سند معرفی دوره آموزشی

مقدماتی(۸ ساعته و ۱۶ ساعته):

« امنیت اطلاعات در سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی : چالش‌ها و راهکارها»

INFORMATION SECURITY IN INDUSTRIAL CONTROL SYSTEMS: CHALLENGES AND SOLUTIONS

نسخه : ۳.۰.۱

www.mmAhmadian.ir

@mmAhmadian www.mmAhmadian.ir mm.Ahmadian@aut.ac.ir

چکیده

در حال حاضر غالب مراکز صنعتی و زیرساخت‌های حیاتی کشوری از سامانه‌های کنترل صنعتی، برای نظارت و کنترل فرآیندهای صنعتی استفاده می‌نمایند. این سامانه‌ها در گذشته به صورت جدا از سایر سامانه‌ها، از جمله شبکه‌های داخلی و جهانی اینترنت به کار گرفته می‌شدند و این امر روشی در امن سازی این سامانه‌ها قلمداد می‌گردید. اتکا فراوان به این ممیزه، تولیدکنندگان و مصرف کنندگان این سامانه‌ها را از پرداختن به سایر لایه‌های امنیتی غافل کرده بود. استفاده از معماری و پروتکل‌های غیر امن و واسطهای غیر استاندارد را می‌توان از نتایج این رویکرد دانست.به دلیل نیازمندی‌های جدید و توسعه فناوری، امروزه این قبیل سامانه به تدریج با انواع جدیدتر جایگزین و به روز رسانی می‌گردند. با توسعه سامانه‌های اسکادا، تجهیزات این سامانه‌ها به سمت اتصالات متقابل و برقراری ارتباط با سایر تجهیزات حرکت کردند. به مرور این سامانه‌ها از شبکه‌های نقطه به نقطه به معماری‌های ترکیبی با ایستگاه‌های کاری متنوع توسعه پیدا کردند. در سامانه‌های جدید از پروتکل‌ها و نقاط دسترسی ارتباطی مشترک در شبکه‌ها استفاده می‌گردد که این امر موجب دسترسی مستقیم و غیر مستقیم به این سامانه‌ها از طریق شبکه‌های مختلف گردیده و آن‌ها را در مقابل تهدیدات سایبری آسیب پذیر نموده است.

از آنجایی سامانه‌های کنترل صنعتی به شکل گسترده در زیر ساخت‌های حیاتی کشورهای مختلف مورد استفاده قرار می گیرند، انتظار می رود که چالش‌ها و آسیب پذیری‌های امنیتی کمی داشته باشند؛ این در حالی است که واقعیت به گونه‌ی دیگری است. هدف این دوره آموزشی که در سطح مقدماتی ۸ ساعته و ۱۶ ساعته طراحی شده است این است که با تمرکز بر سامانه‌های کنترل صنعتی موجود در زیرساخت‌های حیاتی، ضمن بیان چالش‌های امنیتی آنها ، روند حملات و رخدادهای امنیتی مرتبط بررسی شده و در نهایت راهبردها و راهکارهای مقاوم سازی و کاهش مخاطرات امنیتی در این سامانه‌ها معرفی گردد.

@mmAhmadian www.mmAhmadian.ir mm.Ahmadian@aut.ac.ir

دستاورد علمی و عملی شرکت کنندگان از دوره آموزشی مقدماتی ۸ ساعته:

- آشنایی با مقدمه‌ای از سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی
- ارتقاء دانش در حوزه چالش‌های فناوری عملیاتی در برابر فناوری اطلاعات
- ارتقاء دانش در حوزه چالش‌های امنیتی در سامانه های کنترل صنعتی
- اشراف بر روند حملات و رخدادهای سامانه های کنترل صنعتی و مرور ۱۰ رخداد مهم در این حوزه
- آشنایی با راهبردها و راهکارهای مقاوم سازی و کاهش مخاطرات در سامانه‌های کنترل صنعتی

سر فصل مطالب دوره آموزشی مقدماتی:

- مقدمه‌ای بر سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی
- چالش‌های فناوری عملیاتی در برابر فناوری اطلاعات
- چالش‌های امنیتی در سامانه های کنترل صنعتی
- روند حملات و رخدادهای سامانه های کنترل صنعتی
- راهبردها و راهکارهای مقاوم سازی و کاهش مخاطرات در سامانه‌های کنترل صنعتی
- اجرای عملی دموی حملات و دموی راهکارهای دفاعی (با تیم همکار)

جزیئات دوره آموزشی مقدماتی:

@mmAhmadian www.mmAhmadian.ir mm.Ahmadian@aut.ac.ir

- **مدت زمان برگزاری دوره:** محتوای این دوره با توجه به نیازمندی‌های کارفرما و سطح مخاطبین می‌تواند بین ۴ الی ۸ ساعت ارائه گردد.
- **فرض :** پیشفرض کارگاه آموزشی مقدماتی این است که مخاطبین دوره آشنایی اولیه با اصول امنیت اطلاعات را دارا می‌باشند.
- **مخاطبین:**
  - مدیران، متولیان و مسئولان سامانه‌های کنترل صنعتی و زیر ساخت های حیاتی
  - کارشناسان فناوری اطلاعات سامانه‌های کنترل صنعتی و زیر ساخت های حیاتی
  - کارشناسان امنیت اطلاعات سامانه‌های کنترل صنعتی و زیر ساخت های حیاتی
  - کارشناسان و متخصصین شبکه‌های کنترل صنعتی
  - پژوهشگران، دانشجویان و سایر علاقمندان به مباحث امنیت اسکادا و فناوری‌های عملیاتی

@mmAhmadian www.mmAhmadian.ir mm.Ahmadian@aut.ac.ir

دستاورد علمی و عملی شرکت کنندگان از دوره آموزشی مقدماتی ۱۶ ساعته:

- آشنایی با مقدمه‌ای از سامانه‌های کنترل صنعتی ، زیرساخت‌های حیاتی ، پروتکل‌های مربوطه
- آشنایی با مفاهیم اولیه امنیتی نظیر آسیب پذیری‌ها، تهدیدات ، حملات
- ارتقاء دانش در حوزه چالش‌های فناوری عملیاتی در برابر فناوری اطلاعات
- آشنایی با تهدیدات بدافزاری و تهدیدات مانای پیشرفته(APT)
- ارتقاء دانش در حوزه چالش‌های امنیتی در سامانه های کنترل صنعتی
- اشراف بر روند حملات و رخدادهای سامانه های کنترل صنعتی و مرور ۴۰ رخداد مهم در این حوزه جهت اشراف به مقدمه تهدید شناسی[1]
- آشنایی با روند ارزیابی امنیتی سامانه‌های کنترل صنعتی و نحوه همکاری با گروه های ممیزی و ارزیابی
- آشنایی با استانداردهای امنیتی سامانه‌های کنترل صنعتی با توجه به صنعت هدف
- آشنایی با راهبردها و راهکارهای مقاوم سازی و کاهش مخاطرات در سامانه‌های کنترل صنعتی
- آشنایی به مکانیزم‌های امنیتی تجهیزات رایج در صنایع
- آشنایی با مفاهیم جدید و فناوری های نوین در حوزه امنیت سامانه‌های کنترل صنعتی
- مشاهده دمو و شبیه سازی حملات واقعی به صنایع در بستر آزمایشی و نحوه بکارگیری برخی محصولات امنیتی طبق سناریوهای از پیش تعریف شده(با تیم همکار)

[1] Threat Intelligence

@mmAhmadian www.mmAhmadian.ir mm.Ahmadian@aut.ac.ir

سر فصل مطالب دوره آموزشی مقدماتی۱۶ ساعته:

- مفاهیم اولیه اتوماسیون و سامانه‌های کنترل صنعتی
- مقدمه‌ای بر مفاهیم اولیه امنیت اطلاعات
- چالش‌های فناوری عملیاتی در برابر فناوری اطلاعات
- مقدمه ای از بدافزارها و تهدیدات مانای پیشرفته
- مقدمه‌ای از پروتکل‌های صنعتی
- روند حملات و رخدادهای سامانه های کنترل صنعتی
- چالش‌های امنیتی در سامانه های کنترل صنعتی
- ارزیابی امنیتی سامانه‌های کنترل صنعتی
- معرفی استانداردهای امنیتی سامانه‌های کنترل صنعتی
- راهبردها و راهکارهای مقاوم سازی و کاهش مخاطرات در سامانه‌های کنترل صنعتی
- روش های نوین امنیت سامانه‌های کنترل صنعتی
- معرفی قابلیت‌های امنیتی تجهیزات رایج
- دمو و شبیه سازی حملات و محصولات امنیتی

جزیئات دوره آموزشی مقدماتی ۱۶ ساعته:

- **مدت زمان برگزاری دوره:** محتوای این دوره با توجه به نیازمندی‌های کارفرما و سطح مخاطبین می‌تواند بین ۱۶ الی ۲۴ ساعت ارائه گردد.
- **مخاطبین:**
  - مدیران، متولیان و مسئولان سامانه‌های کنترل صنعتی و زیر ساخت های حیاتی
  - کارشناسان فناوری اطلاعات سامانه‌های کنترل صنعتی و زیر ساخت های حیاتی
  - کارشناسان امنیت اطلاعات سامانه‌های کنترل صنعتی و زیر ساخت های حیاتی
  - کارشناسان و متخصصین شبکه های کنترل صنعتی

@mmAhmadian www.mmAhmadian.ir mm.Ahmadian@aut.ac.ir

نکات عمومی دوره‌های آموزشی پیشنهادی:

- نسخه پیش فرض دوره آموزشی هدف برای طیف مشترک فارغ التحصیلان رشته‌های برق، کامپیوتر و فناوری اطلاعات طراحی شده است لذا قابلیت سفارشی سازی دوره برای فارغ التحصیلان رشته برق یا رشته‌های کامپیوتر و فناوری اطلاعات بر حسب نیاز کارفرما وجود دارد.
- نسخه پیش فرض دوره آموزشی برای طیف مشترک مخاطبین در سطوح مدیریتی و کارشناسان فنی طراحی شده است اما چنانچه کارفرما در نظر داشته باشد دوره‌های متفاوتی برای سطوح مدیریتی و کارشناسان فنی ارائه شود، قابلیت سفارشی سازی دوره با نیازسنجی از کارفرما وجود دارد.
- علاوه بر دوره‌ی مقدماتی، دوره‌ی سطح پیشرفته امنیت در سامانه‌های اتوماسیون صنعتی و زیرساخت‌های حیاتی نیز قابل ارائه است که سند معرفی این دوره از طریق مکاتبه با مدرس دوره قابل ارائه است.

مدرس دوره آموزشی:

نام و نام خانوادگی:	محمد مهدی احمدیان مرج	اطلاعات جانبی:	وبگاه: www.mmAhmadian.ir معرفی و رزومه آنلاین: http://www.mmahmadian.ir/aboutme/introduction/ کانال تلگرام: https://t.me/MohammadMehdiAhmadian
مدرک تحصیلی:	• کاندیدای دکتری تخصصی فناوری اطلاعات(گرایش امنیت اطلاعات) از دانشگاه صنعتی امیرکبیر		

@mmAhmadian www.mmAhmadian.ir mm.Ahmadian@aut.ac.ir

پست الکترونیکی: mm.Ahmadian@aut.ac.ir

شماره تماس: ارسال بعد از مکاتبات اولیه

*** جهت استعلام هزینه و سایر شرایط دوره آموزشی با مدرس دوره تماس حاصل شود.

برخی از مراجع مورد استفاده در محتوای دوره:

- *محمد مهدی احمدیان ، بابک رضا زاده ،پروتکل کنترل صنعتی IEC 60870-5-104 از منظر امنیت سایبری ،انستیتو ایزایران، ۱۳۹۶*
- *Ahmadian M. M, Rezazadeh B. , Dezfouli M., Shajari M, Towards Identification of IEC 60870-5-104 Protocol Security Vulnerabilities and Threats [In Persian]. In Information Security and Cryptology (ISCISC), 2017 14th International Iranian Society of Cryptology Conference on 2017 Sep 6-7. IEEE.*
- *N. Mousavi ,Shajari M ,Ahmadian M. M, Implementation of the software testing environment for attacks against the Modbus Protocol [In Persian]. In Information Security and Cryptology (ISCISC), 2017 14th International Iranian Society of Cryptology Conference on 2017 Sep 6-7. IEEE.*
- *Thomas, Roshan K., Alvaro A. Cardenas, and Rakesh B. Bobba. "First Workshop on Cyber-Physical Systems Security and PrivaCy (CPS-SPC): Challenges and Research Directions." Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015.*
- *Edward Chikuni; Maxwell Dondo, Investing the Security of Power System SCADA,Conference proceedings, AFRICON, Sept. 2007.*
- *Clarke, Gordon R., Deon Reynders, and Edwin Wright. Practical modern SCADA protocols: DNP3, 60870.5 and related systems. Newnes, 2004.*
- *Cheah, Zi Bin. "Testing and Exploring Vulnerabilities of the Applications Implementing IEC 60870-5-104 Protocol." Master Thesis,KTH University,Stockholm, Sweden, 2008.*
- *Frank Hohlbaum, Markus Braendle, Fernando Alvarez, Cyber Security Practical considerations for implementing IEC 62351,ABB, Switzerland.*
- *federal cybersecurity research and development strategic plan,ensuring prosperity and national security national science and technology council networking and information technology research and development program,february 2016.*
- *Framework for Improving Critical Infrastructure Cybersecurity,Version 1.0,National Institute of Standards and Technology,February 12, 2014.*
- *IEC60870-5-101, Part 5-101:Transmission protocols –Companion standard for basic telecontrol tasks,International Electrotechnical Commission,2003 .*
- *IEC 60870-1-3, Part 1: General consideration-Section 3: Transmisson Frame Foramt,International Electrotechnical Commission,1997.*

- *Frances Cleveland, WG15 Convenor,IEC TC57 WG15:IEC 62351 Security Standards for the PowerSystem Information Infrastructure,Xanthus Consulting International.2012.*
- *IEC 60870-5-104,Transmission protocols –Network access for IEC 60870-5-101 using standard transport profiles, International Electrotechnical Commission,2006.*
- *IEC 60870-5-1,Part 1: General consideration-Section 3: General Structure of application data,International Electrotechnical Commission,1992.*
- *Pollet J. , Developing a solid SCADA security strategy, Sensors for Industry Conference,2002. 2nd ISA/IEEE, Nov. 2002*
- *Mitchell, Robert, and Ing-Ray Chen. "A survey of intrusion detection techniques for cyber-physical systems." ACM Computing Surveys (CSUR) 46.4 (2014).*
- *Bishop, Matt. Introduction to computer security. Boston, MA: Addison-Wesley, 2005.*
- *IGNAT, Nicoleta. "Dependability and vulnerability of SCADA Systems." Annals of the Oradea University, Fascicle of Management and Technological Engineering, Issue XIII (XXIII) (2014).*
- *Robinson, M. (2013) The SCADA threat landscape. In: First International Symposium for ICs & SCADA Cyber Security Research 2013. Leicester, U.K., 30–41.*
- *Morris, T. H. and Gao, W. (2013) Industrial control system cyber attacks. In: First International Symposium for ICs & SCADA Cyber Security Research 2013. Leicester, U.K., 22–29.*
- *Morris, T., Vaughn, R., and Dandass, Y. S. (2011) A testbed for SCADA control system cybersecurity research and pedagogy. In: Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, CSIIRW '11. New York, NY, USA, 27:127:1.*
- *Pietre-Cambacedes, L., Tritschler, M., and Ericsson, G. N. (2011) Cybersecurity myths on power control systems: 21 misconceptions and false beliefs. IEEE Trans. Power Del., 26 (1). 161–172.*
- *Samineni, N. R., Barbhuiya, F. A., and Nandi, S. (2012) Stealth and semi-stealth MITM attacks, detection and defense in IPv4 networks. In: 2012 2nd IEEE International Conference onParallel Distributed and Grid Computing (PDGC), 364–367.*
- *Pidikiti, Durga Samanth, et al. "SCADA communication protocols: vulnerabilities, attacks and possible mitigations." CSI transactions on ICT1.2 (2013): 135-141.*
- *Yang, Y. et al. (2013) Intrusion detection system for IEC 60870-5-104 based SCADA networks. In: 2013 IEEE Power and Energy Society General Meeting (PES), 1–5.*
- *Czechowski, Robert, and Bernard Wiecha. "Cyber security in communication of SCADA systems using IEC 61850." 2015 Modern Electric Power Systems (MEPS). IEEE, 2015.*
- *Clevland, Enhancing the Reliability and Security of the Information Infrastructure Used to Manage the Power System, Frances Clevelan, d IEEE Member, PES-PSCC, 2007*
- *IEC/TS 62351-5, Part 5: Security for any profiles including IEC 60870-5,International Electrotechnical Commission, technical specification, Edition 2.0 2013.*
- *IEC/TS 62351-3, Power systems management and associated information exchange – Data and communications security– Part 3: Communication network and system security – Profiles including TCP/IP, technical specification.*
- *IEC/ST 62351-1, Part 1:Introduction to the standard ,International Electrotechnical Commission, technical specification, 2007.*
- *ISO/IEC 9798-4, Part 4: Mechnaism using a cryptographic check function , International organisation for standard & International Electrotechnical Commission, , 1999.*
- *IEC/ST 62351-2, Part 2: Glossary, International Electrotechnical Commission,technical specification, 2008.*
- *IEC/ST 62351-9, Part 9: Key Managment, International Electrotechnical Commission, technical specification, 2012.*

- *IEC/TS 60870-5-7,Part 5:Communication profile for basic telecontrol messages -Section 7:Seurity extenstion to IEC 60870-5-101 and IEC 60870-5-104 protocols(Applying IEC 62351) ,International Electrotechnical Commission,technical specification, Edition 1.0 ,2013.*
- *Mitchell, Robert, and Ing-Ray Chen. "A survey of intrusion detection techniques for cyber-physical systems." ACM Computing Surveys (CSUR) 46.4 (2014): 55.*
- *Sooyeon Shin, Taekyoung Kwon, Gil-Yong Jo, Youngman Park, and H. Rhy. 2010. An Experimental Study of Hierarchical Intrusion Detection for Wireless Industrial Sensor Networks. IEEE Transactions on Industrial Informatics 6, 4 (November 2010), 744–757.*
- *Akella, Ravi, Han Tang, and Bruce M. McMillin. "Analysis of information flow security in cyber–physical systems." International Journal of Critical Infrastructure Protection 3.3 (2010): 157-173.*
- *McMillin, Bruce, and Ravi Akella. "Verification of information flow properties in cyber-physical systems." Workshop on Foundations of Dependable and Secure Cyber-Physical Systems (FDSCPS). 2011.*
- *Akella, Rav. (2009)."Verification of information flow security in cyber-physical systems." (Doctoral Dissertations, Missouri University of Science and Technology, Missouri, United States). Retrieved from http://scholarsmine.mst.edu/doctoral_dissertations/2030/*
- *Langner, Ralph. "To kill a centrifuge: A technical analysis of what stuxnet's creators tried to achieve." Online: http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf (2013).*
- *Eric Luiijf and Bert Jan te Paske, Cyber Security of Industrial Control Systems, GCCS2015,March 2015.*
- *Cárdenas, Alvaro A., Saurabh Amin, and Shankar Sastry. "Research Challenges for the Security of Control Systems." HotSec. 2008.*
- *A. Kovacevic, The impact of the Russia–Ukraine gas crisis in south-eastern Europe, Oxford Institute for Energy Studies, March 2009.*
- *G.Thoshitha et al. "Information flow security in cyber-physical systems." Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research. ACM, 2011.*
- *A. Ravi , and B. McMillin. "Model-checking BNDC properties in cyber-physical systems." 2009 33rd Annual IEEE International Computer Software and Applications Conference. IEEE, 2009.*
- *Akella, Rav. (2009). "Information flow properties for cyber-physical systems." (Master's thesis, Missouri University of Science and Technology, Missouri, United States). Retrieved from http://scholarsmine.mst.edu/masters_theses/4657/*
- *A. Ravi , and B. McMillin. "Modeling and verification of security properties for critical infrastructure protection." Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop. ACM, 2013.*
- *A. Ravi. "Process Algebra and Bisimulation Techniques for Information Security."*
- *Warren A. Hunt Jr., "Modeling and verification of cyber-physical systems,"in National Workshop on High-Confidence Automotive Cyber-Physical Systems, April 2008.*
- *M. Pluska and D. Sinclair, "Modelling and verification of cyber-physical system,"in 20th European Meeting on Cybernetics and System Research, 2010.*
- *Krotofil, Maryna, and Dieter Gollmann. "Industrial control systems security: What is happening?." Industrial Informatics (INDIN), 2013 11th IEEE International Conference on. IEEE, 2013*
- *Damiano Bolzoni and Dian Hadziosmanovic,Cyber Security in industrial Control Systems,SysSec Summer School,University Twente,Amsterdam,2012*
- *Gritsai, Gleb, et al. "SCADA safety in numbers V1. 1*." Positive Technologies (2012).*
- *R. Santamarta, "Reversing industrial firmware for fun and backdoors I," 2011*
- *——, "HERE BE BACKDOORS: A jorney into the secrets of industrial firmware," Black Hat USA, 2012.*
- *J. C. Matherly, "man SHODAN," http://www.shodanhq.com/help, 2009.*

- *"ICS-CERT Monthly Monitor," October–December 2012.*
- *M. Sundell et al., "White paper on industrial automation security in fieldbus and field device level," 2011.*
- *S. East, J. Butts, M. Papa, and S. Shenoi, "A taxonomy of attacks on the DNP3 protocol," 2009, pp. 67–81.*
- *M. Majdalawieh, F. Parisi-Presicce, and D. Wijesekera, "DNPSec:Distributed network protocol version 3 (DNP3) security framework,"in Advances in CISSE, 2006, pp. 227–234.*
- *I. Fovino, A. Carcano, M. Masera, and A. Trombetta, "Design and implementation of a secure modbus protocol," 2009, pp. 83–96.*
- *OPC Security 1.00 Specification,OPC Foundation.*
- *The OPC UA Security Model for Administrator,OPC Foundation .*
- *Frances Cleveland, WG15 ConvenorIEC TC57 WG15:IEC 62351 Security Standards for the Power System Information Infrastructure,Xanthus Consulting International.*
- *Ma, Hua-Dong. "Internet of things: Objectives and scientific challenges." Journal of Computer science and Technology 26.6 (2011): 919-924.*
- *Robert CZECHOWSKI,Cyber Security in communication of SCADA systems using IEC 61850*
- *Leyden, John (6 February 2003). "Slammer: Why security benefits from proof of concept code". Register. Retrieved 2008-11-29.*
- *Joanne Pilker,"MS SQL Slammer/Sapphire Worm",Global Information Assurance Certification Paper,SANS Institute*
- *Moore, David et al. "The Spread of the Sapphire/Slammer Worm". CAIDA (Cooperative Association for Internet Data Analysis).*
- *Serazzi, Giuseppe & Zanero, Stefano (2004). "Computer Virus Propagation Models". In Calzarossa, Maria Carla & Gelenbe, Erol. Performance Tools and Applications to Networked Systems. Lecture Notes in Computer Science. Vol. 2965. pp. 26–50*
- *"ISS Security Brief: Microsoft SQL Slammer Worm Propagation". ISSForum. 25 January 2003. Retrieved 2008-11-29.*
- *Jonathan Butts, Sujeet Shenoi,Critical Infrastructure Protection VIII(2008)*
- *Haihui Gao, Yong Peng, Zhonghua Dai, Ting Wang, Xuefeng Han,and Hanjing Li,AN INDUSTRIAL CONTROL SYSTEM TESTBED BASED ON EMULATION,PHYSICAL DEVICES AND SIMULATION*
- *Frances Cleveland,Enhancing the Reliability and Security of the Information Infrastructure Used to Manage the Power System ,IEEE Member, PES-PSCC, 2007.*
- *J. Slay and M. Miller, Lessons Learned from the MaroochyWater Breach. ;In Proceedings of Critical Infrastructure Protection. 2007, 73-82*
- *Durga et al 2013*
- *Liu,Y.,Ning, P.,Reiter, M.: False data injection attacks against state estimation in electric power grids. In: Proceedings of 16th ACM Conference on Computer and Communications Security, CCS '09, pp. 21–32. ACM, New York, NY, USA (2009)*
- *Andrea Carcano, Igor Nai Fovino, Marcelo Masera, and Alberto Trombetta. 2009. Scada Malware, a Proof of Concept. In Critical Information Infrastructure Security, Roberto Setolaand Stefan*
- *Geretshuber(Eds.). LNCS 5508. Springer-Verlag, Berlin, Heidelberg 211-222 Keith Stouffer ,Joe Falco ,Karen Scarfone,Guid to Industrial Control Systems(ICS) Security,NIST,Special Publication 800-82,June 2011*
- *Adepu S, Mathur A, Gunda J, Djokic S. An agent-based framework for simulating and analysing attacks on cyber physical systems. InInternational Conference on Algorithms and Architectures for Parallel Processing 2015 Nov 18 (pp. 785-798). Springer International Publishing.*
- *Zhu, Q., Rieger, C., Bas¸ar, T.: A hierarchical security architecture for cyber-physical systems. In: Resilient Control Systems (ISRCS), 2011 4th International Symposium on. pp. 15–20. IEEE (2011)*

- *Adepu S, Mathur A, Gunda J, Djokic S. An agent-based framework for simulating and analysing attacks on cyber physical systems. InInternational Conference on Algorithms and Architectures for Parallel Processing 2015 Nov 18 (pp. 785-798). Springer International Publishing.*
- *Edward A. Lee. Cyber physical systems: Design challenges, http://www.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-8.html. Technical Report UCB/EECS-2008-8, EECS Department, University of California, Berkeley, Jan 2008.*

برخی سوابق آموزشی مرتبط:

عنوان	عنوان انگلیسی	محل ارائه	زمان	اسلاید
سخنرانی چالش های امنیتی در سامانه‌های سایبر-فیزیکی (با محوریت تحلیل جریان اطلاعات در خطوط لوله نفت و گاز)	*Cyber–Physical Systems Security Challenges (Case study: Information Flow Security Analysis in Natural Gas and Oil Pipeline System)*	ششمین کنفرانس فناوری اطلاعات و ارتباطات در نفت، گاز ،پالایش و پتروشیمی، تهران، دانشگاه شهید بهشتی	۲۷ دی ماه ۱۳۹۶	لینک
شناسایی تهدیدات و آسیب‌پذیری‌های امنیتی پروتکل کنترل صنعتی IEC 60870-5-104	*Towards the Identification of IEC 60870-5-104 Protocol Security Vulnerabilities and Threats*	چهاردهمین کنفرانس بین‌المللی انجمن رمز، شیراز، دانشگاه شیراز	۱۶ شهریور ۱۳۹۶	لینک آگهی
کارگاه آموزشی امنیت اطلاعات در سامانه‌های کنترل صنعتی : چالش‌ها و راهکارها	*Information Security in Industrial Control Systems: Challenges and Solutions*	چهاردهمین کنفرانس بین‌المللی انجمن رمز شیراز، دانشگاه شیراز	۱۴ شهریور ۱۳۹۶	لینک آگهی
ارائه علمی تحلیل و وارسی صوری امنیت جریان اطلاعات در سامانه‌های سایبری-فیزیکی، مطالعه موردی : سامانه انتقال(خطوط لوله) گاز	*Formal Analysis and Verification of information flow security in cyber–physical systems, Case study: natural gas pipeline system*	دانشگاه صنعتی امیرکبیر	مرداد ۱۳۹۵	
ارائه علمی درآمدی بر سامانه‌های سایبری-فیزیکی و چالش‌های امنیتی آن‌ها، حوزه محوری: سامانه‌های کنترل صنعتی	*Introduction to cyber–physical systems and their security challenges, Case study: ICSs*	دانشگاه صنعتی امیرکبیر	شهریور ۱۳۹۵	

سخنرانی چالش‌ها و راهکارهای امنیتی در سامانه‌های کنترل صنعتی	*and security challenges solutions in ICSs*	-----	آبان ۱۳۹۵	
کارگاه آموزشی امنیت سایبری در سامانه‌های کنترل صنعتی	*Cyber Security in Industrial control systems*	شرکت ملی گاز ایران، تهران	اسفند ۱۳۹۴	لینک
سخنرانی امنیت سایبری سامانه‌های کنترل صنعتی در صنایع نفت، گاز، پالایش و پتروشیمی		سومین کنفرانس و نمایشگاه فناوری اطلاعات و ارتباطات در صنایع نفت، گاز، پالایش و پتروشیمی ، تهران، دانشگاه شهید بهشتی	دی ۱۳۹۳	لینک