CSE 465

Information Assurance

IA of Internet of Things

Professor Stephen S. Yau

Spring, 2017

Internet of Things (IoT)

- ***Internet***
- ***Internet of Things (IoT)***
- ***Internet of People (IoP)***
- ***Internet of Everything (IoE)***
- ***Cloud Computing***
- ***Edge Computing***
- ***Fog Computing***

Internet and Related Technologies

- ***Computer networks***
  - ***ARPANET, NSFNet, etc.***
  - ***Wireless networks***
  - ***Sensor networks***
- ***Microelectronics and nanotechnology***
- ***Ubiquitous computing (pervasive computing)***
- ***Autonomous computing***
- ***Cyber physical systems***
- ***<u>IoT Applications</u>***

Additional IA Challenges in IoT

- ***Locations*** of ***IoT sensing devices***:
  - Including sites easily gain access by attackers
  - Common attacks including mode capture. fake node and malicious data injection, and denial of service attack
- Signals from ***IoT devices*** often lack effective ***protection***, and can easily monitored, intercepted and disturbed
  - Common attacks including side channel Attack

Additional IA Challenges in IoT (Cont.)

- More serious ***network security*** challenges exist in IoT as the information transmission of IoT systems relies on mobile and other networks
  - Common threats including more susceptible illegal access, eavesdropping, confidentiality and integrity of data, denial of service, and man-in-the middle attack.
- More effective data ***protection and recovery*** are needed for IoT due to the highly distributed nature of storage and processing of various date in IoT systems. The large number of nodes in IoT management is another reason to need more effective data protection and recovery.

Additional IA Challenges in IoT (Cont.)

- More effective ***identity authentication*** of IoT devices and users is very important and challenging in IoT
  - Continuous authentication of user and devices
  - Mutually authentication between devices and users.
- ***Lightweight*** solutions

Current Research

- ***Continuous authentication*** of devices and users
- Effective access control
- Lightweight ***cryptography*** technology
- Lightweight security ***routing protocols***
- Cluster security problems
- Anti-virus
- Physical security
- Tradeoff between performance and security
- …

References

[1] Wikipedia, “Internet of Things, https://en.wikipedia.org/wiki/Internet_of_things

[2] Zhao, Kai, and Lina Ge. "A survey on the internet of things security." *2013 9th International Conference on Computational Intelligence and Security (CIS),*, pp. 663-667. IEEE, 2013.

[3] Bonomi, Flavio, Rodolfo Milito, Jiang Zhu, and Sateesh Addepalli. "Fog computing and its role in the internet of things." In Proceedings of the first edition of the MCC workshop on Mobile cloud computing, pp. 13-16. ACM, 2012.

[4] Satyanarayanan, Mahadev, Paramvir Bahl, Ramón Caceres, and Nigel Davies. "The case for vm-based cloudlets in mobile computing." *IEEE pervasive Computing* 8, no. 4 (2009).

[5] Garcia Lopez, Pedro, Alberto Montresor, Dick Epema, Anwitaman Datta, Teruo Higashino, Adriana Iamnitchi, Marinho Barcellos, Pascal Felber, and Etienne Riviere. "Edge-centric computing: Vision and challenges." *ACM SIGCOMM Computer Communication Review* 45, no. 5 (2015): 37-42.

[6] Arun Balaji Buduru and Stephen S. Yau, "An Effective Approach to Continuous User Authentication for Touch Screen Smart Devices", *Proceedings of IEEE International Conference on Quality, Reliability and Security (QRS)*, Vancouver, Canada, August 2015, pp. 219-226

[7] I. D. Addo, S. I. Ahamed, S. S. Yau, A. B. Buduru, “Reference Architectures for Privacy Preservation in Cloud-based IoT Applications”, International Journal of Services Computing (IJSC), Vol 2(4), December 2014, pp.65-78.