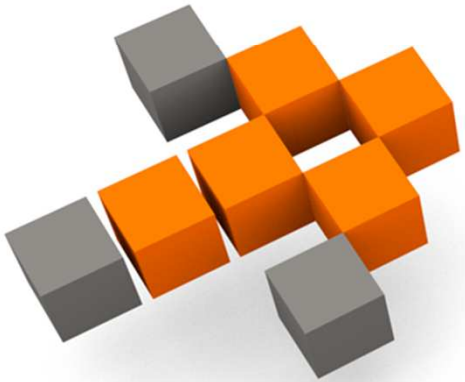
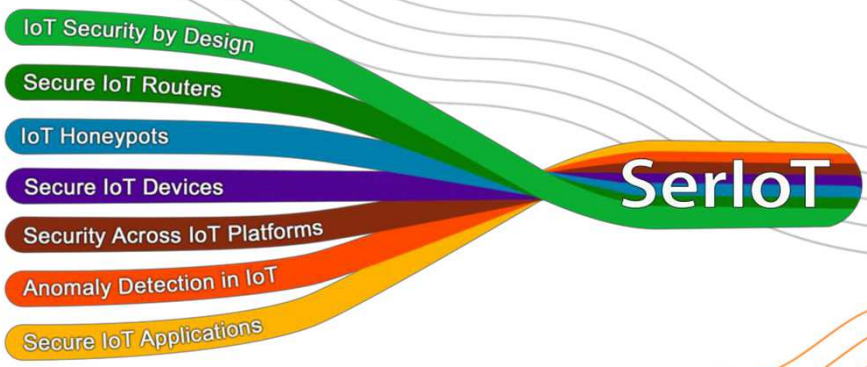
Instytut Informatyki Teoretycznej i Stosowanej Polskiej Akademii Nauk





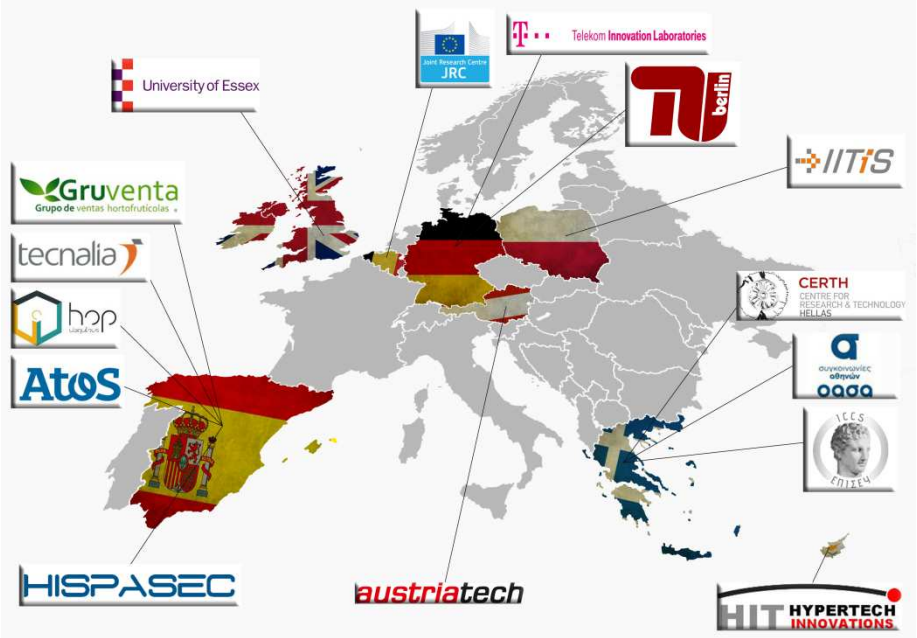
Dr hab. inż. Joanna Domańska – Zespół Sieci Komputerowych

Dr inż. Ryszard Winiarczyk– Zastępca Dyrektora

Dzień informacyjny ICT/FET w Programie Horyzont 2020
Warszawa, 28 listopada 2017

Secure and Safe Internet of Things

- Nazwa konkursu: IoT-03-2017 R&I on IoT integration and platforms
- Numer konkursu: H2020-IOT-2017
- Typ: RIA – Działania badawczo-innowacyjne
- Akronim: SerIoT
- Data rozpoczęcia: 1 stycznia 2018
- Czas trwania: 36 miesięcy
- Słowa kluczowe:
  - Internet Rzeczy
  - Systemy cyber-fizyczne
  - Systemy monitorowania i kontroli
- Budżet: 4 999 083,75 Euro
- Konsorcjum:
  - 15 partnerów z 8 krajów
  - 1 partner z Polski – IITiS PAN - koordynator



Członkowie konsorcjum (wg krajów): (1)

Polska:

- Instytut Informatyki Teoretycznej i Stosowanej PAN (koordynator) (IITiS)

Wielka Brytania:

- University of Essex (UESSEX) - współpraca z Network Convergence Laboratory (testbed)

Niemcy:

- Technische Universitaet Berlin (TUB) – współpraca z Security in Telecommunications (zagadnienia wirtualizacji Honeypotów)
- Deutsche Telekom AG (DT) - współpraca z Telecom Innovation Labolatories (wykrywanie anomalii)

Belgia:

- Joint Research Centre - European Commission (JRC) – współpraca z The Digital Citizen Security Unit G.06 of the Institute for the Protection and the Security of the Citizen (IPSC) (bezpieczeństwo i projektowanie rozwiązań bezprzewodowych)

Grecja:

- Institute of Communication and Computer Systems (ICCS) – specyfikacja architektury
- Ethniko Kentro Erevnas Kai Technologikis Anaptyxis (CERTH) – instytut naukowy
- Organismos Astikon Sygkoinonion Athinon AE (OASA) - przedsiębiorstwo transportowe (sieć testowa)

Członkowie konsorcjum (wg krajów): (2)

Hiszpania

- Hispasec Sistemas S.L. (HIS) – SME (problematyka bezpieczeństwa, testy penetracyjne)
- HOP Ubiquitous SL (HOPU) – SME (wkład w opracowanie bezpiecznej architektury, koordynacja z ciałami standaryzującymi)
- Atos Spain SA (ATOS) – koncern (globalny) IT (definiowanie wymagań dla SerIoT, wsparcie eksperckie)
- Fundacion Tecnalia Research & Innovation (TECNALIA) – przedsiębiorstwo badawcze (komercjalizacja innowacyjnych technologii)
- Grupo De Ventas Hortofruticolas Sl Gruventa (GRUVENTA) – użytkownik końcowy

Austria:

- Austriatech - Gesellschaft des Bundes für Technologiepolitische Maßnahmen GmbH (ATECH) – przedsiębiorstwo (instalacje testowe dla SmartCity)

Cypr:

- Hypertech Innovations Ltd (HIT) – przedsiębiorstwo IT (tworzenie instalacji końcowych w projekcie)

Wyzwania Internetu Rzeczy

- **Internet Rzeczy (IoT)** - codzienne urządzenia włączone do globalnej sieci. Na tej podstawie tworzone są koncepcje inteligentnych domów, miast, przedsiębiorstw, sieci zdrowia, sieci pomiarowych energetycznych itp. Podstawą tej koncepcji jest **komunikacja**.

- **IoT to najważniejsze technologiczne wyzwanie** w obszarze sieci komputerowych. Wymaga modyfikacji i rozwoju wszystkich warstw komunikacji i protokołów, od poziomu fizycznej konstrukcji urządzeń końcowych, do poziomu zarządzania i monitorowania siecią globalną.

Przewiduje się 25 miliardów urządzeń IoT do roku 2020. Wpływ na codzienne życie i procesy biznesowe w niemal wszystkich dziedzinach.

Problem globalny: bezpieczeństwo i zapewnienie prywatności, zarówno na poziomie całej sieci, jak i operatorów systemów IoT oraz użytkowników końcowych.

Planowane rezultaty projektu

Rola SerIoT polega na stworzeniu i zademonstrowaniu bezpiecznej, globalnej technologii Internetu Rzeczy.

- **Stworzenie nowej architektury sieci**, ze szczególnym uwzględnieniem funkcji monitorowania i automatyzacji procedur bezpieczeństwa (np. testów penetracyjnych);
- **Zaprojektowanie mechanizmów** na poziomie warstwy fizycznej urządzeń IoT i mechanizmów dostępu do sieci zapewnienie prywatności i transparentności danych;
- **Zaprojektowanie dedykowanych węzłów sieci (routerów)** poprzez adaptację technologii SDN (Software Defined Network) dla zapewnienie przepływów danych, dostosowanych do wymagań sieci IoT, ze wsparciem dla wykrywania przepływów, realizacji funkcji analitycznych i wykrywania anomalii;
- **Zaprojektowanie i stworzenie honeypotów** dla wykrywania i pozyskiwania danych o nieautoryzowanych próbach dostępu.

Znaczenie projektu

- **Kluczowe znaczenie na poziomie społecznym, związane z opracowaniem bezpiecznej i efektywnej platformy IoT**.

  Bez zapewnienie bezpieczeństwa rozwój (na skalę globalną) poszczególnych zastosowań Internetu Rzeczy nie byłby możliwy.

- **Znaczenie na poziomie gospodarczym związane ze stale rosnącym rynkiem IoT**.

  SerIoT może doprowadzić do stworzenia i rozwoju nowych strategii biznesowych o zasięgu globalnym.

Zadania w projekcie SerIoT

- WP1 – Wymagania dla koncepcji SerIoT oraz definicja struktury bezpieczeństwa IoT
- WP2 – Analiza i synteza architektury IoT
- WP3 – Bezpieczny ruter IoT (lider: IITiS)
- WP4 – Monitorowanie bezpieczeństwa IoT
- WP5 – Honeypoty IoT
- WP6 – Bezpieczeństwo i niezawodność urządzeń IoT i sieci dostępowych
- WP7 – Wdrożenie/Integracja
- WP8 – Demostracja technologii w dużej skali oraz ewaluacja systemu IoT
- WP9 – Rozpowszechnianie wyników, wykorzystanie i standaryzacja
- WP10 – Zarządzanie projektem (lider: IITiS)
- WP11 – Wymagania etyczne (lider: IITiS)

Wybrane prace

- Dostarczenie nowych środków umożliwiających zrozumienie zagrożeń gospodarki opartej na IoT, w tym badania nad wykorzystaniem technologii blockchain w zagadnieniach bezpieczeństwa IoT.
- Opracowanie koncepcji i dostarczenie prototypu implementacji centralnie zarządzanego, samopoznawczego i zorientowanego na IoT Honeypota, możliwego do zastosowania w dowolnej platformie IoT.
- Implementacja prototypu inteligentnego routera SDN służącego do detekcji i zmianie ścieżek przesyłania informacji w sieci IoT, z detekcją miejsc przetwarzania wrażliwych informacji, możliwością definiowania wymagań bezpieczeństwa i jakości ścieżek (zgodnie z mechanizmami SDN) oraz wsparcia bezpiecznej komunikacji z chmurą.
- Wprowadzenie dedykowanej bezpieczeństwu warstwy fizycznej platform i urządzeń IoT dla wsparcia architektury oferującej bezpieczeństwo oraz zdolności monitorowania sieci, wraz badaniem technologii blockchain jako warstwy zapewniającej bezpieczeństwo i prywatność.

Wybrane prace

- Poprawa bezpieczeństwa informacji w sieci IoT w ujęciu całościowym. Planowane jest zastosowanie rozproszonego gromadzenia i przetwarzania informacji adaptującego się dynamicznej struktury sieci
- Rozwinięcie istniejących technologii wspomagania decyzji po stronie kontrolera, gdzie są zbierane wszystkie dane i metadane, aby: wykryć potencjalne zagrożenia, włączyć odpowiedni zestaw analiz oraz wybór strategii reakcji w zależności od rodzaju wykrytych zagrożeń.
- Podniesienie efektywności komunikacji poprzez przyspieszenie procesów komunikacji oraz wybór optymalnych ścieżek przesyłu.
- Weryfikacja opracowanych technologii według reprezentatywnych rzeczywistych scenariuszy, zarówno w małej, jak i w dużej skali, obejmujących niejednorodne urządzenia i platformy IoT.

Okiem koordynatora

- Kontakty, kontakty i jeszcze raz kontakty
- Przygotowanie i złożenie projektu
  - Participant Portal
- Grant Agreement
  - Accession forms
- Consortium Agreement
  - Płatności - harmonogram
  - Ochrona praw intelektualnych – wspólne wyniki
- ……

rzepraszam, za przeciążenie ☺

Dziękuję za uwagę