Abstract for Creating Smart Cities Conference, University of Maynooth, Ireland, 5-6th September 2016

Hacking the smart city and the challenges of security

Martin Dodge

Department of Geography, University of Manchester

The ways that technologies are enrolled in practice and come to shape our cities is often paradoxical, bringing promised benefits (such as enhanced convenience, economic prosperity, resilience, safety) but beckoning forth unintended consequences and creating new kinds of problems (including pollution, inequality, risk, criminality). This paradox is very evident when looking back at earlier rounds of transformative urban technologies, particularly in energy supply, transportation, communication and electro-mechanical systems of automation. The paradox is arguably even more pronounced in relation to the development of smart urbanism and will be examined in terms of the trade-offs around security.

This talk will consider how complex software and networked connectivity at the heart of smart cities technologies (both current, near future implementations and imagined scenarios) is opening up new risks and seems inherently to provide threats to established modes of urban management through security concerns and scope for criminal activities. I will examine how cities are becoming more vulnerable to being 'hacked' in relation to weaknesses directly in the technologies and infrastructures because of how they are designed, procured, deployed and operated. Then I will look at the cyberattacks against the data generated, stored and being shared across digital technologies and smart urban infrastructures. The second half of the talk considers how to defeat (or at least better defend against) those vandals, criminal and terrorists seeking hacking the smart cities, and will focus on available practical means and management approaches to better secure infrastructure and mitigate the impact of data breaches.

CREATING SMART CITIES

Collaboration, Citizenship and Governance

5-6 September 2016
The Programmable City Project
Maynooth University, Ireland

The Programmable City

Maynooth University
National University of Ireland Maynooth

NIRSA

erc
European Research Council

This project is funded by the European Union

v.1.0

Agenda

Sunday 4th September 2016	
18:30 Social dinner reception event at O'Neill's Pub/Restaurant	
Monday 5th September 2016	
09.00 Meet-up in lobby of Glenroyal Hotel / Make own way to Venue	
09.30 - 10:00 Tea / Coffee	
10:00 - 10:30 Opening Talk by Rob Kitchin - Reframing, reimagining and remaking smart cities	
10:30 - 12:30 **Session 1: Governance and regulation**	**1.1** James Merricks White - Governing the City as a System of Systems **1.2** Martin Dodge - Hacking the Smart city and the Challenges of Security **1.3** Aoife Delaney - Coordinated Management and Emergency Response Systems and the Smart City **1.4** Jathan Sadowski - Dumb Democracy and Smart Politics? Transitions and Alternatives in Smart Urban Governance
12:30 - 13:30 Lunch	
13:30 - 15:30 **Session 2: Citizenship and democracy**	**2.1** Taylor Shelton - 'Actually existing smart citizens': expertise and (non)participation in the making of the smart city **2.2** Ayona Datta - From start to smart: A 100 smart cities but where are the citizens **2.3** Gyorgyi Galik and John Lynch - From Engagement to Participation in Future Smart Cities **2.4** Sung-Yueh Perng - Creating infrastructures with citizens: An exploration of Beta Projects, Dublin City Council
15:30 - 16:00 Tea / Coffee	

16:00 - 18:00 **Session 3: Privacy and security concerns in smart cities**	**3.1** Lilian Edwards - Privacy and data protection in smart cities: are the problems insuperable? **3.2** Maria Murphy - Pseudonymisation and the Smart City: Considering the General Data Protection Regulation **3.3** Leighton Evans - The Privacy Parenthesis: The Structural Transformation of the Private Sphere **3.4** Christine Richter et al. - From data subjects to data producers: negotiating the role of the public in urban digital data governance
19:30 Dinner at The Gatehouse	
Tuesday 6th September 2016	
09:30 - 10:00 Tea / Coffee	
10:00 - 12:00 **Session 4: Smart districts and living labs**	**4.1** Alan Wiig - Surveilling the smart city to secure economic development in Camden, New Jersey **4.2** Liam Heaphy & Réka Pétercsák: Building Smart City Partnerships in the 'Silicon Docks' **4.3** Andy Karvonen - University Campuses as Bounded Sites of Smart City Co-Production **4.4** Claudio Coletta - Algorhythmic governance: regulating the city heartbeat with sensing infrastructures
12:00 - 13:00 Lunch	
13:00 - 15:00 **Session 5: Co-design/co-production of smart cities**	**5.1** Niall Ó Brolcháin - The Importance of Enacting Appropriate Legislation to Enable Smart City Governance **5.2** Robert Bradshaw - Technical Citizenry and the Realization of Bike Share Design Possibilities **5.3** Darach MacDonncha - The Political and Economic Realities of Introducing a Smart Lighting System **5.4** Duncan McLaren & Julian Agyeman - Smart for a Reason: sustainability and social inclusion in the sharing city
15:00 – 15:30 Tea / Coffee	
15:30 - 17:00 **Discussion/ wrap-up**	

Abstracts

Introduction from Rob Kitchin – Reframing, reimagining and remaking smart cities

Rob Kitchin, Maynooth University (Rob.Kitchin@nuim.ie)

Over the past decade the concept and development of smart cities has unfolded rapidly, with many city administrations implementing smart city initiatives and strategies and a diverse ecology of companies and researchers producing and deploying smart city technologies. In contrast to those that seek to realise the benefits of a smart city vision, a number of critics have highlighted a number of shortcomings, challenges and risks with such endeavours. This short paper outlines a third path, one that aims to realise the benefits of smart city initiatives while recasting the thinking and ethos underpinning them and addressing their deficiencies and limitations. It argues that smart city thinking and initiatives need to be reframed, reimagined and remade in six ways. Three of these concern normative and conceptual thinking with regards to goals, cities and epistemology, and three concern more practical and political thinking and praxes with regards to management/governance, ethics and security, and stakeholders and working relationships. The paper does not seek to be definitive or comprehensive, but rather to provide conceptual and practical suggestions and stimulate debate about how to productively recast smart urbanism and the creation of smart cities.

Session 1. Governance and regulation

1.1. James Merricks White - Governing the City as a System of Systems

James Merricks White, Maynooth University (james.white.2014@mumail.ie)

Vital to the nascent domain of city standards is an understanding of the city as a system of systems. Borrowed from urban cybernetics, this conception imagines and describes the city as comprised of distinct fields of operation and governance. While this might have previously served a pragmatic purpose, allowing a compromise to be found between centralisation and specialisation, critics argue that it has produced institutional path dependencies which, in the era

of big and open data, are a source of interruption and inefficiency. Put another way, information, action and responsibility are seen to be bound-up in vertically integrated silo-like structures. By breaking down or reaching across these silos, it is hoped that new synergies in urban governance might be unlocked. In this paper I will explore the mechanisms by which three city standards naturalise and respond to the system-of-systems problematic. First, City Protocol Anatomy offers a conceptual model for thinking, communicating and coordinating action across city systems. The city is reconfigured as a body, each of its systems become that body's organs, and a whole linguistic framework emerges for talking about the city at all manner of scales and time frames. Second, ISO 37120 enacts an set of verification and certification mechanisms in an effort to build up a database of robust urban indicators. Within cities this translates into greater communication and information exchange between the departments of a city's authority. Finally, while only a set of policy recommendations PAS 181 is quite explicit in bringing matrix management concepts to urban governance. It imagines small, agile, tactically- specific units capable of acting across legacy governance structures. Although operating in distinct ways, each standard attempts to open up new terrain of and for urban governance. The ramifications of these new state/spaces are only beginning to emerge.

1.2. Martin Dodge - Hacking the Smart city and the Challenges of Security

Martin Dodge, Manchester University (m.dodge@manchester.ac.uk)

The ways that technologies are enrolled in practice and come to shape our cities is often paradoxical, bringing promised benefits (such as enhanced convenience, economic prosperity, resilience, safety) but beckoning forth unintended consequences and creating new kinds of problems (including pollution, inequality, risk, criminality). This paradox is very evident when looking back at earlier rounds of transformative urban technologies, particularly in energy supply, transportation, communication and electro-mechanical systems of automation. The paradox is arguably even more pronounced in relation to the development of smart urbanism and will be examined in terms of the trade-offs around security.

This talk will consider how complex software and networked connectivity at the heart of smart cities technologies (both current, near future implementations and imagined scenarios) is opening up new risks and seems inherently to provide threats to established modes of urban management through security concerns and scope for criminal activities. I will examine how

cities are becoming more vulnerable to being 'hacked' in relation to weaknesses directly in the technologies and infrastructures because of how they are designed, procured, deployed and operated. Then I will look at the cyberattacks against the data generated, stored and being shared across digital technologies and smart urban infrastructures. The second half of the talk considers how to defeat (or at least better defend against) those vandals, criminal and terrorists seeking hacking the smart cities, and will focus on available practical means and management approaches to better secure infrastructure and mitigate the impact of data breaches.

1.3. Aoife Delaney - Coordinated Management and Emergency Response Systems and the Smart City

Aoife Delaney, Maynooth University (aoife.delaney.2011@nuim.ie)

This paper maps out the historic and current organisation of the Irish Emergency Management System and its potential intersections with the Smart Dublin Initiative which could create a truly Coordinated Management and Emergency Response System (CMaERS). It begins with a brief overview of the Framework for Major Emergency Management in Ireland- an unlegislated guidance framework used foremost by the Principal Response Agencies but also by other responding agencies. Further, the paper addresses key barriers which the current Emergency Management System suffers from and which the framework inadequately attempts to overcome, in order to situate the current system. These barriers include: institutional tensions and the historical legacy of agency mandates, organisation, technologies and practices. Finally, the current system is brought into conversation with Smart Dublin to unravel whether the smart city is a barrier or whether it can be an enabler of the current Emergency Management System evolving into a CMaERS. The Smart Dublin initiative is organised across the four local authority agencies which govern Dublin County. This provides four significant opportunities for the merging of the Irish Emergency Management System and the smart city in so far unseen ways. The first opportunity is that the local authorities are, simultaneously, Principal Response Agencies (PRA) for crises and the drivers of Smart Dublin. Secondly, the governance of Smart Dublin could allow for stronger inter-agency collaboration and coordination. Thirdly, there is potential to develop an Incident Command System and finally, the Framework is unlegislated. These opportunities would help to position Dublin to be one of the first smart Emergency Management Systems –a CMaERS which could, potentially, result in better inter-agency coordination, standardised technology across agencies, interlinked control rooms, and a more resilient emergency response system.

Hacking the Smart City and the Challenges of Security

Martin Dodge
Department of Geography
University of Manchester

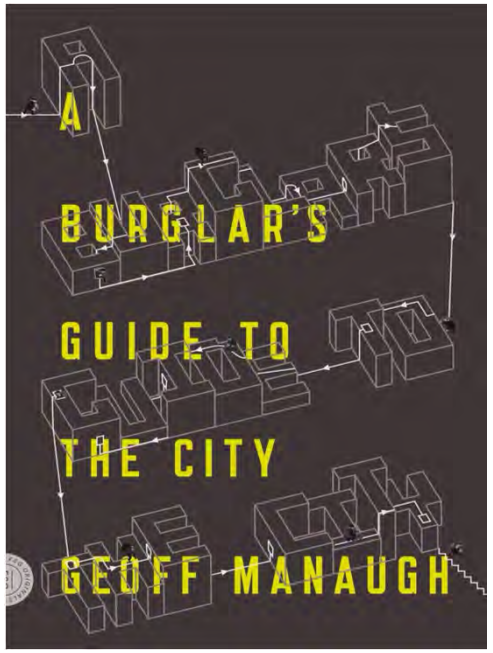
Creating Smart Cities Conference, University of Maynooth, 5th September 2016

1. Paradox of urban technology

- All manner of technologies, over centuries, enrolled in practice and come to shape the ontogenesis of cities
- Exhibit paradoxical outcomes. Promised benefits balanced by unintended consequences and new kinds of problems
- Paradox very evident in earlier rounds of transformative urban technologies in industrial era

2. The city and criminality

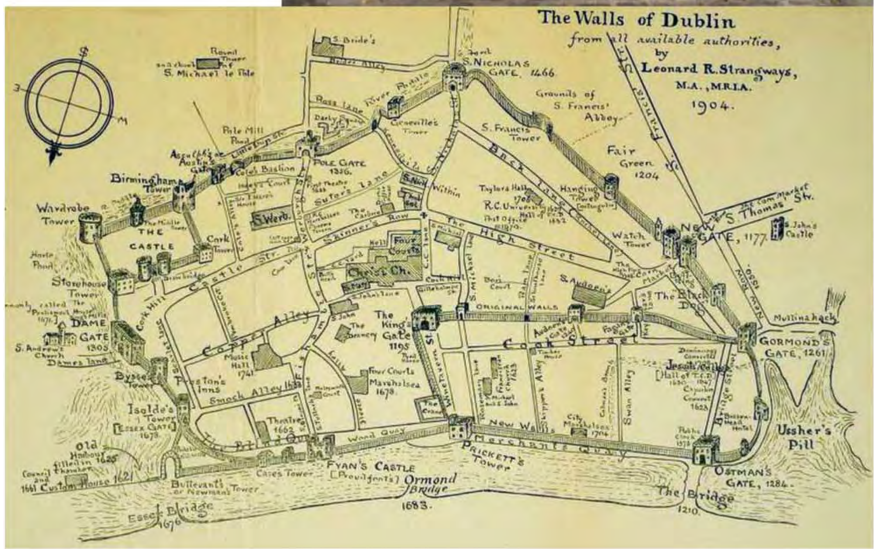
- Long association between social risk, criminality and the degree of urbanity
- Cities are attractive to criminals (lots of valuable assets, array of buildings and structures to exploit, social interactions)
- Many responses through security



"you cannot tell the story of buildings without telling the story of the people who want to break into them: burglars are a necessary part of the tale, a deviant counter-narrative as old as the built environment itself." (p.12)

3. City wall as security

- Encirclement, big, impressively strong
- But all walls can be breached
- Gates are also needed
- Cities thrive on access, interaction, trade (totally walled city is a dead city)
- How to design and operate the gates



4. Locking up space

- Lack of trust in a city of strangers
- We rely on locks
- But every lock can be picked (although takes skills, tools, motivation)
- But better locks are possible

5. Smart cities - a new era for security challenges?

- Such a paradoxical situation applies to smart cities, with unintended consequences of pervasive digital technology, networked access and deep software automation
- Often ignored in boosterish discourse
- Key concern of social sciences to consider where the balancing point between rewards and risk lies. Security as a trade-off
- Smart cities way off balance at moment?

6. Vulnerabilities in smart cities

- Smart city technological systems (both current & near future) are a source of new vulnerabilities and novel risks for established urban management
- Arising at three levels:
- (i) Meta level context; (ii) Systematic weaknesses in software design; (iii) Specific flaws in critical pieces of urban infrastructure

Vulnus: Latin, a wound.

Vulnerable – able to be physically or emotionally hurt; easily influenced or tempted; exposed to attack; financially weak

7. Vulnerabilities in smart cities

(i) Meta-level Context:

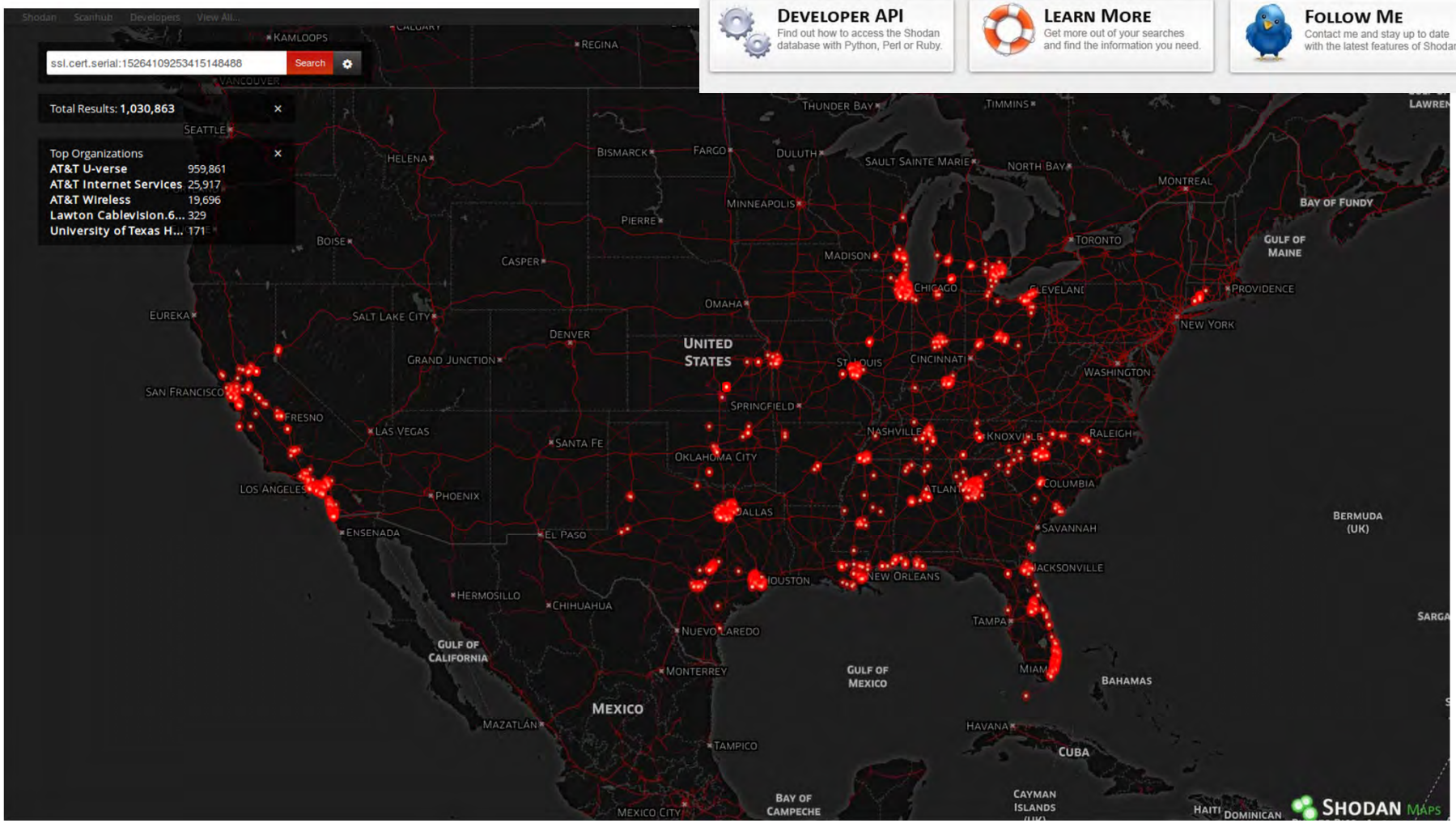
- Complexity – no one really knows how the city works
- Fragmented city management (hollowing out of state; out-sourcing)
- Institutional ‘brittleness’, massive budget constraints in municipal government, coupled with pressure for ‘smart’ delivery
- Recruitment and retention of skilled, motivated staff in IT (and cybersecurity)

8. Vulnerabilities in smart cities

(ii) Systematic weaknesses in software

- Sheer scale of software. Always be bugs, holes and overflows. Produces thousands of potential of ‘zero-day exploits’
- (as consumers we routinely accept ‘faulty’ software that would be unacceptable in other products!)
- Poor software system engineering
- Variable practices of updating and inconsistency of patching vulnerabilities
- Unpatchable ‘forever-day exploits’ in legacy parts of complex infrastructure

‘Security through obscurity’ does not work in an inter-connected, open smart city

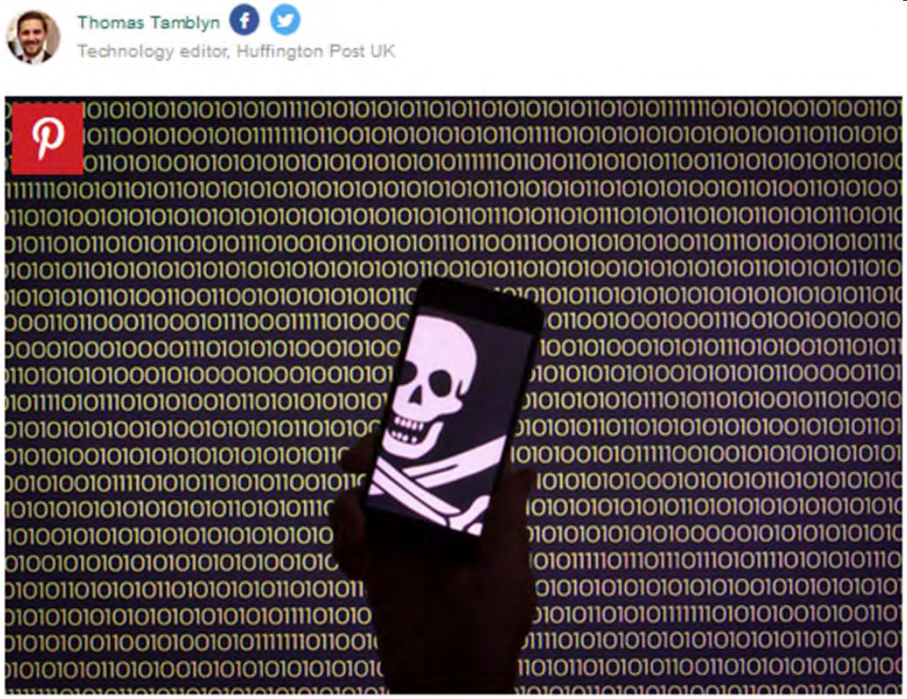


9. Vulnerabilities in smart cities

(iii) Weaknesses in specific components

- Maximum: that total security is only as good as weakest link in the chain
- Humans. Great flexibility but big failures,
  - Social engineering, spoofing; bribery, corruption; insider attacks, disgruntlement
- Go after their smartphones these days,
  - Essential for many people, conduct their (digital) life on the them; including work
  - Personal, promiscuous, accessible, open

900 Million Android Phones Could Be Vulnerable To New “Quadrooter” Hack



Thomas Tamblyn
Technology editor, Huffington Post UK

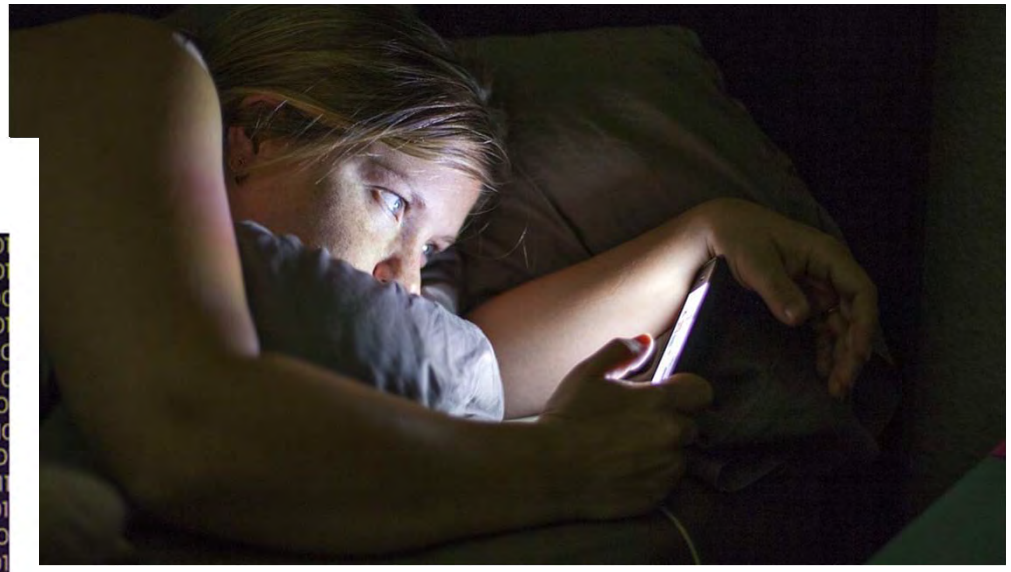
NURPHOTO VIA GETTY IMAGES

A serious security flaw has been discovered in millions of Android phones that could give hackers complete access to the device's data, say security researchers.

Security firm Check Point say they've discovered a vulnerability in the software that runs on chips made by the US company Qualcomm.

As one of the leading chip providers for tablets and smartphones Check Point believes that up to 900 million Android phones could be at risk.

Continuous stories of new vulnerabilities, rogue apps and data breaches



- People trust THEIR phone
- But do they know what’s going on beneath the user interface?
- Who controls YOUR smartphone???

10. Vulnerabilities in smart cities

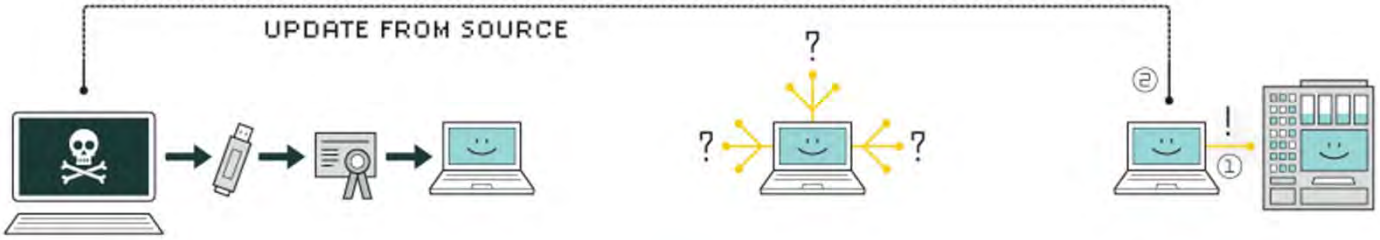
- Switches, communication links
- The string between the tin cans attacked, once inside the communications then malicious action possible
- Revelations post-Snowden show how seriously surveilled communication traffic is by Western intelligence agencies. Certainly other attackers have or will have same capabilities

11. Vulnerabilities in smart cities

- SCADA (supervisory control and data acquisition) systems
- Not known by general public but are absolutely essential to daily reproduction of cities
- Urban infrastructure (electricity grid, water supply, and traffic control), rely on SCADA systems to monitor functions, modulate operation (opening valves,

2009/10: Stuxnet sophisticated worm that design to attack SCADA systems, controlling centrifuges

HOW STUXNET WORKED



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

computerknow.org/article/the-real-story-of-stuxnet

12. Vulnerabilities in smart cities

- Mundane urban street furniture, like a traffic lights. Essential to order space and movement and people tend to trust them
- Networked and dynamic. Hack centre
- Wireless: responsive to emergency services. But unencrypted over-ride commands. So attack devices locally
- Creating the ‘green-wave’
- [Confused.com Mr Greenlight advert!]

This paper appeared in *Proceedings of the 8th USENIX Workshop on Offensive Technologies* (WOOT '14), August 2014.

Green Lights Forever: Analyzing the Security of Traffic Infrastructure

Branden Ghena, William Beyer, Allen Hillaker, Jonathan Pevarnek, and J. Alex Halderman
Electrical Engineering and Computer Science Department
University of Michigan
{brghena, wbeyer, hillaker, jpevarne, jhalderm}@umich.edu

Abstract

The safety critical nature of traffic infrastructure requires that it be secure against computer-based attacks, but this is not always the case. We investigate a networked traffic signal system currently deployed in the United States and discover a number of security flaws that exist due to systemic failures by the designers. We leverage these flaws to create attacks which gain control of the system, and we successfully demonstrate them on the deployment in coordination with authorities. Our attacks show that an adversary can control traffic infrastructure to cause eral attacks against the deployment and are able to change the state of traffic lights on command.

The vulnerabilities we discover in the infrastructure are not a fault of any one device or design choice, but rather show a systemic lack of security consciousness. We use the lessons learned from this system to provide recommendations for both transportation departments and designers of future embedded systems.

2 Anatomy of a Traffic Intersection

The modern traffic intersection is an amalgamation of various sensors, controllers, and networking devices. Figure 1

BloombergView

Traffic Hackers Pull Off 'Italian Job'

AUG 22, 2014 9:03 AM EDT

By Leonid Bershidsky

If you think the Internet of things will be safe from malicious invaders, a team of computer experts at the University of Michigan has a hack for you: traffic lights.

Taking over a city's stoplights has long been an object of aspiration for hackers. Compromised traffic systems have even captured the imagination of Hollywood, playing crucial supporting roles in the 2003 remake of "The Italian Job" and 2007's "Live Free or Die Hard" (the whole movie is worth watching for the traffic-light scene).

Leonid Bershidsky is a Bloomberg View columnist. He was the founding editor of the Russian business daily Vedomosti and founded the opinion website Slon.ru.
Read more
@Bershidsky

MOST POPULAR

Jonathan Bernstein
What the Polls Are Missing About Trump

Eli Lake
Orders for U.S. Forces in Syria: 'Don't Get Shot'

Megan McArdle

The new confused.com advert: taking the Carpool Karaoke road to success

Having achieved stardom stateside with his Late Late Show, James Corden is now shifting car insurance. He's having a good time but he's no Ryan Gosling

Mr Greenlight

Vehicular man's laughter: James Corden in the confused.com advert. Photograph: Youtube

https://www.theguardian.com/tv-and-radio/2016/aug/27/confusedcom-advert-carpool-karaoke-james-corden

13. Hackers and cyberattacks

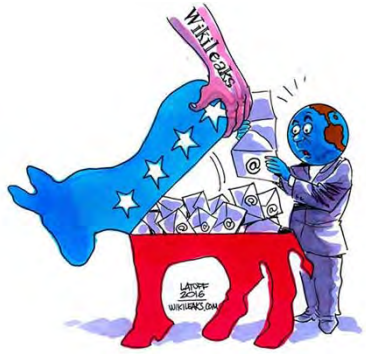
- Cyberattacks can be performed by multiple different actors:
- from nation state intelligence agencies & militaries; terrorist groups; organised criminals, hacker collectives, political & socially motivated activists; classic ‘lone wolf’ hackers; ‘script kiddies’ and bored teenagers. consulting companies for hire
- What ways do they attack : the ‘CIA’ vectors
- *Confidentiality, Integrity, & Accessibility*

“attacks are timeless because the motivations & objectives of attackers are timeless. What does change is the nature of attacks: the tools, the methods, and the results. Bank robbery is a different crime in a world of computers and bits than it is in a world of paper money and coinage.” (Schneier, 2003, p. 73)

14. Hackers and cyberattacks

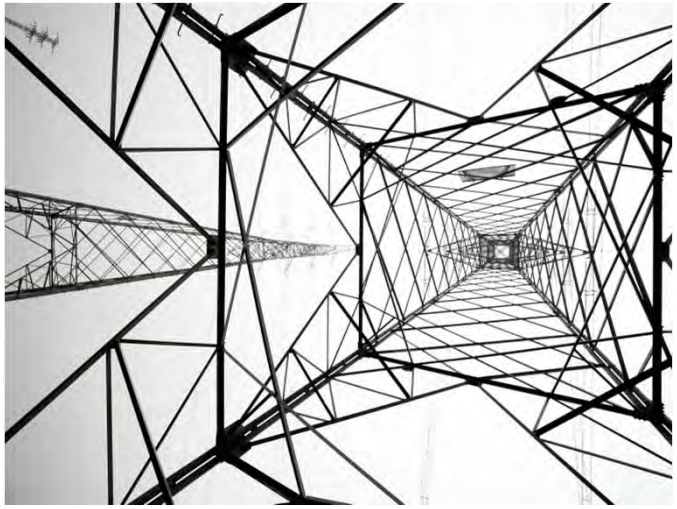
- ‘Confidentiality’ attacks most noticed by news media, and hence politicians and public
- e.g. 2015: Ashley Madison, TalkTalk; U.S. Office of Personnel Management
- ‘Accessibility’ attacks are more concerning; Schneier (2016):
- “It’s one thing if your smart door lock can be eavesdropped upon to know who is home. It’s another thing entirely if it can be hacked to allow a burglar to open the door – or prevent you from opening your door.”

TalkTalk
A brighter home for everyone



15. Hackers and cyberattacks

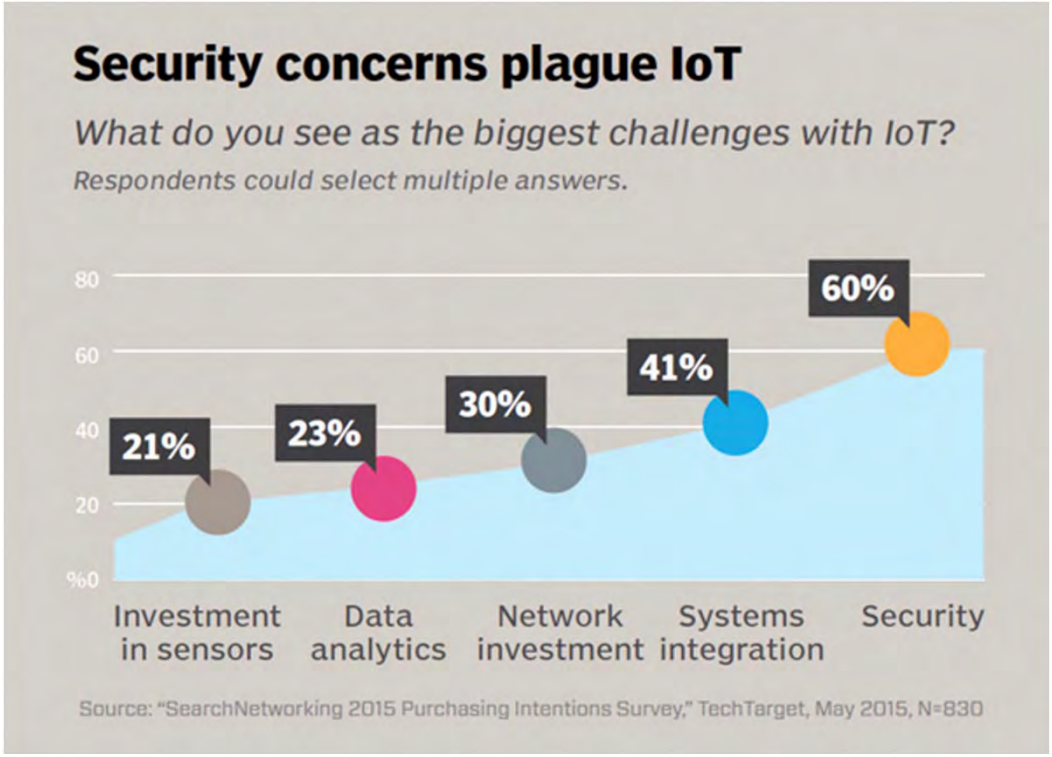
- ‘Accessibility’ attack on Ukrainian power supply, Dec. 2015
- Months in planning, conducted within minutes against three separate control centres
- Power outages affecting approx. 225,000 customers for several hours
- Sophisticated, multi-stage



- Recon and infiltration
- *Primary attack*: SCADA hijack to open breakers
- *Amplifying attacks*: Schedule disconnects for UPS; telephonic floods; KillDisk wiping of workstations; firmware attacks against serial-to-ethernet devices at substations

Cyber-physical automation

- *Internet of Things* - many consumer level gadgets are notoriously vulnerable
- Many more ‘Accessibility’ attacks on the cards!

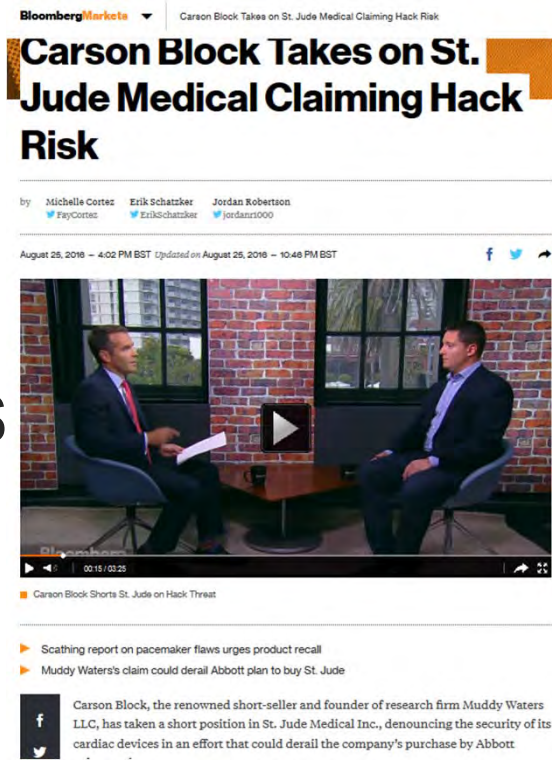


16. Security response: ‘top-down’

- First level involves application of conventional security management; more effective operational policies and some stronger ‘top-down’ regulatory pressures by government
- Setting minimum standards; mandatory reporting of breaches; support for whistle -blowers. Statistical information
- Analogy to automotive industry in the 1970s around safety, 1990s in security

17. Security response: ‘bottom-up’

- Market solutions and communities of best practice within and between cities
- ‘Carrots and sticks’ to foster better security practices by cities and agencies, technology companies, software developers
- Reputational damage as ‘sunshine’ that encourages better security to grow
- Education and training



18. Security response: ‘don’t do it’

- Keep things dumb, keep things more secure
- Sceptical of claimed benefits
- More software does not make things better by itself (myself from techno-evangelist in early 1990s to grumpy middle-aged cynic in 2016)
- Standing in the way of progress, or standing up for more common sense approach?

WHEREAS,

Several EVIL-MINDED PERSONS have assembled together in a riotous Manner, and DESTROYED a NUMBER of

FRAMES,

In different Parts of the Country:

THIS IS

TO GIVE NOTICE,

That any Person who will give Information of any Person or Persons thus wickedly

BREAKING THE FRAMES,

Shall, upon CONVICTION, receive

50 GUINEAS

REWARD.

And any Person who was actively engaged in RIOTING, who will impeach his Accomplices, shall, upon CONVICTION, receive the same Reward, and every Effort made to procure his Pardon.

☞ Information to be given to Messrs. COLDHAM and ENFIELD.

Nottingham, March 26, 1811.

- Neo-Luddites needed in smart cities strategy meetings
- But awkward position to hold

Over-coding life, overly connected??

THE WALL STREET JOURNAL.

Subscrib

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life Real Estate

Smart Tampon? The Internet of Every Single Thing Must Be Stopped

Not every object should connect to our smartphones—and if it does, it should at least work

Smartphone-connected trash cans, water bottles, even egg trays: It is hard to tell if these products are real or jokes. WSJ's Joanna Stern takes a look at the trend of making everything "smarter." Photo/video: Drew Evans/The Wall Street Journal.

"A subset of startups inventing the 'world's first connected [insert any noun here]" believe everything goes better with Bluetooth."

Mail Online

Home | News | U.S. | Sport | TV&Showbiz | Australia | Femail | Health | Science

A smart gadget too far? Controversial tampon uses bluetooth to tell wearer when it needs to be changed

- System includes an accompanied app that tracks your period
- App sends out notifications when to change tampon and learns your cycle
- When not using, the monitor can act as a key chain holder
- my.Flow is expected to work as a monthly subscription once it is released

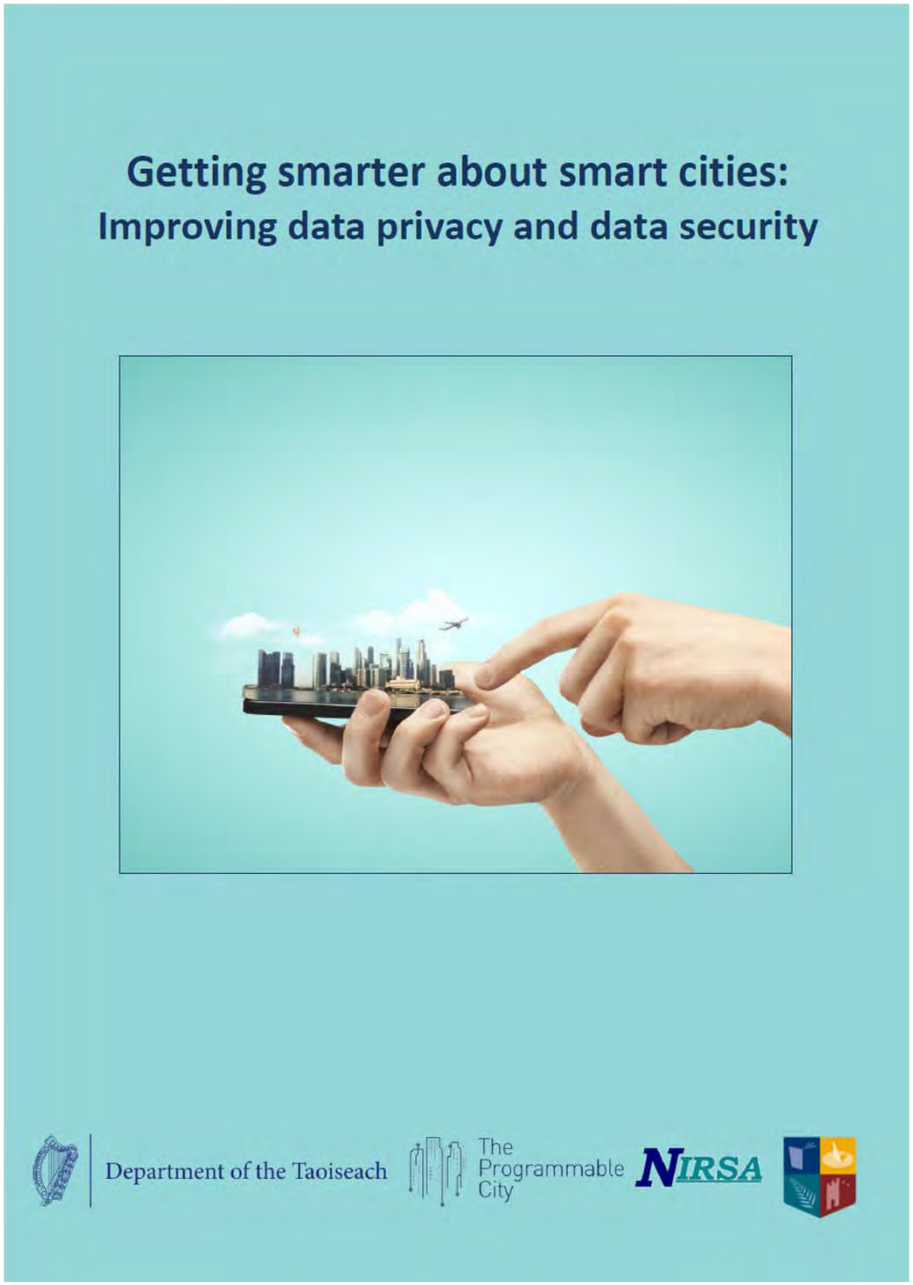
By STACY LIBERATORE FOR DAILYMAIL.COM

PUBLISHED: 20:11, 17 May 2016 | **UPDATED:** 01:17, 18 May 2016

Does this apply to city streets?

19. Cities will get much smarter, can they become more secure?

- Security is a process and city will never be fully secure. (History of the technology paradox and of battle of wits in urban criminality)
- Current state and near future are *too insecure*?
- We've only begun to see the problems of criminality exploiting vulnerabilities, new risks
- Will we need a true 'wake-up call' before concerted action?? (dead bodies in Dublin caused by a crippling cyberattack……)
- Learn from history, need new kinds of city walls and digital locks that are harder to pick?



- Suggested further reading: Kitchin, R. (2016) *Getting Smarter About Smart Cities: Improving Data Privacy and Data Security.* (Data Protection Unit, Department of the Taoiseach, Dublin, Ireland). Available at www.taoiseach.gov.ie/eng/Publications/Publications_2016/Smart_Cities_Report_January_2016.pdf

- Acknowledge the input of ideas from Rob Kitchin in developing this talk.

References and images sources:

- Slide 1: Image from film *The Italian Job* (1969). Source: www.imcdb.org/vehicle_21633-Lancia-Fulvia-818-1963.html
- Slide 2: Image by Gustave Doré wood engraving of Ludgate Hill, London (1872). Source: https://commons.wikimedia.org/wiki/File:Gustave_Dor%C3%A9_-_Ludgate_Hill.png
- Slide 3: Quote from G. Manaugh, 2016, *A Burglar's Guide to the City* (New York: Farrar, Straus and Giroux, 2016), p.12.
- Slide 4: Image of gate in Dublin city wall, source: www.dublincity.ie/image/libraries/ditd036-city-wall-and-gate. Image of *The Walls of Dublin* map, by Leonard Strangways (1904), source: https://twitter.com/ihta_ria/status/524613781360746496
- Slide 5: Image source: www.meetup.com/East-Troy-Computer-Club/events/
- Slide 7: Image screengrab from *BBC News* website, 5 August 2016. Source: www.bbc.co.uk/news/business-36854293

- Slide 10: Image sources: http://fossbytes.com/the-hacker-search-engine-shodan-is-the-scariest-search-engine-on-internet/ ; https://shodanio.wordpress.com/2014/02/18/introducing-shodan-maps/
- Slide 12: Image screengrab from Huffington Post, 8 August 2016. Source: http://www.huffingtonpost.co.uk/entry/900-million-android-phones-could-be-vulnerable-to-a-new-hack_uk_57a859efe4b04ca9b5d391cf
- Slide 13: Image source: http://arstechnica.com/information-technology/2013/05/facebook-aims-to-knock-cisco-down-a-peg-with-open-network-hardware
- Slide 14: Image sources: www.aiche.org/chenected/2013/03/system-attacks-turning-scada-nada
- Slide 15: Main infographic, source: www.kaspersky.com/about/news/virus
- /2012/Kaspersky_Lab_and_ITU_Research_Reveals_New_Advanced_Cyber_Threat. Cartoon, source: https://csc560-network-security.wikispaces.com/5)+Stuxnet+Worm. Photograph, source: www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
- Slide 17: *The Italian Job* (2003) movie poster image, source: http://forum.blu-ray.com/showthread.php?t=262954. Image screengrab of *Bloomberg News*, 22 August 2014, source: www.bloomberg.com/view/articles/2014-08-22/traffic-hackers-pull-off-italian-job

- Slide 18: James Corden in ‘Mr Greenlight‘ advert for Confused.com. Source: www.theguardian.com/tv-and-radio/2016/aug/27/confusedcom-advert-carpool-karaoke-james-corden
- Slide 19: Top image from *WarGames* (1983), source: www.engadget.com/2015/10/15/wargames-reboot-interactive-short/. Lower image, source: www.digitaljournal.com/article/305720. Quote from B. Schneier, *Beyond Fear: Thinking sensibly about security in an uncertain world* (New York: Copernicus Book, 2003) , p.73.
- Slide 20: Image sources: http://media.breitbart.com/media/2016/07/WikiLeaks-DNC-640x480.jpg. Quote from B. Schneier, “Real-world security and the internet of things”, *Motherboard*, 25 July 2016, http://motherboard.vice.com/en_uk/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster.
- Slide 21: Image source: http://internetofthingsagenda.techtarget.com/feature/Enterprise-IoT-security-Is-the-sky-truly-falling
- Slide 23: Image screengrab from *Bloomberg Markets* website, 25 August 2016. Source: www.bloomberg.com/news/articles/2016-08-25/carson-block-takes-on-st-jude-medical-with-claim-of-hack-risk

- Slide 25: Image source: Luddite ‘Frames’ poster https://aes-humanities8.wikispaces.com/luddites
- Slide 26: Image screengrab from *Wall Street Journal*, 25 May 2016, source: www.wsj.com/articles/smart-tampon-the-internet-of-every-single-thing-must-be-stopped-1464198157. Image screengrab from *Daily Mail Online*, 17 May 2016, source: www.dailymail.co.uk/sciencetech/article-3595376/A-smart-gadget-far-Online-backlash-against-tampon-uses-bluetooth-tell-wearer-needs-changed.html