# SECURITY OF HEALTHCARE SYSTEMS

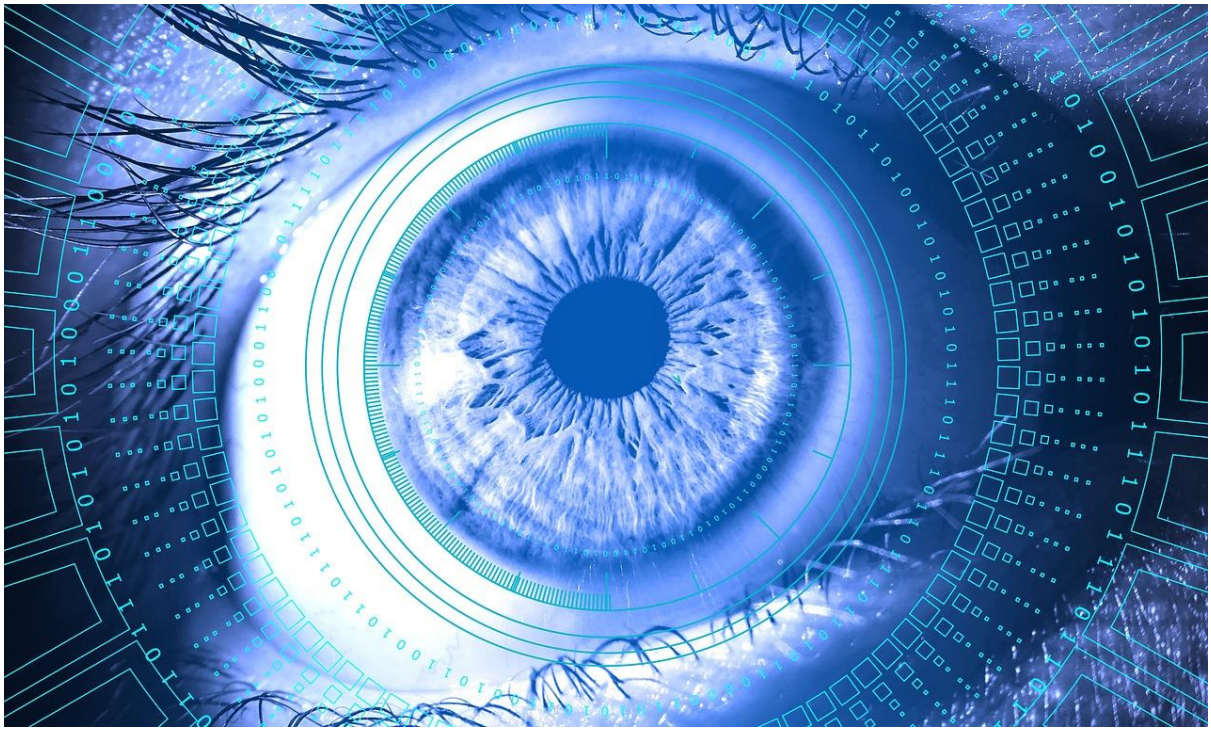

*Image by Pete Linforth from Pixabay*

INCS-CoE held an on-line seminar on the above topic on Tuesday 26 March 2024. We had three speakers whose biographies may be found at the end of this note. All of the speakers agreed that future healthcare delivery systems are likely to be more distributed in the future with a greater need for information sharing between healthcare providers and devices and that this poses significant security and trust challenges.

Emil Lupu opened proceedings by posing the question: how can healthcare be delivered everywhere safely and securely? As Kevin Fu later elaborated, this means that providers must ensure that essential critical functions continue even in the event of a cyber security breach. John Wandelt started his contribution by highlighting the fact that information sharing in such environments require trust and agreement between the sharing parties and posing the challenge that these are hard to scale to real world systems where there are multiple actors.

Emil spoke about integrated healthcare networks and the need for enhanced healthcare records to be shared on a global scale. He highlighted a trend towards the design of bio-degradable devices and asked what security looked like for such resource-constrained devices. He posited a need for new design methodologies that combine safety, security and usability considerations into the design process. He also spoke about the use of artificial intelligence in healthcare systems and the risks that might entail as a consequence of adversarial machine learning. He concluded with some opportunities for re-thinking some of our fundamental concepts to take the human, physical and cyber dimension into account in the medical context.

Kevin cited many examples from the last fifteen or so years, where healthcare systems have been the target of cyber attacks. Particularly chillingly, he reported on transcripts of conversations within hacking groups that had set out to compromise a large number of US hospitals at the height of the Covid pandemic. He demonstrated how critical information is readily retrievable from devices, invariably stored in unencrypted form. He also spoke about recent moves in the US Congress which will see a $1.3billion investment to encourage hospitals to adopt essential and enhanced cybersecurity practices.

John spoke about Trustmarks which have grown out of the White House initiative on trusted identities in cyberspace (NSTIC). A trustmark is a formal statement of conformance to a well-scoped set of requirements and assessment steps. There is an open-source set of tools

available for implementing a trustmark framework. There are well-established case studies in justice and public safety and John reported on some early steps towards employing a trustmark framework in the health sector, both at state, national and global levels.

The key research challenges which emerged during the seminar Included:

1. How can healthcare be delivered safely and securely at the point of need wherever that may be?
2. How can systems be designed and built to ensure that critical functions continue even in the presence of cyber security compromise?
3. How can data minimisation criteria ("need to know") be enforced in a trusted and usable way at scale?
4. What is the right balance between risk and usability in the context of cyber-physical systems in healthcare?
5. How can healthcare be delivered safely and securely when the delivery environment and infrastructure is unknown, underperforming and (partially) untrusted?
6. What does security mean for bio-degradable devices?
7. How does the use of artificial intelligence in healthcare systems impact on the attack surface?
8. Can trustmark frameworks be used to support more agile information sharing environments than those currently proposed at the national (TEFCA) and global levels (WHO)?

More information about the individual presentations and the resulting research questions may be found on the INCS-CoE website (incs-coe.org) or by contacting the speakers. We encourage the community to start conversations which might lead to the solutions of some of these challenges.

# Speakers

## Prof Emil Lupu, Imperial College London

Emil Lupu is Professor of Computer Systems in the Department of Computing at Imperial College London, where he leads the Resilient Information Systems Security Group (rissgroup.org) and a Security Science Fellow with Imperial's Institute for Security Science and Technology. He has made numerous contributions in computer security, network and systems management, IoT systems and software engineering. His current research interests are focussed on the security and resilience of cyber-physical systems to both systems and data spoofing attacks and their ability to continue to operate even when they have been partially compromised.

## Prof Kevin Fu, North-eastern University

Kevin Fu is Professor of Electrical & Computer Engineering, the Khoury College of Computer Sciences, and Bioengineering at Northeastern University in Boston. His research lab focuses on analog cybersecurity—how to model and defend against threats to the physics of computation and sensing. His research led to a decade of revolutionary improvements at medical device manufacturers, global regulators, and international healthcare safety standards bodies. He published widely on medical device security, healthcare ransomware, automobile cybersecurity, RFID security and privacy, secure content distribution, and web security. He served as the inaugural Acting Director of Medical Device Cybersecurity at U.S. FDA's Center for Devices and Radiological Health (CDRH) and Program Director for Cybersecurity at the Digital Health Center of Excellence (DHCoE).

## John Wandelt, Georgia Tech Research Institute

John Wandelt is a Georgia Tech Research Institute Research Fellow and Division Chief for the Trusted Interoperable Systems & Architectures (TISA) Division. He has demonstrated consistent performance in making original and innovative contributions that are widely recognized. Nationally, his vision and leadership has played a significant role in shaping the standards, technologies, architectures, and commercial products that enable secure sharing of information for the justice, public safety, defense, health, and intelligence communities. His work has attracted attention from federal and state

government agencies, national standards committees, commercial vendors, and academic institutions. Today the information sharing standards and products developed by him and his team of researchers enjoys national adoption at the federal, state, and local levels and has been implemented in a wide range of commercial products. Most recently he is spearheading the technical vision and implementation for Georgia's Medicaid Enterprise System Transformation (MEST). This is a highly visible and critical program to the health infrastructure and ecosystem in the state of Georgia with expenditures in the hundreds of millions of dollars and impact to millions of citizens.