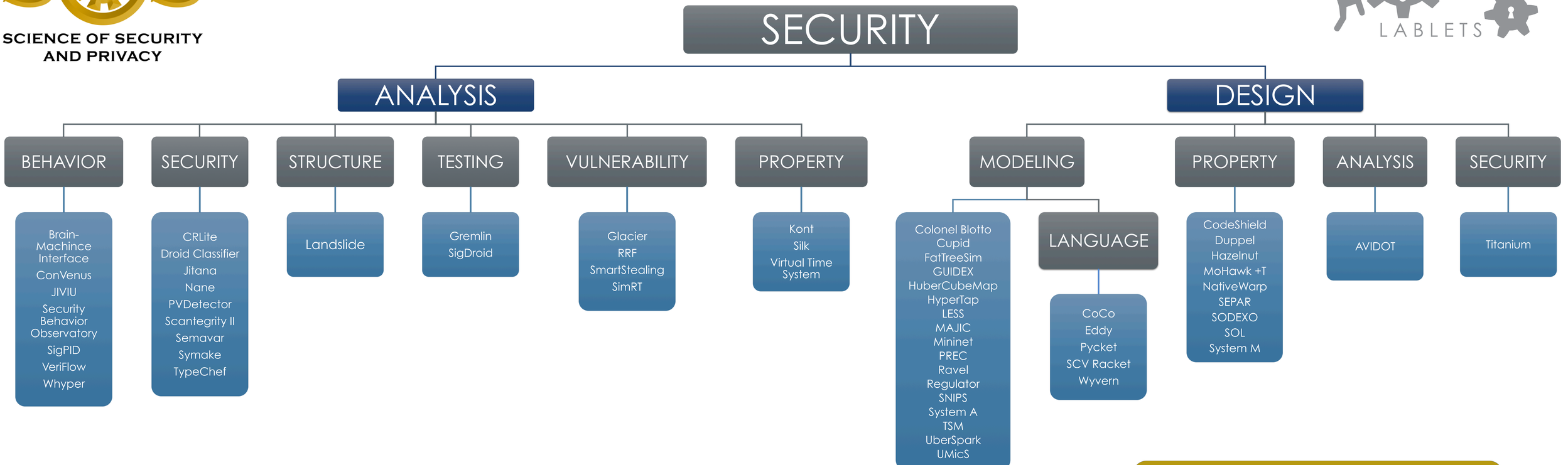
SoS Lablet Researcher-Developed Tools

SCIENCE OF SECURITY AND PRIVACY

Science of Security LABLETS



TOOL DESCRIPTIONS

Tool: *a product such as a system, framework, language, algorithm, software, mechanism, etc. developed as a result of research.*

- **AVIDOT** - *a projection algorithm for strictly monotone linear complementarity problems*
- **Brain-Machine Interface***** - *directs a robot using only "the inputs from an SSVEP-based BMI"*
- **Coco** - *adapts answer-set programming to identify a maximal set of non-dominated commitments*
- **CodeShield** - *personalized application white-listing*
- **Colonel Blotto** - *a three-step, three-player game that explores cyber physical security*
- **ConVenus** - *rapid congestion verification of network updates in software-defined networks*
- ***CRLite**** - *downloads all certificate revocation information on the web, stores it compactly, and disseminates it to all clients*
- **Cupid** - *a demonstrably safe computer language for modeling business practices*
- **Droid Classifier** - *detects and classifies malware on android devices*
- **Duppel**- *enables a tenant virtual machine to defend itself from cache-based side-channel attacks in public clouds*
- **Eddy**** - *checks privacy policy for conflicting requirements*
- **FatTreeSim** - *PDES-based toolkit consisting of a highly scalable fat-tree network model*
- **Glacier**** - *supports transitive class immutability for Java*
- **Gremlin**** - *provides resiliency testing of micro-service applications*
- **GUIDEX** - *an intrusion detection network based on game theory*
- **Hazelnut** - *edits changes within a program for semantics AND syntax*
- **HyperCube Map**
- **HyperTap** - *establishes a root of trust for logging data and events in hypervisors*
- **Jitana**** - *supports large scale compositional analysis and efficient hybrid analysis*
- **JIVIU** - *animates the trace of a user interaction with a graphical interface*
- **Kont***** - *compares trade offs between "liveness" and safety in normative, multi-agent systems*
- **Landslide** - *systematically explores kernels to find race conditions*
- **LESS** - *evaluates large scale network security systems*
- **MAJIC** - *assists developers in applying the Java sandbox to applications*
- **Mininet** - *emulates networks*
- **Mohawk+T** - *addresses ATRBAC-safety*
- **Nane** - *identifies healthcare domain misuses via a semi-automated process*
- **NativeWrap*** - *"wraps" mobile device apps inside of another app that allows the user to set stringent security options*
- **PREC** - *detects and stops root exploits while imposing low interference to benign applications*
- **PV Detector** - *detects privacy policy violations in Android application code*
- **Pycket****- *optimizing compiler for eliminating the costs of behavioral contracts*
- **Ravel** - *implements an entire SDN network control infrastructure within a standard SQL database*
- **Regulator** - *a more secure cryptography API frameworks*
- **RRF** - *reproduces reported process-level races; enables debugging*
- **Scantegrity II** - *end to end cryptographic voting system*
- **SCV Racket**** **-** *functional language with statically verified behavioral contracts*
- **Security Behavior Observatory** - *collects data on hundreds of users and their computer behavior over several years*
- **Semaver***** - *methodology for understanding the relations between security policies and breaches*
- **SEPAR** - *detects previously unknown vulnerabilities and prevents exploitation*
- **SIG-Droid** - *a framework for system testing of Android apps*
- **SigPID** - *a malware detection system based on permission analysis*
- **Silk** - *mechanism for norm emergence in multi agent systems based on user interaction*
- **SimRT** - *automated regression testing framework for use in detecting races introduced by code modifications*
- **SmartStealing**** - *automated decision making for whether to steal and what task to steal from during execution*
- **SNIPS** - *scalable network intrusion detection system*
- **SODEXO** - *creates and leverages deceptive honeybots to gain information from botnets*
- **SOL**** - *simplifies the development of SDN-based network optimization applications*
- **Symake**
- **System A** - *statically verifies a large class of asynchronous communication protocols*
- **System M** - *determines security of un-trusted code*
- **Titanium**
- **TSM(typed syntax macro)** - *syntax extension mechanism*
- **TypeChef**** - *performs variability analysis of C code and correlates variability dense code with vulnerabilities*
- **UberSpark**** *compositionally verifies extensible hypervisor security properties*
- **UMIcS** - *controls the release and use of private data*
- **VeriFlow** - *checks for network-wide invariant violations dynamically between SDN controller and network*
- **Virtual Time System** - *integrates with Mininet to offer virtual time to containers to improve fidelity and scalability*
- **Whyper*** - *identifies sentences that describe the need for a given permission in an application description*
- **Wyvern**** - *object oriented programming language*

CMU **NCSU** **UIUC** **UMD**

*Released to the public
**Released on GitHub
***Released at https://research.csc.ncsu.edu

HOTSOS HOT TOPICS in the SCIENCE OF SECURITY SYMPOSIUM & BOOTCAMP