Privacy preserving protocols for encounter metrics

Angela Robinson and **René Peralta**
Privacy enhancing cryptography group
NIST

Workshop on Challenges for Digital Proximity Detection in Pandemics: Privacy, Accuracy, and Impact, January 2021

Privacy preserving protocols for encounter metrics

Angela Robinson and **René Peralta**
Privacy enhancing cryptography group
NIST

(paper to appear, available upon request)

Workshop on Challenges for Digital Proximity Detection in Pandemics: Privacy, Accuracy, and Impact, January 2021

Motivation

We should be better prepared for the next pandemic

Motivation

We should be better prepared for the next pandemic

- NIST is a metrology institute.

Motivation

We should be better prepared for the next pandemic

- NIST is a metrology institute.
- We frame the proximity detection problem as that of **measuring** levels of interactions in a population of **autonomous agents**.

Motivation

We should be better prepared for the next pandemic

- NIST is a metrology institute.
- We frame the proximity detection problem as that of **measuring** levels of interactions in a population of **autonomous agents**.
- In human populations, higher levels of interaction means faster spread of infectious diseases.

Motivation

We should be better prepared for the next pandemic

- NIST is a metrology institute.
- We frame the proximity detection problem as that of **measuring** levels of interactions in a population of **autonomous agents**.
- In human populations, higher levels of interaction means faster spread of infectious diseases.
- Besides enabling automatic contact tracing, we want to help engineer environments so as to slow the spread of disease.

Encounter metrics

Two people coinciding in a space/time window is an encounter.

Encounter metrics

Two people coinciding in a space/time window is an encounter.

- Detect encounter.

Encounter metrics

Two people coinciding in a space/time window is an encounter.

- Detect encounter.
- Label the encounter (not the parties involved).

Encounter metrics

Two people coinciding in a space/time window is an encounter.

- Detect encounter.
- Label the encounter (not the parties involved).
- Evaluate length or severity of encounter.

Encounter metrics

Two people coinciding in a space/time window is an encounter.

- Detect encounter.
- Label the encounter (not the parties involved).
- Evaluate length or severity of encounter.
- Aggregate and derive encounter metrics statistics.

Encounter metrics

Two people coinciding in a space/time window is an encounter.

- Detect encounter.
- Label the encounter (not the parties involved).
- Evaluate length or severity of encounter.
- Aggregate and derive encounter metrics statistics.
- Use for contact tracing and to engineer our working environments to slow spread of infectious diseases.

Encounter metrics

Two people coinciding in a space/time window is an encounter.

- Detect encounter.
- Label the encounter (**not the parties involved**).
- Evaluate length or severity of encounter.
- Aggregate and derive encounter metrics statistics.
- Use for contact tracing and to engineer our working environments to slow spread of infectious diseases.

A problem that requires mitigation

We are constantly exposing our identity to machines.

- When in front of a security camera, or a traffic camera
- When swiping a credential for accessing a restricted area
- When using a credit card, or at the ATM
- ...

A problem that requires mitigation

We are constantly exposing our identity to machines.

- When in front of a security camera, or a traffic camera
- When swiping a credential for accessing a restricted area
- When using a credit card, or at the ATM
- ...

Pseudonyms being broadcast in all these cases can be linked to an identity.

A problem that requires mitigation

We are constantly exposing our identity to machines.

- When in front of a security camera, or a traffic camera
- When swiping a credential for accessing a restricted area
- When using a credit card, or at the ATM
- ...

Pseudonyms being broadcast in all these cases can be linked to an identity.

In the context of contact tracing for COVID-19, systems that expose the pseudonyms of infected people may also be exposing their identities.

Protect privacy

The system must be used for public health.

The system must not be capable of collecting, processing, or transmitting any more data than what is necessary to achieve this purpose.

Solutions must be fully transparent. The protocols and their implementations, including any sub-components provided by companies, must be available for public analysis.

Protect privacy

The system must be used for public health.

It is problematic if the App is subordinate to commercial processes and constraints.

The system must not be capable of collecting, processing, or transmitting any more data than what is necessary to achieve this purpose.

Solutions must be fully transparent. The protocols and their implementations, including any sub-components provided by companies, must be available for public analysis.

Protect privacy

The system must be used for public health.

It is problematic if the App is subordinate to commercial processes and constraints.

The system must not be capable of collecting, processing, or transmitting any more data than what is necessary to achieve this purpose.

It is problematic if the system is installed on top of a surveillance platform such as current smart phones.

Solutions must be fully transparent. The protocols and their implementations, including any sub-components provided by companies, must be available for public analysis.

Protect privacy

The system must be used for public health.

It is problematic if the App is subordinate to commercial processes and constraints.

The system must not be capable of collecting, processing, or transmitting any more data than what is necessary to achieve this purpose.

It is problematic if the system is installed on top of a surveillance platform such as current smart phones.

Solutions must be fully transparent. The protocols and their implementations, including any sub-components provided by companies, must be available for public analysis.

It is problematic if we are not given low level access to the platform.

Protect privacy

Figure 1: Our colleague Sae Woo Nam.

THANK YOU