Insider Threat: Philosophy, Research and Academic Perspectives

Dr. Shuyuan Mary Ho
Florida State University
Agenda

• Threat taxonomy

• Academic perspectives on insider threats, insider negligence, and advanced persistent threats

• Philosophy and contemporary approaches of insider threat research
<table>
<thead>
<tr>
<th>Cyber Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Worms and viruses</strong> spread by Downloads (drive-by downloads), E-mail, IM attachments, Downloads on Web sites and social networks</td>
</tr>
<tr>
<td><strong>Polymorphic and metamorphic viruses</strong></td>
</tr>
<tr>
<td><strong>Trojan horses, spyware, keyloggers</strong></td>
</tr>
<tr>
<td><strong>SQL injection attacks</strong></td>
</tr>
<tr>
<td><strong>Denial-of-service (DOS) and Distributed DOS</strong></td>
</tr>
<tr>
<td><strong>Hackers vs. crackers</strong>: System intrusion, System damage, Cybervandalism</td>
</tr>
<tr>
<td><strong>Ransomware</strong></td>
</tr>
<tr>
<td><strong>Smartphones as vulnerable as computers</strong></td>
</tr>
<tr>
<td><strong>Spoofing, sniffing, pharming</strong></td>
</tr>
<tr>
<td><strong>Computer Crime</strong>: Identity theft, Phishing, Evil twins</td>
</tr>
<tr>
<td><strong>Cyberterrorism and Cyberwarfare</strong></td>
</tr>
</tbody>
</table>
Intentional Threats

Deliberate attacks

Employees with Issues

- Overly ambitious
- Holding personal grudges

- Lack of Loyalty
- Disgruntled
- Mental issues
Corporate Espionage

- Espionage in cyber-space is much more serious than just the standard environment of industry competition.

- The playing field has totally shifted to cyber-space, and the procurement of strategic documents is an area that cyber-criminals have invested in.

- Nothing is really truly safe; every internet connection can provide a point of access for the rest of your network - any network.

- Ideas still ultimately drive success in this marketplace, so all intellectual property (IP) - even your ideas - are at risk of being capitalized upon if they are expressed in Computer-Mediated Communication (CMC).
benevolent threats

This lifesize sculpture of Edward Snowden, Bradley Manning, and Julian Assange was erected on May 1, 2015 at Alexanderplatz square in Berlin.
Un-intentional Threats

Inadvertent compromises to infrastructure

- User error
- Configuration issues
- User becomes **attack vector** and **victim** due to social engineering, spear phishing, or stolen identity
- Poor software app development
- Equipment failure
- Natural disasters
“Blended” threat due to Negligence

1. Some form of social engineering encourages your click-through
   - A great “deal” you can’t refuse
   - A fed-ex package that was not able to be delivered…
   - An “Easy Pass” email which suggests you owe a fine
   - From American Airlines: Earn miles while you fight breast cancer
   - From a (spoofed) co-worker: “Here’s the file I wanted you to see”

2. You visit a legitimate site which has been infected by malware
   (eg. Cross Site Scripting, or iFrame compromise)

3. Your workstation becomes a staging server (a zombie, or a bot) for a larger covert attack on the network

4. Your network becomes a home for advanced persistent threat (APT)
Advanced Persistent Threat

- **Advanced**
  - Attacks are adapted to defenders’ efforts
  - Attackers can develop or buy Zero-Day exploits
  - High level of sophistication based on investment into software and research

- **Persistent**
  - Attacks are both objective and specific
  - Programmed to continue until goal is reached
  - Sets up within systems files to maintain a long-term presence

- **Threats**
  - Well organized and capitalized entity/s (organized crime or state-sponsored) behind the attack
  - Expect that there’s much more going on than the malware/exploit/attack alone

A.P.T. is generally successful because of employee negligence.
Command & Control

- Escalation of activity to bolster other elements of advanced persistent threat (APT) infrastructure
- Remote servers operated by (attacker controlled) victim PCs (Bots)
- Activity occurs outside of the normal hours to evade detection
- Interface used to control all aspects of the APT process
- Enables attackers to install new malware & measure success
Terrorism and Cyber-Warfare

- **Smart phone** Next-gen phone apps are making EVERYTHING available to cyber-space
- **Smart home** appliances and automation make home heating, cooling and control systems available to cyber-space
- **Smart grid** makes power generation available to cyber-space
- **Smart city** enables millions of sensors placed on utility systems to collect big data for central correlation analysis
- **“Internet of things”** Everything is accessible and assigned with a dhcp IP address. Hackers will get into your “things” and “devices” the same channel as you get into. (e.g., Jeep, aircraft, power plants)
Terrorism and Cyber-Warfare
Impacts and Consequences

- Loss of Privacy
- Technological unpredictability
- A seriously trust-challenged society
- A steep gain in personal control, followed by a steep loss in personal control
Academic Open Infrastructure

• Open architecture
• Liberal policies and lax implementation
• Easy access is a critical requirement (unlike the banks and businesses)
• Student get thousands of SPAM messages each day
Academic Role in Preparing the Workforce

• Students are attracted to technological learning and prefer offensive security rather than defensive security. **Ethics is an important topic in every information security related class.**

• Legalize the learning of different hacking tools in the Cybersecurity Club. **Have them sign codes of conduct.**

• Give students a sandbox environment to perform exercises while on campus **Encourage hands-on defensive exercises.**

• Invite speakers to address classes as an advocate for cyber-awareness / vaccination.
Academic Role in preparing the workforce

- Critical thinking
- IT troubleshooting
- Ethical Hacking
- Cutting-edge technology exposure
- Online team-based classroom games
- Real-time white hat/black hat competition
Recommendations

• Train your staff on good cyber-hygiene practices
• Participate in building next-gen security by collaborating with academia (e.g., FSU)
• Hire my students; they are ready and willing to serve!
Then What?

Next-generation theory and philosophical lens
Insider Threat: Trust, Deception and Computational Approach

Research that is...
Trust and action

- Trust is fundamental to relationships of all kinds. In particular, trust operates to set expectations within relationships.

- “...a generalized expectation...that the word, promise, oral or written statement of another individual or group can be relied on” (Ho and Benbasat 2014; Rotter, 1967, p. 1).

- Trustor is willing to take a risky action or make a risky decision with uncertain outcomes after he or she calculates the risks, and has determined the trustee to be trustworthy (Lewicki, R.J. and B.B. Bunker, 1996).
Collective Trust in Virtual Team Context

- Trust between two or more individuals is complex.

- It is the conscious decision of one actor to be dependent on another to various degrees based on circumstances (Zand, D.E., 1972).

- Individuals in groups are expected to fulfill their respective roles and responsibilities and contribute to the group's collective work in order to achieve collective goals (Kramer, R.M., et al., 1996).

- As successful teams rely on sustainable trust relationships, the ability to understand deceptive cues in a trust-enabled computer-mediated communication will better enable virtual teams to collaborate effectively.
Deceptive language-action cues

Deception in general refers to the active transmission of messages and information to create a false impression leading to a false conclusion (Buller, D.B. and J.K. Burgoon, 1996).

Cues available in face-to-face communication (F2F) (such as body language, facial expression, tone of voice etc.) are not always present in a more limited CMC environment (Ho et al., 2015a, 2015b, 2016a, 2016b).

Online communication is almost exclusively text-based, leaving people with only written words on which to base their trust decision.
Simulation of Multiple Insider Threat Scenarios

• **Hypothesis H1(a):** The language-action cues of a deceptive actor’s communications with his/her group will differ from those of a non-deceptive actor. **Not Supported**

• **Hypothesis H1(b):** The language-action cues used by a deceptive actor in communicating with his/her group will be different before an incentive for deception has been introduced to him/ and after it has been accepted by him/her. **Not Supported**

• **Hypotheses 2(H2):** Language-action features of communication within groups containing a deceptive actor will be significantly different from those in groups without a deceptive actor. **Supported**

• **Hypotheses 3(H3):** The language-action features of a group’s interactions will change after an actor within the group has accepted an incentive for deception. **Supported**
Simulation with Bigger Data collection — Saint vs Sinner
Simulation with Bigger Data collection — Saint vs Sinner
## Model Summary

<table>
<thead>
<tr>
<th>Model</th>
<th>$R$</th>
<th>$R^2$</th>
<th>Adjusted $R^2$</th>
<th>Std. Error of the Estimate</th>
<th>Change Statistics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$R^2$ Change</td>
<td>$F$ Change</td>
</tr>
<tr>
<td>1</td>
<td>.592&lt;sup&gt;a&lt;/sup&gt;</td>
<td>.351</td>
<td>.159</td>
<td>.461</td>
<td>.351</td>
<td>1.832</td>
</tr>
<tr>
<td>2</td>
<td>.559&lt;sup&gt;b&lt;/sup&gt;</td>
<td>.312</td>
<td>.164</td>
<td>.460</td>
<td>.312</td>
<td>2.109</td>
</tr>
<tr>
<td>3</td>
<td>.586&lt;sup&gt;c&lt;/sup&gt;</td>
<td>.344</td>
<td>.164</td>
<td>.460</td>
<td>.344</td>
<td>1.910</td>
</tr>
</tbody>
</table>

a. Predictors: (Constant), Time_lag, you, negemo, discrep, certain, WC, insight, posemo, cause, tentat, incl, excl, quant, l, negate, social, cogmech, affect
b. Predictors: (Constant), Time_lag, you, certain, WC, affect, tentat, quant, incl, excl, l, negate, cogmech, social, posemo
c. Predictors: (Constant), excl, WC, negemo, incl, insight, posemo, quant, l, discrep, certain, tentat, cause, negate, social, you, cogmech, affect
Decision Tree Learning
2D Support Vector Machine (SVM) Linear Kernel

Decision Boundary with linear kernel 70.00%

Decision Boundary with linear kernel 71.67%

- Sinner
- Saint
2D Support Vector Machine (SVM) RBF Kernel
3D Support Vector Machine (SVM) Linear Kernel

Trained with Linear Kernel 75.00%

- Sinner
- Saint
- Support Vectors
3D Support Vector Machine (SVM) RBF Kernel

Trained with rbf Kernel 81.67%

- Sinner
- Saint
- Support Vectors

- cogmech
- posemo
- timelag
How to Capture a Liar Computationally

- Based on the framework of trustworthiness attribution, we may be able to computationally identify deceptive behavior.

- This approach is to extract and process language-action features based on outlier behavior scenarios (data collected from an online human-computer interactive experiment) so as to establish attribution models of trustworthiness.

- A key novelty of our approach is the causality reasoning guided by social science theories on trust and attribution, rather than being only data-driven.

- Context-sensitive semantic aspects of words and resulting actions will be inferred jointly, along with causal inference of motives and other cognitive factors.

- This approach heuristically analyzes language in a context-sensitive human-computer interaction environment.

- Cutting-edge, high-risk, high-quality scientific innovation is required to bring along the transformative scientific impacts to both private and public sector commercialization.
Balancing security with privacy

• Multi-level analysis of data patterns as manifested in online communications

• Looking for anomalous behavior based on previously benchmarked information behavior AND accumulated meta-data

• Several algorithms on each level serve to “flag” certain scenario’s for elevation to next level

• Multiple layers of automated analysis are performed before any behavior (or communication text) actually comes to the attention of a security analyst


National Science Foundation (SaTC-1347113/Ho and 1347120/Hancock) **EAGER: Collaborative: Language-action causal graphs for trustworthiness attribution in computer-mediated communication,** $199,998, 09/01/13-08/31/15.
thank you!

Dr. Shuyuan Mary Ho
Florida State University

Florida Center for Cybersecurity