Krajowy Punkt Kontaktowy
PROGRAMÓW BADAWCZYCH UE

Warszawa, 02.10.2018
Dzień informacyjny dla miast

HORYZONT 2020

ICT - technologie informacyjne i komunikacyjne

Możliwości finasowania

Rafał Duczmal
ICT, Europejskie Infrastruktury Badawcze

Krajowy Punkt Kontaktowy Programów Badawczych UE
Instytut Podstawowych Problemów Techniki PAN
www.kpk.gov.pl

W niniejszej prezentacji wykorzystano materiały udostępnione m.in. przez KE i/lub Ministerstwa oraz Agendy RP

BY-NC-ND

SU-INFRA02-2019: Security for smart and safe cities, including for public spaces

- W miastach, przestrzenie publiczne, takie jak centra handlowe, otwarte zatłoczone miejsca spotkań i wydarzeń oraz nieograniczone obszary infrastruktury transportowej stanowią liczne cele rozłożone na całym obszarze miejskim i są narażone na "tanie" ataki silnie dotykające obywateli.
- Generowanie, przetwarzanie i udostępnianie dużych ilości danych w inteligentnych miastach sprawia, że systemy i usługi miejskie są potencjalnie bardziej elastyczne i mogą działać na podstawie danych w czasie rzeczywistym.
- Inteligentne miasta zapewniają poprawę bezpieczeństwa poprzez wykorzystanie szerokich sieci wykrywania i prewencji.
- Odrębne inteligentne systemy wykrywania i prewencji w ramach inteligentnego miasta wymagają wspólnego podejścia do zarządzania bezpieczeństwem cybernetycznym.

BY-NC-ND

SU-INFRA02-2019: Security for smart and safe cities, including for public spaces

ZAKRES TEMATU:

Propozycje w ramach tego tematu powinny rozwijać i integrować eksperymentalnie (na miejscu), elementy otwartej platformy wymiany informacji i zarządzania informacjami między podmiotami świadczącymi usługi publiczne i praktykami w dziedzinie bezpieczeństwa w dużym, inteligentnym mieście.

Proponowane projekty pilotażowe powinny zaprezentować w jaki sposób można połączyć miedzy innymi:

- Metody wykrywania broni, materiałów wybuchowych, substancji toksycznych
- Systemy nadzoru wideo
- Metody identyfikacji i neutralizacji sprawców przestępstw przy jednoczesnej minimalizacji ingerencji w obszary zatłoczone

BY-NC-ND

SU-INFRA02-2019: Security for smart and safe cities, including for public spaces

Przy projektowaniu platformy należy przedstawić propozycje:

- aktywnie angażować podmioty odpowiedzialne za bezpieczeństwo na obszarze miasta, ich koordynację i zarządzanie nimi;
- rozwiązywać problemy związane z interoperacyjnością oraz zapewniać połączenie i integrację inteligentnych systemów miejskich z systemami wspierającymi lokalnych praktyków bezpieczeństwa, w tym poprzez modelowanie i symulację ich współzależności;
- zwiększenie bezpieczeństwa inteligentnych systemów miejskich, zwłaszcza w zakresie kontroli dostępu (np. za pomocą cyfrowych środków bezpieczeństwa, takich jak warstwowe uwierzytelnianie i dostęp), bezpiecznych komunikacja i przechowywanie danych oraz przeciwdziałanie ich ewentualnym nadużyciom ze strony przestępców;
- rozważyć nowe koncepcje działania wynikające z nowych metod monitorowania, danych dostarczanych przez rozległe sieci czujników i mediów społecznych;
- rozważyć strategie łagodzenia skutków w kontekście różnych scenariuszy w celu zwiększenia odporność;
- integrować moduły symulujące incydenty związane z bezpieczeństwem i ich konsekwencje;
- integrować moduły do pomiaru ilościowego i jakościowego wpływu platformy na bezpieczeństwo;
- zapewnić wymianę, konsolidację i analizę danych pochodzących z wielu źródeł;

BY-NC-ND

SU-INFRA02-2019: Security for smart and safe cities, including for public spaces

Wnioski projektowe powinny dotyczyć co najmniej jednej z następujących kluczowych kwestii

- Symulacja, wykrywanie i analiza dodatkowych zagrożeń i ryzyk związanych z bezpieczeństwem poprzez połączenie inteligentnych systemów (np. Internet Rzeczy (IoT), w szczególności obiekty Internetu Rzeczy wykorzystywane w praktyce w dziedzinie bezpieczeństwa) i inteligentnej infrastruktury (np. inteligentne (rządowe) budynki, inteligentne koleje, inteligentne porty, inteligentne fabryki, inteligentne mosty, inteligentne szpitale, duże skupisko ludzi w inteligentnej infrastrukturze) w ramach inteligentnego miasta;

- Dostarczenie ram bezpieczeństwa cybernetycznego w celu ułatwienia współpracy wszystkich interesariuszy inteligentnych miastach, od urbanistów po operatorów infrastruktury, praktyków bezpieczeństwa, informatyków i usługodawców w inteligentnych organizacjach na terenie miasta;

- Wsparcie i wdrożenie wspólnego podejścia do zabezpieczenia i zarządzania, w niezawodny i nieskazitelny sposób przetwarzania danych ze wszystkich inteligentnych infrastruktur i systemów w inteligentnym mieście wspierając obywateli, władze publiczne, specjalistów ds. bezpieczeństwa i gospodarkę miejską w tworzeniu przejrzystych, efektywnych i odpowiedzialnych cyfrowo zabezpieczonych procesów przetwarzania danych, zgodne z przepisami o ochronie danych.

BY-NC-ND

SU-INFRA02-2019: Security for smart and safe cities, including for public spaces

Expected Impact:

- Stworzenie dedykowanych, zharmonizowanych, zaawansowanych rozwiązań w zakresie bezpieczeństwa cybernetycznego dla inteligentnych miast, przyjmujących wspólne podejście ze wszystkimi zainteresowanymi stronami (np. administratorami inteligentnych miast/portów/transportu), równoważące ich - czasem sprzeczne - cele (np. rozwój obszarów miejskich, wydajność, wzrost, konkurencyjność, odporność).
- Pokazy in situ skutecznych i efektywnych kosztowo rozwiązań dla największej grupy odbiorców, poza uczestnikami projektu.
- Łatwiejszy poziom integracji poprzez opracowanie całościowych ram bezpieczeństwa cybernetycznego dla inteligentnych miast, które przyniosą korzyści wszystkim inteligentnym infrastrukturom znajdującym się w ich obrębie (np. inteligentne budynki, inteligentne porty, inteligentne koleje, inteligentna logistyka).
- Ekosystemy Internetu Rzeczy (a nie rozproszone infrastruktury Internetu Rzeczy) zbudowane przyjmując wspólne podejścia w zakresie zarządzania bezpieczeństwem cybernetycznym, osiągając korzyści skali (np. unikanie powielania wysiłków w zakresie analizy danych z Internetu Rzeczy, wyboru bezpieczeństwa cybernetycznego kontrole).
- Nowe koncepcje operacji uwzględniające wielorakie, heterogeniczne źródła danych oraz media społecznościowe.
- Nowe narzędzia i systemowe podejścia do ochrony obywateli przed zagrożeniami dla celów miękkich w Smart City.

BY-NC-ND

SU-INFRA02-2019: Security for smart and safe cities, including for public spaces

Informacje dodatkowe:

- Wykorzystane technologie powinny oscylować wokół poziomu 7 na sakli gotowości technologicznej TRL.
- Wszystkie zastosowane rozwiązania muszą być zgodne z zasadami przetwarzania i ochrony danych (GDPR – RODO, Data Managment Plan)
- Przewidywane dofinansowanie 8mln Euro (budżet konkursu 16mln Euro)
- Termin zamknięcia naboru wniosków: 22 Sierpnia 2019. Otwarcie konkursu: 14 marca 2019.
- Przynajmniej 2 samorządy lokalne miast lub obszarów metropolitalnych w 2 państwach członkowskich lub krajach stowarzyszonych muszą być beneficjentami (ewentualnie, ale niekoniecznie: koordynatorem) umowy grantowej i powinny być bezpośrednio zaangażowane w realizację zadań przewidzianych w projekcie.
- Wymagany jest udział przemysłu zdolnego do zapewnienia rozwiązań w zakresie bezpieczeństwa.
- Czas trwania proponowanych działań nie może przekraczać 24 miesięcy.

BY-NC-ND

ICT Work Programme 2020

- DT-ICT-12-2020 The smart hospital of the future
- Treść dostępna będzie późną wiosną 2019

Gdzie znaleźć treść Programów Pracy

- ICT
http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-leit-ict_en.pdf
- Security
http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-security_en.pdf

BY-NC-ND

ICT 2018: Imagine Digital - Connect Europe

4-6 grudnia 2018, Wiedeń, Austria

https://ec.europa.eu/digital-single-market/en/events/ict-2018-imagine-digital-c

Informacje o ICT WP2018-20

Networking sessions- prezentacja pomysłów

Fot. ACCOR FOTO / materiały prasowe

Spotkania brokerskie Face2Face

Stoiska projektów i inicjatyw

ZAPRASZAMY DO KONTAKTU

KRAJOWY PUNKT KONTAKTOWY
PROGRAMÓW BADAWCZYCH UE

Instytut Podstawowych Problemów Techniki PAN

Zespół ICT

Małgorzata Szołucha
kom. +48 664 032 128
malgorzata.szolucha@kpk.gov.pl

Rafał Duczmal
kom. +48 664 032 132
rafal.duczmal@kpk.gov.pl

ZAPRASZAMY DO KONTAKTU

KRAJOWY PUNKT KONTAKTOWY
PROGRAMÓW BADAWCZYCH UE

Instytut Podstawowych Problemów Techniki PAN

Zespół Security

Renata Rycerz
kom. +48 508 101 124
renata.rycerz@kpk.gov.pl

Mikołaj Pyczak
kom. +48 664 032 125
mikolaj.pyczak@kpk.gov.pl