Wachemo University

College of Engineering and Technology

Department of Software engineering

COURSE:Fundamentals of Software Security

Section A

Group 6

Group name	ID
1. Olira Duguma.....	1501209
2. Firaol Dereje.....	1500924
3. Eskindir Kibreab.....	1501873
4. Bersufekad Ermias.....	1501758
5. Misgana Tamire.....	1501127

From Jordan episode:

1. List Three Awesome Things

I. Developing an Encyclopedic Knowledge of Explosives at 13"At thirteen and he's already developing an encyclopedic knowledge of explosives, stuff that he probably shouldn't be getting into at that age."Jordan's early curiosity about hacking and mischief led him to collect vast amounts of

information, including text files detailing bomb-making and phreaking techniques. His ability to dive deep into knowledge at such a young age was both surprising and a bit dangerous.

What we learned: Curiosity is great, but it comes with responsibility. Just because you *can* learn something doesn't mean you *should*—it's important to have mentors to help channel knowledge into something positive.

What surprised we:-

ii. Phone Phreaking & Listening to Conversations

"JORDAN: Other things I started learning how to do were diagram and learn a lot about phone systems. We called it phreaking back then... I thought that was fascinating but you would lose them as they went out of reception."

Jordan became obsessed with hacking phone systems, even going as far as stealing a lineman's Ameritech handset. He used it to tap into neighborhood phone lines, spending hours listening to people's conversations. This highlights how insecure analog phone networks were before encryption became the norm.

What we learned: Before modern encryption, phone systems were incredibly vulnerable. It's crazy to think that someone could just clip onto a wire and eavesdrop without anyone knowing.

What surprised we:

iii. **Using a Stolen Credit Card to Order Pizza for His Entire School**

"ORDAN: One time, I decided to go big and I called from a pay phone and used a credit card and I ordered pizza for the next day for my entire middle school."

One of the most shocking moments was Jordan pulling off a massive prank by ordering pizza for his whole school using a stolen credit card. The elaborate setup, including instructing the delivery guy to say "Happy Birthday, Mrs. Jacobson," showed his deep understanding of social engineering—even as a kid. This was a turning point where he realized how serious his actions could be.

What we learned: Early online payment systems didn't properly verify transactions. This shows how weak security measures can be if companies don't validate cardholder information properly.

2. *List Two Things to Advocate*

Cybersecurity: Protecting Your Information in the Digital Age

Jordan's story highlights the importance of cybersecurity. Without proper precautions, your personal information—like phone calls, credit card details, and passwords—can be exposed and exploited. Here's how you can safeguard yourself and those around you:

a. **Secure Your Online Accounts: Why?**
   Just like Jordan intercepted phone calls by exploiting weak security, hackers today steal login credentials from unsecured accounts.

Real-World Example:
Many people reuse passwords. If one account is compromised, hackers can use the same password to break into other services, leading to stolen money and identity theft.

Actionable Tips:

- Enable Multi-Factor Authentication (MFA) to add an extra layer of protection.
- Use strong, unique passwords for each account (consider a password manager).
- Never share login details via email or phone.
- **b. Protect Your Credit Card**
- **Why?**
  Jordan once created fake credit card numbers—imagine what real cybercriminals can do today.
- **Real-World Example:**
  Hackers steal credit card info through phishing scams, fake shopping sites, and public Wi-Fi. Victims often don't realize their card is compromised until fraudulent transactions appear.
- **Actionable Tips:**

- Use virtual credit cards or one-time payment methods online.
- Monitor your bank statements regularly and set up fraud alerts.
- Only enter card details on secure websites (look for "https://" in the URL).

Finally: Ignoring cybersecurity can result in stolen passwords, misused credit cards, and exposed private data—just like Jordan's vulnerable targets. Protect yourself before it's too late.

3.**List one thing that is ACTIONABLE.**

One Actionable Step I'm Taking

After listening to this podcast, I have decided to change all my passwords to strong, unique ones. Previously, I used simple and repeated passwords across multiple websites.

Why?

I have learned that we can never fully anticipate who might attempt to scam us or the level of skill they may have in hacking. If one of my accounts were to be compromised, using the same password across multiple sites would put all my other accounts at significant risk.

What I'm Doing:

- Creating unique, strong passwords for each website.
- Using a password manager to store them securely.
- Enabling Multi-Factor Authentication (MFA) for added security.

This podcast has made me realize how vulnerable we can be without even knowing it. As a result, I am now taking active steps to protect myself.

From Jeremy marketing Episode:-

1.three notable things or insights:

What surprised we from these story after we listened the episode is:-

a.**Exploiting sensitive information simply**:The penetration tester, Tinker, was hired to pose as a new employee in the marketing department. This approach allowed him to exploit internal systems and gather sensitive information without any suspicion. I learned fro this inside attacker is very dangerous from all other attacker.

b.**Using guessable password**: Tinker discovered that many internal systems still used default or easily guessable passwords. This oversight provided him with unauthorized access to critical systems.so I learned from these the importance of changing guessable password to some strong password as much as possible to protect my self from attacker.

c.The importance of physical security in software system:in addition to digital vulnerabilities,tinker identified weaknesses in physical security such as unsecured server room.so physical security is also important in security system.

2.Two things to advocate:

d.**Regular Security Training**: I will educate co-workers,my family,friends and others about how to defense attacks and social engineering tactics. Awareness can prevent inadvertent disclosures of sensitive information.

e.**Using both physical and digital security**:I will tell to co-workers,my family,my friends and others as they use both physical and digital security. Because cybersecurity is not just code its locked room,device encryption and locate our devices in protected area.

3.One Actionable Step :

f.**Implement Multi-Factor Authentication**: i-Factor Authentication (MFA): Enabling MFA adds an extra layer of security, ensuring that even if passwords are compromised, unauthorized access is still prevented.

From No Parking Episode:-

In Episode 40 of Darknet Diaries, titled "No Parking," we follow **Kyle,** a red teamer who tests companies' security by trying to break into their facilities.

Three Awesome Things

- **They try to Creative enter** Kyle use of a dropbox a device made from a cell phone, Raspberry Pi, wireless card to remotely access the company's network was both innovative and surprising.

- Kyle's ability to blend in by dressing (that close is similar to the companies employee) and acting like a regular employee bypassing security measures that's one is incredible one.

- ❖ They are thinking quickly when faced with unexpected challenges, such as locked doors or encountering employees, Kyle's ability to adapt and by “push, twist... nothing” lol 😳 …then unlock and it worked.

❖ Two Things to Advocate

- ❖ Encourage organizations to lock offices containing sensitive documents after hours to prevent unauthorized access.

- Advise companies to divide their networks into segments to limit the impact of unauthorized devices, that’s help to doesn't provide access to the entire network.

One Actionable Item

After listening to this episode, I will assess and improve the physical security in my workplace or in my laptop, ensuring that areas with sensitive information are properly secured and locked 💯 .

This episode tell us the importance of strong security and strategy that includes both digital and physical security.