Innov8 Experiment Profile

Experiment Name	**Cryptanalytic Services**	**Experiment Reference**	
Version		**Date**	
Experiment Owner	[redacted] **(NSA)** [redacted] **(GCHQ)**	**Department**	**NSA/S3/CES GCHQ/PTD**
Experiment Start Date	**06/01/2010**	**Experiment End Date**	**Early 2011**

Part 1 – Experiment Overview

Business Case

*Detail the nature of the Experiment as a high level plain English description. Refrain from using overly technical terms if possible. Justify briefly why this Experiment should run, with a high level summary of Experiment, Conditions, De-risking effort, Business Case and Expected Outcomes/Bene*fits.

As part of the Joint Capability Activity (JCA) in partnership with GCHQ, experiments are to be conducted within the Joint Capability Experiment (JCE) to test the robustness, scalability and interoperability of cryptanalytic services integrated into the corporate high speed DNI architectures of each agency. The cryptanalytic services experiment will explore a new hardware configuration for sensitive cryptanalytic mission applications integrated into a secure processing enclave interfacing to the corporate high speed DNI architecture. This will also include the testing of hardware accelerated decryption at the frontend. The business case for running this experiment is to demonstrate the following:

- Stress the processing capability under heavy load of “tasked” common internet encryption technologies
- Test the throughput capability of common internet encryption technologies processing including:
  - Higher bandwidth common internet encryption technologies streams
  - Throughput of ISLANDTRANSPORT messaging support for CA Service requests to NSAW LONGHAUL key recovery service
  - The temporary storage of encrypted data while waiting for a response from LONGHAUL
- Test the Hardware accelerated (CAVIUM card) common internet encryption technologies processing component
- Test the impact of XKEYSCORE as Stage 2 of TURMOIL for follow on processing of exploited common internet encryption technologies streams

Benefits

Outcome	Expected Benefit	How will benefit be measured?	KPI (CSF)	Reference Number
	Validation of the new hardware chosen for cryptanalytic processing			
	Integration of hardware accelerated decryption			
	Ability to cope with high throughput and bandwidth of common internet encryption technologies			
	Ability to prioritize processing appropriately			
	Ability to process multiple common internet encryption technologies exploitation capabilities concurrently			

Plan

The cryptanalytic Services processing experiment will consist of several additive experiments. The first two will mostly consist of preparatory work. The subsequent experiment will explore scalability and interoperability.

Note that the below list is not exhaustive; this represents the initial list of experiments to be conducted in JCE with respect to cryptanalytic services. Subsequent experimentation upon conclusion of the below experiments will be negotiated with INNOV8 as appropriate.

EXP. 1: Test dataflow (~1 month) This experiment will set up and configure the new cryptanalytic processing hardware as well as basic dataflows into the cryptanalytic services for further experimentation. Streaming dataflows of common internet encryption technologies and ISLANDTRANSPORT dataflows to LONGHAUL for cryptanalytic recovery will be established. This experiment will ensure that the cryptanalytic services can properly process data using existing capabilities from NSA-centric TURMOIL systems. Additionally, the appropriate analytics will be put in place and evaluated to identify viable candidate input streams (case notations) containing the common internet encryption technologies of interest.

EXP. 2: Stress testing (~1 month) This experiment will stress test the current suite of cryptanalytic services to identify the baseline throughput and scalability parameters.

This experiment will leverage and validate candidate input streams (case notations) containing the common internet encryption technologies of interest.

EXP. 3: Integration of new cryptanalytic processing functionality (4-6 months) This experiment will introduce new and enhanced capabilities to increase throughput, scalability and interoperability. This will include but not be limited to hardware accelerated decryption, agile management of buffered encrypted data, the development of an interoperable API for sharing CA services requests across NSA/CES and GCHQ/PTD key recovery architectures, the ability for follow-on processing architectures to consume large volumes exploited common internet encryption technologies of interest.

PUT Involvement

Team members include:

- NSA
  - CES
  - T11
  - T53
- GCHQ
  - CCNE/PTD

Migration Approach

The goal is to transition new cryptanalytic capabilities as they are tested and validated in the JCE environment into the JPC operational environment to provide mission value.

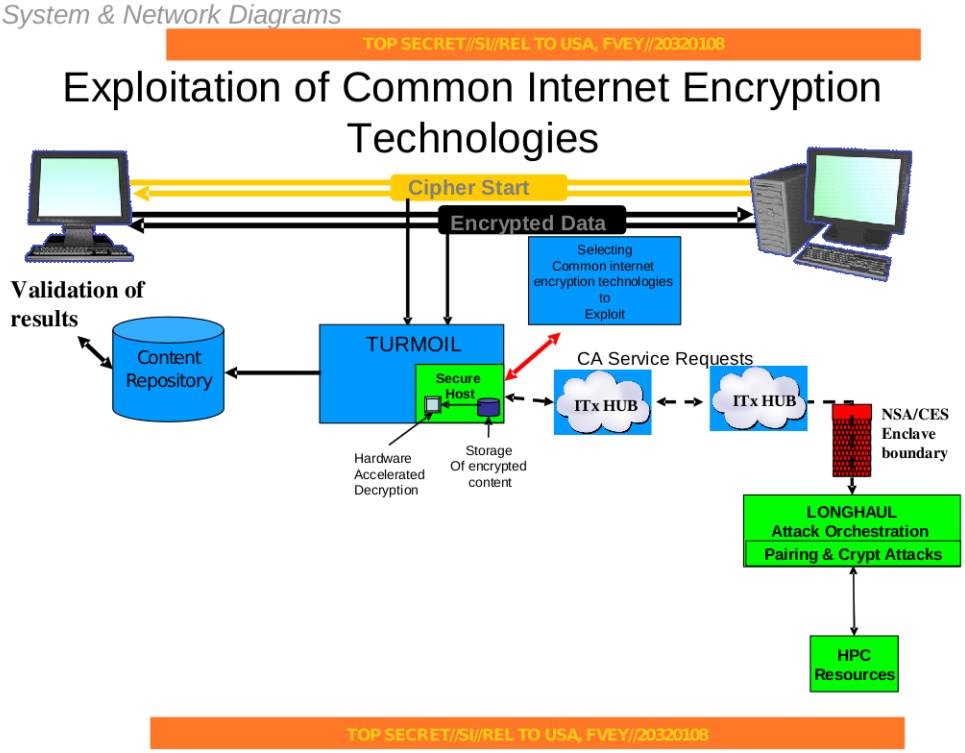
Part 2 - Experiment Detail

High Level Description of Experiment

Same as Business case.

System & Network Diagrams

System & Network Diagrams



Hardware Requirements

The cryptanalytic services experiment requires the inclusion of 4 IBM 3650 M3 servers (2 servers per 10G LPT) to run the sensitive cryptanalytic mission applications. The cryptanalytic processing servers are dedicated to cryptanalytic processing and are firewalled off from the rest of the LPT system. These are an extension of the NSA/CES cryptanalytic enclave and can only be administered by CES approved sys-admins. This will include appropriately cleared GCHQ/PTD for monitoring and auditing purposes. The individuals will need to have a minimum of ECI PIQARESQUE. The results of cryptanalytic processing will be TS//SI/REL FVEY for the purposes of this experiment.

Software Requirements

Owner should detail here any additional software requirements and the steps taken to procure the required items. Note: All software should be registered with SAM.

Connectivity (Dataflows)

The success of the cryptanalytic services experiment relies on the ability to extract and pass crypto-synch parameters associated with common internet encryption technologies to NSAW/LONGHAUL for cryptanalytic attack and recovery. The crypto-synch parameters are extracted in the cryptanalytic processing servers and passed to NSAW/LONGHAUL via a corporate messaging system (ISLANDTRANSPORT) connection. The messages are encrypted prior to leaving the cryptanalytic processing servers using the secure corporate messaging software (ISLANDHIDEAWAY) for security and authentication.

Data Requirements

This experiment will leverage and validate candidate input streams (case notations) containing the common internet encryption technologies of interest.

Data Repositories

Detail the end points of the processed data and the expected volumes. Provide details of Data Retention requirements.

Legalities

Detail any legal issues, which are contrary to the scope detailed in the System ADS. How are these to be resolved? Please also cover any HRA compliance issues. JCE Security requirements can be found via the following link: [redacted]

Additional Support

Detail the level of anticipated support required in the event of hardware or network failure. Identify areas that may be called upon to provide assistance.

Data Access

Detail the method under which the data will be accessed and by whom. Detail the types of data involved. State the Protective Marking of the Data. Include any addition Audit requirements here.

External Dependencies

Detail any external dependencies from other Programmes, Projects, Themes etc.

Previous / Related Work

Highlight any previous / related work (including lessons learnt, test results etc) where appropriate.

Access Control

Serial	Access Given	Full Name	HRA Training Y/N	ECI Cleared	Role	SID	PF No.
1	e.g. Root/User	[redacted]	Y	[redacted]	Developer	[redacted]	11111
2							
3							
4							
5							
6							

SEG Reviewers

Post	Name
GCHQ Service Owner	[redacted]
NSA Service Owner	
Innov8 Service Manager	
Innov8 Engineering	
Innov8 Support Team (Technical)	
Innov8 Compliance Manager	
Data Owner	
Selector Management Team	
ACD (Dataflow)	
SSOS Representative	
OPP-LEG	
IT Services	
IT Services (Bude)	
Bude SSE	
TFE-SSE	
TPS	
SAM Representative	
Security Working Group	

Changes to Experiment Profile

Version	Amendment Date	Changes to the Experiment