This project is co-financed by the European Union
and the Republic of Türkiye

PRESENTER FULL NAME: Dr. ANCA DELIA JURCUT

ORGANIZATION: University College Dublin

WORKSHOP NAME: Digital and Smart Health

E-MAIL: anca.jurcut@ucd.ie

ICTürkiye2025
10 April, İstanbul

UNIVERSITY COLLEGE DUBLIN

Leading Research Excellence
Ranked among Ireland’s top institutions for computer science and innovation.

Interdisciplinary Collaboration:
Strong ties across engineering, business, and industry for real-world impact.

Global Reach & Local Innovation:
Home to international talent and a hub for EU-funded research and cybersecurity.

ICTürkiye2025
10 April, İstanbul

DNS Research Labs

https://dnsresearchlabs.ucd.ie/

Cybersecurity for Constrained Systems

Research on protecting IoT and Industrial embedded systems with real-world constraints

Malware analysis

Conducting in-depth studies to detect and mitigate malicious software threats

IA Data Analytics

Utilizing advanced analytics to interpret complex data patterns in network traffic

Industry Partnerships

Academic Alliances

Government Agencies

AI-Powered Cybersecurity

Blockchain for S&P

Network Monitoring

Threat Detection Systems

ICTürkiye2025
10 April, İstanbul

DNS Lab Research Fields

AI-Driven Cybersecurity
Leveraging artificial intelligence to enhance threat detection and automate responses, thereby increasing accuracy and speed in mitigating cyber threats.

Internet of Things (IoT) Security
Developing robust security frameworks for IoT devices to ensure data integrity and device authentication in interconnected environments.

Blockchain for Security & Privacy
Applying blockchain technology to provide decentralized, tamper-resistant solutions that enhance security and privacy across various domains.

Design & Formal Verification of Security Protocols
Creating and validating quantum-resistant security protocols to ensure robustness against emerging threats, including those posed by quantum computing.

ICTürkiye2025
10 April, İstanbul

DNS Research Lab Projects

Ransomware Detection & Prevention with AI
- Adaptive models to detect evolving ransomware
- Enhance resilience and protection of critical organizational assets

DDoSNet: A Deep Learning Model Against DDoS Attacks in SDNs
- Real-time LSTM-autoencoder IDS protects SDN controllers from DDoS attacks and overload

CMXsafe: IoT Cybersecurity and Network Architectures
- A security proxy layer that enables end-to-end encryption
- Strengthens smart infrastructure security with cloud-ready gateways

MTDS for Multi-Environment Networks
- ML-powered detection of malicious traffic in IoT and SDN networks
- Real-time threat detection across heterogeneous environments

Blockchain for Securing Autonomous Vehicular Networks
- Blockchain to secure V2X communication in autonomous driving
- Real-time threat detection across heterogeneous environments

Blockchain in Healthcare
- Blockchain to manage dynamic patient consent in digital healthcare
- Real-time threat detection across heterogeneous environments

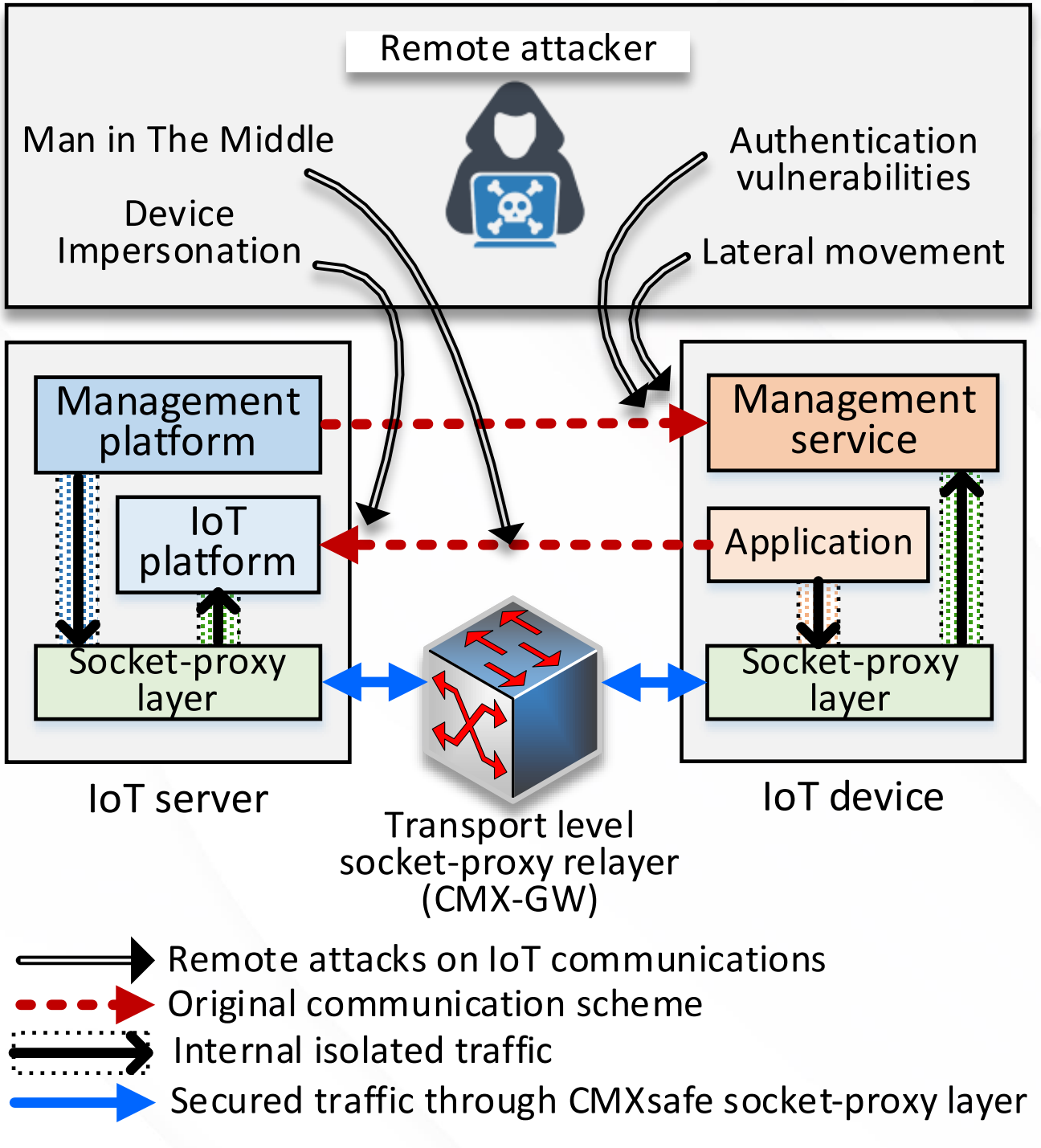
CDVT/AD: Design & Formal Verification of Security Protocols
- Automated tool for logic-based verification of security protocols
- Real-time threat detection across heterogeneous environments

Design of Quantum-Resistant Security Protocols
- Cryptographic protocols resistant to quantum-computing threats
- Ensures long-term security and future-proofs sensitive communications

ICTürkiye2025
10 April, İstanbul

CMXsafe value proposition: Modular IoT Security

- **Modular & SESIP-compliant:** Standards-based design with independent security modules for easy certification and integration
- **Secure for constrained IoT:** Adds mutual authentication and encryption even on microcontrollers like ESP32 with minimal overhead.
- **Regulation-ready:** Aligns with CRA, NIS2, and Zero Trust by enforcing continuous, secure-by-design communication
- **No code changes needed:** Works as an overlay layer. Secures legacy systems without modifying source code or infrastructure



ICTürkiye2025
10 April, İstanbul

Horizon Europe Collaboration
CMXsafe: Secure Interoperability

- **Cross-Partner IoT Security**: Horizon Europe projects often require secure, interoperable communication across diverse IoT systems and organizations
- **CMXsafe as Enabler**: CMXsafe provides a proxy-based security layer with end-to-end encryption and authentication, simplifying development, certification and enabling seamless integration of legacy systems

Industry 4.0 Manufacturing

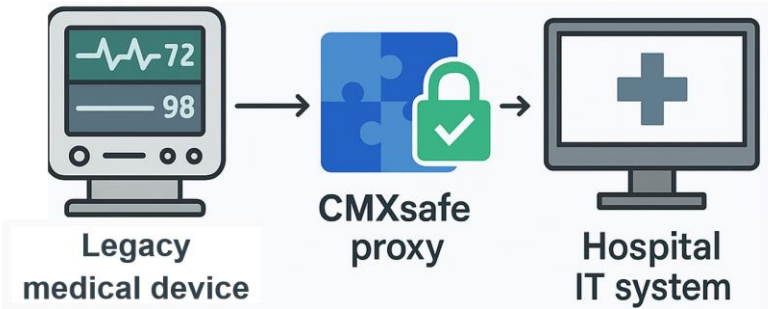
secure, low-latency communication by drop-in proxy layer

Support legacy PLCs, robots, and sensors without firmware changes or hardware replacement.

Healthcare IoT

Mutual authentication and encryption to medical devices

Facilitate regulations compliance thanks to SESIP compliance



Smart Grid

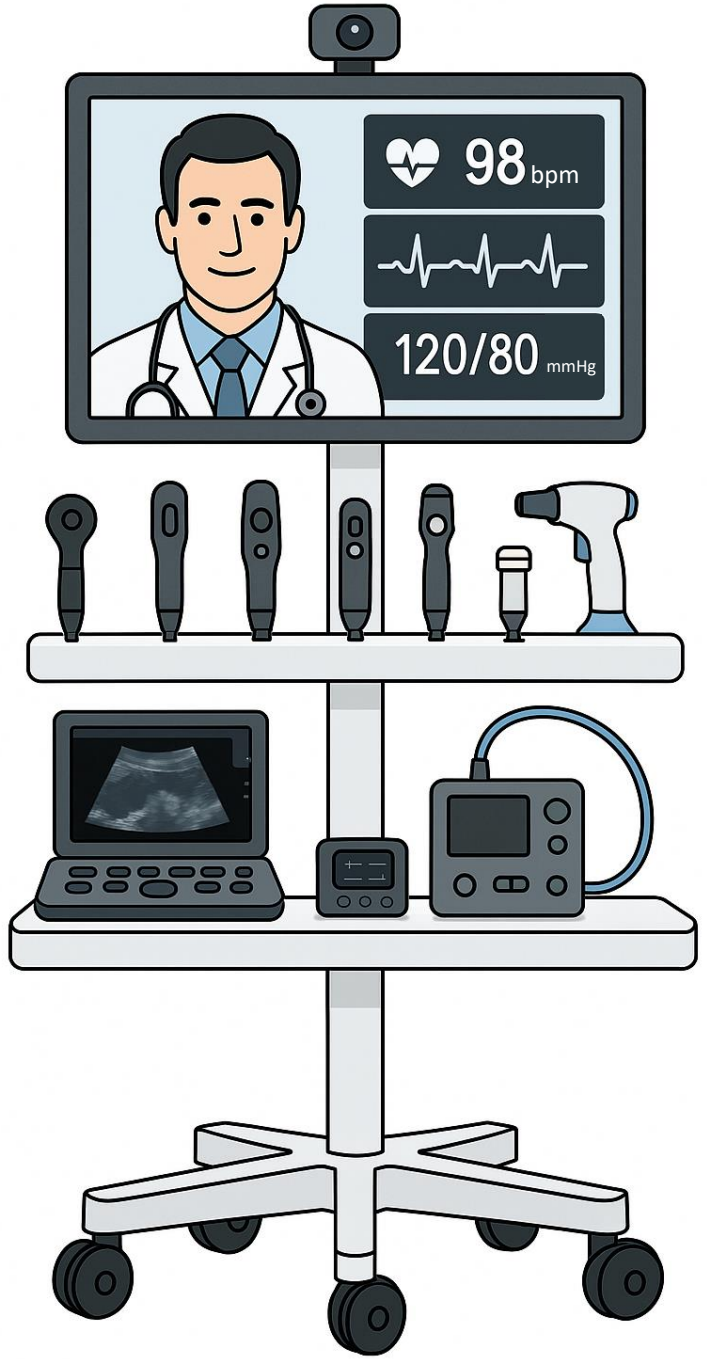
Retrofits legacy power systems with encryption and authentication via transparent proxies

Securing power system protocols without replacing infrastructures

ICTürkiye2025
10 April, İstanbul

Telemedicine example: Cart integration

- **Heterogeneous devices** often of different manufacturers with no built-in security
- **Lack of a unified platform.** Existing middleware may allow extending security features and functionalities, but with vendor lock-in
- **Compliance pressure** CRA, NIS2, ISO/IEC 80001, MDR, HIPAA



CMXSafe

- **Drop-in proxy layer**
- **Secure interoperability**
- **Legacy compatibility**
- **Accelerate certification compliance**
- **Scalable across environments**

ICTürkiye2025
10 April, İstanbul

PRESENTER CONTACT
DETAILS: anca.Jurcut@ucd.ie
COUNTRY: IRELAND,