Hands-on A1: Examine Data Breaches

Hackers selling 117 million LinkedIn passwords
https://money.cnn.com/2016/05/19/technology/linkedin-hack/

1. **What is the breach about, including the victim and impact of damage?**

There are 6.5 million passwords sold on the black market by hackers. Most people prefer to reuse their passwords, and hackers are more likely to gain access to 117 million people's email and bank accounts.

2. **What was the method of leak (if necessary, consult to today's lecture note)?**

LinkedIn had not added a middle layer of security that made the jumbled text harder to decode at that time.

3. **Which technology could have prevented the leak (if necessary, consult to today's lecture note)?**

LinkedIn did not publish the reason for substantial information leakage.
We can investigate the following aspects：
First of all, LinkedIn internal personnel need to investigate whether it is an employee maliciously leaking information.
Second, check the system. Whether the client-side has verification and whether there is a bug allows another script coding to be executed.
Furthermore, the server-side allows cross-domain requests or not. It has a risk of SQL injection and other issues. When the server receives any request, it ensures that the middleware performs its duties.

A hotspot finder app exposed 2 million Wi-Fi network passwords
https://techcrunch.com/2019/04/22/hotspot-password-leak/

1. **What is the breach about, including the victim and impact of damage?**

There are 2 million network passwords exposed and included more information such as precise geolocation.
If the private network is made public, it will occupy the host network bandwidth and affect the user experience. It is also possible to perform network packet capture on specific connected devices under the same wifi network environment, thereby stealing user-sent information.
Hackers can use fake DNS to mislead users and tamper with users' access to websites, thereby trick users into filling in important information, such as usernames, passwords, or payment passwords.

2. **What was the method of leak (if necessary, consult to today's lecture note)?**

The article did not mention how this information was leaked. I guess it might be through brute force.

3. **Which technology could have prevented the leak (if necessary, consult to today's lecture**

note)?

Users regularly change WiFi passwords. Make the WiFi password size longer and more complex as much as possible, thereby increasing the time complexity of brute force cracking.
Users can defend by adjusting routing configuration parameters. For example, set the number of devices that can be connected to the route.
Users regularly use software to refresh the DNS cache to ensure correct DNS resolution.
Do not connect to public WiFi randomly.

*Insider Steals Data of 2 Million Vodafone Germany Customers*https://www.securityweek.com/attacker-steals-data-2-million-vodafone-germany-customers

1. **What is the breach about, including the victim and impact of damage?**

2 Million Vodafone users' information leaked. It includes customer names, addresses, gender, birth dates, bank account numbers and bank sort codes, the telecommunications giant said.

2. **What was the method of leak (if necessary, consult to today's lecture note)?**

The suspect had worked for a contractor of the company and had insider knowledge. The specific method of stealing information was not disclosed.

3. **Which technology could have prevented the leak (if necessary, consult to today's lecture note)?**

Improve the quality of employees and popularize legal knowledge. Clarify the legal liability for damage to company assets.
Regularly evaluate the company system. Clarify employees' management authority over the system, and assign management responsibilities to the system.