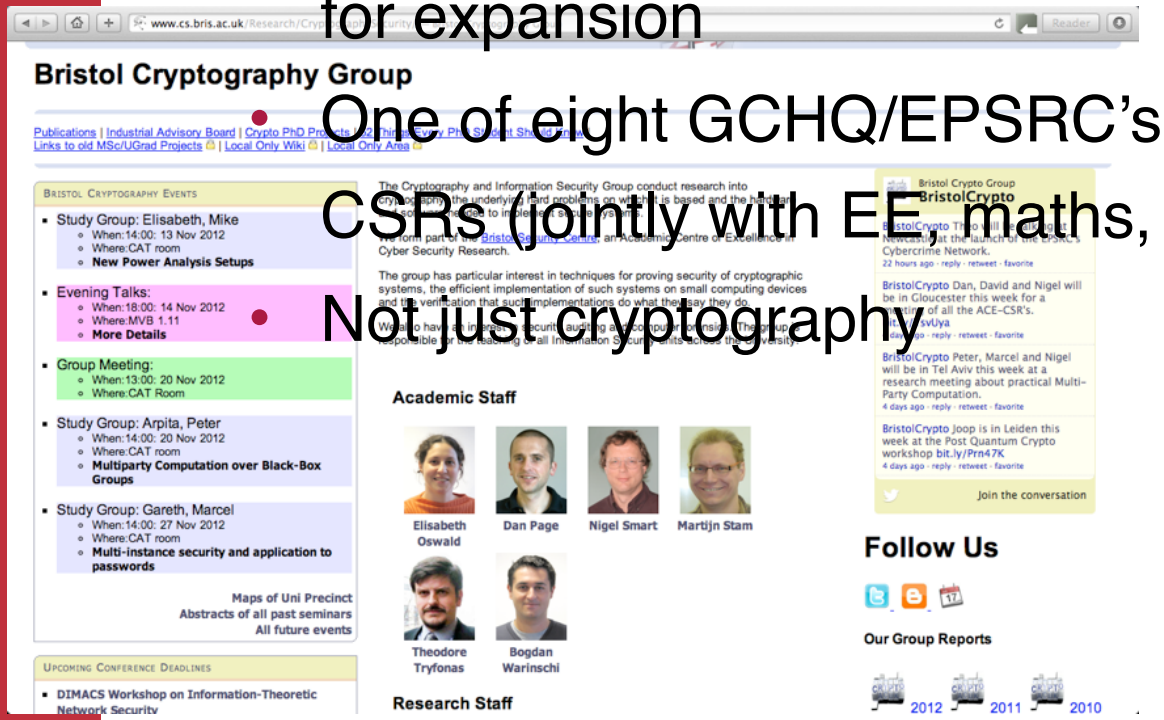
Theo Tryfonas, Cryptography Group

Cybercrime Network

Kick off meeting, Newcastle 9 Nov 2012

Bristol Crypto Group

- Largest cryptography group in the country, one of the largest in the world
- 6 academics, 12 RAs, 17 research students, plans for expansion
- One of eight GCHQ/EPSRC's accredited ACE-CSRs (jointly with EE, maths, applied psychology)
- Not just cryptography



University of BRISTOL

Current activity in the area of Cybercrime

- EU Home DG Project: Forensic Tools against Internet abuse (ForToo, HOME/2010/ISEC/AG/INT-002)
  - Open source tools for forensics in emerging networks and technologies: wireless and mobile, (mobile) social networking, IoT (sensor nets), mobile evidence visualisation
- EPSRC Leadership Fellowship (Elisabeth)
  - cryptological work, but including study of social implications of power analysis attacks

University of BRISTOL

Current activity in the area of Cybercrime
(cont'd)

- Other research in:
  - Chip-and-pin security analysis
  - Understanding malware DDoS attack strategies with game theory
  - DDoS protection via cryptographic puzzles
  - Sensor network (IoT) forensics (infrastructure, access to system integrators)

University of BRISTOL

Indicative pubs

- Andriotis, P., Oikonomou, G. and Tryfonas, T. (2012), “Forensic Analysis of Wireless Networking Evidence of Android Smartphones”, IEEE WIFS 2012
- Petroulakis, N., Askoxylakis, G. and Tryfonas, T. (2012), “Life-logging in Smart Environments: Challenges and Security Threats”,2012 IEEE ICC – WS CONWIRE
- Zaharis, A., Martini, A., Tryfonas, T. Illioudis, C. and Pangalos, G. (2011), “Lightweight Steganalysis based on Image Reconstruction & Lead Digit Distribution Analysis”, Intl Jour. of Digital Crime and Forensics, 3(4), 29-41

University of BRISTOL

Potential applications

- Using Multi-Party Computing to enable sharing of data between crime fighting agencies without revealing all the data (or any of it bar the output of the comparison)
- Looking into the feasibility of power analysis for forensic purposes (Trojan detection etc.)
- Digital evidence visualisations from various stakeholder perspectives (analysts, Jury etc.)
- **EMERGING THEME: Understanding risk from potential abuse of emerging technologies - data provenance in mobile and cloud computing (tech), system design implications (socio-tech)**

University of BRISTOL

Context

- Increased national awareness and topical interest for ‘Cyber-’ topics, e.g.
  - Situational awareness
  - Security Science
  - Program analysis (related to our area)
- But...
  - Continuously increasing challenges (Police workload, sophistication of criminal attacks, emerging threats)
  - Available forensic capability (esp. in the light of efficiencies, e.g. FSS)

University of BRISTOL

Challenge?

Engage further with Government and funders, need for further investment in this area and complement the national security perspective of existing initiatives with the '-crime' agenda

Thank you!

Theo Tryfonas

Bristol Cryptography Group

Faculty of Engineering

theo.tryfonas@bristol.ac.uk

University of BRISTOL