New Zealand DEFENCE FORCE
Te Ope Kātua O Aotearoa

DEFENCE TECHNOLOGY AGENCY

DTA Report 449
NR 1749

Contact Harald Technical Assessment

Nathaniel J De Lautour
Logan J Small
Austin Chamberlain

November 2020

DTA Report 449
NR 1749

CONTACT HARALD TECHNICAL ASSESSMENT

Nathaniel de Lautour, Logan Small, Austin Chamberlain

November 2020

ABSTRACT

At the request of the Ministry of Health, DTA previously carried out an initial assessment of the Contact Harald contact tracer system. This report contains a subsequent technical assessment of the system for use in managed isolation facilities and potential population wide deployment. The contact tracer system comprises Bluetooth Low Energy beacon cards that transmit encrypted identifiers intended for recording social interactions between cardholders. Following a positive COVID-19 test result, a cardholder voluntarily allows their card data to be downloaded to an iPad app, then uploaded to a server for analysis. DTA has reviewed the technical aspects of the system and provided key recommendations for larger deployments of the system. We believe the current system is satisfactory for use in managed isolation facilities and short community trials. However, the level of data security is insufficient for nationwide deployment.

DTA Report 449

Defence Technology Agency
Private Bag 32901
Devonport
Auckland 0744
New Zealand

EXECUTIVE SUMMARY

At the request of the Ministry of Health (MoH), the Defence Technology Agency (DTA) carried out an initial assessment of the *Contact Harald contact tracer*, a Bluetooth card-based contact tracing system, to ascertain whether it was satisfactory for a seven day community field trial. MoH subsequently asked DTA what further development and testing would be needed for a population wide deployment of this technology.

The cards transmit Bluetooth Low Energy advertising packets containing an encrypted identifier allowing other cards to detect and record the interaction. If a peer card is detectable for more than two minutes continuously the contact is stored on the card for later retrieval. When needed, contact logs can be downloaded from the card using an iPad app and then uploaded to a server. User identifiers in the contact logs can be decrypted and matched to people registered with the system. Contact Harald (CH) is intended for use in the workplace, and is currently deployed at a number of sites in Australia.

We have reviewed the technical aspects of the CH system, including card hardware, cryptography, server components and the handling of personally identifiable information. The review was undertaken based on documentation provided by the vendor, an evaluation kit containing sample cards, and access to a CH web application set up for DTA. Where additional information was required the vendor was contacted via email and/or teleconference.

In our view the privacy and security of the CH system is satisfactory for a small-scale community trial, if all personally identifiable information is stored in a separate database. For use in managed isolation facilities we recommend waiting for an upcoming system update that will move the tracing keys to volatile memory on the cards.

To extend the system to national wide use it is recommended that:

- Unique AES-128 tracing keys be used for each card and stored in volatile memory,
- All personally identifiable information is held in a local database operated by the New Zealand government,
- Confirm that accepted certificate management protocols are observed,
- Card firmware, including key material, be loaded prior to registration by trusted agents in New Zealand,
- Over-the-air updates of firmware should be disabled following registration,
- A random variation to the rolling proximity identifier (RPI) change interval should be investigated. This may further mitigate risks of an attacker correlating RPIs across transitions,
- Visitor sign in/out functionality should be disabled in both card firmware and the iPad app,
- Cryptography and data protection be reviewed by an independent security expert,
- An option to view low confidence RSSI contacts should be added in the web application,

- Physical robustness testing is performed,
- The potential for an accelerometer to extend battery life is explored.

Any modifications to the system should continue to ensure that:

- There is no mechanism for a user to access their data for viewing or modification after registration,
- Uploads are one way with a simple acknowledgement of receipt. No inspection or modification of uploaded data should be possible, even to direct administrators of the central database.

Finally, the recommendations in this report are necessary but **not** sufficient to justify a national deployment of the CH contact tracing system. Important additional factors for consideration include user acceptance, distribution channels, the possible need for a mandate, and a cost-benefit analysis of card-based vs. smartphone-based digital contact tracing systems.

SYMBOLS AND ABBREVIATIONS

AES ..... Advanced Encryption Standard

BLE ..... Bluetooth Low Energy

CH ..... Contact Harald

CID ..... Corporate Identifier

DTA ..... Defence Technology Agency

ENF ..... Exposure Notification Framework

IV ..... Initialization Vector

LED ..... Light Emitting Diode

MAC ..... Machine Access Control

MIF ..... Managed Isolation Facility

MoH ..... Ministry of Health

PCB ..... Printed Circuit Board

RAM ..... Random Access Memory

RPI ..... Rolling Proximity Identifier

RSSI ..... Received Signal Strength Indicator

RTC ..... Real Time Clock

SoC ..... System on a Chip

TIN ..... Time Interval Number

UID ..... User Identifer

XOR ..... Exclusive Or

CONTENTS

1 INTRODUCTION **1**

2 SCOPE **1**

3 THE CONTACT HARALD SYSTEM **2**

4 CARD DESIGN **2**

4.1 Battery Life 3

4.2 Firmware 4

4.2.1 Rolling Proximity Identifier (RPI) generation 4

4.2.2 Contact log capacity 4

4.2.3 Firmware stability 4

4.3 Physical robustness 5

5 BLUETOOTH PROXIMITY ESTIMATION **5**

5.1 Range and received signal strength indication (RSSI) 5

5.2 Ground truth testing 5

5.2.1 Anechoic chamber measurements 6

5.2.2 Human body effects 6

5.3 Range estimation 6

5.3.1 Outdoor environments 6

5.3.2 Indoor environments 7

6 PRIVACY AND SECURITY **7**

6.1 Threat analysis 8

6.1.1 Targeting the card 8

6.1.2 Targeting the user 8

6.1.3 Targeting the tracing process 8

6.1.4 Targeting the system 8

6.2 Recommended security protocols 9

6.2.1 Secure cryptography 9

6.2.2 Separation of privileges 9

6.2.3 Limited Access 9

6.2.4 One-way data uploads 9

7 CONTACT HARALD CRYPTOGRAPHY AND DATA SECURITY **10**

7.1 Rolling proximity identifier 10

7.2 AES counter mode encryption 10

7.3 Decryption 10

7.4 Key handling 11

7.5 Discussion 11

8 SUMMARY & RECOMMENDATIONS **12**

9 TERMS OF USE **13**

REFERENCES **14**

1 INTRODUCTION

The New Zealand government has reacted to the COVID-19 pandemic with isolation and quarantine protocols at the border, and regionally based contact tracing teams to contain viral outbreaks.

Since April 2020 the government has maintained a watching brief on the rapidly evolving technologies for digital contact tracing. International efforts so far have mostly been aimed at smartphone platforms. These provide many advantages including CPU power and storage, wide deployment in developed countries, and network connectivity for data upload, download and software updates.

Several European countries have released digital contact tracing apps based on the Google/Apple exposure notification framework (ENF). These apps exchange Bluetooth Low Energy signals containing pseudo-random identifiers that, when decrypted, are uniquely linked to the phone. “Infected” identifiers are uploaded to a server and broadcast over the internet, the app then searches its log to see if any of these identifiers have been encountered. If so, the app can notify the user of a possible exposure and the date on which it took place. However, so far there is no evidence that apps based on the ENF have had a material impact on contact tracing efficacy [1].

Wearable Bluetooth devices have recently emerged as an alternative to smartphone apps for contact tracing. The big advantage of this approach is hardware homogeneity, which should lead to more consistent and accurate proximity estimation and greatly simplify the software development process. There are also significant disadvantages to a wearable system. These include comparatively limited CPU power, storage and battery life, and the difficulty of updating firmware. In addition, the logistics of population wide deployment would be challenging, and resourcing for ongoing technical support and replacement considerable.

At the request of Ministry of Health (MoH), the Defence Technology Agency (DTA) carried out an initial assessment of the *Contact Harald contact tracer*, a Bluetooth card-based contact tracing system, to ascertain whether it was satisfactory for a seven day community field trial. MoH also requested advice regarding further development and testing that would be needed for a population wide deployment of this technology. We have also considered usage in managed isolation facilities, as this application is of interest to other government departments.

This work was carried out for the Ministry of Health under OP PROTECT.

2 SCOPE

This report reviews the technical aspects of the Contact Harald (CH) system, including card hardware, cryptography, server components and the handling of personally identifiable information. We have considered the suitability of the CH system for a short community field trial, and for use by the general public.

Important note: The following issues are very important for a national deployment, but are **not** addressed in this report:

- User acceptance and uptake,
- Analysis of benefit to contact tracing compared to alternatives,
- Realistic cost estimates,
- Quality assurance for production,
- A distribution and registration mechanism,
- A replacement program for lost, defective or expired cards,
- Protocols for the event of a security compromise.

3 THE CONTACT HARALD SYSTEM

The Contact Harald contact tracer is a card-based digital contact tracing system that uses Bluetooth Low Energy signals to detect close proximity between people. It was designed for use in workplaces to assist contact tracing efforts for the COVID-19 pandemic. The Contact Harald (CH) system comprises:

- Bluetooth Low Energy proximity detection cards worn on lanyards,
- An iPad app used to register cards, download contact logs and upload them to a database,
- An online database for storing contact data and personal information,
- A web application providing tools for contact tracing.

The cards are issued and registered to individuals using an iPad app. Personal contact data can be entered as part of the registration process, which is then uploaded to a database hosted on a Microsoft Azure cloud platform. Personal information is stored only on the server, not on the cards. The cards are uniquely identified using two numbers: the corporate identifier (CID) and the user identifier (UID). Together, the CID and UID enable cards to be matched to individuals when contact data is uploaded.

The CID and UID are concatenated to form a single number which is encrypted and transmitted inside a Bluetooth Low Energy advertising signal. If a card is detectable for more than two minutes continuously by another card the interaction is stored for later retrieval. The cards classify contacts using the Bluetooth received signal strength indicator (RSSI) into three range bins: < 1 m, 1–2 m, 2–4 m, based on a RSSI vs. range calibration obtained from open air measurements.

When needed, the contact logs can be downloaded from the card using an iPad app over a Bluetooth connection, and the data is automatically uploaded to the server by HTTPS connection. On the server, the CIDs and UIDs in the contact records are decrypted and matched to the personal contact details uploaded during registration. The system is designed for workplace use and is currently deployed at a number of sites in Australia.

The DTA review of the CH system was undertaken based on documentation provided by the vendor, an evaluation kit containing sample cards, and access to a CH web application set up for DTA. Where additional information was required the vendor was contacted via email and/or teleconference.

4 CARD DESIGN

The main logic chip used to operate the CH card is a Nordic nRF52832, labelled *SoC* in Figure 1 below. This system on a chip (SoC) contains an ARM Cortex-M4 CPU and a Bluetooth Low Energy (BLE) 5.2 capable subsystem. The ARM Cortex-M4 is capable of floating point operations and can operate at low power with integrated sleep modes. This particular SoC variant contains 512kB of flash memory and 64kB of random access memory (RAM).

The card keeps track of real-world time and date with a real time clock (RTC). A 32.768 kHz crystal oscillator is included on the board (labelled *RTC Crystal* in Figure 1) and is standard for embedded systems that depend on real time. Keeping track of real time allows contact logs to be recorded with the exact date and time, up to clock drift. A 32 kHz crystal is also present on the board to act as a reference for the antenna (labelled *Antenna Crystal* in Figure 1).

The Bluetooth Low Energy subsystem is capable of a variable power output from −20 dBm to +4 dBm, with a sensitivity of −96 dBm and an Received Signal Strength Indicator (RSSI) resolution of 1 dB. The card's current firmware has been configured to output at 0 dBm. The PCB antenna is a standard meander line inverted-F pattern, designed for 2.4 GHz. This results in the card having a quasi-omnidirectional radiation pattern in the horizontal plane, with a single null of about 20 dB.

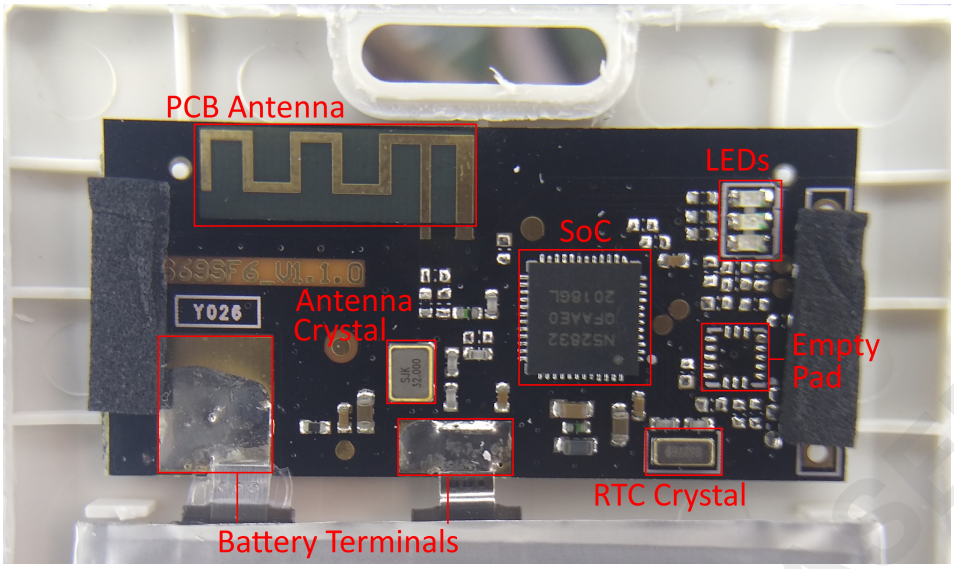

Figure 1: Magnified photo of the internal printed circuit board (PCB), highlighting the system on a chip (SoC), antenna, light emitting diodes (LEDs), real time clock (RTC) and antenna crystal oscillators, battery terminals and an empty pad where an accelerometer was not placed. Not pictured is the tactile metal dome switch located on the back of the board.

The card we have inspected features an empty pad where an accelerometer may be placed during production, but was not present in this particular card. The presence of an accelerometer would enable a card to enter a low power state when it is not being worn, extending the battery life beyond six months. For short trials or use in managed isolation facilities six months battery life is more than sufficient, and an accelerometer would not be required.

For a population-wide deployment, it would be prudent to investigate the benefits of having an accelerometer to extend battery life. These benefits include lower replacement costs, reduced waste and less user friction as it requires people to actively replace their cards less frequently.

4.1 Battery Life

The CH card contains an 800 mAh lithium polymer non-rechargeable battery with a claimed life expectancy of at least six months. The card does not have an off switch, is started at the factory and remains powered on. The Bluetooth contact tracing functionality runs indefinitely after initialisation, unless a vendor specific Bluetooth message is received that de-registers the card, which is part of the visitor sign out functionality. Light emitting diodes (LEDs) indicate whether the card has been registered, is connected and is in the on or off states. The red LED begins to flash intermittently when the battery voltage has dropped below a threshold level indicating imminent end-of-life.

The CH card design is based upon the Minew C7 card beacon and uses the same battery. Specifically, the battery is the Fanso CR224147, who provide indicative voltage and capacity discharge curves [2]. Minew have also provided a voltage discharge curve when drawing a constant 5 mA current from this battery. Contact Harald have carried out a battery life analysis on the Minew C7 card, albeit with an older firmware version [3]. However, we believe that the current hardware and firmware are similar enough that conclusions regarding battery life will remain the same.

The vendor energy usage analysis assumed that a card would be commissioned twice, with six log uploads and 400 total button presses to check status. Under these assumptions, these events used up less than 1% of the total battery life. The Bluetooth scanning and advertising used the remaining 99% of battery life, giving an estimated endurance of 180 days. The assumptions made

are reasonable, and detailed estimates were made based on real power draw measurements. The CH cards have also been used in small and medium scale deployments in Australia for the past few months. As a result, we believe the battery life claim of six months is reasonable.

4.2 Firmware

4.2.1 Rolling Proximity Identifier (RPI) generation

CH cards transmit anonymized identification numbers, known as rotating or rolling proximity identifiers (RPIs), that can be received and recorded by peer cards. Here, “rolling” means that the number is changed according to a schedule, which for CH is every 15 minutes. The RPI is obtained by concatenating the 2-byte corporate identifier (CID) and a 2-byte user identifier (UID), which together uniquely identify a card, and encrypting the result using AES-128. The RPI generation procedure is described in detail in Section 7.

The RPI is then placed in the payload of a Bluetooth Low Energy (BLE) advertising packet (Section 7) and transmitted every 248.75 ms at a power level of 0 dBm. The CH BLE messages can only be received while the card is in scanning mode. The scanning operation lasts for 0.8 seconds every 15 seconds.

We observed that the BLE transmissions from the cards rotate their pseudo-random identifier and machine access control (MAC) address every 15 minutes, as claimed. These numbers remain unique to each card as they are derived from the CID and UID. As the MAC address and random identifier change simultaneously, tracking the card over long periods of time by associating users to identifiers becomes extremely challenging.

4.2.2 Contact log capacity

Contacts are resolved into three generic classes based on minimum RSSI observed in a two-minute window. A Class 0 contact have must have a minimum RSSI of −50 dBm, Class 1 a minimum of −56 dBm, and Class 2 a minimum of −62 dBm (note that the RSSI saturates at −20 dBm when the cards are about 0.5 m apart). A contact record is written to flash memory containing the total counts in each of these classes for each RPI. Each increment of the count represents observation of a unique RPI for which the RSSI meets one of the above class criteria, within a two-minute time window. The count can accumulate up to maximum of 64, i.e. 128 minutes, or about two hours.

The variant of nRF52832 SoC used within the card we have inspected has 512kB of flash memory capacity and 64 kB of RAM. According to the documentation, contact log records contain a 2-byte UID, a 3-byte time interval number (TIN) and three 6-bit fields that store the counts in each contact class in a two-hour time window. The maximum contact log capacity of 20,480 records is based on an 80-bit contact record and consumes 200 kB of flash memory. The claimed contact log capacity is plausible, and leaves space for additional counters for contacts with lower RSSI. Upon reaching the log capacity limit, the card will continue to record new contacts by overwriting the oldest and least significant contact records first.

After 20 days, a contact record is marked as expired and can be overwritten by a new record. On the server, contact records older than 20 days are deleted.

4.2.3 Firmware stability

We have tested a small number of the cards starting with card registration using the iPad app, two days of interaction with other cards in a workplace environment, and then uploading of contact data to the server. The data collection involved realistic scenarios with test subjects wearing the cards on lanyards, and a saturation test where the cards were stacked together and left overnight. All cards remained responsive to button presses, and we were able to successfully upload data using the iPad app without encountering errors or entering unexpected states. Based on these tests, and the

existing deployments of the system overseas, we were confident the firmware was stable enough to proceed with a short community trial.

4.3 Physical robustness

The CH card physical design is based upon the Minew C7 card beacon, with a white ABS plastic housing that has been ultrasonically welded to provide a waterproof casing. The card is approximately the size of a credit card: 90 mm by 60 mm; and it is 4 mm thick.

DTA have *not* performed physical robustness testing on the specific card used in the CH system. However, we have performed several tests on a near-identical Bluetooth card and found it was robust to expected wear and tear: abrasion testing with multiple solvents found no potential issues with the near-identical card design, beyond making the etched numbers unreadable; a three-point bending test intended to simulate stresses when placed in a back pocket while sitting was conducted - this revealed it could undergo significant deformation and remain functional; immersion testing found the near-identical card to be waterproof after submersion at a depth of 1 m for 30 minutes, with no water found inside the weld line; crush testing found the near-identical card could sustain momentary force of up to 100 kN while remaining functional, resulting in temporary battery warming and a reduced card thickness. This represented an extreme crush test and despite still being functional, it is recommended that a card be replaced if it was subject to such extreme deformation.

The previous physical testing results on the near-identical card strongly suggest the current CH card is suitable for mass deployment, and is very unlikely to require significant numbers of replacement cards due to physical failure in typical usage. For surety we recommend these physical tests be performed on the final card design prior to a national deployment.

5 BLUETOOTH PROXIMITY ESTIMATION

5.1 Range and received signal strength indication (RSSI)

Digital contact tracing systems are intended to measure distance and total contact time between individuals. Bluetooth Low Energy based systems do this by inferring range from an estimate of the signal strength known as the received signal strength indication (RSSI). This quantity is used for automatic gain control in the receiver circuit and is usually provided as an 8-bit digital value to the device operating system.

Signal strength generally decreases with range, but the correlation between RSSI and distance is weak. A reliable calibration of RSSI to distance is not possible over the range of environments in which these devices would be used [4–6]. There are many sources of error: differences in RSSI calibration; antenna beam pattern variation; human body shadowing and absorption; body proximity effects on receiver gain; multipath fluctuations from reflecting objects; variation with height above ground.

The use of a card-based system eliminates calibration differences by using common hardware. When the card is worn externally on a lanyard some of the variation due to antenna beam pattern orientation is reduced compared to a smartphone-based system. However, there are still high levels of residual variability from multipath effects which are extremely difficult to mitigate.

5.2 Ground truth testing

In support of their product CH have released additional documentation to DTA concerning signal strength measurements on their Bluetooth Low Energy card. This includes antenna beam pattern testing in anechoic chamber and the open-air testing used for RSSI vs. range calibration.

5.2.1 Anechoic chamber measurements

CH have measured RSSI as a function of card rotation angle in an anechoic chamber to assess antenna beam pattern effects. The horizontal beam pattern was measured with cards mounted on tripods and oriented vertically; RSSI data was collected in 30° card rotation increments for five minutes at each angle. Assuming Bluetooth transmissions every 0.25 s this yields 1200 RSSI measurements at each angle. Only the peak value was reported at each orientation.

The results show a single null of about 23 dB and the remainder of the pattern is omnidirectional to within about 10 dB. RSSI dropped about 6 dB when the card-to-card separation increased from 1 m to 2 m, demonstrating the expected free space path loss in the chamber environment. Without compensation for the observed beam pattern null, there could be a factor of ten uncertainty in range estimates based on RSSI.

5.2.2 Human body effects

CH also conducted signal strength tests in an outdoor environment with the cards worn on lanyards. These showed that RSSI is attenuated by 10–15 dB when the card is in very close proximity to the body (about 1 mm separation), a level of attenuation likely to occur if the card is worn under clothing. With a 0.5 cm separation the attenuation was reduced to 5 dB, and to zero when the separation was increased to 1 cm. Note that these attenuation levels are for a single card, for two cards the attenuations would be additive. These findings underlie the recommendation that the cards be worn externally over clothing.

It is well established that close proximity of the human body degrades antenna performance. The degradation includes distortion of the radiation pattern, loss of efficiency, and detuning of the antenna input impedance. These effects are due to higher capacitive reactance and dielectric losses caused by close proximity to the human body [7]. Future generations of wearable Bluetooth devices may be able to sense body proximity and dynamically adjust their electrical properties to compensate for antenna detuning. However, with the present state of the technology there is no option but to keep the device separated from the body to maintain antenna efficiency.

The CH claim of a modulating effect on the beam pattern by the human body is plausible and consistent with findings by other researchers [8].

As expected, the relative orientation of the test subjects greatly affected the radio signal due to body shadowing. Signal strength is greatest when subjects are facing each other, and most attenuated when both are turned away. Face-to-face orientation may correlate with higher viral transmission risk from respiratory droplets, in which case this would be an advantage. However, there are still uncertainties surrounding transmission risk and orientation is not currently part of the close contact criteria.

5.3 Range estimation

5.3.1 Outdoor environments

In free space, i.e. a vacuum free from reflecting objects, when the distance between source and receiver increases by a factor of two the signal strength drops by 6 dB as long as the antenna radiation pattern is kept constant. However, in real world environments there are reflecting objects, including the ground itself, and the idealized 6 dB loss per doubling of distance may not be correct. In open air measurements the vendor noted the signal was noticeably affected by ground reflection beyond one metre of range. Between four and eight metres range the signal was about 6 dB higher than the free-space path loss model predicted, although as noted this could be due partly to other reflecting objects.

DTA has observed the similar effects in RSSI data collected previously on Raspberry Pi devices in a meeting room. The RSSI between four and eight metres range was higher than expected based on

free-space path loss, and sometimes higher than values recorded at shorter ranges. This makes it difficult to estimate contact distance on the basis of RSSI values except at very short ranges.

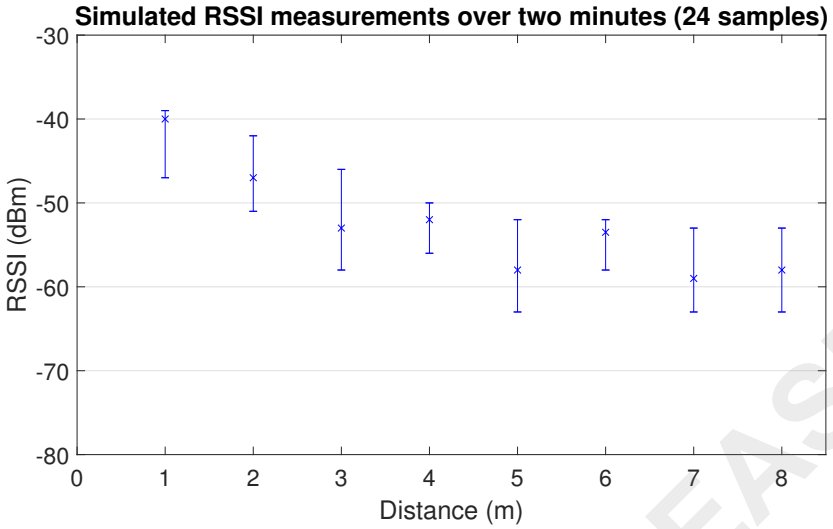

Figure 2: RSSI data captured using Raspberry Pi devices.

CH classifies contacts into three range bins, <1 m, 1–2 m, 2–4 m, based on RSSI data assuming a free-space path loss. This approach is based on the anechoic chamber test results and may lead to misclassification due to ground reflection outdoors.

5.3.2 Indoor environments

In indoor environments there are additional reflecting objects and the multipath effects become more significant and less predictable. The CH ground truth documentation mentions that some attempts were made at indoor RSSI measurements, but that these gave erratic results. This is not surprising as a high level of variability in Bluetooth signal strength has been noted by other researchers and has been evident in our own experimentation.

Viral transmission risk is elevated in poorly ventilated indoor spaces, and this is exactly the scenario in which digital contact tracing might be beneficial. Unfortunately, radio signal strength is highly variable indoors due to multipath effects, and proximity estimation based on RSSI alone is particularly challenging.

We expect CH card performance to be much less consistent in interior environments compared to outdoors. Before proceeding with a population wide deployment further testing in representative real-world situations could be investigated. Scenarios and places of interest include public transport (bus or train), a church, a meeting room, and a managed isolation facility or hotel. Approximate ground truth data could be provided by video surveillance or an indoor positioning system. These tests would help to better understand the reliability and performance of the system, and could be used to refine card sensitivity and contact classification algorithms. This testing should be undertaken by researchers with experience in holding medical trials and the results published.

6 PRIVACY AND SECURITY

Robust data security is critical to protecting privacy and encouraging user acceptance and uptake. These features have attracted the attention of security and cryptography researchers, and the Google/Apple exposure notification framework (ENF) has become a de-facto standard for smartphone-based digital contact tracing systems. Google and Apple have the resources to design robust security architectures and to fix vulnerabilities that emerge after deployment.

Wearable contact tracing devices have been strongly influenced by the ENF and incorporate some of its elements. However, they have unique vulnerabilities that require careful scrutiny as it may not be possible to fix problems identified after deployment.

6.1 Threat analysis

The intention of any contact tracing system is to enable identification of historical inter-personal contacts in the event of a positive SARS-CoV-2 test. By necessity, the maximum number of people must carry the devices continuously, building up a profile of personal contacts. It is assumed in our threat model that devices **do not** store location and have no capability to track. From lowest to highest risk, we now list a number of possible threats to a Bluetooth card-based contact tracing system.

6.1.1 Targeting the card

The card could be targeted for the contact data held. This threat model is the intent of an attacker to determine associates of a given user. To gain access to the data, the attacker would require either physical access to the card, a means to attack the data transfer mechanism, or maliciously modified firmware that permits unauthorized over-the-air download of data. Encrypted and anonymized data and communications shields users from the first two of these threats, while ensuring only trusted agents can load firmware on the device provides defence against the third.

6.1.2 Targeting the user

The attacker uses Bluetooth signals to track the card bearer. This can be defeated by transmitting randomized identifiers and varying these numbers over time, as is done in the ENF. Maintaining security over the key material used to generate random identifiers is critical. Compromise of a single card should not compromise the whole fleet.

6.1.3 Targeting the tracing process

An attacker could attempt to access data by subverting the upload mechanism. When contact data is transferred from a card to the online database for any reason this provides an opportunity to intercept the data. This could be achieved by subverting the human element in the tracing system – that is, coercing the staff who manage the upload. The card data should therefore be inaccessible to the staff involved, i.e. they should be able to initiate the upload process but have no access to the tracing data. This can be achieved by limiting storage of all keys to the cards and the centralized database, so that the device used for download from the cards is only relaying encrypted data.

Another threat to the tracing process is to flood the cards with fake Bluetooth tracing messages, by recording and replaying actual messages (known as a replay attack). This could have the effect of saturating the cards at a specific location, degrading the tracing capability. Mass gatherings in particular may attract this form of attack which is technically straightforward, difficult to defend against and could result in loss of public confidence in the system.

6.1.4 Targeting the system

A contact tracing system distributed across the population would be a highly attractive target for a state-level threat actor. Ability to tamper physically with the cards would depend on the lead time before manufacturing begins. If a state actor knew the form factor, PCB design and chip sets they could prepare modifications before the start of production. Offshore supply chain and manufacturing would greatly increase the risk of card tampering at both a hardware and firmware level. The only mitigation possible is to delay the loading of firmware until the devices arrive in New Zealand. In the distribution phase there is an additional risk that cards which have passed quality assurance testing may be substituted for look-alike devices, with alternative hardware and/or firmware, before reaching the intended users.

A state-level actor might target high-value individuals in the New Zealand government. Alternatively, the state-level actor may target the entire system as a means of influencing New Zealand through general surveillance or by sowing mistrust. A malicious modification of many or all cards would provide the greatest opportunity for such a threat actor; this would allow selective targeting of high-value individuals or general attacks as required. Attacking cards that are already in circulation would be substantially more difficult and require active intervention in the immediate vicinity of the target. This raises the costs and risks of the attack significantly, so although it is possible, the greatest risk is subversion at the production stage.

Such a state-level actor may choose instead to target the software components that enable and support the tracing device. This would allow collection of data useful to the state-level actor; for example, a full list of associates (all employees at a government agency) or contacts with specific individuals at specific times and locations. In the worst-case scenario, an attacker might attempt deliberate SARS-CoV-2 infection of an individual to ensure that a desired set of contact data is uploaded to the online database.

Contact tracing devices that transmit continuously cannot be used in classified environments. This restriction provides some mitigation against attacks targeting high-value individuals in government for data collection purposes or tracking. Much greater mitigation would be provided by a using locally manufactured cards for individuals identified as particularly high-risk targets.

6.2 Recommended security protocols

The following sections describe several data security protocols intended to mitigate the threats identified in Section 6.1. A Bluetooth card-based contact tracing system should implement all of these protocols to be suitable for nationwide use.

6.2.1 Secure cryptography

All encryption should be of current, proven cryptographic ciphers (for example, AES for symmetric encryption). Contact tracing devices should store all contact data in an encrypted format. Keys should be protected from tampering or leaking by storage in volatile memory. All data transfer (for example, uploading contact records from a device to a central system) should verify the parties with a cryptographic exchange. The data transfer itself should be over an encrypted connection.

6.2.2 Separation of privileges

Administrators of the tracing database should not be able to access personal data for any card user. In the event of a positive SARS-CoV-2 test, contact tracers should only be able to access contacts for the person in question. All contact tracing requests should be logged and audited. This will mitigate the risk of subverting the system by persuading a healthcare worker to extract data.

6.2.3 Limited Access

The contact tracing devices will need to be registered to a specific user. This should be a one-off process, with an immediate verification step. There should be no mechanism for a user to access their data for viewing or modification; the risk and impact of data leaks or tampering dictates against allowing any changes to user data once captured. If user details change, a new device should be issued to the user.

6.2.4 One-way data uploads

When cards are registered and contact logs are retrieved, the data must be uploaded into an online database. These uploads should always be one way with a simple acknowledgement of receipt. No inspection or modification of uploaded data should be possible, *even to direct administrators of the central database*. Accepting data transfer completely silently, i.e. with no feedback to the user, may provide marginally more security but creates a significant service risk that failed uploads are lost.

Therefore, on balance we recommend receipt acknowledgement, but no further interaction with the online system should be possible.

7 CONTACT HARALD CRYPTOGRAPHY AND DATA SECURITY

7.1 Rolling proximity identifier

The CH card system identifies cards with two numbers: a 2-byte corporate identifier (CID) and a 2-byte user identifier (UID). The 2-byte format limits each of the CID and UID identifiers to 2^{16} (65,536) possible values, but when used in combination this scheme allows a maximum of 2^{32} (4,294,967,295) uniquely identifiable cards.

The CID and UID are concatenated and encrypted using advanced encryption standard block cipher operating in counter mode (AES-CTR), with a 128-bit key and block size. The encrypted number is known as the rolling proximity identifier (RPI), and is transmitted as part of a Bluetooth Low Energy advertising packet. The AES-128 algorithm is a common symmetric encryption method, and is available in hardware on a co-processor within the nRF52832 SoC.

A weakness of symmetric encryption methods is the use of a single key for both encryption and decryption. If the key used on the remote device to encode the plain text is compromised the message can be decoded. Asymmetric encryption methods avoid this problem, but these are computationally demanding and may impact excessively on battery life.

7.2 AES counter mode encryption

The AES-CTR encryption operates by creating an initialization vector from a number used once (or “nonce”) and a counter which increments by a known amount, usually one, in each new block of plain text. The counter value and the nonce can be combined using any invertible operation, e.g. concatenation, addition or exclusive OR (XOR). In CH a nonce is formed for each block by the concatenation of six randomly generated bytes and the lower five bytes of the MAC address. The MAC address is changed every time a new RPI is generated.

The counter value for AES-CTR is taken from the time interval number (TIN). The TIN is the number of 15 minute intervals elapsed since the real time clock (RTC) on the card was started relative to a common start time across the card fleet. The TIN is concatenated with the CID and the nonce to form the initialization vector (IV), as illustrated below in Figure 3.

The IV is then encrypted with AES using a 128-bit key (the tracing key), and XORed with the plain text to form the cipher text. The plain text is the concatenation of the UID and the CID, which are stored on each card. The 16-byte cipher text output is the RPI, which is included in the payload of a BLE advertising packet and transmitted.

7.3 Decryption

The decryption process, which takes place in a cloud-hosted server, is the same as encryption process shown in Figure 2 but with the cipher text in place of the plain text in the diagram, and the original plain text being produced as output. The elements shaded grey in Figure 3 are needed for decryption and are transmitted along with the RPI in the Bluetooth advertising packet.

The TIN and CID are not transmitted by the card and must be known or reconstructed by the server for decryption. The CID is created as part of the server initialization process and is downloaded onto the cards as part of the registration and firmware loading process. The TIN can be calculated from the number of 15 minute intervals that have elapsed since the card fleet reference time (the *epoch*), which is set prior to the card being issued. The clocks on the cards may drift up to two seconds per day, which equates to a maximum of six minutes after six months. Thus, the server can estimate the TIN with enough accuracy to decrypt card data up to the maximum expected card lifetime.

The current cryptographic protocol for RPI generation is similar to the Google/Apple exposure notification framework. It is designed to protect the identification numbers (UID and CID) which can be matched to personally identifiable information. In addition, changing the RPI periodically prevents cards from being tracked.

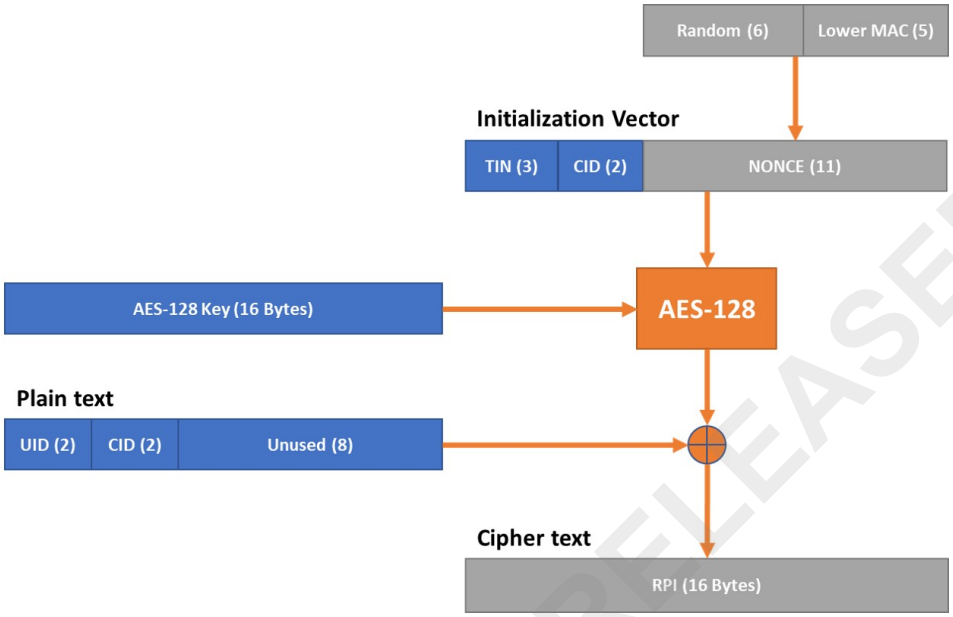

Figure 3: The cryptographic scheme used to generate rotating proximity identifiers (RPIs), which is based on AES-CTR cipher block chain. Here, the TIN provides the counter value. The parenthetic numbers are container sizes in bytes. Items with a gray background are transmitted in the BLE advertising payload; items with a blue background are held on the card but are not transmitted.

7.4 Key handling

The standard CH implementation uses a single AES-128 tracing key for an entire corporate card fleet (i.e. a fleet of cards with a single CID). The UID and CID is encrypted and transmitted in the RPI, and thus is vulnerable to the compromise of key material on a card. By accessing card memory an attacker could gain knowledge of the TIN, the CID and the tracing key. This information is sufficient to decrypt all RPIs in a corporate fleet, and enable those cards to be tracked.

The use of a single tracing key provides adequate security for a one short community trial as long as all personally identifiable information is held on a local database separate from the CH system.

A single tracing key would also be sufficient for use in a managed isolation facility (MIF) if the cards are only used inside the facility, and only anonymized data is held on the CH server. Tracking of cards provides no value to an attacker when they are used within a MIF, and in any case would be logistically very difficult to achieve.

The present user identification system is designed around workplace use and would need modification for a national roll out. The present 2-byte allocation for UID is limited to 65536 users; this could, for example, be aggregated with the CID to form a single 4-byte UID to cover the additional users.

7.5 Discussion

In the current CH firmware a single tracing key is used to generate RPIs across the entire corporate card fleet. This is an unacceptable security risk for nationwide use since the compromise of a single

card renders all data vulnerable to an attacker. Therefore, for a population-wide deployment the use of a unique tracing key for each card is essential. The use of unique tracing keys is technically feasible but it would mean some loss in log capacity on the cards.

We strongly recommend all key material be stored in volatile memory on the cards. In the current version of CH the tracing key is stored in Flash memory, but in a coming release the key will be securely written to RAM using ECDH cryptography [9]. We recommend waiting until this modification has been made before proceeding with any further deployments.

We strongly recommend that all personally identifiable information (e.g. name, address, phone number) be held in a local database operated by the New Zealand government. Contact tracing data can be downloaded in excel spreadsheet format from the CH website, and then uploaded manually to the database in order to resolve user identifiers to individuals. This ensures that personal information is never visible to the vendor.

Contact log data is uploaded from the iPad app to the server over HTTPS. This will provide sufficient security for a nationwide roll out, as long as good certificate management protocols are adhered to.

The ability to update the card firmware is a security weakness as it creates an opportunity for malicious firmware to be loaded. This could be used, for example, to silently upload contact data to an attacker's device or introduce a tracking capability into a card. The use of offshore manufacturing and supply chain also greatly increases the risk of tampering at both a hardware and firmware level. To mitigate these risks we recommend that card firmware, including key material, be loaded prior to registration by trusted agents in New Zealand. Over-the-air updates of firmware should then be disabled.

We recommend a random variation to the RPI change interval be investigated (it is presently fixed at 15 minutes) as this may further mitigate risks of an attacker correlating RPIs across transitions. Currently all CH cards are intended to change their RPI synchronously using the real time clock. However, as the clocks can drift by up to two seconds a day, the card fleet will steadily desynchronize and the tracking of individual cards by observing and timing transitions may become feasible.

Finally, the visitor sign in/out functionality provided in the iPad app is unnecessary for a nationwide roll out, and may introduce security vulnerabilities or otherwise be used maliciously. Therefore, we recommend this feature be disabled in both card firmware and the iPad app before use by the general public.

8 SUMMARY & RECOMMENDATIONS

At the request of the Ministry of Health (MoH), the Defence Technology Agency (DTA) carried out an initial assessment of the *Contact Harald contact tracer*, a Bluetooth card-based contact tracing system, to ascertain whether it was satisfactory for a seven day community field trial. MoH subsequently asked DTA what further development and testing would be needed for a population wide deployment of this technology.

The cards transmit Bluetooth Low Energy advertising packets containing an encrypted identifier allowing other cards to detect and record the interaction. If a peer card is detectable for more than two minutes continuously the contact is stored on the card for later retrieval. When needed, contact logs can be downloaded from the card using an iPad app and then uploaded to a server. User identifiers in the contact logs can be decrypted and matched to people registered with the system. Contact Harald (CH) is intended for use in the workplace, and is currently deployed at a number of sites in Australia.

We have reviewed the technical aspects of the CH system, including card hardware, cryptography, server components and the handling of personally identifiable information. The review was undertaken based on documentation provided by the vendor, an evaluation kit containing sample cards, and

access to a CH web application set up for DTA. Where additional information was required the vendor was contacted via email and/or teleconference.

In our view the privacy and security of the CH system is satisfactory for a small-scale community trial, if all personally identifiable information is stored in a separate database. For use in managed isolation facilities we recommend waiting for an upcoming system update that will move the tracing keys to volatile memory on the cards.

To extend the system to national wide use it is recommended that:

- Unique AES-128 tracing keys be used for each card and stored in volatile memory,
- All personally identifiable information is held in a local database operated by the New Zealand government,
- Confirm that accepted certificate management protocols are observed,
- Card firmware, including key material, be loaded prior to registration by trusted agents in New Zealand,
- Over-the-air updates of firmware should be disabled following registration,
- A random variation to the rolling proximity identifier (RPI) change interval should be investigated. This may further mitigate risks of an attacker correlating RPIs across transitions,
- Visitor sign in/out functionality should be disabled in both card firmware and the iPad app,
- Cryptography and data protection be reviewed by an independent security expert,
- An option to view low confidence RSSI contacts should be added in the web application,
- Physical robustness testing is performed,
- The potential for an accelerometer to extend battery life is explored.

Any modifications to the system should continue to ensure that:

- There is no mechanism for a user to access their data for viewing or modification after registration,
- Uploads are one way with a simple acknowledgement of receipt. No inspection or modification of uploaded data should be possible, even to direct administrators of the central database.

Finally, the recommendations in this report are necessary but **not** sufficient to justify a national deployment of the CH contact tracing system. Important additional factors for consideration include user acceptance, distribution channels, the possible need for a mandate, and a cost-benefit analysis of card-based vs. smartphone-based digital contact tracing systems.

9 TERMS OF USE

This report may **not** be used as supporting evidence for a nationwide deployment of any digital contact tracing technology without first consulting and obtaining permission from the New Zealand Defence Force.

This report may **not** be released to the general public in its current form as it contains commercially sensitive information.

References

[1] K. Chan, “Covid 19 coronavirus: As Europe faces second wave of virus, tracing apps lack impact,” *Associated Press*, September 2020. [Online]. Available: https://apnews.com/article/virus-outbreak-data-privacy-finland-smartphones-adoption-b05e442f8d1bc23252b872c289a2b063

[2] *Electrical characteristics CP224147 3.0V*, Wuhan Fanso Technology Co., Ltd, Wuhan, China.

[3] A. Merry and M. Denton, *Contact Harald Contact Tracer*, VT42 Pty. Ltd., Darlinghurst, Australia, November 2020.

[4] R. Faragher and R. Harle, “An analysis of the accuracy of bluetooth low energy for indoor positioning applications,” in *Proceedings of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2014)*, vol. 812, 2014, p. 201–210.

[5] T. Chowdhury, M. Rahman, S.-A. Parvez *et al.*, “A multi-step approach for RSSI-based distance estimation using smartphones,” in *Proc. 2015 International Conference on Networking Systems and Security (NSysS)*, 2015, pp. 1–5.

[6] J. Paek, J. Ko, and H. Shin, “A Measurement Study of BLE iBeacon and Geometric Adjustment Scheme for Indoor Location-Based Mobile Applications,” *Mobile Information Systems*, vol. 2016, 2016. [Online]. Available: https://doi.org/10.1155/2016/8367638

[7] N. H. Abd Rahman, Y. Yamada, and M. S. Amin Nordin, “Analysis on the effects of the human body on the performance of electro-textile antennas for wearable monitoring and tracking application,” *Materials*, vol. 12, no. 10, p. 1636, 2019.

[8] M. U. Rehman, Y. Gao, Z. Wang, J. Zhang, Y. Alfadhl, X. Chen, C. G. Parini, Z. Ying, and T. Bolin, “Investigation of on-body bluetooth transmission,” *IET Microwaves, Antennas Propagation*, vol. 4, no. 7, pp. 871–880, 2010.

[9] M. Denton, personal communication, November 2020.

DOCUMENT CONTROL SHEET

1. ORIGINATING ACTIVITY Defence Technology Agency, Auckland, New Zealand	2. RELEASE AUTHORISED BY:
3. REPORT NUMBER DTA Report 449	4. CONTROL NUMBER NR 1749
5. DATE November 2020	6. NUMBER OF COPIES 2
7. SECURITY CLASSIFICATION COMMERCIAL-IN-CONFIDENCE	8. RELEASE LIMITATIONS
9. TITLE Contact Harald Technical Assessment	
10. AUTHOR(S) Nathaniel de Lautour, Logan Small, Austin Chamberlain	11. AUTOMATIC DOWNGRADING
12. KEYWORDS EJC THESAURUS TERMS	NON-THESAURUS TERMS

13. ABSTRACT

At the request of the Ministry of Health, DTA previously carried out an initial assessment of the Contact Harald contact tracer system prior to a community trial. This report contains a subsequent technical assessment of the system for use in managed isolation facilities and potential population wide deployment. The contact tracer system comprises Bluetooth Low Energy beacon cards that transmit encrypted identifiers intended for recording social interactions between cardholders. Upon a positive COVID-19 test result, a cardholder voluntarily allows their card data to be downloaded to an iPad app, then uploaded to a server for analysis. DTA has reviewed the technical aspects of the system and provided key recommendations for larger deployments of the system. We believe the current system is satisfactory for use in managed isolation facilities and short community trials. However, the level of data security is not currently sufficient for nationwide deployment.

INITIAL DISTRIBUTION:

	No. of Copies
NEW ZEALAND	
Director DTA	2
Ministry of Health	1 pdf

New Zealand DEFENCE FORCE
Te Ope Kātua O Aotearoa

DEFENCE TECHNOLOGY AGENCY

Devonport Naval Base.
Private Bag 32901.
Devonport, Auckland
New Zealand 0744

T +64 (0)9 445 5902
F +64 (0)9 445 5890
www.dta.mil.nz