University of Edinburgh
Cyber Security and Privacy Research Network
http://cybersecpriv.ed.ac.uk
Glimpses of Cyber Security and Privacy Research

Informatics Forum: Mini Forum 1 (2nd floor, Lunch 12.30pm)
4.31/33 (Talks, 2pm)

October 5, 2016

David Aspinall

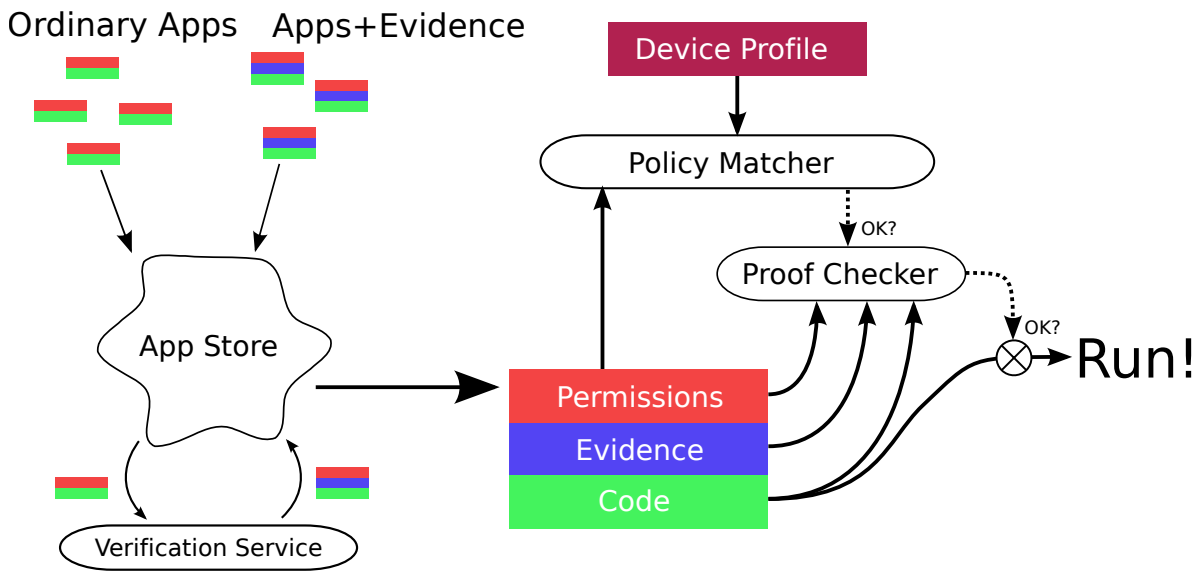
Security with Digital Forms of Evidence

Problem: authentication-based trust is not enough

1. *Digital signatures only say who signed the software*
2. *Sometimes authentication breaks (e.g, signing keys stolen)*
3. *Or, code faulty before signed (e.g., infected or buggy)*

Idea: Proof-Carrying Code

*Equip a program with independently checkable **digital evidence** that it satisfies a security policy. Evidence may be difficult to produce but should be easy to check.*



See **App Guarden** project, `http://groups.inf.ed.ac.uk/security/appguarden`

Myrto Arapanis

Automatic verification of cryptographic protocols

Automatic verification of cryptographic protocols

Automatic verification of cryptographic protocols

Cryptographic protocols are everywhere

Automatic verification of cryptographic protocols

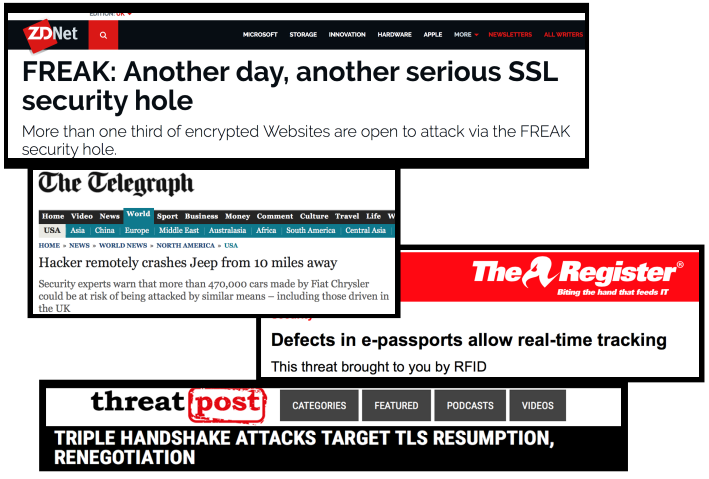
Cryptographic protocols are everywhere

Things often go very wrong :(

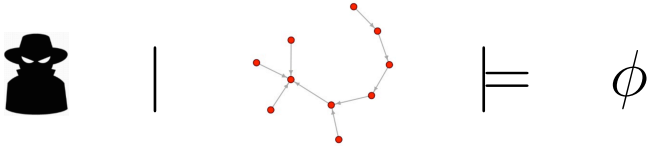
Automatic verification of cryptographic protocols

Cryptographic protocols are everywhere

Things often go very wrong :(



Formal verification



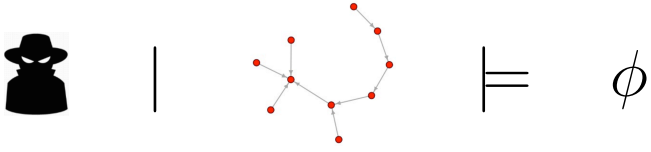
1. Modelling - the protocol, the intended security properties, the attacker
2. Design of verification algorithm

Automatic verification of cryptographic protocols

Cryptographic protocols are everywhere

Things often go very wrong :(

Formal verification



1. Modelling - the protocol, the intended security properties, the attacker
2. Design of verification algorithm

Challenges

Current tools cannot handle new applications

1. New and subtle security and privacy goals: anonymity, unlinkability, proximity, verifiability, ...
2. Non standard cryptographic primitives: homomorphic encryption, proofs of knowledge, blind signatures, ...
3. Tools do not scale to modern systems: tens of protocols running concurrently arbitrarily many times

Angus Bancroft

Resilience in cyber-criminal markets - the role of weak ties

Wei Chen

Swift Behavioural Analysis *for Android Apps*

Understand Behaviours of Android Apps in Market-Scale.

Improve robustness of machine-learning-based malware classifiers.

Fill the gap between security analysis and program analysis.

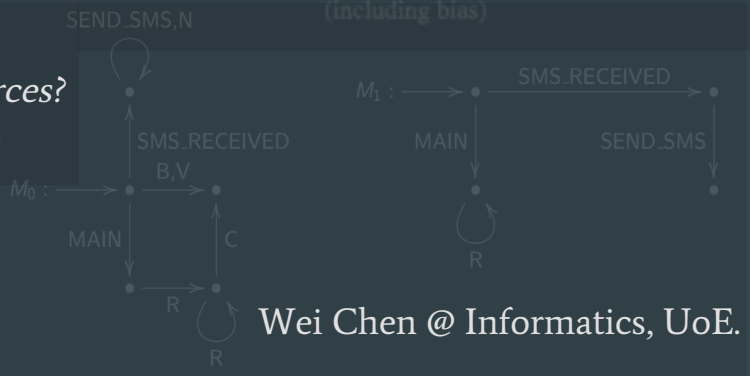
Answer queries like:

How does the app use my cameras, locations, and other resources?
Does the app eavesdrop me, e.g., recording my incoming calls?
What is the bad behaviour of a malware family?

$$\frac{\Gamma, x : \tau_p \vdash t : \tau_r}{\Gamma \vdash (\lambda x : \tau_p . t) : \tau_p \to \tau_r} Lam$$

Tool, tool, tool, ..., in useful, rigorous and efficient way.

$$\frac{\Gamma \vdash t_f : \tau_p \to \tau_r \qquad \Gamma \vdash t_p : \tau_p}{\Gamma \vdash t_f\ t_p : \tau_r} App$$



Wei Chen @ Informatics, UoE.

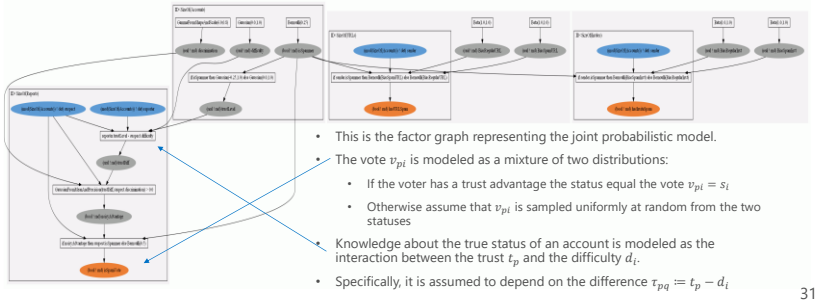
James Cheney

Andy Gordon

Cryptographic and Probabilistic Programming

Andrew D. Gordon
(MSR and University of Edinburgh)

Probabilistic Model for Skype Abuse Detection



- This is the factor graph representing the joint probabilistic model.
- The vote v_{pi} is modeled as a mixture of two distributions:
  - If the voter has a trust advantage the status equal the vote $v_{pi} = s_i$
  - Otherwise assume that v_{pi} is sampled uniformly at random from the two statuses
- Knowledge about the true status of an account is modeled as the interaction between the trust t_p and the difficulty d_i.
- Specifically, it is assumed to depend on the difference $\tau_{pq} := t_p - d_i$

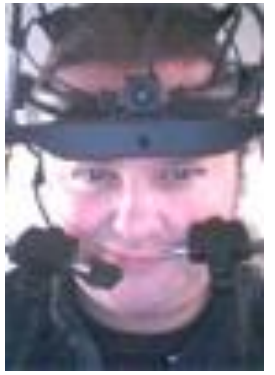
Robin Hill

trust in and through technology

- Human factors & user behaviour
  - Visual and affective factors that encourage stronger security and vigilance, e.g. password generation.
  - Nudge.
  - Biometrics, e.g.
    - Eye-gaze behaviour.
    - Facial microexpressions.
- Trust
  - Adoption and prolonged use of technology.
  - Belief in information presented (FullFact.org):
    - Webpages;
    - social media;
    - Politics.
  - Why people “open the door” willingly.

design informatics

NRlabs
neuropolitics research



Robin Hill

Institute for Language, Cognition & Computation,
School of Informatics
and
Neuropolitics Research Lab,
Politics and International Relations
www.robin.org.uk
r.l.hill@ed.ac.uk

Petros Wallden

The cut-and-choose technique in a quantum world

Petros Wallden

Glimpses of Cyber Security and Privacy Research, Edinburgh

5th October 2016

Security in a Quantum World

1. Secure classical protocols against quantum adversaries (immediate threat)

   (a) Different hard problems, **(b) different proof techniques**, (c) different types of attacks (see Marc Kaplan)

2. Quantum enhanced classical protocols (use quantumness to boost security or efficiency of classical protocols)

3. Quantum Key Distribution (information-theoretic security, applications based on QKD and OTP. e.g. "quantum digital signatures")

- Advance crypto primitives:

  Multi-party computation, Proofs of knowledge, FHE

- Classical techniques for boosting security:

  Cut-and-choose (boost honest-but-curious to malicious), rewinding (required for simulators)

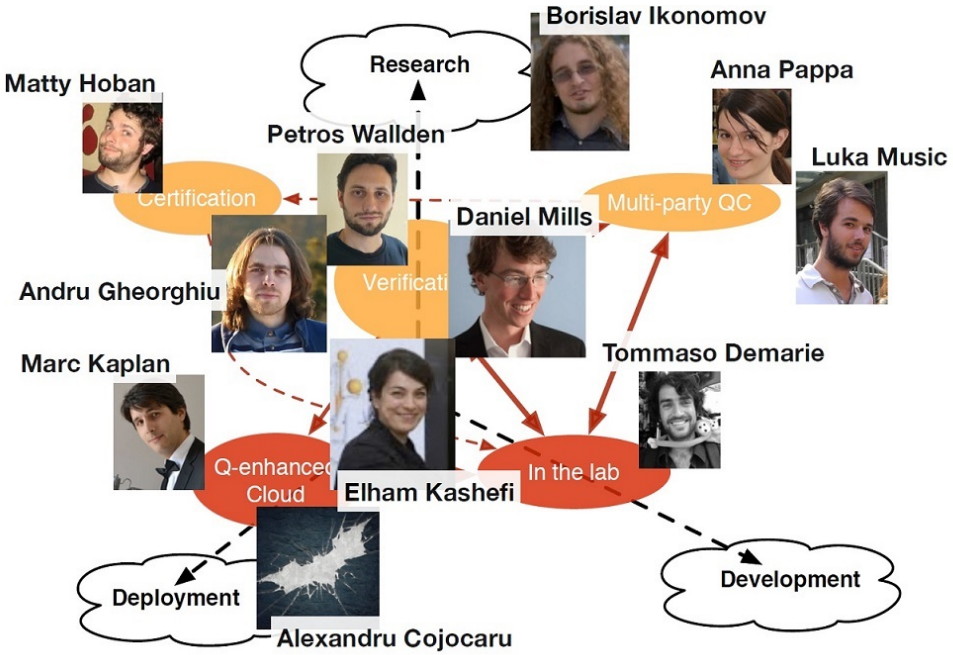
- Quantum limitations

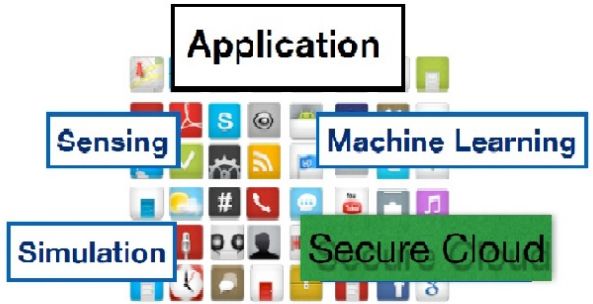
  Cannot apply rewinding (quantum "no-cloning"), etc

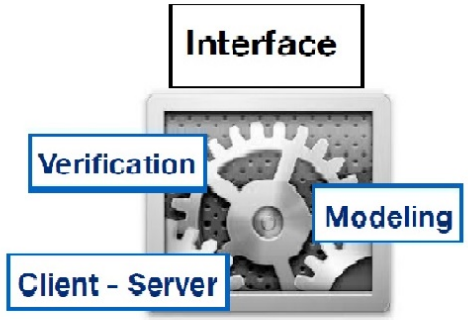
- When is it possible?

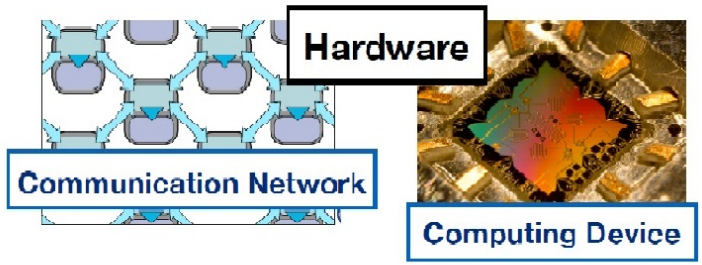
  When to use these generic techniques (application for quantum 2-party computation)

Quantum Group: Vision & People









Aggelos Kiayias

Security, Privacy and Blockchain systems

Aggelos Kiayias

aggelos.kiayias@ed.ac.uk

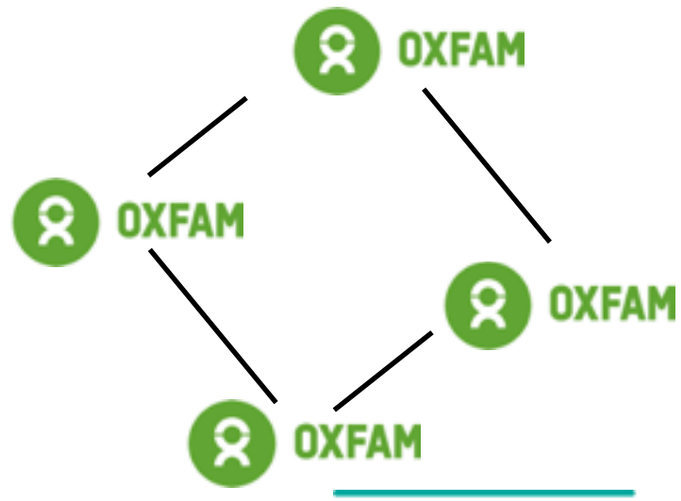
Panoramix

Building a privacy preserving communication infrastructure for Europe.

HORIZON 2020

OXCHAIN

Radically changing the logistical back-end of the Oxfam donation distribution network



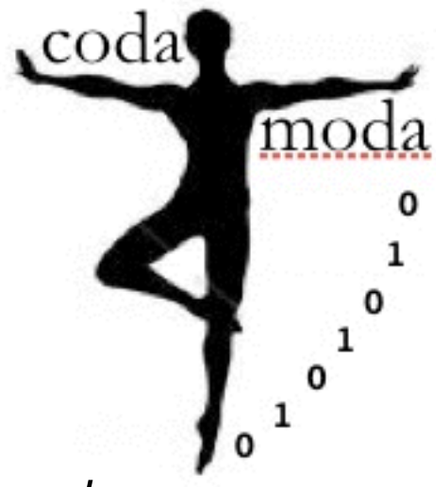
EPSRC
Engineering and Physical Sciences Research Council

dēmos Voting

first system ever with unconditional integrity for electronic elections

http://www-en.demos-voting.com

codamoda



erc European Research Council

we perform foundational research on security of blockchain protocols

one of the most influential bitcoin related papers of 2015, coinbase.com

Joseph Hallett

Digital camera embedded on handheld devices might be disabled in restricted environments, according to 〈Company〉 risk analysis. In sensitive facilities, information can be stolen using pictures and possibly sent using MMS or E-mail services.

In high-security facilities such as R&D labs or design manufacturers, camera MUST be disabled. Furthermore, MMS messages should be disabled as well, to prevent malicious users from sending proprietary pictures.

— SANS Security Policy for Handheld Devices

Joseph Hallett — J.Hallett@sms.ed.ac.uk

Ewa Luger

Using Design Thinking to Communicate Data Protection Principles

Ewa Luger, Design Informatics

Privacy by Design…

"an approach to projects that promotes privacy and ***data protection compliance from the start****"*

locates the user, and their interests, as central to the design of IT systems and business practices

Multidisciplinary tensions…

Law, Social Science & Design

Balancing differing priorities & accepting trade-offs

Accuracy/rigours; conceptual sensitising; stimulating creative thinking

In the wild; Testing in industry and education

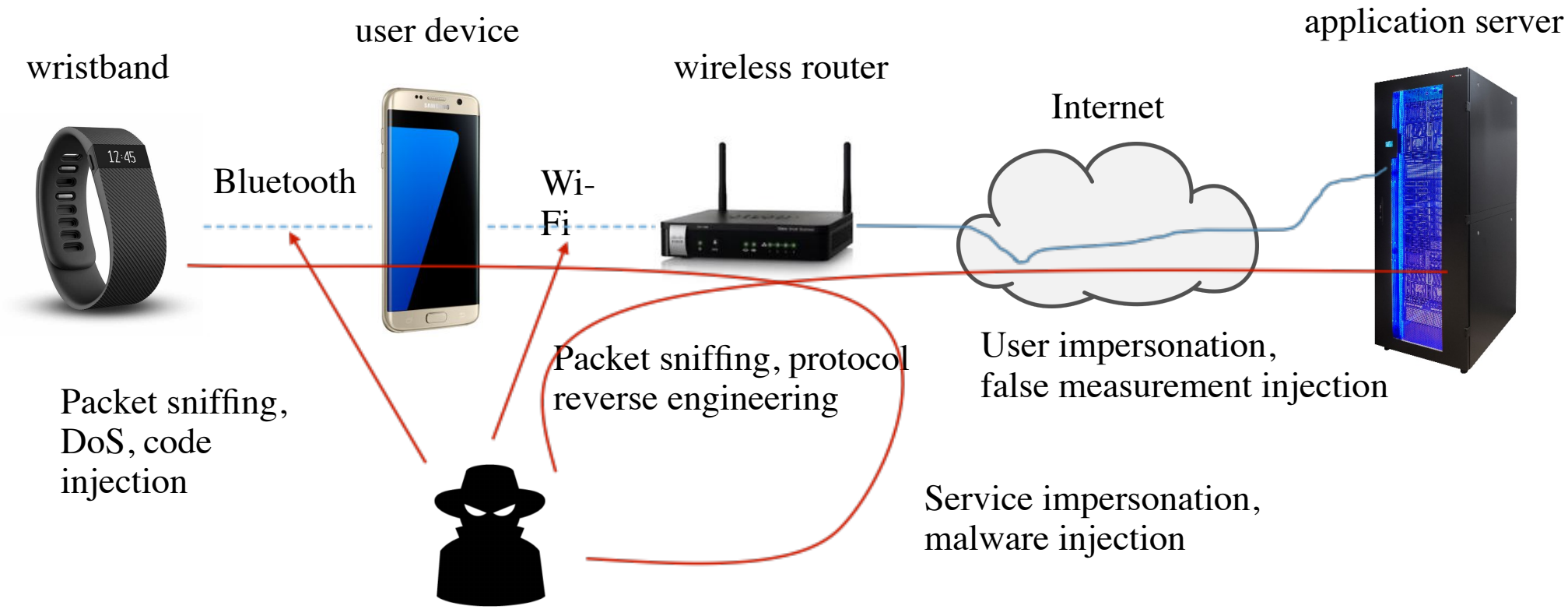
Findings

DP knowledge vague/non concern
The consent issue is unsolved
Regulation not seen as 'protective' but 'inhibitive' (barrier)
Lightweight tools required for agile methodology

Paul Patras

A Glimpse of Wearables' Vulnerabilities

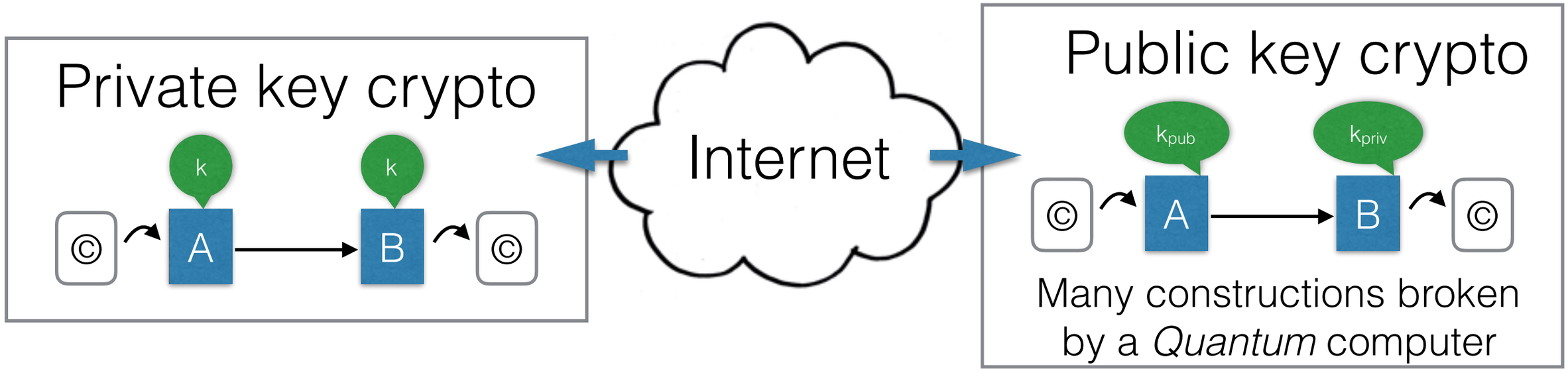
How to identify and repair weakness of indifferent networking parts?



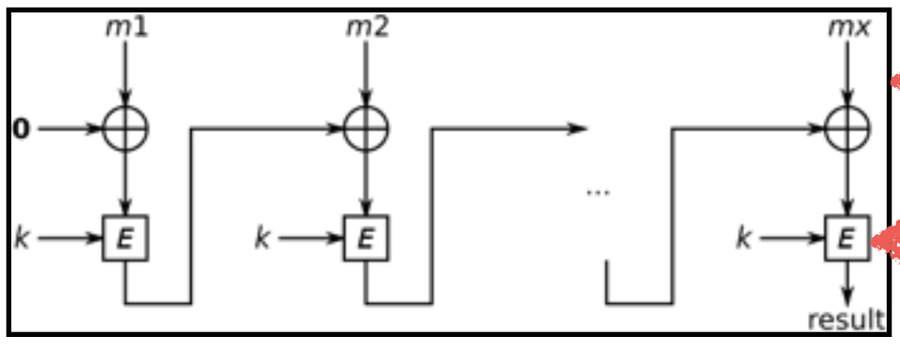
Larissa Pschetz

BitBarista: exploring perceptions of data transactions in IoT

Marc Kaplan



Quantum attacks on modes of operation



NOT quantum safe

quantum safe

Requires a more advanced setting:
Quantum internet for enhanced protocols
Hidden quantum effects
Obfuscation

Post-quantum *symmetric* cryptography requires new proof techniques too

---

Javier Escudero

Tristan Henderson

PREDICTING CONSENT FOR MEDICAL DATA SHARING

- Online social networks are increasingly used for medical purposes (support groups, diagnosis, ...)
- Rights and new regulations means that consent should be obtained (repeatedly) for collecting and using such data
- Obtaining consent in a *sustained* fashion is burdensome, but *secured* consent is inaccurate[1]
- Can we predict when to request consent?[2]
- Can we build systems that alleviate privacy concerns?[3]
- (my day job is at St Andrews, but I'm an interloper in Law and Informatics this year. Please come and talk to me!)
- tnhh.org @tnhh wellcome trust

[1] S. McNeilly, L. Hutton, and T. Henderson. Understanding ethical concerns in social media privacy studies. In *Proc. ACM CSCW Workshop on Measuring Networked Social Privacy: Qualitative & Quantitative Approaches*, 2013

[2] L. Hutton and T. Henderson. "I didn't sign up for this!": Informed consent in social network research. In *Proc. ICWSM*, 2015

[3] Y. Zhao, J. Ye, and T. Henderson. The effect of privacy concerns on privacy recommenders. In *Proc. IUI*, 2016

Larissa Pschetz

University of Edinburgh
Cyber Security and Privacy Research Network

http://cybersecpriv.ed.ac.uk

Glimpses of Cyber Security and Privacy Research
5th October 2016
Informatics Forum: Mini Forum 1 (2nd floor, Lunch 12.30pm); 4.31/33 (Talks, 2pm)

Welcome! This is an introduction event for people in the Cyber Security and Privacy Research Network in the University of Edinburgh. It is aimed at researchers, teaching staff and PhD students.

There will be a series of short "glimpses" into ongoing or future research. Researchers are asked to give a 3 minute overview of some of their recent research in the area of cyber security and/or cyber privacy. The presentation should be understandable to non-specialists, and focus on potential for connections to people in other Schools or subject areas. Talking about potential collaborative research topics is encouraged.

Schedule

- 2:00. Introduction
- 2:05. David Aspinall (Informatics). *Security with Digital forms of Evidence*.
- 2:10. Myrto Arapanis (Informatics). *Automatic Verification of Cryptographic Protocols.*
- 2:15. Angus Bancroft (Sociology). *Resilience of Cyber-criminal Markets.*
- 2:20. Wei Chen (Informatics). *Swift Behavioural Analysis for Android Apps.*
- 2:25. James Cheney (Informatics). *Graph Databases: handling Advanced Persistent Threats in Real Time?*
- 2:30. Andy Gordon (Informatics). *Cryptographic and Probabilistic Programming.*
- 2:35. Robin Hill (Informatics, Politics & International Relations). *Biometrics and Human Behaviour.*
- 2:40. Petros Wallden (Informatics). *The Cut-and-Choose Technique in a Quantum World.*
- 2:45. Aggelos Kiayias (Informatics). *TBA.*
- 2:50. Joseph Hallett (Informatics). *Capturing Security Policies for BYOD.*
- 3:00. Ewa Luger (Design Informatics). *Using Design Thinking to Communicate Data Protection Principles.*
- 3:05. Paul Patras (Informatics). *A Glimpse of Wearables' Vulnerabilities.*
- 3:10. Larissa Pschetz (Design Informatics). *BitBarista: Exploring Perceptions of Data Transactions in IoT*
- 3:15. Marc Kaplan (Informatics). *Quantum Attacks of Symmetric Cryptography.*
- 3:20. Javier Escudero (Engineering). *User Authentication with Brain Activity.*
- 3:25. Tristan Henderson (Uni. of St Andrews). *Towards Predicting Consent for Medical Data Sharing.*
- 3:30. Burkhard Schafer (Law). *Solidarity, cybersecurity and the law*
- 3:35. Remarks from others; comment and discussion.
- 3:50. Close

Additional attendees include: Alan Bundy (Informatics), Charles Raab (Politics & International Relations).

***Cyber Security** is concerned with protecting computer systems and their data against malicious or accidental damage. This includes methods for prevention, detection and response. **Cyber Privacy** is concerned with ensuring privacy of individuals and groups when using computer systems and their data. In the technical scientific community, the study of Cyber Security and Privacy has been intertwined from the start; recently, finding effective notions of privacy management in the digital realm has become vital for cyber security in society at large. As a topic of research, Cyber Security and Privacy concerns many disciplines, ranging from science and engineering, through to human, socio-technical factors, economic incentives, and the legal and political setting. Research at University of Edinburgh reflects this breadth, occurring in numerous research groups across multiple disciplines. The University of Edinburgh Cyber Security and Privacy Research Network was founded to connect people across these different disciplines, bridging subject areas, Schools and Colleges.*