NCL
National Cybersecurity R&DLab

WHO WE ARE

A national infrastructure for running cyber-security experiments. NCL offers :
- Computing Resources - Ready-to-use
- Cyber-security data - Application Services and tools

A data repository for hosting and sharing of cyber-security data and service
- Internet traffic, worm/malware, mobile apps, etc.

A platform facilitating collaboration among researchers in academia, industry as well as government agencies.

WHAT WE DO

- Cyber-security research community
- Education and teaching
- Cyber range exercise and tests
- Cyber-security personnel training

FEATURE LIST

Major Features	Phase One	PhaseTwo	Phase Three
Hardware			
Number of servers	100	100	300 (Intel SGX support, up tp 200)
Networking	3x10 Gbps (OpenFlow enabled, 3 SDN switches)	3x 10 Gbps (OpenFlow enabled, 3 SDN switches)	3x10 Gbps (OpenFlow enabled,9 SDN switches)
Core Software			
VM & Bare Metal Machines Provisioning	v	v	v
Fully Controllable Networks (control of bandwidth, latency, drop rate etc.)	v*	v*	v*
OS Support (Linux, FreeBSD, Windows)	v	v	v
Support of Configuration Management System	-	Ansible	Ansible, Puppet, etc.
Support of Container Technology	-	Docker	Docker
Creation of SDN-related Experiments (evaluation of new switch design, new algorithms for multi-controllers management, resilience protocols and security mechanisms, etc)	-	v*	v
Web built-in Console	v#	v#	v
Data & Data Repository			
Database	Up to 3 (e.g. Rainbow table for GSM A5/1, Click-flaw data, mobile anti-virus apps)	Up to 5 (additional: Alexa top 1,000,000 websites, Internet traffic)	Up to 10 (e.g. including data for network malware, web, mobile and human behavior etc)
Access to External Databases	US IMPACT	US IMPACT	US IMPACT
Seamless Integration with NCL Testbed	- (uploading and downloading only)	- (uploading and downloading only)	- (direct access within experiment nodes)
Analytic Tools within NCL Data Repo (searching,sorting,extraction,anonymization etc.	-	-	-
Services and Tools			
Management Console (Accounts, projects and experiments management through a simple user interface)	v	v	v
GUI to Visualize Network Topology	v	v	v
GUI to Configure Network Topology	-	v	-
Billing & Cost Management Tool	v	v	v
Monitoring & Logging Tool	v	v	v
Usage & Resource Auditing Tool	v	v	v
Network Traffic Generator	Open-source software	Software and high-end dedicated hardware	Software and high-end dedicated hardware
Internet Simulator (detailed Internet model for simulation of Internet-wide events such as worm spread, DDoS, spam etc)	-	v v	v
VM-based Router, Firewall	-	-	v
Support of hot plugging of external devices	-	-	v
Ready-to-use experiment setups			
System vulnerability environments	Up to 20 (well-known ones like Heartbleed, shellshock etc)	Up to 20 (include main vulnerability types like memory corruption, data corruption, crypto implementation flaws)	Up to 100 (include most of the vulnerability types)
Big-Data Platforms	Hadoop, Spark	Additional: Storm, HBase, HIVE	Additional: H2O, Flink, etc
Distributed Ledger System (for validation and testing of new protocols, data structure and security mechanisms, etc)	Bitcoin	Bitcoin and possible others	Bitcoin and possible others
Cyber Range Infrastructure (simulated infrastructure for training to defend against cyber attacks scenarios)	-	1 simple example (e.g. a test lab)	More complex example (e.g. an organization)
Cyber-physical system simulators	-	-	Smart grid simulator
Emulated android environment	-	v	v
Emulated ARM environment	-	-	v
Teaching-ready environments	-	Up to 5	Up to 10
Security			
Access Control (manage user access and encryption keys)	v	v	v
Contained experiments (traffic in one experiment will not affect another)	v	v	v
Internet Access (Accessibility to Internet from experiment nodes)	Isolated (no outgiong Internet access)	Controlled	Controlled
Federation			
NUS Sensor Network Testbed (Indriya)	v	v	v
SUTD Water Testbed	-	-	v

* Feature(s) only available in bare metal provisioning

Feature(s) only available in VM provisioning