25.06.2021

2021 ISOC Fundamentals

Webinar

Internet Society
Serbia Belgrade
Chapter

Predrag Tasevski
SME Cybersecurity

About me

Work:
- Information Security Officer
- Head of IT Security
- Cloud Security Advisor …

Education:
- MSc in Cyber Security, Estonia
- Post-Master in Security in Computer Systems and Communications, France

Membership and Projects:
- Co-founder IGF MKD
- NATO ARW
- SEEDIG
- ICANN Southeast Europe
- DiploFoundation
- Cyber Security Advisor at Kyberturvallisuus RY - Finland Cyber Security Association
- ISOC Member …

More about me: https://predragtasevski.com/pages/about.html

Overview

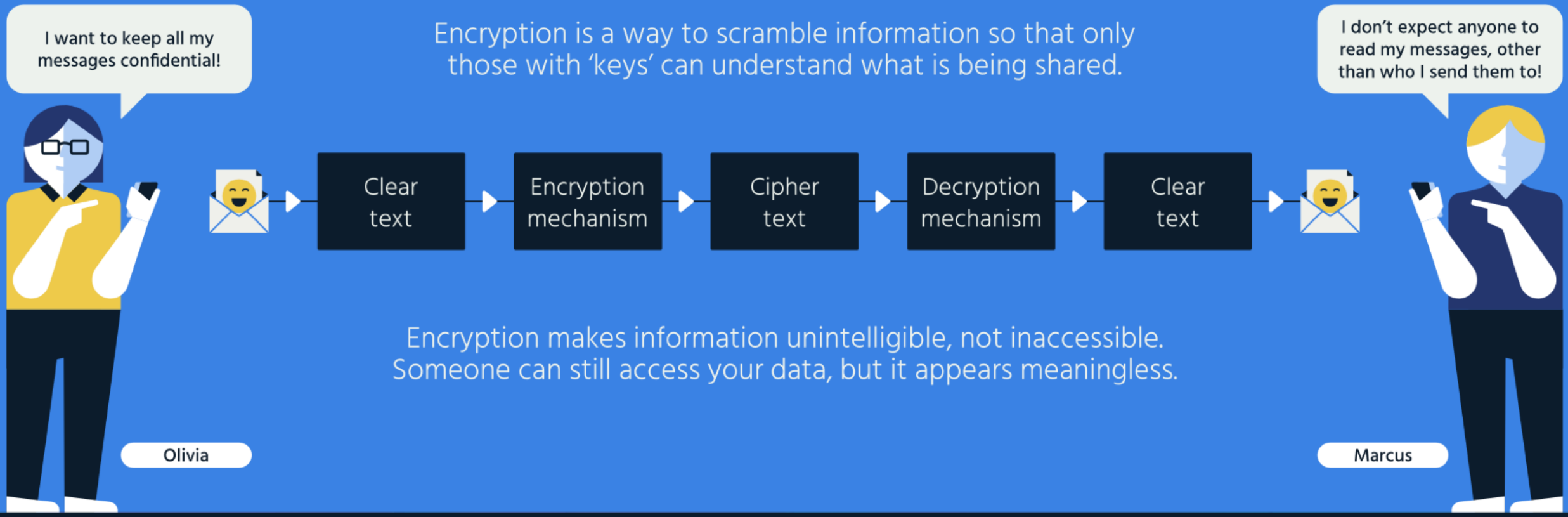
1. Basic encryption and why is it important
2. Basic how to secure webserver using open standards
3. How to build security by default and privacy by default infrastructure
4. Building a bridge between N.Macedonia and Serbia privacy and security community networks.
5. Workshop

1

Basic encryption and why is it important

Encryption

01 What is encryption?



The importance of encryption

In our increasingly digital lives, the role of encryption has never been more essential.

Encryption is a crucial feature of a safe Internet. It ensures your private messages stay private.

From video calls to air traffic control and e-voting, encryption is vital for securing all aspects of our lives.

It keeps your identity safe and stops people from impersonating you, or the people that you trust.

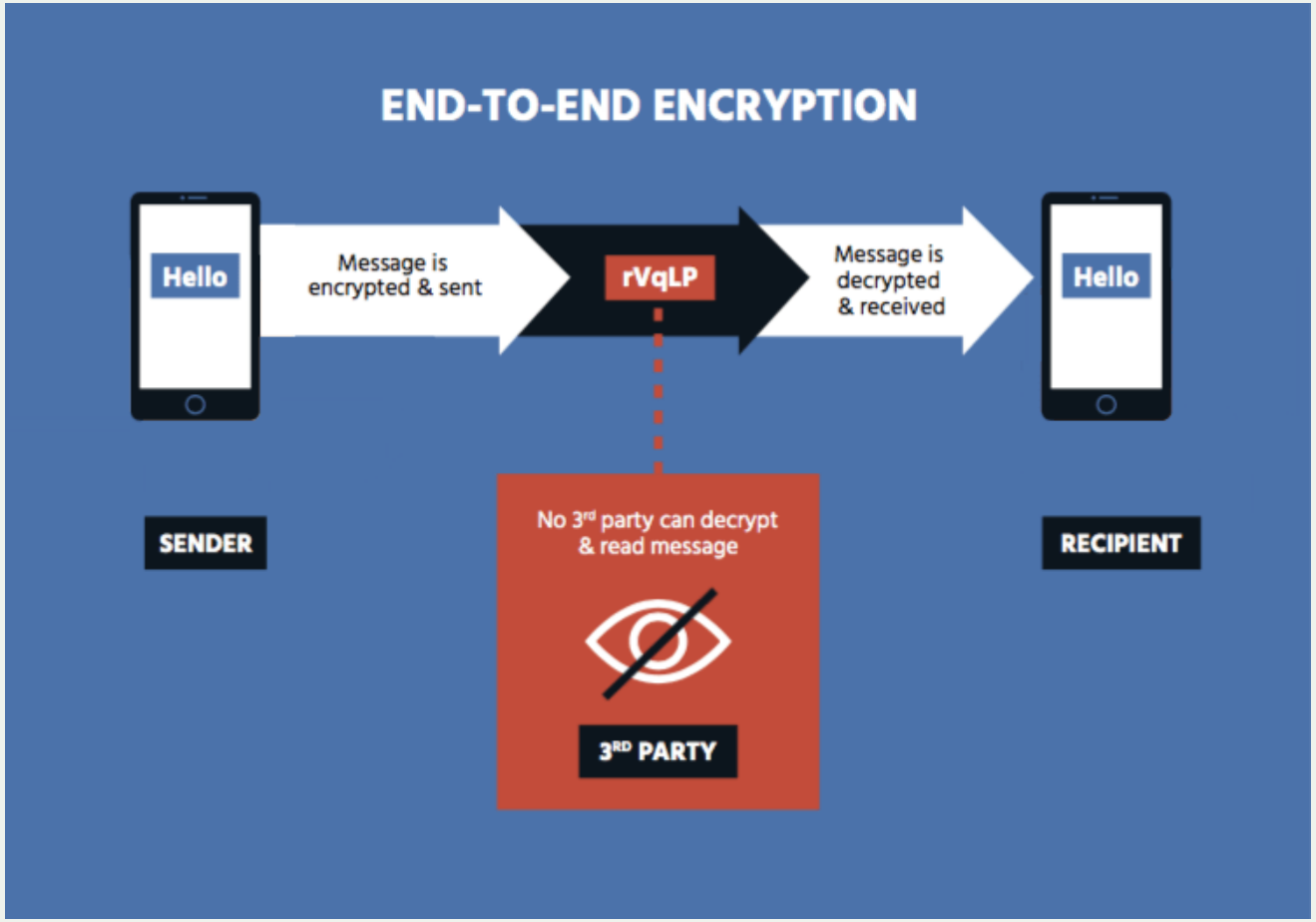
It is critical to national security, protecting society from terrorists, criminals, and hostile governments.

Personal security depends on encryption. It keeps your confidential data out of the hands of criminals.

End-To-End Encryption (E2E)

End-to-end (E2E) encryption is any form of encryption in which only the sender and intended recipient hold the keys to decrypt the message.

- What is Exceptional Access?
- Why Exceptional Access?
- Problems with Exceptional Access



2

Basic how to secure webserver using open standards

Open Standards Everywhere

Open standards are a fundamental building block of an open Internet

IP TCP UDP HTTP(S)
SSH TLS SMTP FTP
QUIC NTP XMPP
DNS BGP SNMP
WebRTC SIP

Open Internet standards are…

… open to all to read/access

… open to all to create

… open / free to all to use

Open

- Based on agreed-upon, voluntary standards that anyone can use to connect with other systems

Globally-connected

- IPv6 – Native connections for new networks (especially mobile)
- HTTP/2 – Faster connections work better for low bandwidth, mobile

Secure and trustworthy

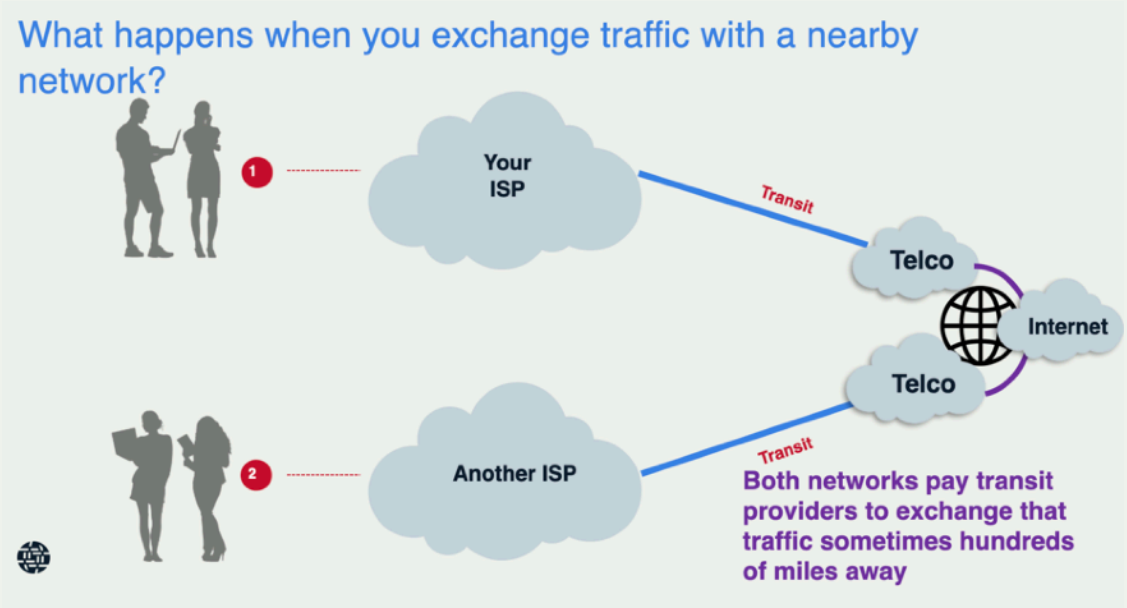
- DNSSEC
- TLS 1.3, HSTS, and more

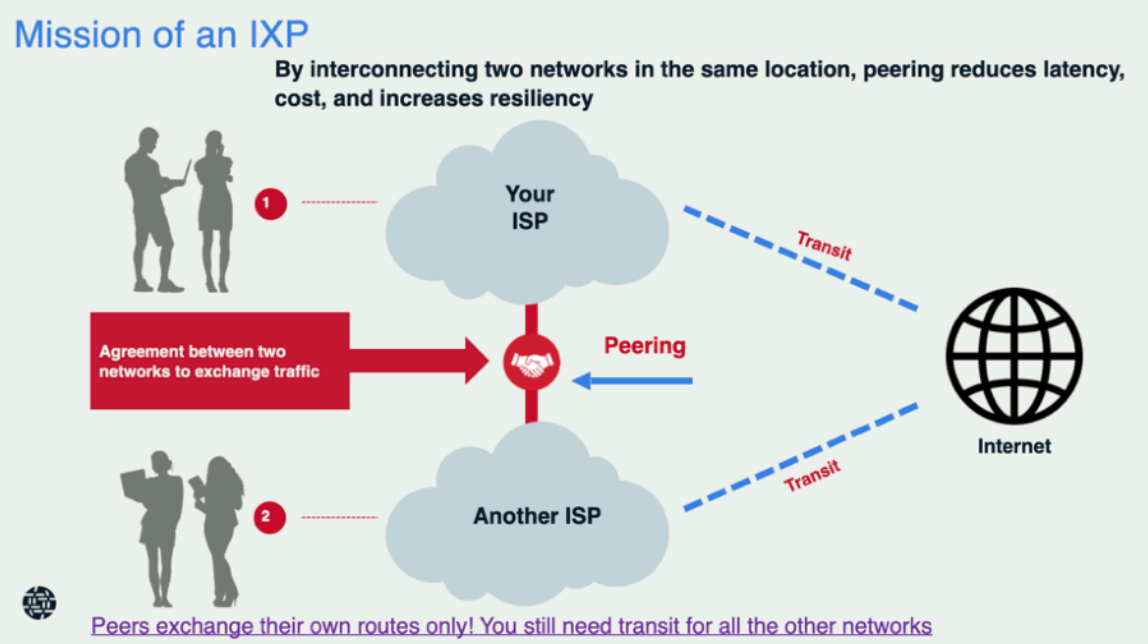
How to build security by default and privacy by default infrastructure

Infrastructure and Community Development

Internet Exchange Points (IXPs)

- What is an IXP?
- Physical locations where different networks connect to exchange Internet traffic via a common switching infrastructure;
- Usually dispersed across countries to enable local networks to efficiently exchange information, thus eliminating the need to exchange local Internet traffic via expensive international links; and
- A vital way to increase the affordability and quality of connectivity in local communities.





The benefits of IXPs

IXPs can be instrumental in developing the local Internet ecosystem because they…

- Lower Internet access costs for end-users,
- Encourage the development of local and regional communications infrastructure,
- Are not expensive to start,
- Build a community of technical experts,
- Attract a variety of other services,
- Incentivise the creation of local content and applications, and
- Facilitate value-added services.

Examples of IXPs

- IXPs Map
- IXP.MK

Link: https://www.datacentermap.com/ixps.html

4

Building a bridge between N.Macedonia and Serbia privacy and security community networks

Community Networks

The Power of Community Networks:Connecting the Unconnected

- ISOC Serbia Belgrade Chapter projects
  - Bolji vazduh
  - Klimerko
- ISOC.MK

Workshop