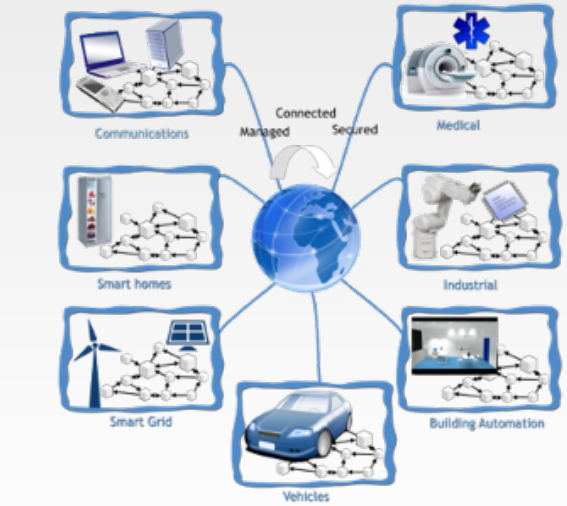
Tackling Data Security and Privacy Challenges for the Internet of Things

Dave Raggett
W3C
Tuesday, 14th June 2016
IoT TechExpo, Berlin

The Promise of the Internet of Things

- Services that are enriched through access to the physical and abstract World
- Smart Homes
- Smart Cities
- Smart Businesses
- Smart Government
- Environment, healthcare, agriculture, manufacturing, logistics and many more



Security and Privacy Challenges for the Internet of Things

- "*Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities* ", NTIA May 2016
- *How long will consumers put up with the IoT's failures?* – IoT support panel, CES 2016
- IoT "plug and pray" all over again, says security consultant David Alexander, PA Consulting, CRESTcon & IISP 2016
- Three quarters of UK's information security professionals think IoT device manufacturers aren't implementing enough security on their products and 73% said there's a general lack of industry standards – ISACA 2015 poll
- 72% of Americans see cyberattacks as a major threat, coming 2nd after ISIS – Pew Research poll, April 2016
- "*All of the potential weaknesses that could afflict IoT systems, such as authentication and traffic encryption, are already well known to the security industry...* ", Insecurity in the Internet of Things, Symantec, March 2015

Eight Internet of Things Fails due to sloppy practices and poor usability

- Target's Heating and Cooling System
  - Hackers gained access through HVAC account, and were able to install card skimming s/w on POS terminals
- Wink's IoT Hubs
  - Consumers found their devices bricked when the Hub security certificate unexpectedly expired
- Insteon connected homes
  - Reporter able to turn lights on and off whilst chatting with home owners over the phone
- Home routers
  - Open to man in the middle attacks when people use default or easy to guess passwords

From: The Observer, 16 July 2015

- Spammy refrigerators
  - Default passwords allowed attacker to use connected refrigerators as part of a `bot net
- TrendNet's nanny cams
  - Easy remote access once you have the camera's IP address
- Samsung's smart TVs
  - Easy to commandeer to view people's living rooms
- Nest thermostat
  - Easy to hack if you can get physical access for a few minutes

Note: these products have either been withdrawn or patched

IoT Security Should Worry Us All

- Breaches of privacy
- Cybercrime
- Physical safety in the home, across the city and within businesses
- Threats to national infrastructure
- Looming risks of cyberwar

Unique Challenges for IoT Security

- IoT relies on microcontrollers with limited memory and computational power
  - This often makes it impractical to implement approaches designed for powerful computers
  - This in turn requires constrained IoT devices to be hidden behind secure gateways
- Threats based upon gaining physical access to IoT devices
- How to bootstrap trust and security, and ways that this can unravel
- Evolving technology
  - More powerful Systems on a Chip (SOC) embedding hardware security support
  - Ecliptic Curve Cryptography with reduced computational demands
- Anything that is exposed to the Internet must be securely software upgradable
- User experience must be good enough to avoid becoming a weak link in the chain
- The necessity of keeping up to date with security best practices

The Challenges for the IoT and Big Data

- Lots of sensors will generate a vast amount of data
  - API Research estimated 200 exabytes in 2014 and 1.6 zettabytes in 2020
  - 90% is currently processed locally, although this varies by domain
- This creates a greater volume of sensitive data, creating a greater risk of
  - Data and identity theft,
  - Device manipulation,
  - Data falsification
  - IP theft, server/network manipulation, etc.
- Impact of introduction of data consolidation and analytics at network edge
  - Cisco, HPE and others
  - App platforms in the cloud or at the network edge will be targets for attacks

Enabling Data Security for the Internet of Things

- Transport and app layer encryption
  - TLS and DTLS for encrypting data transmitted over the Internet
  - App layer encryption for greater security (e.g. as in financial transactions)
  - Secure key exchange algorithms over unsecured channels
- Authentication and Key management
  - IoT devices need to check that the server is who it says it is
  - Servers likewise need to check this for IoT devices
  - Asymmetric Public/Private key pairs vs Symmetric keys
  - Tamper resistant storage of keys and certificates
  - Challenges for provisioning services

Authorisation – Determining Who Can Do What

- Authorisation rules
  - Authentication of the data recipient
  - Simple form of rules as access control lists
  - More general rules with complex conditions
- Capability based security
  - A capability is communicable and unforgeable token of authority
  - The token is associated with a set of access rights
- IETF work on ACE and JOSE
  - ACE: access control in constrained environments
  - JOSE: JavaScript Object Signing and Encryption
- Relationship to models of trust
  - Prior agreements between two parties
  - Attestations by trusted third parties

Privacy and the Internet of Things

- The IoT has the potential to provide huge and unprecedented amounts of personal information
  - This information may last indefinitely
  - Risk of abuse by individuals, criminals, companies and governments
  - Sense of intrusion into your personal space
  - Fear of harm due to disclosure of personal information
- Strongly identifying information
  - Your address, data of birth, sexual orientation, …
  - Principle of data minimisation – high cost to companies for handling personal data securely
  - Privacy policies determining what purposes data can be used for, and for how long
- Weakly identifying information
  - When sufficient such data is combined this can uniquely characterise you
  - Companies need to provide privacy policies on how they handle such data
- Need for adhering to best practices to avoid reputational damage to companies
  - Including regulatory requirements

The IoT and the Web

- Web technologies are increasingly important for the IoT
  - Web protocols like HTTP
  - Semantic descriptions based on RDF
  - HTML5 and the Open Web Platform for human machine interface
- The Web security model and its relationship to the IoT
  - Access rights for web apps are scoped to app's origin
  - The Web is moving to encrypt all communication
  - We're preparing to transition the Web from passwords to public key crypto
    - Users authenticate to the browser, and browser authenticates to the website
- For the IoT, the user (owner) isn't around at the time the device needs to authenticate itself to a service
- We therefore need a way for users to authorize the device in advance
  - This is a form of trust delegation, and introduces the need to authenticate users as well as service providers

Some Take Away Messages

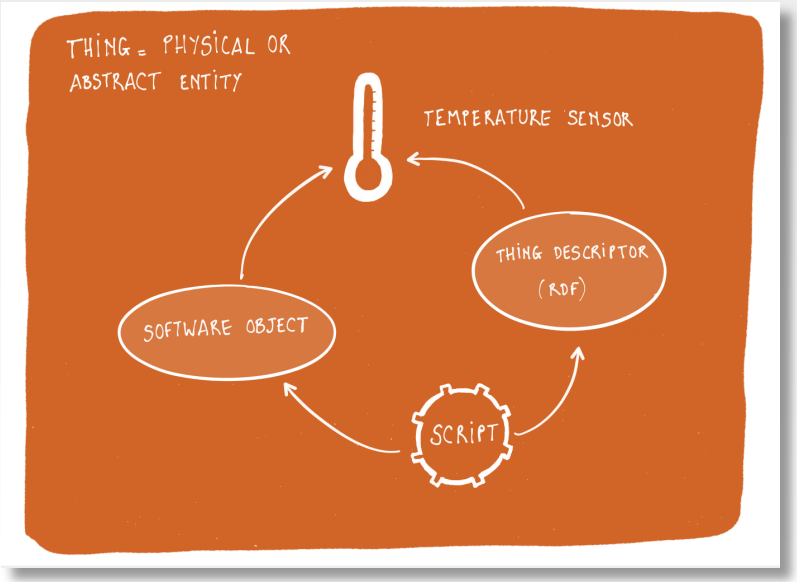
- **Security is crucial and must not be seen as an afterthought**
  - Need to consider security and privacy from the start
  - Need to adhere to evolving best security practices
  - Failure to do so risks reputational and financial damage
- **Recruit experienced security staff**
  - Take advantage of the available resources, e.g.
    - Internet of Things Security Foundation
    - OWASP IoT Security Guidance
    - IAB Privacy & Security studies
      - RFC 7452 – Architectural Considerations in Smart Object Networking
      - RFC 7456 – Cryptographic algorithm agility
    - EU Article 29 Data Protection Working party
      - Anonymization, privacy and the IoT
  - Track the emerging standards, e.g.
    - W3C Security Activity
    - IETF ACE & JOSE
- Some tips from Mike Turner @ Computer Weekly
  - Set up an integrated team of business executives and security specialists
  - Integrate security best practice with the IoT product development process
  - Educate consumers as well as front-line staff in security best practice
  - Address privacy concerns with easy to understand privacy policies

Overcoming the Fragmentation of the Internet of Things

- Today, there are many non-interoperable platforms and a surfeit of technologies and standards
- This creates silos, increases development costs and reduces the market potential
- W3C is the leading organization for Web technology standards
- We're working on approaches to overcoming fragmentation and enabling open markets of services
- Analogy with network services before and after the Internet was introduced
- Get it right and there will be exponential growth in IoT services

The Web of Things

- A heterogeneous set of platforms, serving different needs
  - No one platform and protocol can be expected to win out
- The Web of Things
  - "Things" denoting physical and abstract entities
  - Cross platform standards for application access to "things"
- Rich metadata describing "things"
  - What data and interaction models are exposed to applications?
  - What protocols and communication patterns can be used?
  - What kind of a thing is it (semantic models and constraints)?
  - What are the relationships to other things?
- Web of Things as inter-platform Web technology standards
  - Based upon W3C's established strengths in semantic technologies, web security and the open web platform



Web of Things – Key Challenges

- Semantic interoperability – ensuring that communicating parties share the same meaning for data
  - Platforms may use different protocols and data formats, but without shared meaning, it won't be possible to build services that integrate data across platforms
- Shared trust assumptions for end to end security across platforms
  - How are the entities involved named and authenticated?
  - How is trust established across these entities?
  - How are authorization policies described?
  - Do all of the parties use high levels of security?
- Enabling resilience of services
  - Best practices for dealing with faults and attacks
  - Defence in depth and its implications
  - Security, monitoring, machine learning and policies

World Wide Web Consortium

Mission: lead the Web to its full potential

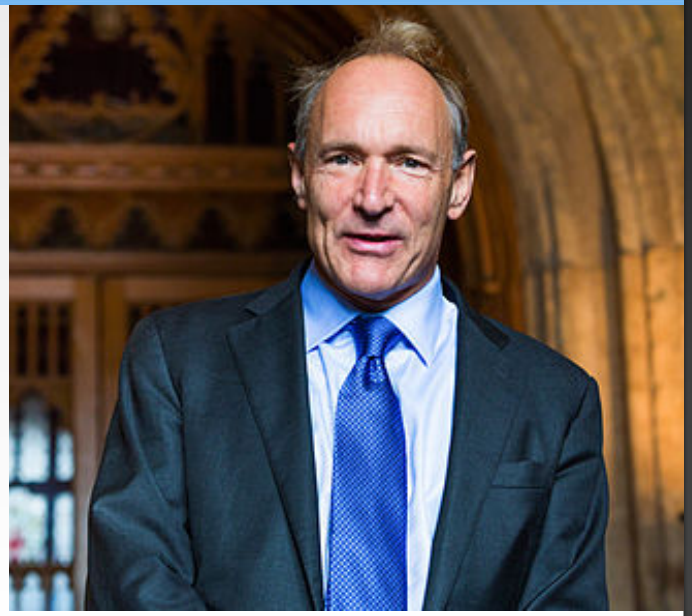
- The Web is the world's largest vendor-neutral distributed application platform

Founded by Sir Tim Berners-Lee, inventor of the Web

- 400+ Members
- Member-funded international organisation

Develops standards for Web and semantic technologies

- HTML, CSS, scripting APIs, XML, SVG, VoiceXML, Semantic Web and Linked Data etc.
- Developer oriented, enabling cooperation between organisations with very different backgrounds
- W3C patent policy for royalty free standards
- W3C staff of engineers actively participating in standardisation
- Increasingly involved in verticals: Mobile, TV, Automotive, Digital publishing



W3C Web of Things

- Web of Things Interest Group – exploring the potential through technology surveys and experimental implementations
- Web of Things Working Group – planned for late 2016 – will develop initial standards
- Web of Things Business Group – under discussion – to guide technical work based upon analysis of business and policy level requirements across many application domains

Web of Things Interest Group, Montreal 2016

The Bottom Line

The Web is essential for realizing the full potential of the IoT

The Web provides a unifying framework for semantic interoperability

The Web acts as a global marketplace for suppliers and consumers of services

Work with us to secure the Web of Things!

For more information on W3C see:

www.w3.org

Thank you!