Science of Security



LABLETS

Writing Guidelines

Improving Quarterly, Annual, and Hard Problem Reports

Purpose

The information and research that we receive from the quarterly and annual lablet reports is used to justify the funding the NSA provides to each university lablet. If the reports are not sufficient in scope and depth, we will be unable to properly justify increased or even continued funding from the NSA.

These guideline will help to ensure that the lablet reports, especially the annual reports, clearly and thoroughly discuss the research being conducted, as well as the hard problems and specific questions the research addresses.



Noted Problems from 2016 Hard Problem ("Before-Now") Status Draft

- Several summaries focused exclusively or almost exclusively on the research from the summarizing lablet instead of including the work of every lablet.
- Not all listed publications were relevant to the research descriptions
- New descriptions of research cited last year's publications.
- Too much emphasis on what was done last year
- More emphasis needs to be placed on Resilient Architecture

Noted Problems from 2016 Annual Reports

- Length, too long or too short
- Spelling and grammar (run-on or incomplete sentences)

Quarterly Report

Format and Content

Each project should have a multi-section report.

The PUBLIC SECTION should include:

- PI(s)
- Co-PI(s)
- Researchers
- Hard Problem addressed
- Publications from the quarter
- Accomplishment highlights to include a general description of the project and progress

Writing style/voice:

- Style and language accessible by someone who is knowledgeable about cybersecurity, but may not be familiar with domain-specific terminology.
- Focus on generating interest in the work and (hopefully) stimulate communication with project researchers that could lead to additional collaborative efforts.

The PRIVATE REPORT (Group Only Content) should include:

- A detailed description of progress on the project:
    - Describe the work/research conducted
    - Present results and conclusions
    - Identify how the results contribute towards solving a specific Hard Problem OR Area of Research
- An accounting of routine tasks such as submitting an IRB package, onboarding new students, etc.

Writing style/voice:

- Style and language for a more technically-minded audience
- Focus on highlighting progress towards a hard problem or specific research question
- Help stimulate collaboration and ability to leverage other research

Quarterly Summary Reports

Format and Content

Organized by project OR hard problem at the writer's discretion.

The PUBLIC REPORT should include:

- Meaningful accomplishments
- Notable achievements (Submitting an IRB package, on-boarding a new student, or preparing a manuscript for submission are routine tasks in research, NOT notable highlights.)
- Work published during the quarter
- Community Engagements
- Educational Advances

Writing style/voice:

- Style and language accessible by someone who is knowledgeable about cybersecurity, but may not be familiar with domain-specific terminology.
- Focus on generating interest in the work and (hopefully) stimulate communication with project researchers that could lead to additional collaborative efforts.

The PRIVATE REPORT (Group Only Content) should include:

- A detailed description of progress on each project:
    - Describe the work/research conducted
    - Present results and conclusions
    - Identify how the results contribute towards solving a specific Hard Problem OR Area of Research
- An accounting of routine tasks such as submitting an IRB package, on-boarding new students, etc.

Writing style/voice:

- Style and language for a more technically-minded audience
- Focus on highlighting progress towards a hard problem or specific research question

Annual Reports

Fomat and Content

The "Burning Questions" for Each Project(you may have seen these before...):

Which researchers participated in the project?

What was completed?	Describe the work/research conducted (2-3 sentences)
What was learned?	Present results and conclusions (1-2 sentences)
How does it help?	Identify how the results contribute towards solving a specific *Hard Problem* OR *Area of Research* (1-2 sentences)

You can't JUST do research:

Community Engagements

Educational Engagements

Publications (new publications only)

Example Paragraph:

This year we developed a module system design that is capability-safe, yet preserves most of the convenience of conventional module systems. We demonstrated how to ensure key security and privacy properties of a program as a mode of use of our module system. Restricting the authority of un-trusted code is difficult in today's systems because, by default, code has the same authority as the user running it. Object capabilities were a promising way to implement the principle of least authority, but they take away many conveniences provided by today's module systems. Scalability and composability is a primary concern of the project. Our research focuses on producing a language and framework that enables the construction of secure mobile applications with known security properties which increases secure composability of projects.

Hard Problems Status Reports

Resilient Architecture

Description:
Resilient Architecture considers how a system behaves when faced with an attack. Resilience is measured in three main areas: stand, deliver, restore. Stand explores a system's ability to statically withstand attack. Deliver explores whether a system can continue to deliver (possibly at a diminished level) essential services during attacks. Restore explores how quickly a system can be restored to full functionality following an attack.

Goal:
Develop **means** to design and analyze system architectures that deliver required service in the face of compromised components.

Questions:

- What specific **means** were researched and or developed?(1-2 sentences)
- What specific problem relating to resiliency inspired the research? (1-2 sentences)
- How do the **means** increase resiliency in system architecture?(1-2 sentences)
- Supporting Documentation: Author(s), ***Title of Paper***, presentation/ publication location, date

Example:

We developed several properties that can be used to define resiliency and demonstrated that they are useful criterion for measurement. These new properties provide a standard by which future researchers and developers can measure the resiliency of their system.

K. Dou, X. Wang, C. Tang, A. Ross, and K. Sullivan. ***An Evolutionary Theory-systems Approach to a Science of the Ilities***. 2015/12/31, Elsevier, Procedia Computer Science 44, pp. 433-442.

Hard Problems Status Reports

Scalability and Composability

Description:
Scalability and composability considers techniques for constructing and analyzing software. The main concerns of this hard problem are to determine if the system can be scaled upward, and to reliably utilize security analysis of independent parts of a system to determine the security of the system as a whole.

Goal:
Develop **methods** to enable the construction of secure systems with known security properties from components with known security properties, without a requirement to fully re-analyze the constituent components.

Questions:

- What specific **method** was researched or developed? (1-2 sentences)
- What specific problem relating to scalability or composability inspired the research? (1-2 sentences)
- How does the **method** further enable the construction of secure systems? (1-2 sentences)
- Supporting Documentation: Author(s), ***Title of Paper***, presentation location, date

Hard Problems Status Reports

Policy-Governed Secure Collaboration

Description:
Policy-governed secure collaboration focuses on developing the scientific principles used to express and enforce standardized policies. Requirements and policies for handling data must address differing usage needs and different user authority domains.

Goal:
Develop **methods** to express and enforce normative requirements and policies for handling data with differing usage needs and among users in different authority domains .

Questions:

- What specific **method** was researched or developed? (1-2 sentences)
- What specific problem relating to policy inspired the research? (1-2 sentences)
- How does the **method** express or enforce requirements and polices for handling data ? (1-2 sentences)
- Supporting Documentation: Author(s), ***Title of Paper***, presentation location, date

Hard Problems Status Reports

Security-Metrics-Driven Evaluation,
Design, Development, and Deployment

Description:
Security-metrics-driven evaluation, design, development and deployments explore the development of research based techniques for effectively measuring and quantifying the extent to which a given system satisfies specified security property

Goal:
Develop security **metrics and models** capable of predicting whether or confirming that a given cyber system preserves a given set of security properties (deterministically or probabilistically), in a given context.

Questions:

- What specific **metric(s) or model(s)** were researched or developed? (1-2 sentences)
- What specific problem relating to metrics inspired the research? (1-2 sentences)
- How do the **metrics or models** predict or confirm security properties ? (1-2 sentences)
- Supporting Documentation: Author(s), ***Title of Paper***, presentation location, date

Hard Problems Status Reports

Understanding and Accounting
for Human Behavior

Description:
Understanding and accounting for human behavior seeks to understand the human element of cybersecurity by addressing the unpredictability of human actors in computer system usage. Research-based models of human behavior can be used to design and implement computer systems which counteract or minimize the impact of humans on the security of the system

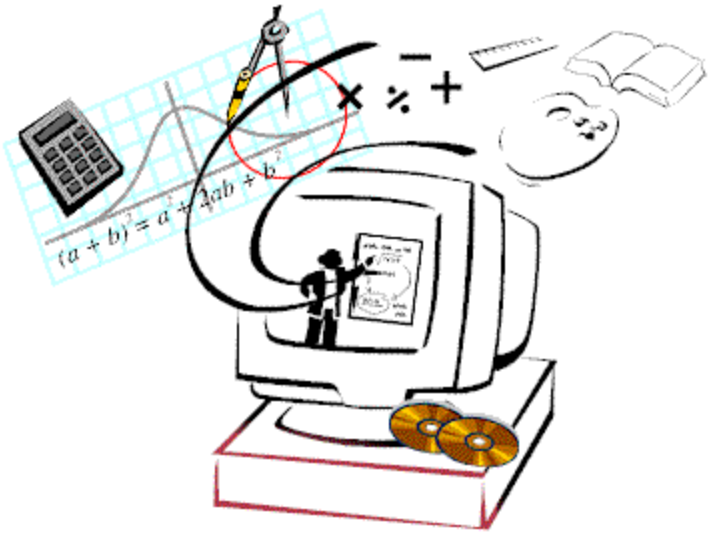
Goal:
Develop models of human behavior (of both users and adversaries) that enable the design, modeling, and analysis of systems with specified security properties .

Questions:

- What specific **model(s) were** researched or developed? (1-2 sentences)
- What specific problem relating to human behavior inspired the research? (1-2 sentences)
- How do the **models** explain or advance system security ? (1-2 sentences)
- Supporting Documentation: Author(s), ***Title of Paper***, presentation location, date

Content Considerations

All Reports



There should be about an 80/20 disbursement of emphasis on new work vs. summarizing past work,

Words such as “good”, “bad”, “done”, “better”, “big”, etc. are imprecise and should be avoided.

*****Specific, descriptive terminology effectively conveys a precise message regarding the accuracy of research results. *****

VS.

*****Big words are better for explaining good results. *****

Lengthy, rambling sentences are confusing and difficult to follow. Clear, concise writing is essential to clear communication of ideas.

Please avoid numbering within the paragraph. We are looking for a written report not an outline or list.

Spell Check.

Use complete sentences.

Although each lablet has been tasked to summarize one hard problem specifically for the Hard Problem Summary, we expect to see the work of each lablet reflected in each **hard problem summary**, not just the work of the summarizing lablet.