DS 05

PRESENTER	Contact e-mail
Salih Ergün	salih.ergun@erarge.com.tr
Ignasi Garcia-Milà Vidal	ignasi.garcia-mila@eurecat.org
Marcos Sacristán / Jaime Medina	marcos.sacristan@treelogic.com
Levent Kıdak	leventkidak@gmail.com
Ulrich Seldeslachts / Richard Chisnall	ulrich@leadersinsecurity.org
Tuomas Tammilehto	Tuomas.tammilehto@laurea.fi
Andreas Zalonis	azalonis@iit.demokritos.gr
Michelle Ryan	Michelle.M.Ryan@ul.ie

CRITICAL-CHAINS: Hardware-based Security System for New Generation IoT enabled Blockchain Applications in Critical Sectors

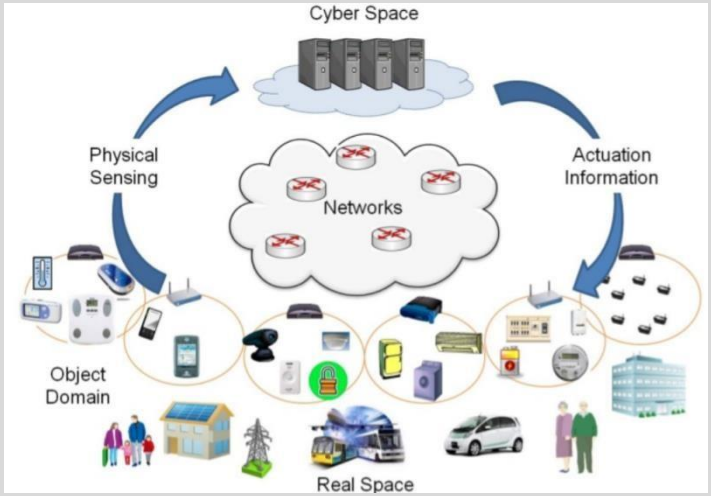
- *Salih Ergün, PHD (Tokyo Univ)*
- *Alper Kanak, PHD (GTU)*
- *salih.ergun@erarge.com.tr*
- *alper.kanak@erarge.com.tr*
- *ERARGE Research Oriented SME*

- Role: *S/T provider*

- Proposal activity:

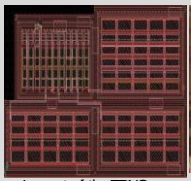
  SU-DS05-2018-2019: Digital security, privacy, data protection and accountability in critical sectors

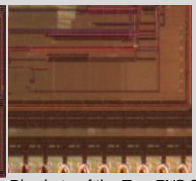
Proposal idea/content

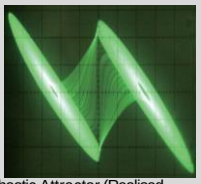


Proposed novel cyber-physical architecture for critical sectors

Targeted Practical Areas in the project (in discussion):
- Transport & mobility
- Blockchain industry
-Health
-...


Layout of the TRNG (Realised, awarded)


Die photo of the True RNG (Realised, awarded)


Chaotic Attractor (Realised, awarded)

- *Hardware-based crypto tools are mandatory for secure transactions in transport, environment and healthcare (quality of life)*
- *Blockchain industry is booming (noy only bitcoin) in critical sectors as there is a growing need to exchange information in secure environments*
- *There is a need on strong semantic relation between these concepts*
- *IoT (but secure and privacy preserving) is a must*
- *Very fast and mostly miniaturized hardware-based security tools needed (IC-TRNGs, crypto tools)*
- *Secure IoT backbone & cloud infrastructure is targeted*
- *Secure payment/certification/validation*
- *Security, privacy, trust and ethical analysis by a formal model*
- *Scalable, credible, interoperable scheme*
- *Threat and vulnerability analysis with advanced techniques (like chaos theory, Machine Learning)*

Salih Ergün, PHD, salih.ergun@erarge.com.tr

Project participants

- Project consortium according to their fields of expertise

Transportation domain	Blockchain Industry/ epayments	IoT Domain	Health
• Ford Otosan (TR) • Otokar (TR) L. Enterprise • Univ. Surrey (UK) • VTT (Fin) • eVConsult (NL) • İstanbul/İzmir... Mun. (TR) • Transportation GOs/NGOs (NL, AUS, Fin, TR, UK ...)	• ERARGE • Softtech (İş Bankası) • NETAŞ (formerly Nortel Telecom, TR) • Cardtek (TR) • HSBC (NL) • Logo CyberSecurity (TR) • ...	• ERARGE • ENTES Large Enterprise (TR) • FOG (Fin) • VTT (Fin) • Darmstadt University (DE) • Bosch...	• Acıbadem Hospital (NL, TR) • Ministry of Health (TR) • ...

- Looking for end users
- Looking for transportation experts
- Looking for VLSI design partners
- Looking for health stakeholders
- Non-profit organizations and public institutions are needed

Salih Ergün, PHD, salih.ergun@erarge.com.tr

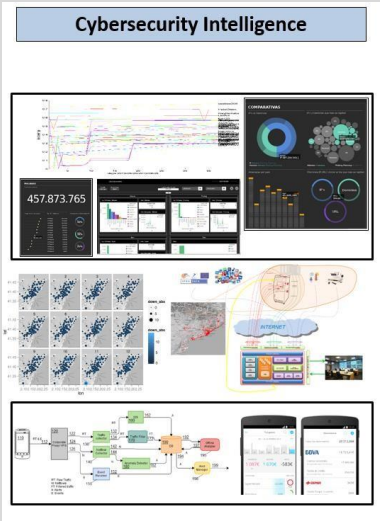
Security, Privacy & Data Protection in finance

- *Ignasi Garcia-Milà Vidal*
- *ignasi.garcia-mila@eurecat.org*
- *Eurecat*
- Role: *Proposal coordinator/WP leader*

- Proposal activity: *DS-05-2018*
  (c) [2018]: Digital security, privacy and personal data protection in finance

Proposal idea/content

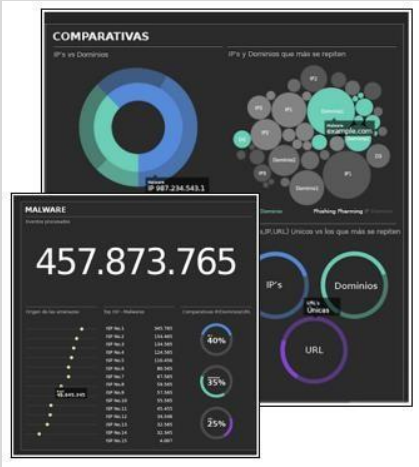
Development of resilience enhancing technologies



- The use of algorithms, techniques and methodologies based on artificial intelligence is the basis to know the attacker, and apply the necessary defensive measures to discourage him in his action (ATM, online banking, etc.).
- Adaptation and integration of access control and authorization solutions based on biometric technologies, as well as BTPS algorithms, increase system security and user privacy.
- Application of standards to ensure interoperability between different organizations that collaborate to address future threats and attacks.

Challenge

- Development of an active defense system or set of tools (AI-based) that discourage the attacker from stealing information
- Integration of authentication and authorization mechanisms based on biometric techniques
- Integration of tools and mechanisms for collaboration among different organizations: CERTs/CSIRTs, financial institutions, etc.



Ignasi Garcia-Milà – ignasi.garcia-mila@eurecat.org

Project participants

- Proposed coordinator: *Eurecat [IT Security, Data Privacy]*
- Partners / Other participants: Large Bank (CERT) [ES], Technology solution provider for finance sector [ES]

- Looking for partners with the following expertise/ technology/ application field:
  - *Finance sector companies (insurance, payment solutions, investment, ...)*
  - *Research organisation supporting the implementation of local pilot*
  - *Technology providers*

Ignasi Garcia-Milà – ignasi.garcia-mila@eurecat.org

Federated machine learning for digital security, privacy, data protection and accountability in finance

- *Marcos Sacristán, marcos.sacristan@treelogic.com*
  Jaime Medina, jaime.medina@treelogic.com
- *Treelogic*
  - *Spanish SME*
  - *Participation in 20+ EU projects (+50% as coordinator)*
  - *8 EU projects in SEC*
- Role: *Coordination*

  Big Data; Data Mining & Machine Learning
- Proposal activity: *SU-DS05-2018-2019: Digital security, privacy, data protection and accountability in critical sectors (c) [2018]: Digital security, privacy and personal data protection in finance (IA)*

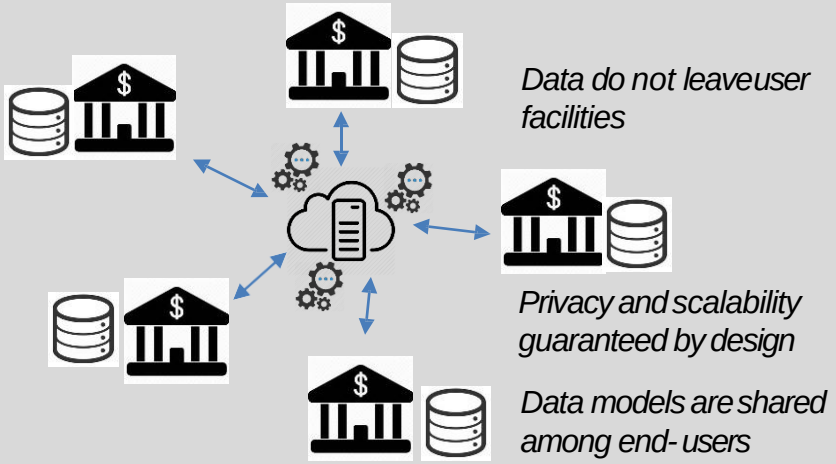
Proposal idea/content

With this proposal we aim to obtain a validated federated ***privacy-preserving machine learning platform on finance*** *that is demonstrably:*

- *safe enough (privacy-preserving in the face of legitimate and illegitimate (attempted) access and use)*
- *interoperable, scalable and efficient enough to be deployed to a significant representation of the private data in the finance sector.*

Toolkit:

- *Privacy preserving platform*
- *Personal data protection*
- *Cybersecurity*
- *Federated Machine Learning*
- *Finance-oriented*



Marcos Sacristán (TREELOGIC) – marcos.sacristan@treelogic.com

Project participants

- Proposed coordinator: *TREELOGIC (Open)*
- Partners / Other participants:
  - Experts in federated machine learning
  - Academics on privacy-preserving learning

- Looking for partners with the following expertise:
  - ***Operators*** *(end-users) in* ***financial sector*** *(banks, insurance, FinTech and InsurTech)*
  - ***Data providers*** *in financial sector*
  - ***CERT****/****CSIRTS*****
  - ***Cybersecurity experts*** *in financial sector*

**CERT, Computer Emergency Response Team*
***CSIRT , Computer Security Incident Response Team*

Marcos Sacristán (TREELOGIC) – marcos.sacristan@treelogic.com

CYBERSAFE HEALTHCARE (CSHC)

- Prof. Dr. **Levent Kıdak** *MD., PhD.*
- *leventkidak@gmail.com*
- *Izmir Katip Celebi University, Turkey,*
- *Healthcare Management Department, Head of Department*
- Role: *Partner, WP leader*
- Proposal activity: *SU-DS05-2018*

Ongoing Project;
TD 1405 European Network for the Joint Evaluation of Connected Health Technologies (ENJECT) COST Action

Proposal idea/content

- *Healthcare industry as well as the privacy and personal data are in high risk for cyber attacks that can cause life damages*
- *These vulnerabilities may be overcome by applying distributed and decentralized perspective,*
- Our aim under this heading is to participate an evaluation project of blockchain in healthcare by analyzing data interchange nodes in the system,
- With examining pros and cons, it is thought to create a roadmap for shifting from traditional system to peer-to-peer system gradually,
- In addition, evaluation may give a deeper examination on health information chain and create opportunity to evaluate weaker points in the information chain and give insight for how to overcome these weaknesses.

Prof. Dr. Levent KIDAK leventkidak@gmail.com

Looking for Project participants

Proposed coordinator:

Partners / Other participants: Research Centers, Hospital

Looking for partners with the following expertise/ technology/ application field:

- Technologic partners
- Research centers
- Hospital
- SMEs

Prof. Dr. Levent KIDAK leventkidak@gmail.com

SafeXchange

- Ulrich Seldeslachts / Richard Chisnall
- ulrich@leadersinsecurity.org / richard.chisnall@leadersinsecurity.org

- LSEC- Leaders In Security : a non-profit European (vzw) industry association (300+), cluster and user community (3500+ end users) supporting innovation & development of cyber security. ECSO Member and Global EPIC partner.

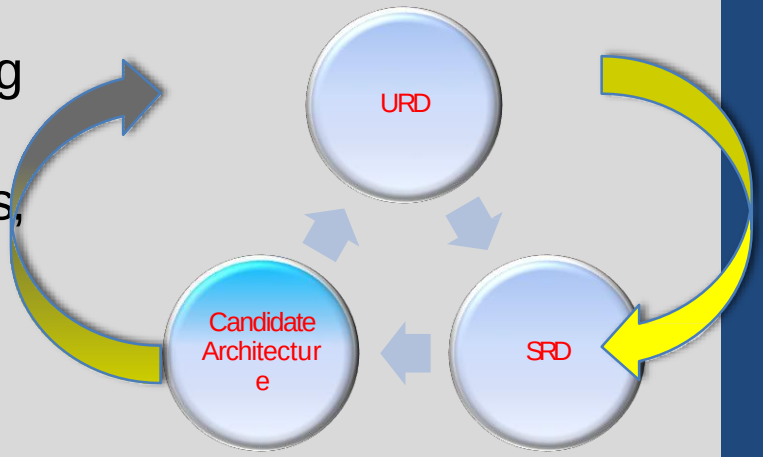
- Coordinator or WP leader on
  - Systematically capturing user needs to shape development of resilience enhancing technologies
  - Validation and verification
  - Market exploitation and dissemination

- Proposal activity: SU-DS05-2018-2019:
  Digital security, privacy, data protection and accountability in critical sectors
  (c) (1 & 3)[2018]: Digital security, privacy and personal data protection in finance

Proposal idea/content

Idea

- Coordinate and/or Lead WP on capturing user needs and capability gap analysis.
- Cyber Security Open Banking Challenges, Banking Appstore Security Services.
- Use System Engineering approach from Requirements Definition to Verification to maximise impact.



- Maximising impact through: market analysis; outreach to industry and wider dissemination.

Experience

- Building on track record in FP7/H2020 projects and working with the finance sector, Cyber Security Industry Market Analysis
- User Requirements capture in Finance, e-Government, Health, Transport, Etc.

Ulrich Seldeslachts ulrich@leadersinsecurity.org (richard.chisnall@leadersinsecurity.org)

Project participants

- Corporate Banking and Insurance institutions in 4 European countries,
- Searching for additional financial services and insurance organizations
- Searching for specific fintech and cybersecurity solutions expertise for web applications & Regulatory Technical Standards.
- Coordinator **or** Consortium where we can **build on our experience in this domain** and gap analyses from earlier work to address user needs and market requirements (rather then technology-push) to maximise impact.

Ulrich Seldeslachts ulrich@leadersinsecurity.org (richard.chisnall@leadersinsecurity.org)

Critical Security

- *Tuomas Tammilehto*
- *Tuomas.tammilehto@laurea.fi*
- *Laurea University of Applied Sciences, Finland*
- Role: *Proposal partner / WP Leader*

- SU-DS05-2018 - **Digital security, privacy, data protection and accountability in critical sectors**
  - ***[2018]: Digital security, privacy and personal data protection in finance***

Proposed role in the project

- *WP leader on* **End-User engagement**
- Collaboration and engagement of banking and financial market infrastructures in Finland and EU
- Defining sector-specific common requirements about digital security, privacy and personal data protection
- Co-creation workshops with multi-stakeholder engagement

- *WP leader on* **Exploitation and Dissemination**
  - Awareness building, competence development and training
  - Policy dialogs in CIP
  - Business models and sustainability of the project results
    - Laurea is a member of e.g. EOS, ECSO, ESDC

Tuomas Tammilehto, tuomas.tammilehto@laurea.fi

Project participants

- Partners / Other participants:
- 1 - Cyber Services, Hungary– SME
- 2 – Laurea UAS, Finland – HEI/RD

- Looking for partners with the following expertise/technology/ application field:
  - *Coordinator*
  - *Industry cooperation groups*
  - *Research organizations*
  - *Critical infrastructure as end user - finance*
  - *Legal/data privacy expert*

Tuomas Tammilehto, tuomas.tammilehto@laurea.fi

Digital security, privacy and personal data protection

- *Andreas Zalonis*
- *azalonis@iit.demokritos.gr*
- *NCSR DEMOKRITOS*
- Role: *WP leader and S/T provider*
- Proposal activity: *SU-DS05-2018, Digital security, privacy, data protection and accountability in critical sectors*

  (c) [2018]: Digital security, privacy and personal data protection in finance

Dr. Andreas Zalonis
Research Associate at the Integrated Systems Laboratory
Email: azalonis@iit.demokritos.gr
Phone number: (+30) 210 650 3189

Dr. Stelios C.A. Thomopoulos
Institute Director and Head of Integrated Systems Laboratory
Email: scat@iit.demokritos.gr
Phone number: (+30) 210 650 3154
Mobile: (+30) 6944 986699

Proposal key points

- Proof of concept testing and validation in controlled virtual environment
- Testing of cyber security incidents propagation effects
- Complexity assessment
- Tools for economic impact assessment and cost-efficiency
- Real time interaction and information sharing – monitoring, analytics, recommendations
- Tools for efficient investment polices
- Testing and validation in a federated customizable dynamic simulation platform based on the NCSRD's agent–based simulation engine
- Virtual environments and background processes tailored for the finance domain
- Behavioral model design based on experts theoretical use cases and log datasets
- Data mining, data analytics, personalization and recommendation engine

Andreas Zalonis – azalonis@iit.demokritos.gr

Project participants

NCSRD expertise and assets:

- Econometric analysis and models, Information sharing and efficient investment policies, data collection and analysis tools – SAINT project (Coordinator), DOGANA, CyberRoad, PACT
- Agent–based simulation engine and federated simulation platform for the creation of a controlled virtual environment – developed in FLYSEC (Coordinator), AF-3, TASS, PYRONES, PERSEUS

Consortium – looking for partners:

- Coordinator
- Banking industry, financial market infrastructures
- Digital security, privacy and personal data protection experts
- Insurance companies
- Fintech companies
- Experts in Information Systems security

Andreas Zalonis – azalonis@iit.demokritos.gr

Digital security, privacy data protection and accountibilityin critical sectors

- *Michelle Ryan*
- *Michelle.M.Ryan@ul.ie*
- *University of Limerick: Emerging Risk Group*
- Role: *Partner*

- Proposal activity: *SU-DS05 2018-2019 <Sub-topic A & C>*

Proposal idea/content

- Critical sectors need to access risk transfer mechanisms avaiable via the insurance markets to meet the sectors needs.
- We can working closely with insurers to demonstrate the gap between science and demonstrate the economic impact of risk transfer.
- In Transport Data Security and GDPR rules will be vital to the integrity of the autonomous driving market; demonstrating the use of data and security RT to end users will be essential.
- Common standards across markets should be driven by the insurance sector, and our unique viewpoint adds to any proposal.

Michelle Ryan / Michelle.M.Ryan@ul.ie

Project participants

- Proposed coordinator: *Looking to join a consortium*
- Partners / Other participants: *Looking to join a consortium*

- Looking for partners with the following expertise/technology/ application field:
  - *Experience in Autonomous Driving Research*
  - *Access to Financial Services Companies*
  - *Expertise with machine learning technology*

Michelle Ryan / Michelle.M.Ryan@ul.ie