Reference: OPC-TDSD/TECH/21
Date: 27th April 2010

PCS Harvesting at Scale

██████████ (OPC-TDSD)
██████████ (OPC-TDSD)
████████ (OPC-CAP)
█████████ (OPC-TDSD)

Summary

This report explores the introduction of an automated approach to Ki harvesting in OPC-TDSD with the aim of increasing the volume of keys that can be collected. Methods are also explored to use data from the automated system to assess the effectiveness of current techniques and improve TDSD's knowledge of mobile network operations. Work was carried out between January and April 2010 in OPC-TDSD and OPC-CAP.

Distribution (all softcopies, via email)

OPC-TDSD (████████████████████████████
████████████████████)
OPC-HQ (████████)
OPC-CDP (██████████████)
OPC-MCR (██████████████)
ICTR (██████)
OPC-CAP (████████████████████)
OPD-GTAC (███████████████████)
NSA (████████████████)
TDB (█████████████)
OPD-SDH (████████)
TEA (██████████)

PCS Harvesting at Scale

Introducing Automation to Ki Harvesting Efforts in TDSD

████████████ OPC-TDSD

April 2010

Contributions from ████████████, ██████████ and ████████████

Summary

Individual Subscriber Authentication Keys, or Ki values, are required to decrypt GSM communications. They are stored both on the mobile user's SIM card and at a Home Location Register operated by the provider. TDSD has developed a methodology for intercepting these keys as they are transferred between various network operators and SIM card providers. This is now a core part of TDSD's business carried out by analysts in the team. This report explores the introduction of an automated technique with the aim of increasing the volume of keys that can be harvested. Methods are also explored to use data from the automated system to assess the effectiveness of current techniques and improve TDSD's knowledge of mobile network operations.

Table of Contents

1 Introduction

TDSD's key harvesting methodology centres around collecting Ki values in transit between mobile network operators and SIM card personalisation centres. Provisioning information is often sent between these organisations by email or FTP with simple encryption methods that can be broken out by OPC-CAP, or occasionally with no encryption at all[1]. With targeting in place, a large volume of IMSI and associated Ki values can be harvested from UDAQ – GCHQ's corporate C2C data repository.

With known individuals and operators targeted, items of interest can often be returned from bulk C2C data using a simple search for the terms 'Ki' and 'IMSI' in close proximity. Results will often contain a large number of unrelated items, however an analyst with good knowledge of the operators involved can perform this trawl regularly and spot the transfer of large batches of Kis.

Work has already been carried out to automate this sifting of bulk data; reference 1 describes techniques successfully trialled so far. This work builds upon these techniques introducing a system to bulk query UDAQ itself, perform the sifting operation on data to identify items of interest, packaging these up in a form that can usefully be interpreted by researchers in OPC-CAP. Summary information is also produced for the use of analysts in TDSD.

The main desired outcomes from this work are to:

- Improve TDSD's effectiveness at finding Kis in C2C content repositories. By automating the approach it should be possible to perform a more thorough search than TDSD has had the manpower to do at present. This is likely to bring higher volumes of Kis and IMSIs to light in addition to spotting interesting items that would not have come to the attention of analysts previously.
- Improve TDSD's target knowledge. A more complete picture of IMSI/Ki data in C2C repositories will allow TDSD to view the effectiveness of current targeting, spot trends as target behaviour changes and also spot any obvious gaps in coverage – for example providers for whom this type of harvesting is ineffective.
- Develop and enhance TDSD's harvesting methodology. This methodology is based around knowledge of how network operators, SIM suppliers and hardware providers co-operate to share cryptographic data. By looking at the types of organisations associated with traffic seen in the wild we can test assumptions about communication patterns we expect to take place, improving our knowledge of relationships between these companies.

---

[1] It should also be noted that TDSD have observed the use of strong encryption products being used (eg. PGP products). These have become increasingly common and used as standard for large SIM suppliers/personalisation centres to exchange SIM output and input data with mobile network operators.

Additionally it is likely that similar opportunities exist to introduce this type of automation to other analyst tasks. This work will help develop requirements for such services and bring more automation opportunities to light.

2 Approach

Figure 1 shows a high level overview of TDSD's current manual harvesting methodology.
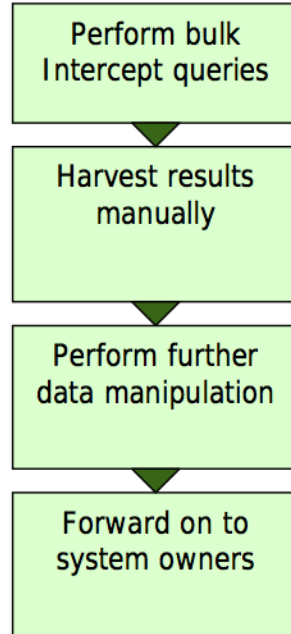
```
┌─────────────────────┐
│   Perform bulk      │
│  Intercept queries  │
└─────────────────────┘
          │
          ▼
┌─────────────────────┐
│   Harvest results   │
│      manually       │
└─────────────────────┘
          │
          ▼
┌─────────────────────┐
│  Perform further    │
│  data manipulation  │
└─────────────────────┘
          │
          ▼
┌─────────────────────┐
│   Forward on to     │
│   system owners     │
└─────────────────────┘
```

**Figure 1 - Manual Ki
Harvesting Process**

Analysts in the team regularly perform queries on targeted C2C intercept using UDAQ. A number of queries exist designed to return results likely to contain IMSI and Ki values. Queries often return results with a high noise threshold – of several thousand results perhaps a few hundred will contain items of value. The next stage is to trawl these results for items of value. If a list of IMSI and Ki values is found this can be copied from the tool and sent on to OPC-CAP for further processing. In the best case lists of several hundred thousand Kis associated with IMSI values can be found. However, a large number of messages each contain only a few associated Ki values. The responsibility of converting IMSI/Ki lists into a storable form lies with OPC-CAP; TDSD analysts can only spend limited time manipulating the layout of data before forwarding.

2.1 Automated Technique

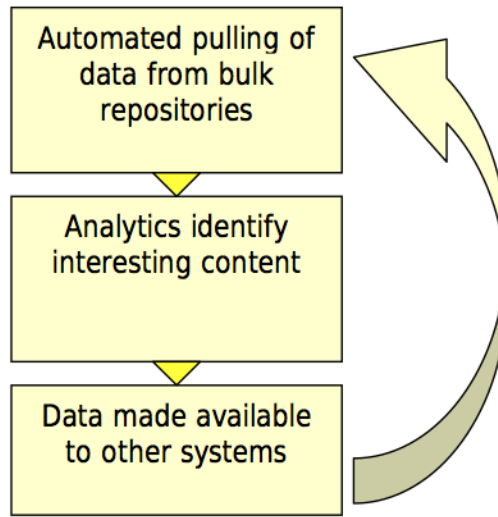Figure 2 describes 3 stages of the automated method developed.

Figure 2 - Automated Ki Harvesting Process

Details of each stage is provided below:

2.1.1 Bulk Data Retrieval

ICTR provide a bulk data download capability using the research server LLANDARCYPARK. This was used to automate the querying of C2C content in UDAQ. Given a standard SQL query wrapped in an XML form this will return a package containing all matching C2C intercept.

A base query, a proximity search for the strings 'IMSI' and 'Ki', was used for this experiment. This can be seen in Appendix 1. Date fields are marked with placeholders so these can be automatically filled out using regular expressions at run time.

Results are returned as a compressed file containing a CCDF[2] mesh. A routine was then written to unpack this mesh, allowing results to be treated from then on as a set of plain text files.

Scripts were developed to perform all steps of the operation automatically, retrieving packaged data to be interpreted by the user (reference 6). This operates as follows:

The script *./runRemoteQuery.sh* is used to launch the process. This:

- Requests a date range to query
- Rewrites the query XML file with required dates

---

[2] Cryptologic Common Data Format. Details are described in reference 4.

- Transfers all required files onto the LLANDARCYPARK server, including *pulludaq.sh*

pulludaq.sh is then executed on LLANDARCYPARK. This:

- Executes the bulk IIB query (can take 5-10 mins)
- Retrieves query results as compressed CCDF files
- Unpacks the CCDF contents into a directory as plain text for processing.

The next stage is to identify content of interest in the processed files.

2.1.2 Identifying Content

Once plain text is retrieved from IIB this is parsed to identify items containing IMSI and Ki values. A previously proven rule based approach is used to identify content of interest.

The routine scrapes the plain text identifying lines containing IMSI and Ki values, which may appear in intercept in any conceivable format. The technique also attempts to identify header information describing the contents, as well as associating results with a UDAQ identifier that can be later researched. Further technical discussion on this technique is available in reference 1, *TDSD Technical Note 11: What Makes a Good PCS Key Harvester?*.

A final stage generates statistics and additional information linked to the results, developed in consultation with TDSD analysts. This includes:

- A list of unique UDAQ item identifiers resulting in valid Ki / IMSI data. This allows analysts to conduct further research into these traffic sources. These are ranked according to the number of sections of IMSI data seen in each UDAQ item.
- A list of network and country codes identified. These are derived from the first 6 characters of an IMSI and used to provide an overview of countries and networks identified.
- A list of associated email addresses. This is generated by scraping all email addresses from results found to contain valid Ki data. These are then ranked by the number of occurrences of each address.

Care should be taken when interpreting ranking positions. In the case of email addresses a higher score does not necessarily indicate association with more Kis, however they can provide an indication of how active an address is.

An example set of statistics produced is shown in Appendix 2.

2.1.3 Processing / storing

Output files generated by the previous step typically take the form shown in Appendix 3 – section markers separate the UDAQ item reference, potential header information and IMSI/Ki content. This format was developed alongside OPC-CAP. It should be noted that although the content will contain IMSI and Ki data it could take any conceivable form – it is presented as found in raw intercept. It is the task of OPC-CAP to interpret any additional data in any recognised header section, decoding as necessary. Ki values may still be encrypted at this stage.

OPC-CAP have developed and successfully trialled techniques to speed up the task of importing these scripts, indentifying expected column header names and mapping these to data fields, and even automating the final decryption stage.

Once properly interpreted these Ki values can be stored, encrypted or clear, in relevant databases and shared with partners as necessary.

2.2 Possible improvements

A number of improvements have been identified for the above technique. These are described below:

- Improved access rights for bulk data retrieval
  Access to ICTR's bulk access capability runs on research prototype hardware and is supported only on a best endeavours basis. Making use of a processing user to obtain data, the maximum classification that can be returned is TOP SECRET STRAP2 UK Eyes Only. This means that some data currently retrieved using the manual method, such as password-recovered items, is not available to the automated system. An improved system would allow bulk access to more intercept data.
- Processing performance
  Performance of queries on LLANDARCYPARK is comparable to that of UDAQ, however when large numbers of items are retrieved the generation of statistics can take some time (sometimes hours for large sets). Some simple code optimisations could significantly improve this performance.
- Improvements to summary information scores and ranking
  The value of using ranks to assess the usefulness of an email or UDAQ item identified is limited, since the score used relates to the number of sections of Ki data in a given file. This means where a very large number of IMSIs are identified, but they appear in a single block, a low score is awarded. A value relating to the number of IMSI items would be more useful to identify the most important results.

3   Running Trials

The automated harvesting technique was used to extract IMSI and Ki values from bulk data over a 3-month period. This was performed over six 2-week intervals. The resulting number of IMSIs, Kis and associated statistics produced are shown in Table 1.

Query Start	Query End	Unique email addresses identified	UDAQ items	# unique country codes	# IMSIs paired with Ki
30-Dec-09	14-Jan-10	130	18	10	7,802
13-Jan-10	28-Jan-10	4	39	11	8,960
27-Jan-10	11-Feb-10	18	42	12	1,809
10-Feb-10	25-Feb-10	4	50	18	2,348
24-Feb-10	11-Mar-10	6	3	3	84,937
10-Mar-10	25-Mar-10	9	8	16	473

Table 1 - Details of Trial Queries

The technique can be seen to identify a steady stream of IMSI and Ki data over a period of time. UDAQ item identifiers which contain the IMSI and Ki data can additionally be provided to analysts allowing sources to be further investigated.

These results are further analysed in the following section:

3.1 Activity of Networks

Unique country codes identified in each of the time periods were correlated to produce the chart shown in Figure 3. Only networks with significant results are shown – raw data can be seen in Appendix 4.
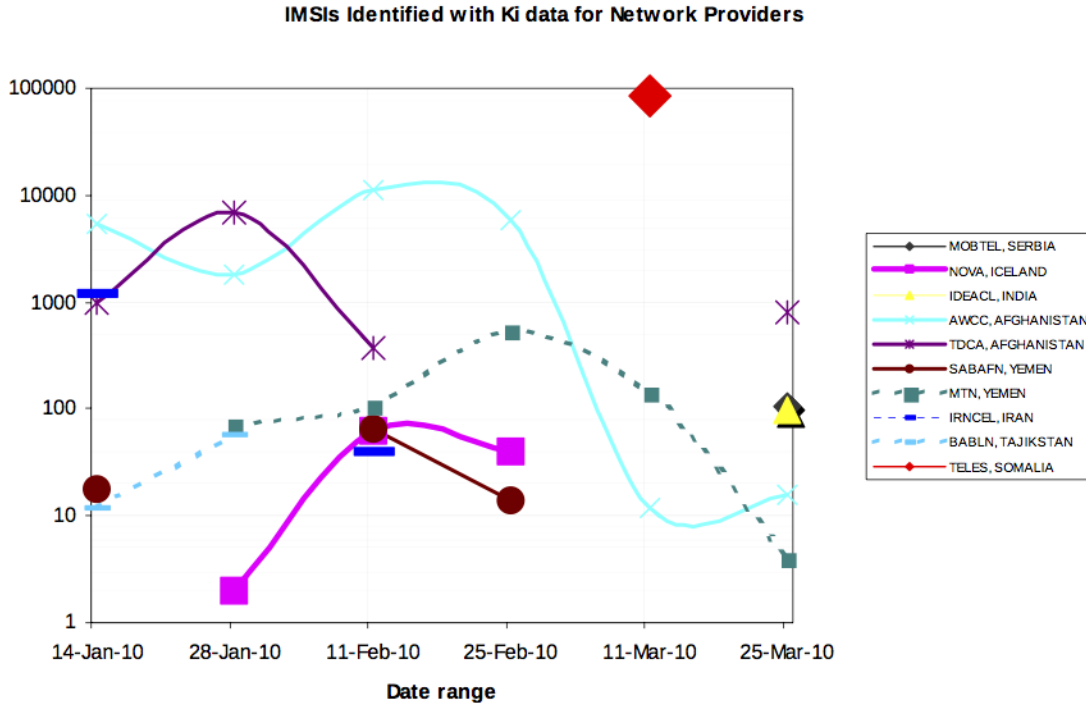
IMSIs Identified with Ki data for Network Providers

Figure 3 - IMSIs identified with Ki data for Network Providers

This shows the number of IMSIs found with Ki data in each period for the providers shown, portraying a steady rate of activity from several networks of interest. New Ki and IMSI pairs are regularly seen for AWCC, TDCA and MTN.

A large batch of Somali Kis was recovered in mid-March using this automated process. Somali providers are not on GCHQ's list of interest, hence it is likely this item would have been missed by manual collection, however this was usefully shared with NSA. A number of other unexpected providers were brought to light including Babilon-Mobile in Tajikistan and Icelandic provider Nova 3G.

This has demonstrated that an automated Ki recovery method can effectively identify IMSI and Ki pairs from bulk C2C sources for key targets, with the added benefit of identifying content that would not normally come to analyst attention. The chart presented provides an overview of networks accessible in C2C repositories.

3.2 Target Discovery

An experiment was carried out to make use of results from this technique for target discovery.

Statistics produced alongside IMSI/Ki results include email addresses appearing in communications alongside this content. These email addresses are scored by the number of times they are seen. It was proposed that analysis of these addresses should bring to light common communication patterns between operators, as well as help identify actors most involved in the sharing of Ki data.

UDAQ C2C collection is targeted; hence any traffic found will originate from an identifier in GCHQ's corporate systems. However it was surmised that additional useful contact addresses could be found associated with traffic.

All email addresses associated with traffic in each of the 6 periods were compiled together. This resulted in a list of 154 unique email addresses, each associated with a score. From this it was possible to identify a number of candidate targets for further research that scored highly:

- ███████████@gmail.com – target's email handle suggests an Ericsson employee using a webmail account
- ██████@huawei.com – this was the highest scoring overall address, a previously unknown target on the Huawei network.
- ██████@gmail.com – highest scoring webmail address, indicating lots of activity associated with IMSIs and Kis, was a previously unknown target.
- mtn_ics.mc – a number of users associated with this previously unknown domain. JEDI research shows international gateway for South African provider MTN
- ███████@msn.com – an MSN address found to be associated with IMSIs and Kis

This has demonstrated a number of opportunities to apply this harvesting technique to target discovery efforts.

3.3 Measuring Targeting Effectiveness

An experiment was carried out to discover the effectiveness of TDSD's current targeting methods.

Email addresses identified in the previous section were converted into a list of domains, again scored by the number of associations with IMSI/Ki data. The complete list can be seen in Appendix 5.

It was then possible to group domains into 5 categories:

- **Hardware Companies** – Organisations such as Huawei, Ericsson, who manufacture PCS hardware.
- **Network Operators** – Operators of mobile networks such as MTN Irancell, Belgacom.
- **SIM Suppliers** – SIM Suppliers or SIM Personalisation centres, for example Bluefish.
- **Mail Providers** – Users of general email providers (Gmail, Yahoo etc). These may be in use by employees of any of the above.

- **Other / Unknown**

Most of TDSD's targeting effort is focussed on SIM suppliers and network operators, hence it was expected that most associated addresses would fall into these categories.

Category	Associations
Hardware Companies	743
Mail Providers	298
Sim Suppliers	38
Network Operators	603
Other / Unknown	37

Table 2 - Types of organisations associated with IMSI/Ki traffic

Table 2 shows how often each type of organisation was associated with Ki traffic. Contrary to expectation the vast majority of addresses seen belonged either to network operators or hardware companies.

This could indicate increased use of strong encryption products amongst SIM suppliers, leaving only the other groups open to this method of exploitation. TDSD may wish to ensure that targeting for SIM suppliers is up to date, as well as investigating the possibility of targeting hardware companies and network operators to improve results.

3.4 Comparison with present efforts

3.4.1 Manually collected Kis

A manual trawl of UDAQ data was performed against AWCC for the period between 28th March and 10th April 2010. This was compared directly against results from an automated run over the same period, not targeted against any particular provider.

In the manual trawl 14 UDAQ items were identified, all containing 1 or more IMSI/Ki pair for AWCC. The automated run found 12 UDAQ items, 3 of which had been identified in the manual trawl. A summary of results is shown in Table 3:

Result #	Date	Found in search		Details	Comments
		Manual	Automated		
1	29-Mar-10	●		AWCC	No occurrence of "IMSI"
2	2-Apr-10	●		AWCC	No occurrence of "IMSI", multi-line
3	3-Apr-10		●	Huawei, HLR inconsistency, 83 lines	
4	6-Apr-10	●		AWCC	No occurrence of "IMSI", multi-line
5	5-Apr-10	●		AWCC, only pin/puk info	
6	5-Apr-10		●	AWCC new activation	
7	5-Apr-10	●	●	AWCC	
8	5-Apr-10		●	AWCC new activation	
9	5-Apr-10		●	AWCC new activation	
10	8-Apr-10	●	●	AWCC	
11	7-Apr-10	●		AWCC	No occurrence of IMSI, multi-line
12	6-Apr-10		●	Roshan new sim vendor query	
13	6-Apr-10	●	●	AWCC	
14	7-Apr-10	●		AWCC	No occurrence of IMSI
15	7-Apr-10	●		AWCC	No occurrence of IMSI
16	7-Apr-10	●		AWCC	No occurrence of IMSI, multi-line
17	8-Apr-10	●		AWCC	No occurrence of IMSI, multi-line
18	8-Apr-10	●		AWCC	No occurrence of IMSI, multi-line
19	8-Apr-10	●		AWCC	No occurrence of IMSI, multi-line
20	8-Apr-10		●	AWCC sim replacement	
21	8-Apr-10		●	AWCC sim replacement	
22	7-Apr-10		●	AWCC new activation	
23	3-Apr-10		●	HLR update containing 83 items	Same as item 3

Table 3 - Results of Ki / IMSI trawl

The manual search resulted in a total of 27 IMSI values for AWCC. The automated search resulted in 320 values, 26 of which were from the AWCC network. The automated methods also identified 10 unique IMSIs from Roshan and 83 from MTN Yemen (results 3 and 23).

It can be seen that the automated search missed the majority of manually recovered items. Reasons for this are noted in the comments column: in all cases the string IMSI did not appear in the results file, hence these items were not returned in the initial bulk query. The majority of these items also had IMSI and Ki data split across multiple lines, meaning they would not have been identified by the detection techniques employed in this work in any case. Both techniques found comparable quantities of IMSIs for AWCC with the result sets being mostly complimentary.

This has demonstrated that although the automated method is able to return a representative set of items from bulk data, and often-larger volumes of Kis, it tended to miss items found manually. More work is required both at the initial bulk query stage as well as with processing and detection techniques.

3.4.2 Overall harvesting efforts

TDSD and OPC-CAP collect overall stats for Kis harvested from networks of interest (reference 5). Overall rates of Kis received over a 3-month period, January – March 2010, were compared against those from the automated technique. Figure 4 shows this comparison for a range of networks.
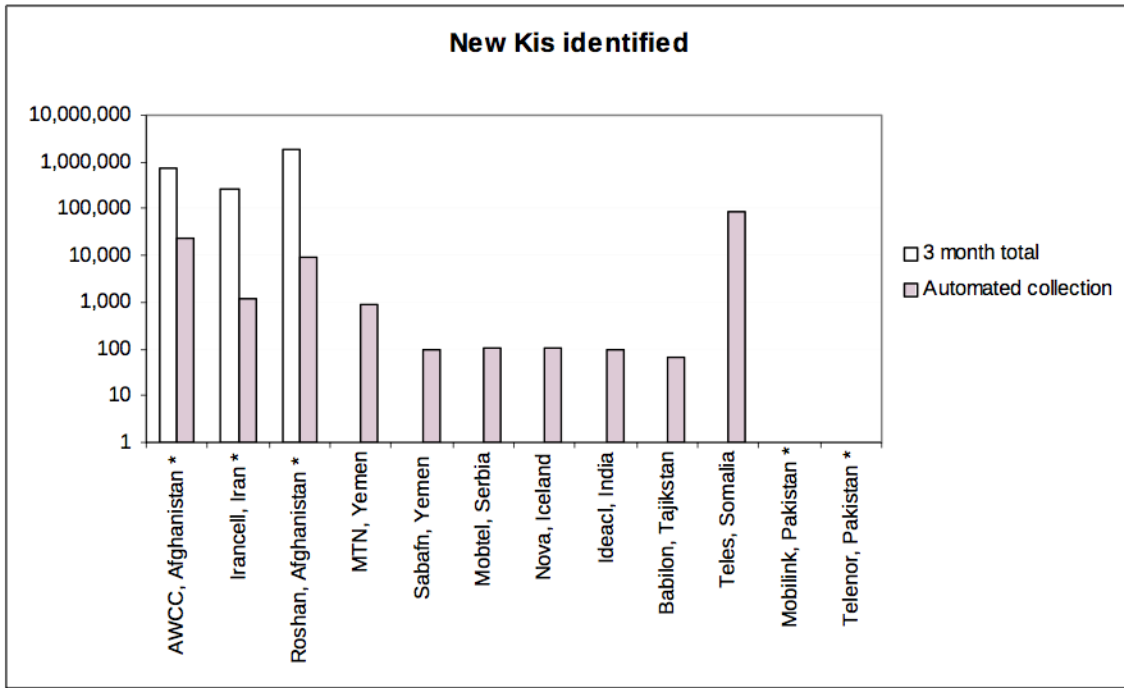
New Kis identified

**Figure 4 - comparing data from the trial to historical data
(priority targets marked *)**

The overall data set contains values gained from a range of sources including Ki generation techniques and information sharing with partners.

It can be seen that for the first three providers; AWCC, Irancell and Roshan; the number of keys collected by automated harvesting is comparatively small. Many of the larger batches of Kis received in this period were provided by partners on request, and it is difficult to estimate the real time period they were collected over. Additionally, the value of a small number of Kis should not be underestimated as these can often be used as seeds to generate much larger batches.

It is clear that the automated technique is able to identify Kis for a greater range of networks, successfully identifying a large batch of Kis for a particular Somali provider.

This comparison did bring to light a number of networks where the C2C harvesting method is not bringing results, notably the Pakistani networks Mobilink and Telenor for whom we do have a store of Kis. There could be a number of explanations: it is possible that these

networks now use more secure methods to transfer Kis, or targeting for those networks might be ineffective.

In summary, the automated technique is unlikely to bring in very large batches of Ki data of the size produced with Ki generation schemes or received from partner repositories. However it can bring in a steady stream of data over a period of time. These smaller volumes can fill gaps where no other data is available, and also provide essential seed points from which Ki generation can be applied.

4 Conclusions

This work has demonstrated that an automated method of Ki recovery, once in place, can deliver significant results with little manual effort compared to current harvesting methods. In addition to Ki harvesting a number of further applications have been demonstrated: the monitoring of mobile network activity, where views have been provided over a 3-month period; discovery of new target identifiers associated with detected traffic; and methods of measuring the effectiveness of current techniques.

A picture of types of organisations associated with Ki traffic has been constructed providing a new view of mobile network operations to TDSD.

It has also been shown that although the automated method is able to return a representative set of items from bulk data, it often fails to detect all items that would be found manually. More work is required at the initial bulk query stage and also with detection techniques to ensure accurate and full coverage of Ki data.

Whilst problems have been identified such as limits on coverage due to access restrictions, this work makes a strong case that such harvesting efforts will continue to deliver results in TDSD and areas such as the CP SD team.

It is the author's view that increased levels of corporate support for such bulk data processing activities would allow TDSD, as well as many other business areas, to benefit from more applications of these techniques.

4.1 Future Work

A number of items of follow-up work have been identified:

- **Improving initial query effectiveness**
  It has been shown that the initial base 'proximity' query is not effective enough to return all results currently found using manual harvesting. Work should be carried out to identify more effective queries to process data on. An alternative option is to run the technique repeatedly against a number of result sets.
- **Improved detection techniques**
  Detection techniques are unable to identify Ki and IMSI data where the fields of interest appear on separate lines (see section 3.4.2). An improved technique would ensure these results are also detected and included.
- **Improved summary information**
  Summary information currently consists of a list of email addresses, UDAQ item identifiers and network codes associated with simple scores. Analysts would like to be able to find the UDAQ item associated with a particular IMSI or email address more easily. An improved scoring system would also help analysts more accurately

prioritise items found. Additionally, the accuracy of results could be improved by detecting only IMSIs with valid country and network codes.

- **Bulk access limitations**

  The maximum classification that can be returned from LLANDARCYPARK is TOP SECRET STRAP2 UK Eyes Only. This limits access to some data likely to contain IMSI and Ki values, such as password-recovered items. An improved system would allow bulk access to the full range of data.

- **Adapting technique to be used for other key types**

  This technique currently identifies only IMSI and Ki values. In time it should be extended to also support efforts against OTA keys, UMTS and more.

- **Data mining opportunities**

  Opportunities exist to mine bulk data produced during this process, potentially detecting further items of interest and developing knowledge of targets involved. Proposed ideas include detecting requests for batches of data by identifying messages containing maximum and minimum SIM values.

- **Corporate support for bulk C2C processing**

  Access to ICTR's bulk access capability is restricted to a small number of users, however a number of business units have expressed an interest. This work should continue to be used to develop requirements for a corporate solution allowing more business units to benefit from these types of techniques.

References

1. TDSD Technical Note 11: What Makes a Good PCS Key Harvester?
   ████████████, *TDSD, 12th January 2010, available on request from TDSD*
2. DRAFT METHODOLOGY for investigating SIM card supplier relationships with Target Mobile phone operators
   ████████████, *TDSD, 2010, available from* ████
3. ICTR Bulk IIB Download Capability
   ████████████████████████
4. Cryptologic Common Data Model FAQ
   ████████████████
5. TDSD Non EPR Statistics
   ████████████████████
   ████████████████

6. PCS Harvesting Scripts are stored under ClearCase and can be accessed and run from the following location:
   ████████████████

Appendix

1   Example IMSI/Ki proximity query used by LLANDARCY PARK

```
<?xml version="1.0" encoding="UTF-8"?>
<cib:query xmlns:cib="urn:gchq:cib" countOnly="false" exportQuery="true" maxResultsCount="10000">
  <cib:query-text>
    SELECT Item_ID FROM CIB.CIB WHERE
      (
        Date_Of_Intercept &lt;= {d &apos;    END_DATE    &apos;} AND
        Date_Of_Intercept &gt;= {d &apos;    START_DATE    &apos;} AND
        Content = &apos;( imsi AND Ki WITHIN 60 )&apos;
      ) AND
      Item_Type IN (&apos;IIB_Intercept&apos;,&apos;Strong_Net&apos;,&apos;          C2C&apos;,&apos;          &apos;)
  </cib:query-text>
  <cib:queryMetadata>
    <cib:property name="interceptType">All intercept</cib:property>
    <cib:property name="username">someusr</cib:property>
    <cib:property name="classification">TOP SECRET STRAP1</cib:property>
    <cib:property name="mirandaNumber">          </cib:property>
    <cib:property name="jicPurpose">NS</cib:property>
    <cib:property name="hraJustification">Mobile Theme CRYPT RESEARCH INTO SIM CARD SUPPLY GSM OPERATORS OPI-MENA AND OPI-AP</cib:property>
  </cib:queryMetadata>
</cib:query>
```

2   Example stats.txt produced by script

```
IMSI results:

Emails:
9 items
2          @idea.adityabirla.com
4          @bluefish.com
4          @idea.adityabirla.com
4          @grameenphone.com
4          @grameenphone.com
6          @bluefish.com
10         @bluefish.com
```

```
12              ███████@bluefish.com
18              ███████@grameenphone.com

UDAQ Item Identifiers used:
8 items
1       ████████████████████████
1
2
3
6
7
7
7

Country Codes:
16 items
4       421020
8       340041
8       612060
9       404040
10      410011
12      220018
16      412012
18      404120
26      648032
40      452048
40      510890
42      470010
56      220020
99      404041
108     220012
809     412200

IMSIs:
473 items
1       █████████████
1
2
2
2
...
```

3   Example PCS Ki output file

```
***** NEW FILE *****
***** SOURCE *****
█████████

***** HEADER *****
Action;OrderId;ServiceId;ObjectId;Priority;IMSI;MSISDN;Opcode(Short);ICCID;Ki;PIN;PIN2;PUK;PUK2;reserved(Boolean)

***** CONTENT *****
```

███████████████████████████████████████

`...`
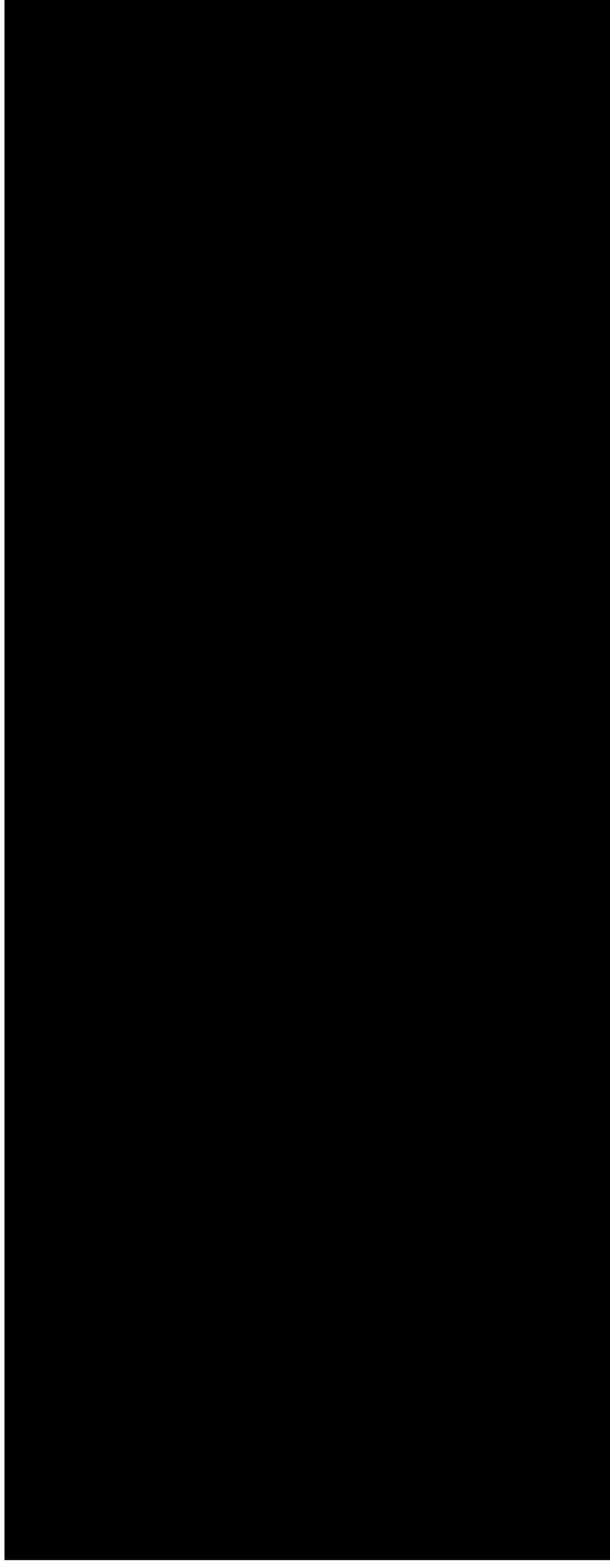
4   IMSI results broken down by network code

Network code	Location	Period 1	Period 2	Period 3	Period 4	Period 5	Period 6
000000	INVALID			4			
008821	INVALID		6	6			
012409	INVALID			2	2		
111111	INVALID				4		
123454	INVALID				38		
201002	INVALID		4				
210231	INVALID	1					
220012	MOBTEL, SERBIA						108
222013	ITLCBL, ITALY		2	2			
220018	ITLCBL, ITALY						12
220020	PROMNT, MONTENEGRO						56
274113	NOVA, ICELAND		2	62	40		
340041	, MARTINIQUE; FRENCH GUIANA; DOMINICA; GUADELOUPE AND SAINT MARTIN						8
345126	INVALID				22		
345612	INVALID				6		
357646	INVALID	31					
357891	INVALID	115					
358453	, SAINT LUCIA	27					
404040	IDEACL, INDIA						9
404041	IDEACL, INDIA						99
404120	IDEAMB, INDIA						18
404602	VDFNDG, INDIA				30		
410011	PMCL, PAKISTAN						10
412012	AWCC, AFGHANISTAN	5364	1834	11403	5927	12	16
412200	TDCA, AFGHANISTAN	986	6973	376			809
421010	SABAFN, YEMEN	18		64	14		
421020	MTN, YEMEN		72	108	542	140	4
432350	IRNCEL, IRAN	1188		40			
432352	IRNCEL, IRAN	60					
435670	INVALID				2		
436046	BABLN, TAJIKSTAN	12	57				
438320	INVALID, TURKMENISTAN				2		
444440	INVALID				8		
444441	INVALID				128		
452048	VIETEL, VIETNAM						40
457010	LTC, LAOS			12	12		
469072	INVALID				4		
470010	GRMPHN, BANGLADESH						42
510890	HUTCH, INDONESIA						40
612060	, COTE DIVOIRE				20		8
628040	USAN, GABON			4			
637019	TELES, SOMALIA					84874	
637602	NLINK, SOMALIA		2				
648032	TELCEL, ZIMBABWE						26
649011	MOBTEL, NAMIBIA		6				
984519	INVALID				68		
992918	INVALID		2				

5   **Domains connected to IMSI/Ki traffic**

Most fruitful domains