The importance of security in application development

Topics

1. Introduction and Fundamentals
    a. Why is Security Important?
    b. Security Concept in Development
2. The Current Threat Landscape
    a. The Reality of Data Exposure
    b. Common Threats in Web and Mobile Apps
    c. The Hacker's Motivation
3. Implementing Security Measures
    a. Basic Security You Should Have
    b. Security Lifespan
    c. Policies and Legality
4. Conclusion

Introduction

Good morning / afternoon, everyone. Thank you for joining us today.
My name is Sonia Cabrera, and I'm presenting with my patterns: Chengzhe Li, Diego Alexander, and Enrique de los Pinos.

Our topic today is **Security in Application Development**—specifically, why security is critical when building any new application.

We have a clear agenda for you:

1. Chengzhe will begin by covering the fundamentals of security.
2. Next, Enrique and Diego will discuss the current threat landscape.
3. Finally, I will explain how to effectively implement security measures.

Now, to start, I'd like to hand over to Chengzhe

Fundamentals

First of all, could somebody explain in his own words what security means?

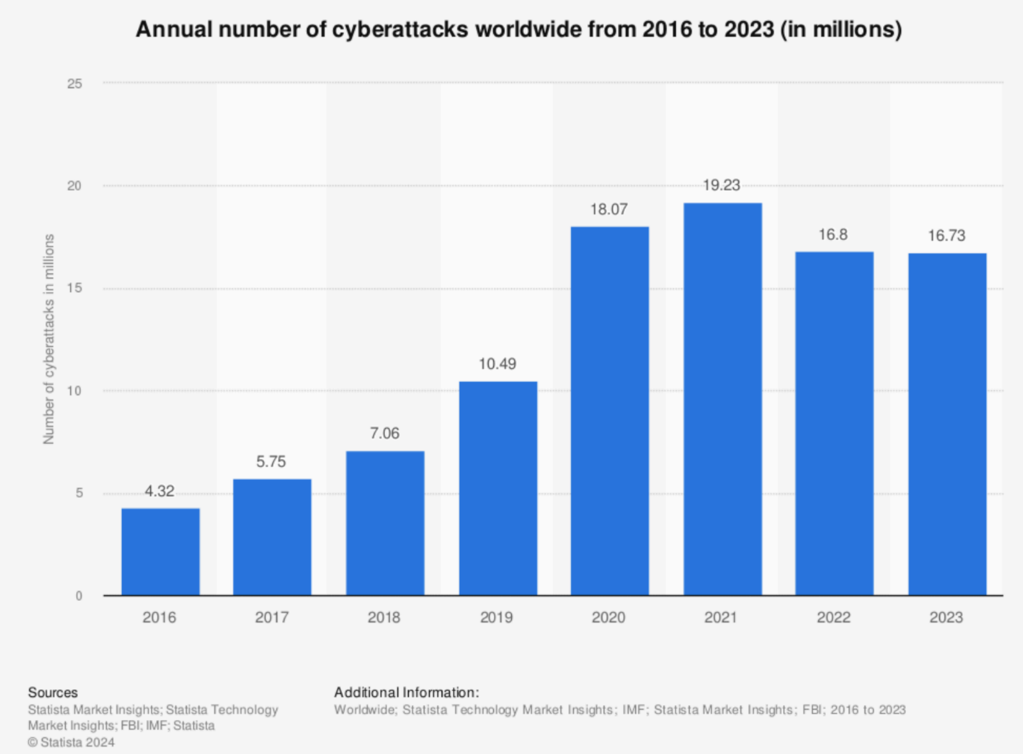
According to the dictionary of Cambridge: **Security is "the protection of people, organizations, countries, etc. against a possible attack or other crime".**

Why is Security Important?

Security has been a concern since the beginning of humanity. From predators chasing us, to protecting from hackers trying to steal our data.

Despite all efforts made to ensure safety along the history of our humanity, security remains an ongoing challenge. Furthermore, with the rise of the Internet era, new threats concerning our cybersecurity have appeared.

As a matter of fact, cyberattacks have increased exponentially over the last few years, according to Statista:



Sources
Statista Market Insights; Statista Technology Market Insights; FBI; IMF; Statista
© Statista 2024

Additional Information:
Worldwide; Statista Technology Market Insights; IMF; Statista Market Insights; FBI; 2016 to 2023

In summary, security is more important and needed than ever. It not only protects our data from being stolen but also prevents financial losses and helps maintain the trust of others, etc.

Security Concept in Development

The next topic we'll be talking about is the security concept in development.

In software development, security refers to a sequence of protocols to ensure our application and database is safe.

In order to achieve that, developers need to know and follow these concepts:

- Data encryption: Sensitive data like bank account, password, etc. needs to be encrypted.
- Input validation: Preventing attacks by validating user input.
- Authentication: Ensuring that only verified users can access the system, and only to the resources they are allowed to see.

By applying these principles, developers can build more reliable and secure applications that protect users and data from cyber threats. However, even if the software did follow these principles and seems safe, developers need to follow the trends and evolution of cyberattacks to implement countermeasures.

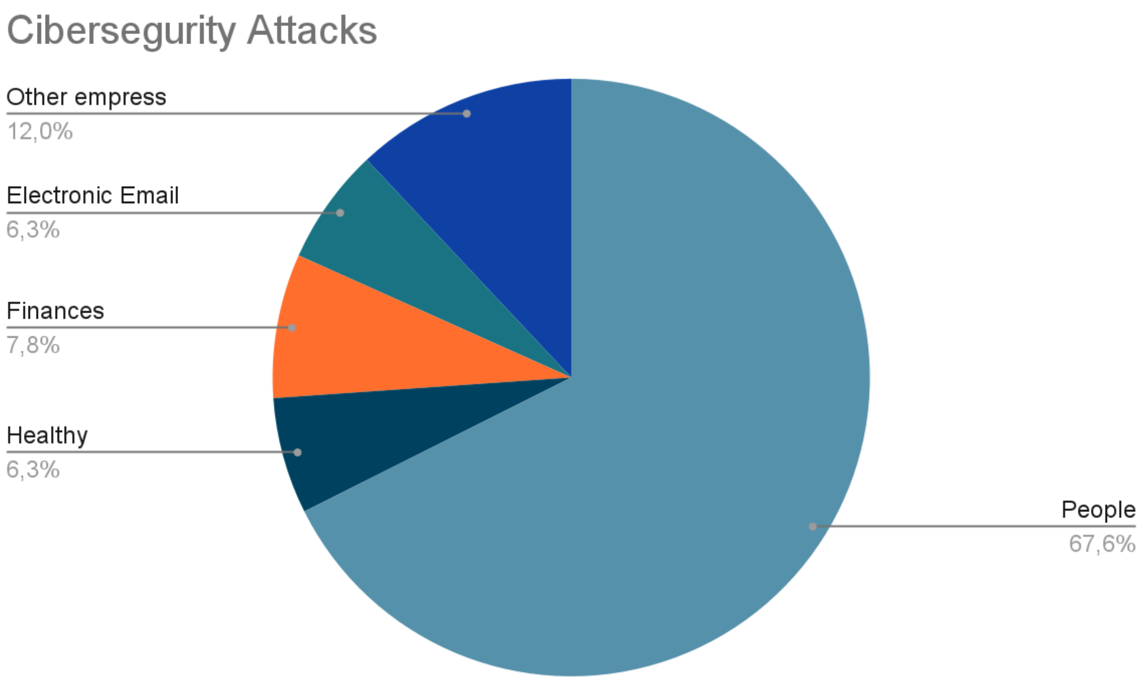
The Current Threat Landscape

a) Diego

The reality of data exposure
What is data exposure? Is it unusual that people suffer from such problems?

In today's digital world, data exposure has become a common and serious problem for individuals, companies, and governments. It happens when sensitive or confidential information becomes accessible to unauthorized parties, either through cyberattacks or simple human mistakes.

With so much personal data stored online, from bank details to social media profiles, the risk of exposure keeps growing. Even organizations with strong cybersecurity measures can experience breaches, showing that no system is completely safe.



Causes of Data Exposure

1. **Cyberattacks and Hacking Attempts**
   Malicious hackers often exploit vulnerabilities in software or systems to gain access to sensitive data. Phishing, ransomware, and malware attacks are among the most common tactics used to steal personal and financial information.

2. **Human Errors or Misuse of Information**
   Not all data breaches are the result of criminal activity. Sometimes, simple mistakes such as sending confidential files to the wrong recipient, using weak passwords, or losing unencrypted devices can lead to serious exposure of private data.

3. **Businesses Storing or Mishandling Personal Data**
   Many companies collect large amounts of customer data for marketing or operational purposes. However, when these organizations fail to secure this information properly, they put users at risk. Poor storage practices, outdated security systems, or negligent handling of data can easily result in leaks.

Damages Caused by Data Exposure

1. **Theft of Personal Data or Identity**
   Once personal information such as social security numbers, bank details, or login credentials are exposed, cybercriminals can use them to commit identity theft or

financial fraud.

2. **Loss of Trust in the Affected Business**
   When a company suffers a data breach, it often loses the trust of its customers and partners. Rebuilding credibility can take years, and some businesses never fully recover from the reputational damage.

3. **Legal Consequences for Both Businesses and Individuals**
   Depending on the nature of the exposure and local privacy laws, affected companies may face heavy fines, lawsuits, or regulatory penalties. Individuals responsible for mishandling data may also be held accountable.

b) Enrique

Common Threats in Web and Mobile Apps

- Brief overview of the growing importance of web and mobile applications.

- Mention the increasing number of cyberattacks targeting these platforms.

- Purpose: to identify and understand the most common threats.

  Web and mobile applications are amongst the most commonly used technologies by businesses, organizations, and individuals today. They have made accessing essential functions, such as communication, healthcare, education, and banking, extremely convenient. Given the increasing usage of these technologies, there has been a parallel increase in the number of cyberattacks launched against these technologies. In cyberattacks, hackers take advantage of vulnerabilities in web and mobile applications to steal data, disrupt services, or gain unauthorized access to sensitive information. The growing threat landscape highlights the need to discover, and understand, the most prevalent security threats to web and mobile technologies so that developers and organizations can develop adequate protective measures.

Hackers

- Define what a hacker is: an individual who explores, manipulates, or exploits systems for various purposes.

- Explain that not all hackers are malicious motivations vary widely.

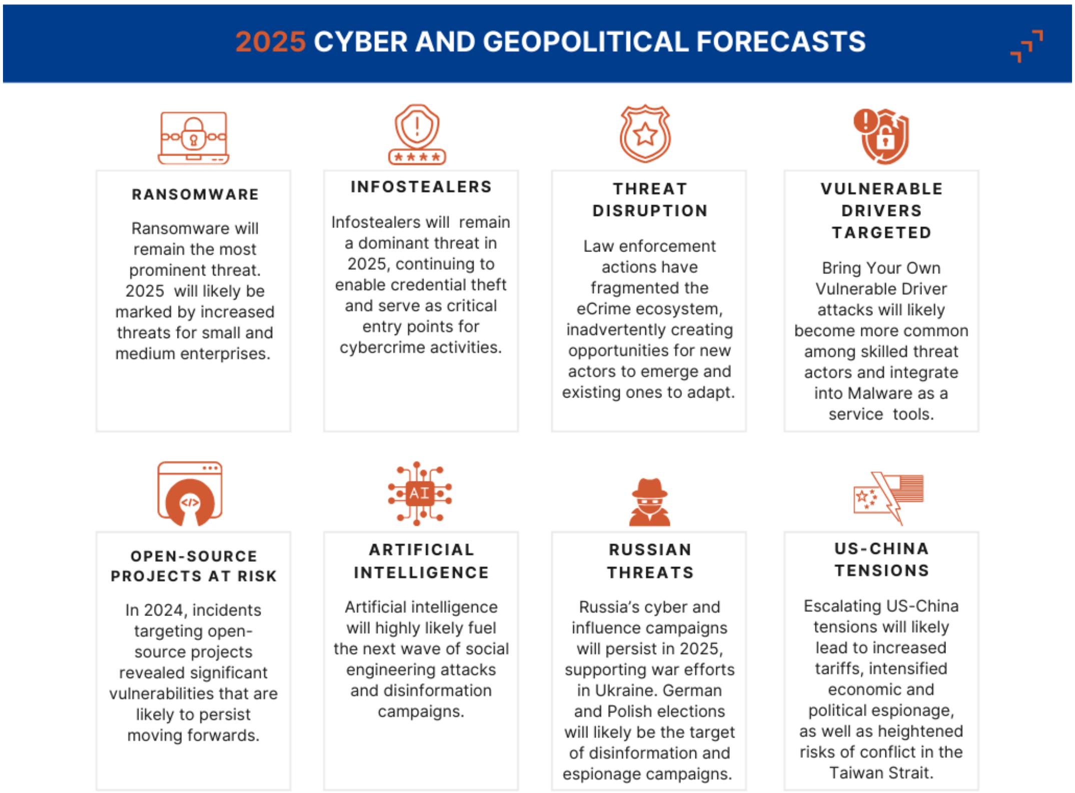
- Introduce the main categories of hacker motivations.

A hacker is an individual who studies, alters, or takes advantage of computer systems and networks in order to better understand the way they function or to obtain a desired outcome.

It is typically assumed that hackers are always evil and commit criminal acts, but there are many reasons people choose to hack, such as attention or curiosity, to learn more about computers, as a form of rebellion or activism against authority and/or for financial gain.

Generally speaking, hackers are categorized in line with their intent and their commitment to ethics. White-hat hackers are individuals who use their hacking for the benefit of security. They do this by looking for vulnerabilities that need to be patched. Black-hat hackers misuse vulnerabilities for their benefit, usually at the expense of others. Black-hat hackers may commit data theft, initiate breach of system integrity, or impede online service. Grey-hat hackers fall somewhere in between. They may violate laws or access networks without permission, however they don't generally have malicious intent, and sometimes they are acting in the public interest, by bringing attention to a security defect that can be patched.

Recognizing the different motivations is critical to developing appropriate defenses and cybersecurity defenses as well as understanding the vulnerability landscape.



2025 CYBER AND GEOPOLITICAL FORECASTS

RANSOMWARE

Ransomware will remain the most prominent threat. 2025 will likely be marked by increased threats for small and medium enterprises.

INFOSTEALERS

Infostealers will remain a dominant threat in 2025, continuing to enable credential theft and serve as critical entry points for cybercrime activities.

THREAT DISRUPTION

Law enforcement actions have fragmented the eCrime ecosystem, inadvertently creating opportunities for new actors to emerge and existing ones to adapt.

VULNERABLE DRIVERS TARGETED

Bring Your Own Vulnerable Driver attacks will likely become more common among skilled threat actors and integrate into Malware as a service tools.

OPEN-SOURCE PROJECTS AT RISK

In 2024, incidents targeting open-source projects revealed significant vulnerabilities that are likely to persist moving forwards.

ARTIFICIAL INTELLIGENCE

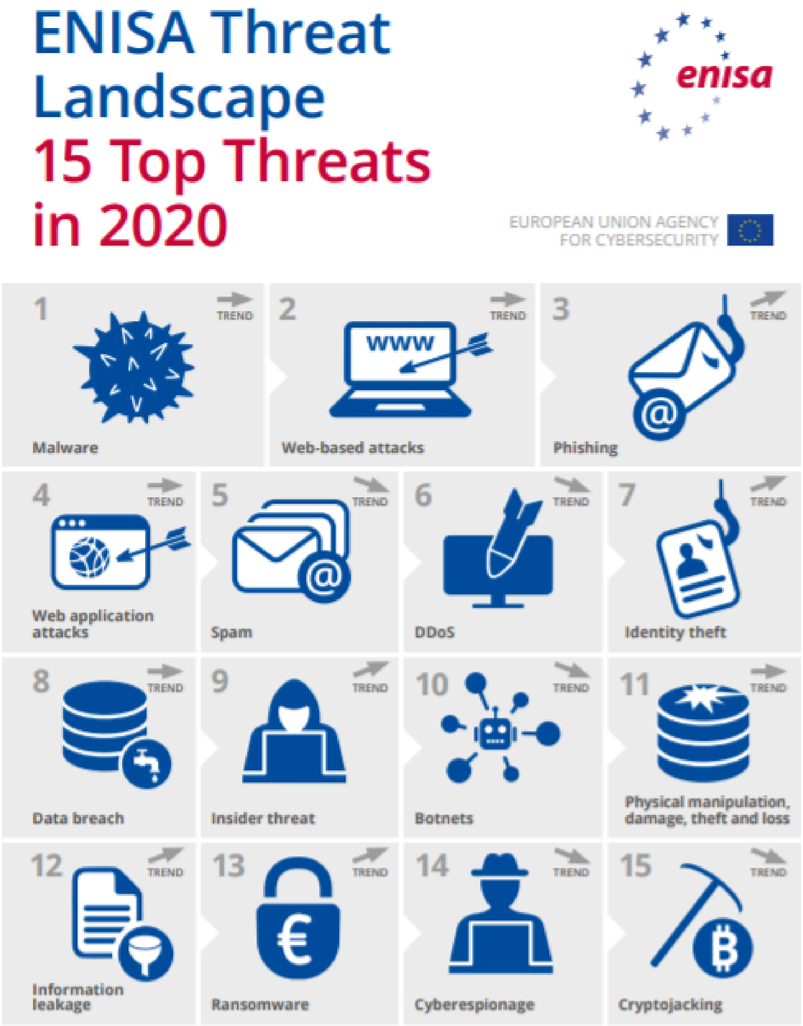
Artificial intelligence will highly likely fuel the next wave of social engineering attacks and disinformation campaigns.

RUSSIAN THREATS

Russia's cyber and influence campaigns will persist in 2025, supporting war efforts in Ukraine. German and Polish elections will likely be the target of disinformation and espionage campaigns.

US-CHINA TENSIONS

Escalating US-China tensions will likely lead to increased tariffs, intensified economic and political espionage, as well as heightened risks of conflict in the Taiwan Strait.



ENISA Threat Landscape
15 Top Threats
in 2020

enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

1 Malware

2 Web-based attacks

3 Phishing

4 Web application attacks

5 Spam

6 DDoS

7 Identity theft

8 Data breach

9 Insider threat

10 Botnets

11 Physical manipulation, damage, theft and loss

12 Information leakage

13 Ransomware

14 Cyberespionage

15 Cryptojacking

Implementing Security Measures (Sonia)

Finally, I will explain how to implement security measures using three key main areas.

A. Basic Security You Should Have

Good habits when writing code (making the program):

1. **Check what users type (Validate User Input):** Don’t trust what people write in forms (like name, email, etc.) because someone might try to do harm.
   - *Example:* We must **sanitize** data to prevent **injection attacks**, which are common flaws.
2. **Safe passwords (Secure Storage):** Store passwords in a secure way, using special tools that “scramble” them so they can’t be read easily.
   - *Example:* We should always use **hashing algorithms** like bcrypt to protect passwords.
3. **Use safe and updated programs (Dependency Management):** If you use parts of other programs (called libraries), make sure they are updated. Old ones may have problems or be unsafe.
   - *Example:* We must **patch** all **third-party libraries** regularly to **mitigate** known **vulnerabilities**.

B. How Long Does Security Last?

1. **Security never ends (Continuous Process):** It’s not something you do only once. You always have to check and improve it, making it part of the **SDLC** (Software Development Life Cycle).
2. **Fixes and updates (Prompt Patching):** New problems come up all the time. It’s very important to install security updates as soon as they are available.
   - *Example:* This process is critical for handling **zero-day vulnerabilities** that hackers discover.
3. **Security tests (Pentesting):** Do tests pretending to be a hacker, so you can find problems before bad people do.
   - *Example:* **Penetration testing** helps us find the most critical security flaws in the application.

C. Privacy Laws and Rules (Legal Compliance)

1. **Tell users what happens with their data (Transparency):** You must clearly explain what information you collect, why you collect it, and how long you keep it. This is part of laws like **GDPR** in Europe.
2. **Right to delete data (Data Subject Rights):** People can ask to have their information deleted (**Right to Erasure**) or to receive a copy of it (**Data Portability**).

3. **Person responsible for data protection (DPO):** Some companies need to have someone in charge of keeping information safe (called a **Data Protection Officer** or **DPO**).

And that covers our three areas of security implementation. That concludes my section. Now, I'll hand it over to Diego for the conclusion.

Conclusion

To sum up, security in application development is not just something extra. It's something essential. It helps protect our data, keeps users' trust, and makes sure our systems work safely.

In summary, we started by learning what security means and why it's so important today. Then, we looked at the current threats, like data exposure and cyberattacks, and how they can affect people and companies. Finally, we talked about how to apply good security measures such as writing safe code, keeping systems updated, and following privacy laws.

To conclude, security is a continuous process. Developers need to think about it from the very beginning and always stay alert to new risks. By doing this, we can build safer and more reliable applications for everyone.

BIBLIOGRAPHY

https://www.qualisys.es/seguridad-informatica-en-el-desarrollo-de-software-protege-tus-aplicaciones/
https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/?srsltid=AfmBOopt5uWaymH9QKqIWn5MqFSeIJI_nTZ4xZ1XpHxXq9Z1z4KCeStn
https://www.cyberseek.org/heatmap.html
https://www.statista.com/forecasts/1485031/cyberattacks-annual-worldwide
https://www.invicti.com/blog/web-security/7-principles-of-secure-design-in-software-development-security
https://www.securitycompass.com/blog/what-is-secure-development
https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape