The Advancement of Science in Cybersecurity

Laurie Williams
North Carolina State University
#metoosecurity
A game of cat and mouse ...
Why the Science of Security?

“... nagging perception that too much of the research is opportunistic, lacks rigor, has weak methodology, and fails to produce material advances on underlying hard problems.”

(NSA BAA Industry Day, 2013)
The three missions of the Science of Security Lablets

- **Build a science of security community**
- Advance research methods in the context of cybersecurity to build a sound science of security
- “Solve” hard security problems through the application of scientific research
Through diversity of opinion, creativity and unity is born.
Focus areas
Through collaboration and unity, we can accelerate change on a larger scale.
Competition-free zone
Science of Security Lablets & Sub-Lablets

- National Security Agency
- Lablet (4)
- Sub-Lablet (26)
Science of Security Lablets, Sub-Lablets, and Collaborators

National Security Agency
Lablet (4)
Sub-Lablet (26)
SURE (4)
Collaborator (64)
Science of Security International Sub-Labellets and Collaborators

Sub-Labelt (26)  Collaborator (64)
The three missions of the Science of Security Lablets

- Build a science of security community
- Advance research methods in the context of cybersecurity to build a sound science of security
- “Solve” hard security problems through the application of scientific research
Those “pesky” and ever-present tough questions

*Where’s the beef... science?*

*I just rolled my eyes so hard... I saw my brain*
Tough questions lead to great(er) insight.

“The quality of your answers is in direct proportion to the quality of your questions.”
--Albert Einstein
It’s so easy to fall back to “engineering-ish” research.
Principles, Theories, Laws, Hypotheses ... Science
May be just a “subtle change”
Stand on the shoulders of giants.
## Types of Validation

<table>
<thead>
<tr>
<th>Type of result</th>
<th>Accepted (ICSE 2002)</th>
<th>Accepted (ICSE 2016)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>Evaluation</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td><strong>Experience</strong></td>
<td><strong>8 (19%)</strong></td>
<td><strong>4 (4%)</strong></td>
</tr>
<tr>
<td>Example</td>
<td>16 (37%)</td>
<td>1 (1%)</td>
</tr>
<tr>
<td>Persuasion</td>
<td>0 (0%)</td>
<td>1 (1%)</td>
</tr>
<tr>
<td>Underspecified</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>No validation mentioned</td>
<td>6 (14%)</td>
<td>0 (0%)</td>
</tr>
</tbody>
</table>
### Types of Validation

<table>
<thead>
<tr>
<th>Type of result</th>
<th>Accepted (ICSE 2002)</th>
<th>Accepted (ICSE 2016)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>Evaluation</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>Experience</td>
<td>8 (19%)</td>
<td>4 (4%)</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><strong>16 (37%)</strong></td>
<td><strong>1 (1%)</strong></td>
</tr>
<tr>
<td>Persuasion</td>
<td>0 (0%)</td>
<td>1 (1%)</td>
</tr>
<tr>
<td>Underspecified</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>No validation mentioned</td>
<td>6 (14%)</td>
<td>0 (0%)</td>
</tr>
</tbody>
</table>
## Types of Validation

<table>
<thead>
<tr>
<th>Type of result</th>
<th>Accepted (ICSE 2002)</th>
<th>Accepted (ICSE 2016)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis</td>
<td>…</td>
<td>…</td>
</tr>
<tr>
<td>Evaluation</td>
<td>…</td>
<td>…</td>
</tr>
<tr>
<td>Experience</td>
<td>8 (19%)</td>
<td>4 (4%)</td>
</tr>
<tr>
<td>Example</td>
<td>16 (37%)</td>
<td>1 (1%)</td>
</tr>
<tr>
<td><strong>Persuasion</strong></td>
<td>0 (0%)</td>
<td>1 (1%)</td>
</tr>
<tr>
<td>Underspecified</td>
<td>…</td>
<td>…</td>
</tr>
<tr>
<td>No validation mentioned</td>
<td>6 (14%)</td>
<td>0 (0%)</td>
</tr>
</tbody>
</table>
## Types of Validation

<table>
<thead>
<tr>
<th>Type of result</th>
<th>Accepted (ICSE 2002)</th>
<th>Accepted (ICSE 2016)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>Evaluation</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>Experience</td>
<td>8 (19%)</td>
<td>4 (4%)</td>
</tr>
<tr>
<td>Example</td>
<td>16 (37%)</td>
<td>1 (1%)</td>
</tr>
<tr>
<td>Persuasion</td>
<td>0 (0%)</td>
<td>1 (1%)</td>
</tr>
<tr>
<td>Underspecified</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>No validation mentioned</td>
<td>6 (14%)</td>
<td>0 (0%)</td>
</tr>
</tbody>
</table>
Science of Security Copycats

- Guidelines
- Seminars
- Research plan reviews
- Workshops
- Conference (Hot SoS)
Security Paper Study

128 Papers (CCS)
55 Papers (S&P)
7 Reviewers

Author
## Paper Characteristics

<table>
<thead>
<tr>
<th>Process</th>
<th>Empirical</th>
<th>Proof</th>
<th>Discussion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tool</td>
<td>104</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Model</td>
<td>23</td>
<td>18</td>
<td>0</td>
</tr>
<tr>
<td>Protocol</td>
<td>21</td>
<td>20</td>
<td>5</td>
</tr>
<tr>
<td>Theory</td>
<td>7</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Paper Completeness

- Descriptive Statistics
- Study Context
- Data Collection
- Sample Characteristics
- Discussion of Results
- Subject Sampling
- Analysis
- Results
- Research Objectives
- Threats to Validity

Percentage:
- Yes
- Partial
- No
The three missions of the Science of Security Lablets

- Build a science of security **community**
- Advance **research methods** in the context of cybersecurity to build a sound science of security
- “Solve” **hard security problems** through the application of scientific research
Through focus, progress is made.

1. Thing 1
2. Thing 2
3. Thing 3
4. Thing 4
5. Thing 5
6. Thing 6
7. Thing 7
8. Thing 8

Do This!

DON’T DO THIS!

You wouldn’t do it anyway.
Science of Security **Focus**

1. Scalability and composability
2. Policy-governed secure collaboration
3. Encryption algorithms
4. Predictive security metrics
5. Intrusion Detection
6. Resilient architectures
7. Human behavior

Do This!

DON’T DO THIS!
Hard Problem 1: **Scalability and Composability**

**Challenge**

- Develop methods to enable the construction of secure systems with known security properties.
Component and Configuration Change

```
boolean z = hasA();
true if(z) {
    method1();
    boolean b = hasB();
    if(z && !b) {
        method2();
    }
}
else {
    method3();
}
```

API Access

```
Z
\[ A \quad A \land B \quad A \land \neg B \]
```

\[ A \land \neg A \rightarrow \text{unsatisfiable} \]

\[ A \land A \rightarrow A \]
Hard Problem 2: Policy-Governed Secure Collaboration

Challenge

- Develop methods to express and enforce normative requirements and policies for handling data with differing usage needs and among users in different authority domains.
Implied security and privacy requirements

The system shall provide a means to edit discharge instructions for a particular patient.

(a) Confidentiality (of patient’s discharge instructions);
(b) Integrity (when editing);
(c) Accountability (who performed the edit);

Confidentiality:
“The system shall enforce access privileges that \texttt{enable} \texttt{| prevent} <subject> to <action> <resource>.
“The system shall encrypt <resource> and store <resource> ....”

Confidentiality:
“The system shall enforce access privileges that enable authorized users to edit discharge instructions. ...”
Hard Problem 3: **Predictive Security Metrics**

**Challenge**

- 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.
Leveraging stack traces from crash dumps
Risk-based attack surface approximation

Windows: 48% of all binaries crash, 95% of vulnerable binaries crash.
Firefox: 16% of all files crash, 74% of vulnerable files crash.
Fedora: 8% of all packages crash, 60% of vulnerable packages crash.
Hard Problem 4: **Resilient Architectures**

**Challenge**

- Develop means to **design** and **analyze** system architectures that deliver required service in the **face of compromised components**
Synthesizing Network Security Configurations

- Topology: i.e., links, hosts connectivity
- Host Info: i.e., service/software requirements
- Mission: e.g., connectivity requirements
- Business Constraints: e.g., budget, usability constraint

Resiliency Configurations Synthesis

- Attack Graph Model
- Diversity Model
- Impact Model
- Isolation Model

Resiliency Requirements

- Design Specifications
  - Resiliency metrics
  - Usability
  - Deployment/Cost

Resiliency Configurations
- Isolation patterns
- Security device placements
- OS/Service/Software to be installed
Hard Problem 5: **Human Behavior**

Develop models of human behavior (of both users and adversaries) that enable the design, modeling, and analysis of systems with specified security properties.
Phishing: Personality & Persuasion
YOU BETTER WATCH YOURSELF.....
LinkedIn Resets Passwords As 117M Logins For Sale On Dark Web - UPDATED
## LinkedIn Passwords

<table>
<thead>
<tr>
<th>Rank</th>
<th>Password</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>123456</td>
<td>753,305</td>
</tr>
<tr>
<td>2</td>
<td>linkedin</td>
<td>172,523</td>
</tr>
<tr>
<td>3</td>
<td>password</td>
<td>144,458</td>
</tr>
<tr>
<td>4</td>
<td>123456789</td>
<td>94,314</td>
</tr>
<tr>
<td>5</td>
<td>12345678</td>
<td>63,769</td>
</tr>
<tr>
<td>6</td>
<td>111111</td>
<td>57,210</td>
</tr>
<tr>
<td>7</td>
<td>1234567</td>
<td>49,652</td>
</tr>
<tr>
<td>8</td>
<td>sunshine</td>
<td>39,118</td>
</tr>
<tr>
<td>9</td>
<td>qwerty</td>
<td>37,538</td>
</tr>
<tr>
<td>10</td>
<td>654321</td>
<td>33,854</td>
</tr>
<tr>
<td>11</td>
<td>000000</td>
<td>32,490</td>
</tr>
<tr>
<td>12</td>
<td>password1</td>
<td>30,981</td>
</tr>
<tr>
<td>13</td>
<td>abc123</td>
<td>30,398</td>
</tr>
<tr>
<td>14</td>
<td>charlie</td>
<td>28,049</td>
</tr>
<tr>
<td>15</td>
<td>linked</td>
<td>25,334</td>
</tr>
</tbody>
</table>
Protect users from themselves ... easily!
My Intentions

Security

Collaborative Research

Science

Life

1. Thing 1
2. Thing 2
3. Thing 3
4. Thing 4
5. Thing 5
6. Thing 6
7. Thing 7
8. Thing 8

Do This!

DON'T DO THIS!

You wouldn't do it anyway.
Attackers Unceasing

Cybersecurity is all of our responsibility.
Slide photos - 1

- http://www.tomandjerryonline.com/images/TrapHappy1.jpg
- http://www.leftlion.co.uk/articles.cfm/title/the-three-musketeers/id/1539
- https://www.reddit.com/r/pics/comments/1aw3f3/pathway/
  http://www.bbc.co.uk/bristol/content/image_galleries/tunnel_gallery.shtml
- http://www.thomthom.net/gallery/everything/tunnel-vision/
- http://davemeehan.com/cycling/ojos-negros-tunnel-vision
- http://www.troll.me/images/pissed-off-obama/you-better-watch-yourself_thumb.jpg
Slide photos - 2

- https://bizpsycho.files.wordpress.com/2015/05/colored_puzzle_connection_1600_wht_9893.png
- https://scottmccown.wordpress.com/category/competition/
- http://www.findmemes.com/eye-roll-memes
- http://memegenerator.net/instance/59256035
- http://lorettalovehuffblog.com/
- https://www.bing.com/images/search?view=detailV2&ccid=Y%2bfsSC%2b6&id=00072BAC4D3C77ECF8E4AFFF513CCBFE0EC8E8A12&thid=OIP.Y-fsSC-6cSVEL_8ECb-wigEsC7&q=capability+brown++bridges&simid=608050771047878264&selectedIndex=7&ajaxhist=0
Slide photos - 3

- https://cdn.psychologytoday.com/sites/default/files/field_blog_entry_images/ext.jpg
- http://www.zdnet.com/article/these-are-the-worst-passwords-from-the-linkedinhack/
- https://www.iii.com/sites/default/files/imce/Elizabeth_Image_for_Blog_July_2015.png
- http://thecybersaviours.com/intrusion-detection-system-ids