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

SKM, October 8, 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.

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

D-Lib Magazine
July/August 1998

ISSN 1082-9873

NSF/DARPA/NASA Digital Libraries Initiative

A Program Manager's Perspective

Stephen M. Griffin
Division of Information and Intelligent Systems (IIS)
Program Director: Special Projects Digital Libraries Initiative
National Science Foundation
Arlington, Virginia USA
sgriffin@nsf.gov

NIJ National Institute of Justice
STRENGTHEN SCIENCE. ADVANCE JUSTICE.

Digital Government (DigitalGov)

Program Solicitation
NSF 04-521
Replaces Document 02-156

National Science Foundation
Directorate for Computer and Information Science and Engineering
Division of Information and Intelligent Systems

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

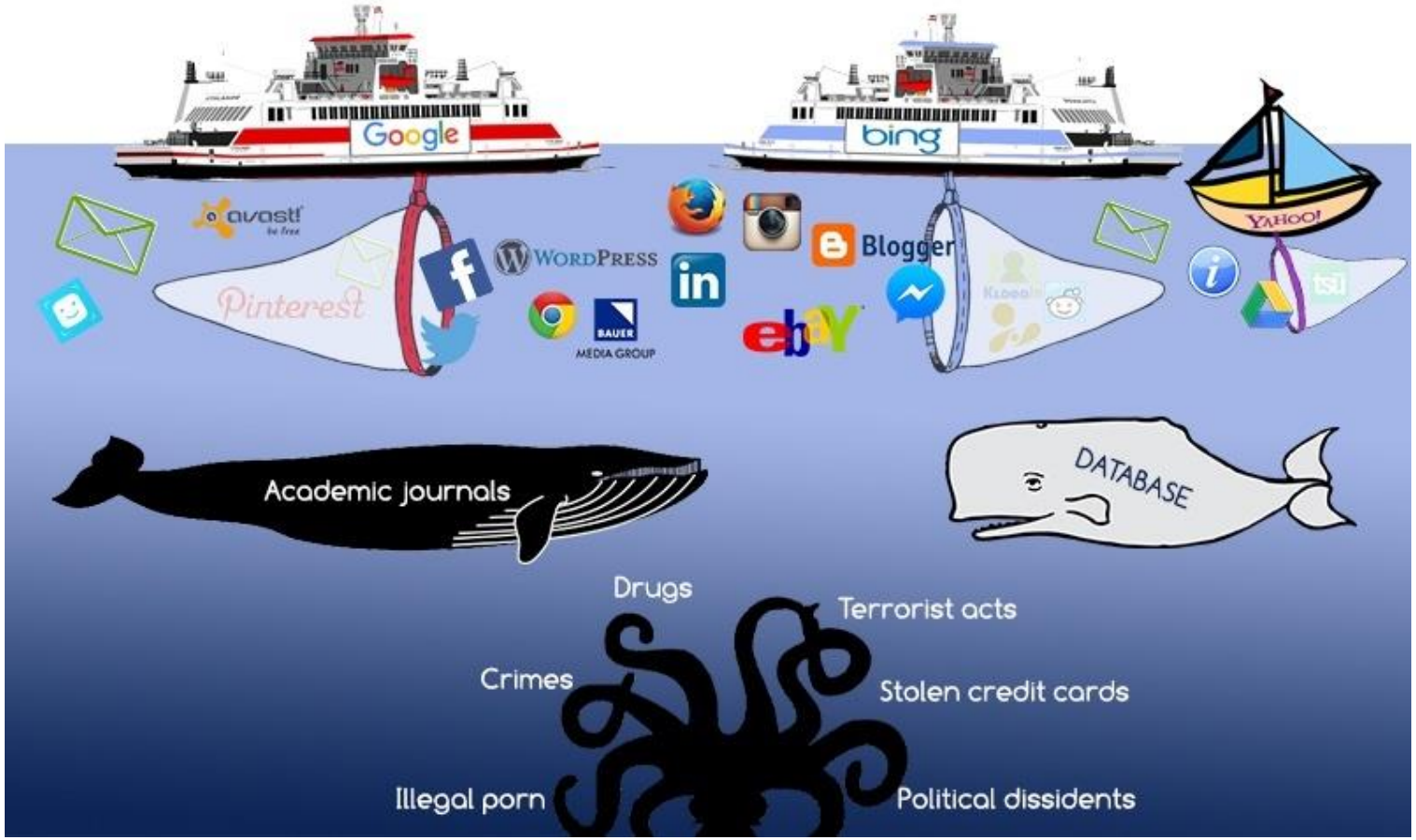
Surface Web

Deep Web

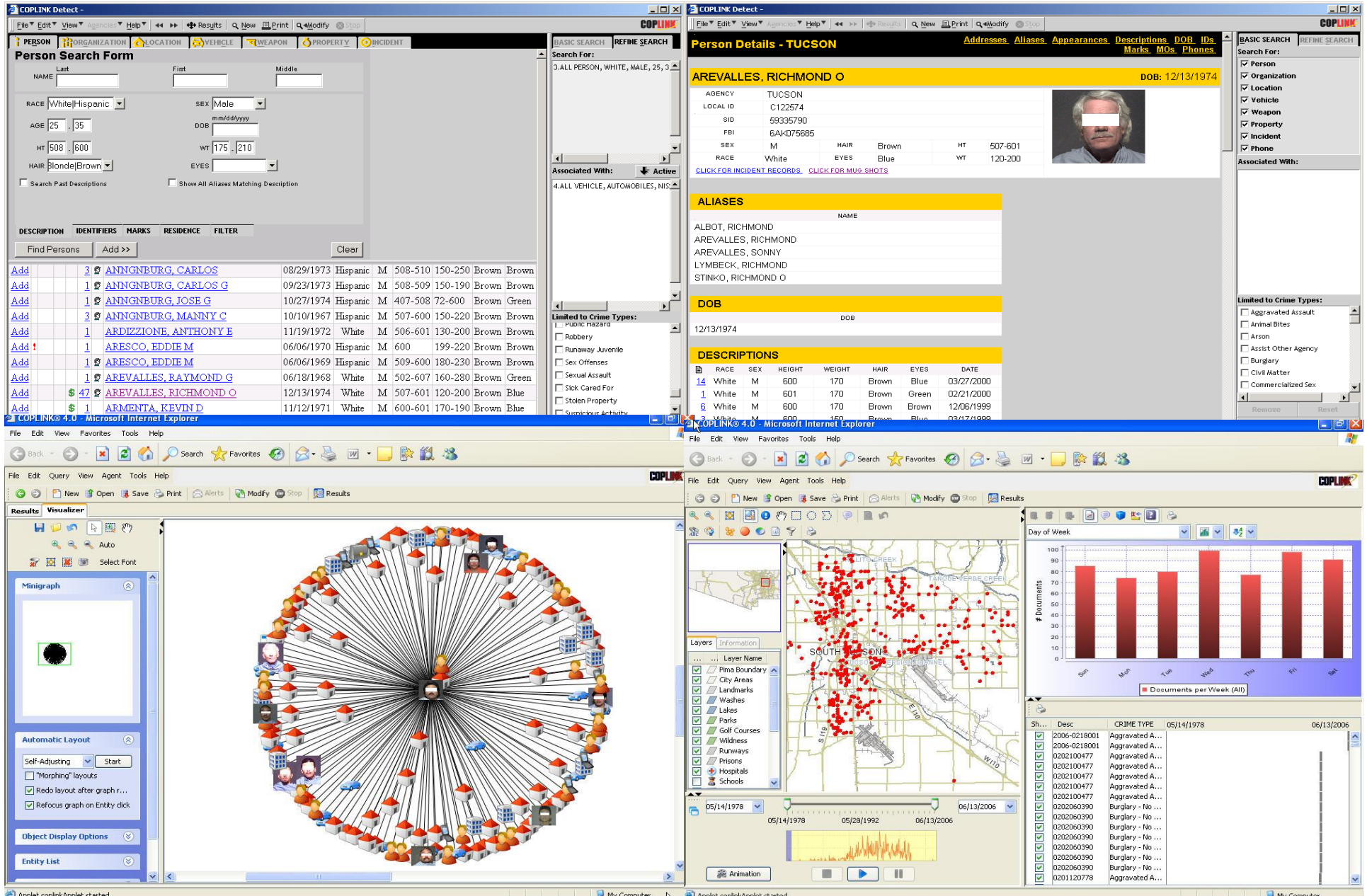
Dark Web

DarkNet

Hacker Web



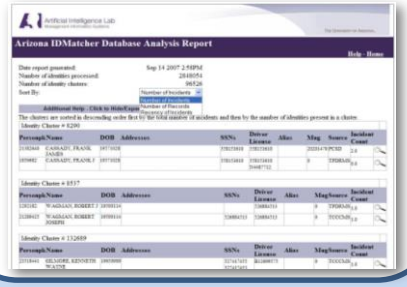
COPLINK: Crime Data Mining (1997-2009)



COPLINK Identity Resolution and Criminal Network Analysis

Cross-jurisdictional Information Sharing/Collaboration

Arizona IDMatcher



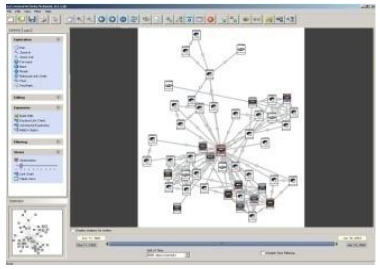
Law-enforcement Data

AZ | CA | TX

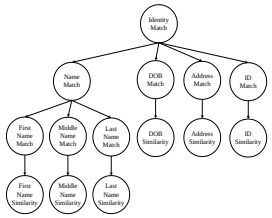
Border Crossing Data (AZ, CA, TX)

Vehicles | People

CAN Visualizer



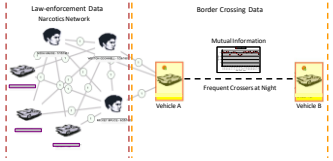
Identity Resolution



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

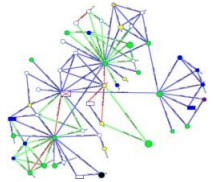
Criminal Network Analysis

High-risk Vehicle Identification



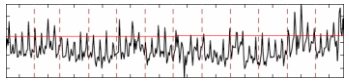
Identify high-risk vehicles using association techniques like mutual information using border crossing and law enforcement data.

Criminal Link Prediction



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

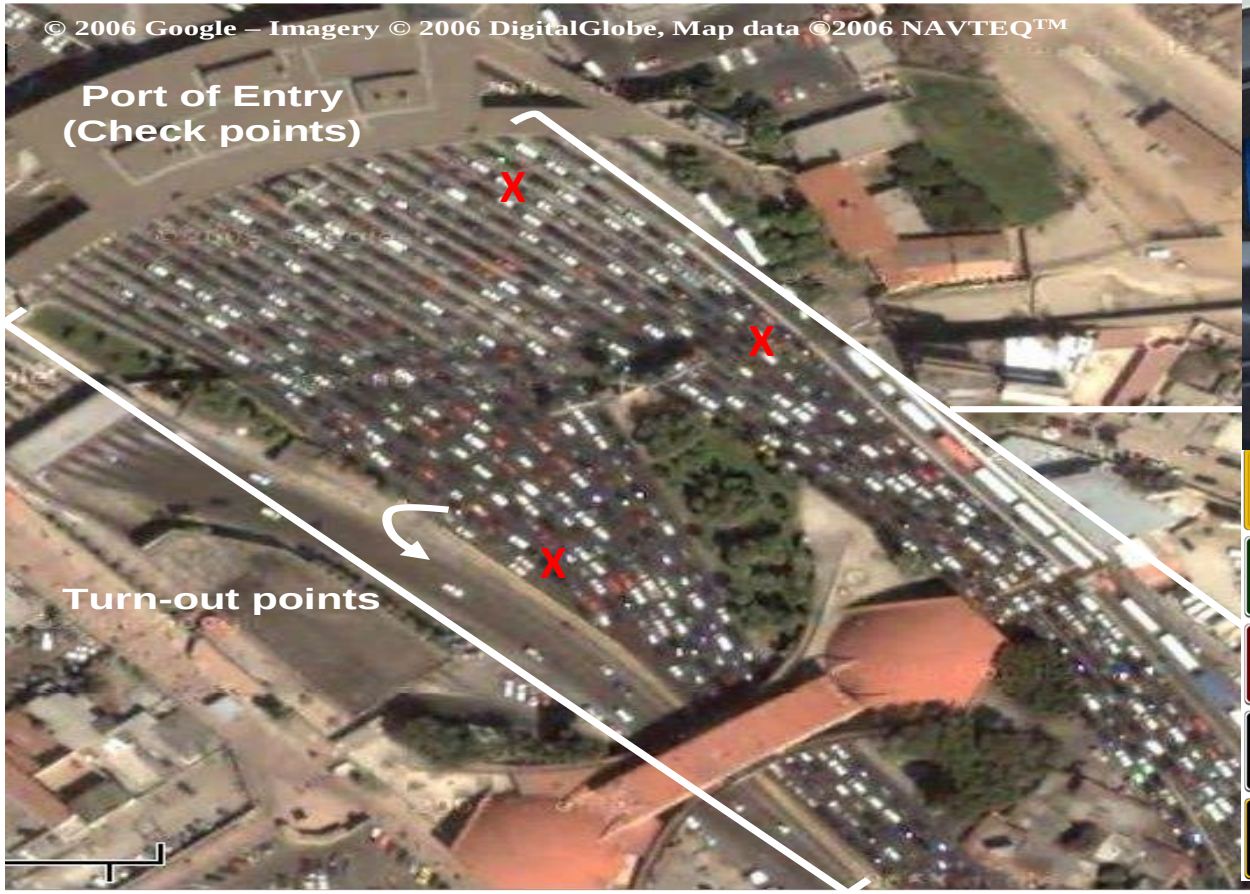
Suspect Traffic Burst Detection



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

Border Security: High-risk Vehicle Identification (LPR + DM/SNA)



COPLINK: Crime Data Mining

ABC News April 15, 2003

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

Arts & Ideas

The New York Times

SATURDAY, NOVEMBER 2, 2002

An Electronic Cop That Plays Hunches

Interconnecting Police Files Through New Computer System Helps Prosecutors in Sniper Case

By MINDY SINK

TUCSON, Oct. 28 — Officials building a case against the Washington-area sniper suspects are using a new investigative tool to help trace their movements across the country. It is an Internet-based system called Coplink, developed at an artificial intelligence laboratory here, that allows police departments to establish links quickly among their own files and to those of other departments.

During the 21 days in which snipers terrorized the area, investigators used everything from specialized ballistics testing to geographic and criminal profiling to radio and television announcements to track them down. Then, in what turned out to be the 11th hour of the pursuit, they finally reached out to Coplink. As it turned out, John Muhammad and Lee Malvo were arrested before it was fully installed, but now the post-arrest task force is using the system to help connect the dots.

All of the information that was collected — including that from other computer database systems like the Federal Bureau of Investigation's Rapidstart — is now being downloaded into the Coplink database so that the accumulated data can be compared, said Robert Griffin, president of Knowledge Computing Corporation of Tucson, which is turning the prototype in the laboratory into a commercial product. "The more data you get, the better Coplink works," he said.

Coplink was designed by Hsinchun Chen, the director of the Artificial Intelligence Laboratory at the University of Arizona. "It's the Google for law enforcement," he said, referring to a speedy popular Internet search engine that, given a couple of words, can find an array of related Web sites. "Things that a human can do intuitively we are getting the computer to do, too."

During the sniper investigation, which generated hundreds of thousands of tips, the number of potential clues to assimilate was daunting. "We were mobilizing a massive effort," said Lt. Mitch Cunningham of the Montgomery County police. "We had tactile resources, the military, federal, state and local law enforcement agencies and information technology using several products where each one of these had a role." So when the National Institute of Justice, the Justice Department's research and development arm, suggested that the sniper task force try Coplink, the officials agreed.

While no one is suggesting that old-fashioned detective work is being replaced by machines, the idea behind Coplink is to provide a computer program that can save busy police officers precious time and sometimes even help solve cases. That's some-

Agence France-Presse

Above, old-fashioned shoe leather still essential to the police. Left, Hsinchun Chen, the director of the Artificial Intelligence Laboratory at the University of Arizona, who has developed Coplink, a new investigative tool that he says can consolidate and analyze police data nationwide.

Chris Richards for The New York Times

at the scene, "Shorty did it." The name Shorty was put into Coplink and cross-referenced with the victim's personal data, and within minutes the records showed that the two men had been in prison together.

The program also allows users to look at lists of data or to create graphs and charts showing affiliations among different criminals.

At the moment, the Tucson Police Department is the only one in the country where Coplink is fully installed, although about a half-dozen other cities have begun to introduce Coplink into their existing computer systems. The cost of the program and

IBM i2 COPLINK

Accelerating law enforcement investigations

Palantir **($54B, IPO 2020)**

abc NEWS

Newsweek

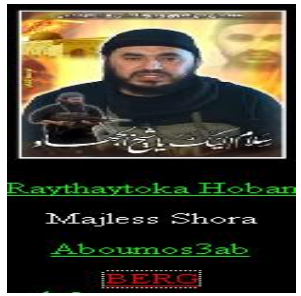
COPLINBK Commercialization Timeline

- **1994-1997, NSF DLI projects, DL, SE**
- **1997, NIJ $1.2M project, UA/TPD**
- **2000, NSF DG $1.6M, UA/TPD/PPD**
- **2000, KCC founding, UA tech transfer; $2.6M VC funding**
- **2001, Tucson, Phoenix, San Diego**
- **2002, bubble burst, $2M additional funding (anti-dilution clause)**
- **2003, DC snipper investigation use, NYT cover article; AZ, CA, NJ, IL**
- **2009, SilverLake PE fund; COPLINK + i2**
- **2011, sold to IBM ($500M); Chen exit**
- **2017, IBM sold COPLINK to Forensic Logic**

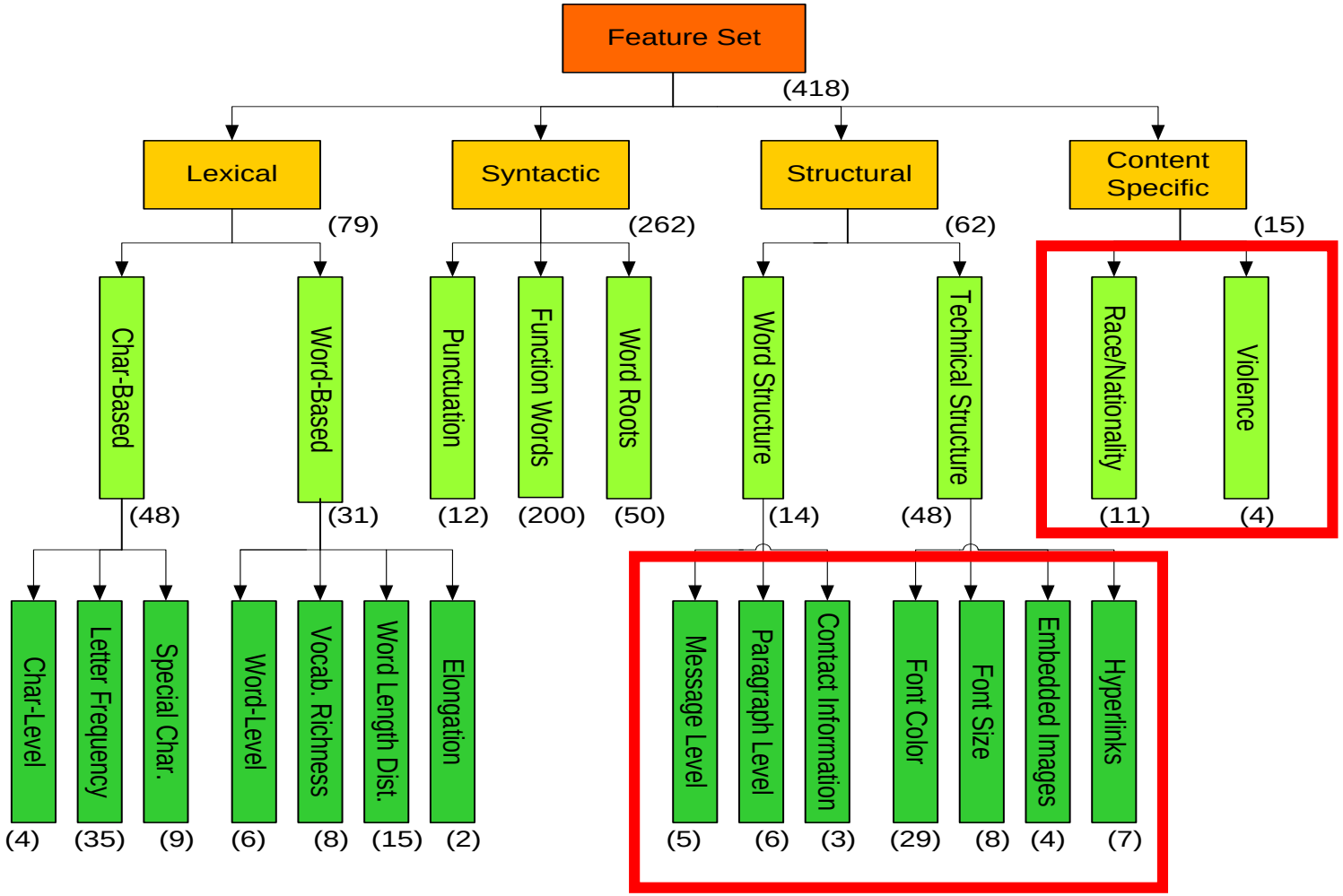
➔ COPLINK is in use in 5,000+ law enforcement jurisdictions and intelligence agencies in the U.S. and Europe, making significant contribution to public safety worldwide.

Dark Web: Countering Terrorism (2003-2014)

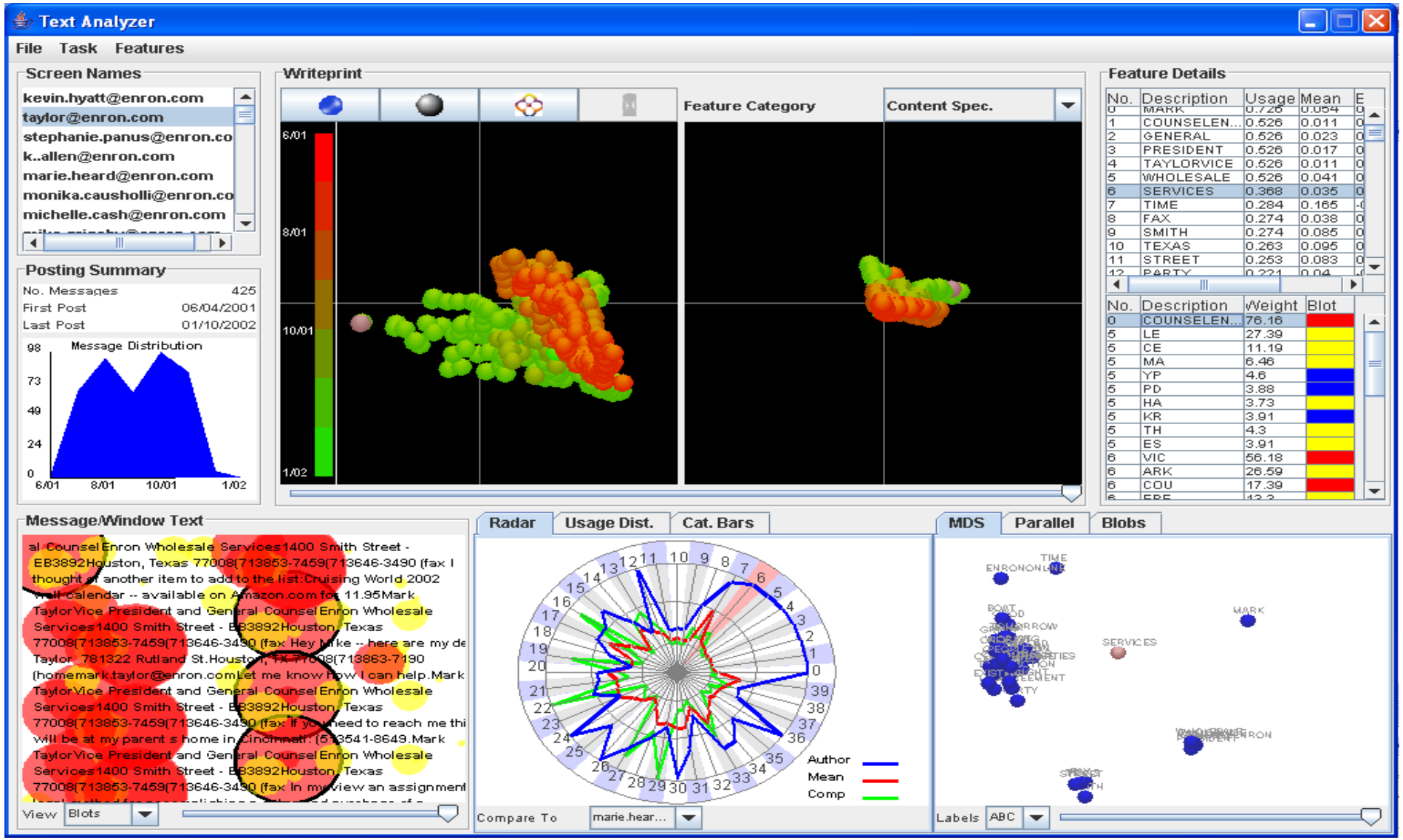
- Dark Web: Terrorists' and cyber criminals' use of the Internet
- Collection: Web sites, forums, blogs, YouTube, etc.
- 20 TBs in size, with close to 10B pages/files/messages (the entire LOC collection: 15 TBs)



Arabic Writeprint Feature for Authorship Analysis



CyberGate (Abbasi, et al., MISQ, 2008)



The Dark Web project in the Press

Associated Press

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

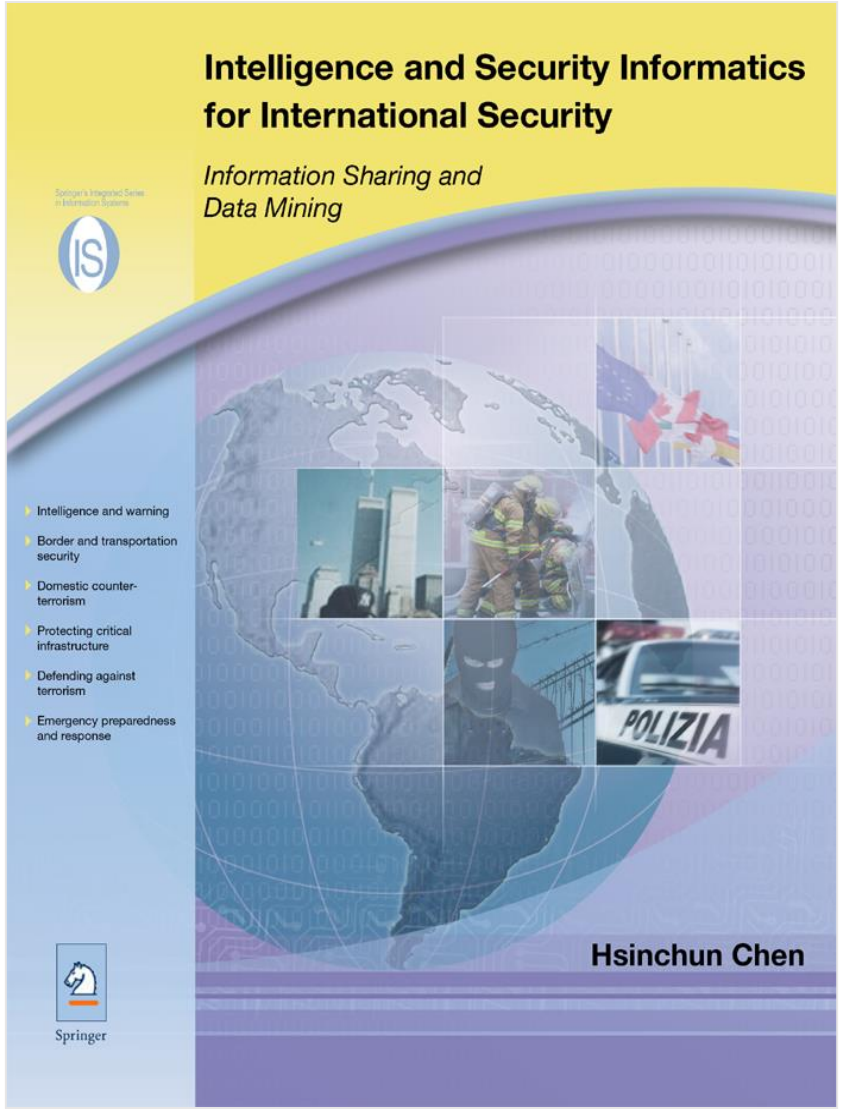
USA TODAY

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

npr

Mathematicians Work to Help Track Terrorist Activity, 9/14/2007

ISI, Springer, 2006

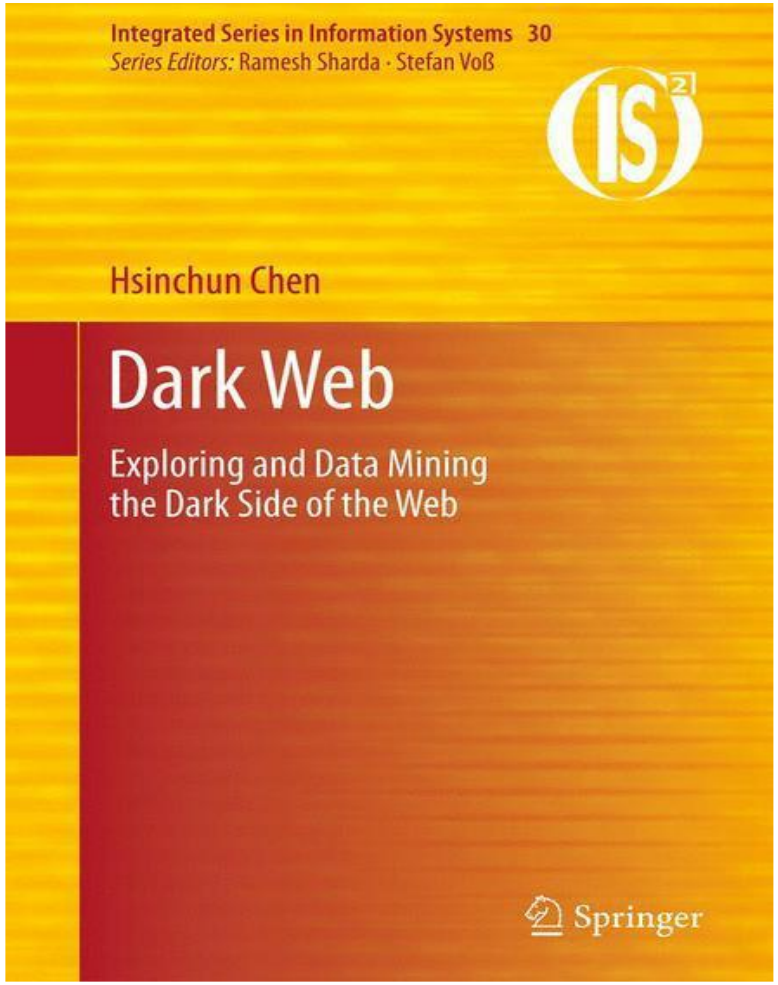


- Intelligence and Security Informatics (ISI) (Chen, *2006*)

- Data, text, and web mining
- From COPLINK to Dark Web

- **IEEE ISI, EISIC, PAISI ➔ 4000+ scholars, since 2003**

Dark Web, Springer, 2012



22 chapters, 451 pages, 150 illustrations (81 in color); Springer Integrated Series in Information Systems, 2012.

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

AZSecure Cybersecurity Analytics Program (2010-present): SaTC, SFS, ACI

Secure and Trustworthy Cyberspace (SaTC)

PROGRAM SOLICITATION
NSF 21-500

REPLACES DOCUMENT(S):
NSF 19-603

National Science Foundation

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

CyberCorps(R) Scholarship for Service (SFS)
Defending America's Cyberspace

PROGRAM SOLICITATION
NSF 21-580

REPLACES DOCUMENT(S):
NSF 19-521

National Science Foundation

Directorate for Education and Human Resources
Division of Graduate Education

Cybersecurity Innovation for Cyberinfrastructure (CICI)

PROGRAM SOLICITATION
NSF 21-512

REPLACES DOCUMENT(S):
NSF 19-514

National Science Foundation

Directorate for Computer and Information Science and Engineering
Office of Advanced Cyberinfrastructure

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.

nature doi:10.1038/nature16961

Mastering the game of Go with deep neural networks and tree search

David Silver[1]*, Aja Huang[1]*, Chris J. Maddison[1], Arthur Guez[1], Laurent Sifre[1], George van den Driessche[1], Julian Schrittwieser[1], Ioannis Antonoglou[1], Veda Panneershelvam[1], Marc Lanctot[1], Sander Dieleman[1], Dominik Grewe[1], John Nham[2], Nal Kalchbrenner[1], Ilya Sutskever[2], Timothy Lillicrap[1], Madeleine Leach[1], Koray Kavukcuoglu[1], Thore Graepel[1] & Demis Hassabis[1]

nature doi:10.1038/nature24270

Mastering the game of Go without human knowledge

David Silver[1]*, Julian Schrittwieser[1]*, Karen Simonyan[1]*, Ioannis Antonoglou[1], Aja Huang[1], Arthur Guez[1], Thomas Hubert[1], Lucas Baker[1], Matthew Lai[1], Adrian Bolton[1], Yutian Chen[1], Timothy Lillicrap[1], Fan Hui[1], Laurent Sifre[1], George van den Driessche[1], Thore Graepel[1] & Demis Hassabis[1]

AI & Deep Learning: From AlphaGo to Autonomous Vehicles (2012-)

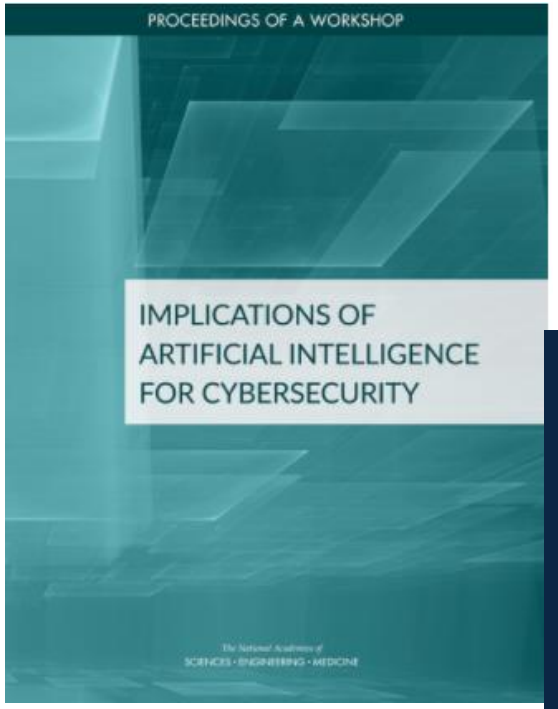
➔

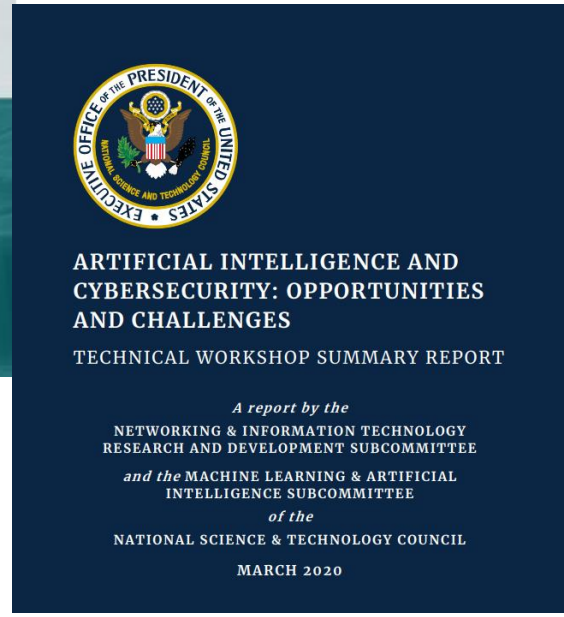
Hacker Web, AZSecure projects at UA/MIS AI Lab (2010-present)

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

MIS Quarterly

SPECIAL ISSUE

MOVING TOWARD BLACK HAT RESEARCH IN INFORMATION SYSTEMS SECURITY: AN EDITORIAL INTRODUCTION TO THE SPECIAL ISSUE

By: M. Adam Mahmood
University of Texas at El Paso
mmahmood@utep.edu

Mikko Siponen
University of Oulu, Finland
mikko.siponen@oulu.fi

Detmar Straub
Georgia State University
dstraub@gsu.edu

H. Raghav Rao
State University of New York at Buffalo
mgmtrao@buffalo.edu

T. S. Raghu
Arizona State University
raghu.santanam@asu.edu

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 digress from the tradition of summarizing the papers in-depth and, instead, would like to take this opportunity to encourage researchers to conduct

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 overemphasizing 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 readier 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 Nunamaker 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

National Science Foundation
WHERE DISCOVERIES BEGIN

QUICK LINKS

SEARCH

HOME | FUNDING | AWARDS | DISCOVERIES | NEWS | PUBLICATIONS | STATISTICS | ABOUT NSF | FASTLANE

Email Print Share

Discoveries

Discoveries
Search Discoveries
About Discoveries

Discoveries by Research Area
Arctic & Antarctic
Astronomy & Space
Biology
Chemistry & Materials
Computing
Earth & Environment
Education
Engineering
Mathematics
Nanoscience
People & Society
Physics

Discovery

When hackers talk, this research team listens

Online conversations help fill critical gap in cybersecurity knowledge about attackers' motivations, possible targets

NSF-supported researchers have shed new light on how hackers communities interact.
Credit and Larger Version

October 8, 2015

Hsinchun Chen leads a research project that explores the motivations of cyberattackers.
Credit and Larger Version

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-

Secure and Trustworthy Cyberspace (SaTC)

PROGRAM SOLICITATION
NSF 21-500

REPLACES DOCUMENT(S):
NSF 19-603

National Science Foundation

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

CyberCorps(R) Scholarship for Service (SFS)
Defending America's Cyberspace

PROGRAM SOLICITATION
NSF 21-580

REPLACES DOCUMENT(S):
NSF 19-521

National Science Foundation

Directorate for Education and Human Resources
Division of Graduate Education

Cybersecurity Innovation for Cyberinfrastructure (CICI)

PROGRAM SOLICITATION
NSF 21-512

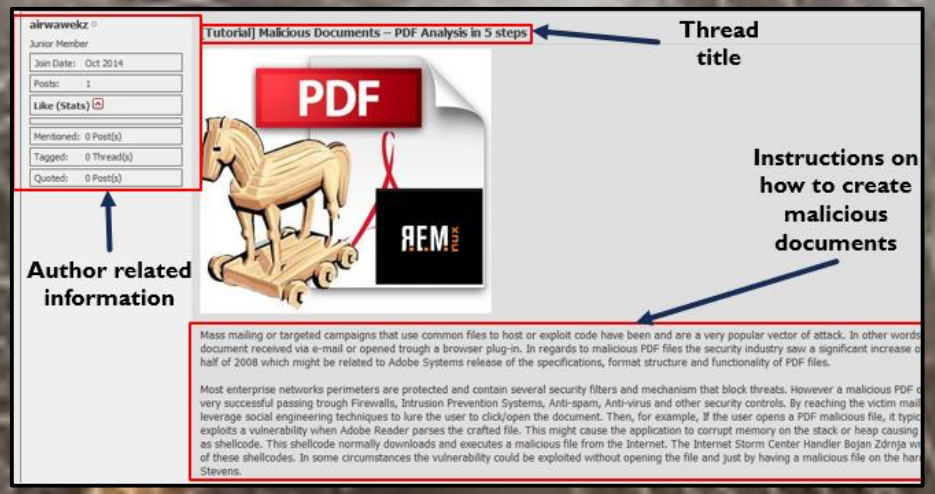
REPLACES DOCUMENT(S):
NSF 19-514

National Science Foundation

Directorate for Computer and Information Science and Engineering
Office of Advanced Cyberinfrastructure

Hacker Web

Forum post with source code to exploit Mozilla Firefox 3.5.3



Tutorial on how to create malicious documents

Forum post with BlackPOS malware attachment.

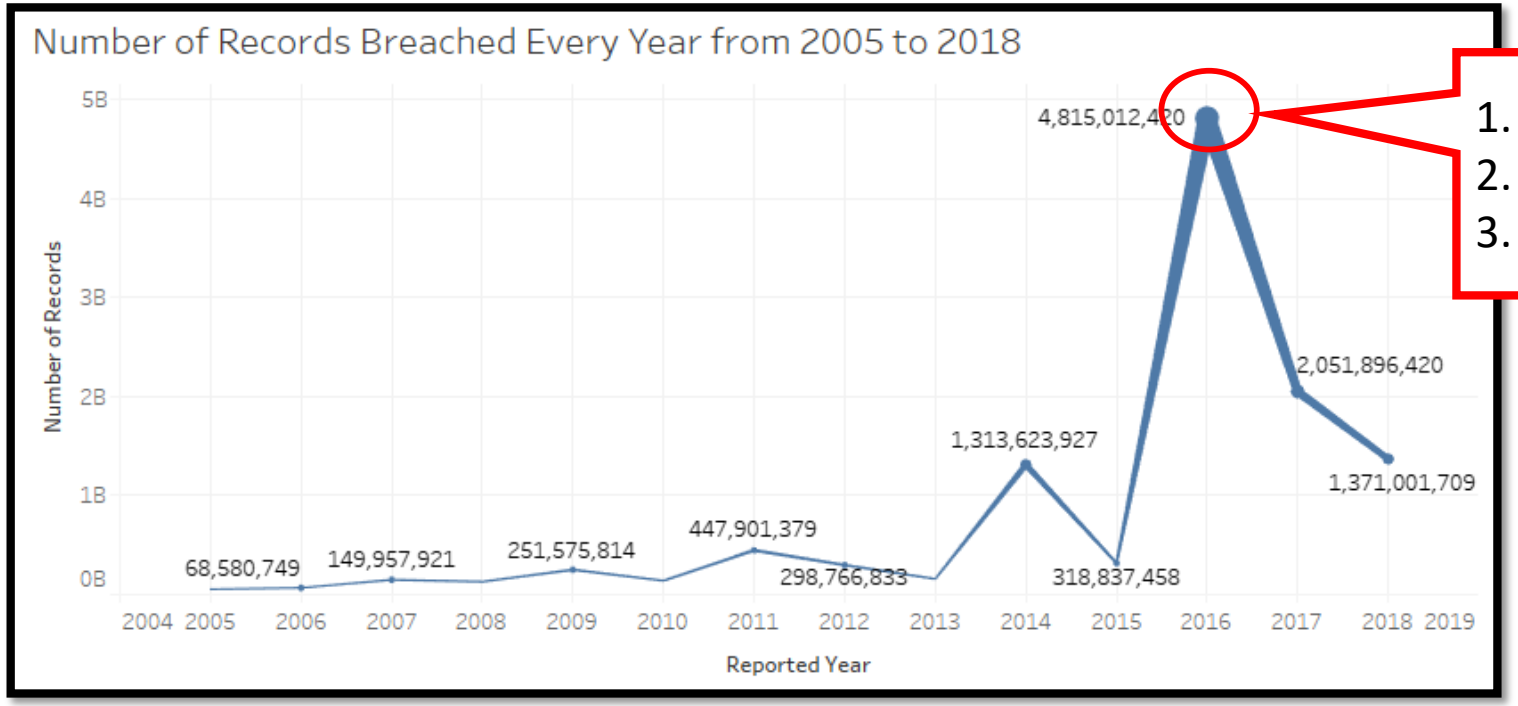
Selected data breaches in 2014

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

Are your data breached? Do you even know?

Data Breaches since 2005 (FTC, Clearinghouse, 2019)

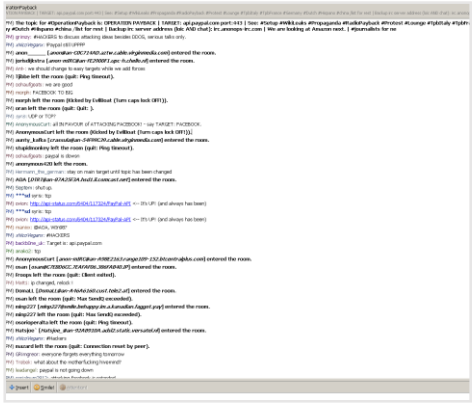
- # of records breached: 11,582,808,013
- # of data breaches: 9,071



2016 Data Breach

1. Yahoo! : 3.5B user accounts
2. FriendFinder : 412M user accounts
3. MySpace : 360M passwords

Hacker Community Platforms – *"Know your enemy"*

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

US → cybercrime and general hacking
Russia → underground economy, financial fraud
China → cyberwarfare content

MIS Quarterly

MIS Quarterly Vol. 43 No. 1, pp. 1-22/March 2019

METHODS ARTICLE

DICE-E: A FRAMEWORK FOR CONDUCTING DARKNET IDENTIFICATION, COLLECTION, EVALUATION WITH ETHICS[1]

Victor Benjamin

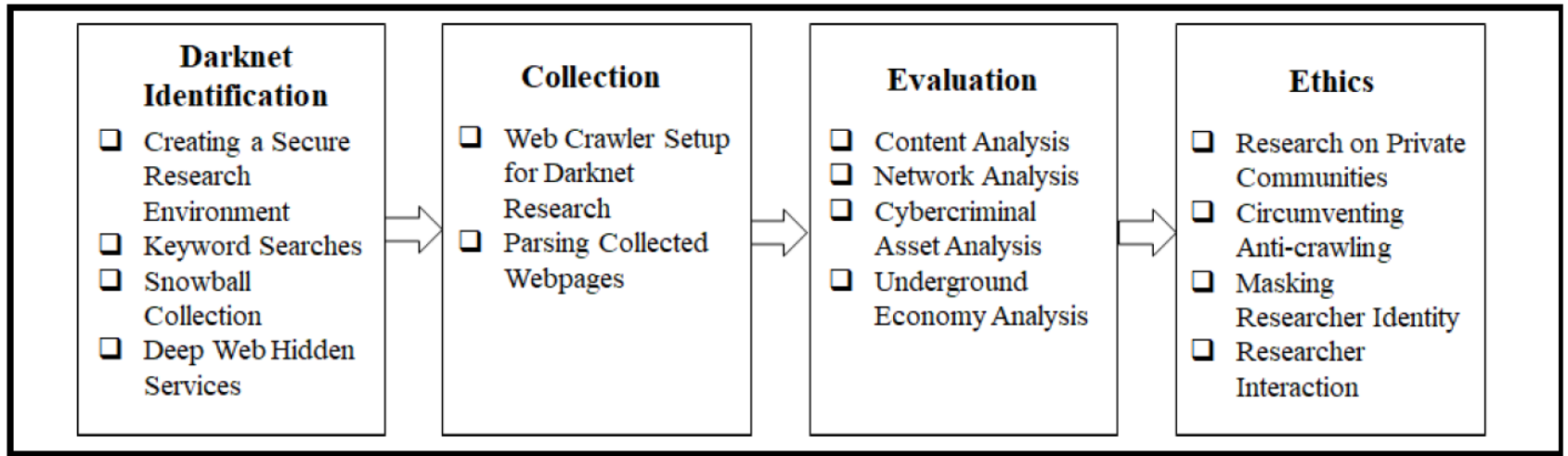


Figure 2. The DICE-E Framework

Identify Hacker Assets/Tools

Sagar Samtani (JMIS, January 2018)

Routledge
Taylor & Francis Group

Journal of Management Information Systems

ISSN: 0742-1222 (Print) 1557-928X (Online) Journal homepage: http://www.tandfonline.com/loi/mmis20

Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence

Sagar Samtani, Ryan Chinn, Hsinchun Chen & Jay F. Nunamaker Jr.

Hacker Asset/Tool Examples

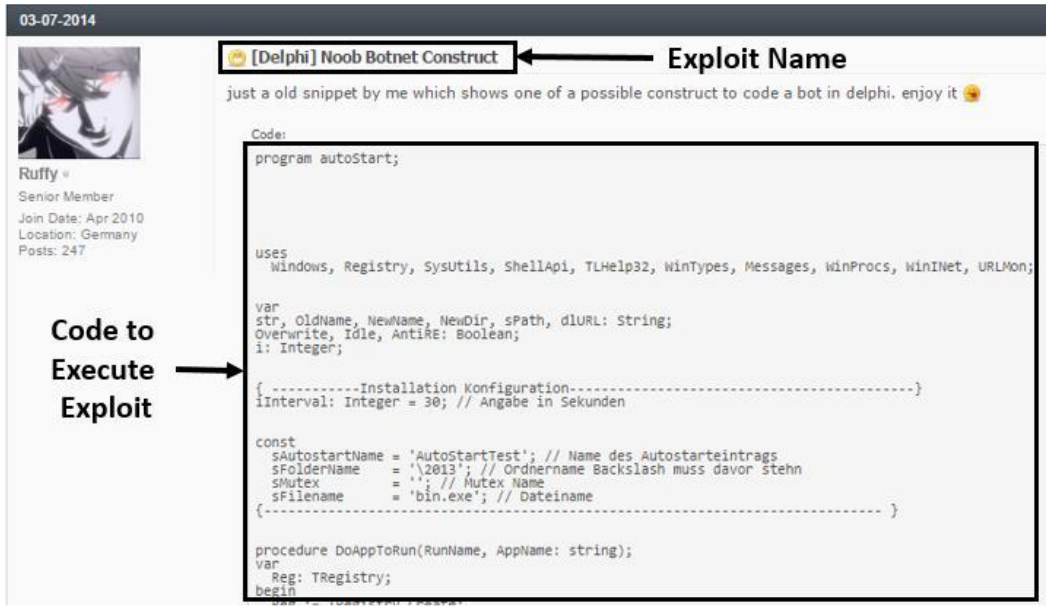


Figure 1. Forum post with source code to create botnets

Figure 2. Forum post with BlackPOS malware attachment

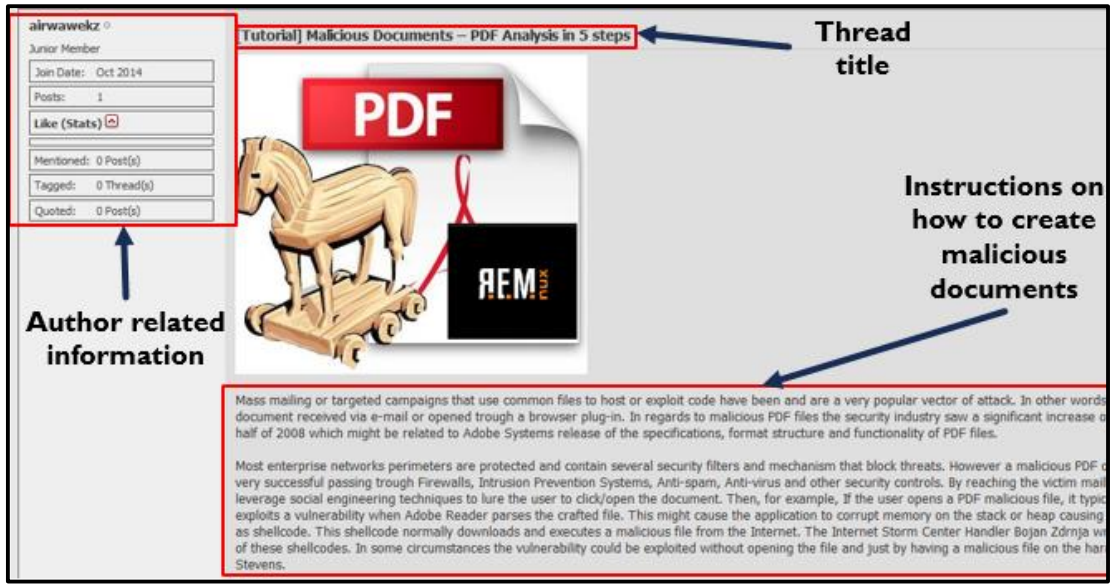
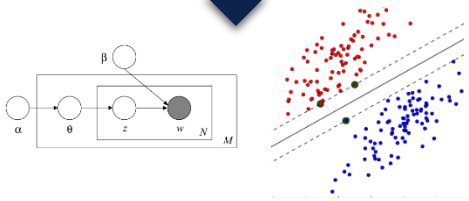


Figure 3. Tutorial on how to create malicious documents

AZSecure Hacker Assets Portal System

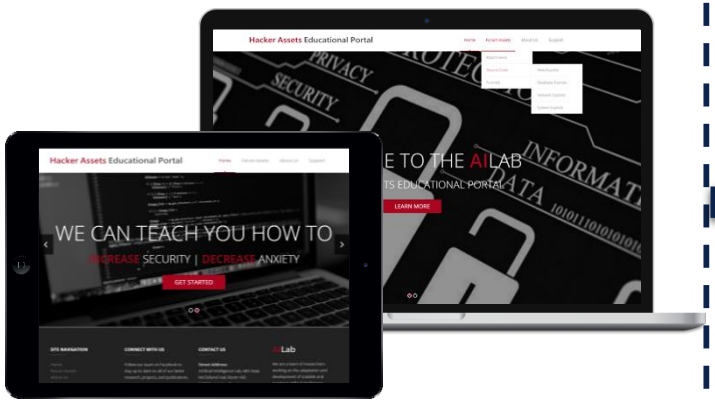
Data Collection and Analytics



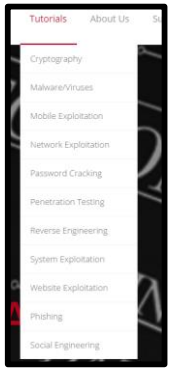
Latent Dirichlet Allocation (LDA) and Support Vector Machine (SVM) Analytics

987 tutorials, 15,576 source code, and 14,851 attachments

Web Hosting and Access



System Functionalities

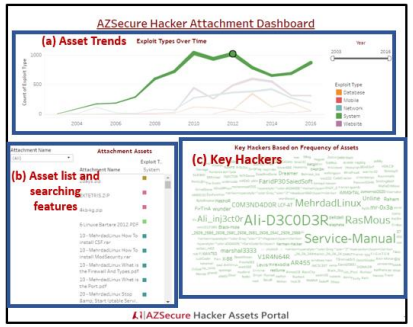


Browsing

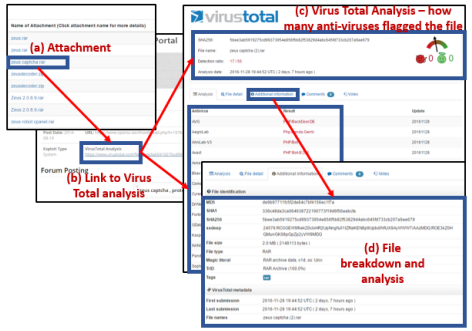
Searching

Downloading

System Analytics



Cyber Threat Intelligence Dashboard

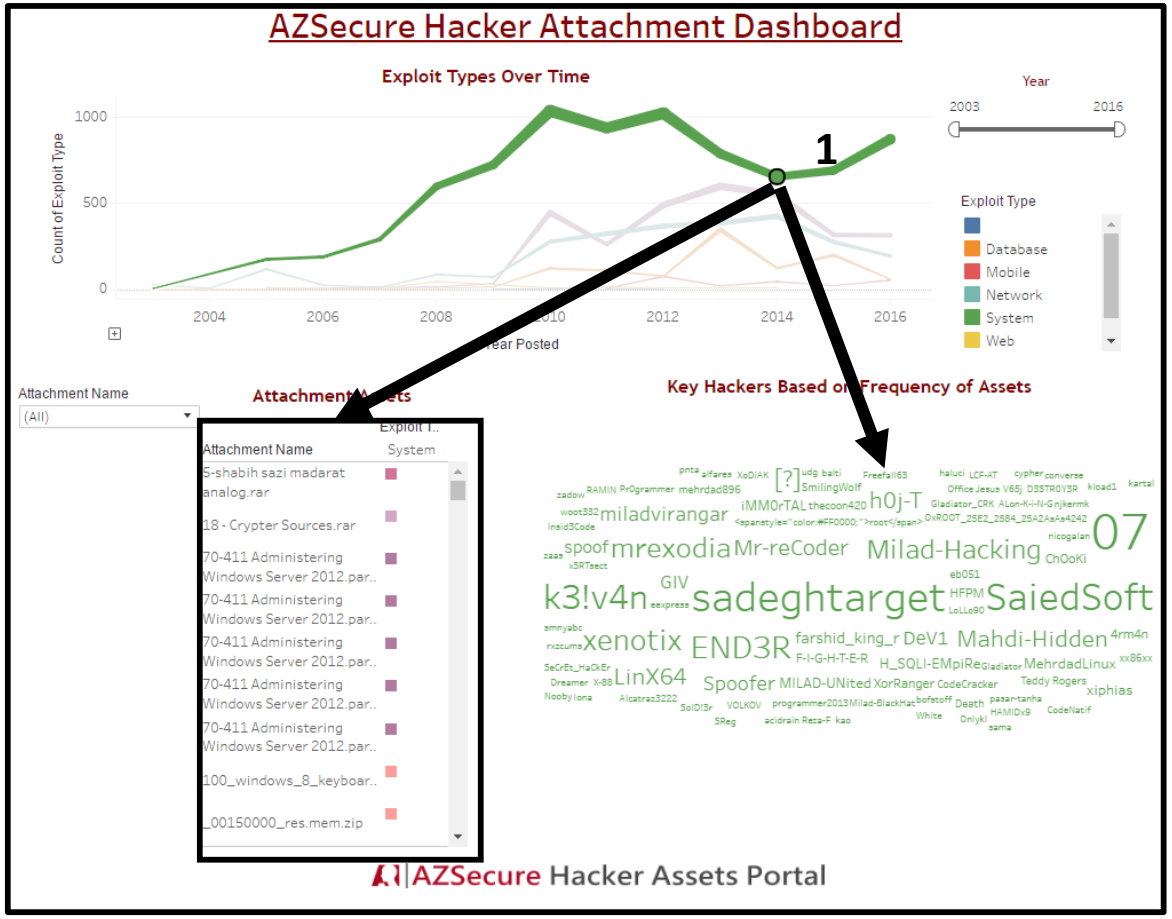


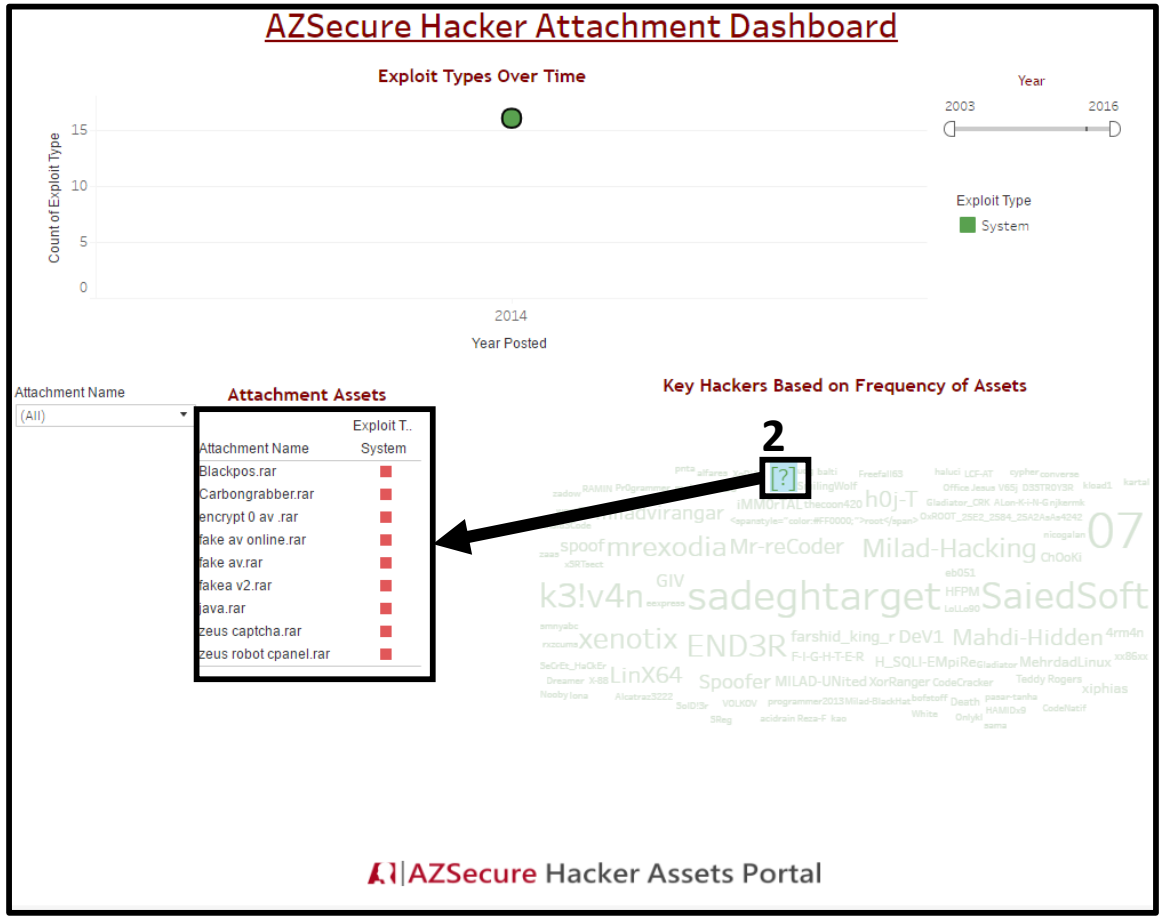
VirusTotal Malware Analysis

AZSecure Hacker Assets Portal (English, Russian, Arabic)

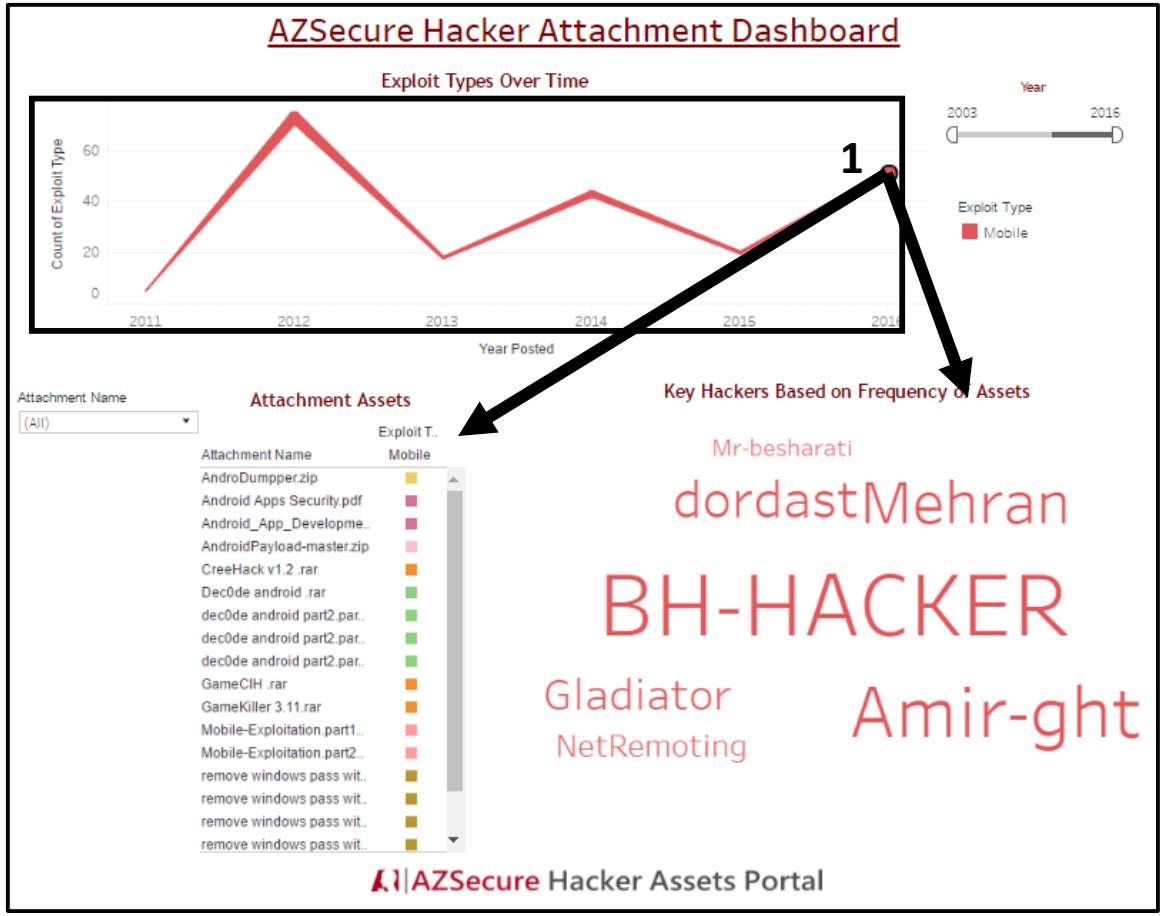
Forum	Language	Date Range	# of Posts	# of Members	# of source code	# of attachments	# of tutorials
OpenSC	English	02/07/2005-02/21/2016	124,993	6,796	2,590	2,349	628
Xeksec	Russian	07/07/2007- 9/15/2015	62,316	18,462	2,456	-	40
Ashiyane	Arabic	5/30/2003 – 9/24/2016	34,247	6,406	5,958	10,086	80
tuts4you	English	6/10/2006 – 10/31/2016	40,666	2,539	-	2,206	38
exelab	Russian	8/25/2008 – 10/27/2016	328,477	13,289	4,572	-	628
Total:	**-**	**02/07/2005- 10/31/2016**	**590,699**	**47,492**	**15,576**	**14,851**	**987**

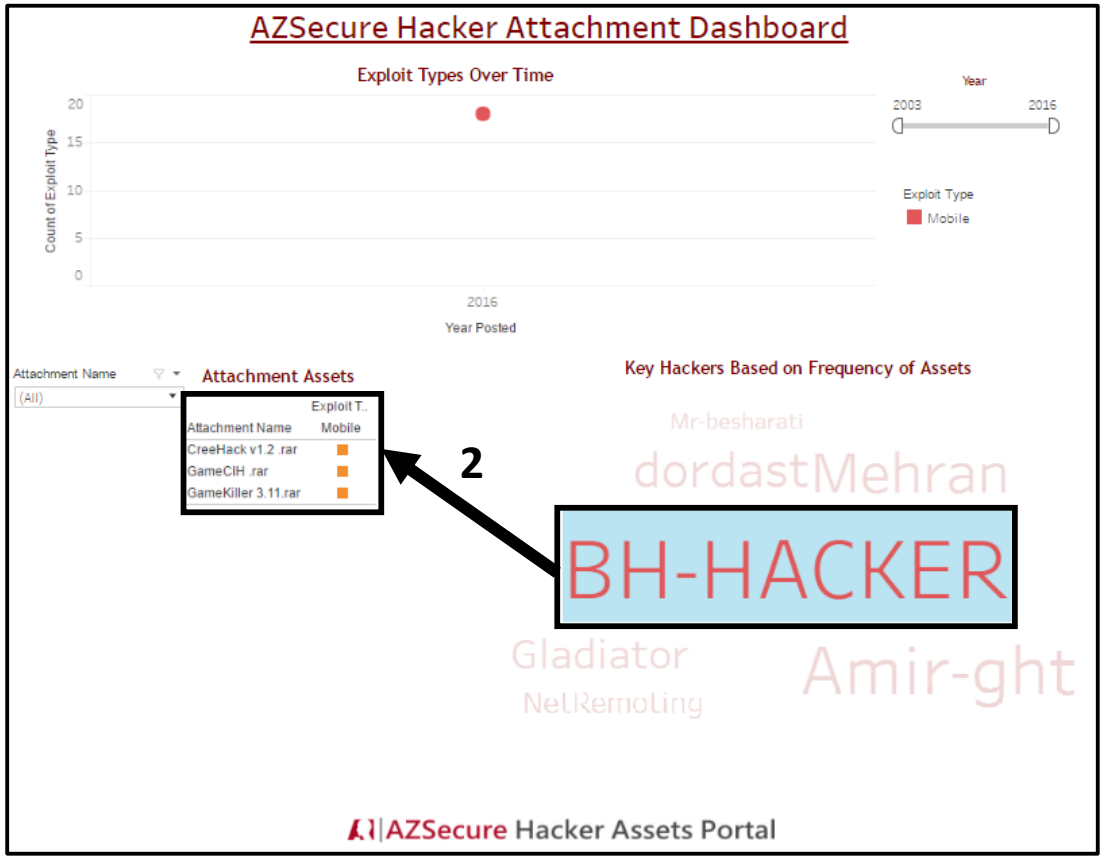
Cyber Threat Intelligence (CTI) Example – Bank Exploits (e.g., BlackPOS)





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))

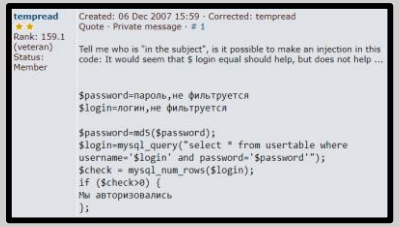
Literature Review: Hacker Forum Exploit Analysis

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

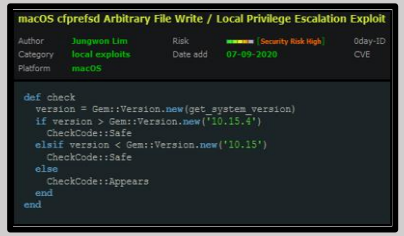
- **Key Observations:**
  1. Studies focus on general forums, but not exploit DNMs or public repositories.
  2. Although source code contains valuable information, many studies omit them from analysis.
  3. The most common task is to categorize post content by exploit category.

Proposed Research Design

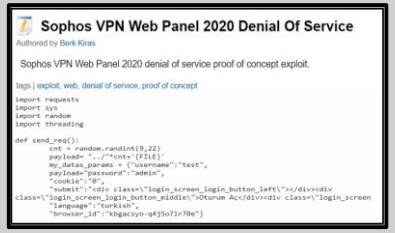
Data Collection



Traditional Hacker Forums



Exploit DNMs



Public Exploit Repositories

Pre-Processing and Dataset Construction

Programming Language Classifier

↓

Remove stop words, low frequency words, and lemmatize

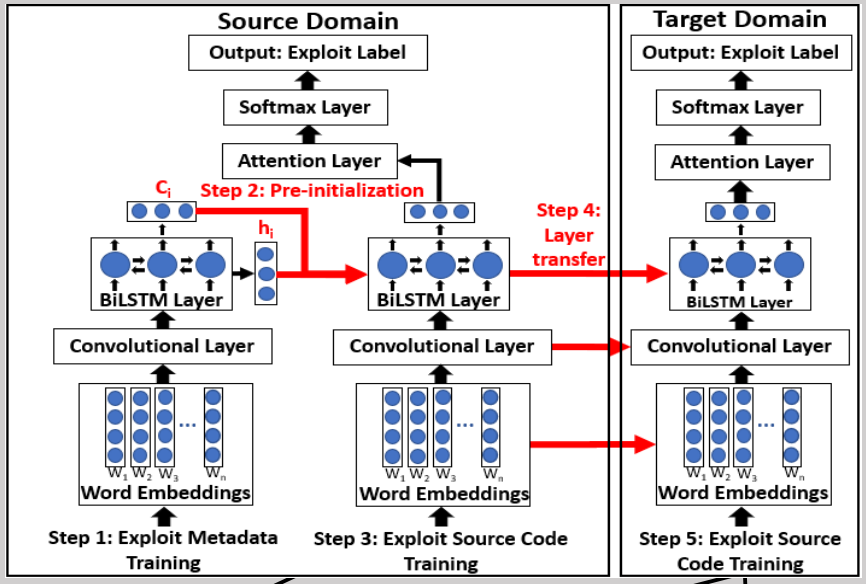
↓

Tokenizer and Sequence Padder

↓

Gold-Standard Dataset Construction

Deep Transfer Learning Exploit Labeler (DTL-EL) Model



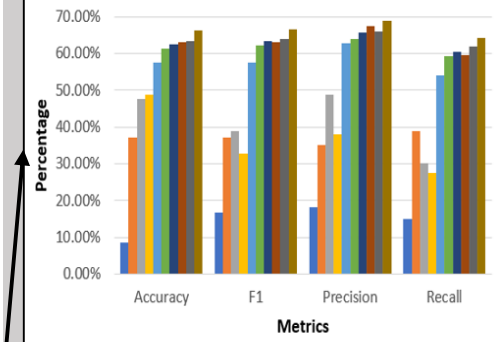
Experiment 1: DTL-EL against prevailing classification methods on source domain

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

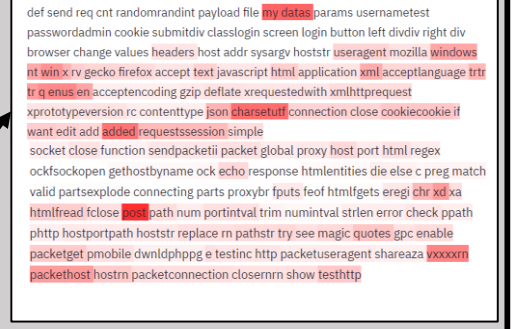
Experiment 3: DTL-EL against transfer learning layer selection on target domain

Evaluations and Visualization

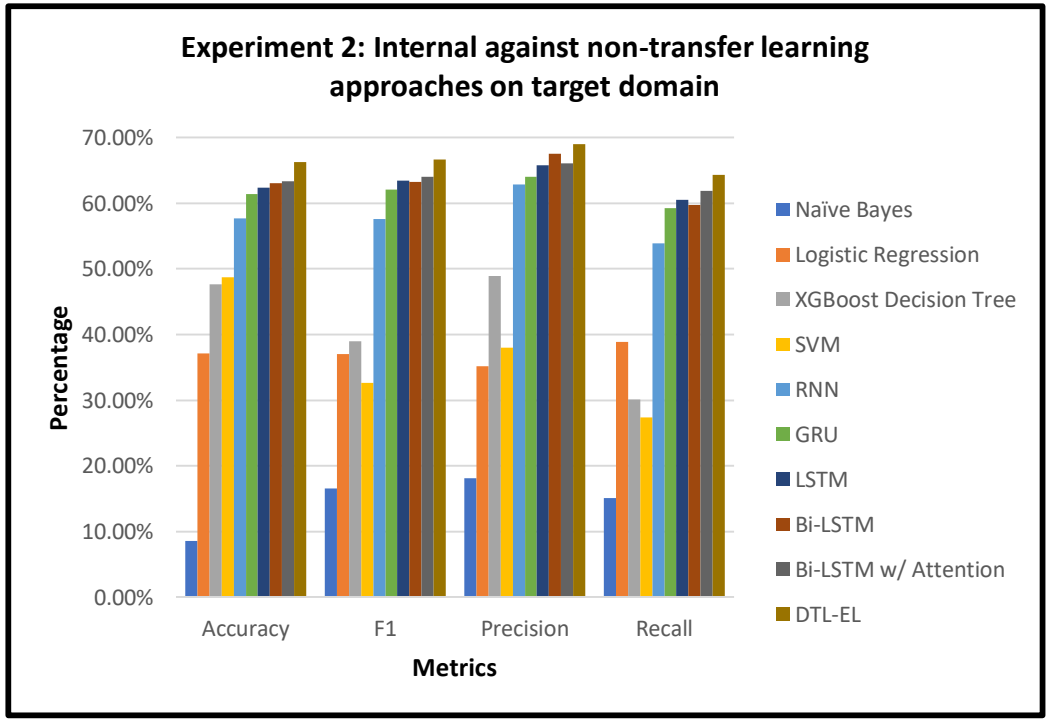
Benchmark Comparisons



Visualized Attention Comparison



Results and Discussion: DTL-EL Model



Experiment 2: Internal against non-transfer learning models		Results			
Model	**Layer Weights**	**Accuracy**	**Precision**	**Recall**	**F1**
Naïve Bayes	Random	8.59% ***	18.09% ***	15.08% ***	16.45% ***
Logistic Regression	Random	37.16% ***	35.13% ***	38.85% ***	36.9% ***
XGBoost Decision Tree	Random	47.65% ***	48.87% ***	30.06% ***	37.22% ***
SVM	Random	48.72% ***	37.98% ***	27.38% ***	31.82% ***
RNN	Random	57.64% ***	62.89% ***	53.93% ***	57.62% ***
GRU	Random	61.34% ***	64.06% ***	59.27% ***	62.09% ***
LSTM	Random	62.39% ***	65.77% ***	60.49% ***	63.42% ***
BiLSTM	Random	63.05% ***	67.56% ***	59.71% ***	63.21% ***
BiLSTM w/ Attention	Random	63.38% ***	66.04% ***	61.88% ***	64.02% ***
DTL-EL (Our model)	Transferred	**66.17%**	**68.25%**	**64.99%**	**66.61%**

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.

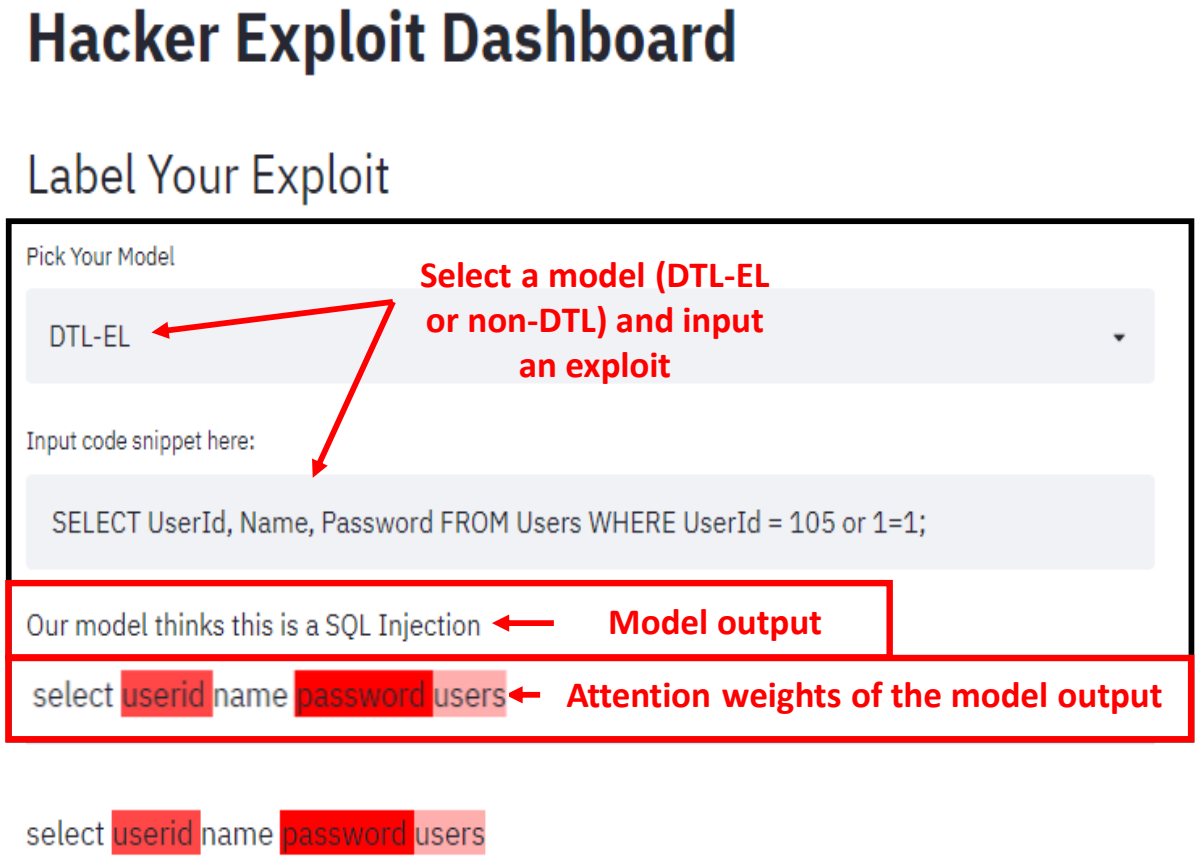


Figure 16. Hacker Exploit Portal For Further Analysis

Detecting Cyber Threats with AI Agents: Multilingual, Multimedia DNM Content

Reza Ebrahimi (JMIS, MIS, IEEE PAMI)

Detecting Cyber Threats with AI Agents

- **Intelligence Source:** Dark web
  - A large conglomerate of platforms that facilitate illegal transactions among hackers
- **DarkNet Market Places** (Amazon for illegal products; hidden from search engines) → Attract cybercriminals
  - **Hacker Assets:** Hacking tools (Remote Access Trojan); malicious executables; hacking tutorials
  - **Non-Hacker Assets:** Digital goods (credit card information); copyrighted software; pirated e-books; counterfeits; drugs; forged documents

Dark Net Marketplaces (DNMs)

- Other 654
- Security 388
- Software 1061

- Digital Goods 43611
- Drugs 46109
- Drugs Paraphernalia 278
- Services 3835
- Other 3370

฿ Exchange

BTC	1.0
mBTC	1000.0
USD	16088.0
EUR	13729.3
GBP	12040.6
CAD	20552.8
AUD	20758.8
SEK	134094.9
NOK	130044.7
DKK	102160.3
TRY	61054.5
CNH	105455.4
HKD	124855.0
RUB	931264.5
INR	1030953.6
JPY	1822398.0

Onion mirrors

t3e6ly3uoif4zcw2.onion
verified

jd6yhuwcivehvdt4.onion
t3e6ly3uoif4zcw2.onion
7ep7acrkunzdcw3l.onion
vilpaqbrnvizecjo.onion
igyifrhnvxq33sy5.onion
6qlocfg6zq2kyacl.onion
x3x2dwb7jasax6tq.onion
bkjcpa2klkkmowwq.onion
xytjqcfendzeby22.onion
nhib6cwhfsoyiugv.onion
k3pd243s57fttnpa.onion

19 20 ... 44 45 46 47 48 49 50 51 52 53 54

Hacking For Newbies
฿0.0000621
HappyEyes (5200) (4.79★)
WW → WW
ESCROW Order

731986-Hacker's Desk Reference
฿0.0001864
color (8000) (4.76★)
GB → WW
ESCROW Order

Premium Carding Package
฿0.0003107
OnePiece (7400) (4.83★)
PH → WW
ESCROW Order

6 BITCOIN RANSOMWARE EASY MONEY SYSTEM
฿0.0003107
TheWealthMaker (1550) (4.78★)
WW → WW
ESCROW Order

Go to Windows updates anonymously
฿0.0000621
HappyEyes (5200) (4.79★)
WW → WW
ESCROW Order

HACK ANYONE USING THEIR IP ADDRESS
฿0.0002486
TopNotchMoneyMaker (4500) (4.74★)
WW → WW
ESCROW Order

PayPal - Scam Page (Phising site) [Looks Great]
฿0.00031
MicroDroper (2350) (4.91★)
WW → WW
ESCROW Order

PASSWORD MANAGER KIT
฿0.0001224
ElCartel (1800) (4.86★)
WW → WW
ESCROW Order

PayPal - Scam Page (Phising site) [Looks Great]

Vendor	MicroDroper (2350) (4.91★) (ⓐ 67/1/3)
Price	฿0.00031 ($4.99)
Ships to	Worldwide, Worldwide
Ships from	PM
Escrow	Yes

Seller

Price

Product Description

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

฿0.00 ($0) You will get download link

Quantity 1 Add to cart

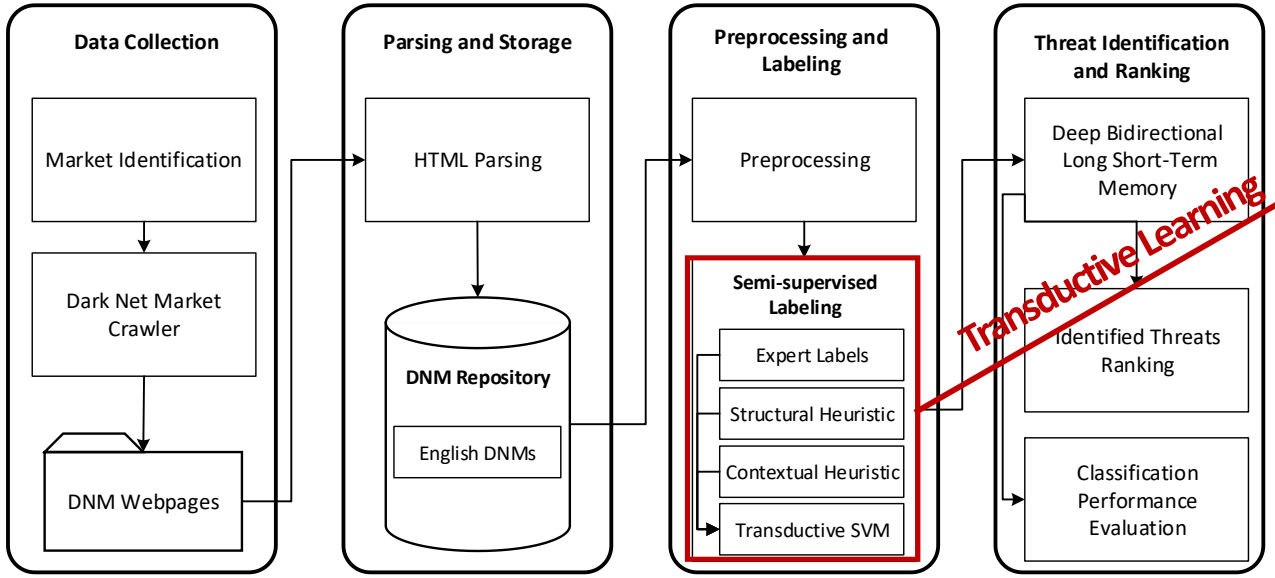
Product Reviews

Product ratings

53d ★★★★★ Enter your comments here

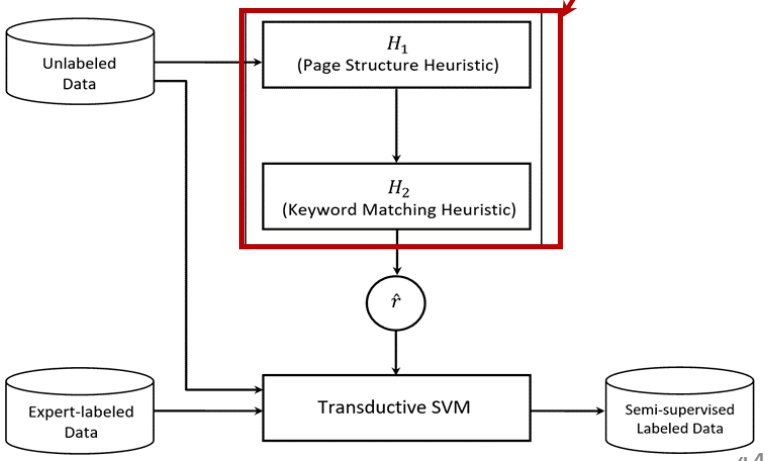
Essay I: Learning From Unlabeled Cybersecurity Content (JMIS, March 2020)

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



$$\min_{w}\left(\frac{\lambda}{2}\|w\|^2+\frac{1}{2L}\sum_{i=1}^{L} l(y_i, w^T x_i)+\frac{\lambda'}{2U}\sum_{j=1}^{U} l(y_i', w^T x_j')\right)$$

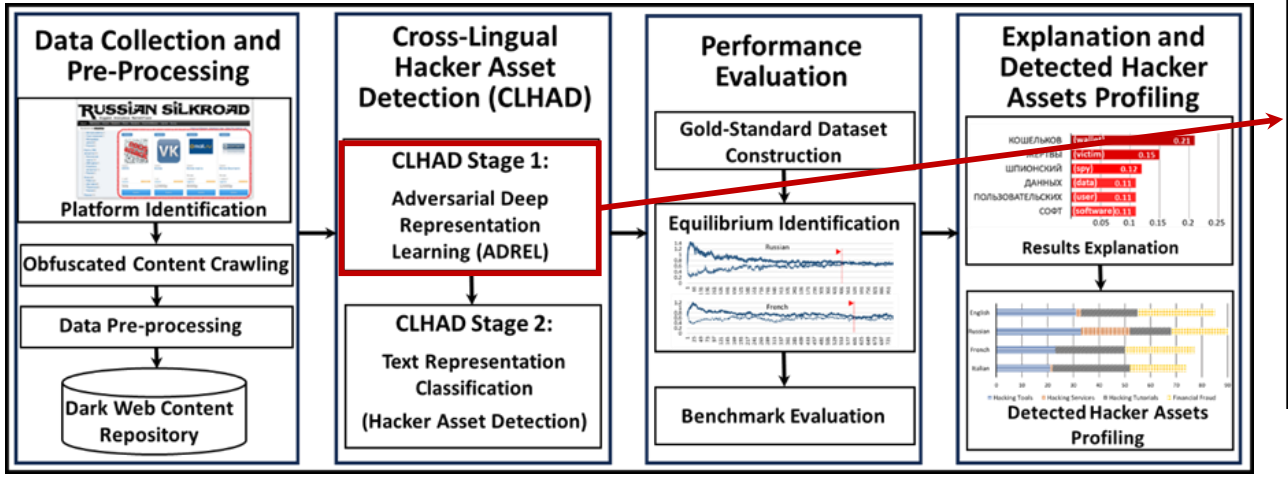
$$\text{subject to:}\quad \frac{1}{U}\sum_{j=1}^{u}\max(0, \text{sign}(w^T x_j')) = \boxed{r}$$

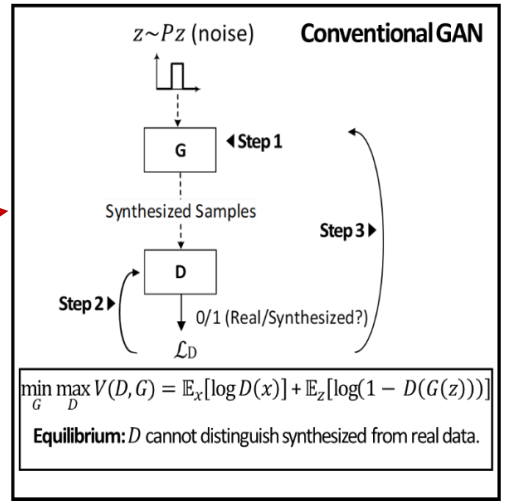


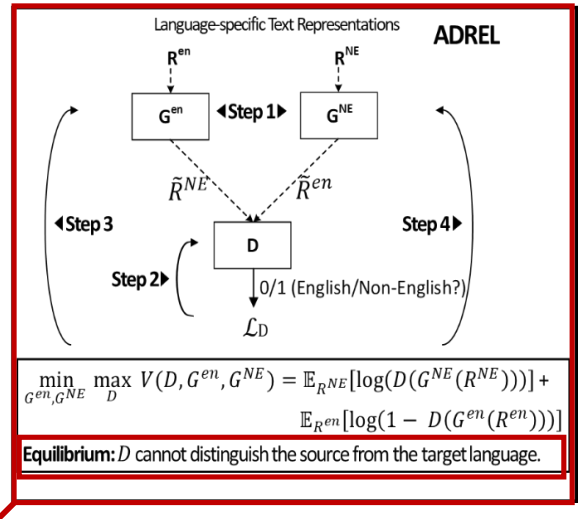
- Significantly decreased reliance on human supervision for cyber threat detection.

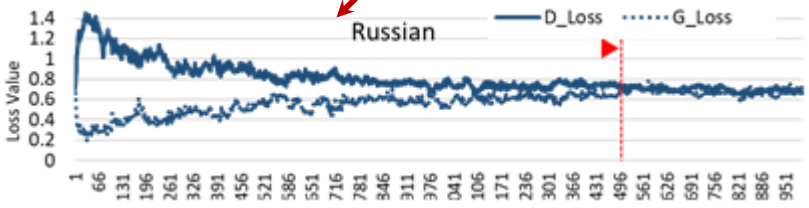
Essay II: Learning from Heterogeneous Cybersecurity Content (MISQ, Forthcoming)

- 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**





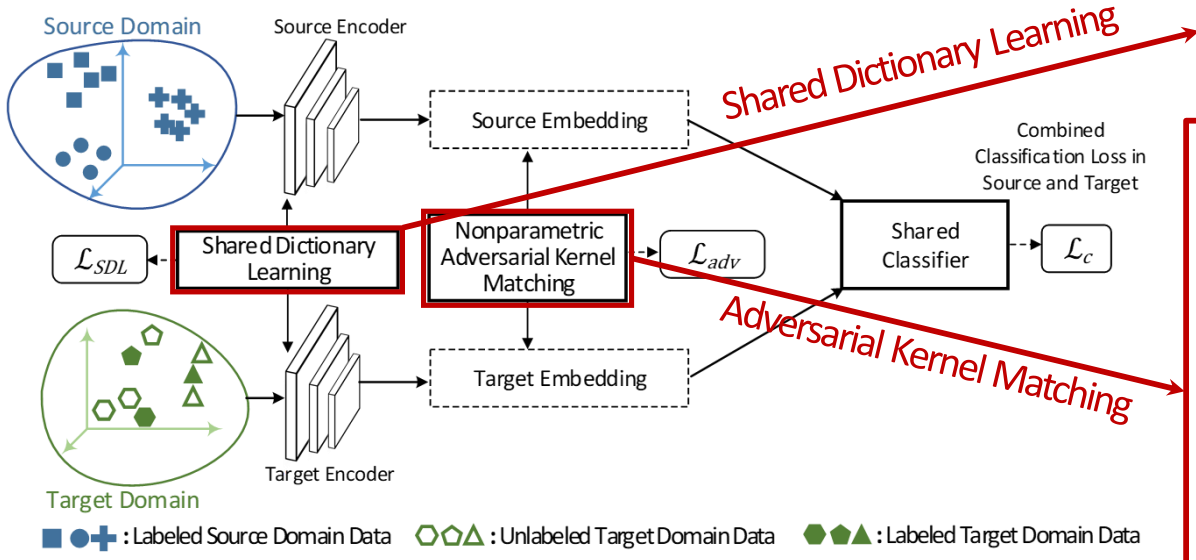




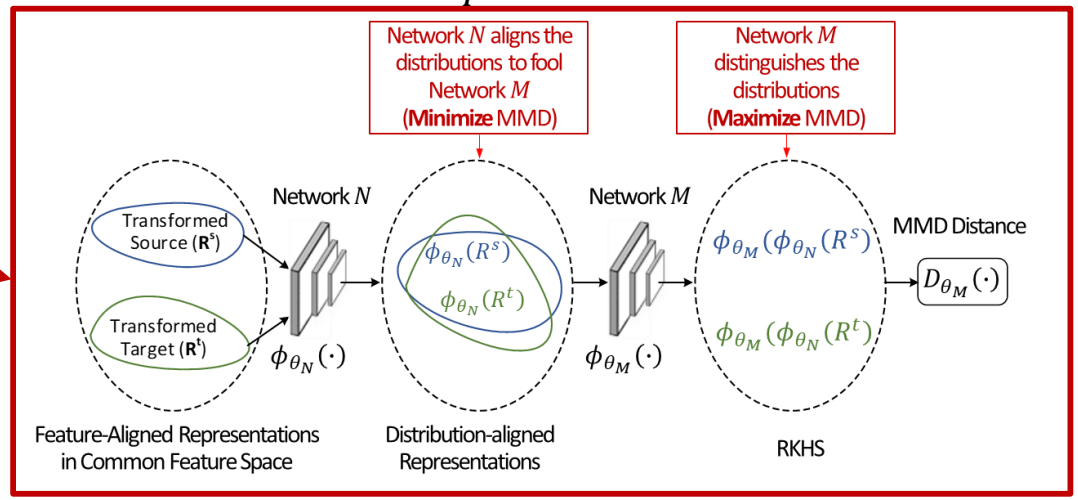
- Significantly decreased reliance on human supervision and outperformed machine translation.

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**



$$\min_{P^s,P^t,D,R^s,R^t} \|P^sX^s - DR^s\|_F^2 + \left\|P^tX^t - DR^t\right\|_F^2 + \lambda\|R\|_1; \quad \text{s.t.}\ \|d_i\|_2 \le 1$$



- 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-)

Secure and Trustworthy Cyberspace (SaTC)

PROGRAM SOLICITATION
NSF 21-500

REPLACES DOCUMENT(S):
NSF 19-603

National Science Foundation

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

CyberCorps(R) Scholarship for Service (SFS)
Defending America's Cyberspace

PROGRAM SOLICITATION
NSF 21-580

REPLACES DOCUMENT(S):
NSF 19-521

National Science Foundation

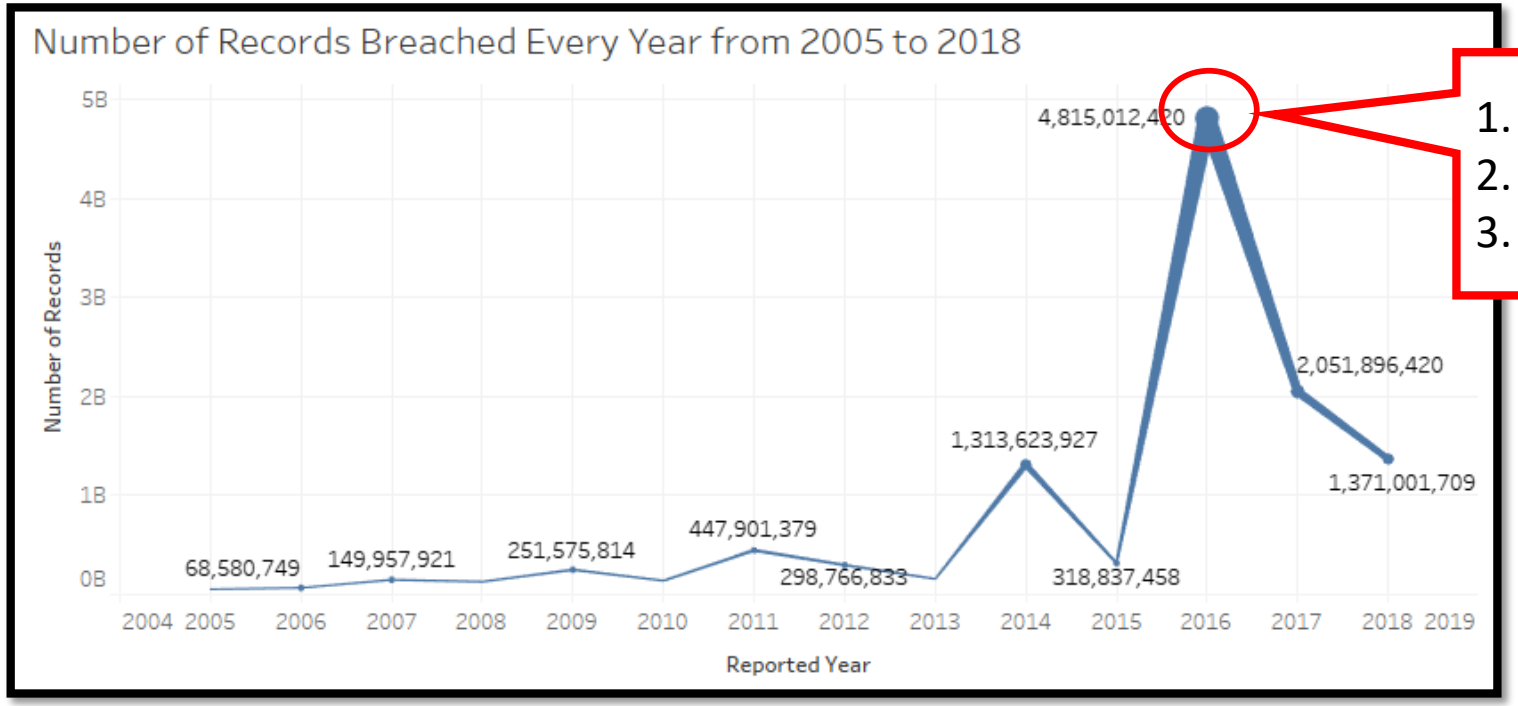
Directorate for Education and Human Resources
Division of Graduate Education

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

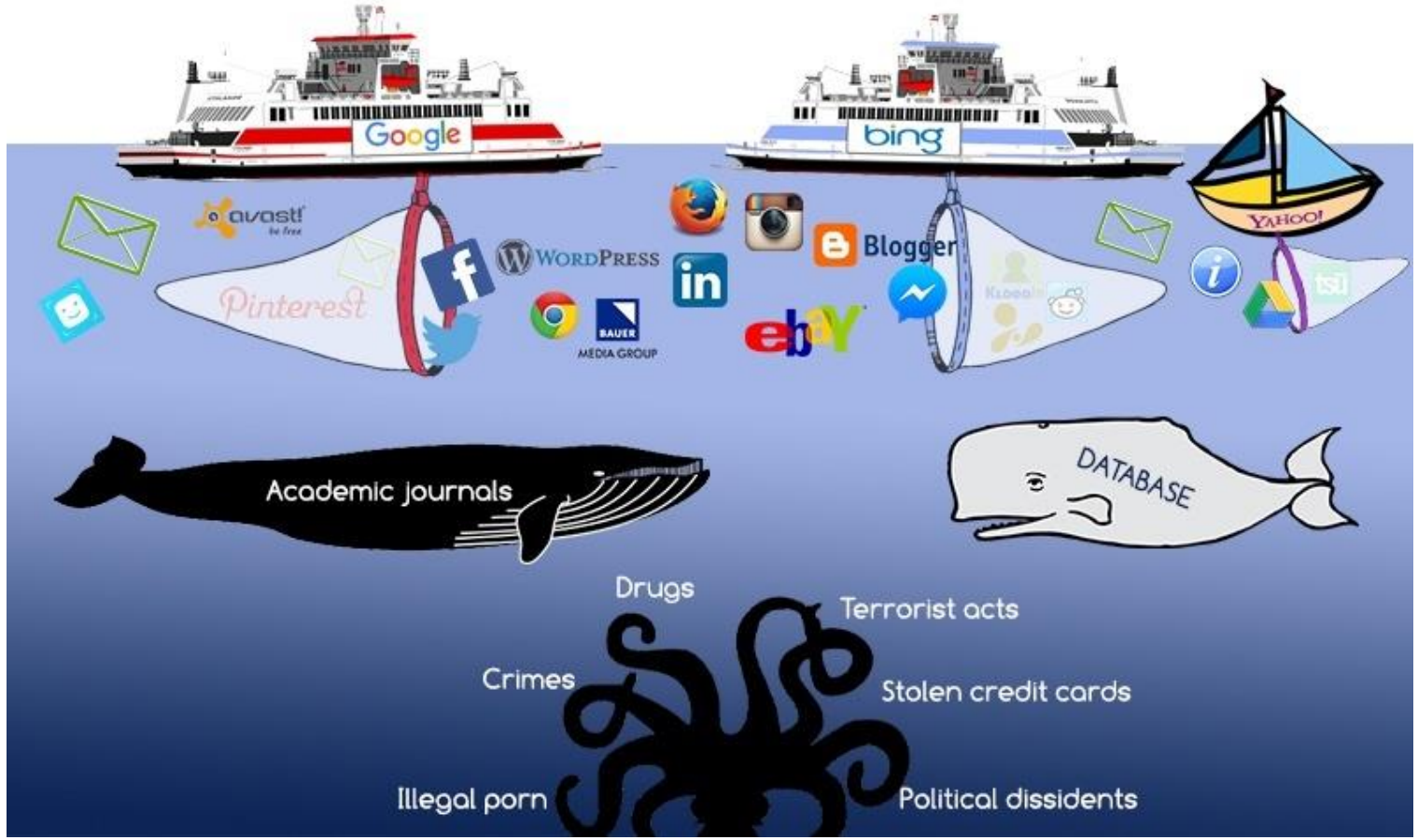
Surface Web

Deep Web

Dark Web

DarkNet

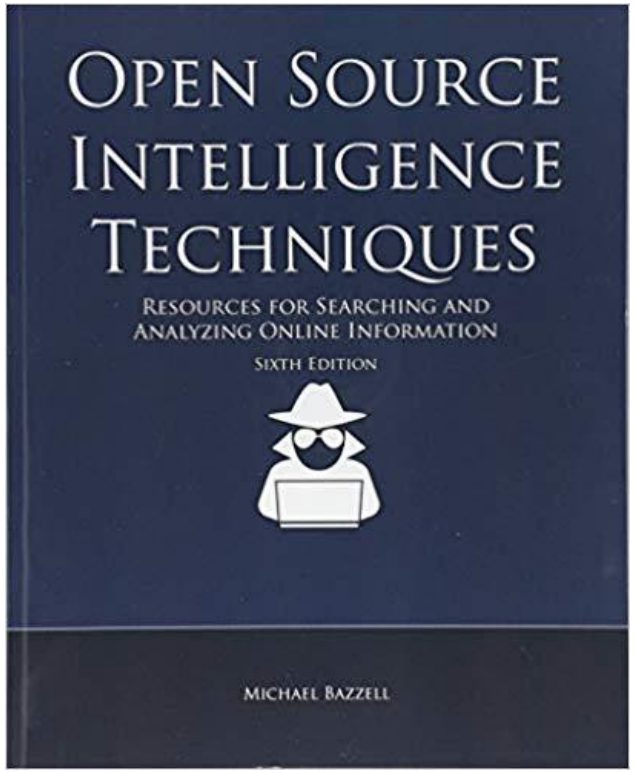
Hacker Web

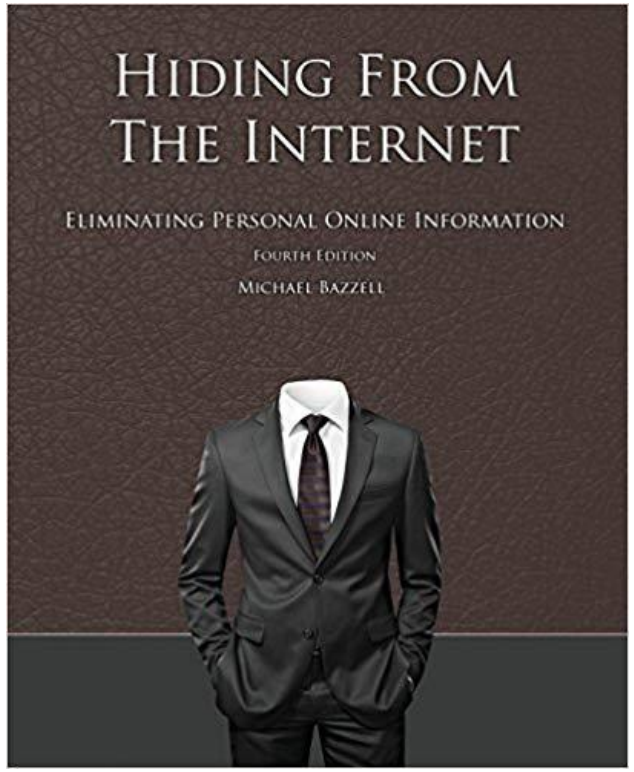


IRB, HIPAA, GDPR, PII

➔ Cybersecurity to Privacy

➔ **Michael Bazzell** + From Dark Web to Surface Web





Dark Web Intelligence Sources (May, 2021)

Source	Description	Size*	Promising Attributes
Stolen Account Collection	Stolen social media and e-mail accounts	**25 billions**	**Username**
			Password
Stolen Credit Card - Tormarket	Stolen credit and debit card owner information * No card number	**832 thousands**	**Full name**
			Country
			State
			City
			Zip
Stolen SSN - Buyssn	Personal information of SSN owners *No SSN	**5.75 millions**	**Full name**
			YOB
			City
			State
			Zip
			Country

"Passwords are like underwear… change often, don't share…"

Stolen Accounts

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

Popular Passwords

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

AZSecure Privacy Portal Design

LifeLock
Relentlessly Protecting Your Identity™

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

mongoDB

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

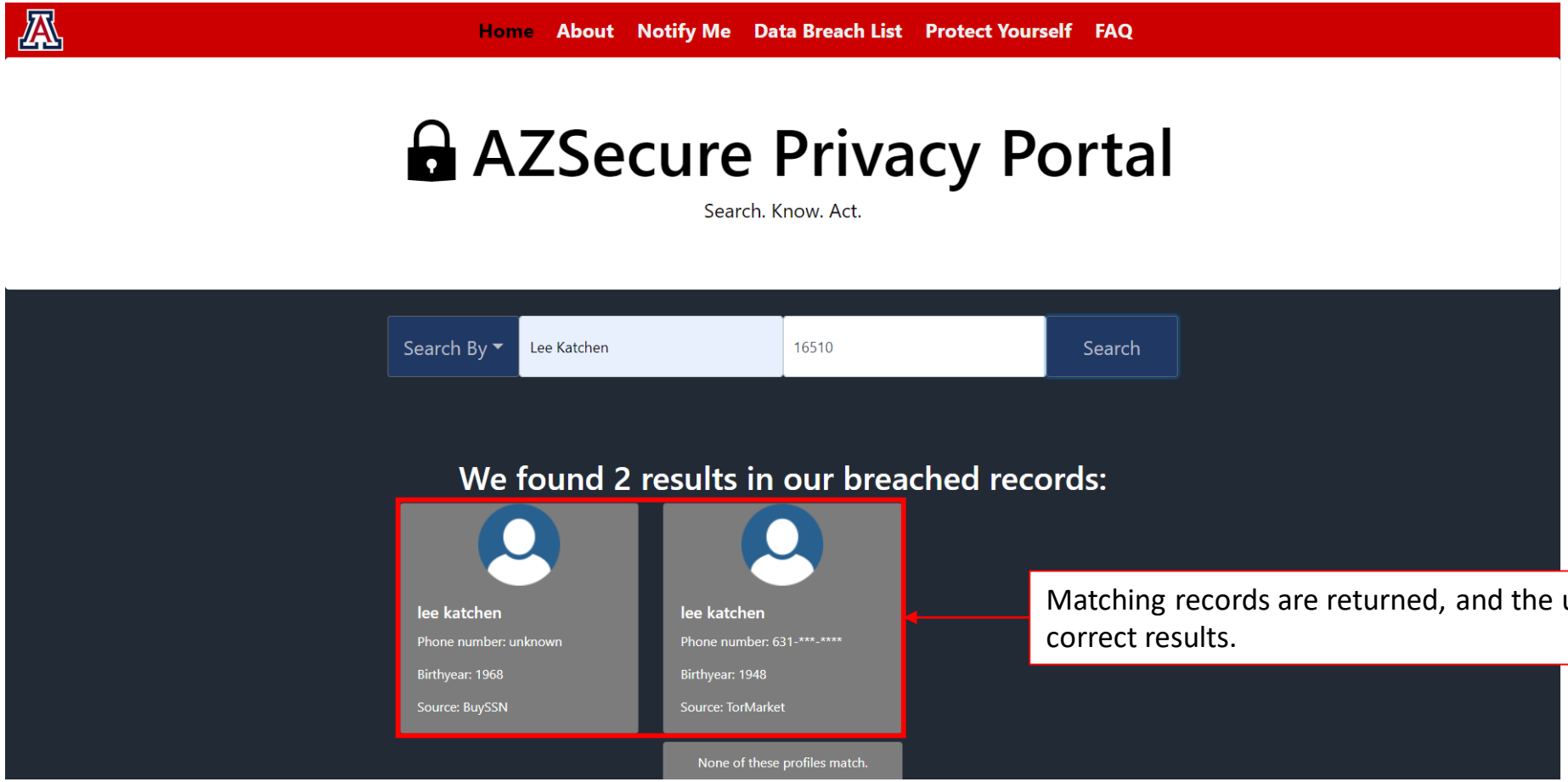
Portal Frontend

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



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

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

Return Exposed PII

Your information has been **compromised** in 1 breach:
TorMarket

What was compromised? phone number, address, birthday, home town, current town, job details, relationship status, political views, religious views

Your privacy is at **high** risk compared to others in your age group.
Your privacy risk score is **8.8**

Find out what this score means here.

How do I protect myself? Find out here.

Result from our database:

Platform	Leaked Attributes
TorMarket	name: lee katchen | zip: 16*** | address: 1234 Ma********** | jobDetails: carpenter | relationshipStatus: married | politicalViews: moderate | religiousViews: buddhist | birthyear: 1948 | phoneNumber: 631-***-**** | city: er******

Results from surface web search engines:

Platform	Leaked Attributes	MCA Matching Results	TF/IDF Matching Results
Zabasearch	name: Lee R Katchen | state: Pennsylvania | address: 5551 Fr********** | birthyear: 1948 | phoneNumber: 814-***-**** | city: Er******	✔	⊗
Anywho	name: Lee R Katchen | state: PA | address: 1024 Ap********** | city: Er****** | phoneNumber: 814-***-****	✔	⊗
Anywho	name: Lee R Katchen | state: PA | address: 3747 Bi********** | Age: 52 | city: Er****** | phoneNumber: 814-***-****	⊗	⊗
Anywho	name: Lee R Katchen | state: PA | address: 3747 Bi********** | city: Er****** | Age: 52 | phoneNumber: 814-***-****	⊗	⊗

Figure 9. Mock-ups of a comprehensive exposed PII profile

AZSecure Cybersecurity Analytics Program (2010-present): SaTC, SFS, ACI

Secure and Trustworthy Cyberspace (SaTC)

PROGRAM SOLICITATION
NSF 21-500

REPLACES DOCUMENT(S):
NSF 19-603

National Science Foundation

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

CyberCorps(R) Scholarship for Service (SFS)
Defending America's Cyberspace

PROGRAM SOLICITATION
NSF 21-580

REPLACES DOCUMENT(S):
NSF 19-521

National Science Foundation

Directorate for Education and Human Resources
Division of Graduate Education

Cybersecurity Innovation for Cyberinfrastructure (CICI)

PROGRAM SOLICITATION
NSF 21-512

REPLACES DOCUMENT(S):
NSF 19-514

National Science Foundation

Directorate for Computer and Information Science and Engineering
Office of Advanced Cyberinfrastructure

Azsecure Cybersecurity Analytics Program: Looking into the Future

(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.

For questions and comments

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