2015 Symposium & Bootcamp on the Science of Security, HotSoS, Urbana IL

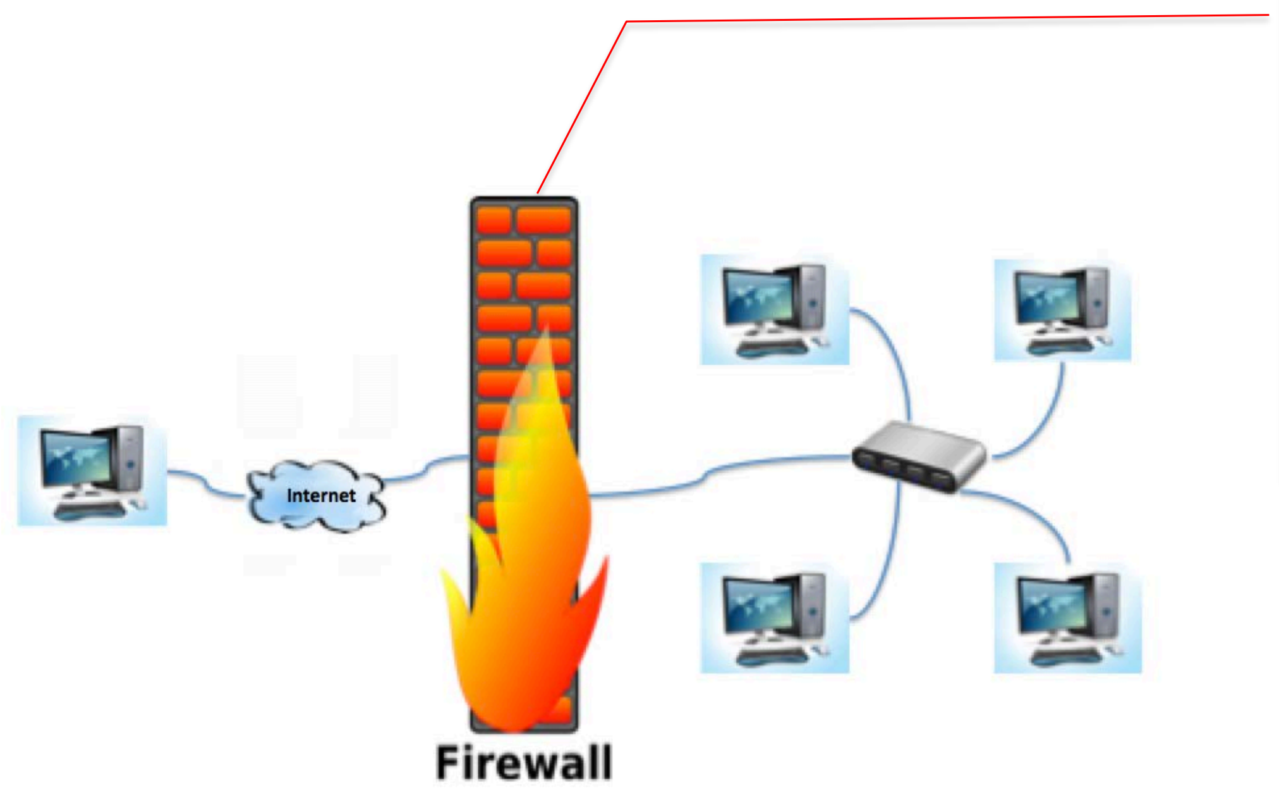
# Towards Quantification of Firewall Policy Complexity

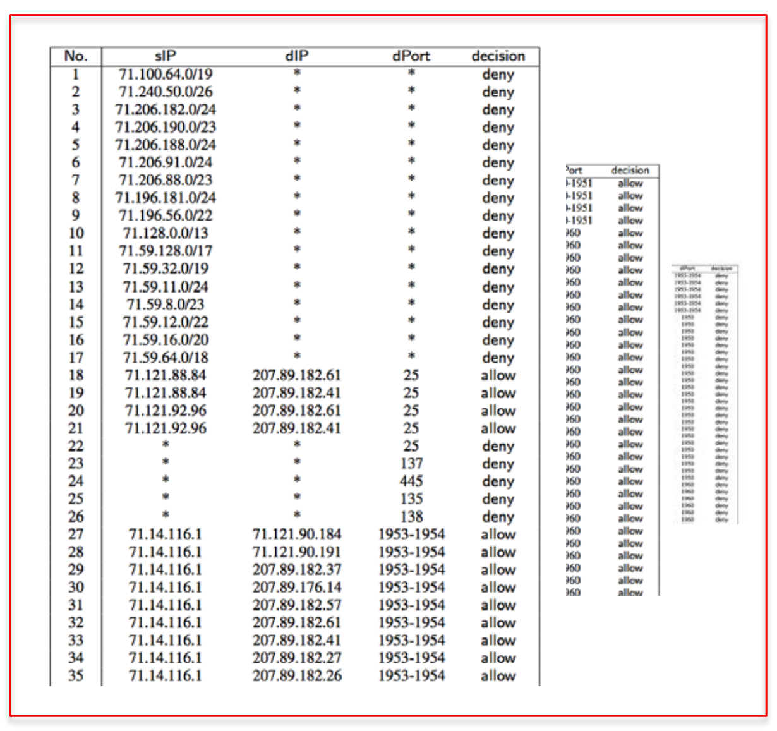
**Haining Chen, Omar Chowdhury, Jing Chen, Ninghui Li, and Robert Proctor**

{chen623, ochowdhu, chen548, ninghui, rproctor}@purdue.edu

Purdue University · Computer Science · Psychological Sciences at Purdue University

## Motivations





| No. | sIP | dIP | dPort | decision |
|---|---|---|---|---|
| 1 | 71.100.64.0/19 | * | * | deny |
| 2 | 71.240.50.0/26 | * | * | deny |
| 3 | 71.206.182.0/24 | * | * | deny |
| 4 | 71.206.190.0/23 | * | * | deny |
| 5 | 71.206.188.0/24 | * | * | deny |
| 6 | 71.206.91.0/24 | * | * | deny |
| 7 | 71.206.88.0/23 | * | * | deny |
| 8 | 71.196.181.0/24 | * | * | deny |
| 9 | 71.196.56.0/22 | * | * | deny |
| 10 | 71.128.0.0/13 | * | * | deny |
| 11 | 71.59.128.0/17 | * | * | deny |
| 12 | 71.59.32.0/19 | * | * | deny |
| 13 | 71.59.11.0/24 | * | * | deny |
| 14 | 71.59.8.0/23 | * | * | deny |
| 15 | 71.59.12.0/22 | * | * | deny |
| 16 | 71.59.16.0/20 | * | * | deny |
| 17 | 71.59.64.0/18 | * | * | deny |
| 18 | 71.121.88.84 | 207.89.182.61 | 25 | allow |
| 19 | 71.121.88.84 | 207.89.182.41 | 25 | allow |
| 20 | 71.121.92.96 | 207.89.182.61 | 25 | allow |
| 21 | 71.121.92.96 | 207.89.182.41 | 25 | allow |
| 22 | * | * | 25 | deny |
| 23 | * | * | 137 | deny |
| 24 | * | * | 445 | deny |
| 25 | * | * | 135 | deny |
| 26 | * | * | 138 | deny |
| 27 | 71.14.116.1 | 71.121.90.184 | 1953-1954 | allow |
| 28 | 71.14.116.1 | 71.121.90.191 | 1953-1954 | allow |
| 29 | 71.14.116.1 | 207.89.182.37 | 1953-1954 | allow |
| 30 | 71.14.116.1 | 207.89.176.14 | 1953-1954 | allow |
| 31 | 71.14.116.1 | 207.89.182.57 | 1953-1954 | allow |
| 32 | 71.14.116.1 | 207.89.182.61 | 1953-1954 | allow |
| 33 | 71.14.116.1 | 207.89.182.41 | 1953-1954 | allow |
| 34 | 71.14.116.1 | 207.89.182.27 | 1953-1954 | allow |
| 35 | 71.14.116.1 | 207.89.182.26 | 1953-1954 | allow |

A *firewall* filters packets based on a *firewall policy* which usually includes a large number of rules

> *"Firewalls are (still) poorly configured, and a rule set's complexity is (still) positively correlated with the number of detected configuration errors."*
>
> \- Avishai Wool [Trends in firewall configuration errors, 2010]

**Legal traffic**

**Illegal traffic**

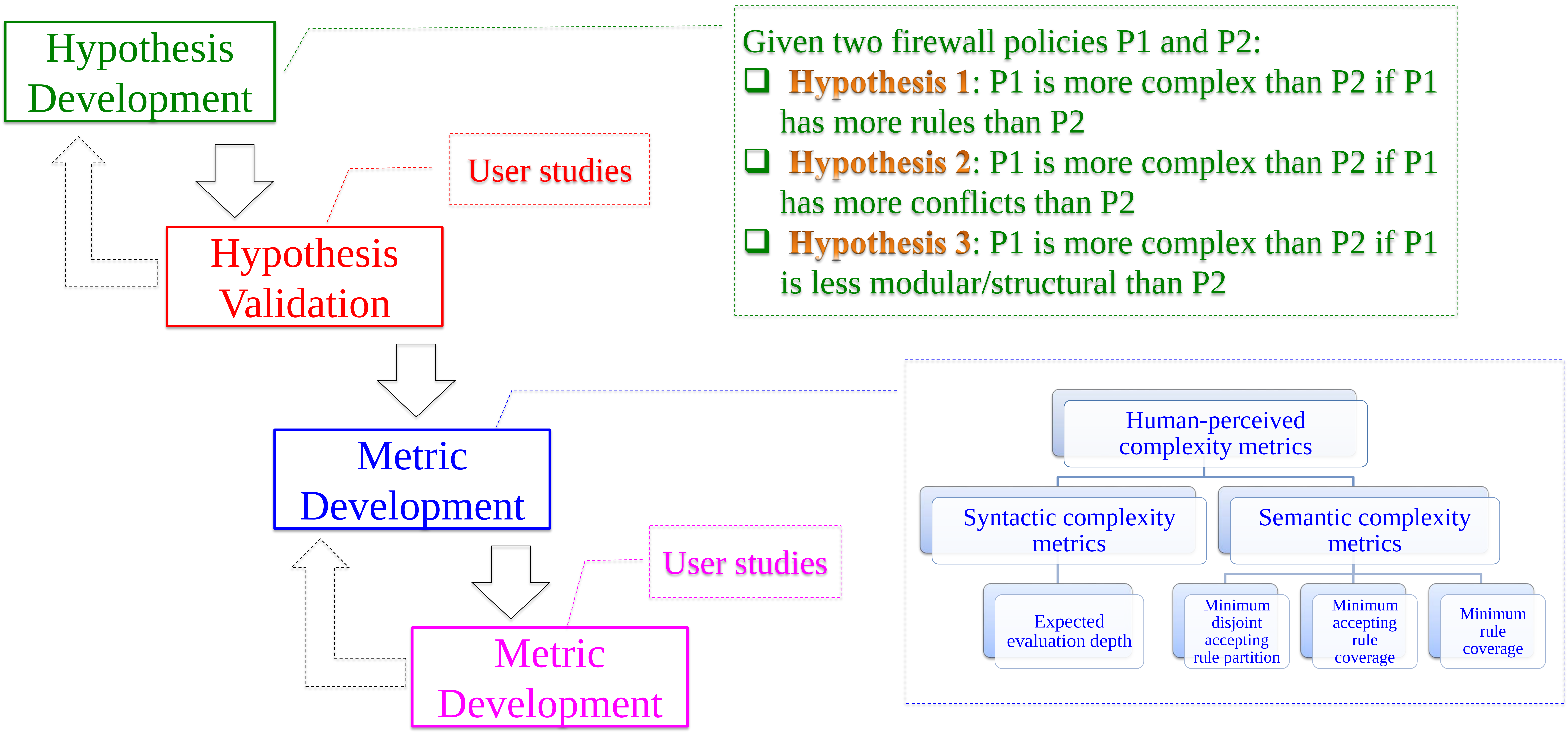
## Problem Definition

*How to find objective metrics that measure and quantify human-perceived complexity of firewall policies?*

## Contributions

- ❑ Proposed a workflow for designing, developing, and empirically validating metrics for quantifying complexity of firewall policies
- ❑ Presented three hypotheses capturing inherent properties of firewall policies that make them syntactically or semantically complex
- ❑ Identified two types of human-perceived complexity and suggested objective metrics

## Workflow for Exploring Complexity Metrics


Hypothesis Development
User studies
Hypothesis Validation
Metric Development
User studies
Metric Development
Human-perceived complexity metrics
Syntactic complexity metrics
Semantic complexity metrics
Expected evaluation depth
Minimum disjoint accepting rule partition
Minimum accepting rule coverage
Minimum rule coverage

Given two firewall policies P1 and P2:

- ❑ **Hypothesis 1**: P1 is more complex than P2 if P1 has more rules than P2
- ❑ **Hypothesis 2**: P1 is more complex than P2 if P1 has more conflicts than P2
- ❑ **Hypothesis 3**: P1 is more complex than P2 if P1 is less modular/structural than P2

**http://hot-sos.org/**

The Science of Security initiative is funded by the National Security Agency.