ISC

(BTech III Jan-April 2024)
Week#3 – Jan 19, 2024

Dhiren Patel

LATEST CYBERSECURITY HEADLINES

- Unpatched Rapid SCADA Vulnerabilities Expose Industrial Organizations to Attacks
- Millions of Old Passwords Distributed on Hacking Forum
- Ransomware Group Targets Foxconn Subsidiary Foxsemicon
- Software Supply Chain Security Startup Kusari Raises $8 Million
- Russian APT Known for Phishing Attacks Is Also Developing Malware, Google Warns
- Energy Department to Invest $30 Million in Clean Energy Cybersecurity Solutions
- Oleria Secures $33M Series A Investment
- Toyota Insurance Customer Data Exposed Due to Misconfigurations
- Outsmarting Ransomware's New Playbook

Key Definitions

- Information Manipulation and Interference describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes.
- Such activity is manipulative in character, conducted in an intentional and coordinated manner.
- Foreign IMI can be carried out by state or non-state actors, including their proxies inside and outside of their own territory.
- E.g. USA Election 2020, 2016

Key definitions

- A supply chain attack targets the relationship between organizations and their suppliers.
- Threat groups exhibit an increasing capability by using employees as entry points. Threat actors will continue to target employees with elevated privileges, such as developers or system administrators
- A zero-day attack takes place when hackers exploit the flaw before developers have a chance to address it. (Hackers or malicious actors spot the vulnerability before the software developers do).
- A zero-day vulnerability is a software vulnerability discovered by attackers before the vendor has become aware of it.
- A zero-day exploit is the method hackers use to attack systems with a previously unidentified vulnerability.

Trends

- Geopolitics continue to have a strong impact on cyber operations
- Several threat actors further professionalized
- Double extortion has witnessed a notable rise
- ‘Cheap fakes’ and AI-enabled manipulation of information continues to be a cause for concern

AI-driven misinformation (Ack: Open AI)

- Generative AI and its potential misuse, including AI-generated deepfakes, have become a central part of the conversation around AI's meteoric rise
- Misleading "deepfakes", scaled influence operations,
- E.g. Tendulkar "deep fake" video
- The threat of artificial intelligence to democracy being a top concern for policymakers and voters worldwide.
- E.g. Chatbots impersonating candidates
- OpenAI laid out its plan to help ensure transparency on AI-generated content and improve reliable voting information ahead of the 2024 USA elections.

Requirements

- Protecting the integrity of elections requires collaboration from every corner of the democratic process
- safety work by elevating accurate voting information, enforcing measured policies, and improving transparency
- safety systems, threat intelligence, legal, engineering, and policy teams to quickly investigate and address potential abuse
- improve factual accuracy, reduce bias, and decline certain requests

Counter measures for safety

- E.g. These tools provide a strong foundation for work around election integrity. For instance, DALL·E has guardrails to decline requests that ask for image generation of real people, including candidates
- People want to know and trust that they are interacting with a real person, business, or government. For that reason, we don’t allow builders to create chatbots that pretend to be real people (e.g., candidates) or institutions (e.g., local government).
- We don’t allow applications that deter people from participation in democratic processes—for example, misrepresenting voting processes and qualifications (e.g., when, where, or who is eligible to vote) or that discourage voting (e.g., claiming a vote is meaningless)

Countermeasures

- Provenance efforts - a provenance classifier, a new tool for detecting images generated by DALL·E
- the Coalition for Content Provenance and Authenticity's digital credentials—an approach that encodes details about the content's provenance using cryptography—for images generated by DALL·E 3
- ChatGPT is increasingly integrating with existing sources of information—for example, users will start to get access to real-time news reporting globally, including attribution and links. Transparency around the origin of information and balance in news sources can help voters better assess information and decide for themselves what they can trust.

Help

- ChatGPT will direct users to CanIVote.org, the authoritative website on US voting information, when asked certain procedural election related questions—for example, where to vote.

Information Security

- Safeguarding data at transit, at store (rest), on cloud, on-prim and off-prim, access control….
- Access control list (ACL) – assets/data v/s grouped entities
- Access control matrix of 1s and 0s (Role Based Access Control - RBAC)
- Encrypting information – symmetric/asymmetric keys
- <Replace encrypted data?? Decrypting key won’t work – attack!!>
- Data integrity, Hash function – message digest
- Message Authentication Code (MAC)
- Digital signatures <Non-Repudiation>

Back to Classical Cryptography

- Substitution Cipher – Caesar Cipher
- Permutation Cipher
- Transposition Cipher
- Mono-alphabetic Cipher
- Poly-alphabetic Cipher
- Poly-gram Cipher

Polygram substitution

- Groups of characters being substituted (simultaneously) by other groups of characters from the same alphabet
- Sequences of two plaintext characters (*digrams*) be replaced by other digrams;
- key space is large
- Applicable to trigrams to n-grams

Playfair cipher

- Invented By Sir Charles Wheatstone in 1854 (named for his friend B. Playfair)
- A digram substitution defined by arranging the characters of a 25-letter alphabet (*I* and *J* are equated) in a 5 x 5 matrix as a key (example on next slide)
- A mnemonic aid (a meaningful keyphrase) may be used to easily remember the 5x5 square
- repeated letters are not considered again and the remaining characters included alphabetically at the end.

Example – Key Matrix

- The key phrase “PLAYFAIR IS A DIGRAM CIPHER” would define a square with rows PLAYF, IRSDG, MCHEB, KNOQT, UVWXZ.

P	L	A	Y	F
I/J	R	S	D	G
M	C	H	E	B
K	N	O	Q	T
U	V	W	X	Z

Playfair – Encryption Rules

- Adjacent plaintext characters are paired (p1,p2).

  p1 → c3, p2 → c4; pair (c3,c4) is defining cipher text

- Rule 1: If p_1 and p_2 are in distinct rows and columns, they define the corners of a sub-matrix, with the remaining corners c_3 and c_4, c_3 is the character in the same row as p_1.
- Rule 2: If p_1 and p_2 are in a common row, c_3 is the character immediately to the right of p_1 and c_4 that immediately right of p_2 (the first column is viewed as being to the right of the last). For decryption, use left direction.
- Rule 3: If p_1 and p_2 are in the same column, the characters immediately (circularly) below them are c_3 and c_4. For decryption, use up direction
- Rule 4: If $p_1 = p_2$, an infrequent plaintext character (such as X) is inserted between them and the plaintext is re-grouped. E.g. word *Balloon* would become *ba lx lo on*.

Playfair cipher: Work Example

Plain text: Meet at five pm behind P lab.

- The key phrase “PLAYFAIR IS A DIGRAM CIPHER”
- *Plain text Written as digrams*:

ME ET AT FI VE PM BE HI ND PL AB

- *Encrypted as*:

CB QB OF GP CX IK MB SM RQ LA HF

- *Decrypted back* to plain text as:

ME ET AT FI/J VE PM BE HI/J ND PL AB.

P	L	A	Y	F
I/J	R	S	D	G
M	C	H	E	B
K	N	O	Q	T
U	V	W	X	Z

Example – do it yourself

- Pass phrase / Key phrase
- INDIA WON SEMIFINAL MATCH AGAINST NZ
- Create Playfair key (matrix = 5x5)

- Encrypt Kkrish
- KKRISH == KX KR IS H(X) Padding

Arranging plain text in proper digrams

- VIRRAT TON (original 9 characters)
- VI RR AT TO N
- VI RX RA TT ON
- VI RX RA TX TO NX (final 12 characters)

Playfair cipher - variant

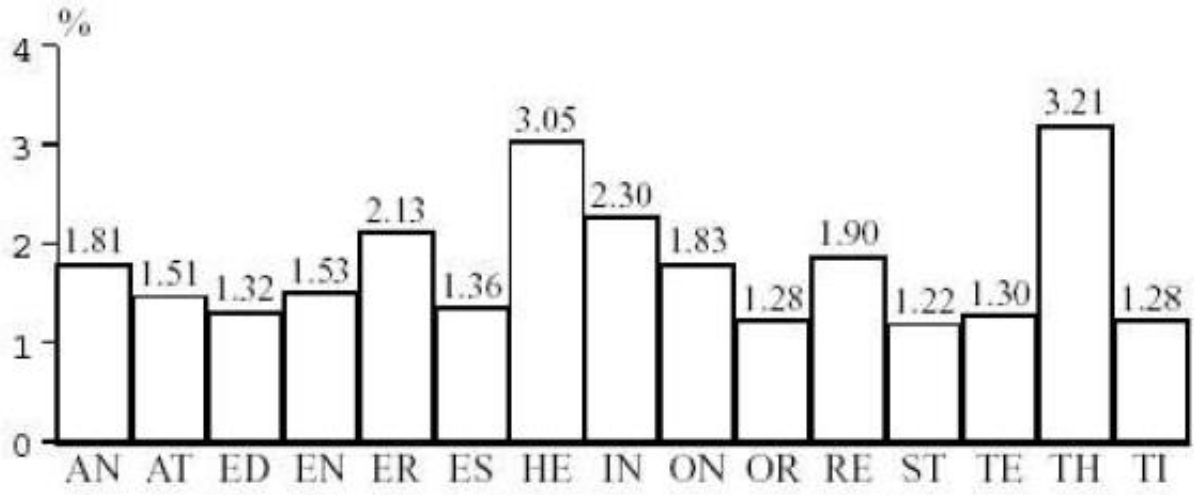
- Another example of designing a Playfair cipher for 26-alphabet and 10 numerals, we can use 6 x 6 matrix that can accommodate all 36 symbols (without equating I and J)
- Take a key phrase: Course No 821 Winter 2K05 Sem 7 Inf Sec and Cry by Patel H9

C	O	U	R	S	E
N	8	2	1	W	I
T	K	0	5	M	7
F	A	D	Y	B	P
L	H	9	G	J	Q
V	X	Z	3	4	6

- To avoid the trailing characters always being from the end of the alphabet, a further shift cipher could be applied to the resulting character string.

Polygram ciphers (attacks)

- polygram substitution ciphers (Playfair, Hill) are linear transformation, and fall under known-plaintext attack.
- Frequency analysis (digrams)



Similarly -- Trigrams - The most common trigrams (triples) in English language are: THE, ING, AND, HER, ERE, ENT, THA and NTH.

Lab next week – implementation of Playfair cipher

- 5x5 key matrix and 6x6 matrix both
- Program to read key phrase and create a key matrix
- Program to understand encryption and decryption rules
- Input1 – key phrase, Generate key matrix
- Input2 – plain text, arrange into valid digrams
- Output – print Key matrix, print plain txt, and encrypted output
- Repeat for decryption – Input2 is cipher txt, no need to rearrange, output plain txt, remove padding