建構智慧城市對網絡安全的挑戰與機遇

香港應用科技研究院有限公司信息安全與數據科學部高級總監許志光博士

2018-04-11

免责声明

- 本简报所包含之资料及/ 或数据只供阁下参考，如日后有所改动，恕不另行通知。
- 这些资料及/ 或数据的真实性、准确性和完整性并未得到保证，亦可能未包含有关香港应用科技研究院有限公司及/或其相关联公司（统称 “应科院” ）的所有重大讯息。
- 应科院对其所载之资料及/ 或数据的真实、准确或完整性不作任何保证或陈述，并且不承担任何责任。
- 此外，这些资料及/ 或数据可能包含预测和前瞻性声明， 只反映应科院对未来事件和财务表现的当前看法。这些观点都是基于当前的一些假设，这些假设有可能随着时间而改变。

  应科院对于这些未来事件是否会发生、预测是否实现，或应科院的假设是否正确，不作任何保证。
- 最后，此简报并不构成应科院作出任何要约（包括应科院就其相关技术及 /或服务的要约）。

內容

- 應用科技研究院 ASL 簡介
- 智慧城市
- 網絡安全的挑戰
- 網絡安全的機遇
- 結論

應用科技研究院 ASL

- 使命
- 在香港建立一個世界級的資訊安全研發團隊;
  - 提供先進的安全顧問，評估和審查;
  - 開發先進的資訊安全技術;
  - 培育本地和國家的資訊安全專家和從業人員

智慧城市

- 智慧家庭 Smart home
- 智能電網 Smart Grid
- 交通 Smart Transportation
- 醫療 Smart Health
- 商業 Smart Commerce
- 製造業 Smart Manufacturing
- …

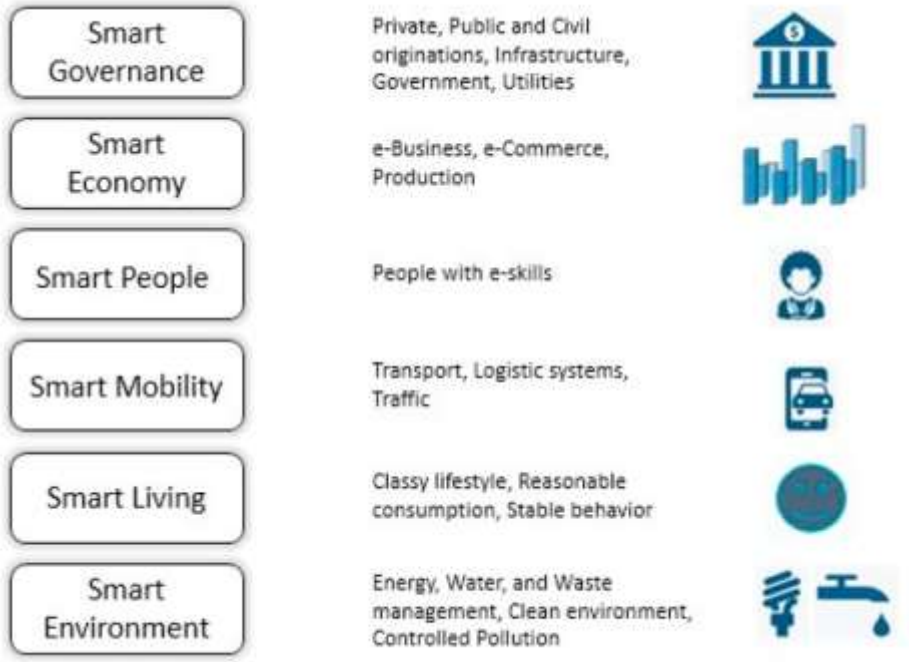


Fig. 1. Dimensions of Smart Cities

另一種觀點: Cyber Security Attacks on Smart Cities and Associated Mobile Technologies, by AlDairi & Tawalbe, Procedia Computer Science, V.109, 2017, 1086-1091, https://www.sciencedirect.com/science/article/pii/S1877050917310669?via%3Dihub

ASTRI

智慧城市: 不同的層面

- 管理層面 (**Management level**),數據層面(**data level**), 網絡層面(**network level**)

管理層面(Management Level): 商業流程，法律需求
(Business Process, Legal requirements)

數據層面(Data Level): 雲端資料收集，大數據分析，數據加密
(Collection of data, Big data analysis, data encryption at Cloud)

0100
1101

網絡層面(Network Level): 雲服務器， 網絡， 設備， 人員
(Cloud Server, Network, Devices, People)







一些事件 (1)

- 勒索軟件
- 來源: https://security.radware.com/ddos-experts-insider/ert-case-studies/how-multinational-bank-handled-ransom-threat-ssl-attack/

3/6/2017

Ransomware Attacks on Multinational Bank & How They Prevented Them

In 2016, the financial services industry suffered 44 million cyberattacks, more than any other industry. Everything from hacktivist motivated ransomware attacks to Internet of Things (IoT) assaults targeted leading banks, financial service institutions, and markets, resulting in hundreds of millions in lost revenue.

ASTRI

一些事件 (2)

- 入侵學校的設備 (2017)
- 來源: https://campustechnology.com/articles/2017/02/13/university-hackers-attacked-5000-iot-devices-on-campus.aspx

ASTRI

一些事件 (3)

- 患者入侵醫院的設備 (2014)
- 來源: https://www.massdevice.com/hospital-patient-hacks-his-own-morphine-pump-massdevicecom-call/

Hospital patient hacks his own morphine pump | MassDevice.com On Call

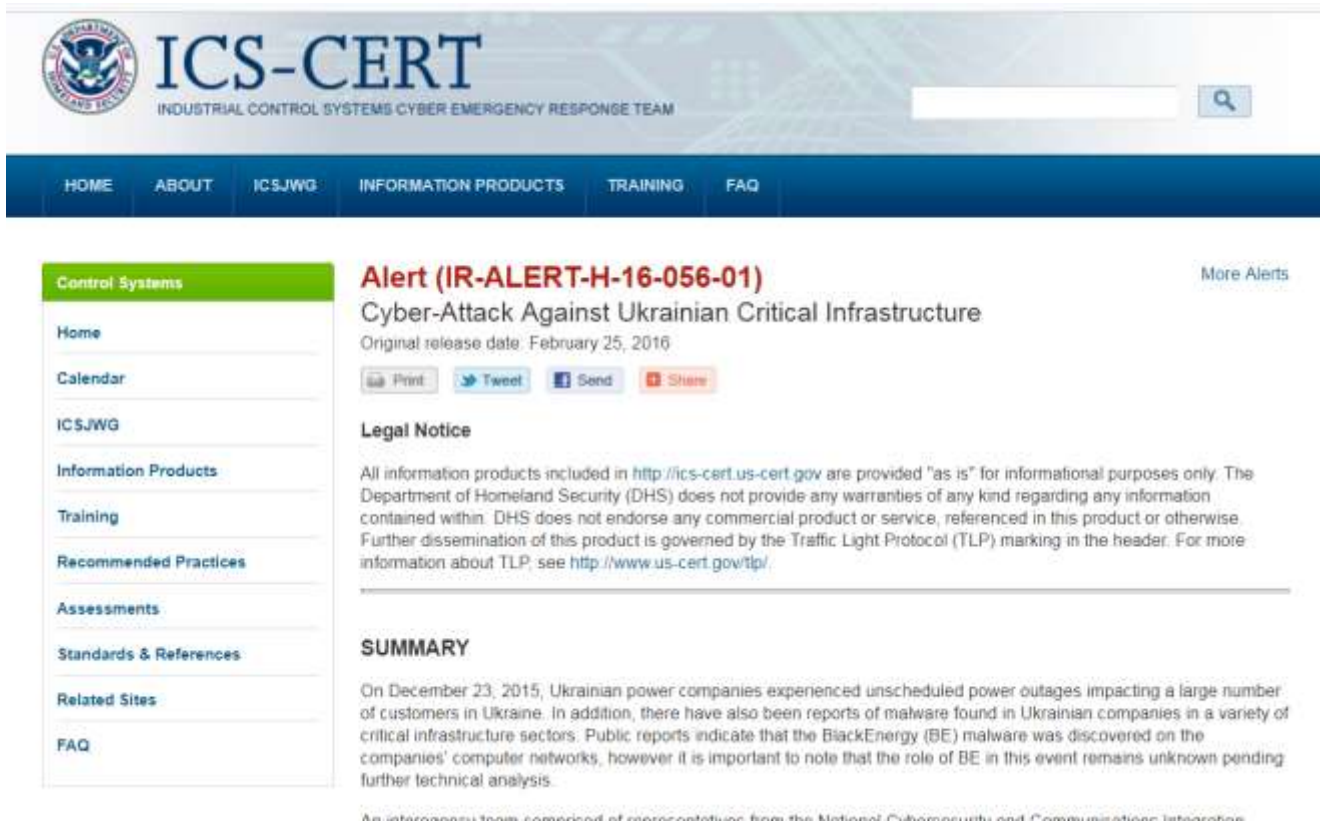
AUGUST 15, 2014 BY AREZU SARVESTANI — LEAVE A COMMENT

MASSDEVICE ON CALL — A pair of patients at an Austrian hospital became addicted to morphine after one of them hacked their drug pumps to boost their dosage, according to a local report.

The unidentified patients had to be treated for addiction after becoming dependent on high doses of morphine. Their usage was so severe, according to the *Austrian Times*, that one of the patients suffered respiratory arrest.

一些事件 (4)

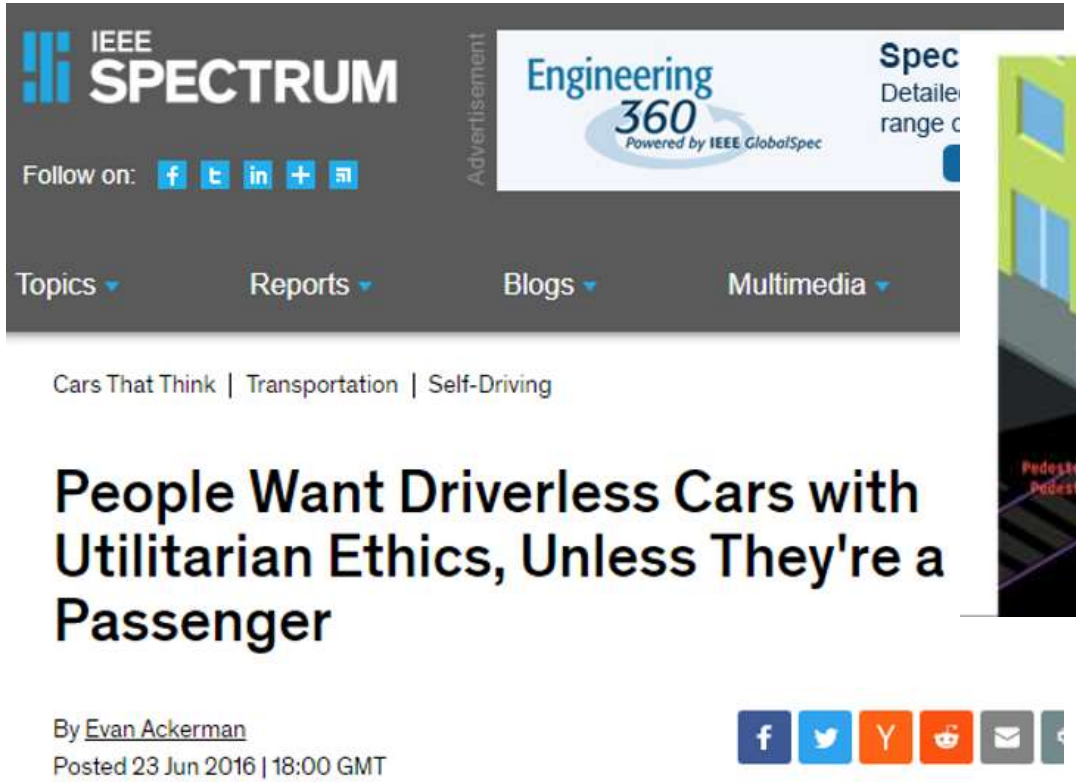
- 智能電網 Scada (2015)
- 來源: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

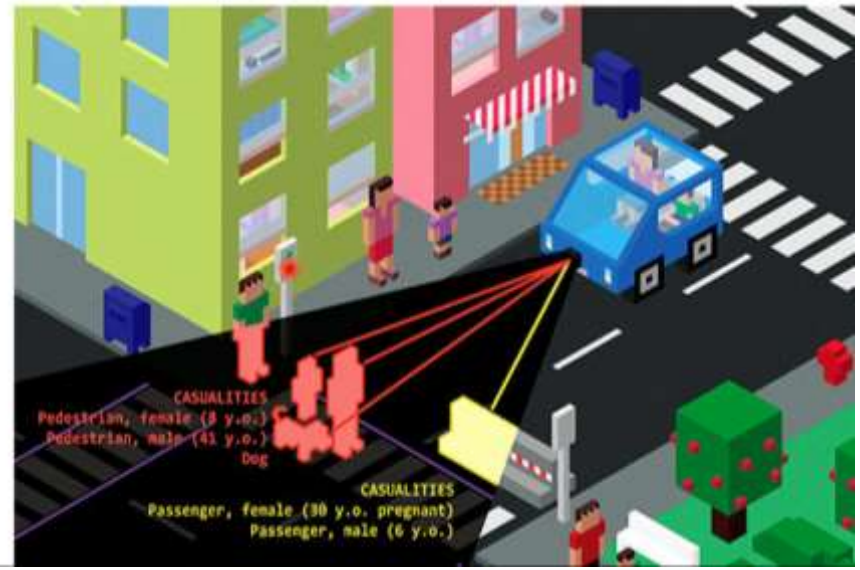


一些問題

- 數學模型完善嗎?
- 管理?

Source: https://spectrum.ieee.org/cars-that-think/transportation/self-driving/people-want-driverless-cars-with-utilitarian-ethics-unless-theyre-a-passenger





ASTRI

智慧城市: 網絡安全的挑戰

管理層面(Management Level): 商業流程，法律需求
(Business Process, Legal requirements)

事件响應 (Incidence Response)

商業糾紛 (Business Disputes)

流程分解 (Process Breakdown)

詐欺 (Fraud)

數據層面(Data Level): 雲端資料收集，大數[illegible]據加密
(Collection of data, Big[illegible]s, data encryption at Cloud)

違反規則 (Breaching Regulations)

數據丟失 (Data loss)

0100
1101

數據洩漏 (Data leakage)

網絡層面(Network Level): 雲服務器， 網絡， 設備， 人員
(Cloud Server, Network, Devices, People)

分布式拒絕服務 (DDoS)

入侵(hacking)

竊聽(Eavesdropping)

入侵(hacking)

竊聽(Eavesdropping)

入侵(hacking)

竊聽(Eavesdropping)

社交工程 (Social Engineering)

ASTRI

智慧城市: 網絡安全的機遇

安全評估(Security Assessment);
設計評價(Design Evaluation);
風險管理(Risk Management);
犯罪調查(Crime Investigation);
數字取證(Digital Forensics);

事件响應 (Incidence Response)

商業糾紛 (Business Disputes)

流程分解 (Process Breakdown)

詐欺 (Fraud)

管理層面 程，法律需求 ss Process, Legal requirements)

身份管理(Identity Management);
隱私檢查(Privacy check);

數據層面 料收集，大數 據加密 ion of data, Big s, data encryption at Cloud)

違反規則 (Breaching Regulations)

數據丟失 (Data loss)

0100
1101

數據洩漏 (Data leakage)

網絡層面(Network Level):

雲服務器， (Cloud Server,

網絡， Network,

設備， Devices,

人員 Peop

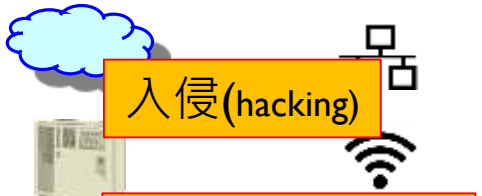
專業訓練(Training of Professional);
用戶感知/教育(User Awareness/Edu);
新設備設計(Design of new devices);

終端保護(End-point protection);
設備測試(Testing of Devices);
安全測試(Security Testing);
滲透測試(Penetration Test);
事件响應(Incidence Response);
數據加密(Data Encryption);

式拒絕服務 DDoS)

acking)

avesdropping)



入侵(hacking)

竊聽(Eavesdropping)

入侵(hacking)

竊聽(Eavesdropping)

社交工程 (Social Engineering)

ASTRI

智慧城市: 網絡安全的機遇 (2)

- 上述問題與機會出現於智慧城市的每一個環節。

  (The above-mentioned problems and opportunities appear in EVERY aspects of Smart City.)

- 智慧城市使用各種不同的物聯網設備，因此其管理問題將會比傳統互聯網系統更加複雜。

  (Smart City will use a lot of different, diversified IoT devices, therefore the management problem is more complicated than a traditional Internet system.)

- 犯罪者會使用高級技術發動網絡攻擊，而且其技術也將不斷更新。

  (Criminals will use advanced technology to launch cyberattacks, and their technology will also advance from time to time.)

- 這意味著安全技術的更迫切需要。

  (This implies a greater need of security technology.)

- 網絡安全專家的人力市場需求也更加提升。

  (Also demands a greater number of Cyber Security professionals.)

結論

- 個人見解(**A simple remark**)
  - 實體世界中的系統具備安全組件

    (Physical world systems have safety/security components)
  - 數位世界中的系統必須具備安全組件

    (Digital world systems should have safety/security components)
  - 越來越多的人類活動由實體世界逐漸轉移到數位世界

    (Human activities move more from physical world to digital world)
  - **...** 自然而然，我們必須針對數位工作的安全來挹注更多資源與努力

    (... it is natural that, we should put more resources/effort in digital work safety/security)

- 謝謝!
- lucashui@astri.org