factor Authentication

- Additional code from token, application, text, email
- Use whenever possible
- Can allow for shorter passwords

Click here or not

- Ransomware
  - Ransomware is a type of malware that can be covertly installed on a computer without the user's knowledge or intention.
  - It restricts access to the infected computer system in some way and demands that the user pay a "ransom" to the malware operators to remove the restriction.
- Malware
  - Malware is software designed to infiltrate or damage a computer system without the owner's informed consent.
  - Malware should not be confused with defective software, that is, software which has a legitimate purpose but contains bugs.



Click here or not

- Know what you are clicking
  - Avoid clicking on links or opening attachments and emails from people you don't know or companies with whom you don't do business
- Redirects
  - Bitly, Rebrandly,
  - TinyURL, BL.INK,
  - Shorby, Short.io,
  - Sniply

What Should I Do?

Scott Your Setup Has Reached Completion, Next Step Inside Inbox ×

Support Program grnt@grantadvisorusa.com via c.kajabimail.net
to me

View in Web Browser

Hey there Scott,

Support programs are available to help millions of Americans today, and you may be qualified for one of the grant programs.

Once considered eligible, you may receive up to $6,495* every year that can be used for your daily expenses, educational needs, or even career advancement.

You may discover your qualification through the page below without any charge at all.

Go Through the Application Process

Many people have already qualified, and it's time to find out your own eligibility.

All the best,
Mae

*https://studentaid.gov/understand-aid/types/grants/pell

https://studentaid.gov/understand-aid/types/grants/pell

Personal Currency

- Who doesn't love new stuff
  - Make sure your software is up-to-date
    - *Reboot your system on a regular basis (i.e., weekly) to install patches*
- Software
- OS
- Virus scanners

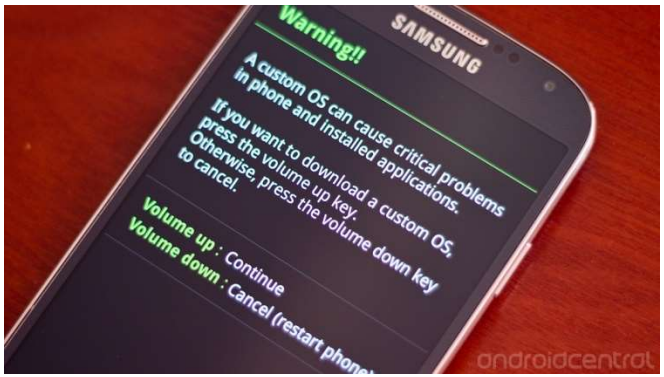
CISA
CYBER+INFRASTRUCTURE

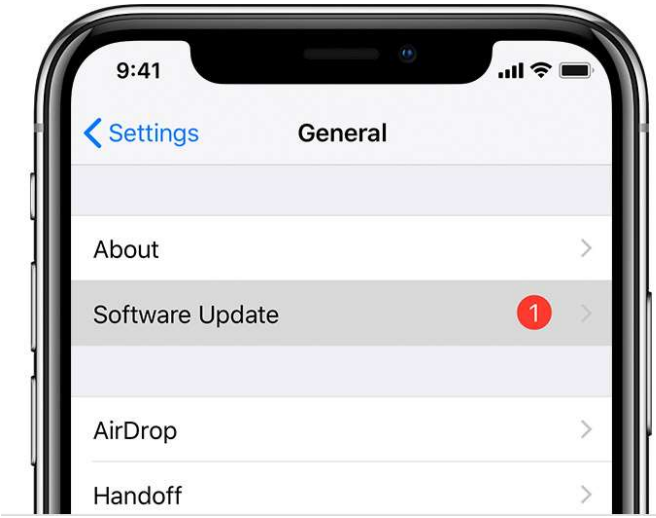
Application Security

Application Development

- Currency
  - Same as with personal security
  - Keep current
- Libraries
  - Open source libraries
  - Get from a reputable site

Software Update





OWASP

- What is it
  - Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit organization focused on improving the security of software
- Top 10
  - Updated this year
- Code Review Top 9

OWASP Top 10

- A1-Broken Access Control
- A2-Cryptographic Failures
- A3-Injection
- A4-Insecure Design
- A5-Security Misconfiguration
- A6-Vulnerable and Outdated Components
- A7-Identification and Authentication Failures
- A8-Software and Data Integrity Failures
- A9-Security Logging and Monitoring Failures
- A10-Server-Side Request Forgery

OWASP Code Review Top 9

The Nine Source Code Flaw Categories

- **Input validation**
  - Cross-site scripting
  - SQL injection
  - XPATH injection
  - LDAP injection
  - Cross-site request forgery
  - Buffer overflow
  - Format bug
- **Source code design**
  - Insecure field scope
  - Insecure method scope
  - Insecure class modifiers
  - Unused external references
  - Redundant code
- **Information leakage and improper error handling**
  - Unhandled exception
  - Routine return value usage
  - NULL pointer dereference
  - Insecure logging

OWASP Code Review Top 9

The Nine Source Code Flaw Categories

- **Direct object reference**
  - Direct reference to database data
  - Direct reference to file system
  - Direct reference to memory
- **Resource usage**
  - File system objects
  - Memory
  - CPU
  - Network bandwidth
- **API usage**
  - Insecure database calls
  - Insecure random number creation
  - Improper memory management calls
  - Insecure HTTP session handling
  - Insecure strings manipulation

OWASP Code Review Top 9

The Nine Source Code Flaw Categories

- **Best practices violation**
  - Insecure memory pointer usage
  - NULL pointer dereference
  - Pointer arithmetic
  - Variable aliasing
  - Unsafe variable initialization
  - Missing comments and source code documentation
- **Weak Session Management**
  - Not invalidating session upon an error occurring
  - Not checking for valid sessions upon HTTP request
  - Not issuing a new session upon successful authentication
  - Passing cookies over non SSL connections (no secure flag)
- **Using HTTP GET query strings**
  - Passing sensitive data over URL /query string

- https://www.bsidescharleston.org/
- https://cybermap.kaspersky.com/
- https://threatmap.checkpoint.com/
- https://hackaday.com/
- https://www.ethicalhacker.net/
- https://www.bt3.no/
- https://attack.mitre.org/
- https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material
- https://jeremylong.github.io/DependencyCheck/dependency-check-gradle/index.html
- https://www.abuseipdb.com/
- https://seedsecuritylabs.org/
- https://threatpost.com/
- https://qifi.org/
- https://www.ultimatewindowssecurity.com/
- https://www.sans.org/security-resources/
- https://mvnrepository.com/
- https://securecodewarrior.com/
- https://www.cisa.gov/about-cisa
- https://www.kali.org/
- https://www.abuseipdb.com/
- https://www/blackhillsinfosec.com/
- https://informationisbeautiful.net/
- https://github.com/jivoi/awesome-osint

- https://www.humblebundle.com/
- https://www.holidayhackchallenge.com/

- Hacking Humans
- SecurityNow
- Recorded Future – Inside Security Intelligence
- Cyberwire daily
- Defensive Security
- Hackable
- DevSecOps
- Darknet Diaries
- MaliciousLife
- SANS Internet StormCenter Daily (Daily StormCast)
- OWASP PodCast
- The Great Security Debate
- The Jordan Harbinger Show

Get Involved

- Taking the first step
- Participate in cons
  - Bsides
  - Thotcon
  - Defcon
  - Wild West Hackin Fest
- Capture the flag events
- OWASP

Give Back

- Volunteer
- Speak
- Share with friends, family, co-workers

Some Favorite Phrases

- If you cannot determine the product then you are the product.
- It is not paranoia when they really are out to get you.
- If it sounds too good to be true, it is.
- You cannot use beef stew for your password because it is not stroganoff.