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 Inter 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

Figures

Tables

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.

Obejective 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.

<u>Objective 2:</u>

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)

1.5 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.

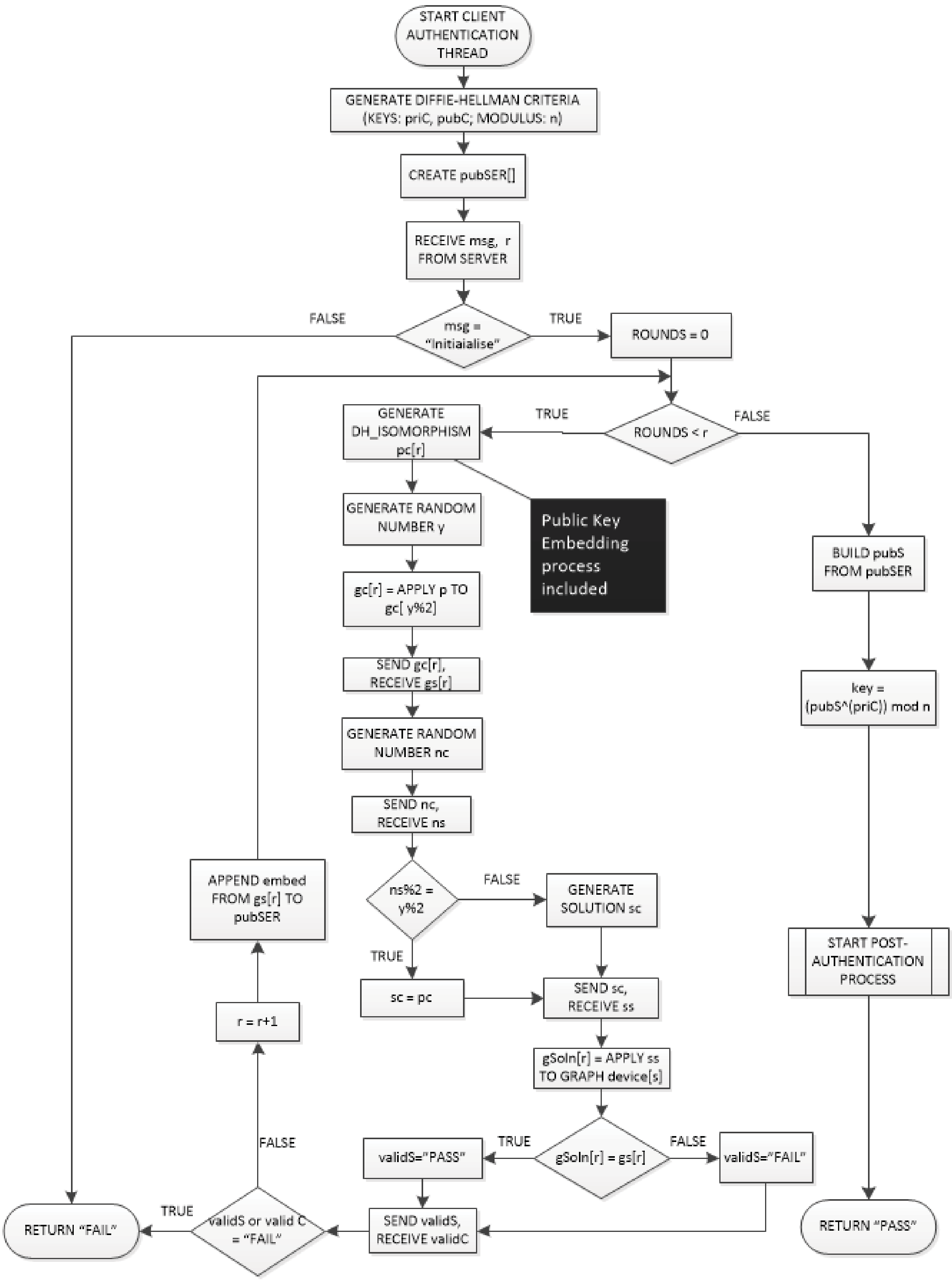
To fully assess the requirements of such a protocol, extensive research into the environments and standards of the Internet of things and general Internet security needed to be undertaken. The results of this research are present in the literature review and frequently referred to throughout the research. 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 inital static Diffie-Hellman key exchange



Bibliography

ABC News. (2013, August 13). *Baby Monitor Hacking Alarms Houston Parents.* Retrieved August 20, 2014, from ABC News: http://abcnews.go.com/blogs/headlines/2013/08/baby-monitor-hacking-alarms-houston-parents/

Amadio, M. (2012, April 5). *Puppy 5.28 Lucid.* Retrieved August 20, 2014, from PuppyLinux.org: puppylinux.com/wikka/Puppy526

Apple Computers. (2014, February 21). *About the security content of iOS 7.0.6.* Retrieved May 30, 2014, from Apple.com: http://support.apple.com/kb/HT6147

Aronsson, H. A. (1995). *Zero Knowledge Protocols and Small Systems.* Department of Computer Science, Helsinki University of Technology.

Arora, M. (2012, May 7). *How secure is AES against brute force attacks?* Retrieved August 20, 2014, from Electronic Engineering Times: http://www.eetimes.com/document.asp?doc_id=1279619

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A Survey. *Computer networks, 54*(15), 2787-2805.

Bamford, J. (2012, March 15). *The NSA Is Building the Country's Biggest Spy Centre (Watch What You Say).* Retrieved August 5, 2014, from Wired: http://www.wired.com/2012/03/ff_nsadatacenter/all/1

Barker, E., & Roginsky, A. (2012). *Special Publication 800-57.* National Institute of Standards and Technology.

Barr, M., & Mass, A. (2006). *Programming embedded systems: with C and GNU development tools.* O'Reilly Media Inc.

Bernstein, D. J. (2006). Curve25519: New Diffie-Hellman Speed Records. *Public-Key Cryptography-PKC 2006*, 207-228.

Beth, T. (1988). *Efficient zero-knowledge identification scheme for smart cards.* Berlin: Springer.

Bluetooth. (2014). *Baseband Architecture.* Retrieved August 24, 2014, from Bluetooth Developer Portal: https://developer.bluetooth.org/TechnologyOverview/Pages/Baseband.aspx

Bluetooth. (2014b). *Bluetooth Smart Devices List.* Retrieved August 20, 2014, from Bluetooth: http://www.bluetooth.com/Pages/Bluetooth-Smart-Devices-List.aspx

Braden, R. (1989). *RFC 1122.* IETF.

Buettner, M., Prasad, R., Sample, A., Yeager, D., Greenstein, B., Smith, J. R., et al. (2008). RFID sensor networks with the Intel WISP. *Proceedings of the 6th ACM conference on Embedded network sensor systems* (pp. 393-394). ACM.

Chown, P. (2002). *RFC 3268.* IETF.

Cisco. (2012). *The Internet of Things.* Retrieved May 30, 2014, from Cisco Visualization: http://share.cisco.com/internet-of-things.html

Cisco. (2014, January). *The Internet of Everything—A $19 Trillion Opportunity.* Retrieved May 30, 2014, from Cisco.com: http://www.cisco.com/web/services/portfolio/consulting-services/documents/consulting-services-capturing-ioe-value-aag.pdf

Comodo Group. (2011, March 23). *Report of Incident on 15-MAR-2011.* Retrieved May 30, 2014, from Comodo.com: https://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., & Polk, W. (2008). *RFC 5280.* IETF.

Curtin, M., & Dolske, J. (1998, May). A Brute Force Search of DES Keyspace. *;login:*.

Dearing, G. (2013, December 12). *Why GE and Others are Investing in the Internet of Things.* Retrieved August 20, 2014, from Forbes: http://www.forbes.com/sites/centurylink/2013/12/12/why-ge-and-others-are-investing-in-the-internet-of-things/

Debian Project. (2014). *Debian -- The Universal Operating System.* Retrieved August 20, 2014, from debian.org: www.debian.org

Deering, S., & Hinden, R. (1998). *RFC 2460.* IETF.

Dierks, T., & Allen, C. (1999). *RFC 2246.* IETF.

Dierks, T., & Rescorla, E. (2008). The Transport Layer Security (TLS) Protocol Version 1.2. *RFC 5246*.

Dierks, T., & Rescorla, E. (2014). *The Transport Layer Security (TLS) Protocol Version 1.3 draft-ietf-tls-rfc5246-bis-00.* IETF.

Diffie, W. (1988). The first ten years of public-key cryptography. *Proceedings of the IEEE, 76*(5), 560-577.

Diffie, W., & Hellman, M. E. (1976a). Multiuser cryptographic techniques. *Proceedings of the June 7-10, 1976, National computer conference and exposition.* ACM.

Diffie, W., & Hellman, M. E. (1976b). New directions in cryptography. *IEEE Transactions on Information Theory, 22*(6), 644-654.

Ellison, C., & Schneier, B. (2000). Ten risks of PKI: What you're not being told about public-key infrastructure. *Comput Secu J, 16*(1), 1-7.

Evans, D. (2013, July 16). *Moving to IPv6: Rebuilding the Heart of the Internet Without Missing a Beat.* Retrieved August 15, 2014, from Cisco Blogs: http://blogs.cisco.com/ioe/moving-to-ipv6-rebuilding-the-heart-of-the-internet-without-missing-a-beat/

Feige, U., Fiat, A., & Shamir, A. (1988). Zero-knowledge proofs of identity. *Journal of cryptology, 1*(2), 77-94.

Fiveash, K. (2014, April 24). *DeSENSORtised: Why the 'Internet of Things' will FAIL without IPv6.* Retrieved August 5, 2014, from TheRegister.co.uk: http://www.theregister.co.uk/2014/04/24/ipv6_iot/

Friedl, M., Provos, N., & Simpson, W. (2006). *RFC 4419.* IETF.

Gartner. (2014, March 19). *Gartner Says the Internet of Things Will Transform the Data Center*. Retrieved August 5, 2014, from Gartner Newsroom: http://www.gartner.com/newsroom/id/2684616

Gerich, E. (1993). *RFC 1466.* IETF.

Gimmer, M., Petras, K., & Revol, N. (2004). Multiple precision interval packages: Comparing different approaches. In *Numerical Software with Result Verification* (pp. 64-90). Springer Berlin Heidelberg.

Goldreich, O. (2007). *Foundations of Cryptography: Volume 1, Basic Tools.* Cambridge University Press.

Goldreich, O., Micali, S., & Wigderson, A. (1991). Proofs that Yield Nothing But Their Validity or All Languages in NP Have Zero-Knowledge Proof Systems. *Journal of the ACM, 38*(3), 690-728.

Goldwasser, S., Micali, S., & Rackoff, C. (1985). The knowledge complexity of interactive proof-systems. *STOC '85: Proceedings of the seventeenth annual ACM symposium on Theory of computing*, 291-304.

Google. (2014). *IPv6 - Statistics.* Retrieved August 15, 2014, from Google: https://www.google.com/intl/en/ipv6/statistics.html

Google. (n.d.). *IPv6 - Overview.* Retrieved from Google.com: http://www.google.com/intl/en/ipv6/

Greenberg, A. (2013, June 20). *Leaked NSA Doc Says It Can Collect And Keep Your Encrypted Data As Long As It Takes To Crack It.* Retrieved August 20, 2014, from Forbes: http://www.forbes.com/sites/andygreenberg/2013/06/20/leaked-nsa-doc-says-it-can-collect-and-keep-your-encrypted-data-as-long-as-it-takes-to-crack-it/

Greenwald, G., MacAskill, E., Poitra, L., Ackerman, S., & Rushe, D. (2014, July 12). *Microsoft handed the NSA access to encrypted messages.* Retrieved August 5, 2014, from The Guardian: http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

Grzonkowski, S., Zaremba, W., Zaremba, M., & McDaniel, B. (2008). Extending web applications with a lightweight zero knowledge proof authentication. *Proceedings of the 5th international conference on Soft computing as transdisciplinary science and technology* (pp. 65-70). ACM.

Gutmann, P. (2001). *Everything you never wanted to know about pki but were forced to find out.* Retrieved August 20, 2014, from University of Auckland: https://www.cs.auckland.ac.nz/~pgut001/pubs/pkitutorial.pdf

Gutmann, P. (2002). PKI: It's not dead, just resting. *Computer, 35*(8), 41-49.

Guttman, B., & Roback, E. A. (1995). *An introduction to computer security: the NIST handbook.* DIANE Publishing.

Harkins, D., & Carrel, D. (1998). *RFC 2409.* IETF.

Hawkes, A. M., Katko, A. R., & Cummer, S. A. (2013). A microwave metamaterial with integrated power harvesting functionality. *Applied Physics Letters, 103*(16).

Hewlett Packard. (2014). *Internet of Things Research Study.* Retrieved from HP Fortify Protect: http://fortifyprotect.com/HP_IoT_Research_Study.pdf

Hill, K. (2013, July 26). *When 'Smart Homes' Get Hacked: I Haunted A Complete Stranger's House Via The Internet.* Retrieved August 20, 2014, from Forbes: http://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/

Hoffman-Andrews, J. (2013, November 22). *Forward Secrecy at Twitter.* Retrieved August 5, 2014, from Twitter Blob: https://blog.twitter.com/2013/forward-secrecy-at-twitter

Holohan, E., & Schukat, M. (2010). "Authentication using Virtual Certificate Authorities - A New Security Paradigm for Wireless Censor Networks". *The 9th IEEE International Symposium on Network Computing and Applications (IEEE NCA10).*

Housley, R., Curran, J., Huston, G., & Conrad, D. (2013). *RFC 7020.* IETF.

Hui, J., & Thubert, P. (2011). *RFC 6282.* IETF.

IBM Corporation. (2013, August 13). SPSS Statistics 22.0.

ISO/IEC . (2011). *ISO/IEC 9899:201x - Programming Languages - C.* International Organisation for Standardization.

Kaufman, C., Perlman, R., & Speciner, M. (2002). *Network Security: Private Communication in a Public World.* Prentice Hall Press.

Kauler, B. (2003). Puppy Linux.

Kim, E. (2014, July 30). *News Report Shows Edward Snowden's Revelations Are Seriously Damaging US Tech Firms.* Retrieved August 5, 2014, from Business Insider: http://www.businessinsider.com/edward-snowden-us-tech-firms-2014-7

Kleinjung, T., Aoki, K., Franke, J., Lenstra, A. K., Thomé, E., Bos, J. W., et al. (2010). Factorization of a 768-bit RSA modulus. *Advances in Cryptology-CRYPTO 2010*, 333-350.

Knuth, D. (1981). *The Art of Computer Programming, Vol 2: Seminumerical Algorithms.* Reading, Mass.: Addison-Wesley.

Kocher, P. C. (1996). Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. *CRYPTO '96 Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*, 104-113.

Kohlar, F., Schage, S., & Schwenk, J. (2013). On the Security of TLS-DH and TLS-RSA in the Standard Model. *IACR Cryptology ePrint Archive*.

Langley, A. (2013, December 7). *Further improving digital certificate security.* Retrieved August 20, 2014, from Google Online Security Blog: http://googleonlinesecurity.blogspot.ie/2013/12/further-improving-digital-certificate.html

Lee, J.-S., Su, Y.-W., & Shen, C.-C. (2007). A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. *IECON 2007. 33rd Annual Conference of the IEEE* (pp. 46-51). IEEE.

Marine, A., Reynolds, J., & Malkin, G. (1994). *RFC 1594.* IETF.

Marine, A., Reynolds, J., & Malkin, G. (1994). *RFC 1594.* IETF.

Mettler, A., Raman, V., & Zhang, Y. (2014, August 20). *SSL Vulnerabilities: Who listens when Android applications talk?* Retrieved August 20, 2014, from FireEye: http://www.fireeye.com/blog/technical/2014/08/ssl-vulnerabilities-who-listens-when-android-applications-talk.html

Michael, R. G., & S. Johnson, D. (1979). *Computers and intractability: a guide to the theory of NP-completeness.* San Francisco: WH Freeman & Co,.

Mutton, P. (2014, April 8). *Half a million widely trusted websites vulnerable to heartbleed bug.* Retrieved August 3, 2014, from Netcraft: http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html

National Bureau of Standards. (1977). *FIPS PUB 46.*

National Institute of Standards and Technology. (1997). Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard (AES). *Federal Register, 62*(177), 48051-48058.

National Institute of Standards and Technology. (2001). *FIPS PUB 197: Announcing the Advanced Encryption Standard.* National Institute of Standards and Technology.

National Institute of Standards and Technology. (2005, May 19). Announcing Approval of the Withdrawal of Federal Information Processing Standard (FIPS) 46–3, Data Encryption Standard (DES); FIPS 74, Guidelines for Implementing and Using the NBS Data Encryption Standard; and FIPS 81, DES Modes of Operation. *Federal REgister, 70*(96), 28907-28908.

Nordmark, E., & Gilligan, R. (2005). *RFC 4213.* IETF.

Postel, J. (1981b). *RFC 793.* IETF.

Postel, J. (1981c). *RFC 791.* IETF.

Poster, J. (1981a). *RFC 801.* IETF.

Press, G. (2014, August 18). *It's Official: The Internet of Things Takes Over Big Data As The Most Hyped Technology.* Retrieved August 20, 2014, from Forbes: http://www.forbes.com/sites/gilpress/2014/08/18/its-official-the-internet-of-things-takes-over-big-data-as-the-most-hyped-technology/

Puppy Community. (2014). *About Puppy.* Retrieved August 20, 2014, from PuppyLinux: www.puppylinux.com/about.htm

Regalado, A. (2014, May 20). *Business Adapt to a New Style of Computer.* Retrieved August 5, 2014, from Technology Review: http://www.technologyreview.com/news/527356/business-adapts-to-a-new-style-of-computer/

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM, 21*(2), 120-126.

Rose, A. (2013, January 11). *The Internet of Things Has Arrived - And So Have Massive Security Issues.* Retrieved August 20, 2014, from Wired: http://www.wired.com/2013/01/securing-the-internet-of-things/

RSA Laboratories. (2014). *Public-Key Cryptography Standards: What key size should be used?* Retrieved August 20, 2014, from EMC.com: http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/key-size.htm

Salowey, J. (2014, March 26). *[TLS] Confirming Consensus on removing RSA key Transport from TLS 1.3.* Retrieved August 5, 2014, from IETF Mail Archive: http://www.ietf.org/mail-archive/web/tls/current/msg11621.html

Schneier, B. (1995). *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (2nd ed.). John Wiley & Sons.

Schneier, B. (2009, July 1). *New Attack on AES.* Retrieved August 20, 2014, from Schneier on Security: https://www.schneier.com/blog/archives/2009/07/new_attack_on_a.html

Schneier, B. (2013, November 6). *Elliptic Curve Crypto Primer - Comments.* Retrieved May 30, 2014, from Schneier on Security: https://www.schneier.com/blog/archives/2013/11/elliptic_curve.html#c2200076

Schneier, B. (2014a, April 9). *Heartbleed.* Retrieved May 31, 2014, from Schneier on Security: https://www.schneier.com/blog/archives/2014/04/heartbleed.html

Schneier, B. (2014b, January 6). *The Internet of Things is Wildly Insecure - And Often Unpatchable.* Retrieved August 20, 2014, from Schneier on Security: https://www.schneier.com/essays/archives/2014/01/the_internet_of_thin.html

Schnorr, C. P. (1991). Efficient signature generation by smart cards. *Journal of cryptology 4.3*, 161-174.

Scott, M. (2014). *MIRACL Cryptographic SDK*. Retrieved August 20, 2014, from Certivox: www.certivox.com/miracl

Singh, S. (1999). *The Code Book: the evolution of secrecy from Mary, Queen of Scots, to quantum cryptography.* Doubleday.

Smith, S., & Marchesini, J. (2007). *The Craft of System Security.* Pearson.

Soghoian, C., & Stamm, S. (2012). Certified Lies: Detecting and defeating government attacks against SSL (short paper). *Financial Cryptography and Data Security*, 250-259.

Sotirov, A., Stevens, M., Appelbaum, J., Lenstra, A., Molnar, D., Osvik, D. A., et al. (2008, December 30). *MD5 considiered harmful today: Creating a rogue CA certificate.* Retrieved August 20, 2014, from Eindhoven University of Technology: http://www.win.tue.nl/hashclash/rogue-ca/

Sparkes, M. (2014, July 30). *Average Internet of Things device has 25 security flaws.* Retrieved August 30, 2014, from The Telegraph: http://www.telegraph.co.uk/technology/internet-security/11000013/Average-Internet-of-Things-device-has-25-security-flaws.html

Stallings, W. (2001, November 30). *TCP/IP Architecture and Operation: TCP and UDP*. Retrieved August 15, 2014, from Informit: http://www.informit.com/articles/article.aspx?p=24258&seqNum=5

Stallings, W. (2011). *Data and Computer Communications* (9 ed.). Pearson Education.

Stallings, W. (2014). *Cryptography and Network Security: Principles and Practice* (6 International ed.). Pearson Education.

Stinson, D. R. (2005). *Cryptography: Theory and Practice* (3rd ed.). Chapman and Hall/CRC.

Tanenbaum, A., & Van Steen, M. (2002). *Distributed Systems: Principles and Paradigms.* Pearson Prentice Hall.

Taylor, D., Wu, T., Mavrogiannopoulos, N., & Perrin, T. (2007). *RFC 5054.* IETF.

The Electronic Frontier Foundation. (1998, July 17). *"EFF DES Cracker" Machine Brings Honesty to Crypto Debate.* Retrieved August 15, 2014, from Electronic Frontier Foundation: https://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_descracker_pressrel.html

Thomas, P. (2014, January 23). *Despite the News, Your Refrigerator is Not Yet Sending Spam.* Retrieved August 20, 2014, from Symantec: http://www.symantec.com/connect/blogs/despite-news-your-refrigerator-not-yet-sending-spam

Thompson, K. (2007, March). Backup Encryption. *SysAdmin.*

Trustwave SpiderLabs. (2013, August 8). *Hard-Coded Bluetooth PIN Vulnerability in LIXIL Satis Toilet.* Retrieved August 20, 2014, from Trustwave: https://www3.trustwave.com/spiderlabs/advisories/TWSL2013-020.txt

Turner, S., & Polk, T. (2011). *RFC 6176.* IETF.

van Beijnum, I. (2006, September). IPv6 Internals. *The Internet Protocol Journal, 9*(3).

van Beijnum, I. (2014, June 12). *With the Americas running out of IPv4, it's official: The Internet is full.* Retrieved August 15, 2014, from Ars Technia: http://arstechnica.com/information-technology/2014/06/with-the-americas-running-out-of-ipv4-its-official-the-internet-is-full/

VMware Inc. (2014). *VMware Workstation*. Retrieved August 20, 2014, from vmware.com: www.vmware.com/products/workstation

Warren, C. (2014, April 14). *Heartbleed Exposes a Problem With Open Source, But It's Not What You Think.* Retrieved August 20, 2014, from Mashable: http://mashable.com/2014/04/14/heartbleed-open-source/

Watts, J. (2013, September 9). *NSA accused of spying on Brazilian oil company Petrobras.* Retrieved August 20, 2014, from The Guardian: http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras

Weiser, M. (1991). The computer for the 21st century. *Scientific American*, *265*(3), 94-104.

Wheeler, D. A. (2014, April 29). *How to Prevent the Next Heartbleed.* Retrieved August 20, 2014, from dwheeler.com: http://www.dwheeler.com/essays/heartbleed.html

Wireshark. (2014). *About*. Retrieved August 20, 2014, from Wireshark: www.wireshark.org/about.html

Yang, Y. (2006). The Taiwanese notebook computer production network in China: Implication for upgrading of the Chinese electronics industry. *Personal Computing Industry Center*.