UNIVERSITÀ DEGLI STUDI FIRENZE
DINFO
Dipartimento di Ingegneria dell'Informazione
Department of Information Engineering
cnit consorzio nazionale interuniversitario per le telecomunicazioni

Sicurezza e privacy nella IoT

Una iniziativa europea

Enrico Del Re

Sicurezza informatica

Requisiti

- Autenticazione
  - Garanzia che le entità in comunicazione siano effettivamente chi sostengono di essere
- Controllo degli accessi
  - Garanzia di un utilizzo autorizzato ad una risorsa
- Integrità dei dati
  - Garanzia che i dati ricevuti siano *esattamente* quelli inviati
- Non ripudiabilità
  - Protezione contro la possibilità che il mittente (o il destinatario) possano negare l'invio (o la ricezione) dei dati
- Disponibilità del servizio
  - Garanzia che il servizio sia disponibile al momento della richiesta
- Riservatezza dei dati
  - Protezione dei dati contro ogni accesso e utilizzazione non autorizzati

Sicurezza e Posizione UE

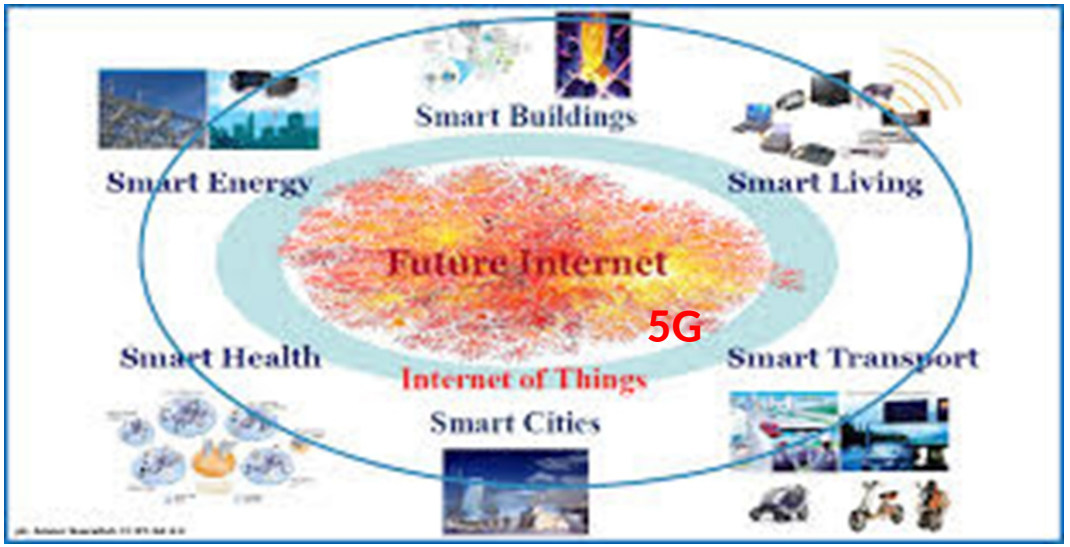
- "**Building trust in the online environment is key to economic development.** Lack of trust makes consumers hesitate to buy online and adopt new services, including public e-government services. If not addressed, this lack of confidence will continue to slow down the development of innovative uses of new technologies, to act as an obstacle to economic growth and to block the public sector from reaping the potential benefits of digitisation of its services, e.g. in more efficient and less resource intensive provisions of services. This is why data protection plays a central role in the Digital Agenda for Europe, and more generally in the Europe 2020 Strategy." [1]

[1] European Commission, 25.01.2012, SEC(2012)72 final, page 4.

- Gli ultimi sviluppi delle tecnologie ICT hanno reso ancora più critico lo scenario:
  - Potenza di elaborazione (bruta e algoritmi)
  - Flessibilità (HW e SW)
  - Internet (e soprattutto IoT)
  - Reti wireless (5G)
  - Cloud computing
  - Big Data
  - Pervasività

IoT (e IoE)

- IoT (Internet delle Cose)
  - Oggetti e sensori intelligenti in rete
  - > 50 miliardi nel 2020
  - Per alcuni in prospettiva 1000 miliardi
- IoE (Internet di Ogni cosa)
  - Non solo oggetti, ma qualunque fonte di informazione e/o di azione (IoX)



- 5G
  - Capacità di connettere e interagire con gli oggetti della IoT

Sicurezza informatica e IoT

- Dati personali acquisiti, memorizzati, elaborati, trasmessi, utilizzati ***anche*** all'insaputa degli interessati (*data subjects*)
- Rischio di violazione dei diritti fondamentali delle persone

Sicurezza informatica e IoT

- Tutti i requisiti di sicurezza sono **oggi** realizzati da enti terzi (i fornitori dei servizi e/o gli operatori di rete) mediante opportune procedure (protocolli) offerte all'utente al momento della richiesta di un servizio
- Per i primi cinque: inevitabile e corretto
- Le attuali tecniche tradizionali per la protezione delle informazioni sono **adatte a garantire la riservatezza dei dati personali nella futura IoT?**
- Rischio di rifiuto parziale o totale dei nuovi servizi da parte di utenti in **mancanza di fiducia nelle nuove tecnologie** [vedi UE,2012]
- O, peggio, rischio per le persone di diventare oggetti sfruttati di alcune (poche) grandi organizzazioni (anche sovranazionali)

Alcune dichiarazione UE su Sicurezza e Riservatezza[1]

La progettazione dei nuovi sistemi deve includere come requisiti iniziali:

- *Diritto alla cancellazione*
- *Diritto all'oblio*
- *Portabilità dei dati*
- *Protezione e riservatezza dei dati*

tenendo in considerazione due principi generali:

- *IoT (e IoE) non deve violare l'identità e l'integrità umana, i diritti umani, la privacy o le libertà individuali e pubbliche*
- ***Gli individui devono mantenere il controllo dei propri dati personali generati o trattati**, a meno che ciò sia in contrasto con il principio precedente.*

[1] European Commission. IoT Privacy, Data Protection, Information Security.
http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753

A che punto siamo? (1/2)

- Ieri (25 maggio 2018) è entrato in vigore in tutta la UE il GDPR (*General Data Protection Regulation*)
- Precisato da *Working Party Articolo 29: Guidelines on consent under Regulation 2016/679 last Revised and Adopted on 10 April 2018.*
- *Consent: freely given, specific, informed and unambiguous*
- Non dato una volta per sempre, ma rinnovato ogni volta che i dati personali sono utilizzati per scopi diversi da quelli autorizzati inizialmente
- Sanzioni pesanti per i fornitori di servizi che non rispettano il GDPR
- È un significativo passo avanti, ma è sufficiente?

A che punto siamo? (2/2)

- La riservatezza è ***ancora*** affidata al rispetto delle regole da parte dei fornitori di servizi
- Si può realizzare: *Gli individui devono mantenere il controllo dei propri dati personali generati o trattati* ?
- È una soluzione studiata nell'ambito del cosidetto paradigma "user-centric security and privacy" (solo in ambito UE?)

User-centric Security and Privacy

- Sicurezza e riservatezza "by design" fin dall'inizio dello sviluppo di applicazione/servizio (e non aggiunte successivamente)
- Sicurezza e riservatezza dei dati dell'utente sotto il **controllo del possessore** con soluzioni tecniche più efficienti e semplici possibili
- **Coinvolgimento sociale attivo degli utenti** fin dall'inizio:
  - Educazione e consapevolezza dei propri diritti
  - Soluzioni tecniche adeguate per soddisfare requisiti condivisi

Bando UE CHIST-ERA 2015:
User-Centric Security, Privacy and Trust in the Internet of Things

- Numero proposte: 36
- Accettate: 6 (durata 3 anni dal 2017)

Cocoon: *Emotion psychology meets cyber security in IoT smart homes* BE, CH, NL, **UK**
-emotional psychology of IoT users
-implementation of an Intrusion Detection System in the home environment

ID_IOT: *IDentification for the Internet Of Things* CH, FR, **NL**
-quantum secure authentication by optical Physical Unclonable Functions (PUF)

SPIRIT: *Security and PrIvacy foR the Internet of Things* CH, FR, **UK**
-semantic firewall e content-based signature per i documenti
-crittografia a livello fisico

SUCCESS: *SecUre aCCESSibility for the internet of things* FR, NL, **UK**
- protezione dati nella sanità (Alzheimer)

UPRISE-IoT: *User-centric PRivacy & Security in the IoT* **CH**, FR, UK
-controllo sull'utilizzo delle app (smartphones) dei dati dell'utente

USEIT: *User empowerment for Security and prIvacy in Internet of Things* **CH**, ES, FR, NL
-symmetric criptography
-smart vehicles, dynamic environments

Bando UE CHIST-ERA 2015:
User-Centric Security, Privacy and Trust in the Internet of Things
Considerazioni

- Aspetti specifici nei progetti in corso
  - Smartphones, documenti, crittografia a livello fisico, sanità, mobilità, domotica
  - Manca una visione complessiva della IoT
  - Controllo degli interessati spesso solo nella fase iniziale del consenso e non in ogni fase successiva
- *Blockchains*
  - Strumento utilissimo per la verifica *a posteriori* dell'utilizzo dei dati utente, non adatto al controllo preventivo e *in itinere*
  - Presenti in molte delle 36 proposte, in nessuna di quelle accettate

Information-centric cybersecurity

- **Paradigma rivoluzionario**: **autoprotezione (interna) dei dati** invece della protezione (esterna) da parte dei sistemi e/o delle applicazioni
- **Incorporare intelligenza** nel dato stesso
- Dati che si **autodifendono** in qualunque contesto applicativo
- Definizione di **una politica di uso** del dato
- Al **momento dell'accesso** il dato consulta la sua 'politica di uso' e dà il consenso solo se il contesto è affidabile e coerente con la sua politica di uso

R. Chow, et al., *Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control*, *ACM CCSW'09*, 2009
R.B Lee, *Rethinking computers for cybersecurity*, *IEEE Computer*, 2015
IEEE Communications Mag., Jan. 2017

Grazie per l'attenzione

Q&A ?