Leveraging Organizational Etiquette to Improve Internet Security

Niklas Carlsson
University of Calgary, Canada

Martin Arlitt
HP Labs, USA

Presentation at IEEE ICCCN, Zurich, Switzerland, August 4, 2010
Motivation

- Organizations increasingly rely on the Internet
  - Enterprises
  - ISPs
  - Universities
  - etc.

- Continuous battle for control of IT assets

- Internet crime more prevalent and better organized
  - Follow the money
  - Increasingly sophisticated techniques
  - Leverage geographical and legal boundaries
A shift in security practices

- Current Internet security practices primarily focus on what others are doing to our resources, rather than giving equal consideration to what our resources are doing to others.

- We argue that responsible organizations also must strive to improve their organizational etiquette;
  - i.e., must reduce the negative impact the machines (and users) on our domain(s) have on other organizations.

- Organizations should also help other (trusted) organizations achieve the same goal;
  - Primarily through systematic sharing of useful information.
The OE system

- The OE system (after “Organizational Etiquette”)
  - Organizations need to take greater responsibility for the traffic that leaves their edge network(s)
  - Reducing the negative impact an organization and its machines may have on others
  - Help organizations become better Internet citizens

- OE can systematically
  - identify and eliminate malicious activity on edge networks
  - exchange non-sensitive information (to enable other organizations achieve the same goal)
Host accountability

- Improving organizational etiquette will make the Internet more secure
- Design is based on the premise that “security rests on host accountability” [Xie et al. 2009]
- Non-negligible improvements could be obtained by following five simple rules:
  - don't attack
  - don't scan
  - don't intrude
  - don't infect
  - don't spam
Benefits of improving local security and information sharing are intuitive
- Little progress has been made on designing a solution
- We quantify the benefits of our proposed solution of a (single) large organization

Metcalfe's Law suggests that
- Improved etiquette and sharing of information across a set of organizations would have a much greater positive effect on overall Internet security
- So, please weed your lawn ...

Please weed your lawn ...
Our proposed method

- There is an adage that you cannot manage what you cannot measure
- Unfortunately, this reflects the state of many edge networks today ...
  - Management of edge networks has transformed very slowly and conservatively
  - Many tasks are still done manually, which limits the number of events that can be acted upon
- In contrast, miscreants effectively leverage automation to achieve their goals ...
System design

- Overarching goal of our design is to automate as much of the system operation as possible, including data gathering, processing, and system management.

- Our system consists of three primary components:
  - Information management
  - Security planes
  - OE manager
The OE system

Security planes

Internet (external organizations)

Local machines

OE Manager

Information Management

Primary foundation that our system design builds upon
Information management

- Actionable information is critical for improving security!!

**Local machines**

```
<table>
<thead>
<tr>
<th>Automation</th>
<th>Systematic monitoring</th>
<th>Sharing with trusted friends</th>
</tr>
</thead>
<tbody>
<tr>
<td>Candidate events (suspicious activity)</td>
<td>Transaction records (evidence)</td>
<td>Sharable records (less sensitive)</td>
</tr>
</tbody>
</table>
```

```
“inner edge”
```

```
Organizations Internet ingress/egress point(s)
```

```
“outer edge”
```

```
Internet (external organizations)
```

Primary foundation that our system design builds upon.
Machines easily being moved between different security planes, potentially with different Internet accessibility and/or security restrictions

Implemented as isolated virtual networks
**OE manager**

- **Threshold-based policies**
  - Determine which plane (or security restrictions) each machine on the network should be assigned

- **Self-help service**
  - Help individual clients improve their security so that they can be moved to planes with greater accessibility without requiring increased manual efforts
  - Host accountability

- **Management of essential resources**
  - Static policies can be worked around or even make things easier for miscreants
  - Manage essential resources more closely
The OE system
E.g., Sharing with friends

- A friend (organization) may “hint” that one of our machines A attacked one of their machines at time T.
- Using our logs we can corroborate that information to see if we have evidence that support such event and machine A should be moved to a different layer.
Proof of concept analysis

- A year-long trace of an edge network's traffic
  - Characterize different types of undesirable activity
  - Introduce specific solutions to these activities
- Quantify effectiveness of our proposed solution
  - Reduce the volume of malicious or non-productive traffic
  - Improve the security of the edge network itself
- Considers how miscreants have achieved their current levels of success
  - Use those insights to make it more difficult for miscreants to achieve their various goals in the future
- More advanced/better policies applicable
**Connection data:** Detailed summaries of all inbound and outbound connections (e.g., source and destination IP and port numbers, connection state).

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration</td>
<td>1 year (Apr/08 – Mar/09)</td>
</tr>
<tr>
<td>Connections</td>
<td>39.3 billion</td>
</tr>
</tbody>
</table>

External Host = Source IP

External Host = Destination IP

Inbound Connection

Outbound Connection

Campus Host = Destination IP

Campus Host = Source IP
Example results: DDoS

Is egress filtering doing the job??

- No!

- Static threshold-based policy
  - Based on unused address space

- Better yet ... Management of essential resources
  - Keep track of which IP addresses should be in use
  - Solutions at the “inner edge” ...
Conclusions

- Promoting a shift in security practices
  - Current primary focus is on what others are doing to you
  - We argue that responsible organizations must strive to improve their *organizational etiquette* and to become better Internet citizens
  - Organizations should also help other (trusted) organizations achieve the same goal
- Organizations need to take greater responsibility for the traffic that leaves their edge network(s)
- The OE system (after “Organizational Etiquette”)
  - Reduce the negative impact an organization have on others
- Quantify effectiveness of our proposed solution
Questions?

Email: niklas.carlsson@ucalgary.ca