UNIVERSITY OF BIRMINGHAM

School of Computer Science
College of Engineering and Physical Sciences

MSc. Project

Machine Learning & Deep Learning Approaches to Predict Credit Card Default

Submitted in conformity with the requirements
for the degree of MSc. Artificial Intelligence & Computer Science
School of Computer Science
University of Birmingham

Sarathkumar Padinjare Marath Sankaranarayanan
Student ID: 2359859
Supervisor: Dr.Kashif Rajpoot

September 2022

Abstract

The material contained within this report has not previously been submitted for a degree at the University of Birmingham or any other university. The research reported within this report has been conducted by the author unless indicated otherwise.

Sarathkumar Padinjare Marath Sankaranarayanan

Declaration

The material contained within this report has not previously been submitted for a degree at the University of Birmingham or any other university. The research reported within this report has been conducted by the author unless indicated otherwise.

Signed Sarathkumar Padinjare Marath Sankaranarayanan

"You have to learn the rules of the game.
And then you have to play better than anyone else"

Albert Einstein

MSc. Project
Machine Learning & Deep Learning Approaches to Predict Credit Card Default

Sarathkumar Padinjare Marath Sankaranarayanan

Contents

Table of Abbreviations

Introduction

Background Knowledge

Literature Review

Materials

Methodology

Results & Discussions

Conclusion & Summary

References

Amin Ghafari, V. & Mohajeri, J. (2011), 'An improved attack on A5/1', *Information Security and Cryptology (ISCISC), 2011 8th International ISC Conference on* pp. 41–44. Available: http://dx.doi.org/10.1109/ISCISC.2011.6062339. Online; accessed 1 August 2015.

Barker, W. C. & Barker, E. (2012), 'Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher', Available: http://csrc.nist.gov/publications/nistpubs/800-67-Rev1/SP-800-67-Rev1.pdf. Online; accessed 20 August 2015.

BBC News (2000), 'How the safety systems work', Available: http://news.bbc.co.uk/1/hi/uk/941526.stm. Online; accessed 6 August 2015.

Biham, E. (2002), 'How to decrypt or even substitute DES-encrypted messages in 228 steps', *Information Processing Letters* **84**(3), 117 – 124. Available: http://dx.doi.org/10.1016/S0020-0190(02)00269-7 Online; accessed 23 August 2015.

Blanchet, B. & Cheval, V. (2015), 'ProVerif: Cryptographic protocol verifier in the formal model', Available: http://prosecco.gforge.inria.fr/personal/bblanche/proverif/. Online; accessed 22 August 2015.

Bombardier (2015), 'Radio Block Centre - Rail Control Products - Bombardier', Available: http://www.bombardier.com/en/transportation/products-services/rail-control-solutions/products/radio-block-centre.html. Online; accessed 18 August 2015.

Briginshaw, D. (2014), 'Interoperability in Europe - still as elusive as ever?', Available: http://www.railjournal.com/index.php/signalling/interoperability-in-europe-still-as-elusive-as-ever.html. Online; accessed 10 August 2015.

BSI (2010), 'BS EN 50159:2010 – Railway applications. Communication, signalling and processing systems. Safety-related communication in transmission systems', Available: https://bsol.bsigroup.com/Bibliographic/BibliographicInfoData/000000000030202175. Online; accessed 12 July 2015.

BSI (2011), 'BS ISO/IEC 9797-1:2011 – Information technology. Security techniques. Message authentication codes (MACs). Mechanisms using a block cipher', Available: https://bsol.bsigroup.com/Bibliographic/BibliographicInfoData/000000000030105371. Online; accessed 15 July 2015.

Butcher, L. (2010), 'Railways: West Coast Main Line', Available: www.parliament.uk/briefing-papers/SN00364.pdf. Online; accessed 6 August 2015.

Calle-Sanchez, J., Molina-Garcia, M. & Alonso, J. I. (2012), 'Top Challenges Of LTE To Become The Next Generation Railway Communication System', *Computer in Railways* (13), 85–97. Available: http://dx.doi.org/10.2495/CR120081 Online; accessed 19 June 2015.

Cecchetti, G., Ruscelli, A. L., Cugini, F. & Castoldi, P. (2013), 'An implementation of EURORADIO protocol for ERTMS/ETCS systems', *World Academy of Science, Engineering and Technology* **7**, 354–363. Available: http://waset.org/publications/2166/an-implementation-of-euroradio-protocol-for-ertms-systems Online; accessed 8 June 2015.

Chothia, T. & Smirnov, V. (2010), 'A traceability attack against e-passports', *Financial Cryptography and Data Security* **6052**. Available: http://dx.doi.org/10.1007/978-3-642-14577-3_5. Online; accessed 18 August 2015.

Clear CinCom (2009), 'A short history and specifications overview of GSM-R', Available: http://gsmr-info.com/gsm-r_history.html. Online; accessed 2 August 2015.

Department for Transport (2007), 'ERTMS National Implementation Plan', Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/197194/ukertmsplan.pdf. Online; accessed 13 July 2015.

Department for Transport (2014), 'Rail Trends, Great Britain 2013/14', Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/363718/rail-trends-factsheet-2014.pdf. Online; accessed 10 July 2015.

Department for Transport (2015), 'Rolling Stock Perspective – Moving Britain Ahead', Available: https://www.angeltrains.co.uk/Portals/0/News_Downloads/DfT%20rolling-stock-perspective-July%202015.pdf. Online; accessed 12 August 2015.

Deutsche Bahn AG (2012), 'Public Roaming in the "P-GSM D" network', Available: fahrweg.dbnetze.com/fahrweg-en/technic/gsmr/public_roaming.html. Online; accessed 5 July 2015.

Dudoyer, S., Deniau, V., Slimen, N. B. & Adriano, R. (2012), 'Susceptibility of the GSM-R Transmissions to the Railway Electromagnetic Environment', *InTech* **1**(20), 503–522. Available: http://dx.doi.org/10.5772/36149. Online; accessed 16 July 2015.

European Commission (2013), 'What do we want to achieve ? - Rail', Available: http://ec.europa.eu/transport/modes/rail/index_en.htm. Online; accessed 12 August 2015.

Feix, B. & Thiebeauld, H. (2014), 'Defeating ISO9797-1 MAC Algo 3 by Combining Side-Channel and Brute Force Techniques', Available: http://eprint.iacr.org/2014/702.pdf. Online; accessed 18 August 2015.

Finnegan, M. (2014), 'Network Rail: Cyber security will be 'major issue' as business goes digital', Available: http://www.computerworlduk.com/news/data/network-rail-cyber-security-will-be-major-issue-as-business-goes-digital-3524405/. Online; accessed 10 May 2015.

Franekova, M., Rastocny, K., Janota, A. & Chrtiansky, P. (2011), 'Safety Analysis of Cryptography Mechanisms used in GSM for Railway', *International Journal of Engineering* **11**(1), 207–212. Available: http://annals.fih.upt.ro/pdf-full/2011/ANNALS-2011-1-34.pdf Online; accessed 7 June 2015.

Global Rail News (2011), 'Wholesale closure of almost every signal box on the network', Available: http://www.globalrailnews.com/2011/09/06/wholesale-closure-of-almost-every-signal-box-on-the-network/. Online; accessed 4 August 2015.

Gradowski, P., Bialon, A. & Gryglas, M. (2014), ' Function of Motive Situation in Procedure of Leadership of Train Equipped with System ERTMS', *Logistics and Transport* **23**(3), 55–62. Available: https://logistics-and-transport.eu/index.php/main/article/viewFile/280/322 Online; accessed 5 August 2015.

Green, M. (2013), 'Why I hate CBC-MAC', Available: http://blog.cryptographyengineering.com/2013/02/why-i-hate-cbc-mac.html. Online; accessed 10 July 2015.

GSM-R Industry Group (2014), 'GSM-R user procedures (cab radio)', Available: http://www.ertms-conference2014.com/assets/SESSION-PRESENTATIONS/S2/UIC-ERTMS-WC-2-1-Final1.pdf. Online; accessed 12 August 2015.

GSM-R Operators Group (2014), 'EIRENE - Systems Requirements Specification Version 15.4.0', Available: http://www.uic.org/IMG/pdf/p0028d004.3r0.5-15.4.0.pdf. Online; accessed 5 July 2015.

Handschuh, H. & Preneel, B. (2004), 'Minding Your MAC Algorithms?', *Information Security Bulletin* **9**, 213–220. Available: http://www.isg.rhul.ac.uk/static/msc/teaching/ic2/resources05/copies05/ISB0906HHBP.pdf Online; accessed 22 July 2015.

Hongjie, L., Lijie, C. & Bin, N. (2013), 'Petri net-based analysis of the safety communication protocol', *Telkomnika* **11**(10), 6034–6041. Available: http://findit.bham.ac.uk/44BIR_VU1:CSCOP_44BIR_DEEP:TN_scopus2-s2.0-84884711576 Online; accessed 9 June 2015.

IBM (n.d.), 'ANSI X9.19 Optional Procedure 1 MAC', Available: http://www-01.ibm.com/support/knowledgecenter/linuxonibm/com.ibm.linux.z.wskc.doc/wskc_c_ansix919opm.html. Online; accessed 18 August 2015.

Jain, A. & Chaudhari, N. S. (2013), 'Two trivial attacks on A5/1:A GSM stream cipher', *CoRR* **abs/1305.6817**. Available: http://arxiv.org/abs/1305.6817. Online; accessed 1 August 2015.

Karstensen, L. (2015), 'GSM A5/1 rainbow tables in Oslo, Norway', Available: https://lassekarstensen.wordpress.com/2013/08/08/gsm-a51-rainbow-tables-in-oslo-norway/. Online; accessed 1 August 2015.

Kendelbacher, D., , Schilling, H., Stein, F. & Siemens AG (2009), '(WO2009027380) METHOD FOR ETCS ONLINE KEY MANAGEMENT', Available: https://patentscope.wipo.int/search/en/detail.jsf?docId=WO2009027380. Online; accessed 8 August 2015.

Kessell, C. (2013), 'The future of GSM-R and its possible replacement', Available: http://www.railengineer.uk/2013/04/18/the-future-of-gsm-r-and-its-possible-replacement/. Online; accessed 18 July 2015.

Kim, J.-H., Kim, S.-H. & Choi, K.-H. (2014), 'A New RBC handover scheme for LTE-R system', *Journal of International Council on Electrical Engineering* **4**(3), 245–250. Available: http://dx.doi.org/10.5370/JICEE.2014.4.3.245 Online; accessed 19 June 2015.

KPMG (2013), 'IT Security Threat identification, Risk Analysis and Recommendations', Available: http://www.ertms.be/pdf/IT_Security_Threat_identification.pdf. Online; accessed 10 June 2015.

Lockstone, K. (2000), 'Active Attacks on Stream Ciphers with Cyclic Redundancy Checks (CRCs)', Available: http://www.cix.co.uk/~klockstone/crchack.htm. Online; accessed 3 July 2015.

Lu, J., Li, Z. & Henricksen, M. (2015), 'Time–Memory Trade-off Attack on the GSM A5/1 Stream Cipher Using Commodity GPGPU', *Proceedings of ACNS 2015 — The 13th International Conference on Applied Cryptography and Network Security* pp. 321–340.

Miller, C. & Valasek, C. (2015), 'Remote Exploitation of an Unaltered Passenger Vehicle', Available: http://illmatics.com/Remote%20Car%20Hacking.pdf. Online; accessed 12 August 2015.

Network Rail (2009), 'Connecting Local Communities – Route 18 - West Coast Main Line', Available: https://www.networkrail.co.uk/browse20documentsStrategicBusinessPlanRoutePlans\2009Route20182020West20Coast20Main20Line.pdf. Online; accessed 6 August 2015.

Network Rail (2012), 'Modernising the signalling on the Great Western main line has started', Available: http://www.networkrail.co.uk/news/2012/apr/modernising-the-signalling-on-the-Great-Western-main-line-has-started/. Online; accessed 12 August 2015.

Network Rail (2013), 'Cyber Security Strategy', Available: https://www.networkrail.co.uk/WorkArea/DownloadAsset.aspx?id=30064788605. Online; accessed 19 June 2015.

Network Rail (2015*a*), 'European Rail Traffic Management System (ERTMS)', Available: http://www.networkrail.co.uk/aspx/12275.aspx. Online; accessed 23 June 2015.

Network Rail (2015*b*), 'Introduction to ERTMS', Available: http://ertmsonline.com/what-is-ertms/. Online; accessed 18 June 2015.

Network Rail (2015*c*), 'London North Western South Sectional Appendix LNW(S)1', Available: http://www.networkrail.co.uk/browse%20documents/sectional%20appendix/london%20north%20western%20south%20sectional%20appendix.pdf. Online; accessed 10 August 2015.

Network Rail (2015*d*), 'Performance and Punctuality (PPM)', Available: http://www.networkrail.co.uk/about/performance/. Online; accessed 23 August 2015.

Network Rail (2015*e*), 'Railway Communications System (RCS)', Available: http://www.networkrail.co.uk/aspx/6386.aspx. Online; accessed 23 June 2015.

Network Rail (2015*f*), 'Your guide to European Rail Traffic Management System (ERTMS)', Available: http://ertmsonline.com/wp-content/uploads/2015/02/ERTMS-Guide.pdf. Online; accessed 21 July 2015.

openETCS (2015), 'OpenETCS Project Members', Available: https://itea3.org/project/openetcs.html. Online; accessed 10 July 2015.

RAIB (2012), 'Rail Accident Report: Incident at Llanbadarn Automatic Barrier Crossing (Locally Monitored), near Aberystwyth, 19 June 2011', Available: https://assets.digital.cabinet-office.gov.uk/media/547c8fdded915d4c0d000171/120627_R112012_Llanbadarn.pdf. Online; accessed 6 July 2015.

Rail Engineer (2013), 'Evolution of signalling control', Available: http://www.railengineer.uk/2013/05/21/evolution-of-signalling-control/. Online; accessed 25 July 2015.

Rail Safety and Standards Board (2013), 'Glossary of Railway Terminology - GERT8000', Available: http://www.rssb.co.uk/rgs/rulebooks/gert8000-gloss%20iss%201.pdf. Online; accessed 21 July 2015.

railway-technology.com (2015), 'Channel Tunnel Rail Link (CTRL), United Kingdom', Available: http://www.railway-technology.com/projects/chunnel/. Online; accessed 18 June 2015.

Rete Ferroviaria Italiana (2009), 'Protocollo Vitale Standard', Available: http://www.gare.italferr.it/cms-file/allegati/gare-italferr/PA-1146_ProtocolloVitaleStandard-RFI-DT-revA.pdf. Online; accessed 18 June 2015.

Rosaria, E., Armando, L., Pietro, M. & Angela, S. (2005), 'FORMAL VERIFICATION OF ERTMS EURORADIO SAFETY CRITICAL PROTOCOL', Available: http://www.math.unipd.it/~tullio/CS/Dispense_2005/Articolo-3.pdf. Online; accessed 20 June 2015.

RSSB (2012), 'GE/GN8608: Guidance on ERTMS/ETCS National Values', Available: http://author.rssb.co.uk/rgs/standards/GEGN8608%20Iss%201.pdf. Online; accessed 12 August 2015.

SmartWater Technology (2015), 'Network Rail extends SmartWater contract', Available: http://www.smartwater.com/news/network-rail-extends-smartwater-contract.html. Online; accessed 10 August 2015.

SR Labs (2010), 'Decrypting GSM phone calls', Available: https://srlabs.de/decrypting_gsm/. Online; accessed 3 August 2015.

Stevenson, A. (2015), 'National Rail cyber chief: Everyone must be vigilant against digital security threats', Available: http://www.v3.co.uk/v3-uk/news/2411642/national-rail-cyber-chief-everyone-must-be-vigilant-against-digital-security-threats. Online; accessed 15 June 2015.

UNIFE (2014), 'ERTMS Signalling Levels', Available: http://www.ertms.net/?page_id=42&1534-D83A_1933715A. Online; accessed 19 June 2015.

UNIFE (2015), 'Deployment Worldwide Map — ERTMS', Available: http://www.ertms.net/?page_id=55&1534-D83A_1933715A. Online; accessed 13 August 2015.

UNISIG (2012*a*), 'SUBSET-038: Off-line Key Management FIS', Available: http://www.era.europa.eu/Document-Register/Documents/Set-2-Index011-SUBSET-038%20v300.pdf. Online; accessed 18 June 2015.

UNISIG (2012*b*), 'SUBSET-044: FFFIS for Euroloop', Available: http://www.era.europa.eu/Document-Register/Documents/Set-2-Index016-SUBSET-044%20v240.pdf. Online; accessed 25 June 2015.

UNISIG (2012*c*), 'SUBSET-098: RBC-RBC Safe Communication Interface', Available: http://www.era.europa.eu/Document-Register/Pages/UNISIGSUBSET-098.aspx. Online; accessed 18 June 2015.

UNISIG (2012*d*), 'SUBSET-104: ETCS System Version Management', Available: http://www.era.europa.eu/Document-Register/Documents/Set-2-Index060-SUBSET-104%20v310.pdf. Online; accessed 25 June 2015.

UNISIG (2014*a*), 'FIS for the RBC/RBC Handover', Available: http://www.era.europa.eu/Document-Register/Documents/SUBSET-039%20v310.pdf. Online; accessed 15 June 2015.

UNISIG (2014*b*), 'SUBSET-026-3: System Requirements Specification – Chapter 3 - Principles', Available: http://www.era.europa.eu/Document-Register/Pages/SUBSET-026v300.aspx. Online; accessed 23 June 2015.

UNISIG (2014*c*), 'SUBSET-026-7: System Requirements Specification – Chapter 7 - ERTMS/ETCS language', Available: http://www.era.europa.eu/Document-Register/Pages/SUBSET-026v300.aspx. Online; accessed 23 June 2015.

UNISIG (2014*d*), 'SUBSET-026-8: System Requirements Specification – Chapter 8 - Messages', Available: http://www.era.europa.eu/Document-Register/Pages/SUBSET-026v300.aspx. Online; accessed 5 July 2015.

UNISIG (2014*e*), 'SUBSET-037: EuroRadio FIS', Available: http://www.era.europa.eu/Document-Register/Pages/UNISIGSUBSET-037.aspx. Online; accessed 18 June 2015.

Verdult, R., Garcia, F. D. & Ege, B. (2015), 'Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer', *USENIX* (22), 702–718. Available: https://www.usenix.org/sites/default/files/sec15_supplement.pdf Online; accessed 3 September 2015.

Wright, R. (2013), 'Crossrail and Thameslink take different approaches to risk', Available: http://www.ft.com/cms/s/0/82428d72-b272-11e2-8540-00144feabdc0.html. Online; accessed 18 June 2015.

Zetter, K. (2010), 'Hacker Spoofs Cell Phone Tower to Intercept Calls', Available: http://www.wired.com/2010/07/intercepting-cell-phone-calls/. Online; accessed 10 August 2015.

Zhang, Y., Tang, T., Li, K., Mera, J., Zhu, L., Zhao, L. & Xu, T. (2011), 'Formal verification of safety protocol in train control system', *Science China Technological Sciences* **54**(11), 3078–3090. Available: http://findit.bham.ac.uk/44BIR_VU1:CSCOP_44BIR_DEEP:TN_springer_jour10.1007/s11431-011-4562-2 Online; accessed 22 June 2015.

1 Appendix One: Code

1.1 Directory Structure

1.2 Running the Provided Code