Safeguarding Academic Accounts and Resources with the University Credential Abuse Auditing System

Jing Zhang\textsuperscript{1}, Robin Berthier\textsuperscript{2}, Will Rhee\textsuperscript{1}, Michael Bailey\textsuperscript{1}, Partha Pal\textsuperscript{3}, Farnam Jahanian\textsuperscript{1}, and William H. Sanders\textsuperscript{2}

\textsuperscript{1}University of Michigan  
\textsuperscript{2}University of Illinois at Urbana-Champaign  
\textsuperscript{3}BBN Technologies, Cambridge, MA
About the Research

• Who we are?
  
  Network and Security Research Group at University of Michigan

  Performability Engineering Research Group at the University of Illinois at Urbana-Champaign

• What we do?
  
  We are happy to talk with security officers and operational teams

• What is interesting?
  
  Some people steal university accounts to access the library.

- 613 incidents related to unauthorized use of university accounts during 2010 and first 6 months of 2011 at UofM
- 26 compromised accounts were reported in the first half of 2011 at UIUC
Why is it interesting?

• What is known to us?

Financial data is routinely topping the list of stolen data

Anti-Phishing Working Group trend report 2011-1H

<table>
<thead>
<tr>
<th>Country</th>
<th>Institutions (#)</th>
<th>Accounts (#)</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>60</td>
<td>4,287</td>
</tr>
<tr>
<td>IT</td>
<td>34</td>
<td>1,459</td>
</tr>
<tr>
<td>DE</td>
<td>122</td>
<td>641</td>
</tr>
<tr>
<td>ES</td>
<td>18</td>
<td>228</td>
</tr>
<tr>
<td>PL</td>
<td>14</td>
<td>102</td>
</tr>
<tr>
<td>Other</td>
<td>162</td>
<td>1,593</td>
</tr>
<tr>
<td>Total</td>
<td>410</td>
<td>8,310</td>
</tr>
</tbody>
</table>

A malware takeover research revealed that Torpig obtained 8,310 credentials at 410 institutions in ten days. Top targeted institutions: PayPal, Poste Italiane, Capotal One, Etread, and Chase.

• What is surprising?

• University accounts?!
• Library and VPN?!
New Attack Motivation

- What did they do with the compromised accounts?
  Netflow data analysis
  - Library website repeatedly visited
  - 8.2% of HTTP flows visited consist of 10 websites blocked in China
  - Login to accounts at 7 universities

- Market place for the compromised university accounts
  - 500 RMB ~ less than 100 USD = access to multiple databases for a year
  - $20 = UofM account with VPN and Library access

New motivation of attackers who steal university credentials:

Free and unfettered access to information
Anomaly and Fraud Detection

- **Goal**
  - Detect compromised accounts
  - Shorten the detection period
  - Prevent further abuse
  - Protect university resources and reputation
  - Invisible to end users
  - Limited manpower

- **Machine-learning techniques**
  - Successfully used for anomaly and fraud detection
  - Credit card fraud \([e.g., \text{Aleskerov}'97, \text{Chen}'05, \text{Panigrahi}'09]\)
  - Telecommunication fraud \([e.g., \text{Cox}'97, \text{Phua}'04, \text{Agarwal}'05]\)
  - Computer and network intrusion \([e.g., \text{Brutlag}'00, \text{Heller}'03, \text{Esponda}'04]\)
  - Malicious domain and URL \([e.g., \text{Ma}'09, \text{Whittaker}'10, \text{Antonakakis}'11]\)
Agenda

1. University Credential Abuse Auditing System (UCAAS)

2. Evaluation
   - Feature Evaluation
   - Model Evaluation
   - Empirical Evaluation

3. Discussion and Future work
Agenda

1. University Credential Abuse Auditing System (UCAAS)

2. Evaluation
   - Feature Evaluation
   - Model Evaluation
   - Empirical Evaluation

3. Discussion and Future work
UCAAS – Architecture

- **Training Data** → **Training** → **Classifier Model** → **Classification** → **Detection Output**

- **Feature Extraction** → **Classification**

- **Authentication Logs** → **Feature Extraction**

- **Final Results** → **Verify**
UCAAS – Architecture

1. **Training Data**
   - **Training**
   - **Classifier Model**

2. **Feature Extraction**
   - **Classification**

3. **Authentication Logs**
   - **Detection Output**
   - **Verify**
   - **Final Results**
### University Authentication Infrastructure

<table>
<thead>
<tr>
<th>UserID</th>
<th>Time</th>
<th>Service Type</th>
<th>Event Type</th>
<th>Original IP</th>
<th>Desc</th>
</tr>
</thead>
<tbody>
<tr>
<td>User A</td>
<td>2011-06-01 10:01:48</td>
<td>Web service</td>
<td>Logon Failure</td>
<td>1.2.3.4</td>
<td>Webmail</td>
</tr>
<tr>
<td>User B</td>
<td>2011-06-01 10:02:10</td>
<td>VPN</td>
<td>Logon OK</td>
<td>1.2.3.5</td>
<td></td>
</tr>
<tr>
<td>User B</td>
<td>2011-06-01 10:03:01</td>
<td>Web Service</td>
<td>Logon OK</td>
<td>1.2.3.6</td>
<td>Ctools</td>
</tr>
<tr>
<td>User C</td>
<td>2011-06-01 10:04:23</td>
<td>Wireless</td>
<td>Logon OK</td>
<td>1.2.3.7</td>
<td></td>
</tr>
</tbody>
</table>

Web-service and VPN logs are used in UCAAS
UCAAS – Architecture

Feature selection:
- Several-years experiences of security officers
- Thorough analysis on the incidents in past 3 years
Suspicious Behavior Features

- **Temporal-Spatial Violation**
  - Activities of account owner and attackers are independent
  - Inconsistencies in the location and time of activities

Impossible to travel from the U.S. to China in an hour!
Suspicious Behavior Features

- Temporal-Spatial Violation
  - Activities of account owner and attackers are independent.
  - Inconsistencies in the location and time of activities

- Suspicious IP Address
  - Attacker tests multiple stolen accounts
  - More than half of compromised account in 2009 and 2010 were accessed by those malicious IP addresses

<table>
<thead>
<tr>
<th>UserID</th>
<th>Time</th>
<th>Service Type</th>
<th>Event Type</th>
<th>Original IP</th>
<th>Desc</th>
</tr>
</thead>
<tbody>
<tr>
<td>User A</td>
<td>2011-06-01 10:01:48</td>
<td>VPN</td>
<td>Logon OK</td>
<td>121.227.32.232</td>
<td></td>
</tr>
<tr>
<td>User B</td>
<td>2011-06-01 10:02:10</td>
<td>VPN</td>
<td>Logon Failure</td>
<td>121.227.32.232</td>
<td></td>
</tr>
<tr>
<td>User C</td>
<td>2011-06-01 10:03:01</td>
<td>VPN</td>
<td>Logon OK</td>
<td>121.227.32.232</td>
<td></td>
</tr>
<tr>
<td>User D</td>
<td>2011-06-01 10:04:23</td>
<td>VPN</td>
<td>Logon OK</td>
<td>121.227.32.232</td>
<td></td>
</tr>
</tbody>
</table>
Suspicious Behavior Features

- **Temporal-Spatial Violation**
  - Activities of account owner and attackers are independent.
  - Inconsistencies in the location and time of activities

- **Suspicious IP Address**
  - Attacker tests multiple stolen accounts
  - More than half of compromised accounts in 2009 and 2010 were accessed by those malicious IP addresses

- **Suspicious Usage Pattern**
  - Aim at inactive accounts used only by illegitimate attackers.
  - Abuse VPN and library resources
Profile-based Features

- Illegitimate activities will not match the habits of account owner

- **Profile Fitness**
  - The probability that the new activity fits in the historical usage pattern
  - For a new authentication attempt on Sunday, the fitness score is 2.8%

Sample user profile built over a week of activity

<table>
<thead>
<tr>
<th>Feature</th>
<th>Time of the Day</th>
<th>Day of the Week</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>00:00–04:00: 3%</td>
<td>Monday: 17.2%</td>
</tr>
<tr>
<td></td>
<td>04:00–08:00: 7%</td>
<td>Tuesday: 12.2%</td>
</tr>
<tr>
<td></td>
<td>08:00–12:00: 30%</td>
<td>Wednesday: 21.0%</td>
</tr>
<tr>
<td></td>
<td>12:00–16:00: 40%</td>
<td>Thursday: 19.0%</td>
</tr>
<tr>
<td></td>
<td>16:00–20:00: 15%</td>
<td>Friday: 20.0%</td>
</tr>
<tr>
<td></td>
<td>20:00–00:00: 5%</td>
<td>Saturday: 7.8%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sunday: 2.8%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Feature</th>
<th>Domain Names</th>
<th>ASN</th>
<th>Country Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>example.com: 86.9%</td>
<td>27432: 79.6%</td>
<td>US: 91.2%</td>
</tr>
<tr>
<td></td>
<td>example.net: 9.1%</td>
<td>123: 20.4%</td>
<td>CN: 8.8%</td>
</tr>
<tr>
<td></td>
<td>example.org: 4.0%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Feature</th>
<th>Usage Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>VPN: 22.3%</td>
</tr>
<tr>
<td></td>
<td>Wireless: 77.7%</td>
</tr>
</tbody>
</table>
Additional Features

• IP Address-based Features
  ▪ Geographic location
  ▪ Autonomous System Number (ASN)
  ▪ Host name

• Resource Usage-based Features
  ▪ Number and ratio of VPN and Web authentication attempts
  ▪ Number and ratio of websites visited
Feature Vector

1,0,1,0.95,0.08,1.00,…,0,0,1,0,0,…,0,0,0,1,0,…,6,14,0.3,0.7

<table>
<thead>
<tr>
<th>Feature</th>
<th>Number of Bits</th>
<th>Value Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspicious Behavior</td>
<td>3</td>
<td>binary</td>
</tr>
<tr>
<td>Profile-based</td>
<td>5</td>
<td>0 – 100%</td>
</tr>
<tr>
<td>Geolocation (Country code)</td>
<td>238</td>
<td>binary</td>
</tr>
<tr>
<td>Topological (ASN)</td>
<td>65535</td>
<td>binary</td>
</tr>
<tr>
<td>Resource - Number</td>
<td>552</td>
<td>integer</td>
</tr>
<tr>
<td>Resource - Ratio</td>
<td>552</td>
<td>0 – 100%</td>
</tr>
</tbody>
</table>
UCAAS – Architecture

- Training Data
- Training
- Classifier Model
- Feature Extraction
- Authentication Logs
- Classification
- Detection Output
- Verify
- Final Results
Classifier

• Logistic Regression in Weka
  - The dependent variable is dichotomous: data coded as 1 (true) or 0 (false)
  - Estimated regression model:
    \[ L = a + \sum B_i X_i. \]
  - \( L \) is the natural logarithm of the odds that the events represented by the dependent variable happens.
    \[ L = \ln \frac{\hat{p}}{1 - \hat{p}}. \]
  - \( \hat{p} \) is the probability that the characteristic variable is true
Agenda

1. University Credential Abuse Auditing System (UCAAS)

2. Evaluation
   - Feature Evaluation
   - Model Evaluation
   - Empirical Evaluation

3. Discussion and Future work
Datasets

Training set

• *UofM*
  - June 14 – 28, 2011
  - 108,366 unique users
  - 2,129,275 authentication attempts
  - After filtering out users who did not have VPN/Library related activities and validation:
    - 2,441 benign users
    - 87 compromised accounts

• *UIUC*
  - June 19 – July 2, 2011
  - 25,530 unique users
  - 104,172 successful logins
  - After filtering and validation:
    - 4,692 benign users
    - 6 compromised accounts
Datasets

Training set

- **UofM**
  - June 14 – 28, 2011
  - 108,366 unique users
  - 2,129,275 authentication attempts
  - After filtering out users who did not have VPN/Library related activities and validation:
    - 2,441 benign users
    - 87 compromised accounts

- **UIUC**
  - June 19 – July 2, 2011
  - 25,530 unique users
  - 104,172 successful logins
  - After filtering and validation:
    - 4,692 benign users
    - 6 compromised accounts

How to obtain the ground truth?
- Known incidents
- Manual evaluation
Agenda

1. University Credential Abuse Auditing System (UCAAS)

2. Evaluation
   - Feature Evaluation
   - Model Evaluation
   - Empirical Evaluation

3. Discussion and Future work
## Suspicious Behavior Features

- **UofM**

<table>
<thead>
<tr>
<th>Suspicious Behavior</th>
<th>Success in benign users</th>
<th>Success in compromised users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temporal-Spatial Violation</td>
<td>1.74%</td>
<td>42.08%</td>
</tr>
<tr>
<td>Suspicious IP Address</td>
<td>1.67%</td>
<td>0.00%</td>
</tr>
<tr>
<td>Suspicious Usage Pattern</td>
<td>18.03%</td>
<td>37.60%</td>
</tr>
</tbody>
</table>

- **UIUC**

<table>
<thead>
<tr>
<th>Suspicious Behavior</th>
<th>Success in benign users</th>
<th>Success in compromised users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temporal-Spatial Violation</td>
<td>0.32%</td>
<td>11.88%</td>
</tr>
<tr>
<td>Suspicious IP Address</td>
<td>0.24%</td>
<td>2.43%</td>
</tr>
<tr>
<td>Suspicious Usage Pattern</td>
<td>72.97%</td>
<td>75.10%</td>
</tr>
</tbody>
</table>
Are the Profile-based Features Useful?

Complementary cumulative distribution (CCDF) of Profile Fitness Features

Country Code
AS Number
Domain Name

Day of the week
Time of the day
Resource Usage

Less useful features
Are the Profile-based Features Universal?
Other features

• IP Geographic Location
  - A large proportion of malicious login attempts came from China and Iran
  - Login activities from the U.S. were usually legitimate

• Autonomous System Number
  - Lots of malicious activities originated from the China-Telecom AS
  - Activities from local operator ASes and University ASes were more likely to be benign

• Resource Usage Features
  - VPN and Library resources are heavily abused by attackers
  - Benign users use web-based resources more frequently
Agenda

1. University Credential Abuse Auditing System (UCAAS)

2. Evaluation
   - Feature Evaluation
   - Model Evaluation
   - Empirical Evaluation

3. Discussion and Future work
Jing Zhang

DSN’2012: Safeguarding Academic Accounts and Resources with the University Credential Abuse Auditing System

ROC Curve

- **UofM**

Average # of VPN users per day $\sim$ 1,000
Max # of false alarms per day = 2
FPR = 0.2%

**FPR = 0.2%**
**TPR = 95.4%**
**Window size = 11 days**

---

FPR = 0.2%
TPR = 95.4%
Window size = 11 days
Jing Zhang

DSN'2012: Safeguarding Academic Accounts and Resources with the University Credential Abuse Auditing System

ROC Curve

- **UIUC**

![ROC Curve Diagram]

- **FPR = 0.2%**
- **TPR = 100%**
- **Window size = 9 or 11 days**
Agenda

1. University Credential Abuse Auditing System (UCAAS)

2. Evaluation
   - Feature Evaluation
   - Model Evaluation
   - Empirical Evaluation

3. Discussion and Future work
Empirical Evaluation

Apply the model built with training dataset into real operation

- **UofM**
  - Two weeks from September 14, 2011
  - 126 unique users are flagged by UCAAS
    - **124 are confirmed to be compromised**
    - 2 accounts had been shared with family members living in a foreign country

- **UIUC**
  - July 9 - July 23, 2011
  - 11 unique users are flagged by UCAAS
    - **One is confirmed to be compromised**
    - The other 10 are overlapped with training set
Empirical Evaluation

Apply the model built with training dataset into real operation

- **UofM**
  - Two weeks from September 14, 2011
  - 126 unique users are flagged by UCAAS
    - 124 are confirmed to be compromised
    - 2 accounts had been shared with family members living in a foreign country

- **UIUC**
  - July 9 - July 23, 2011
  - 11 unique users are flagged by UCAAS
    - One is confirmed to be compromised
    - The other 10 are overlapped with training set

It's gratifying our project has already made a tangible, positive, real-world difference: because of your research we’re now finding more compromised accounts *proactively* than we find as a result of reacting to abuse complaints. I feel like we’re starting to get ahead of the curve.

- Will Rhee
  Information technology User Advocate
Agenda

1. University Credential Abuse Auditing System (UCAAS)

2. Evaluation
   - Feature Evaluation
   - Model Evaluation
   - Empirical Evaluation

3. Discussion and Future work
Conclusion

• Contribution
  - Confirm the techniques also work well in this new problem domain
  - Universal and distinct findings at two different universities

• Future Work
  - More experience on both universities and productionize the system
  - Mitigate compromised accounts through prevention approaches
Thanks!