Securing the Internet of Things:
A ZKP-based Approach

Padraig Flood
M.Sc. Software Design and Development
National University of Ireland, Galway

Discipline of Information Technology
College of Engineering & Informatics
31st September 2014

Head of Discipline:
Dr Michael Madden

Supervisor:
Dr Michael Schukat
Abstract

Over the past few years, the Internet of Things has made significant steps towards becoming a reality. Until now, this has been largely the widespread usage of smartphones and tablets but further technological advancements are required before it can truly reach its potential. While advancements are being made for hardware issues which serve as barriers for potential new products (e.g. low-power network connectivity), as of yet, there has been little progress made in the way of developing new security standards. The estimated 50 billion internet-connectable devices in circulation by the year 2020 raises major questions about the scalability and suitability of existing internet security mechanisms.

The existing mechanisms used to provide privacy, data integrity and end-entity authentication between communicating peers are well-established (e.g. TLS). Designed 20 years ago with systems such as home computers primarily in mind and involving complex computational processes, they may not be feasible for devices with limited resources such as the small embedded systems which will permeate the Internet of Things. The currently Internet-security infrastructure has also had its reputation seriously damaged by recent events such as the disclosure of the PRISM surveillance programme.

This research paper proposes an alternative authentication protocol using a graph theory based zero-knowledge proof which is suitable for the resource constrained networks and systems of the Internet of Things. While the protocol currently requires a-priori knowledge about the network setup and structure, it includes provisions to handle a key-sharing approach which guarantees perfect forward secrecy.

The purpose of this research is to further determine the requirements of a security infrastructure for the embedded processors of the Internet of Things while assessing the feasibility and practicalities of the alternative authentication protocol proposal through the development of an initial prototype.
## Contents

1 Introduction.........................................................................................................................1

Overview.............................................................................................................................1

1.1 Motivation .................................................................................................................1

1.2 Research Hypothesis .................................................................................................2

1.3 Scope .........................................................................................................................2

1.4 Published Works........................................................................................................3

1.5 Thesis Layout ............................................................................................................4

2 Literature Review ...............................................................................................................5

Overview.............................................................................................................................5

2.1 Internet Protocol Suite (TCP/IP)................................................................................6

2.1.1 Internet Protocol ............................................................................................7

2.1.1.1 IPv4 ...............................................................................................7

2.1.1.2 IPv6 ...............................................................................................8

2.1.2 Transmission Control Protocol......................................................................9

2.2 Computer Security and Cryptography.....................................................................10

2.2.1 Symmetric Cryptography ............................................................................10

2.2.1.1 The Data Encryption Standard ........................................................11

2.2.1.2 The Advanced Encryption Standard ...........................................11

2.2.2 Public-Key Cryptography (Asymmetric Cryptography).............................12

2.2.2.1 Diffie-Hellman Key Exchange...................................................13

2.2.2.1.1 The Algorithm .......................................................14

2.2.2.1.2 Perfect Forward Secrecy........................................14
### Contents

2.2.2.2 The RSA Encryption Algorithm ........................................... 15

2.2.3 Public-Key Infrastructure ........................................................... 15
   2.2.3.1 Digital Certificates .............................................................. 16
   2.2.3.2 Transport Layer Security ...................................................... 17
      2.2.3.2.1 Record Protocol .......................................................... 18
      2.2.3.2.2 Cipher Change Spec Protocol ................................. 18
      2.2.3.2.3 Alert Protocol .............................................................. 18
      2.2.3.2.4 Handshake Protocol ...................................................... 19
   2.2.3.3 Infrastructure Weaknesses .................................................... 20
      2.2.3.3.1 X.509 Standards and Certificate Authorities ............ 20
      2.2.3.3.2 RSA Key Encapsulation ........................................... 20
   2.2.3.4 Recent Noteworthy Events ................................................... 20
      2.2.3.4.1 Heartbleed .............................................................. 20
      2.2.3.4.2 Certificate Authorities ........................................... 21
      2.2.3.4.3 NSA Surveillance Disclosures ............................... 21
      2.2.3.4.4 Transport Layer Security Version 1.3 ...................... 22

2.3 Zero Knowledge Proofs ........................................................................ 23
   2.3.1 Interactive Proof Systems ....................................................... 23
   2.3.2 Zero-Knowledge ......................................................................... 23
   2.3.3 The Graph Isomorphism Problem ............................................... 24
      2.3.3.2 The Graph Isomorphism Zero-Knowledge Protocol ........... 25

2.4 Internet of Things .................................................................................. 27
   2.4.1 History and Development ........................................................... 27
   2.4.2 Process of Evolution ................................................................... 28
   2.4.3 Required Technologies ............................................................... 29
      2.4.3.1 Uniquely Identifiable Objects .......................................... 29
## Contents

2.4.3.2 Resource-Efficient Network Connectivity ...........................................30
  2.4.3.2.1 Low-Power Wireless Communication Standards ......................................30
  2.4.3.2.2 Power Harvesting ...............................................................................31

2.4.3.3 Security Concerns .............................................................................31
  2.4.3.3.1 Complexity of Existing Security Infrastructure ......................................31
  2.4.3.3.2 Current Product Development Practices ...............................................31
  2.4.3.3.3 Reports of Vulnerabilities ..................................................................32

3 Design ........................................................................................................33
  Overview .........................................................................................................33

3.1 Specifications ............................................................................................33
  3.1.1 Initial Authentication Prototype ...................................................................33
  3.1.2 A Public-Key Infrastructure ......................................................................33

3.2 Peer-to-Peer ...............................................................................................34

3.3 The Authentication Protocol .....................................................................36
  3.3.1 Initial Requirements ..................................................................................36
  3.3.2 Digital Representations of Graphs and Processes ........................................37
  3.3.3 Step-by-step ............................................................................................38
  3.3.4 Key Negotiation Procedure ......................................................................38
    3.3.4.1 Ensuring Authenticity ...........................................................................39
    3.3.4.2 Steps Including EDH ..........................................................................40

3.4 Allocation of Limited Resources .................................................................41

3.5 Comparison to TLS ...................................................................................41

4 Implementation .............................................................................................42
  Overview .........................................................................................................42

4.1 Initial Development Decisions ....................................................................42
4.2 Peer-to-Peer Network ........................................................................................................43

4.3 The Authentication Protocol ..............................................................................................44

4.3.1 Regular Graphs .............................................................................................................45

4.3.2 Isomorphic Graphs ........................................................................................................46

4.3.2.1 Storage and Generation of an Isomorphism ..................................................46

4.3.2.2 Building an Isomorphic Graph ............................................................................47

4.3.3 Table of Devices ...........................................................................................................49

4.3.4 Authentication Process ................................................................................................49

4.3.4.1 Generating Proof .................................................................................................49

4.3.4.2 Verifying Proof ....................................................................................................50

4.4 Maximising Limited Resources .......................................................................................51

4.4.1 Compressed Graphs .....................................................................................................51

4.4.2 Memory Management ..................................................................................................53

4.5 Key Negotiation ................................................................................................................54

4.5.1 Large Numbers .............................................................................................................54

4.5.1.1 The MIRACL Library ..........................................................................................54

4.5.1.1.1 Initialisation .....................................................................................................54

4.5.1.1.2 Limitations .....................................................................................................55

4.5.2 Diffie-Hellman Key Exchange .....................................................................................55

4.5.3 Embedding Process .......................................................................................................56

4.5.3.1 Preparation ............................................................................................................56

4.5.3.2 Encoding Process ..................................................................................................58

4.5.3.3 Decoding Process ..................................................................................................59

4.5.3.4 Security Concerns .................................................................................................59

4.6 Debugging ........................................................................................................................60

4.6.1 Functions ......................................................................................................................60
Figures

Figure 2.1: Visual representation of an IPv4 Header ................................................................. 7
Figure 2.2: Graph outlining the projected growth rate of connected devices and internet users relative to the IPv4 address limit ............................................................................. 8
Figure 2.3: Graph displaying the percentage of devices accessing Google services over IPv6 on a daily basis between 1st January 2012 and 28th June 2014 ........................................ 8
Figure 2.4: Visual representation of an IPv6 header ................................................................................................. 9
Figure 2.5: TCP header .............................................................................................................. 9
Figure 2.6: Comparison of encryption algorithms .............................................................................. 12
Figure 2.7 Example of a CA’s role in a public-key infrastructure with digital certificates .... 16
Figure 2.8: Visual representation of the TLS protocol stack ................................................................. 18
Figure 2.9: TLS handshake protocol .............................................................................................................. 19
Figure 2.10: An isomorphic graph with the isomorphism and corresponding edges labelled 24
Figure 2.11: Visual representation of the Graph-Isomorphism Protocol .................................................. 25
Figure 3.1: Peer to Peer ............................................................................................................ 34
Figure 3.2: Client-Server ......................................................................................................... 34
Figure 3.3: Peer-to-Peer Flowchart .......................................................................................... 35
Figure 3.4: Representing a graph using two-dimensional arrays .................................................. 37
Figure 3.5: Segment of protocol flowchart for the verification round ........................................ 38
Figure 3.6: Piecewise encoding of public-key ............................................................................. 39
Figure 4.1: Visual display of the permutation process ............................................................. 48
Figure 4.2: Matrix repeating graph information ............................................................................. 51
Figure 4.3: Solution to repeat information problem ................................................................. 51
Figure 4.4: A sample program built using the MIRACL library from the MIRACL manual .55
Figure 4.5: Wireshark unencrypted data .................................................................................... 60
Figure 4.6: Unencrypted permutations ............................................................................................. 61
Figure 4.7: Debian 7.6 on VMware Workstation v10 ................................................................. 63
Figure 4.8: Lucid Puppy Linux 5.285 running on VMware Workstation with 94MB of RAM ..............................................64
Figure 4.9: SPSS 22 output file viewer ...................................................................................................................64
Figure 5.1: Screengrab of one round’s worth of data over a network for 64-vertex graphs...........................................66
Figure 5.2: OS performance comparison ..................................................................................................................71
Figure 5.3: Barchart representation of the data from table 5.4 ...............................................................................72
Figure 5.4: Comparison of costs on basis of public-key size ..................................................................................73
Figure 5.5: Boxplot results of key size performance tests ......................................................................................74
Figure 5.6: Trend lines across a collection of thread durations ................................................................................74
Figure 6.1: An elliptic curve .................................................................................................................................75
Figure 6.2: Cooja network simulator on Instant Contiki ........................................................................................................77

Tables

Table 2.1: TCP/IP Layers ........................................................................................................................................6
Table 2.2: comparing complexity of key sizes depending on type ...........................................................................13
Table 2.3 Diffie-Hellman Key Exchange ................................................................................................................14
Table 2.4: Content of a digital certificate ................................................................................................................17
Table 3.1: Prototype comparison with TLS ............................................................................................................41
Table 4.1: List of macros located throughout code ..................................................................................................44
Table 4.2: Comparing the computational complexity of graph isomorphism problem ........................................45
Table 4.3: The Fisher-Yates Shuffle .......................................................................................................................46
Table 4.4: Possible solutions routes for Protocol ....................................................................................................50
Table 4.5: Potential reductions allowed for 4 of the most likely graph size implementations .............................52
Table 4.6: Memory allocation functions ................................................................................................................53
Table 4.7: Diffie-Hellman related MIRACL functions .............................................................................................56
Table 5.1: Computational overheads per round ....................................................................................................65
Table 5.2: Total communication overheads of protocol ..........................................................................................66
Table 5.3: Communication overheads for graphs in protocol ................................................................................66
Table 5.4: SPSS produced output of graph size performance ................................................................................72
1 Introduction

Overview
The Internet of Things (IoT) is only beginning to become a reality, with a high level of interest from a wide variety of industries keen to exploit the possibilities it offers, as evidenced at CES this year by the likes of Internet-connectable toothbrushes (Clark & Fowler, 2014), it can only continue to rise in prominence for the foreseeable future. Forecasted growth rates for the number of IoT devices in circulation range are universally high.

The emergence of the Internet of Things (IoT) is set to radically alter the face of the Internet, significantly increasing the number and range of devices connected to the internet. However, existing internet security standards were designed with systems such as home computers in mind and therefore may not be suitable for the smaller internet enabled devices. This research looks into the issues IoT is currently facing regarding the secure transmitting of data.

1.1 Motivation
Privacy, data integrity and end-entity authentication are essential features of computer communication. The lack of a standardised approach with which to adequately achieve these features for small embedded systems was the primary motivation of this research.

The de-facto standard to provide these features is Transport Layer Security (TLS), which utilises digital certificates and asymmetric cryptography for authentication and the sharing of a symmetric key for continued confidentiality of data. Nearing 20 years of age, TLS was not designed with embedded systems in mind and there has yet to be any signs of an IoT-friendly variation to the standard emerging in the foreseeable future.
Without a public-key infrastructure, the security capabilities of small embedded systems within the Internet of Things are severely constrained, having to either depend on compromises such as pre-shared and manually inputted keys to encrypt data, or transmit data without encryption. The anticipated increase in the number of resource-constrained Internet-enabled devices in the next few years as the Internet of Things continues to emerge will bring with them a whole new range of security concerns which need to be addressed.

1.2 Research Hypothesis

The emergence of the Internet of Things raises questions about the suitability and scalability of existing computer communication security standards. Zero-Knowledge Proofs (ZKP) offer an alternative means of authentication with significantly lower overheads which may be an ideal alternative to existing approaches for resource-constrained devices.

The role of this research was to evaluate the existing and projected environment of the Internet of Things. From this understanding, develop an authentication protocol using ZKPs which meets the requirements of Internet security as best possible without the need for resource-consuming processes.

1.3 Scope

The limited timeframe and lack of prior research materials available to work from put considerable limitations onto the scope of the research. Primarily, this research aims to provide the initial groundwork with which to build a new public-key infrastructure for the resource constrained networks and devices of the Internet of Things.

The problem was approached from the following two angles so as to meet the desired objectives of the thesis statement.

Objective 1:

With the rapid development of the Internet of Things, there were constant new developments occurring for the duration of this research. To ensure the research remained relevant, there was a need to present a thorough understanding of the advancements being in research made from the hardware side toward a fully-realised Internet of Things.
Due to the inextricably linked nature of IoT to the existing Internet framework, a solid understanding of existing Internet standards was also necessary along with some background information as to how and why standards are developed. A thorough understanding of the cryptographic approaches involved in modern Internet standards was very important for assessing the quality of alternative approaches.

Objective 2:

In conjunction with the generalised research into IoT, an alternative authentication approach has been proposed as an alternative to TLS which utilises a zero-knowledge proof to reliably authenticate devices for a relatively low computational overhead (Goldwasser, Micali, & Rackoff, 1985). An initial proof-of-concept prototype was to be developed to ensure the protocol’s viability. Following the successful implementation of this initial prototype, the focus moved toward achieving a means with which to ensure confidentiality of data sent over the network and an updated version of the prototype was produced which aims to achieve this goal.

1.4 Published Works

The work undergone in the research process for this thesis led to papers for the work being accepted at two conferences to be presented over the summer of 2014. This thesis expands upon the content of these papers by delving into the subject in significantly greater detail. It also features a practical implementation of the protocol.

- “ZKP in M2M Communications”
  Irish Signals & Systems Conference 2014; Limerick, Ireland
  (Schukat & Flood, 2014a)
- “Peer-to-Peer Authentication for Small Embedded Systems”
  10th Annual Conference on Digital Technologies, Zilina, Slovakia
  (Schukat & Flood, 2014b)
1. Introduction

1.5 Thesis Layout

- The proceeding chapter of the thesis provides a broad overview of the range of areas which a reasonable range of knowledge is necessary to be able to adequately assess the requirements of the Internet of Things:
  - Existing Internet standards and the system through which they were both created and are maintained
  - Technical and historical aspects of computer security
  - The Internet of Things itself, covering the current environment, future projections and steps being taken to advance the concept
  - A brief overview of the underlying concepts in zero-knowledge proofs.

- Chapter 3 focuses in detail on the individual design objectives for the prototype; the reasons behind these choices and assessed alternatives are also covered. This chapter effectively covers the steps involved prior to the development of a working protocol.

- Chapter 4 expands upon the design objectives by delving into the technical aspects of how they were implemented into the overall programme and areas for potential improvement.

- Chapter 5, assesses the initial recorded results of each multiple versions of our protocol to each other and to differing hardware specifications.

- Chapter 6 attempts to provide a brief overview of some of the potential avenues which future work may go down.

- The final chapter contains the author’s concluding comments regarding the research and their ideas for future work.
7 Conclusion

The purpose of this research was to assess whether there was a need for a resource-efficient alternative to the existing Internet security standards given the emergence of the Internet of Things. To further understand and gauge the viability of such a proposal, a protocol had to be designed with a prototypical implementation.

To fully assess the requirements of such a protocol, extensive research into the environments and standards of the Internet of things and general Internet security needed to be undertaken. The results of this research are present in the literature review and frequently referred to throughout the research. Additional research efforts into areas were also undertaken but are largely tangential to the purposes of this research paper (e.g. graph theory, programming).

Over the period of time in which this research has occurred both the Internet of Things and concerns regarding the security of the Internet of Things have risen significantly in prominence. While the latest version of TLS which is in development removes some of the noted weaknesses of the current infrastructure such as the lack of perfect forward secrecy, there has been little to suggest that there will be any particular efforts made to cater for the small embedded systems and wireless sensor nodes of the Internet of Things.

The results of the testing process as outlined in chapter 5 show that the protocol already operates well on low-powered home computers. With considerable scope for optimisation in all areas other than the communication overheads of the protocol, there is little reason to not continue developing the protocol.
Appendix

Flow-chart specifications for the initial static Diffie-Hellman key exchange
Bibliography


http://www.wired.com/2012/03/ff_nsadatacenter/all/1


www.puppylinux.com/about.htm


https://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_descracker_pressrel.html

http://www.symantec.com/connect/blogs/despite-news-your-refrigerator-not-yet-sending-spam


www.vmware.com/products/workstation

http://mashable.com/2014/04/14/heartbleed-open-source/

http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras

