Building the UA/Eller/MIS AZSecure Cybersecurity Analytics Program: My Journey

Hsinchun Chen, Ph. D.
Regents’ Professor, Thomas R. Brown Chair
Director, AI Lab, AZSecure Cybersecurity Program
Fellow, ACM, IEEE, AAAS
University of Arizona
U of Maryland Seminar, October 1, 2021

Funding Acknowledgements: NSF (SaTC, SFS, ACI)
Outline

• Security Informatics & Analytics: COPLINK, BorderSafe, Dark Web

• Azsecure Cybersecurity Analytics:
  (1) Dark Web Analytics for studying international hacker community, forums, and markets;
  (2) Privacy and PII (Personally Identifiable Information) Analytics for identifying and alleviating privacy risks for vulnerable populations;
  (3) Adversarial Malware Generation and Evasion for adversarial AI in cybersecurity; and
  (4) Smart Vulnerability Assessment for scientific workflows and OSS (Open Source Software) vulnerability analytics and mitigation.

• Some Advice
Computational Design Science Research
at UA/Eller/MIS AI Lab

• Applications/problems: digital libraries, search engines, biomedical informatics, healthcare data mining, security informatics, business intelligence, cybersecurity analytics

• Approaches: web collection/spidering, databases, data warehousing, data mining, text mining, web mining, statistical NLP, machine learning, deep learning, ontologies, social media analytics, interface design, information visualization, economic modeling, assessment

• Structure: federal funding (NSF/DOD/NIH), director, affiliated faculty, post-docs, Ph.D./MS/BS students ➔ tech transfer, commercialization

• Major phases: DLI ➔ COPLINK ➔ Dark Web ➔ AZSecure
Security Informatics & Analytics: COPLINK & Dark Web
DLI: Visualization Research in AI Lab

From YAHOO! To OOHAY?

Object Oriented Hierarchical Automatic Yellowpage
Visualization Research in AI Lab

OOHAY: Visualizing the Web
Cancer Map: 2M CancerLit articles, 1500 maps (OOHAY, DLI)
大腸直腸癌

近年來因經濟的起飛，人口結構的老化，加上生活型態的改變，西式飲食的盛行，導致台灣地區之大腸直腸癌發生率及死亡率節節上揚。就死亡率而言，大腸直腸癌目前已是台灣地區因惡性腫瘤死亡人口的第三位，僅次於肝癌及肺癌。不論在我國或先進國家，大腸直腸癌已是今日公共衛生重要的一環。近年來有關大腸直腸癌的流行病學研究甚多，其中較具體的結論是遺傳與飲食。

我們大概可以說家族一等親中若有人得到大腸直腸癌，則其一生中得到相同癌症的機會約為一般人的三倍。目前公認纖維質食物攝取太少，以及攝取太多的肉類，由於會導致大便通過大腸的平均時拉長，所以致癌的機會也會大增。就大腸直腸癌病變而言，
Global Security Impacts

• “War on terror” (Iraq and Afghanistan) surpassed cost of Second World War, $5 trillion...Time Magazine

• Hacker costing $1 trillion globally... President Obama
From the Surface Web to the Dark Web

- Surface Web
- Deep Web
- Dark Web
- DarkNet
- Hacker Web
COPLINK: Crime Data Mining (1997-2009)
COPLINK Identity Resolution and Criminal Network Analysis

Cross-jurisdictional Information Sharing/Collaboration

Arizona IDMatcher

Law-enforcement Data
AZ CA TX

Border Crossing Data (AZ, CA, TX)
Vehicles People

CAN Visualizer

Identity Resolution
Detect false and deceptive identities across jurisdictions using a probabilistic naive-Bayes based resolution system.

Criminal Network Analysis

High-risk Vehicle Identification
Identify high-risk vehicles using association techniques like mutual information using border crossing and law enforcement data.

Criminal Link Prediction
Predict interaction between individuals and vehicles using link prediction techniques to identify high-risk border crossers.

Suspect Traffic Burst Detection
Detect real-time anomalies and threats in border traffic using Markov switching and other models.

* Only the grayed datasets are available to the AI Lab
**COPLINK: Crime Data Mining**

ABC News  April 15, 2003

Google for Cops: Coplink software helps police search for cyber clues to bust criminals

**IBM i2 COPLINK**

*Accelerating law enforcement investigations*

$54B, IPO 2020
Dark Web: Countering Terrorism (2003-2014)

- Dark Web: Terrorists’ and cyber criminals’ use of the Internet
- Collection: Web sites, forums, blogs, YouTube, etc.
- 20 TBs in size, with close to 10B pages/files/messages (the entire LOC collection: 15 TBs)
Arabic Writeprint Feature for Authorship Analysis

Feature Set

Lexical
- Char-Based
  - Letter Frequency
  - Specific Char
  - Word-Level
  - Word Length Dist.
  - Elongation
  - (48)
- Word-Based
  - Special Char.
  - Word Richness
  - Vocab. Richness
  - (31)
- Punctuation
  - (12)
- Function Words
  - (200)
- Word Roots
  - (50)
- Word Structure
  - (14)
- Technical Structure
  - (15)
  - Race/Nationality
  - Violence
  - (11)
  - (4)

Syntactic
- Message Level
  - (5)
- Paragraph Level
  - (6)
- Contact Information
  - (3)
- Font Color
  - (29)
- Font Size
  - (8)
- Embedded Images
  - (4)
- Hyperlinks
  - (7)
  - (418)

Structural
- (62)

Content Specific
- (48)

Specific Feature Set
- (418)
Arabic Feature Extraction Component

1. Incoming Message

2. Elongation Filter

Filtered Message

3. Root Clustering Algorithm

Root Dictionary

4. Generic Feature Extractor

Feature Set

- Similarity Scores (SC)
  - أنجاز: 0.54
  - أنقلل: 0.21
  - أنقلل: 0.31

- All Remaining Features Values

- max(SC) + 1

- Count + 1

- Degree + 5
CyberGate (Abbasi, et al., MISQ, 2008)
The Dark Web project in the Press

Project Seeks to Track Terror Web Posts, 11/11/2007

Researchers say tool could trace online posts to terrorists, 11/11/2007

Mathematicians Work to Help Track Terrorist Activity, 9/14/2007
• Intelligence and Security Informatics (ISI) (Chen, 2006)

• Data, text, and web mining

• From COPLINK to Dark Web

• IEEE ISI, EISIC, PAISI ➔ 4000+ scholars, since 2003
Selected TOC:

- Forum Spidering
- Link and Content Analysis
- Dark Network Analysis
- Interactional Coherence Analysis
- Dark Web Attribution System
- Authorship Analysis
- Sentiment Analysis
- Affect Analysis
- CyberGate Visualization
- Dark Web Forum Portal
- Case Studies: Jihadi Video Analysis, Extremist YouTube Videos, IEDs, WMDs, Women’s Forums
Fraud Cues

Table 2. Examples of Fraud Cues Incorporated in AZProtect

<table>
<thead>
<tr>
<th>Category</th>
<th>Attribute Group</th>
<th>Fraud Cues</th>
<th>Fake Site Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web page text</td>
<td>Word phrases</td>
<td>&quot;member FDIC&quot; , &quot;about FDIC&quot;</td>
<td>Concealed</td>
<td>References to Federal Deposit Insurance Corporation rarely appear in concealed bank websites.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;what is FDIC&quot; , &quot;FDIC&quot;</td>
<td>Concealed</td>
<td>Concealed copyrights often appear in concealed websites.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;fee calculator&quot;</td>
<td>Concealed</td>
<td>Concealed cargo delivery websites provide competitive phony estimates to customers. Legitimate sites typically offer estimates in-person through sales representatives.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;pay by phone&quot; , &quot;call toll free&quot;</td>
<td>Concealed</td>
<td>Fraudsters prefer to engage in online transactions. They rarely offer phone-based payment options.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;password management&quot;</td>
<td>Concealed</td>
<td>Concealed websites do not provide considerable support for returning customers since they generally do not have any.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;enter your account&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lexical measures</td>
<td>Average sentence length</td>
<td>Concealed</td>
<td></td>
<td>Sentences in concealed websites tend to be two to three times longer than ones in legitimate sites.</td>
</tr>
<tr>
<td></td>
<td>Average word length, frequency of long words</td>
<td>Concealed</td>
<td></td>
<td>Concealed websites often contain concatenated words (e.g., &quot;groundtransport&quot; and &quot;safetybankingcenter&quot;), resulting in unusually lengthy words.</td>
</tr>
<tr>
<td></td>
<td>Average number of words per page</td>
<td>Concealed</td>
<td></td>
<td>Concealed websites pages are more verbose than legitimate sites—containing twice as many words per page, on average.</td>
</tr>
<tr>
<td>Spelling and grammar</td>
<td>&quot;Adobe Acrobat&quot;</td>
<td>Concealed</td>
<td></td>
<td>Concealed web pages contain many misspellings and grammatical mistakes.</td>
</tr>
<tr>
<td></td>
<td>&quot;fraudulent&quot;</td>
<td>Concealed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;never the&quot;</td>
<td>Concealed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;think forwarder&quot;</td>
<td>Concealed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>URLs</td>
<td>&quot;HTTP&quot;</td>
<td>Concealed, Spoof</td>
<td></td>
<td>Fake websites rarely use the secure sockets layer protocol.</td>
</tr>
<tr>
<td></td>
<td>Random characters in URLs (e.g., &quot;spider&quot;, &quot;spiderbot&quot;)</td>
<td>Concealed, Spoof</td>
<td></td>
<td>Since fake websites are mass produced, they use random characters in URLs. It also allows new fake websites to easily circumvent lookup systems that rely on blacklists of exist URLs.</td>
</tr>
<tr>
<td></td>
<td>Number of slashes (/) in URL</td>
<td>Spoof</td>
<td></td>
<td>Spoof sites often piggyback off of legitimate websites or third-party hosts. The spoofers are buried deep on these websites servers.</td>
</tr>
<tr>
<td>Anchor Text</td>
<td>Errors in the URL descriptions (e.g. &quot;conclude&quot;)</td>
<td>Concealed</td>
<td></td>
<td>Anchor text is used to describe links in web pages. Concealed websites occasionally contain misspelled or inaccurate anchor text descriptions.</td>
</tr>
<tr>
<td>Source Code</td>
<td>HTML and JavaScript commands</td>
<td>Concealed, Spoof</td>
<td></td>
<td>This HTML command is used to transmit code. It often appears in pages that are unsecured (i.e., &quot;HTTP&quot; instead of &quot;HTTPS&quot;).</td>
</tr>
<tr>
<td></td>
<td>&quot;METHOD POST&quot;</td>
<td>Concealed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Image Preloading</td>
<td>Concealed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;&lt;a href=&quot; http://&quot;</td>
<td>Concealed, Spoof</td>
<td></td>
<td>Stylistic and syntactic elements in the source code can help identify automatically generated fake websites.</td>
</tr>
<tr>
<td>Images</td>
<td>&quot;//&quot; + &quot;// +&quot; + &quot;//&quot; +&quot; /&quot; +&quot; /&quot;</td>
<td>Concealed, Spoof</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>File name, file extension, format, file size</td>
<td>Concealed, Spoof</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pixel colors</td>
<td>Concealed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linkage</td>
<td>Number of input links</td>
<td>Concealed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Number of links, number of absolute/relative links</td>
<td>Concealed, Spoof</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Escrow Kernel for Detecting Fake Web Sites

Represent each page \(a\) with the vectors:

\[ x_a = (\text{Sim}_{x_1}(a, b_1), ..., \text{Sim}_{x_m}(a, b_m); y_a = (\text{Sim}_{y_1}(a, b_1), ..., \text{Sim}_{y_n}(a, b_n)) \]

Where:

\[
\text{Sim}(a, k) = \lambda \left( \frac{1}{l_v + l_v} \sum_{i=1}^{l_v} \left( 1 - \frac{\text{in}_a - \text{in}_i}{\text{in}_a + \text{in}_i} \right) + \left( 1 - \frac{\text{out}_a - \text{out}_i}{\text{out}_a + \text{out}_i} \right) \right) + (1 - \lambda) \left( 1 - \frac{1}{m} \sum_{k=1}^{m} |a - k| \right)
\]

\[
\text{Sim}_{x_i}(a, b) = \frac{1}{m} \sum_{k=1}^{m} \text{Sim}(a, k)
\]

\[
\text{Sim}_{y_i}(a, b) = \arg \max_k \text{Sim}(a, k)
\]

For:

\(p\) web sites in the training set; \(k \in m\) pages in site \(b\); \(a_1, ..., a_n\) and \(k_1, ..., k_m\) are page \(a\) and \(k\)'s feature vectors;

\(l_v, \text{in}_a, \text{in}_i\) and \(\text{out}_a, \text{out}_i\) are the page level and number of in/out links for page \(a\);

The similarity between two pages is defined as the inner product between their two vectors \(x_1, x_2\) and \(y_1, y_2\):

\[
\text{Linear Composite Kernel: } K(x_1, y_1, x_2, y_2) = \frac{(x_1, x_2)}{\sqrt{(x_1, x_1)} \cdot \sqrt{(y_1, y_1)}} + \frac{(y_1, y_2)}{\sqrt{(y_1, y_1)} \cdot \sqrt{(y_1, y_1)}}
\]

Figure 4. Linear Composite SVM Kernel for Fake Website Detection

<table>
<thead>
<tr>
<th>Category</th>
<th>Comparision Websites</th>
<th>Legitimate Web Page</th>
<th>Spoof Web Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sim_{x_i}(a, b)</td>
<td>Sim_{y_i}(a, b)</td>
<td>Sim_{x_i}(a, b)</td>
</tr>
<tr>
<td>Legitimate</td>
<td><a href="http://www.bankofamerica.com">www.bankofamerica.com</a></td>
<td>0.492096</td>
<td>1.000000</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.citibank.com">www.citibank.com</a></td>
<td>0.278434</td>
<td>0.577704</td>
</tr>
<tr>
<td>Fake</td>
<td>false</td>
<td>0.317638</td>
<td>0.353798</td>
</tr>
<tr>
<td></td>
<td>ebay</td>
<td>0.257576</td>
<td>0.297611</td>
</tr>
</tbody>
</table>

Figure 5. Comparing Two Web Pages Against Legitimate and Fake Websites
Performance vs. Classifier and Lookup Systems

### Table 3. Performance Results (%) for Classifier and Lookup Systems

<table>
<thead>
<tr>
<th>System</th>
<th>Overall Accuracy (n = 900)</th>
<th>Real Websites (n = 200)</th>
<th>Concocted Detection (n = 350)</th>
<th>Spoof Detection (n = 350)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AZProtect</td>
<td>92.56</td>
<td>85.21</td>
<td>76.29</td>
<td>96.50</td>
</tr>
<tr>
<td>eBay AG</td>
<td>44.89</td>
<td>44.64</td>
<td>28.73</td>
<td>100.00</td>
</tr>
<tr>
<td>Netcraft</td>
<td>83.00</td>
<td>72.13</td>
<td>56.74</td>
<td>99.00</td>
</tr>
<tr>
<td>SpoofGuard</td>
<td>70.00</td>
<td>57.28</td>
<td>41.90</td>
<td>90.50</td>
</tr>
<tr>
<td>EarthLink</td>
<td>42.67</td>
<td>43.55</td>
<td>27.87</td>
<td>99.50</td>
</tr>
<tr>
<td>IE Filter</td>
<td>55.33</td>
<td>49.87</td>
<td>33.22</td>
<td>100.00</td>
</tr>
<tr>
<td>FirePhish</td>
<td>54.89</td>
<td>49.63</td>
<td>33.00</td>
<td>100.00</td>
</tr>
<tr>
<td>Sitehound</td>
<td>47.33</td>
<td>45.77</td>
<td>29.67</td>
<td>100.00</td>
</tr>
</tbody>
</table>

### Figure 8. ROC Curves for Classifier and Lookup Systems
### Table 6. Performance Results (%) for Various Learning-Based Classification Techniques

<table>
<thead>
<tr>
<th>Learning Technique</th>
<th>Overall Accuracy (n = 900)</th>
<th>Real Websites (n = 200)</th>
<th>Concocted Detection (n = 350)</th>
<th>Spoof Detection (n = 350)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVM</td>
<td>92.56</td>
<td>85.21</td>
<td>76.29</td>
<td>96.50</td>
</tr>
<tr>
<td>Logistic regression</td>
<td>89.00</td>
<td>78.53</td>
<td>69.36</td>
<td>90.50</td>
</tr>
<tr>
<td>J48 Decision Tree</td>
<td>88.77</td>
<td>75.66</td>
<td>73.01</td>
<td>78.50</td>
</tr>
<tr>
<td>Bayesian Network</td>
<td>88.56</td>
<td>77.27</td>
<td>69.18</td>
<td>87.50</td>
</tr>
<tr>
<td>Naive Bayes</td>
<td>77.67</td>
<td>63.12</td>
<td>49.86</td>
<td>86.00</td>
</tr>
<tr>
<td>Winnow</td>
<td>76.11</td>
<td>58.73</td>
<td>47.66</td>
<td>76.50</td>
</tr>
<tr>
<td>Neural Network</td>
<td>66.22</td>
<td>54.21</td>
<td>38.79</td>
<td>90.00</td>
</tr>
</tbody>
</table>

#### Figure 9. ROC Curves for Various Learning Classifiers
AZSecure Cybersecurity Analytics Program (2010-present): SaTC, SFS, ACI
Azsecure Cybersecurity Analytics Program:

(1) **Dark Web Analytics** for studying international hacker community, forums, and markets;

(2) **Privacy and PII (Personally Identifiable Information) Analytics** for identifying and alleviating privacy risks for vulnerable populations;

(3) **Adversarial Malware Generation and Evasion** for adversarial AI in cybersecurity; and

(4) **Smart Vulnerability Assessment** for scientific workflows and OSS (Open Source Software) vulnerability analytics and mitigation.
AI & Deep Learning: From AlphaGo to Autonomous Vehicles (2012-)

Hacker Web, AZSecure projects at UA/MIS AI Lab (2010-)
AI and Cybersecurity

• AI and Cybersecurity → not just buzzwords!
  • Noted as a national security priority by NSF, NSTC, and NAS.

• Role of AI for Cybersecurity:
  1. Automate common cybersecurity tasks
  2. Identify patterns in large datasets
AI for Cybersecurity – An Analytics Approach

Phase 1: Fundamental Cybersecurity Principles and Tasks
Description: Identify intelligence needs of organization, critical assets, and their vulnerabilities
Approaches: threat trending, vulnerability assessments, asset discovery, diamond modelling

Phase 2: Data Collection and Aggregation
Description: Identify and collect relevant data
Data sources: internal network data, external threat feeds, OSINT, human intelligence

Phase 3: AI-enabled Analytics
Description: Analyze collected data to develop relevant, timely, and actionable intelligence
Approaches: malware analysis, event correlation, ML, network science, DL

Phase 4: Knowledge Usage and Dissemination
Description: Mitigate threats and disseminate intelligence
Approaches: manual and automated threat responses, intelligence standards, visualizations
MOVING TOWARD BLACK HAT RESEARCH IN INFORMATION SYSTEMS SECURITY: AN EDITORIAL INTRODUCTION TO THE SPECIAL ISSUE

Black Hats Versus White Hats
Versus Grey Hats

What exactly is this white hat versus the black hat dichotomy? When making movies about the Old American West, filmmakers made a symbolic distinction at times between the good guys, wearing white hats, and the bad guys, wearing black hats. If, for the sake of our basic theme, we can adopt this distinction momentarily, we would like to go on to asseverate that the information systems field is heavily over-emphasizing research on white hats to the detriment of studies on black hats. It is easy to see how this would, quite naturally, occur. Scholars have better access to white hats, although even here, white hat managers do not typically want to share detailed information about their losses and have responded in this manner for some time (Hoffer and Straub 1989). Thus it is a reader’s access to data that has led information security researchers to gravitate toward white hat issues.

Whereas we could offer more extensive evidence of the prevalence of white hat IS research studies, a quick review of the papers in this special issue indicates that only the paper by Abbasi, Zhang, Zimbra, Chen, and Neumauer attempts to empirically represent the activities of black hats, but even with this representation, we are at arm’s length from black hat motivations and future dark plans.

We need to state unequivocally that our argument for more emphasis on the black hat type of research in no way diminishes the contributions of the white hat papers in this special issue.

Introduction

The MIS Quarterly Special Issue on Information Systems Security in the Digital Economy received a total of 80 manuscripts from which we accepted nine for publication in the Special Issue. To introduce the readers to the special issue papers, we have chosen to digest from the tradition of summarizing the papers in-depth and, instead, would like to take this opportunity to encourage researchers to conduct...
Dark Web Analytics: studying international hacker community, forums, and markets

* ACI, 2012-2017; SaTC 2013-2018; SFS-1, 2012-2018
* SaTC 2019-; SFS-2, 2019-
Hacker Web

**Forum post with source code to exploit Mozilla Firefox 3.5.3**

**Tutorial on how to create malicious documents**

**Attachment Name**: BlackPOS.rar
**Description of Attachment**: 5.4 KB, 143 views
## Selected data breaches in 2014

<table>
<thead>
<tr>
<th>Victim</th>
<th>Date</th>
<th>Ramification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target</td>
<td>2013.12</td>
<td>40M credit/debit cards; 70M customer records; 46% drop in annual profits (<strong>seller: Rescator</strong>)</td>
</tr>
<tr>
<td>Neiman Marcus</td>
<td>2014.3</td>
<td>282K credit/debit cards</td>
</tr>
<tr>
<td>Sally Beauty</td>
<td>2014.3</td>
<td>25K credit/debit cards</td>
</tr>
<tr>
<td>P.F. Chang</td>
<td>2014.6</td>
<td>8 month of customer data from 33 stores</td>
</tr>
<tr>
<td>J.P. Morgan Chase</td>
<td>2014.8</td>
<td>83M accounts</td>
</tr>
<tr>
<td>UPS</td>
<td>2014.8</td>
<td>51 stores customers</td>
</tr>
<tr>
<td>Dairy Queen</td>
<td>2014.9</td>
<td>395 store systems</td>
</tr>
<tr>
<td>Home Depot</td>
<td>2014.9</td>
<td>56M credit/debit cards</td>
</tr>
<tr>
<td>Jimmy Jones</td>
<td>2014.9</td>
<td>216 store systems</td>
</tr>
<tr>
<td>Staples</td>
<td>2014.10</td>
<td>51 store systems</td>
</tr>
</tbody>
</table>

*Are your data breached? Do you even know?*
Data Breaches since 2005 (FTC, Clearinghouse, 2019)

• # of records breached: 11,582,808,013
• # of data breaches: 9,071

2016 Data Breach

1. Yahoo!: 3.5B user accounts
2. FriendFinder: 412M user accounts
3. MySpace: 360M passwords
**Hacker Community Platforms – “Know your enemy”**

<table>
<thead>
<tr>
<th>Hacker Forums</th>
<th>DarkNet Markets</th>
<th>Carding Shops</th>
<th>IRC Channels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discussion board allowing hackers to freely share malicious tools and knowledge</td>
<td>Markets facilitating the sale of illicit goods (e.g., new exploits, drugs, weapons)</td>
<td>Shops selling sensitive information (e.g., credit cards, SSN’s)</td>
<td>Plain-text IM service commonly used by hacktivist groups (e.g., Anonymous)</td>
</tr>
</tbody>
</table>

US → cybercrime and general hacking  
Russia → underground economy, financial fraud  
China → cyberwarfare content
DICE-E: A FRAMEWORK FOR CONDUCTING DARKNET IDENTIFICATION, COLLECTION, EVALUATION WITH ETHICS

Victor Benjamin

Figure 2. The DICE-E Framework
Identify Hacker Assets/Tools

Sagar Samtani (JMIS, January 2018)
Hacker Asset/Tool Examples

Figure 1. Forum post with source code to create botnets

Figure 2. Forum post with BlackPOS malware attachment

Figure 3. Tutorial on how to create malicious documents
AZSecure Hacker Assets Portal System

Data Collection and Analytics
- Latent Dirichlet Allocation (LDA) and Support Vector Machine (SVM) Analytics
- 987 tutorials, 15,576 source code, and 14,851 attachments

Web Hosting and Access
- AWS

System Functionalities
- Browsing
- Searching
- Downloading

System Analytics
- Cyber Threat Intelligence Dashboard
- VirusTotal Malware Analysis
## AZSecure Hacker Assets Portal (English, Russian, Arabic)

<table>
<thead>
<tr>
<th>Forum</th>
<th>Language</th>
<th>Date Range</th>
<th># of Posts</th>
<th># of Members</th>
<th># of source code</th>
<th># of attachments</th>
<th># of tutorials</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenSC</td>
<td>English</td>
<td>02/07/2005-02/21/2016</td>
<td>124,993</td>
<td>6,796</td>
<td>2,590</td>
<td>2,349</td>
<td>628</td>
</tr>
<tr>
<td>Xeksec</td>
<td>Russian</td>
<td>07/07/2007- 9/15/2015</td>
<td>62,316</td>
<td>18,462</td>
<td>2,456</td>
<td>-</td>
<td>40</td>
</tr>
<tr>
<td>Ashiyane</td>
<td>Arabic</td>
<td>5/30/2003 – 9/24/2016</td>
<td>34,247</td>
<td>6,406</td>
<td>5,958</td>
<td>10,086</td>
<td>80</td>
</tr>
<tr>
<td>tuts4you</td>
<td>English</td>
<td>6/10/2006 – 10/31/2016</td>
<td>40,666</td>
<td>2,539</td>
<td>-</td>
<td>2,206</td>
<td>38</td>
</tr>
<tr>
<td><strong>Total:</strong></td>
<td></td>
<td><strong>02/07/2005- 10/31/2016</strong></td>
<td><strong>590,699</strong></td>
<td><strong>47,492</strong></td>
<td><strong>15,576</strong></td>
<td><strong>14,851</strong></td>
<td><strong>987</strong></td>
</tr>
</tbody>
</table>
Cyber Threat Intelligence (CTI) Example – Bank Exploits (e.g., BlackPOS)
Cyber Threat Intelligence (CTI) Example – Mobile Malware
Labeling Hacker Exploits for Proactive Cyber Threat Intelligence: A Deep Transfer Learning Approach

Benjamin Ampel (MISQ, 2nd Round)
### Literature Review: Hacker Forum Exploit Analysis

<table>
<thead>
<tr>
<th>Year</th>
<th>Author</th>
<th>1. Data Source</th>
<th>2. Data Type Used</th>
<th>Analytics</th>
<th>Identified Exploits</th>
<th>3. Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019</td>
<td>Schafer et al.</td>
<td>General purpose forums</td>
<td>Forum titles, users, message, topic, keywords</td>
<td>SNA, LDA</td>
<td>Leaks, botnets, DDoS</td>
<td>Trend identification</td>
</tr>
<tr>
<td>2019</td>
<td>Benjamin et al.</td>
<td>General purpose forums</td>
<td>Post content, attachments, source code, keywords, reputation</td>
<td>OLS Regression</td>
<td>Rootkit, XSS, SQLi, DDoS, shellcode, drive-by</td>
<td>Darknet identification, collection, evaluation</td>
</tr>
<tr>
<td>2018</td>
<td>Williams et al.</td>
<td>General purpose forums</td>
<td>Sub-forum name, author, post content, attachment metadata</td>
<td>LSTM</td>
<td>Crypters, keyloggers, RATs, DDoS, SQLi</td>
<td>Exploit categorization</td>
</tr>
<tr>
<td>2018</td>
<td>Goyal et al.</td>
<td>Forums, Twitter, Blogs</td>
<td>Post content, Tweet content, blog content</td>
<td>LSTM, RNN</td>
<td>Trojan, Windows, Apple OSX, phishing</td>
<td>Cyber attack prediction</td>
</tr>
<tr>
<td>2018</td>
<td>Deliu et al.</td>
<td>Nulled.IO leak</td>
<td>Post content</td>
<td>SVM, CNN</td>
<td>Botnet, crypter, keylogger, malware, rootkit</td>
<td>Exploit categorization</td>
</tr>
<tr>
<td>2017</td>
<td>Samtani et al.</td>
<td>General purpose forums</td>
<td>Post content, assets, thread, author, source code</td>
<td>LDA, SVM</td>
<td>Crypters, keyloggers, RATs, botnets</td>
<td>Exploit categorization</td>
</tr>
<tr>
<td>2017</td>
<td>Grisham et al.</td>
<td>General purpose forums</td>
<td>Post content, date, author, role, attachments</td>
<td>RNN</td>
<td>Mobile malware</td>
<td>Malware identification/ Proactive CTI</td>
</tr>
<tr>
<td>2017</td>
<td>Deliu et al.</td>
<td>Nulled.IO leak</td>
<td>Post content</td>
<td>SVM, LDA</td>
<td>Backdoor, botnet, crypter, DDoS, exploit, malware, password, rootkit</td>
<td>Exploit categorization</td>
</tr>
</tbody>
</table>

### Key Observations:

1. Studies focus on general forums, but not exploit DNMs or public repositories.
2. Although source code contains valuable information, many studies omit them from analysis.
3. The most common task is to categorize post content by exploit category.
Proposed Research Design

Data Collection

- Traditional Hacker Forums
- Exploit DNMs
- Public Exploit Repositories

Pre-Processing and Dataset Construction

- Programming Language Classifier
- Remove stop words, low frequency words, and lemmatize
- Tokenizer and Sequence Padder
- Gold-Standard Dataset Construction

Deep Transfer Learning Exploiter Labeler (DTL-EL) Model

Source Domain
Output: Exploit Label

Softmax Layer
Attention Layer

Step 1: Exploit Metadata Training

Convolutional Layer
BILSTM Layer

Word Embeddings

Target Domain
Output: Exploit Label

Softmax Layer
Attention Layer

Step 4: Layer transfer

Convolutional Layer
BILSTM Layer

Word Embeddings

Step 2: Pre-initialization

Experiment 1:
DTL-EL against prevailing classification methods on source domain

Experiment 2:
DTL-EL against non-transfer learning approaches on target domain

Experiment 3:
DTL-EL against transfer learning layer selection on target domain

Evaluations and Visualization

Benchmark Comparisons

Visualized Attention Comparison

Percentage

Metrics

Accuracy
F1
Precision
Recall
Research Design: DTL-EL

Source Domain
- Output: Exploit Label
  - Softmax Layer
  - Attention Layer
  - BiLSTM Layer
- Convolutional Layer
  - Word Embeddings

Step 1: Exploit Metadata Training

Target Domain
- Output: Exploit Label
  - Softmax Layer
  - Attention Layer
  - BiLSTM Layer
- Convolutional Layer
  - Word Embeddings

Step 2: Model initialization
Step 3: Exploit Source Code Training
Step 4: Layer transfer
Step 5: Exploit Source Code Training
### Results and Discussion: DTL-EL Model

#### Experiment 2: Internal against non-transfer learning models

<table>
<thead>
<tr>
<th>Model</th>
<th>Layer Weights</th>
<th>Accuracy</th>
<th>Precision</th>
<th>Recall</th>
<th>F1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Naïve Bayes</td>
<td>Random</td>
<td>8.59% ***</td>
<td>18.09% ***</td>
<td>15.08% ***</td>
<td>16.45% ***</td>
</tr>
<tr>
<td>Logistic Regression</td>
<td>Random</td>
<td>37.16% ***</td>
<td>35.13% ***</td>
<td>38.85% ***</td>
<td>36.9% ***</td>
</tr>
<tr>
<td>XGBoost Decision Tree</td>
<td>Random</td>
<td>47.65% ***</td>
<td>48.87% ***</td>
<td>30.06% ***</td>
<td>37.22% ***</td>
</tr>
<tr>
<td>SVM</td>
<td>Random</td>
<td>48.72% ***</td>
<td>37.98% ***</td>
<td>27.38% ***</td>
<td>31.82% ***</td>
</tr>
<tr>
<td>RNN</td>
<td>Random</td>
<td>57.64% ***</td>
<td>62.89% ***</td>
<td>53.93% ***</td>
<td>57.62% ***</td>
</tr>
<tr>
<td>GRU</td>
<td>Random</td>
<td>61.34% ***</td>
<td>64.06% ***</td>
<td>59.27% ***</td>
<td>62.09% ***</td>
</tr>
<tr>
<td>LSTM</td>
<td>Random</td>
<td>62.39% ***</td>
<td>65.77% ***</td>
<td>60.49% ***</td>
<td>63.42% ***</td>
</tr>
<tr>
<td>Bi-LSTM</td>
<td>Random</td>
<td>63.05% ***</td>
<td>67.56% ***</td>
<td>59.71% ***</td>
<td>63.21% ***</td>
</tr>
<tr>
<td>Bi-LSTM w/ Attention</td>
<td>Random</td>
<td>63.38% ***</td>
<td>66.04% ***</td>
<td>61.88% ***</td>
<td>64.02% ***</td>
</tr>
<tr>
<td><strong>DTL-EL (Our model)</strong></td>
<td><strong>Transferred</strong></td>
<td><strong>66.17%</strong></td>
<td><strong>68.25%</strong></td>
<td><strong>64.99%</strong></td>
<td><strong>66.61%</strong></td>
</tr>
</tbody>
</table>

---

![Experimen2: Internal against non-transfer learning approaches on target domain](image-url)
Case Study: Identifying Key Hackers - SQLi

• Since 2017, SQL injections are the most prevalent exploit in Russian forums.

• The five hackers with the most SQL injections posted on Russian forums are:
  1. karkajoi (13 exploits)
  2. sepo (12 exploits)
  3. BenderMR (12 exploits)
  4. Zmi666 (6 exploits)
  5. fandor9 (6 exploits)
Case Study: System Integration

• Hacker exploit source code can be input for classification with attention weights.

• The system applies a DTL-EL label upon the collection of new hacker forum text, providing real-time information to researchers.
  • APIs allow for forums to be downloaded in their entirety with related programming languages and exploit labels for source code.

Figure 16. Hacker Exploit Portal For Further Analysis
Detecting Cyber Threats with AI Agents: Multilingual, Multimedia DNM Content

Reza Ebrahimi (JMIS, MIS, IEEE PAMI)
## Dark Net Marketplaces (DNMs)

### Product Reviews

<table>
<thead>
<tr>
<th>Seller</th>
<th>Price</th>
<th>Product</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MicroDropper (2350)</td>
<td>$4.99</td>
<td>Hacking For Newbies</td>
<td>HappyEyes (5200) (4.79 W)</td>
</tr>
<tr>
<td>6 BITCOIN RANSOMWARE EASY MONEY SYSTEM</td>
<td></td>
<td>OnaPiece (7400) (4.83 W)</td>
<td>PW - WW</td>
</tr>
<tr>
<td>Go to Windows updates anonymously</td>
<td></td>
<td>TopHatMoneyMaker (4600)</td>
<td>(4.74 w)</td>
</tr>
<tr>
<td>HACK ANYONE USING THEIR IP ADDRESS</td>
<td></td>
<td>PASSWORD MANAGER KIT</td>
<td>5000 MICRODROPPER (4.91 W)</td>
</tr>
</tbody>
</table>

### Seller Information
- MicroDropper
- Price: $4.99
- Product: Hacking For Newbies
- Description: HappyEyes (5200) (4.79 W)

### Product Information
- Seller: MicroDropper
- Price: $4.000031 (4.67/1/3)
- Ship to: Worldwide
- Pay with: PM
- Escrow: Yes

### Product Description
You will get all files for build phishing PayPal site. Look perfect.

We are not include support to the product, so if you have 0% knowledge about site building and php - please do not make an order.

### Shipping Options
- PayPal - Scam Page (Phising site) [Looks Great]
- Password Manager Kit
- Quantity: 1
- Add to cart

### Product Ratings
5/5 stars
Essay I: Learning From Unlabeled Cybersecurity Content (JMIS, March 2020)

• Learning from examples → supervised by human-labeled data → Expensive!
• Unlabeled data improves cyber threat detection with transductive learning theory

- Significantly decreased reliance on human supervision for cyber threat detection.
Essay II: Learning from Heterogeneous Cybersecurity Content (MISQ, Forthcoming)

• Cyber threat detection in non-English content → lack of non-English training data
• Transfer cyber threat knowledge from high-resource English platforms to non-English ones with **transfer learning theory**

• Significantly decreased reliance on human supervision and outperformed machine translation.
Essay III: Learning from Heterogeneous Cybersecurity Content (IEEE TPAMI, 2nd Round)

- Learning from two domains (multilingual text, source code, image representations)
- Align different data distributions & feature spaces with domain adaptation theory

\[
\min_{P_s, P_t, R_s, R_t} \left\| P_s X_s - DR_s \right\|_F^2 + \left\| P_t X_t - DR_t \right\|_F^2 + \lambda \|R\|_1; \quad \text{s.t. } \|d_i\|_2 \leq 1
\]

- Enables heterogeneous data analytics (multilingual text, images) in any online market.
Privacy and PII (Personally Identifiable Information) Analytics:
identifying and alleviating privacy risks for vulnerable populations

* SaTC 2019-; SFS-2, 2019-
Exploring Privacy Risk of Exposed Digital Personally Identifiable Information (PII): A Neighbor Attention-Based Approach

Fangyu Lin and Hsinchun Chen
Data Breaches since 2005 (FTC, Clearinghouse, 2019)

- # of records breached: 11,582,808,013
- # of data breaches: 9,071

2016 Data Breach

1. Yahoo!: 3.5B user accounts
2. FriendFinder: 412M user accounts
3. MySpace: 360M passwords
Revealing and Protecting PII: From Dark Web to Surface Web
IRB, HIPAA, GDPR, PII

- Cybersecurity to Privacy
- Michael Bazzell + From Dark Web to Surface Web
### Dark Web Intelligence Sources (May, 2021)

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
<th>Size*</th>
<th>Promising Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stolen Account Collection</strong></td>
<td>Stolen social media and e-mail accounts</td>
<td>25 billions</td>
<td>Username</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Password</td>
</tr>
<tr>
<td><strong>Stolen Credit Card - Tormarket</strong></td>
<td>Stolen credit and debit card owner information</td>
<td>832 thousands</td>
<td>Full name</td>
</tr>
<tr>
<td></td>
<td>* No card number</td>
<td></td>
<td>Country</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>State</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>City</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Zip</td>
</tr>
<tr>
<td><strong>Stolen SSN - Buyssn</strong></td>
<td>Personal information of SSN owners</td>
<td>5.75 millions</td>
<td>Full name</td>
</tr>
<tr>
<td></td>
<td>* No SSN</td>
<td></td>
<td>YOB</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>City</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>State</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Zip</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Country</td>
</tr>
</tbody>
</table>
### Stolen Accounts

<table>
<thead>
<tr>
<th>Rank</th>
<th>E-mail Domains</th>
<th>Numbers</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>yahoo.com</td>
<td>244,769,117</td>
<td>20.41%</td>
</tr>
<tr>
<td>2</td>
<td>hotmail.com</td>
<td>182,564,724</td>
<td>15.22%</td>
</tr>
<tr>
<td>3</td>
<td>gmail.com</td>
<td>103,435,791</td>
<td>8.62%</td>
</tr>
<tr>
<td>4</td>
<td>mail.ru</td>
<td>90,371,699</td>
<td>7.53%</td>
</tr>
<tr>
<td>5</td>
<td>aol.com</td>
<td>44,830,568</td>
<td>3.74%</td>
</tr>
<tr>
<td>6</td>
<td>yandex.ru</td>
<td>36,336,003</td>
<td>3.03%</td>
</tr>
<tr>
<td>7</td>
<td>rambler.ru</td>
<td>23,521,080</td>
<td>1.96%</td>
</tr>
<tr>
<td>8</td>
<td>hotmail.fr</td>
<td>16,571,495</td>
<td>1.38%</td>
</tr>
<tr>
<td>9</td>
<td>web.de</td>
<td>12,918,595</td>
<td>1.08%</td>
</tr>
<tr>
<td>10</td>
<td>live.com</td>
<td>11,661,375</td>
<td>0.97%</td>
</tr>
<tr>
<td>11</td>
<td>msn.com</td>
<td>11,248,354</td>
<td>0.94%</td>
</tr>
<tr>
<td>12</td>
<td>gmx.de</td>
<td>10,800,404</td>
<td>0.90%</td>
</tr>
<tr>
<td>13</td>
<td>163.com</td>
<td>10,492,032</td>
<td>0.87%</td>
</tr>
<tr>
<td>14</td>
<td>bk.ru</td>
<td>9,416,062</td>
<td>0.78%</td>
</tr>
<tr>
<td>15</td>
<td>yahoo.fr</td>
<td>8,886,223</td>
<td>0.74%</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>817,823,522</td>
<td>68.18%</td>
</tr>
</tbody>
</table>

### Popular Passwords

<table>
<thead>
<tr>
<th>Rank</th>
<th>Passwords</th>
<th>Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>123456</td>
<td>3,370,644</td>
</tr>
<tr>
<td>2</td>
<td>123456789</td>
<td>1,187,812</td>
</tr>
<tr>
<td>3</td>
<td>Homelesspa*</td>
<td>546,648</td>
</tr>
<tr>
<td>4</td>
<td>password</td>
<td>522,529</td>
</tr>
<tr>
<td>5</td>
<td>abc123</td>
<td>516,091</td>
</tr>
<tr>
<td>6</td>
<td>password1</td>
<td>435,753</td>
</tr>
<tr>
<td>7</td>
<td>12345</td>
<td>382,970</td>
</tr>
<tr>
<td>8</td>
<td>qwerty</td>
<td>376,099</td>
</tr>
<tr>
<td>9</td>
<td>12345678</td>
<td>357,654</td>
</tr>
<tr>
<td>10</td>
<td>1234567</td>
<td>287,453</td>
</tr>
<tr>
<td>11</td>
<td>1234567890</td>
<td>252,929</td>
</tr>
<tr>
<td>12</td>
<td>111111</td>
<td>236,852</td>
</tr>
<tr>
<td>13</td>
<td>iloveyou</td>
<td>211,593</td>
</tr>
<tr>
<td>14</td>
<td>123456a</td>
<td>205,807</td>
</tr>
<tr>
<td>15</td>
<td>123123</td>
<td>191,450</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>9,082,284</td>
</tr>
</tbody>
</table>

*Passwords are like underwear... change often, don’t share…*
AZSecure Privacy Portal Design

Breached Data Collection

Data Breach Monitoring System and Breached Data Collection
- Stolen SSN collection
  - SSN Shops
- Stolen Card Collection
  - Carding Shops
- Stolen Account Collection
  - Database Sharing and Marketplace Forums

Breached Data Management

Portal Backend

Data Retrieval from DB

People Search Engines (PSEs) API Integration and PII Extraction

Entity Resolution

Multi-Context Attention (MCA) Model

Privacy Risk Score Calculation

Portal Frontend

Functionalities

Search Function

Privacy Risk Assessment Report

Data Breach List

Protect Yourself

Data Breach Notification

Figure 1. AZSecure Privacy Portal Project Overview
Search in AZSecure Privacy Portal

Figure 5. A mock-up response when records are found

Matching records are returned, and the user can select the correct results.
Return Exposed PII

Figure 9. Mock-ups of a comprehensive exposed PII profile
Adversarial Malware Generation and Evasion: adversarial AI in cybersecurity

* SaTC 2019-; SFS-2, 2019-
Defending Cybersecurity AI Agents

Reza Ebrahimi (JMIS, MISQ)

• **Essay 1:** Learning to Protect Malware Detectors
• **Essay 2:** Learning to Protect any Defense AI agent
Defending Cybersecurity AI Agents

• Cybersecurity firms are adopting AI agents for autonomous cyber defense (Rai et al. 2019).
  • Automate threat detection and remediation at a large scale (Tolido et al. 2019).

• However, AI agents have shown to be vulnerable to adversarial attacks.

• Inputs meticulously modified to mislead them (Yuan et al. 2019). → Known as adversarial attacks (Apruzzese et al. 2019).

• How can we protect cyber defense AI agents?
Defending Cybersecurity AI Agents

Cyber Defense AI Agent

Adversarial Input (Modified malware)
- Network packet
- Email
- Customer reviews
- News article

Network Intrusion Detector
Spam Detector
E-commerce Fake Reviews Detector
Fake News Detector

Undetected

Symantec
Google
Amazon
Facebook
Essay I: Learning to Protect Malware Detectors
(JMIS, In sub.)

• Malware attack is #1 cause of damage to IT infrastructure (Bissell et al. 2019).
• Malware detector is the first line of defense. → Can be misled by adversarial inputs.
  • Language modeling helps emulate these inputs.

\[
\maximize_{\delta \in \Delta} \mathcal{L}(\mathcal{H}_{\theta}(x + \delta), y)
\]

• Significantly improves the robustness of malware detectors against adversarial attacks.
Essay II: Learning to Protect any Defense AI Agent
(MISQ, 1st Round)

• Modern AI agents can be misled by adversarial attacks. → Emulating these attacks is vital for defense.

• A game between adversary and defender helps emulation.

• Strengthened the robustness of AI agents against adversarial attacks.
Smart Vulnerability Assessment: scientific workflows and OSS vulnerability analytics and mitigation

* CICI 2019-; SFS-2, 2019-
Linking Hacker Community Exploits to Known Vulnerabilities for Proactive Cyber Threat Intelligence: An Attention-based Deep Structured Semantic Model Approach

Sagar Samtani (MISQ, forthcoming)
Protecting Scientific Instruments and Cyberinfrastructure: From iPlant/CyVerse (life sciences) to BioSphere 2/LEO (earth sciences)...

a new UA/USF/AZSecure NSF CICI project, 2019-2022
Hacker Forum Exploits

• **Key Characteristics:**
  1. Descriptive tool names (target, operations, etc.)
  2. Clear categories of exploits (e.g., target system)
  3. Post date of when exploit was posted
### Key Attributes Returned by Modern Vulnerability Scanners

<table>
<thead>
<tr>
<th>Category</th>
<th>Metadata</th>
<th>Description</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description 1.</td>
<td>Name</td>
<td>Short, descriptive name of vulnerability</td>
<td>Short text</td>
</tr>
<tr>
<td></td>
<td>Family Name</td>
<td>Family vulnerability belongs to (e.g., Windows, etc.)</td>
<td>Categorical</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Lengthy text description about vulnerability</td>
<td>Long text</td>
</tr>
<tr>
<td></td>
<td>Synopsis</td>
<td>Short description of vulnerability</td>
<td>Short text</td>
</tr>
<tr>
<td></td>
<td>Solution</td>
<td>Description or solution links</td>
<td>Short text</td>
</tr>
<tr>
<td></td>
<td>Vulnerable Systems</td>
<td>List of systems susceptible to vulnerability</td>
<td>Short text (list)</td>
</tr>
<tr>
<td>Risk</td>
<td>CVSS</td>
<td>Value between 0.0-10.0 indicating vulnerability severity</td>
<td>Continuous</td>
</tr>
<tr>
<td></td>
<td>Risk Factor</td>
<td>Categorical rating of risk (High, Low)</td>
<td>Categorical</td>
</tr>
<tr>
<td></td>
<td>CVE</td>
<td>Vulnerability reference number</td>
<td>Categorical</td>
</tr>
<tr>
<td></td>
<td>Publication Date</td>
<td>Date vulnerability was publicly published</td>
<td>Date</td>
</tr>
</tbody>
</table>

### Key Characteristics:

1. Short, descriptive title of vulnerability
2. List of systems susceptible to vulnerability
3. Common Vulnerability Severity Score (0.0 – 10.0)
Proposed Exploit Vulnerability Attention-DSSM

- Key Limitation with DSSM $\rightarrow$ lack of interpretability.

- **Contribution:** EVA-DSSM integrates an attention mechanism into the DSSM. Identifies and outputs key exploit features essential for creating links.
## Experiment Results: EVA-DSSM vs Deep Learning Matching Algorithms

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Remote Exploits</th>
<th>Local Exploits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NDCG@1</td>
<td>NDCG@3</td>
</tr>
<tr>
<td>ANMM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ARC-I</td>
<td>0.2589***</td>
<td>0.3683***</td>
</tr>
<tr>
<td>ARC-II</td>
<td>0.3964***</td>
<td>0.5450***</td>
</tr>
<tr>
<td>KNRM</td>
<td>0.4571***</td>
<td>0.5521***</td>
</tr>
<tr>
<td>Conv-KNRM</td>
<td>0.5411</td>
<td>0.6330*</td>
</tr>
<tr>
<td>DRMM</td>
<td>0.5339</td>
<td>0.6420</td>
</tr>
<tr>
<td>DUET</td>
<td>0.5232</td>
<td>0.6014*</td>
</tr>
<tr>
<td>MATCHLSTM</td>
<td>0.1536***</td>
<td>0.3220***</td>
</tr>
<tr>
<td>MV-LSTM</td>
<td>0.5393</td>
<td>0.6250**</td>
</tr>
<tr>
<td>DSSM</td>
<td>0.3339***</td>
<td>0.5019***</td>
</tr>
<tr>
<td>Left EVA-DSSM</td>
<td>0.1607***</td>
<td>0.2934***</td>
</tr>
<tr>
<td>EVA-DSSM</td>
<td>0.5469</td>
<td>0.6499</td>
</tr>
</tbody>
</table>

### Web Applications

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>NDCG@1</th>
<th>NDCG@3</th>
<th>NDCG@5</th>
<th>MRR</th>
<th>MAP</th>
<th>NDCG@1</th>
<th>NDCG@3</th>
<th>NDCG@5</th>
<th>MRR</th>
<th>MAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANMM</td>
<td>0.3125***</td>
<td>0.4527***</td>
<td>0.5114***</td>
<td>0.5075***</td>
<td>0.4704***</td>
<td>0.1790***</td>
<td>0.2691***</td>
<td>0.3640***</td>
<td>0.3969***</td>
<td>0.3532***</td>
</tr>
<tr>
<td>ARC-I</td>
<td>0.0906***</td>
<td>0.3378***</td>
<td>0.4275***</td>
<td>0.3637***</td>
<td>0.4042***</td>
<td>0.1176***</td>
<td>0.2111***</td>
<td>0.2717***</td>
<td>0.2828***</td>
<td>0.3233***</td>
</tr>
<tr>
<td>ARC-II</td>
<td>0.3250***</td>
<td>0.4894***</td>
<td>0.5410***</td>
<td>0.5275***</td>
<td>0.5405***</td>
<td>0.2053***</td>
<td>0.2881***</td>
<td>0.3395***</td>
<td>0.3687***</td>
<td>0.3864***</td>
</tr>
<tr>
<td>KNRM</td>
<td>0.5312</td>
<td>0.6248**</td>
<td>0.6728**</td>
<td>0.6727*</td>
<td>0.6768*</td>
<td>0.2684***</td>
<td>0.3166***</td>
<td>0.3461***</td>
<td>0.3817***</td>
<td>0.4022***</td>
</tr>
<tr>
<td>Conv-KNRM</td>
<td>0.5531</td>
<td>0.6716*</td>
<td>0.6973*</td>
<td>0.7122</td>
<td>0.6864*</td>
<td>0.2825*</td>
<td>0.3291***</td>
<td>0.3913***</td>
<td>0.4293***</td>
<td>0.4468***</td>
</tr>
<tr>
<td>DSSM</td>
<td>0.3619**</td>
<td>0.4874***</td>
<td>0.5497***</td>
<td>0.5156***</td>
<td>0.5373***</td>
<td>0.2333**</td>
<td>0.2954***</td>
<td>0.3493***</td>
<td>0.4052**</td>
<td>0.3851***</td>
</tr>
<tr>
<td>Left EVA-DSSM</td>
<td>0.1063***</td>
<td>0.2906***</td>
<td>0.4187***</td>
<td>0.3606***</td>
<td>0.3838***</td>
<td>0.2986</td>
<td>0.3452*</td>
<td>0.4102*</td>
<td>0.4652</td>
<td>0.4472**</td>
</tr>
<tr>
<td>EVA-DSSM</td>
<td>0.6281</td>
<td>0.7602</td>
<td>0.7885</td>
<td>0.7684</td>
<td>0.7863</td>
<td>0.3579</td>
<td>0.4550</td>
<td>0.4954</td>
<td>0.5133</td>
<td>0.6009</td>
</tr>
</tbody>
</table>

### DoS Exploits

- EVA-DSSM outperforms all deep learning benchmarks
- Conv. or LSTM operations achieved lower performances
- Indicates that integrating an attention mechanism into the DSSM architecture does not deteriorate performance
Case Studies: SCADA and Hospitals

• 20,461 SCADA Devices from major vendors (e.g., Rockwell)

• Motivation: SCADA → control critical infrastructure

• 1,879 devices from top 8 US hospitals

• Motivation: Hospitals → popular target for hackers

Procedure

Device Identification → Vulnerability Scanning → EVA-DSSM → DVSM
## Hospital Case Study

### Hospital Device Information

<table>
<thead>
<tr>
<th>Hospital Name</th>
<th># of Vulnerable Devices/# of devices</th>
<th>Device Type</th>
<th># of Vulnerabilities</th>
<th>Vulnerabilities</th>
<th>DVSM</th>
</tr>
</thead>
<tbody>
<tr>
<td>12x.x.x.x</td>
<td>133/808</td>
<td>FTP/SSH Server</td>
<td>3</td>
<td>FTP issues</td>
<td>4.591</td>
</tr>
<tr>
<td>19x.x.x.x</td>
<td>27/301</td>
<td>SSH Server</td>
<td>3</td>
<td>SSH issues</td>
<td>4.376</td>
</tr>
<tr>
<td>17x.x.x.x</td>
<td>31/274</td>
<td>eCare web portal</td>
<td>47</td>
<td>XSS, OpenSSL, buffer overflow, DoS</td>
<td>61.761</td>
</tr>
<tr>
<td>16x.x.x.x</td>
<td>59/160</td>
<td>Medical computing portal</td>
<td>5</td>
<td>PHP and SSH issues</td>
<td>4.863</td>
</tr>
<tr>
<td>14x.x.x.x</td>
<td>64/130</td>
<td>Web Server</td>
<td>3</td>
<td>SQL Injections</td>
<td>7.528</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Apple TV</td>
<td>2</td>
<td>Buffer overflow</td>
<td>5.381</td>
</tr>
<tr>
<td>14x.x.x.x</td>
<td>14/107</td>
<td>SSH/Web server</td>
<td>4</td>
<td>PHP and SSH issues</td>
<td>3.871</td>
</tr>
<tr>
<td>6x.x.x.x</td>
<td>9/52</td>
<td>Informational diabetes portal</td>
<td>3</td>
<td>SVN and Unix vulnerabilities</td>
<td>7.159</td>
</tr>
<tr>
<td>16x.x.x.x</td>
<td>7/47</td>
<td>Web Server</td>
<td>6</td>
<td>XSS, HTMLi</td>
<td>9.367</td>
</tr>
<tr>
<td><strong>Total:</strong></td>
<td><strong>344/1,879 (18.31%)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Device Severity Score Information for Selected Devices

<table>
<thead>
<tr>
<th>Vulnerability Name (CVSS Score)</th>
<th>Exploit Name (Post Date)</th>
<th>Severity Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;OpenSSL Unsupported&quot; (10.0)</td>
<td>&quot;OpenSSL TLS Heartbeat Extension – Memory Disclosure&quot; (4/8/2014)</td>
<td>3.366</td>
</tr>
<tr>
<td>&quot;Multiple XSS Vulnerabilities&quot; (4.3)</td>
<td>&quot;Portal XSS Vulnerability&quot; (5/28/2010)</td>
<td>1.261</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total:</strong></td>
<td></td>
<td><strong>61.761</strong></td>
</tr>
</tbody>
</table>

- Portals are a common avenue for hackers to access sensitive records (Ayala 2016).
- Analysis shows an eCare portal with a large attack surface: 47 vulnerabilities for a DVSM of 61.761.
- Network admins can prioritize this device when analyzing their weaknesses.
Some Advice for Junior Faculty and Ph.D. Students: Journals and Grants
Major Journals: i-School, c-School, b-School

• i-School ($80K) & health informatics Journals: JASIST, ACM TOIS; JAMIA, JBI ➜ “informatics” (text) focused, system driven; helpful for NSF & NIH/NLM funding

• c-School ($100K) Journals: ACM TOIS, IEEE TKDE, CACM, IEEE IS, IEEE Computer, IEEE SMC ➜ algorithm/computing focused, data driven; helped significantly with NSF funding (same for major CS conferences)

• b-School ($180K) Journals: MISQ, ISR, JMIS, MS, ACM TMIS, DSS ➜ “design science” focused, managerial framework/principle/knowledge base; helped get jobs in major b-schools (little federal funding)
Major Journals: Chen, i-, c-, b-school, CISE

- Work hard; be persistent; colleagues & students help a lot; a little bit of luck helps
Major Journals: MISQ & JMIS

- MISQ: A+ journal, #1 in MIS
  - behavior/management focused traditionally (most SEs)
  - recent focus in business analytics & data sciences (SEs: HRR, GA, IB, PK, JP) ➔ selecting the right SEs/AEs
  - Computational design science: application-inspired novelty (algorithm, representation, framework, HCI) + societal impact ➔ significant content & mature writing (40+ pages)
  - MIS-specific lit review + methodology/framework/design “theory” + contribution to KB + principles (research abstraction) ➔ right packaging

- JMIS: A journal, #3 in MIS
  - Same as above; more system driven
  - Zwass + Nunamaker; HICSS special issue

A Deep Learning Approach for Recognizing Activity of Daily Living (ADL) for Senior Care: Exploiting Interaction Dependency and Temporal Patterns
Hongyi Zhu, Sagar Samtani, Randall A. Brown, and Hsinchun Chen

Forthcoming, 2020

Special Issue, Business Analytics; 5250 citations

Health Analytics; Deep Learning

2012

[214] Hsinchun Chen, Roger H. L. Chiang, Veda C. Storey:
Business Intelligence and Analytics: From Big Data to Big Impact. MIS Q.

2010

Jr.:

2008

[139] Ahmed Abbasi, Hsinchun Chen:

Security Analytics; Best Paper, ICIS, 2010

Social Media Analytics
Connecting Systems, Data, and People: A Multidisciplinary Research Roadmap for Chronic Disease Management

Indranil Bardhan
Department of Information, Risk and Operations Management, McCombs School of Business, The University of Texas at Austin, Austin, TX 78705 U.S.A. (indranil.bardhan@mccombs.utexas.edu)

Hsinchun Chen
MIS Department, Eller College of Management, The University of Arizona, Tucson, AZ 85721-0108 U.S.A. (hsinchun@email.arizona.edu)

Elena Karahanna
MIS Department, Terry College of Business, The University of Georgia, Athens, GA 30602 U.S.A. (ekarah@uga.edu)

Special Issue: The Role of Information Systems and Analytics in Chronic Disease Prevention and Management

Special Issue Articles

Trajectories of Repeated Readmissions of Chronic Disease Patients: Risk Stratification, Profiling, and Prediction
Ofir Ben-Assul and Rema Padman (pp. 201-226; DOI: 10.25300/MISQ/2020/15101)

Chronic Disease Management: How IT and Analytics Create Healthcare Value Through the Temporal Displacement of Care
Steve Thompson, Jonathan Whitaker, Rajiv Kohli, and Craig Jones (pp. 227-256; DOI: 10.25300/MISQ/2020/15085)

Go to You Tube and Call Me in the Morning: Use of Social Media for Chronic Conditions
Xiao Liu, Bia Zhang, Anjana Susarla, and Rema Padman (pp. 257-285; DOI: 10.25300/MISQ/2020/15107)

A Data Analytics Framework for Smart Asthma Management Based on Remote Health Information Systems with Bluetooth-Enabled Personal Inhalers
Junbo Son, Patricia Flatley Brennan, and Shiyou Zhou (pp. 286-303; DOI: 10.25300/MISQ/2020/15092)

A Comprehensive Analysis of Triggers and Risk Factors for Asthma Based on Machine Learning and Large Heterogeneous Data Sources
Wenli Zhang and Sudha Ram (pp. 305-349; DOI: 10.25300/MISQ/2020/15106)

Examining How Chronically Ill Patients’ Reactions to and Effective Use of Information Technology Can Influence How Well They Self-Manage Their Illness
Azadeh Saeidi, Henri Barki, and Guy Paré (pp. 351-386; DOI: 10.25300/MISQ/2020/15103)

The Effects of Participating in a Physician-Driven Online Health Community in Managing Chronic Disease: Evidence from Two Natural Experiments
Qianqian Ben Liu, Xiaoxiao Liu, and Xitong Guo (pp. 391-419; DOI: 10.25300/MISQ/2020/15102)
Major Journals: MISQ CDS Common Issues

• MISQ, My Experience: no paper/involvement before 2008 (no SE in design science); Abbasi 2008 (CyberGate), 2010 (AZProtect, ICIS best paper); Guest Editor, BI&A special issue, 2010-2012 (Straub); SE 2016-2019 (Rai); Guest Editor, Health IT/Analytics special issue, 2016-2020 (Rai)

• Design Science paper common issues:
  • Where is the theory? Is this MIS? (early reviewers’ critiques)
  • Few qualified/sympathetic design science SEs, AEs, reviewers. (overly critical)
  • Long review cycle (2-4 rounds/years) and uncertainty (rejection at late round).

  ➔ but
  • BI&A and data sciences are hot, in society and in b-school curriculum!
  • Young MIS CDS scholars need 1-2 MISQ/JMIS papers accepted or in deep round.
  • Mid-career MIS CDS scholars need 3-5 MISQ/JMIS papers for tenure.
Major Journals: MISQ CDS Paper Template

• Computational design science (Chen in Rai, 2017): application-inspired novelty (algorithm, representation, framework, HCI) + emerging high-impact problems

• Significant content & mature writing (40+ pages)

• MIS-specific lit review (3-4 pages) ⇒ Who/what had (been) published in MISQ/ISR/JMIS (10-20 MIS references, taxonomy, analytics relevance)

• Methodology/framework/design “theory” (2-3 pages) ⇒ underlying methodological foundation (not behavioral theory of +/- hypotheses), e.g., Systematic Functional Linguistic Theory, Kernel Learning Theory, etc.

• Contribution to KB + principles (research abstraction; 2-3 pages) ⇒ What have been learned about the design, use and general knowledge gained?

⇒ Carefully study sample MISQ DS papers, e.g., (Abbasi, 2008; 2010).
Major Grants: NIH, DARPA, DHS, IARPA

• NIH: NLM is informatics-focused; “translational” research with some application-inspired health-related novelty; need pubs and networking in AMIA/JAMIA; strong health informatics (NLM) tradition and turf (strong personality) ➔ Chen as NLM Scientific Counselor, 2002-2006

• DOD/DARPA: was innovative, basic/foundational, long-term (ARPA Net); now mission-critical, system-driven, short-term; commercial company (defense contractor) as prim, academic as sub; bi-monthly milestones/metrics/reporting ➔ Chen early success with DARPA/IARPA/DHS for COPLINK/Dark Web research

• DHS, IARPA: similar to DARPA, but aspiring; lesser scientific quality (strong personality)

➔ Not my focus any more! (Need to smell like them.)
Major Grants: NSF Org Chart

NATIONAL SCIENCE FOUNDATION

OFFICE OF THE DIRECTOR
703.292.8000
Sethuraman Panchanathan
Director
Vacant
Deputy Director
F. Fleming Crim
Chief Operating Officer

NATIONAL SCIENCE BOARD (NSB)
703.292.7000
Diane L. Souvaine
Chair
Ellen Ochoa
Vice Chair

OFFICE OF INSPECTOR GENERAL (OIG)

OFFICE OF THE DIRECTOR OF APPLIED RESEARCH (ODAR)
703.292.7000
John J. Healy
Director

OFFICE OF THE GENERAL COUNSEL (OGC)
703.292.8800
Barbara Scherb
Vice President, General Counsel

OFFICE OF INTERNATIONAL AFFAIRS (OIA)

OFFICE OF LEGISLATIVE & PUBLIC AFFAIRS (OLPA)
703.292.8679
Alexandra Vlass, Deputy Director

OFFICE OF INTELLIGENCE & SECURITY (OIS)

DIRECTORATE FOR BIOLOGICAL SCIENCES (BIO)
James A. Thomson
Director

DIRECTORATE FOR COMPUTER & INFORMATION SCIENCE & ENGINEERING (CISE)
William T. Pecor
Director

DIRECTORATE FOR EDUCATION & HUMAN RESOURCES (EHR)
Sandra N. Garfinkel
Director

DIRECTORATE FOR ENGINEERING (ENG)
Richard S. Frensley
Director

DIRECTORATE FOR GEOGRAPHIC SCIENCE (GEO)
Johannes E. Niemann
Director

DIRECTORATE FOR GEOLOGY & PHYSICAL SCIENCES (GeP)
William M. Groß
Director

DIRECTORATE FOR MATHEMATICAL & PHYSICAL SCIENCES (MPS)
Alan J. Aldrich
Director

DIRECTORATE FOR SOCIAL, BEHAVIORAL, & ECONOMIC SCIENCES (SBE)
John C. Conklin
Director

DIRECTORATE FOR INFORMATION & RESOURCE MANAGEMENT (IRMM)
Michelle Johnson
Director

DIRECTORATE FOR EDUCATION & RESOURCE MANAGEMENT (EDRM)
Rhonda Evans
Director

DIRECTORATE FOR INTEGRATIVE ACTIVITIES (IAA)

DIRECTORATE FOR INTERNATIONAL SCIENCE & ENGINEERING (ISE)

DIRECTORATE FOR INFORMATION OFFICER (CIO)

($8.3B)
Major Grants: NSF CISE/IIS/III

CISE

IIS/OAC

- Directorate for Computer & Information Science & Engineering
- Office of Advanced Cyberinfrastructure
- Division of Computing and Communication Foundations
- Division of Computer and Network Systems
- Division of Information and Intelligent Systems

CISE/OAD

CISE/OAC

CISE/CCF

CISE/CNS

CISE/IIS

III

- IIS: Human-Centered Computing (HCC)
- IIS: Information Integration and Informatics (III)
- IIS: Robust Intelligence (RI)
- OAC: OAC Core Research (OAC Core)
Major Grants: NSF CISE/IT Societal Impacts (NAS)

University research ➔ Industry R&D ➔ Products ➔ $1B Market (job and wealth creation)
Major Grants: NSF Programs

• CORE: NSF CISE/IIS/III CORE most relevant to fundamental research in AI, machine learning, WWW, data sciences, NLP; acceptance rate 6-8%, highly competitive, critical young CS reviewers ➔ IIS Core ($100M/yr)

• OAC: NSF CISE/OAC relevant to applied cyberinfrastructure for sciences; acceptance rate 20-30%, less competitive, reviewers including CS, SBE, and domain sciences ➔ DIBBs, CICI ($25M-30M/yr; my focus)

• Applied Programs: Many emerging cross-directorate (e.g., EHR, SBE, CISE) and cross-agency (e.g., NSF, NIH, DOD) high-impact applied research programs (e.g., security, health); acceptance rate 15-20%, less competitive, reviewers including CS, SBE, and SME ➔ SaTC, SFS, CCRI, SCH, BIGDATA, I-DSN, National AI Institutes ($50M-100M/yr; my focus)

• Young Scholars: Many opportunities for early-career scholars; acceptance rate 10-20%, competitive, for early career; valuable for obtaining tenure! ➔ CRII, CAREER + EAGER ($200K-$1M for each award)
Major Grants: NSF Proposal Observations

• Computational Design Science (CDS) has excellent chance for successful proposals (CISE). in general, not so much for behavioral or economics MIS researchers (SBE; too basic, too incremental, not novel).

• “Business” (finance, accounting, marketing) school research is not considered STEM. need to position for larger societal/STEM problems.

• CDS research needs to compete with CS researchers (“locusts” in emerging technical fields); deep & novel domain application for emerging societal problems could be viable. my approach at least, for the past 30 years: digital library, intelligence, health, cybersecurity, etc.

• Need application or domain-inspired novelty for applied cross-directorate programs. senior Ph.D. students; last 1-2 dissertation chapters

• A lab or center can help with sustainable advantage and funding. developing collection, prototype system, etc.; structure & organizational memory
Major Grants: NSF Proposal Template

• Proposal title: short and succinct; need a multi-disciplinary team
• Project summary: Summarize problems and approach; include IM + BI
• Main text (15 pages)
  • Need mature writing; good diagrams
  • Need methodological/algorithmic novelty (IM, 60%); need strong impacts (BI, 40%)
  • Need good lit review (state-of-the-art) & promising preliminary results
• CV: need relevant ACM/IEEE references; MISQ/ISR pubs help very little
• Others: Good to have office support, e.g., budget, facilities, DMP, routing, etc.
Major Grants: NSF General Advice for CDS Scholars

• Develop methodological novelty and application-specific strengths over your career. ➔ world-class excellence vs. other CS scholars

• Train your Ph.D. students well. ➔ their last 2 dissertation chapters could be fundable; they can be trained to write proposals (scale & efficiency)

• Build a center/lab/group. ➔ more sustainable and impressive (common in CS, ECE, MED)

• Improve your grantsmanship. ➔ get to know your PDs and become frequent NSF panelists (getting into their heads)

• Improve your success rate to 30% (one in 3). ➔ target repeating programs for re-submissions

• Monitor and anticipate current and emerging programs. ➔ prepare the next proposals; repeat the cycle!
Parting Thoughts: Hard Work + A Bit of Luck

• Societal Impact > Academic Impact
  • Looking for high-impact societal problems (NYT, WSJ, The Economists)

• IT > MIS
  • MIS is a smaller subfield within broader IT/computing.

• CISE > SBE
  • Computational Design Science can make a difference.

• New > Old
  • Looking for new, interesting, unknown problems

• EQ > IQ
  • Hard work, discipline, aspiration, etc. always beat raw talent. Plus a bit of luck!
For questions and comments

hchen@eller.Arizona.edu
http://ai.Arizona.edu