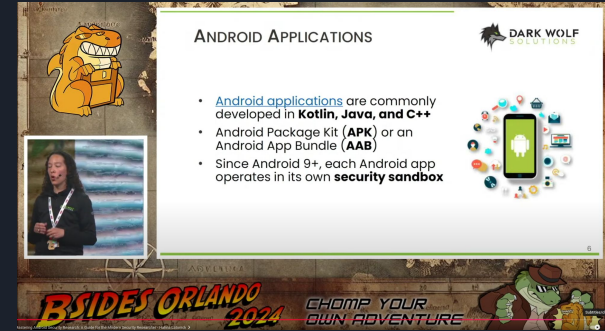# Level 0x05

SCM

Topics

- Cyberquest
- Hacking History
- SCM
- Git demo

Events

- **Videos from B-Sides Orlando**
  - [Cyberwarefare in Finland](#)
  - [AI Generated Disinformation](#)
  - [Beginning Android Security Research](#)
- [Maker Faire Orlando](#)
  - Nov 9 and 10 (this weekend)
  - Central Florida Fairgrounds
  - $15 - $20 per person
  - 3d-printing, robotics, makers / crafters, cosplay

More Video Game Hacking

- [Reverse engineering of Dreamcast Ecco the Dolphin](#)

```
1. Go to the VMU Menu > New game > Enter your initials screen.
2. Enter one of these sequences, making sure not to end after 3 letters.

GYUGYU+XXX : Unlock all levels
SOCCER+XXX : Unlock bonus stage*
EXBBERX+XXX: Immortality mode*
QQRIQ+XXX  : Show FPS*
XYZZYX+XXX : Show time*
POPELY+XXX : Nothing?
```

Joel Reymont

- Drone Hacker from Spain working in Ukraine
- [Twitter/X thread](#)
  - Drones lose signal and GPS on front-line
  - How can we get expensive surveillance drone back home?
  - Advanced GPS radio receiver
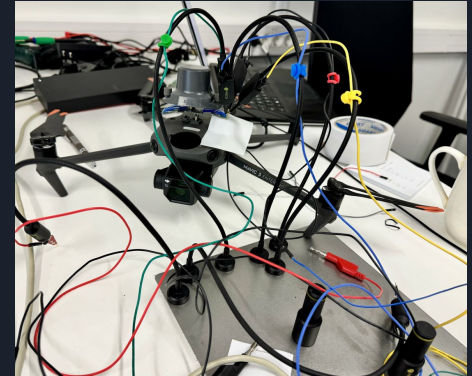
Software Configuration Management (SCM)

How we manage changes and releases of software artifacts during software development

1. Identifying Configuration Items: source code, documents
2. Version Control: keep a history of different versions
3. Build Management: compilers and building tools (make, cmake)
4. Change Management: multiple users, merging, code reviews
5. Release Management: release packages

Tapes, Floppys, Zips

- Stored our programs on tape / floppy disks
- Shared by walking to our friends house (sneakernet)
- Floppy Disks
  - 8-inch: 250 KB
  - 5 ¼ inch: 360 KB - 1.2 MB
  - 3 ½ inch: 1.44 MB
- File Containers
  - Tape Archive (tar). Unix 1979, Windows 2018
    - No compression
  - Lempel-Ziv algorithms: LZ77/LZ78 -> LZMA (7zip)
    - Many patent issues / lawsuits
  - PKWare's PK Zip. DOS 1989
  - DEFLATE: 1993 Zip2.0 and GZip

Diff

```
mwales@Metroid:~/scratch/patch_test$ cat hw.c
#include <stdio.h>

int main(int argc, char** argv)
{
        printf("Hello World\n");
        return 0;
}
```

```
mwales@Metroid:~/scratch/patch_test$ cat hw_rev2.c
#include <stdio.h>

int main(int argc, char** argv)
{
        printf("Hello World\n");
        printf("Goodbye Cruel World\n");
        return 0;
}
```

`diff` creates a little snippet of the code change between 2 versions of a file

Can email the diff to maintainer

```
mwales@Metroid:~/scratch/patch_test$ diff -u hw.c hw_rev2.c
--- hw.c         2024-04-25 01:19:40.909594695 -0400
+++ hw_rev2.c    2024-04-25 01:20:15.006166220 -0400
@@ -3,6 +3,7 @@
 int main(int argc, char** argv)
 {
        printf("Hello World\n");
+       printf("Goodbye Cruel World\n");
        return 0;
 }
```

Patch

- Apply diff / patch file to update your copy of the code
- "Patch" word comes from "patching" punched holes in paper tape programs

```
mwales@Metroid:~/scratch/patch_test$ diff -u hw.c hw_rev2.c > patch.txt
mwales@Metroid:~/scratch/patch_test$ patch hw.c patch.txt
patching file hw.c
```
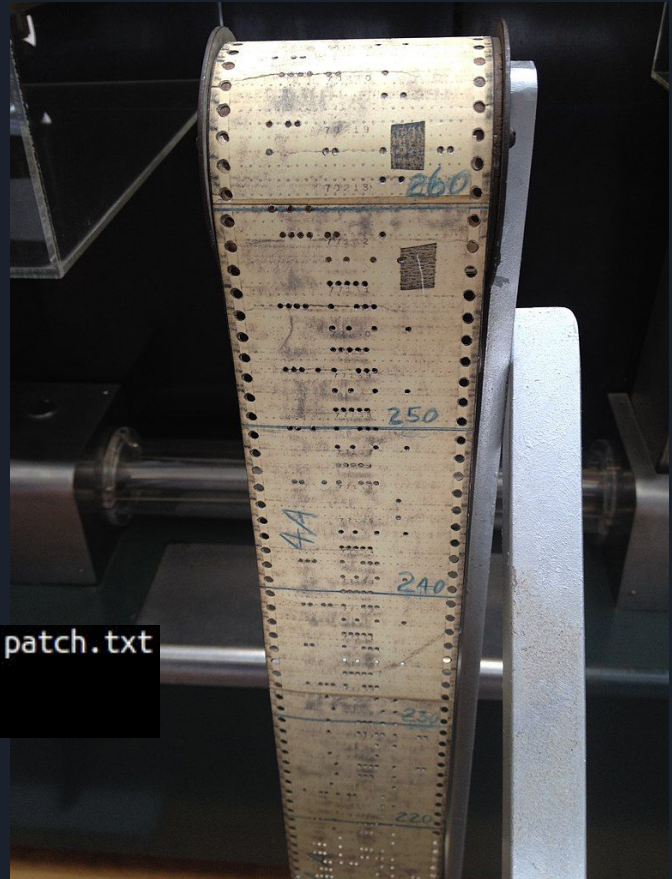
Graphical Diff Tools

- Kompare, meld, Beyond Compare, and Github/Gitlab have graphical diff

Centralized Version Control

- Have a central server and collect / store all those patches together!
    - Add username / password to protect the source code
    - Manage changesets over time / history of code
    - Label certain versions as releases
- Branching
    - Make long / complicated changes on branches by themselves so you don't break the build for others
- SCCS (Source Code Control System): Unix 1972
- RCS (Revision Control System): 1980 and CVS (Concurrent Versioning System): 1990
- SVN (Subversion): 2000
- IBM Rational Clearcase: Used by L3Harris for 20 years. Cost $$$$

Distributed Version Control

- Large projects like Linux needed a non-centralized tool (2000s)
  - Developers are all over the world, single central server would be expensive and taxed
  - Want to be able to make software changes when not connected
  - Centralized system also slower (especially large projects)
- BitKeeper (2000) became the Linux kernel CM tool
  - Had some weird license that let Linux devs use it for free
  - Controversial / flamewars
  - Drops free version used by Linux after 2 years
- Linux kernel needed a new CM tool
  - Linux Torvalds starts development of git over the course of 2 weeks
  - A few years later, it finally matures to become kernel's official CM tool
- Every computer has a full copy of the source repo
  - Slow to do initial clone
  - Really fast for EVERYTHING else

GitHub / Gitlab

- GitHub launches in 2008
  - Hosts git repo online - easily reachable by all
  - Free for open source development, $$ for proprietary repos (later free option too)
- Git / Github quickly become industry standard
  - L3Harris was not so quick to make the switch
- Gitlab starts in 2014
- GitHub and GitLab evolve into collaboration tools
  - Documentation: markdown, wiki
  - Discussions / bug tracking
  - Task management
  - Automation tools for testing, building, deploment
- DevOps

Documentation

- Most git browsers have built-in markdown preview
- What is Markdown?
  - Lightweight markup language (easier than HTML)
  - Supports image embedding, tables, lists, linking, etc
  - Styling doesn't interfere much with readability
- Markdown (Wikipedia)
- Github Markdown Syntax
- What are we documenting?
  - What does your application do?
  - How do you build it?
  - How do you run it?
  - Future work?
  - How does it work?

Leaking Secrets
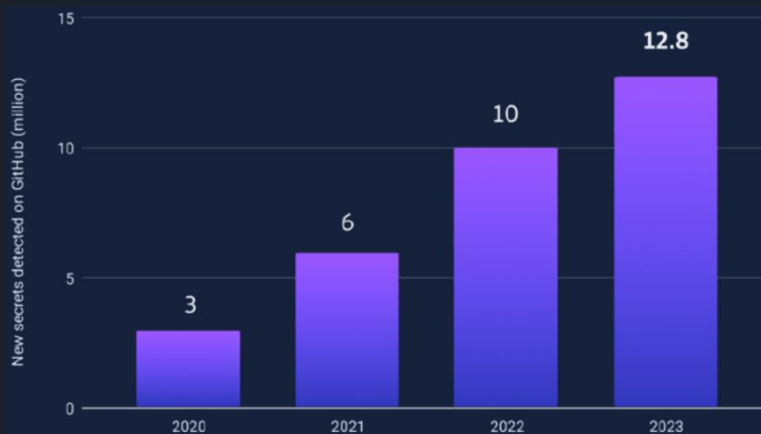
Top 10 Valid Specific Secrets Detectors in 2023

- Other 15.4%
- Facebook App Keys 1.2%
- GitHub OAuth App Keys 1.6%
- PostgreSQL Credentials 1.8%
- MySQL Credentials 2.1%
- AWS IAM 3.5%
- Google Cloud Keys 6.1%
- Telegrambot Bot Token 10.0%
- OpenWeatherMap Token 11.4%
- Google API Key 24.6%
- MongoDB Credentials 22.2%
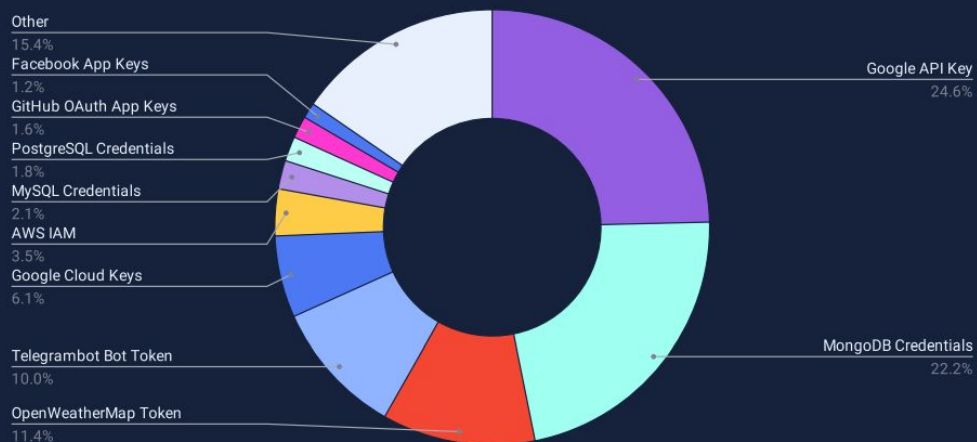
Start using GitHub

- Install git
- Create an ssh keypair on your PC
- Create an account on github
- Add your public SSH key to git account

Create a repo on github.com
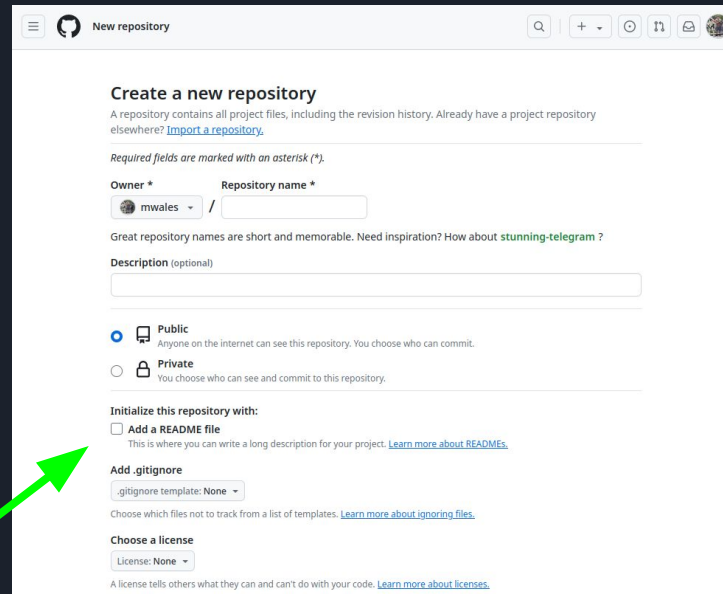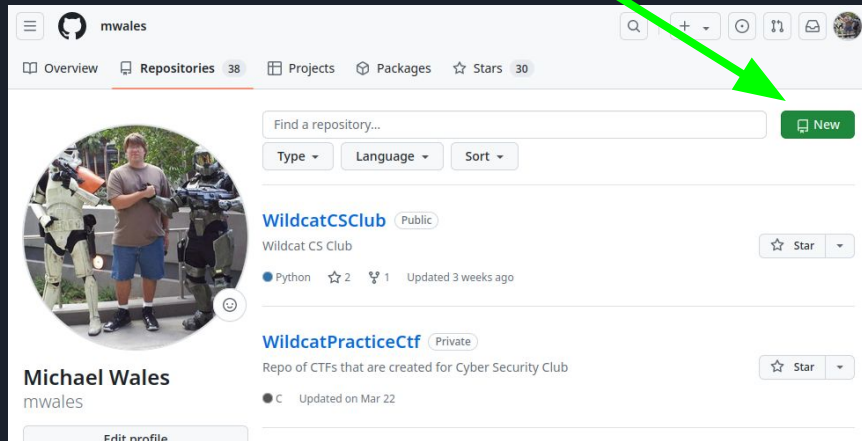
Grab the URL for the repository

Clone the repo

Update your code

mwales@Metroid: ~/scratch/WildcatCSClub

File   Edit   View   Search   Terminal   Help
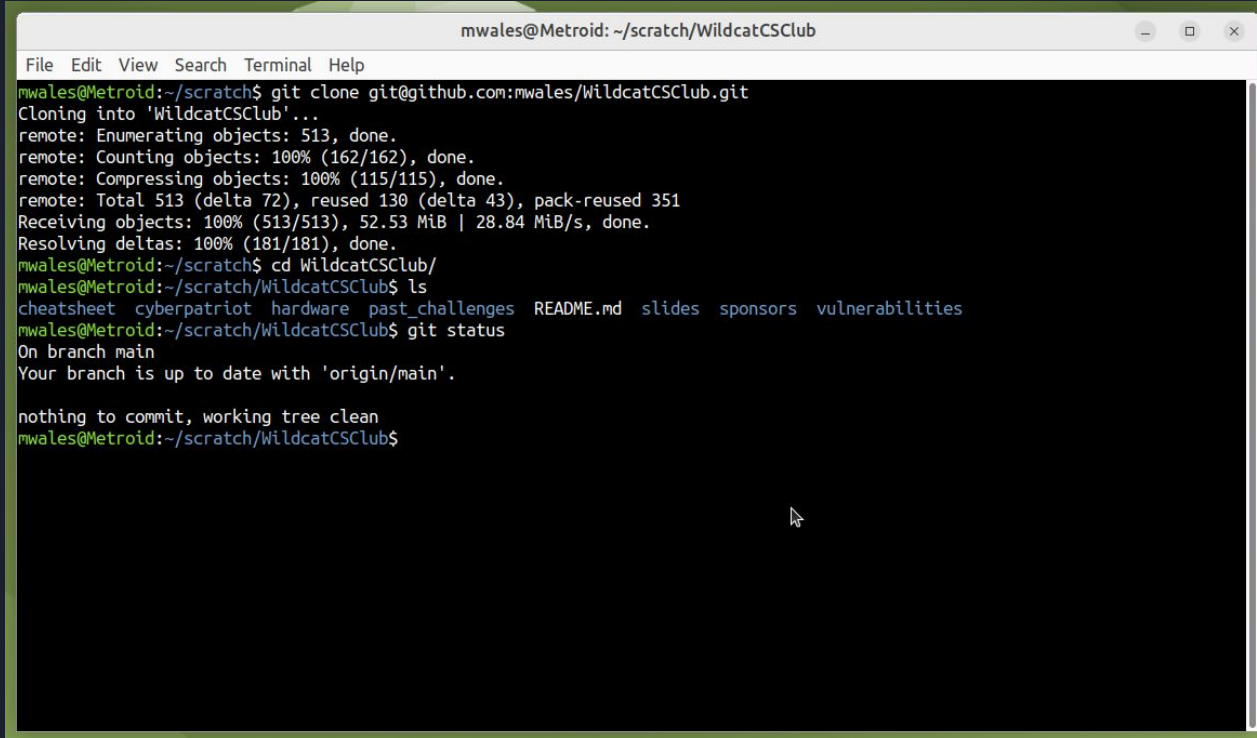
mwales@Metroid:~/scratch/WildcatCSClub$ ls
cheatsheet   cyberpatriot   hardware   past_challenges   README.md   slides   sponsors   vulnerabilities
mwales@Metroid:~/scratch/WildcatCSClub$ git status
On branch main
Your branch is up to date with 'origin/main'.

Changes not staged for commit:
  (use "git add <file>..." to update what will be committed)
  (use "git restore <file>..." to discard changes in working directory)
        modified: README.md

no changes added to commit (use "git add" and/or "git commit -a")
mwales@Metroid:~/scratch/WildcatCSClub$ git diff
diff --git a/README.md b/README.md
index b6bf753..e5a51e1 100644
--- a/README.md
+++ b/README.md
@@ -14,6 +14,8 @@ of the 50 or so challenges the we worked on over the year.
 * [2023 Code Quest Pictures](https://lockheedmartin.smugmug.com/Code-Quest/Code-Quest-2023/FL-Orlando/)
 * [Lockheed Martin Cyber Quest Information](https://www.lockheedmartin.com/en-us/who-we-are/communities/cyber-quest.html)
 * [2023 Cyber Quest Pictures](https://lockheedmartin.smugmug.com/CYBERQUEST/CYBERQUEST-2023/Orlando-FL/)
+* [2024 Code Quest Pictures](https://lockheedmartin.smugmug.com/Code-Quest/2024-Code-Quest/FL-Orlando/)
+* [2024 Cyber Quest Pictures](https://lockheedmartin.smugmug.com/CYBERQUEST/Cyber-Quest-2024/FL-Orlando/)

 ## Other possible in-person competition option for 2023-2024

mwales@Metroid:~/scratch/WildcatCSClub$

add, commit, push

Git history

Links

- https://www.britannica.com/topic/ARPANET/A-packet-of-data
- https://ethw.org/History_of_Lossless_Data_Compression_Algorithms
- https://www.bleepingcomputer.com/news/security/over-12-million-auth-secrets-and-keys-leaked-on-github-in-2023/
-