Welcome To The 10th Annual Hacking Conference
Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session on the app!

2002-2005 US Naval Postgraduate School Network Security
Group Division Officer
sk3wl 0f r00t team member

2003-2008: InfoWorld Test Center
Contributing Product Reviewer – Network and Information Security

2005-2012 DoD Security, Data & Workflow Consultant

2012-2016: Consulting Security Architect for Lancope then
Cisco Systems

2016 CTO & co-founder at WitFoo
Disclaimer

Information in this presentation is intended to protect against illegal or harmful social engineering and human manipulation or to be used in benevolent endeavors.

Please do good and obey the law.
Old School Social Engineering

• Based on “Confidence Games” (Cons)
• Target a “mark” to achieve inappropriate action
• Requires understanding of “mark” (agent)
• Manipulates existing human vulnerability
Second Generation Social Engineering

- Bulk, mass attacks
- Phishing
- Robocalls
Social Engineering with ML

• Need the Cohort (not a specific agent) to take action
• Long term training will transform agent values (create vulnerability)

They talk of a man betraying his country, his friends, his sweetheart. There must be a moral bond first. All a man can betray is his conscience.

Joseph Conrad
Relentless Manipulation

• “We’ve created a world in which online connection has become primary. Especially for younger generations. And yet, in that world, anytime two people connect, the only way it’s financed is through a sneaky third person who’s paying to manipulate those two people. So, we’ve created an entire global generation of people who were raised within a context with the very meaning of communication, the very meaning of culture, is manipulation.” – Jaron Lainer in The Social Dilemma
Machine Learning Basics
Supervised Learning

Input: Age: 3

Model:

Data:

<table>
<thead>
<tr>
<th>Age</th>
<th>Height</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>20”</td>
</tr>
<tr>
<td>5</td>
<td>38”</td>
</tr>
<tr>
<td>20</td>
<td>72”</td>
</tr>
<tr>
<td>50</td>
<td>72”</td>
</tr>
</tbody>
</table>

Output: Height: 29”

Confirmation / Action
Data and Models
Common Models

• *Naive Bayes*
• Nearest Neighbor
• Decision Trees
• Linear Regression
• Support Vector Machines (SVM)
• Neural Networks

https://towardsdatascience.com/types-of-machine-learning-algorithms-you-should-know-953a08248861
Naïve Bayesian Python

- https://machinelearningmastery.com/naive-bayes-classifier-scratch-python/
Reinforcement Learning

Agent

Content/Output

Reward

Model

Action/Input
A/B Testing of Output / Signal / Content

32%

8%

82%
Types of Content

• Text Ad
• Video Ad
• Promoted Pages
• Email
• Snail Mail
• Images
Message Considerations

- Alignment with Values
- Suspicion Triggers
- Language & Dialect Use
- Use of Nostalgia
- Trauma Triggers (Crossing a line)
- Bias Reinforcement
- Trusted Corroboration
- Social Corroboration
- Pain vs. Reward
A/B Testing of Action

14%

82%

31%
Types of Actions

• Click to Page
• Watch Video
• Play Game
• Fill out Form
• Join a Group
• Install an Application
• Comment / Engage
A/B Testing of Reward

96% → [Female] → [Gold Trophy]
3% → [Female] → [Silver Trophy]
31% → [Female] → [Bronze Trophy]
Types of Reward

- Public Praise – like, retweet, comment
- Artificial Prize - badge, points
- Physical Prize - cash, gift card, prize, beer, meal
- Education Credit – CEU, certification
- Celebrity Interaction – virtual or physical
- Promise of job
- Romantic Relationship or Encounter
- Confirmation Reinforcement
Cohort Targeting
Common Cohort Dimensions

- Gender
- Age
- Ethnicity
- Religious Belief
- Income
- Location
- Family Status
- Job Type

- Employer Type
- Education Level
- Affiliations
- Relationships
- Entertainment
- Credit Rating
- Net Worth
- Political Association
Facebook Audiences

Locations
United States

Detailed Targeting
Include people who match

Behaviors > Education
Demographics > Education
College grad

Interests > Additional Interests
Grand Rapids, Michigan
The Hacking Universe

Behaviors > Music

Income
Household income: top 10% of ZIP codes (US)
Household income: top 10%-25% of ZIP codes (US)
Household income: top 25%-50% of ZIP codes (US)
Household income: top 5% of ZIP codes (US)

Work
Employers
Industries
Job Titles

Soccer
Friends of Soccer fans
Soccer fans (high content engagement)
Soccer fans (moderate content engagement)
LinkedIn Audience

Who is your target audience?

Include people who have ANY of the following attributes:

Member Interests
Open Source Software

AND also have ANY of the following attributes:

Job Titles (Current)
Software Engineer

AND also have ANY of the following attributes:

Company (Current Jobs)
Steelcase

Narrow audience further

Exclude people by audience attributes and Matched Audiences

LinkedIn tools may not be used to discriminate based on personal characteristics like gender, age, or actual or perceived race/ethnicity. Learn more

Useable on Bing Search
Google Audience
Other Sources of Information

• Breach Data (Cambridge Analytica, etc)
• Intellius
• Scraping Social Media Sites
• Public Records
Cohort Collison vs Relationship

- Male
- F500 Employee
- Software Dev
- GitHub Account

- Member of OSS Lovers
- 1st Connect
- Microsoft
- Male
Launching Campaigns
Humans Move Slowly

Sales cycles as detailed here can take **months or years** to complete as agents progress through the process.

Successful progressions will have small, incremental steps requiring the lowest amount of agent change per stage.
Agent Transformation

- Bias Reinforcement
- Influence Action
- Influence Thought
Key Tracking Metrics

- Agent ID (Preferred) or Cohort ID
- Content ID
- Action ID
- Action State
- Proposed Reward ID

Behavior Flow Analysis
Improving Cohort Definitions

• What characteristics are shared among funnel exits?
• Are those characteristics missing in continuations?
• Tracking interaction counts to conversion

<table>
<thead>
<tr>
<th>ID</th>
<th>Age</th>
<th>Politics</th>
<th>Income</th>
<th>Role</th>
<th>Music</th>
</tr>
</thead>
<tbody>
<tr>
<td>1003</td>
<td>57</td>
<td>Near Left</td>
<td>$120k</td>
<td>PM</td>
<td>EDM</td>
</tr>
<tr>
<td>1198</td>
<td>45</td>
<td>Far Left</td>
<td>$200k</td>
<td>Exec</td>
<td>EDM</td>
</tr>
<tr>
<td>2876</td>
<td>33</td>
<td>Near Right</td>
<td>$85k</td>
<td>Dev</td>
<td>EDM</td>
</tr>
</tbody>
</table>
Multi-stage Cultivation

Obtain Followership

Level 1 Exposure

1st Action

Level 2 Exposure
Maintaining a Campaign

- Data Mining for Cohort Definition
- Large, diverse, effective content
- Ability to maintain audience (Groups, followers, mail lists, games)
- A/B testing of action delivery
- Reward types
- Decent Model (Naive Bayes)
- Growing Dataset for Model
- Detection Avoidance
Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session on the app!