EBU
OPERATING EUROVISION AND EURORADIO

# MEDIA CYBER SECURITY SEMINAR 2017

## TUESDAY 21 FEBRUARY 2017

10:20 – 10:30

***Welcome & Introduction***

**S. Fell** is Director of Technology & Innovation for the EBU, a position he took up in September 2013. He has more than 35 years' experience in senior broadcasting technology roles, including at British broadcaster ITV, where he was Director of Future Technologies (2008-2009) and Controller of Emerging Technologies (2004-2006).From 1991 to 2004 Mr Fell worked for Carlton Television, the ITV franchise holder for the London region, where he held several executive roles linked to operations and emerging technologies. Mr Fell, prior to joining the EBU, was Chairman of the Technical Council at the Digital Television Group, the industry association for digital television in the UK. He also represented UK broadcasters on the EBU Technical Committee between 2006 and 2009 ***/***

**A. Kouadio** (EBU)

## SESSION 1 MEDIA SECURITY STANDARDS

10:30 – 11:00

**EBU: Overview of Security standards and best practices for Media companies.**

Introduction to the current state of recommendations provided by the EBU MCS group and plans for further recommendations.

**Andreas Schneider** (SRG/SSR) born and raised in Munich, Germany, entered the field of IT Security at an early stage. Having completed his apprenticeship (System Programmer), he soon was responsible for a regional bank institute's entire mainframe landscape security. He continued specializing in the field of IT Security and IT Risk Management ever since throughout different roles and branches and after more than 10 years of international experience currently holds the position of Chief Information Security Officer (CISO) at SRG SSR, Switzerland's nationwide broadcasting corporation. He further holds several well-respected professional certifications, such as the C-CISO, CISM, CISSP, and is also certified in ISO 27001 as well as ITIL V3. He lives with his wife in Zurich, Switzerland.

11:00 – 11:30

**NABA / UK DPP Security initiative.**

The Digital Production Partnership (DPP) is an international not-for-profit membership organisation that works with the broadcast and media industry to fast track business change. Its members highlighted that security and trust was a major concern for them and in doing so worked with the DPP to develop a user friendly Supplier Security Checklist to be used by consumers and suppliers of connected services.

The DPP also worked with its partner - the North American Broadcasters Association (NABA) and its Broadcaster members to agree a minimum set of cyber security requirements for suppliers. This presentation provides an overview of this work and other initiatives undertaken by the DPP.

**Abdul Hakim** (UK DPP) has over 15 years' experience in the Broadcasting and IT Industry with a comprehensive background in Project Management and Operations at the BBC as well as in the commercial sector. At the DPP he's been managing its work on cyber security, conducting research and has been working on metadata specifications for news exchange.

Previously, Abdul's roles included leading technology at BBC Media Action, the BBCs international development charity, as the Head of Information Systems and Change, where he developed and delivered the global technology strategy and managed operations across Europe, Africa and Asia. He has also worked as a Technology Manager for BBC World Service delivering connectivity solutions for its international bureaus.

11:30 – 12:00

**ISO/IEC – Overview of ISO standard on security**

**Eyal Adar (EIC)**

12:00 – 12:30

**Production migration from SDI to IP**

Users want to benefit from an "all-IP" approach while vendors are concerned about migrating their products. But what will happen about security? Currently we rely on separation between technical facilities and other networks but can/should this still apply with IP? I shall outline the state of the industry on live IP - technologies, techniques and protocols, with an overview of typical security issues that broadcasters face, and identify some of the many areas which will need to be considered.

**Peter Brightwell** is a Lead Engineer at BBC R&D with an extensive background in broadcast and production technology and is helping lead BBC's migration to IP. He is a frequent collaborator on international projects on metadata, media services and networked media. He has been a significant contributor to the industry's JT-NM and EBU's FNS group, and is currently chair of AMWA's Networked Media Incubator, developing the open specifications for networked media.

## SESSION 2: CONTENT AND ASSETS SECURITY

14:15 – 14:45

**Content Piracy: Evolution of threats and distribution methods.**

With the increased availability of high bandwidth connections worldwide the piracy landscape is changing. Previously attacks on broadcast content protection technologies where very expensive perform, today with redistributing content over the internet can be done in an instant and without any deep technological expertise. In this presentation we will explore this evolution and provide some direction for today's content protection.

**&**

An overview on DTV piracy evolution, and necessary 360° approach to protect content.

**José-Emmanuel Pont** (NAGRA, Kudelski Group) leads anti-piracy programs worldwide within NAGRA's Anti-Piracy Group. He has over 15 years of experience in digital tv security and cybersecurity**.**

**&**

**Pierre Sarda** (NAGRA; KUDELSKI) Graduate of 'ISEN' (Lille-1998), held innovation positions at Renault and Philips. Pierre was the key innovator within Medialive, a french start-up developing new means for video protection. Since joining the KUD group, Pierre plays a key role in assimilating new technologies particularly those related to Media & Cybersecurity and incubating innovating products. He is an author of 20+ patents and has lived in France, Germany and Switzerland.

14:45 – 15:00

**Vulnerability investigations in broadcast equipment**

**Adi Kouadio** (EBU)

15:00 – 15:30

**Managed Secure File Ingest & Cleaning Solution**

- Question: How can we verify and guarantee the delivery of "proper" files entering our Company?
- Answer: SRG's "Secure Ingest & Cleaning Solution" protects against "*Malware"*… and other advanced (online) threats that have made Antivirus obsolete and ineffective!
- Way Out: How to get along with "*Malware"* in Media File?

**Martin Jacober** (SRG/SSR) is a well Rounded IT Professional with Expertise in Media, Data & Security - Risk Management and works today as IT Media Specialist for SRG SSR – "Schweizerische Radio- und Fernsehgesellschaft".

The parent company comprises five Enterprise Units: Radiotelevisione svizzera (RSI), Radiotelevisiun Svizra Rumantscha (RTR), Radio Télévision Suisse (RTS), Schweizer Radio und Fernsehen (SRF) and swissinfo.ch (SWI).

Previously he worked for over 2 years for tpc, "tv production ag", a SRG subsidiary, assisting coordination and steering of nationwide projects.

As a MXF and Quality Control Specialist, he was heavily involved to design and implement file based workflows solutions in media production.

Mr. Jacober joined as Media Technology Specialist SRG SSR in 2012 in the Department of “Generaldirektion, Technik und Informatik”.

In this actual role, he oversees design and implementation of SRG’s Reference Architecture, Communications and Security Solutions across Swiss National Broadcast Services. Mr. Jacober also manages affiliate SRG SSR partnerships and related programs for Broadcast Sciences: e.g. @ ARD ZDF Media-Academy, BBC, EBU and IRT.

15:30 – 16:00

**Securing the Internet of Things**

IoT security has become a hot topic over the past months and weeks. Recent attacks exploiting known vulnerabilities of connected objects shown how the IoT devices can use used as attack vector to disrupt critical services. In this presentation we will walk through some of the recent attacks and discuss what the industry should be doing to address the raising cybersecurity concerns

**Telemaco Melia** (KUDELSKI is a seasoned telecom professional with over 15 years experience in cutting edge wireless technologies. He currently leads business development activities on low power wide area networks within Kudelski Security)

## SESSION 3: HANDS ON SECURITY TUTORIALS

16:30 – 18:00

**Tutorial 1 – [WEB] Secure web app programming**

How do I approach secure code? Eoin shall discuss common pitfalls and demonstrate vulnerabilities from the ground up. Covering much of the OWASP Top 10 and items such as how phishing and ransomware drive-by attacks can damage your business and how to code securely to reduce the risk of breach.

**Eoin Keary CISA**, CISSP was previously on the Global board of directors and vice/chair of the OWASP foundation. He was the lead of the OWASP Code review guide and testing guides for many years. He currently is the CEO of edgescan.com, a cloud based SaaS managed service, dedicated to vulnerability management of 1000's of hosting, cloud and web application systems globally.

16:30 – 18:00

**Tutorial 2 – [RANSOMWARE] How do ransomware attacks work and how to mitigate them.**

**This tutorial aims at presenting the basic mechanisms used by ransomware to infect computers as well as providing hints about detection and mitigation.**

Sergio Alves Domingues (SCRT)

Chief Technical Officer at SCRT. 10+ years of working experience in information security.

16:30 – 18:00

**Tutorial 3 – [DDOS] Hands on DDoS mitigation session.**

A live demonstration of DDOS attack vectors and their effect, and the mitigations that can be used to defend against them.

**James Crocker**, Having spent 10 years as a Network Security product SME at Citrix Systems in the APJ region, moved to Cloudflare to help make the internet faster, better and more secure.

&

**James Ball** (Cloudflare) Previously spent nine years working as a network engineer for several U.N. Organisations in Switzerland, the Philippines, Malaysia and the United States. Now enjoying helping to make the internet a safer place as a Solutions Engineer at Cloudflare.

## WEDNESDAY 22 FEBRUARY 2017

### SESSION 3: HANDS-ON SECURITY TUTORIALS

09:00 – 10:30

**Tutorial 1 – [WEB] Secure web app programming**

**Eoin Keary** (same as above)

09:00 – 10:30

**Tutorial 2 – [LIVE HACKING DEMO] Live Hacking of TV devices**

HbbTV merges traditional DVB with the capabilities of the internet. This opens a new world for broadcasters but also for hackers. Combining the bidirectional communication of the internet with the insecure unidirectional DVB streams results in almost insurmountable security risks.

We demonstrate how these risks can be exploited remotely without user interaction to gain control over TVs. These techniques allow us to create a massive TV-botnet or spy on companies and private individuals.

**Rafael Scheel** (OneConsult) finished his IT apprenticeship at the ETH/SLF in 2011. Afterwards he studied business information technology while working for a leading Swiss IT security vendor.In 2014 Rafael joined Oneconsult focusing on penetration testing and security research with an emphasis on exploit development and became a senior penetration tester in 2016. Among others he is an Offensive Security Certified Professional (OSCP) and holds the GIAC Reverse Engineering Malware (GREM).

09:00 – 10:30

**Tutorial 3 – [DDOS] Hands on DDoS mitigation session.**

A live demonstration of DDOS attack vectors and their effect, and the mitigations that can be used to defend against them.

**James Crocker & James Ball** (Cloudflare)

### SESSION 4: IMPROVING SECURITY WITHIN YOUR ORGANISATION.

11:00 – 11:30

**How to set up an efficient Security Operation Centre (SOC): insource/outsource or hybrid?**

After the recent major cyberattacks on media companies, we are all trying to improve our cyber security level and most of us want to have a Security Operation Center. What is a SOC, what's in and how to set it up. We will try to explore different options a broadcast company can have when starting such an activity.

**David Garcia** (France TV) has been CISO at France Télevisions since 2010. Previously he was in charge with the networks of France 3 where he developed and operated a broadcast contribution nertwork over IP. He has worked several years for Thomson Broadcast Systems and then EMC2 before joining France 3 and France Télévisions in 2004.

11:30 – 12:00

**Cybersecurity for journalist.**

**Gerben Dierick** (VRT)

12:00 – 12:30

**Identity and Access Management. Implementing an IAM system.**

An identity management access (IAM) system is a framework for business processes that facilitates the management of electronic identities. The framework includes the technology needed to support identity management. Based on this concept, and in our experience in RTVE, this presentation shows the process of integrating an IAM system into a broadcaster, and the benefits and challenges that will also bring with it.

**Alvaro Martin Santos** is Cybersecurity Officer in RTVE, where started working on IT Security and IAM 9 years ago. He is Computer Science Engineer and is pursuing a PhD in Industrial Engineering, with a specialization in Security of IP broadcasting technologies at UNED - Universidad Nacional de Educación a Distancia.

12:30 – 13:00

**Security considerations for cloud-based document sharing solutions (Office365 / Dropbox / Box).**

How customized security can improve security

**Lena Vretling &**

**Johan Ribberheim** (SVT)

SESSION 5: LEGAL FRAMEWORKS : CERTIFICATIONS & REGULATIONS

14:00 – 14:30

**Consideration for Service Migration into the Cloud**

Overview about existing standards and legal considerations if you move services into the cloud and architectural requirements that need to be designed before migrating into public cloud environments.

**Andreas Schneider** (SRG) – same as above

14:30 – 15:00

**Data Privacy and Sovereignty - Challenges in the Expanding Regulatory Environment**

Data Privacy and Sovereignty are two of the biggest challenges facing global companies today. As technology advances with the introduction of the cloud and IoT, companies need to recognize the importance of data privacy compliance and understand the critical difference between privacy and security. The impact of the new EU GDPR will be discussed during this presentation, as well as the important of privacy due diligence. .

**Sheila FitzPatrick** (NETAPP) has over 30 years experience as an international data protection attorney. Sheila is one of the world's leading experts in data privacy laws and works closely with DPAs in 165 countries. She is recognized by DPAs around the world for her depth of comprehension and commitment to data privacy compliance.

Sheila holds undergraduate and law degrees (BA & JD) from Santa Clara University, an MBA from Syracuse University and a law degree (LLM) from Trinity College in Dublin.

15:00 – 15:30

**Why is the Swiss PPP approach quite unique?**

Can collaboration between Government and Public Service Media be successful? What is the difference of PPP in Switzerlande compared to other countries?

**Max Klaus** (MELANI) has been working for the Swiss Government since 2002 and has a polytechnic degree in IT security. He started in the Swiss Federal Chancellery, where he worked for different E-Government and E-Voting projects.
After 18 months as IT Security Officer in the Federal Department of Defense, People’s Protection and Sports, he started his work as Deputy Head of MELANI on September 1st, 2008.

## SESSION 6: NEXT GEN. THREATS, HACKING TECHNIQUES & SECURITY TECH.

15:45 – 16:15

**Conducting a security assessment for media companies.**

Conducting a security assessment for media companies.
How to start?
Where are the priorities?
What are the options?
Focus on intrusion testing (including in broadcast environment)
What is the right level of feedback (including for executives)?

**Aurélien PERROT-DELAHOUSSE** MANAGING CONSULTANT, CISSP AIRBUS DEFENCE AND SPACE - CYBERSECURITY
Aurélien Perrot-Delahousse is consultant, program manager and auditor. Now head of the intrusion testing team, he delivers information systems security services for Airbus, the public and the private sector (bank & insurance, energy, media, transportation, aeronautics).
During his missions he notably delivered assessment programs and remediation roadmaps for media companies.

16:15 – 16:45

**The Enterprise Immune System**

The Enterprise Immune System is a new technological approach to cyber defense, based on unsupervised machine learning and mathematical models. Inspired by the self-learning intelligence of the human immune system, this new approach is delivered by cutting-edge technology that is capable of learning ‘self’ within an organization in real time – enabling it to detect emerging threats that bypass other security controls.

**Ennio Di Rosa**, Senior Business Manager at Darktrace, has in-depth experience in the Cyber Security-space in the EMEA region. With his legal background and detailed knowledge of the privacy concerns in Europe, he has helped international organisations in the corporate environment to become more efficient and to mitigate their enterprise vulnerabilities.

16:45 – 17:15

**Machine learning in web application security testing: ImmuniWeb**

**Johnathan Schumann** (High-Tech Bridge)

## SESSION 7: WRAP-UP

17:15 – 17:30

**Conclusions**

**Adi Kouadio** (EBU)