Lero THE IRISH SOFTWARE RESEARCH CENTRE

Science Foundation Ireland sfi For what's next

University of Limerick, Ollscoil Luimnigh

Engineering Forensic-Ready Systems

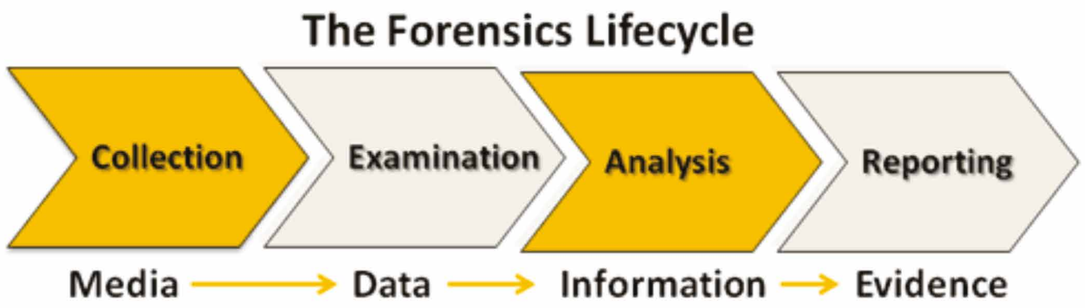
George Grispos, Supervised by: Prof. Bashar Nuseibeh

1 Motivation

» Globally, **1 billion** data records were compromised in 2014 and it is estimated that cybercrime costs the Irish economy **€630 million** a year [1].

» Cisco: **"wherever users go, cyber-criminals will follow"** [2] – increased need for digital forensic investigations in environments such as cloud computing and smart buildings.

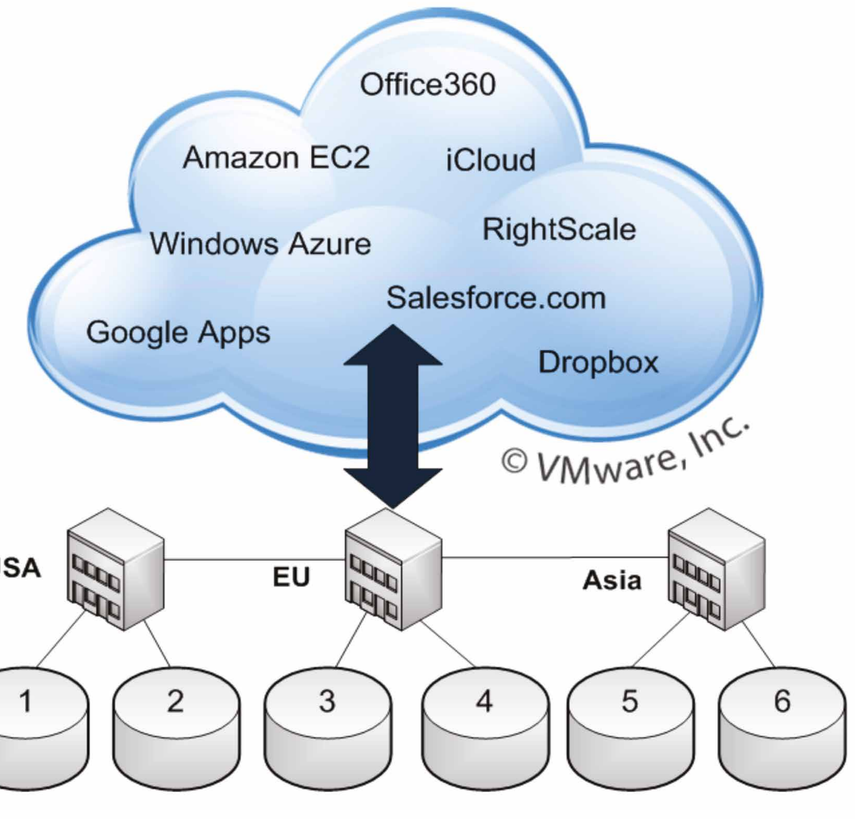
» Traditional forensic approaches involve acquiring data from storage media *after* a security incident or crime occurs.



» However, this can result in several problems:
  › Lost data from volatile sources;
  › Large amount of data from multiple sources;
  › No evidence to collect because of a lack of forensic-readiness.

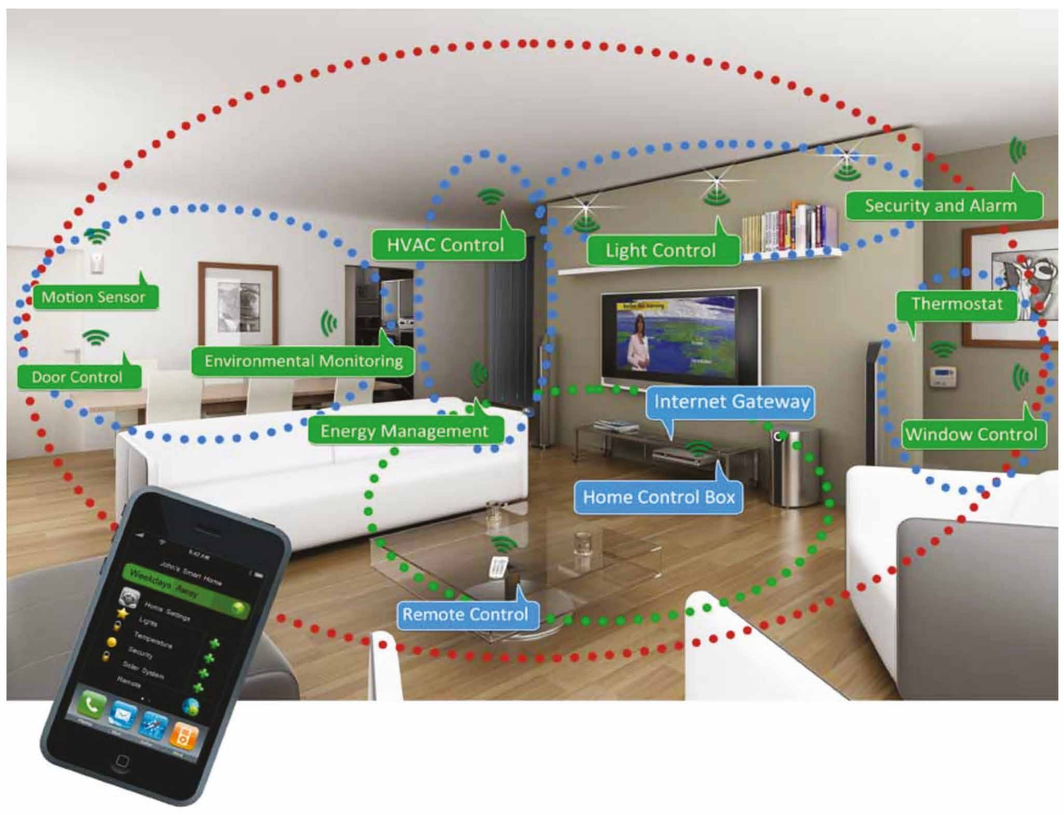
How do we avoid these problems and engineer forensic-ready systems?

2 Problem Examples (I)



» The remote, distributed and virtualised nature of the cloud obstructs the conventional approach to evidence acquisition [3-5]:
  › Distributed nature of the cloud can make the identification of a single storage device containing relevant data impractical;
  › Evidence acquisition can be obstructed by cross-border jurisdictions;
  › Lack of tools available to recover evidence in a forensically-sound manner.

3 Problem Examples (II)



» Smart home/building forensics pose similar challenges [6]:
  › Large amount of data stored in a variety of locations – will this data actually be useful to a forensic investigation?
  › Short data retention times are projected;
  › Physical-end devices may be neither readily accessible nor easily locatable;
  › Lack of evidence correlating information.

4 Proposed Research

» The research will look to address the following research questions:
  › What is a forensic-ready system?
  › How can we integrate forensic-readiness into new systems?
  › How can we integrate forensic-readiness into existing systems?
  › Can we automate, at the design stage, how we engineer forensic-ready systems?

» How is forensic-readiness impacted by the Internet of Things and Emerging Critical Systems?

» Development of Forensic Readiness Framework.

» Manual application of framework to use cases and real-world case studies.

» Development of automated tools to assist with determining level of forensic-readiness at design-time.

» Evaluation of prototype tools against case studies and development of strategies to enhance forensic-readiness of smart buildings and cloud computing.

References

[1] RTE News. Cybercrime costs Irish economy €630m a year http://www.rte.ie/news/business/2014/0403/606405-cybercrime-costs-irish-economy-630m-per-year/

[2] Cisco. Cisco 2011 Annual Security Report: http://www.cisco.com/c/dam/en/us/products/collateral/security/security_annual_report_2011.pdf

[3] Grispos, George; Tim Storer; and William Bradley Glisson. (2012). Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics. International Journal of Digital Crime and Forensics (IJDCF) 4(2), pp. 28-48.

[4] Ruan, Keyun; Joe Carthy; Tahar Kechadi; and Mark Crosbie. (2011). Cloud forensics. In Advances in Digital Forensics VII, pp. 35-46.

[5] Dykstra, Josiah, and Alan T. Sherman. (2011). Understanding issues in cloud forensics: two hypothetical case studies. In Proceedings of the Conference on Digital Forensics, Security and Law, pp. 45-54.

[6] Sutherland, Iain; Theodoros Spyridopoulos; Huw Read; Andy Jones; Graeme Sutherland and Mikhailia Burgess. (2015). Applying the ACPO Guidelines to Building Automation Systems. In Human Aspects of Information Security, Privacy, and Trust, pp. 684-692.

Ireland's European Structural and Investment Funds Programmes 2014-2020
Co-funded by the Irish Government and the European Union

European Union
European Regional Development Fund

United Technologies Research Center

SOUTHERN Regional Assembly
Promoting our Region