

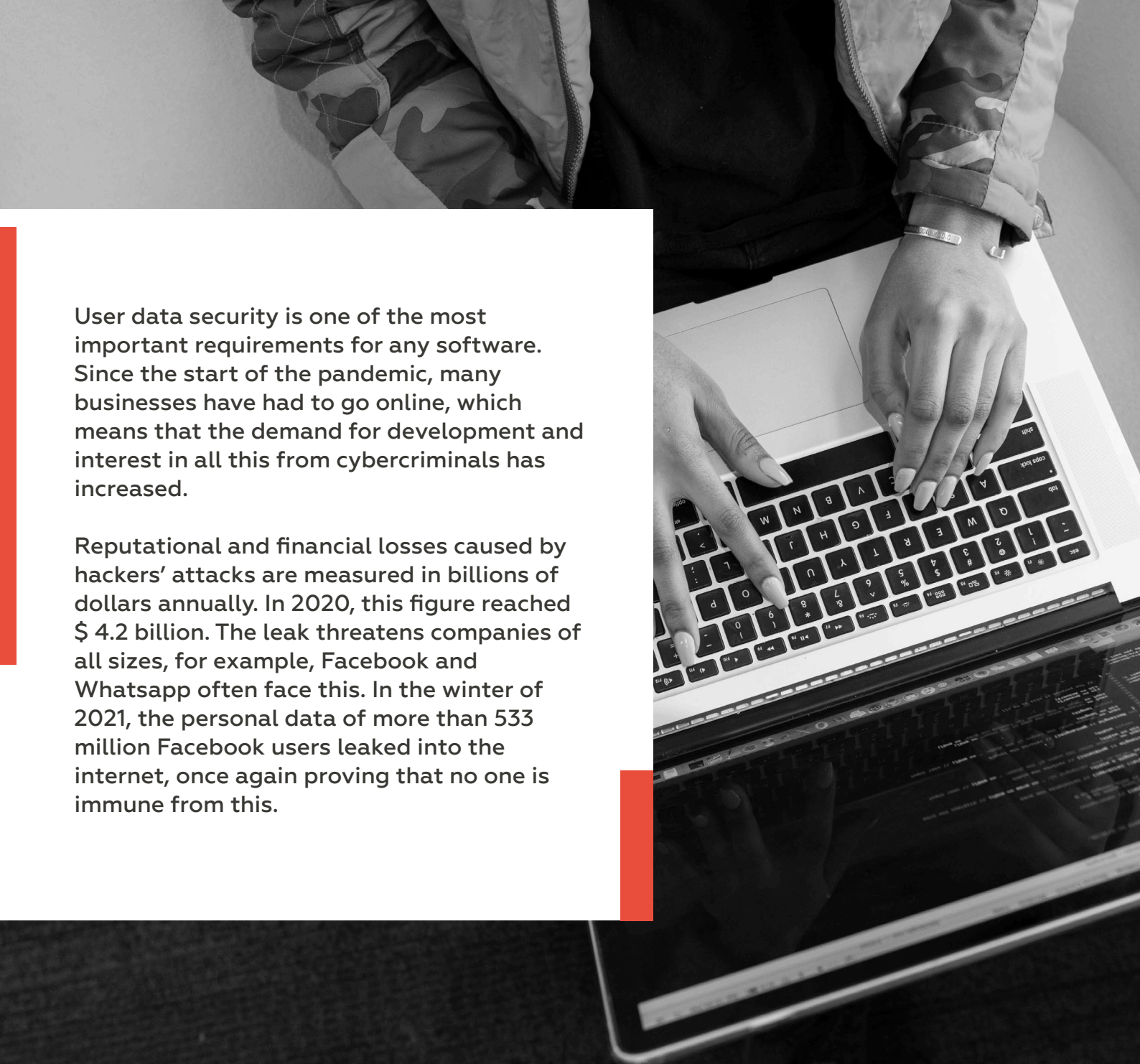


# DATA SECURITY:

## CORE TECHNOLOGIES TO PROTECT DATA IN YOUR ORGANIZATION

---

- How to properly consider security risks in development?
- HTTPS and it's progressiveness
- End-to-end encryption and its applications
- The Diffie-Hellman algorithm
- Using NaCl
- Crunch Data Security
- Technologies



User data security is one of the most important requirements for any software. Since the start of the pandemic, many businesses have had to go online, which means that the demand for development and interest in all this from cybercriminals has increased.

Reputational and financial losses caused by hackers' attacks are measured in billions of dollars annually. In 2020, this figure reached \$ 4.2 billion. The leak threatens companies of all sizes, for example, Facebook and Whatsapp often face this. In the winter of 2021, the personal data of more than 533 million Facebook users leaked into the internet, once again proving that no one is immune from this.



**TODAY, THERE ARE SEVERAL MAIN WAYS TO ENSURE DATA SECURITY. LET'S LEARN THEIR MAIN FEATURES.**

# HOW TO PROPERLY CONSIDER **SECURITY** **RISKS** IN DEVELOPMENT?

Development should always consider potential risks and model threats in the early development stages. There is a certain step-by-step risk assessment strategy, following which you can clearly understand which risks can be ignored and which are critical.

01

Determine the risk

02

Estimate the likelihood of the risk occurring

03

Evaluate the impact of risk on processes and reputation.

04

Assess the severity of the risks

05

Determine how and what can be fixed

06

Customize your risk management model

AFTER GOING THROUGH ALL THESE STEPS, YOU CAN MOVE ON TO **HTTPS CHECKS AND DATA ENCRYPTION.**

# HTTPS

## AND IT'S PROGRESSIVENESS

**HTTPS (SECURE HYPERTEXT TRANSFER PROTOCOL) IS AN ADVANCED AND MORE RELIABLE ALTERNATIVE TO HTTP. THE PROTOCOL PERFECTLY COPE WITH THE TASKS OF SITES THAT ACCEPT ONLINE PAYMENTS.**

One of the features of HTTPS is fast and clear redirects. Since this protocol is normal HTTP over TLS or SSL, even entering `http: //` will redirect you to a secure encrypted `https: //` connection.

In short, HTTPS uses public and private key cryptography to encrypt and decrypt, respectively. It is important to note that the keys are randomly generated and stored on your server.

Each browser has its own key certification lists. In the address bar, this is indicated by a green padlock, which certifies the power of attorney and ownership of the browser.

# WHAT IS THE ROLE OF TLS / SSL IN DATA PROTECTION?

Data interception occurs by intercepting the HTTP session cookie. Encryption methods like WPA allow hackers to act as an authenticated user, while TLS / SSL can provide protection against such outside interference and even guarantee the security of microservices' connections to databases and load balancers.

The same situation with data occurs in mobile applications, where the rejection of SSL leads to the transmission of unprotected data over the network for verification.

But it's important to remember that HTTPS is only part of the cryptographic puzzle. It does not encrypt data at rest and does not control what happens after the HTTPS connection is broken. That is, if the services for processing or any other are in different places, even if the web API endpoint is your service, you will not be able to confirm the encryption of the data and this will give vulnerability.



**This vulnerability can only be avoided with end-to-end encryption.**

# END-TO-END ENCRYPTION AND ITS APPLICATIONS

It is the most reliable data encryption system today, as it allows you to encrypt data at both ends of the conversation. This excludes intervening at intermediate stages and theft of information, since only the sender and the recipient have the private key.

Most of the systems we use all the time, such as e-mail services and online chats, most often go through the company's servers. This approach gives rise to a possible hacker attack.

“

*That is, in fact, encryption and decryption take place on the devices of two users, and the service provider's server works only for data transmission.*



Today, asymmetric encryption is increasingly working, which has improved the essence of end-to-end encryption. In this case, a key pair is used: the sender's public key and the recipient's private key. Despite the fact that the message may pass through several messenger servers along the way, the cipher text remains private for everyone except the recipient with the key.



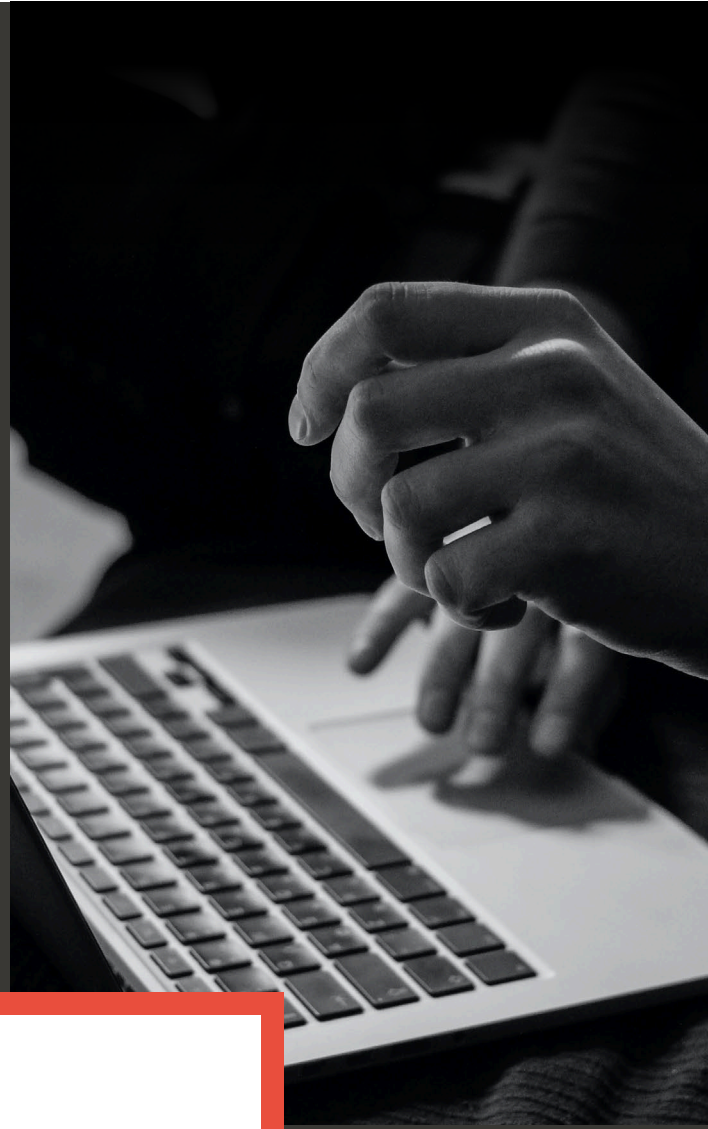
## HOW ARE THE KEYS THEMSELVES GENERATED?

- Initiating chat generation
- Key generation and

End-to-end encryption is relevant not only for chats, but also for e-mails and online banking.

Speaking of the latter, all the data entered by the user remains encrypted until it enters the acquirer or payment processor. For example, the PayPal payment system not only monitors all transactions around the clock, but also encrypts the buyer's card information from the merchant when using the PayPal storage API.

One of the main issues of end-to-end encryption is ensuring a high level of digital privacy.



THIS IS WHERE THE **DIFFIE-HELLM ALGORITHM** COMES TO THE RESCUE, WHICH PROVIDES A SECURE CHANNEL.

# THE DIFFIE-HELLMAN ALGORITHM

How does the Diffie-Hellman algorithm improve the security of key exchange? The Diffie-Hellman algorithm is one of the first successful implementations of asymmetric keys to address the issue of key exchange security.

The Diffie-Hellman algorithm is just about creating a secure channel for transmitting such a key.



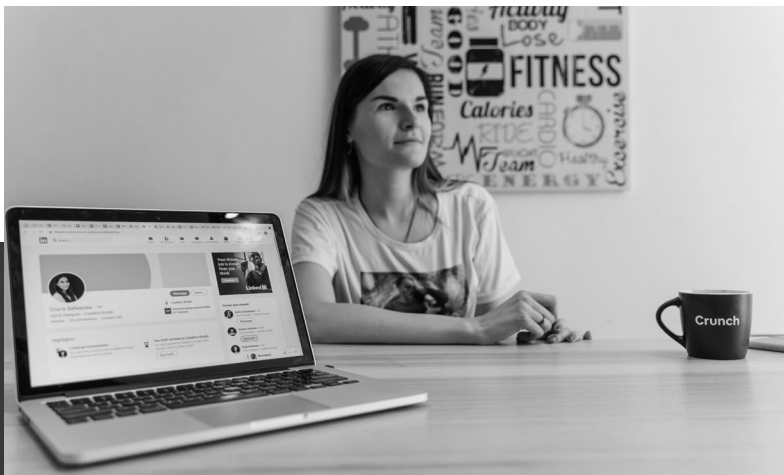
DIFFIE-HELLMAN WORKS  
ON THE PRINCIPLE OF  
INCOMPLETE ENCRYPTION  
KEY EXCHANGE OVER THE  
NETWORK.



Each party has a public key (which can be seen by everyone, including the hacker) and a private key (only the computer user can see it). User A does not have access to B's private key, and vice versa.



# USING NaCl



WITH NaCl, YOU GET ALL THE OPERATIONS YOU NEED TO CREATE THE BEST CRYPTOGRAPHIC TOOLS.

The Native Client is a technology that allows machine code to execute directly in the browser, transparently and securely. With the release of the updated SDK for Native Client, it is possible to make a big move towards making Native Client modules as portable and secure as JavaScript.

In addition, NaCl prevents secrets from flowing to the instruction pointer and branch predictor, which works well for high-speed computing. It also avoids the transfer of secret data to addresses stored in the cache, which is also often a vulnerability for hacker attacks.

NaCl has no dynamic memory allocation or any copyright restrictions. It is important to distinguish between the rules for how NaCl works in C languages and, for example, Python. In the first case, small stacks are used, which are measured by separate tests.



# CRUNCH DATA SECURITY TECHNOLOGIES



AT CRUNCH WE USE ALL OF THE TECHNOLOGIES LISTED ABOVE, CLOSELY MONITORING TRENDS AND INNOVATIVE SOLUTIONS IN THIS AREA.

For example, to ensure security in group chats, we use key generation and exchange, as well as an integrated approach to ensuring the security of data on the project.

The Diffie-Hellman algorithm and Curve25519 elliptic curve help with this. Such a secret key can be used both to encrypt further exchange and to generate a new key, which can then be used for subsequent exchange of information using symmetric encryption algorithms.

In each case, we use an individual approach to ensure data protection. Sometimes it may be necessary to combine encryption methods with restricting access by roles.



# INSTEAD OF CONCLUSIONS



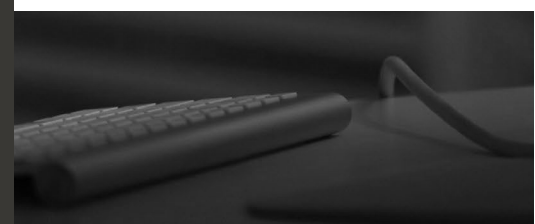
Cryptographic standards are considered to be the main solution to the data security issue today. Their relevance is still at the level, and this trend will continue in the next 6+ years.

Most of the data encryption requirements are documented in NIST. There are also native solutions and built-in cryptographic mechanisms.

Data security is a must for every company. This is the only way to retain customers and maintain a reputation. Need a skilled and trustworthy vendor to create a highly-secured digital product? Crunch expert team is at your service.

NEED A SKILLED AND TRUSTWORTHY  
VENDOR TO CREATE A HIGHLY-SECURED  
DIGITAL PRODUCT?

**CRUNCH EXPERT TEAM IS AT YOUR SERVICE.**





Crunch is a trusted digital solutions company for the world's leading enterprises and startups. We bring together the best engineering talent and wide technological expertise to empower digital transformation while meeting all the business needs of every customer. Our development and management team is 80% Senior and Middle specialists, so you can be sure to have your project delivered on time and within the budget.



Come over for a chat!  
Feel free to [contact us](#) at any time that works for you.

**MICHAEL PIHOSH**

✉ [michael@crunch.is](mailto:michael@crunch.is)

**in** Mykhailo Pihosh

crunch 