OFFICIAL (ISC)² CHAPTER | HELLENIC

24ο Συνέδριο infocom | infocom world 2022 | media

Connect | Educate | Inspire | Secure

What about Secure Communications? Considerations and Solutions

Δημήτριος Γεωργίου MA MSc CISSP CPFA CPSP

CC. SSCP. CISSP. CCSP. CAP. CSSLP. HCISPP.

Δημήτρης Γεωργίου

- Ιδρυτής και Chief Security Officer της Alphabit, Master στην Επιστήμη Πληροφορικής, πιστοποιημένος ειδικός στην Ασφάλεια Πληροφοριών και Τεχνικός Πραγματογνώμων.
- Μέλος του Δ.Σ. του (ISC)² Hellenic Chapter και μέλος στους διεθνείς οργανισμούς BCS, IEEE και ACM.
- Διαθέτει πολυετή εμπειρία στην Πληροφορική και την Κυβερνοασφάλεια με ειδίκευση σε Incident Response και Digital Forensics.
- Υπέρμαχος της Κυβερνοασφάλειας και της ασφάλειας των παιδιών στο διαδίκτυο.

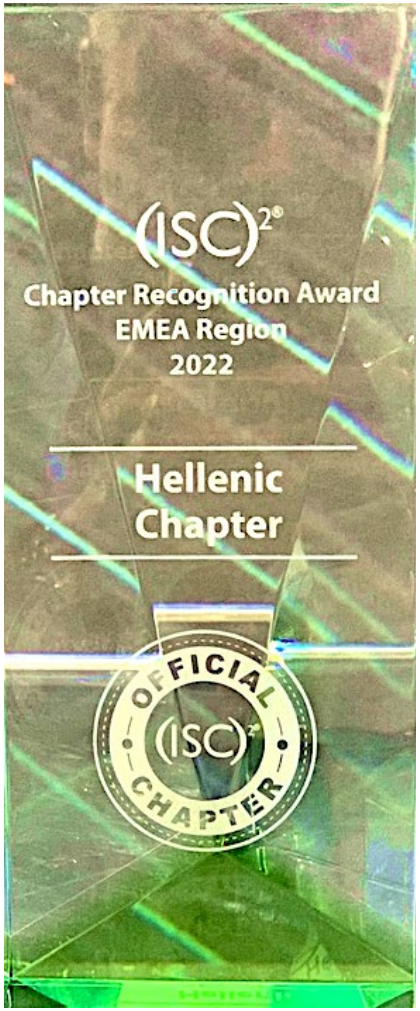
OFFICIAL (ISC)² CHAPTER | HELLENIC

(ISC)²

- International Information Systems Security Certification Consortium, established in 1989
- Non-profit consortium of information security industry leaders
- Supports security professionals throughout their careers
- Global Standard for Information Security: (ISC)² CBK®
- Over 170,000 certified professionals; over 170 countries

(ISC)² Hellenic Chapter

- More than 300 members in Greece, established in 2015



OFFICIAL (ISC)² CHAPTER | HELLENIC

Telecoms? Networks? IT? Content? Convergence!

Multi-play or Unified Communications

- Wired
- Mobile
- Internet
- TV and Radio
- Other services…

Calls? Messaging? Sharing? Collaboration? Social Interaction? Super-convergence!

Multiple possibilities

- Instant messaging
- Photo-Video sharing
- File sharing and storage
- Conferencing and shared screen collaboration
- Social interaction
- Access to user terminals

The traditional landscape

Regulated - Licensed

Publicly licensed wire-line voice/data communications

- Public telephone system (PSTN, ISDN, VoIP)
- Public Internet access (xDSL, FTTH/FTTB)
- Leased data networks (PtP, MPLS)

Publicly licensed wireless voice/data communications

- Public telephone system (2G,3G,4G,5G)
- Public Internet access (2,5G,3G,4G,5G)
- Leased data networks (WiMAX, LMDS, PtP, PtMP)
- Licensed radio communications (VHF/UHF, Tetra, IRIDIUM, etc.)
- Radio/TV

The traditional landscape

Regulated - Unlicensed

Private use unlicensed wire-line networks

- Local area networks (LAN)
- Metropolitan (MAN) and Wide Area Networks (WAN) via Private Virtual Network (VPN)

Private use unlicensed spectrum

- Private voice communications (e.g. CB, PMR, LPD)
- Private wireless networks (WLAN, WMAN)

Legal framework (Greece)

GOVERNING FRAMEWORK:

- Constitutionally guaranteed Communications Security and Privacy
- Governing laws

REGULATORY AND SUPERVISORY BODIES

- Hellenic Telecommunications and Post Commission
- Hellenic Authority for Communication Security and Privacy

ENFORCEMENT AUTHORITIES

- Judiciary / Police / National Intelligence Service

OFFICIAL (ISC)² CHAPTER | HELLENIC

Confidentiality of communication?

a. public communication without technical assurance of confidentiality
b. public communication with a regulatory obligation of technical confidentiality assurance (e.g. physical media protection, encryption, access control etc.)

Communication integrity?

a. communication without technical assurance of integrity
b. communication with a technical obligation to ensure technical integrity (e.g. anti-jamming)

Communication availability?

a. communication without institutional/technical assurance for availability
b. communication with technical assurance of universal access and best effort availability
c. communication with Service Level Agreements to ensure mission critical availability

A Brave New World!

Transcending Boundaries and Regulatory Domains

Considerations

1. Communication no longer denotes exchange of real-time audio or video or simple email. It refers to social interaction with the transmission of recorded audio and video messages, texts, files of all kinds, their storage in potentially unregulated locations and relay to other channels via other routes. It can also mean M2M telemetry or profiling communication.

Considerations

2. Communication can be **opaque**, originate and terminate to uncontrolled endpoints via unknown number of nodes
3. Confidentiality mechanisms and especially **end-to-end encryption** is not always transparent or independently audited and verified
4. There is widespread proliferation of communication and collaboration applications located in jurisdictions and geographic locations far from the users and the protection they enjoy from their local authorities.

Considerations

5. There is widespread proliferation of surveillance applications often hidden behind terms such as "parental control", “find my…” and "fleet management" in official application stores.
6. It is easy to find illegal monitoring and tracking software (spyware, trojans, etc.) on the Dark Web

Considerations

7. Reports of a post-COVID rapid rise in cybercrime and financially motivated cyberattacks are looming
8. There are indications of a rise in industrial and state-sponsored cyber espionage which aims in compromising communications for further exploitation

Considerations

9. There are reports by the press and international NGOs for the development of professional-grade surveillance software for use by law enforcement and intelligence agencies, which is suspected to be used illegally for unsanctioned monitoring.
10. Several cases of illegal interception of communications have been made public

”Modern era communication, collaboration and social networking apps push existing regulatory frameworks and technical control capabilities to their limits”


Solutions

Solutions

A. Institutional:

1. Stricter international oversight on the makers and operators of communication applications and their security and privacy requirements
2. Categorization of privacy-sensitive communication applications for

- *personal use,*
- *business use*
- *government use*

with an easy to understand explanation on the expectation of security and privacy each one offers

Solutions

3. Restriction on the use of unauthorized communication applications (or whitelisting) for specific purposes e.g. government use, use by minors etc.
4. Widening the concept of communication privacy and security to include user terminals as they contain stored communications
5. Use of security by design to all communication apps imposing strict assurance requirements.

Solutions

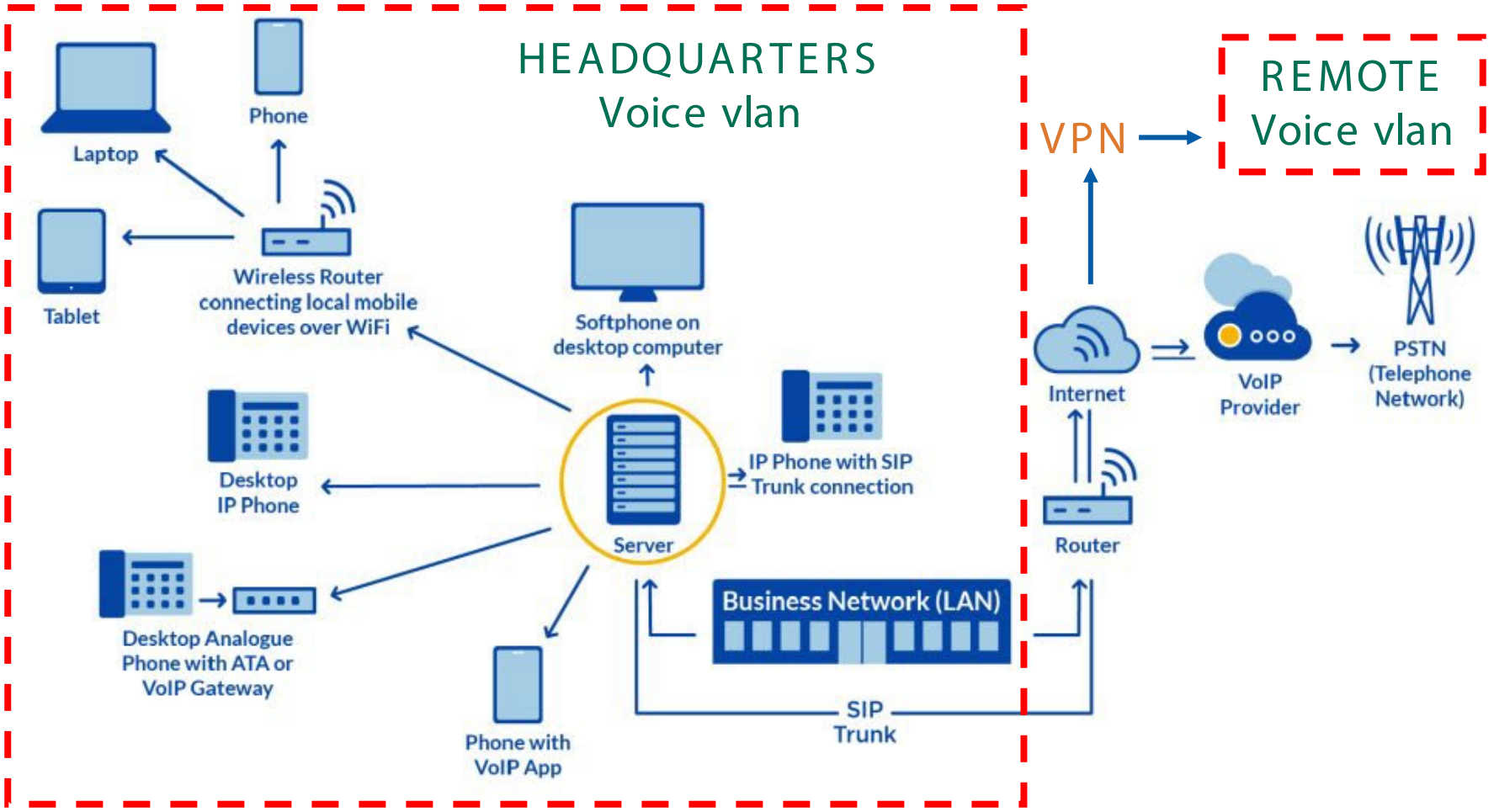
B. Technical

6. Control application access and network-use rights using Zero Trust Architectures
6. Minimize application access permissions on user terminals
7. Use intranets, extranets and VPNs for secure collaboration and communication
8. Minimize the circle of people handling secrets pertaining to the security of communication – use need-to-know and separation of duties.

Solutions

9. Employ industry-standard authentication and encryption mechanisms throughout your communication systems both for administration and service delivery.
10. Segment communication systems from other generic infrastructure.

A private approach to secure communications for the Enterprise



Email: d.georgiou@isc2-chapter.gr, georgiou@alphabit.gr
LinkedIn: https://www.linkedin.com/in/dgeorgiou