CYBERSECURITY WORKSHOP AGENDA

feat. defense against the dark cyber arts

by Vitaly Ford @ Arcadia University

July 2025

Big Picture

DAY 1

Intro, grant housekeeping, pre-workshop survey, core cyber concepts, cyber.org registration, OS security, intrusion detection

3

DAY 2

Pentesting (ethical hacking), OSINT, social engineering, simple malware analysis

23

DAY 3

Passwords (manager, hash, salt) & MFA, VPN, zero-trust model, backups, TryHackMe rooms

30

DAY 4

Speaker, cryptography, Linux, bash scripting, Capture The Flag (CTF), cyber competitions

34

DAY 5

Wi-Fi security, ethics and privacy, CTF Unplugged, unplugged exercises from teaching materials, famous hacks, VirtualBox and Kali Linux installation, feedback, closing

49

DAY 1

Intro, grant housekeeping, pre-workshop survey, core cyber concepts, cyber.org registration, OS security, intrusion detection

whoami

Introductions

Why are we here?

Structured and spontaneous scaffolded learning

Joint NSF Grant: Elmhurst University & Arcadia University

Grant Housekeeping

- Stipend ($400, prorated based on the attended ## hours) after the workshop ends
  - You will send W-9 directly to our Accounts Payable, and I will take care of the check requests
  - Stipend will be prorated based on the completed hours
- Up to 36 CE hours, reported to PDE at the beginning of August
- Availability of an extra $225 to register a student team at the Cyber Patriot competition
- Pre- and post-surveys (today and in the fall, respectively)
- Teaching materials
  - Each topic with a lesson plan, quiz [Kahoot-ready], homework, exercise, and slides
  - Also available as an online self-paced platform at https://cysia.vford.com (work-in-progress)
- Free existing resources outside of the grant

CE Hours and PPID

- Email me your PPID if you need the hours to be registered
  - PPID can be found at
    https://www.perms.pa.gov/screens/wfpublicaccess.aspx
  - Hours will be sent to MCIU
  - MCIU will provide them to PDE

PRE-WORKSHOP SURVEY

HTTPS://ELMHURST. CO1.QUALTRICS.CO M/JFE/FORM/SV_0C G1BBUZUGAFXDC

Cybersecurity Careers

- Refer to https://www.cyberseek.org

Teaching Materials Google Drive Folder

- https://drive.google.com/drive/folders/1XCEZ2DmGTV_k-Bda59eHQV12IF6NAOy6?usp=sharing

Cyber.org: Cyber Range Registration

- Refer to the Cyber.org teaching materials available at

  https://drive.google.com/drive/folders/1XCEZ2DmGTV_k-Bda59eHQV12IF6NAOy6?usp=sharing

"Hacker" Terms (ex. FB market)

- Threat

- Vulnerability

- Exploit

- Attack (passive/active, software/network/human)

  - Refer to:

    - https://attack.mitre.org

    - https://www.shodan.io/dashboard with search queries like `has_screenshot:true camera` and https://github.com/jakejarvis/awesome-shodan-queries

Core Cyber Concepts (ex. Website)

- CIA Triad (Confidentiality, Integrity, Availability)
- Authentication/authorization
- Non-repudiation
- Defense in Depth
- Secure by Design
- Least Privilege
- Risk Management (id, impact, mitigate, monitor)
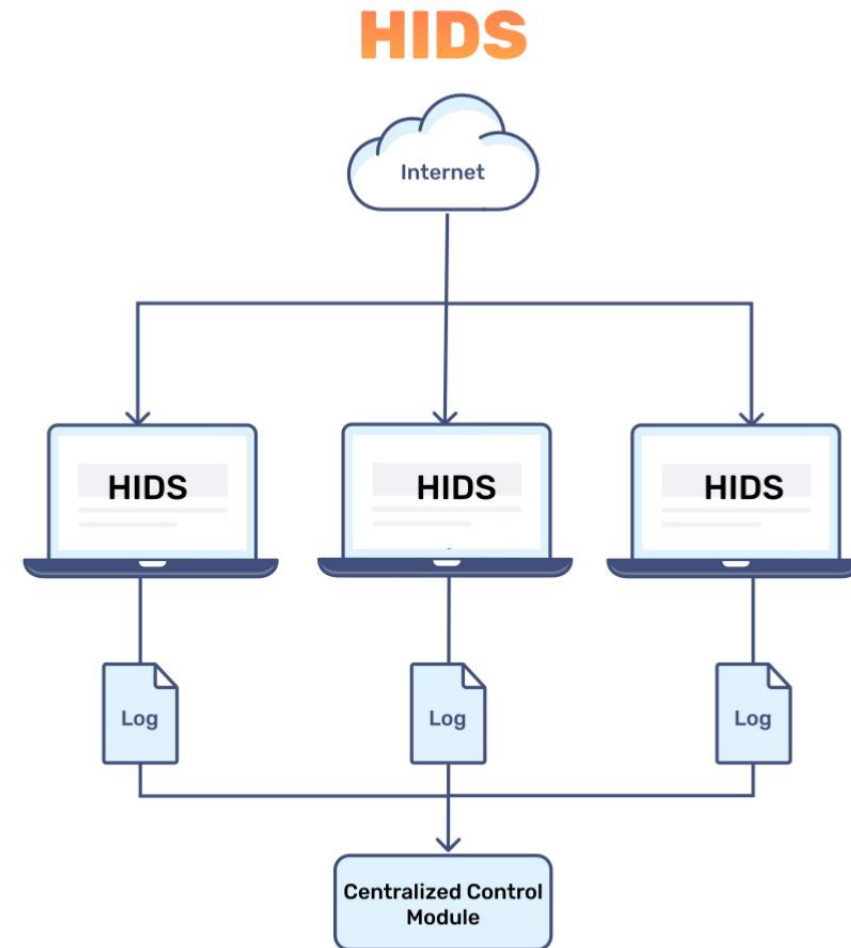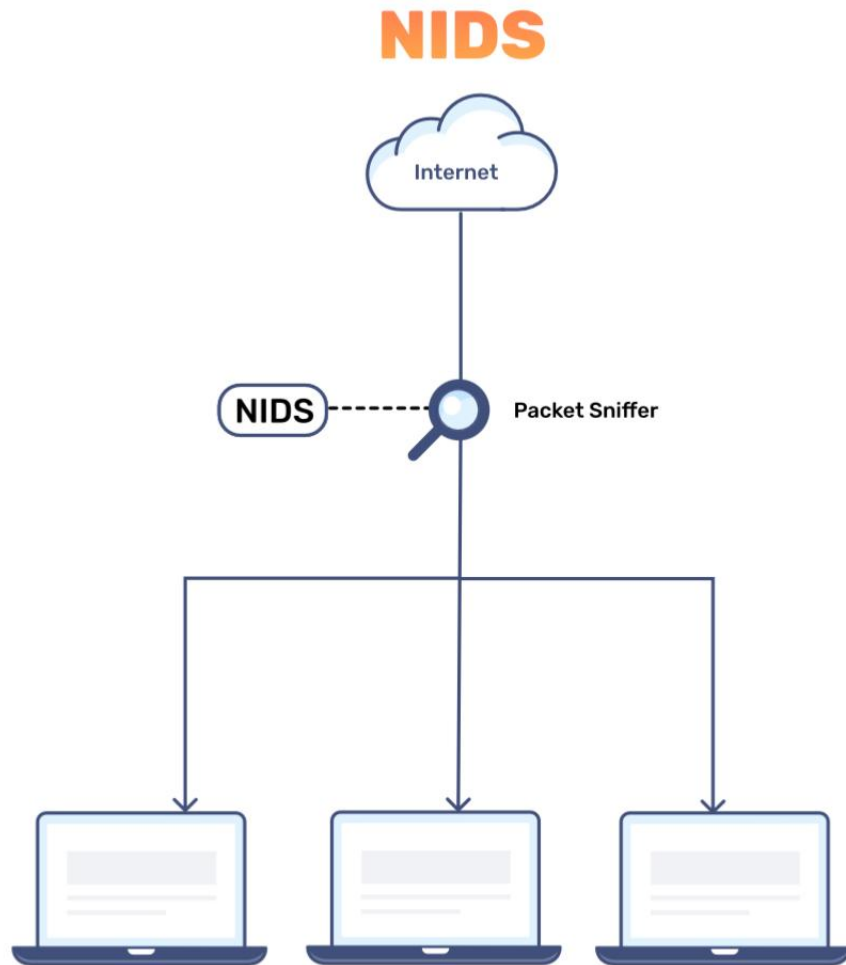- User Education

Operating System (OS) Security

- How do people get hacked in the first place?
  - Refer to phishing, smishing, vishing, and malware teaching materials
- Default antivirus
- Free on-demand virus scanners (BitDefender*, Malwarebytes*)
- Firewall VS anti-virus
  - Intro to networking concepts: IP, port, host, network
  - Refer to the How the Internet Works teaching material and https://netflow.vford.com
- Adblocker (uBlock Origin; uBlock Origin Light for Chrome) or Brave Browser (for mobile too)
  - But why?
- User/admin access/permissions/local security policies
- Domain-level restrictions
- Storage encryption, BIOS/UEFI password, TPM (Trusted Platform Module)
- Startup executables & sysinternals for Windows
- Windows Defender advanced settings
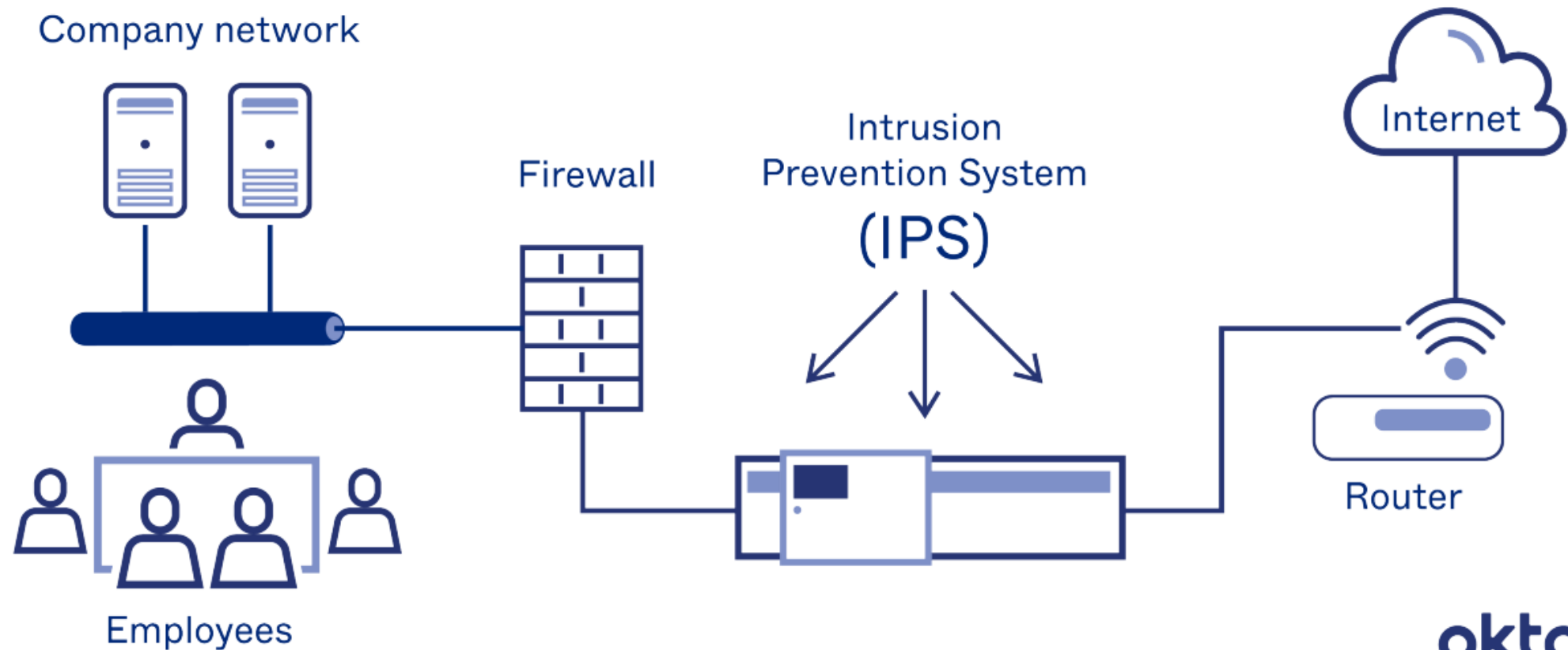
Defenses Against Intrusions

- IDS (Intrusion Detection System)
    - HIDS/NIDS (Host/Network-based Intrusion Detection System)
- IPS (Intrusion Prevention System)
- EDR (Endpoint [threat] Detection and Response)

- XDR (Extended Detection and Response)
- SIEM (Security Information and Event Management)
- SOAR (Security Orchestration, Automation, and Response)
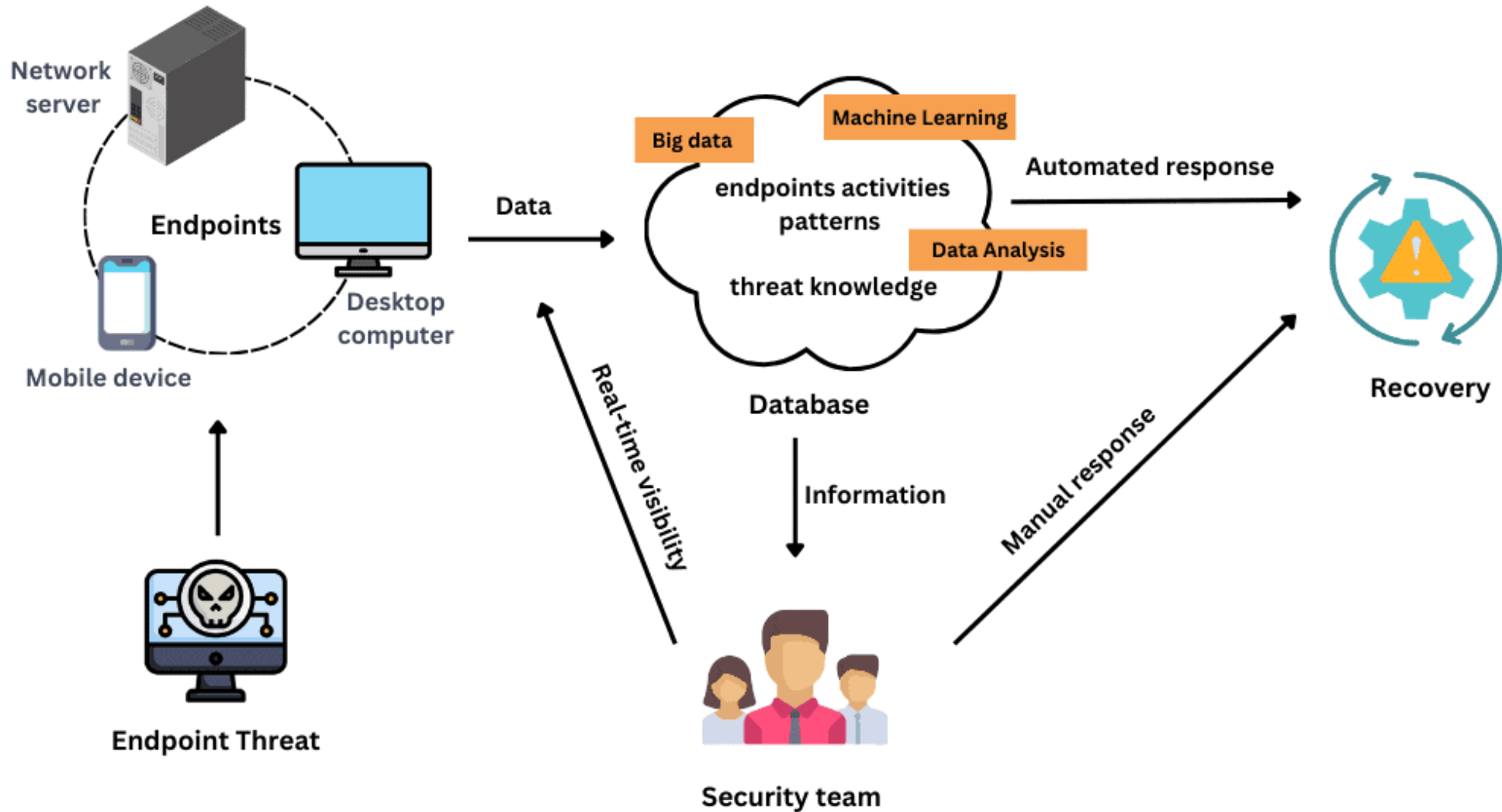- SOC (Security Operations Center)

IDS (HIDS/NIDS)

https://cyberhub.sa/posts/5259

IPS

Intrusion Prevention Systems

EDR

https://www.baeldung.com/cs/edr

XDR → SIEM/SOAR

https://www.trendmicro.com/en_my/what-is/xdr.html

19
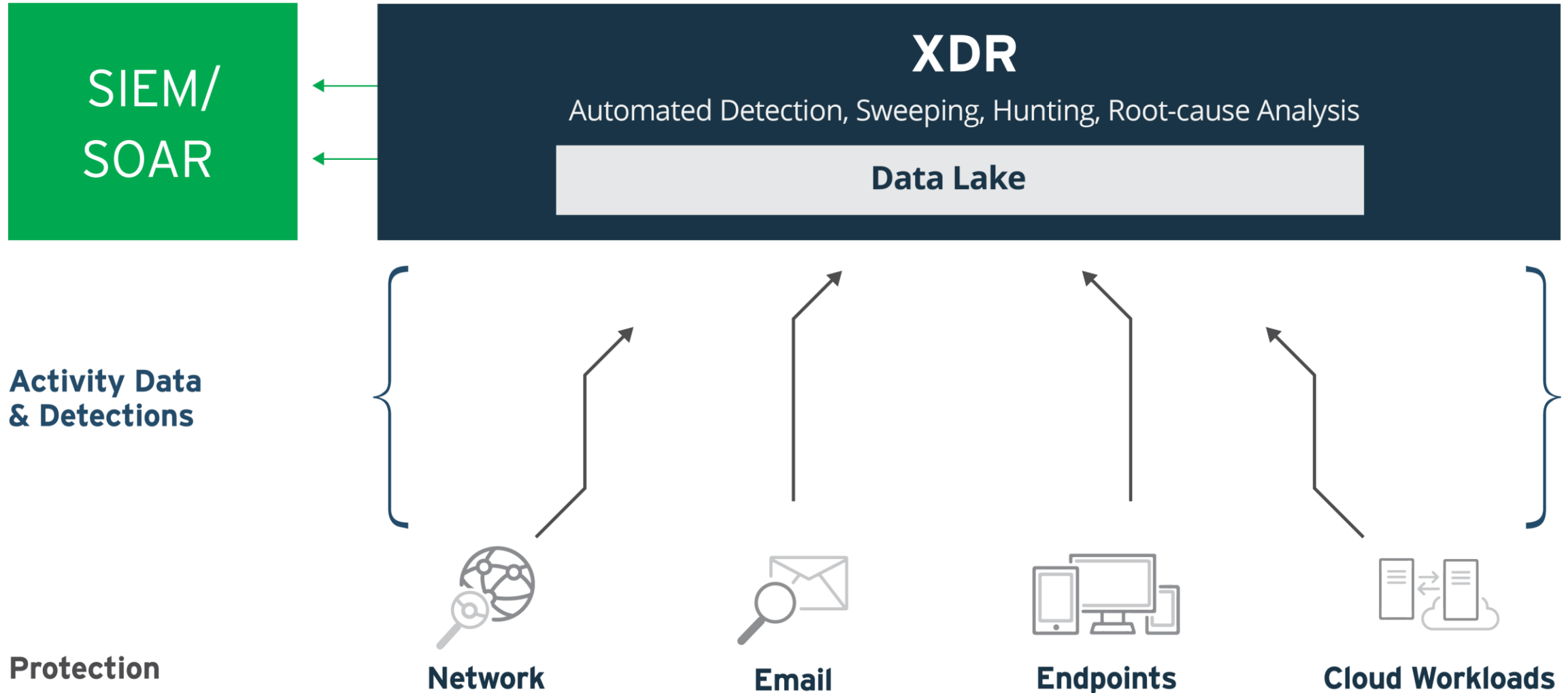
SOC

OpenSOC

- Refer to https://opensoc.io

Cyber.org Cyber Range

- Get familiar with the machines

- If time permits, register on TryHackMe.com

DAY 2

Pentesting (ethical hacking), OSINT, social engineering, simple malware analysis

Fun Cyber and Social Engineering

- Refer to the videos section at https://teachcyber.vford.com/nifty (skip password videos for later during Day 3)
- Refer to https://github.com/drk1wi/Modlishka
- Refer to https://github.com/SygniaLabs/evilginx3
- Refer to https://getgophish.com
- Refer to https://github.com/Ahaz1701/EvilWorker

"I Bypassed The Firewall" (?!)

- A famous line in movies

- Let's draw it out

Penetration Testing by [Peter Kim](#)

1. Intelligence Gathering

2. Initial Foothold

3. Local/Network Enumeration

4. Local Privilege Escalation

5. Persistence

6. Lateral Movement

7. Domain Privilege Escalation

8. Dumping Hashes

9. Data Exfiltration

10. Reporting

OSINT

- Open-source intelligence gathering

  - https://haveibeenpwned.com

  - https://truepeoplesearch.com

  - Google Dorking (GHDB), exploits databases (exploit-db, vulmon.com)

  - Automated toolsets

    - Metasploit: https://www.offsec.com/metasploit-unleashed

    - Cobalt Strike: https://www.cobaltstrike.com

    - Cybersecurity AI: https://github.com/aliasrobotics/cai

Simple Malware Analysis

- Refer to the malware teaching materials

- Refer to https://virustotal.com

- Refer to https://hybrid-analysis.com

- Refer to https://www.joesandbox.com

- Generate malware using `msfvenom` (Metasploit) and upload to the above

TryHackMe Rooms

- Register at TryHackMe and launch https://tryhackme.com/room/blue
  - If TryHackMe is giving us trouble with captchas, check out
    https://youtu.be/U4uZktyGfkM (my recording of a full compromise of Windows 7
    using a generated malware with `msfvenom`)
- Show how to run your own Kali/Ubuntu box with VPN for TryHackMe
  access on Cyber.org
- If time permits, launch https://tryhackme.com/room/basicpentestingjt
  and use the OpenVPN (no limits) to connect to the room instead of
  the Attack Box (it's limited to 1 hour/day)

DAY 3

Passwords (manager, hash, salt) & MFA, VPN, zero-trust model, backups, TryHackMe rooms

Passwords

- Refer to the password videos at

  https://teachcyber.vford.com/nifty

- Refer to the passwords teaching materials

  - Hash cracking (+try on Kali on cyber.org)

  - MFA, 2FA, biometrics, passkeys

- Password manager (sign up and install Bitwarden)

Backups

- Ensure you backup your phone

- Use Google Drive, Dropbox, OneDrive, iCloud Drive

- Some cloud providers give you lifetime access for a lump sum

  - E.g., pCloud.com gives 2 TB for $400

TryHackMe Rooms

- Use Cyber.org Kali or Ubuntu machines
- Start with https://tryhackme.com/hacktivities
- Launch https://tryhackme.com/room/offensivesecurityintro and switch to https://tryhackme.com/soc-sim (SOC sim can take 10-15 mins)
  - While waiting to boot SOC simulator, go back to the offensive security intro room
- Go over https://tryhackme.com/room/introtonetworking

DAY 4

Speaker, cryptography, Linux, bash scripting, Capture The Flag (CTF), cyber competitions

SPEAKER

Sarah Putterman, retired teacher in Cheltenham

Cryptography (the next 4 slides)

- Refer to the cryptography teaching material
  - Simple ciphers
  - Asymmetric/symmetric encryption
  - Digital signatures and HTTPS certificates

confidentiality

asymmetric

symmetric   one key

enc/decr

digital
signatures

pub
key
enc

priv
key   enc

(C I ~~A~~)   can we
protect
both?
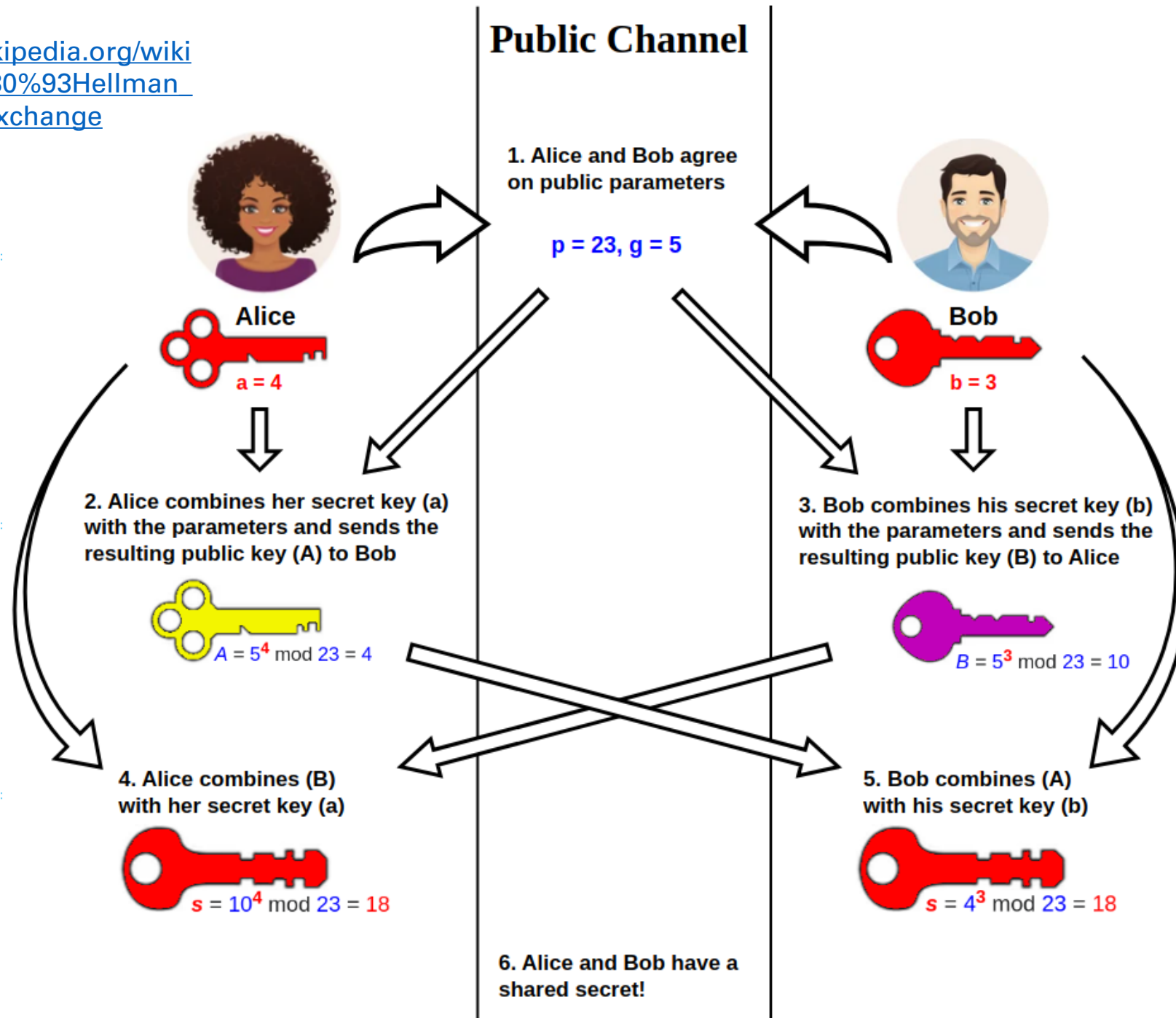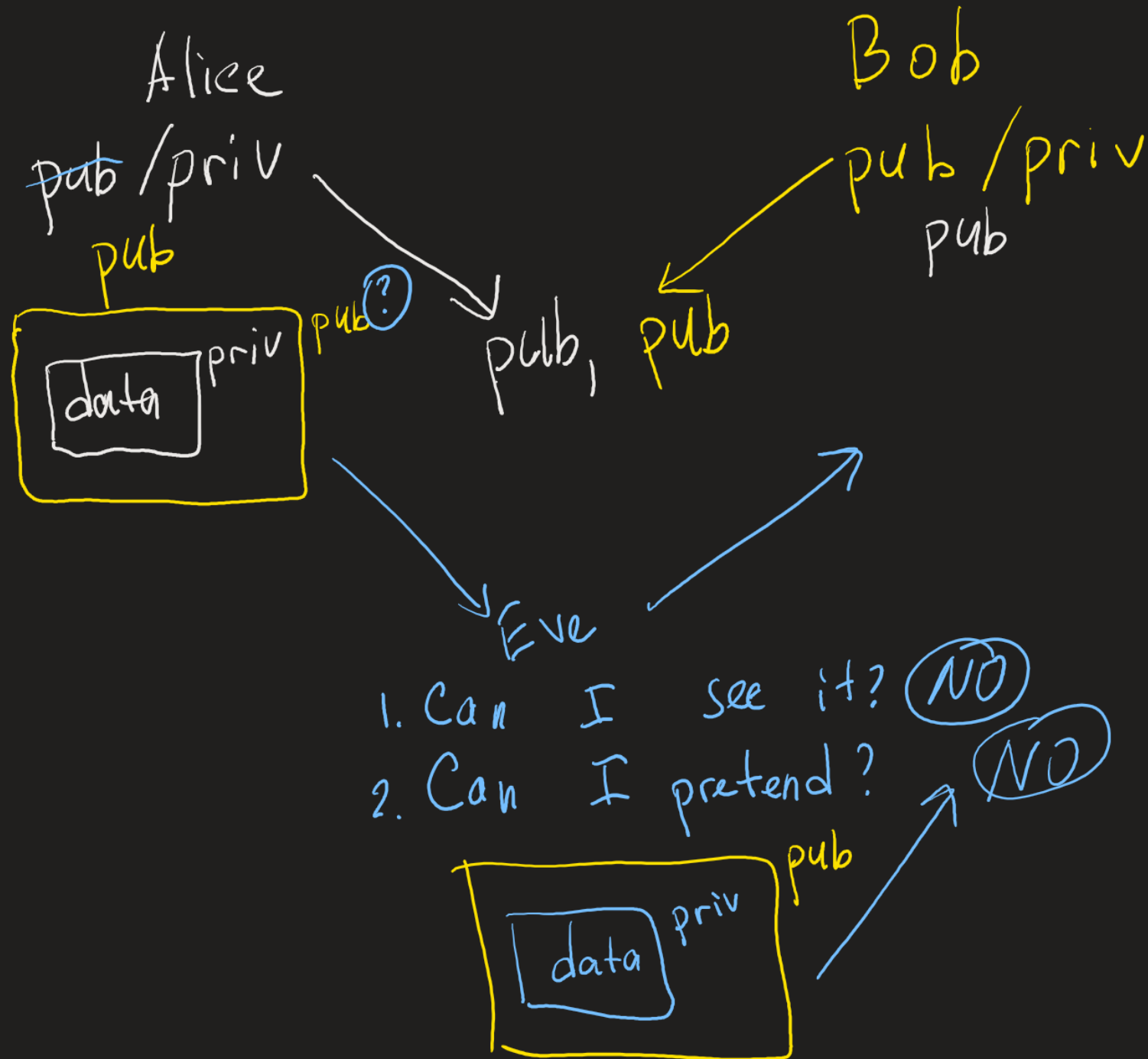
Alice → Bob
AES (256) bits   AES (256) bits
key   key
128   128

Eve

Public Channel

1. Alice and Bob agree on public parameters

$p = 23, g = 5$

Alice

$a = 4$

Bob

$b = 3$

2. Alice combines her secret key (a) with the parameters and sends the resulting public key (A) to Bob

$A = 5^4 \bmod 23 = 4$

3. Bob combines his secret key (b) with the parameters and sends the resulting public key (B) to Alice

$B = 5^3 \bmod 23 = 10$

4. Alice combines (B) with her secret key (a)

$s = 10^4 \bmod 23 = 18$

5. Bob combines (A) with his secret key (b)

$s = 4^3 \bmod 23 = 18$

6. Alice and Bob have a shared secret!

38
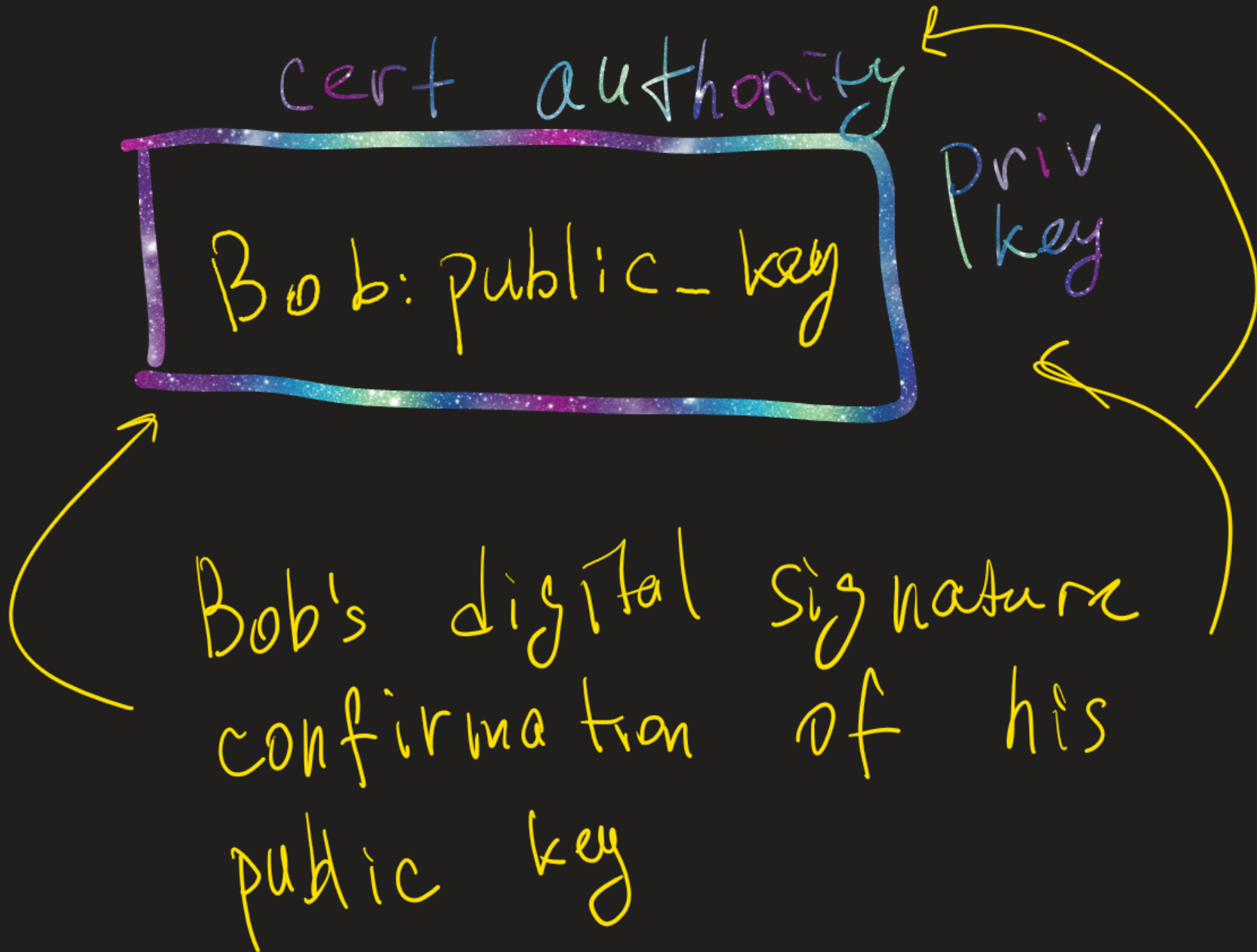
Linux

- Open and go into town in the Ubuntu and Kali machines on cyber.org cyber range

  - Refer to https://linuxjourney.com for Linux learning

  - Refer to https://overthewire.org/wargames/bandit/ to practice

Bash

- Refer to https://www.learnshell.org for Bash scripting and automation

  - You can even use ChatGPT for both Linux simulation and script generation

CTF

- Capture The Flag
  - https://practice.ctfcyber.org
  - https://picoctf.org
  - https://316ctf.com
  - https://ctf.vford.com (secure coding CTF)
  - https://gencybercoin.vford.com (secure coding CTF)
  - TryHackMe does Advent of Cyber every December
  - For more skilled folks, try hackthebox.com
  - List of global CTFs: https://ctftime.org
- CTF write-ups

CTF: Try it out

- Engage in cyber.org CTF and

  https://gencybercoin.vford.com for secure coding CTF (bug

  bounty hunting) and OSINT

  - Show https://gchq.github.io/CyberChef

Cyber Competitions

- **National Cyber Cup**: https://cyber.org/national-cyber-cup

- National Cyber League: https://nationalcyberleague.org

- Cyber Patriot: https://www.uscyberpatriot.org

- Local CTF competitions like

  https://sites.google.com/site/ccsceastern/participation/competition

- CSAW: https://www.csaw.io/ctf

- Learn (videos) and practice: https://mitrecyberacademy.org

- https://www.uscybergames.com

GenCyber Summer Camps

- Both camp types - teacher and students:

  https://public.cyber.mil/gencyber/camp-catalog

President's Cup by CISA

- https://github.com/cisagov/prescup-challenges

TryCyber

- If we have time, let's try https://trycyber.us

DAY 5

Wi-Fi security, ethics and privacy, CTF Unplugged, unplugged exercises from teaching materials, famous hacks, VirtualBox and Kali Linux installation, feedback, closing

Wi-Fi Attacks

- Evil twin like [Hak5 Pineapple](#)

- Rogue access point pretending to be real

- Man-in-the-middle (MITM) like [bettercap](#)

- Wi-Fi phishing captive portal

- MAC address (aka physical ID of the device issued by the manufacturer) spoofing

  - [ARP spoofing](#) as a follow up

- Refer to https://wigle.net

Wi-Fi Defense

- Do not use public Wi-Fi unless you have a VPN

  - Free unlimited VPNs usually have red flags, except Proton VPN (my personal top pick among free ones), Hide.me, and Windscribe (10GB)

  - Google Pixel and Pixel Tablets have built-in "VPN by Google"

- Ensure using the latest (at least WPA2, but better WPA3) security enabled at home, with a long passphrase

  - Hide your Wi-Fi SSID at the router level

Ethics and Laws (non-exhaustive list)

- **Permission** separates an ethical hack from an illegal activity

- **Take it Down Act** (2025)
  - Criminalizes publishing nonconsensual, sexually explicit images and videos (including AI-generated) and requires platforms to remove the content within 48 hours of notice
- **COPPA** (Children's Online Privacy Protection Act, 1998)
  - Requires websites to obtain parental consent before collecting, using, or disclosing personal information from children under 13
- **CFAA** (Computer Fraud and Abuse Act, 1986)
  - Prohibits unauthorized computer access

Tech and Privacy

- [Apple vs. FBI (2016)](#)
  - The FBI demanded Apple unlock an iPhone used by a terrorist; Apple refused to create a backdoor, citing privacy and security risks ([q/a ideas](#))
- [Facebook-Cambridge Analytica Scandal (2018)](#)
  - Data from millions of users harvested without consent and used for political influence
- [TikTok and National Security Concerns](#) (Ongoing)
  - Concerns over Chinese ownership of TikTok and potential data sharing with the Chinese government.
- [Google Project Maven (2018)](#)
  - Google helped the Pentagon use AI to analyze drone footage, sparking internal protests from employees as their work would be weaponized

CTF Unplugged

- Available at https://vford.me/ctf-unplugged/CTF_Unplugged_May_2019.docx
  - Contact Vitaly Ford for answers

Go over unplugged exercises

- Refer to the teaching materials

Real Hacks and OSINT of Real Hackers

- Going after a famous Conti ransomware developer ($10m prize by FBI): https://justpaste.it/k72mv

- Famous hack of the Hacking Team by Phineas Fisher: https://gitlab.com/brn1337/phineas-fisher-collection/-/blob/master/2015_HackingTeam.txt?ref_type=heads

VirtualBox and Kali Linux

- Install VirtualBox and its extensions

- Open downloaded Kali in VirtualBox

Resources

- Structured content (check out cyber.org teaching material for instructions): https://cyber.org
- Various random nano-modules for all levels: https://clark.center
- NCYTE Curriculum: https://www.ncyte.net/academia/faculty/cybersecurity-curriculum
- Comprehensive high school cyber PDF content in different languages: https://www.hackerhighschool.org/lessons.html
- Cybersecurity guide: https://cybersecurityguide.org
- Cyber seek interactive visualization for careers: https://www.cyberseek.org
- 15 hours of video, 10 week course, with notes and detailed demonstration of a full penetration test: https://github.com/hmaverickadams/Beginner-Network-Pentesting
- Networking videos: https://www.elithecomputerguy.com/2010/11/tcp-ip-and-subnet-masking/
- Find more at https://teachcyber.vford.com/diy/

News Feeds

- https://news.ycombinator.com/

- https://krebsonsecurity.com/

- https://www.reddit.com/r/netsec/

- https://bytebytego.com/guides/

- https://dev.to/

Open Discussion

- Sign and write down your PPID

  - Pass around the hours list for signatures

- Feedback: https://forms.gle/3op6kBYJPyPiozku6

- Time to reflect and chat

Stay Connected!

- Email: fordv@arcadia.edu

- Discord: vitalyford