

Quantitative Cyber-Security

Colorado State University

Yashwant K Malaiya

CS559

Quick Research Presentations Th b



CSU Cybersecurity Center
Computer Science Dept

Thursday

- Everyone must participate
 - Share questions/comments
 - Take notes
- Presenters: limit yourself to 5 minutes, 1 minute for q/c
 - Upload your slides and be ready to present
- Ujwal will run videos/presentations by some distance students
- The Peer Review Form (Canvas Assignments) due on Sat. Novelty/ Interest, Technical/ Research, Presentation

Presentations Today

T11 Quant. examination of phishing

Shree Harini Ravichandran

10 Examination of the time a vulnerability remains undiscovered

Luis Rodriguez

Luis Pineiro Rivera

Austen Weaver

9 Quant modeling of the time to vulnerability discovery

Alexandre Dubois

8 Quant modelling of Vulnerability markets

Wei Chen

Waylon Jepsen

7 Annual security breach costs incurred to society/government/nations

Zijuan Liu

Ya-Hsin Cheng

Sarah Houlton

3 Quant. Examination of schemes for discovering previously unknown vulnerabilities

Don Neumann

5 Assessing probability of security breaches

Siddhi Kotian

Dhruv Padalia

Annual Security Breach Costs Incurred to Nations

Name: Zijuan Liu

Background

Twitter account were attacked to scam other users of Twitter by transferring bitcoin on July 7th, 2020.

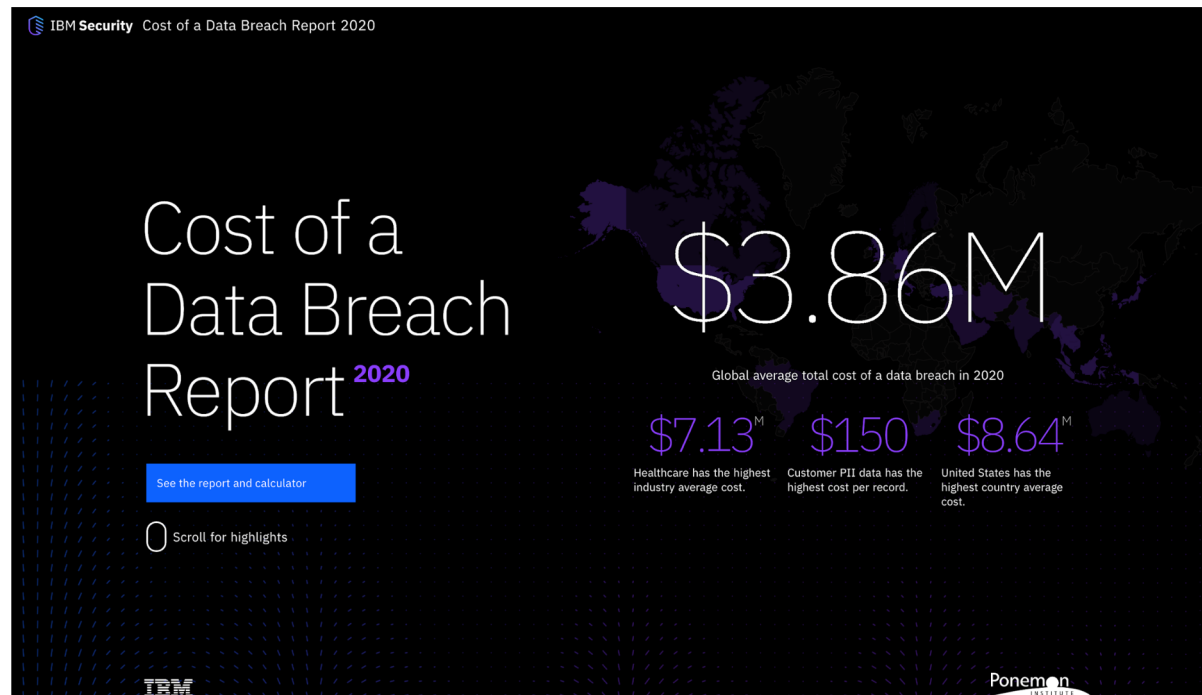
- Security breach cost is around \$120,000
- Using internal Twitter tool, which is used for account management, to control Musk's, Apple's et.al. account



Security Breach Report in 2020

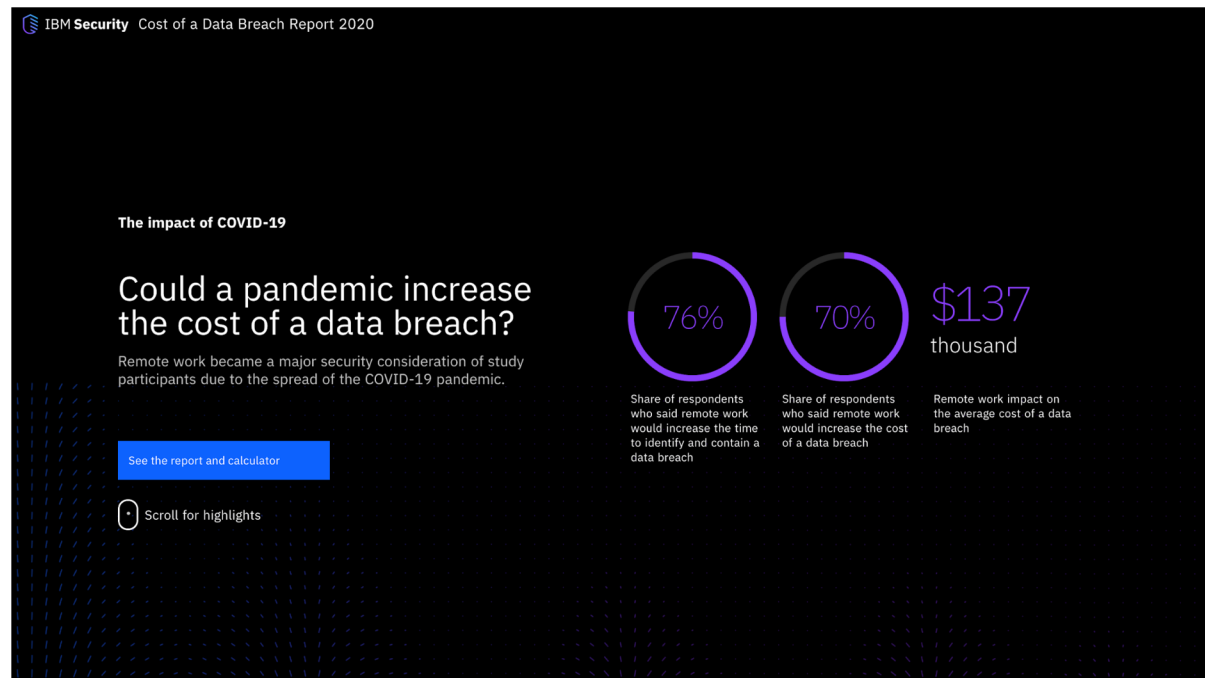
Cost of Data Breach

- The global average total cost of a data breach in 2020 is 3.86 million dollars [3]
- The highest industry average cost is healthcare[3]
- The highest country average cost is definitely the United States [3]
- The United State of American average cost is up to 8.64 million dollars [3]



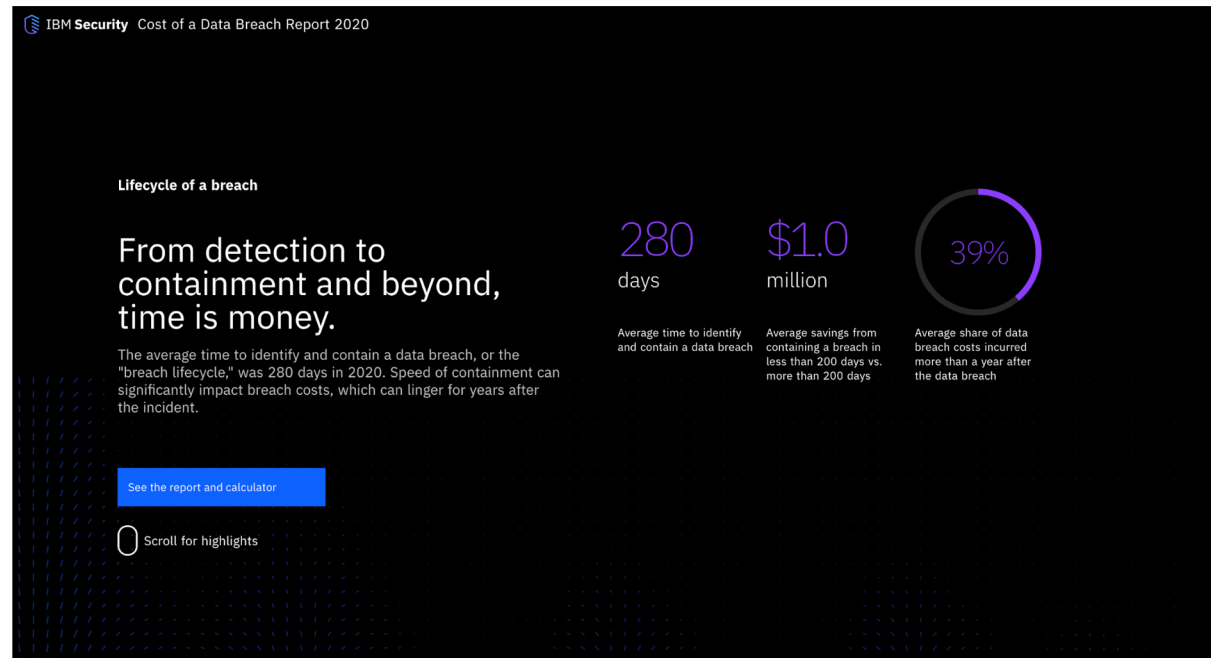
The Impact of COVID-19

- COVID-19 increased the average cost of data breaches because of remote works [3]
- Time to identify and contain a data breach increased by about 76% [3]
- Average cost could increase by around 70% [3]
- Average cost for remote work would up to 137 thousand [3]



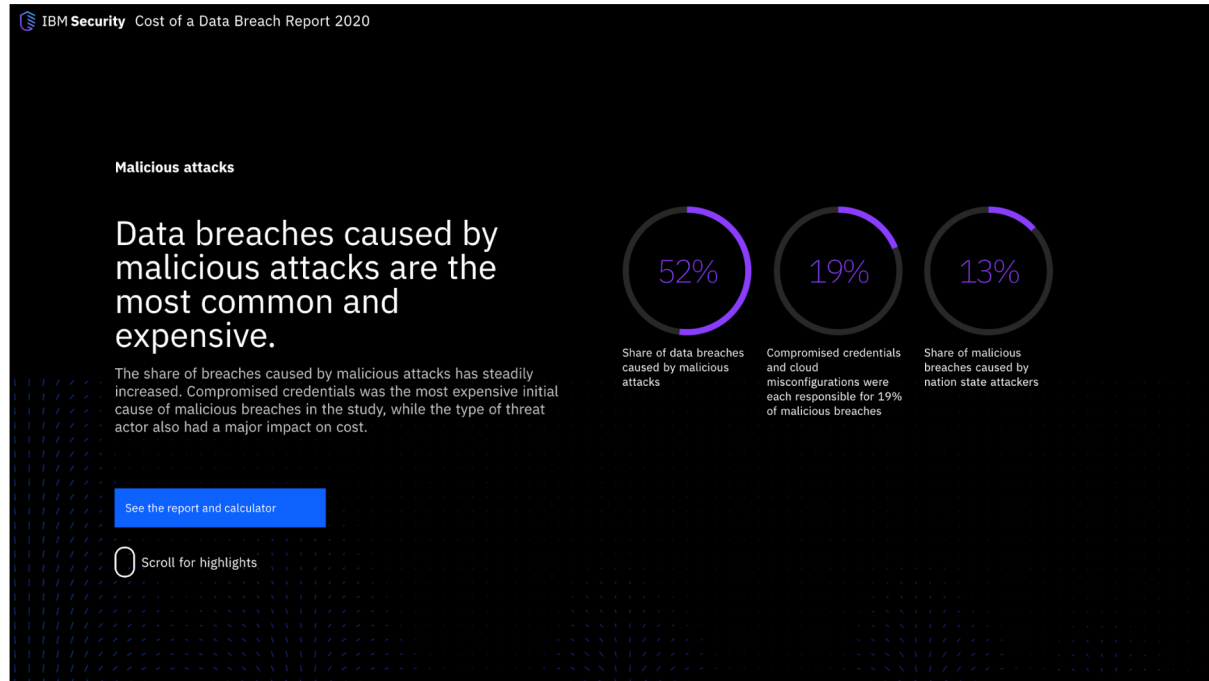
Lifecycle of A Breach

- The breach lifecycle is the average time to identify and contain a data breach, and 280 days was the breach lifecycle in 2020 [3]
- Containment time directly impacts the average cost of a data breach, so the difference in average cost between less 200 days and more 200 days was one million dollars [3]



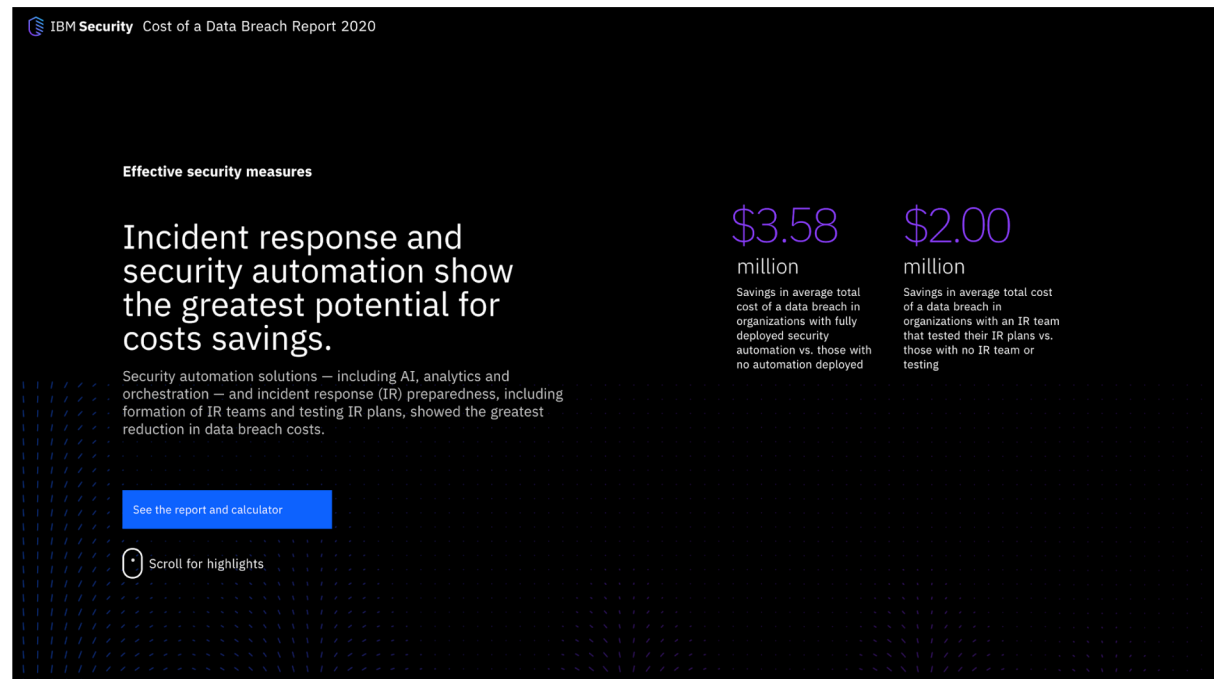
Malicious Attacks

- Malicious attacks is the most common way of data breaches, and it is also the most expensive way [3]
- The percentage of malicious attacks was steadily increasing, and 52% of malicious attacks would cause data breaches [3]



Effective Security Measures

- Security automation and incident response are the greatest way to improve security and decrease the cost of breaches [3]
- Saving 3.58 million dollars if your company used security automation system [3]
- Saving 2 million dollars if your company with IR teams [3]



The Cost of Security/Data Breaches : The Impact In The Industry/Public

Ya-Hsin Cheng

Department of Computer Science
Colorado State University



Colorado State University



Outline


- Current state and Development of security breaches
- Practical and Actual implementation methods
- Brief Summary

Current state

- Security breaches cost a lot of money lost from the industries to the nations
- In the past few years, the number of data breaches has been increasing
- The healthcare industry has the highest average cost
- In 2015, the famous insurance company Anthem Inc. was attacked by hacker

Data breach costs diverged

The global average cost of a data breach declined slightly in 2020, but costs were much higher than average in some organizations based on factors such as geography, industry and level of security maturity.

 \$3.86M ↓ 1.5%

Global average total cost of a data breach

Change in average total cost, 2019-2020

Data Breach Up To \$3.86 Million Per Year

Report made by IBM and
the Ponemon Institute, 2020

Practical and Actual implementation methods

- Artificial Intelligence(AI), Machine Learning
- Using machine learning to diagnose network and manage network automatically
 - ✓ To optimize the effect and prevent security breach risk
- Data Mining
 - ✓ Analyzing the past hacked logs, find the certain pattern and methods that the hacker did
 - ✓ Prevent it happens again in the future

Security automation saved millions

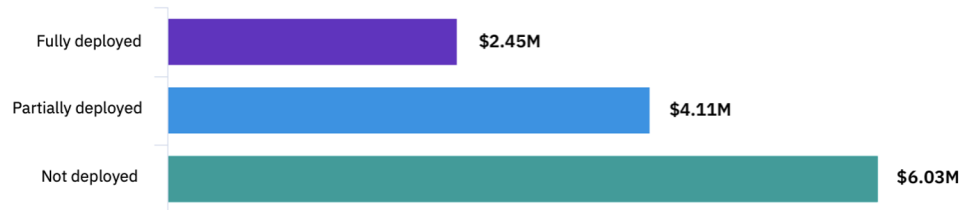
Security automation – using technologies such as AI, analytics and automated orchestration – was most effective at mitigating data breach costs.

\$3.58M

Reduction in average total cost for fully deployed vs. no security automation

Average total cost by security automation level

Measured in US\$



The Money Saved by Security Automation

Report made by IBM and the Ponemon Institute, 2020

Summary

- Long-term Issue
- Three organizations that research security breaches and cyber crimes
 - ✓ IBM
 - ✓ Ponemon Institute
 - ✓ FBI

Thank you



Colorado State University



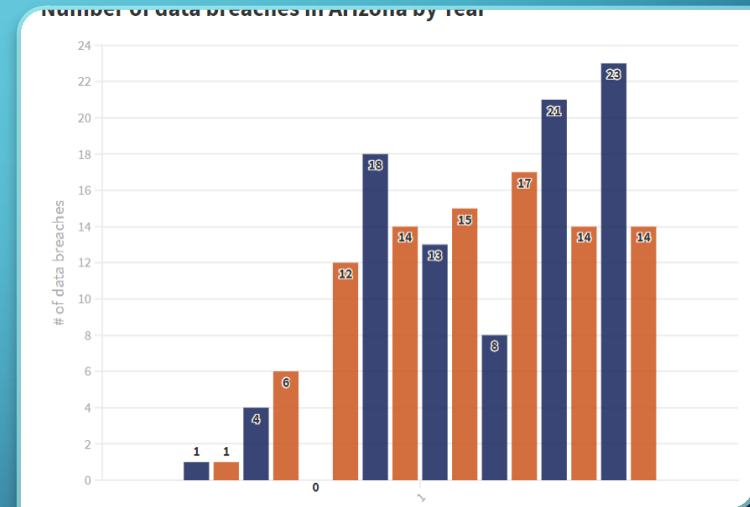
ANNUAL SECURITY BREACH COSTS INCURRED TO LOCAL GOVERNMENT

SARAH HOULTON

CS 559 QUANTITATIVE SECURITY

DATA BREACHES ARE ON THE RISE

- Both local and federal government are at risk of data breaches
- The same trends are seen in other local governments
- Known attacks increased 58.5% from 2018-2019 [2]
- Federally, there were 23,000 incidents and 320 confirmed breaches in 2019 [3]



RANSOMWARE

- Ransomware is the most common form of attack on governments
- The average cost of ransom between 2017 and 2020 was \$125,697 [2]
- Assuming the government paid this average on all 320 confirmed breaches in 2019, \$40,223,040 would have been lost to ransomware

CURRENT STATE OF CYBER SECURITY

- NIST framework is very popular but doesn't inspire mature security
- The biggest risk is human error
- Ransomware risk acknowledgement is low in local governments
 - 48% of elected councilors and/or commissioners found to be unaware of the importance of cybersecurity measures [2]
- Reduced by
 - Password hygiene
 - Two-factor authentication
 - General cybersecurity awareness



<https://www.telemessage.com/reducing-security-breaches-caused-by-human-error/>

CURRENT DEVELOPMENTS

- **Cybersecurity Maturity Model Certification (CMMC)**
 - “add a certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level” [4]
- **Johns Hopkins Applied Physics Lab SOAR tools**
 - Four states are involved in this project
 - Automation of security tasks such as blacklisting
- **UK government pledged \$10 million over four years to nine teams researching cybersecurity**

REFERENCES

- [1] J. MacDonald-Evoy, “Arizona has lost \$1B from data breaches since 2005,” *AZMirror*, 05-Aug-2020. .
- [2] D. Reading, “As Cyberattacks Soar, US State and Local Government Entities Struggle to Keep Up,” *Dark Reading*, 08-Jul-2020. .
- [3] S. Pritchard, “The latest government data breaches in 2019/2020,” *The Daily Swig*, 27-Feb-2020. .
- [4] D. Lohrmann, “Should State and Local Governments Obtain Cybersecurity Maturity Model Certification?,” *government technology*, 22-Aug-2020. .
- [5] B. Freed, “Four states join cybersecurity automation pilot,” *statescoop*, 16-Jul-2020. .
- [6] “U.K. Government Invests £10 Million to Develop Cybersecurity Technologies,” *GTSC Homeland Security Today*, 15-Jun-2020. .
- [7] S. Kanowitz, “Cyberattacks on state, local government up 50%,” *GCN*, 04-Sep-2020. .

A decorative graphic on the left side of the slide, consisting of white lines that resemble a circuit board or a tree structure. The lines are vertical and horizontal, with small circles at the ends, creating a complex, branching pattern.

THANK YOU

ANY QUESTIONS?

Quant examination of schemes for discovering previously unknown vulnerabilities

Don Neumann, CS559



Colorado State University

Topic Overview

- Quantitative technique usage in vulnerability discovery is in its infancy
- Topic refined to utilizing quantitative techniques in fuzzing per Dr. Malaiya
- Fuzzing - automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program [Wikipedia]
- Fuzzing began with creation of the first tool in 1990 [1]

[Wikipedia] <https://en.wikipedia.org/wiki/Fuzzing>

Fuzzing Taxonomy

- Black box - No knowledge or analysis of internal program structure, can observe only input and output.
- White box - Uses symbolic execution for program analysis, can include programs source code.
- Grey box - Leverages coverage feedback (think tracing stack frames) for input (seed) mutation to increase code coverage

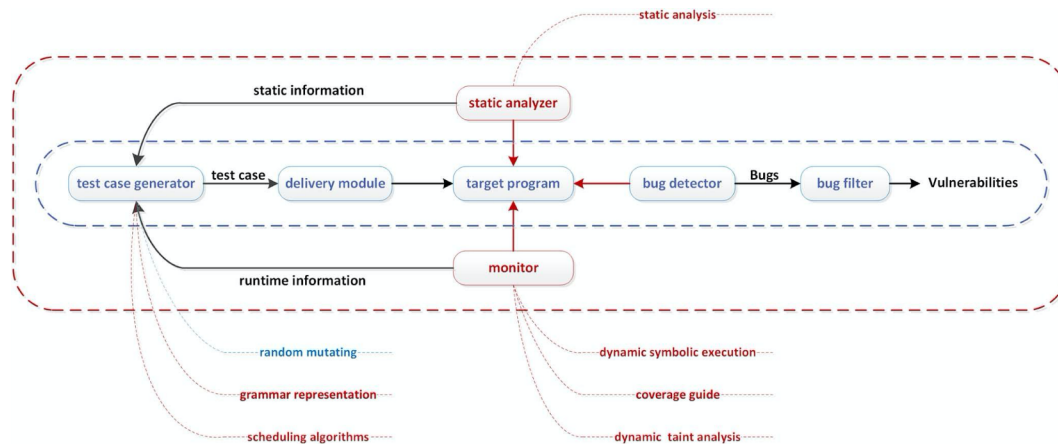


Image source: [2]

ExploitMeter

- Quantifies software exploitability
- Determine deployment and insurance risk
- Grey box testing
- Uses multiple fuzzers
- Leverages machine learning
- Bayes rule used in exploitability quantification

ID	Vulnerability Type	Description	Category
1	<i>ReturnAv</i>	Access violation during return instruction	EXPLOITABLE
2	<i>UseAfterFree</i>	Use of previously freed heap buffer	EXPLOITABLE
3	<i>SegFaultOnPc</i>	Segmentation fault on program counter	EXPLOITABLE
4	<i>BranchAv</i>	Access violation during branch instruction	EXPLOITABLE
5	<i>StackCodeExecution</i>	Executing from stack	EXPLOITABLE
6	<i>StackBufferOverflow</i>	Stack buffer overflow	EXPLOITABLE
7	<i>PossibleStackCorruption</i>	Possible stack corruption	EXPLOITABLE
8	<i>DestAv</i>	Access violation on destination operand	EXPLOITABLE
9	<i>BadInstruction</i>	Bad instruction	EXPLOITABLE
10	<i>HeapError</i>	Heap error	EXPLOITABLE
11	<i>StackOverflow</i>	Stack overflow	PROBABLY_EXPLOITABLE
12	<i>SegFaultOnPcNearNull</i>	Segmentation fault on program counter near NULL	PROBABLY_EXPLOITABLE
13	<i>BranchAvNearNull</i>	Access violation near NULL during branch instruction	PROBABLY_EXPLOITABLE
14	<i>BlockMoveAv</i>	Access violation during block move	PROBABLY_EXPLOITABLE
15	<i>DestAvNearNull</i>	Access violation near NULL on destination operand	PROBABLY_EXPLOITABLE
16	<i>SourceAv</i>	Access violation near NULL on source operand	PROBABLY_NOT_EXPLOITABLE
17	<i>FloatingPointException</i>	Floating point exception signal	PROBABLY_NOT_EXPLOITABLE
18	<i>BenignSignal</i>	Benign	PROBABLY_NOT_EXPLOITABLE
19	<i>SourceAvNotNearNull</i>	Access violation on source operand	UNKNOWN
20	<i>AbortSignal</i>	Abort signal	UNKNOWN
21	<i>AccessViolationSignal</i>	Access violation	UNKNOWN

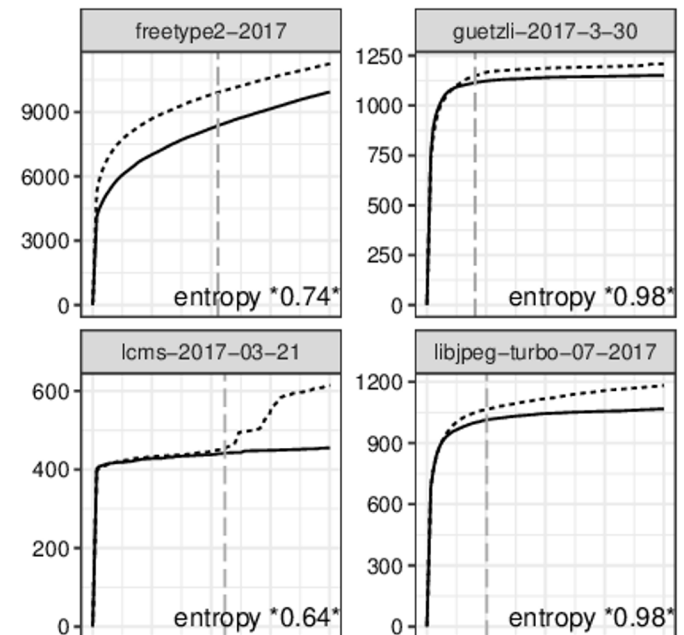
Reference: [3]

Boosting Fuzzer Efficiency

- Information theoretic approach to increase fuzzer efficiency
- Entropy (average information) determined based on input behavior
- Mutates input (seeds) based on entropy
- Grey box testing

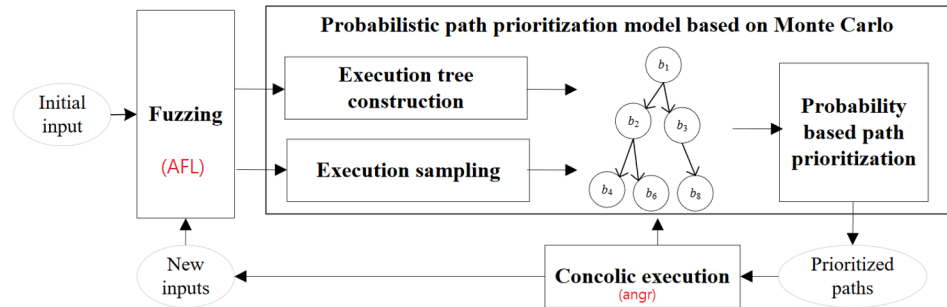
- Accepted for publication
- Resulting product Entropic
- Invited for integration into popular framework libfuzzer [9]
- Increases code coverage compared to deterministic libfuzzer default

Reference: [8]



Probabilistic Path Prioritization

- DigFuzz: Leverages concolic execution to increase code coverage and vulnerabilities discovered
- Concolic execution - hybrid of symbolic execution and concrete execution
- Built on popular fuzzer AFL (American Fuzzy Lop) [6]
- Execution paths treated as Markov Chains
- Monte Carlo technique used to identify promising paths for concolic execution
- Increased code coverage compared to AFL



Reference:[5]

References

- [1] B. Miller, L. Fredriksen and B. So, "An empirical study of the reliability of UNIX utilities", Communications of the ACM, vol. 33, no. 12, pp. 32-44, 1990. Available: 10.1145/96267.96279.
- [2] V. Manes et al., "The Art, Science, and Engineering of Fuzzing: A Survey", IEEE Transactions on Software Engineering, pp. 1-1, 2019. Available: 10.1109/tse.2019.2946563.
- [3] G. Yan, J. Lu, Z. Shu, and Y. Kucuk, ExploitMeter: Combining Fuzzing with Machine Learning for Automated Evaluation of Software Exploitability, 2017 IEEE Symposium on Privacy-Aware Computing (PAC), 2017.
- [4] T. Tan, B. Wang, H. Zhang, G. Chen, J. Wang, Y. Tang, and X. Zhou, "A New Quantitative Evaluation Method for Fuzzing," Lecture Notes in Computer Science Artificial Intelligence and Security, pp. 181190, 2019.
- [5] L. Zhao, Y. Duan, H. Yin, and J. Xuan, "Send Hardest Problems My Way: Probabilistic Path Prioritization for Hybrid Fuzzing," Proceedings 2019 Network and Distributed System Security Symposium, 2019.
- [6] M. Zalewski, american fuzzy lop. [Online]. Available: <https://lcamtuf.coredump.cx/afl/>. [Accessed: 09-Sep-2020].
- [7] N. Stephens, J. Grosen, C. Salls, A. Dutcher, R. Wang, J. Corbetta, Y. Shoshitaishvili, C. Kruegel, and G. Vigna, "Driller: Augmenting Fuzzing Through Selective Symbolic Execution," in Proceedings 2016 Network and Distributed System Security Symposium, 2016.
- [8] M. Bhme, V. Mans, S. K. Cha, "Boosting fuzzer efficiency: An information theoretic perspective," Proceedings of the 14th Joint meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering, ESEC/FSE, pp. 1-11, 2020.
- [9] libFuzzer: a library for coverage-guided fuzz testing, [Online]. Available: <https://llvm.org/docs/LibFuzzer.html>. [Accessed: 09-Sep-2020]

Thank you



Colorado State University

Assessing Probability of Security Breach - CS559 Quantitative Security

by Siddhi Kotian



Introduction

→ **What is Security Breach?**

Unauthorized access to any data, applications, network or devices resulting in Unauthorized access to data.

→ **Why is data so important?**

if there is a security breach at a government agency, it will result in top secret information being leaked

→ **What is Risk?**

Risk = Probability X Impact



Current Status

- Covid - 19
 - Moved to online platform
 - Employees work from home
- Telehealth
 - Online tools for patients
 - High risk of leaking sensitive data

Perimeter	Description	Compliance requirements	Security requirements
Privacy	Protection of personal, sensitive and judicial data	National Law and Technical Annexes, Internal Guidelines	Security guidelines, ISO 27001:2013
Financial Data	Protection and tracking of financial transactions, money transfers and financial information	National Law and Technical Annexes, Internal Guidelines	PCI-DSS, Security guidelines for protection of payment systems
Central Bank	Compliance with provisions of management and control issued by CB	National Authority Regulation, National Regulator Terms of Reference	Security guidelines for electronic payments
Traffic Data	EU Communication Directive, Traffic (Phone/Internet) Data Management	Nat. Authority Regulation, Technical Annex to Law, Internal Guidelines	Guidelines for critical infrastructure

		Impact:		
		Minor	Severe	Critical
Likelihood:	Rare	Low	Low	Med.
	Frequent	Low	Med.	High
	Certain	Med.	High	High

Recent Developments

- Compliance of regulations and adherence to the standards
 - Perimeter
 - Description
 - Compliance requirement
 - Security Requirement

- Likelihood estimations
 - Average threat level posed by a vulnerability
 - Estimated probability of receiving an attack

2. Does anyone in your organisation take company-owned mobile devices (e.g. laptops, smartphones & USB drives) with them, either home or travelling? *

Yes No Unsure

3. Does your organisation use Cloud-based software or storage? *

Yes No Unsure

Your Score
25

Escalated Risk: 55-100

High Risk: 30-50

Moderate Risk: 15-25

Low Risk: 0-10

Current Products and Technology

- CyberBee Calculator
 - Estimates company's risk by answering some questions



Organizations having Influential role in this field

→ **MIT**

The Wall Street Journal posted that researchers at MIT have developed a model that will help quantify security risk

→ **IBM**

They created a Data Breach Report 2020

→ **Ponemon**

This institute various studies related to cyber security breaches on various topics like password and authentication security, measuring and managing cyber risk, etc.



References

[1] What is a security breach?

[2] Big Data Facts

[3] Probability of Data breaches increases

[4] What's the Probability of a Data Breach Happening to You? Or is That The Wrong Question?


[5] Assessing Health Data Privacy Damages During A Pandemic

[6] Data for Cyber Security Risk Estimation

[7] CyberBee

[8] IBM Security

[9] Cyber Chiefs Calculate Data Breach Costs to Explain Risks to Executives



Assessing probability of security breaches - CS559 Quick Research

by Dhruv Ashok Padalia



Introduction

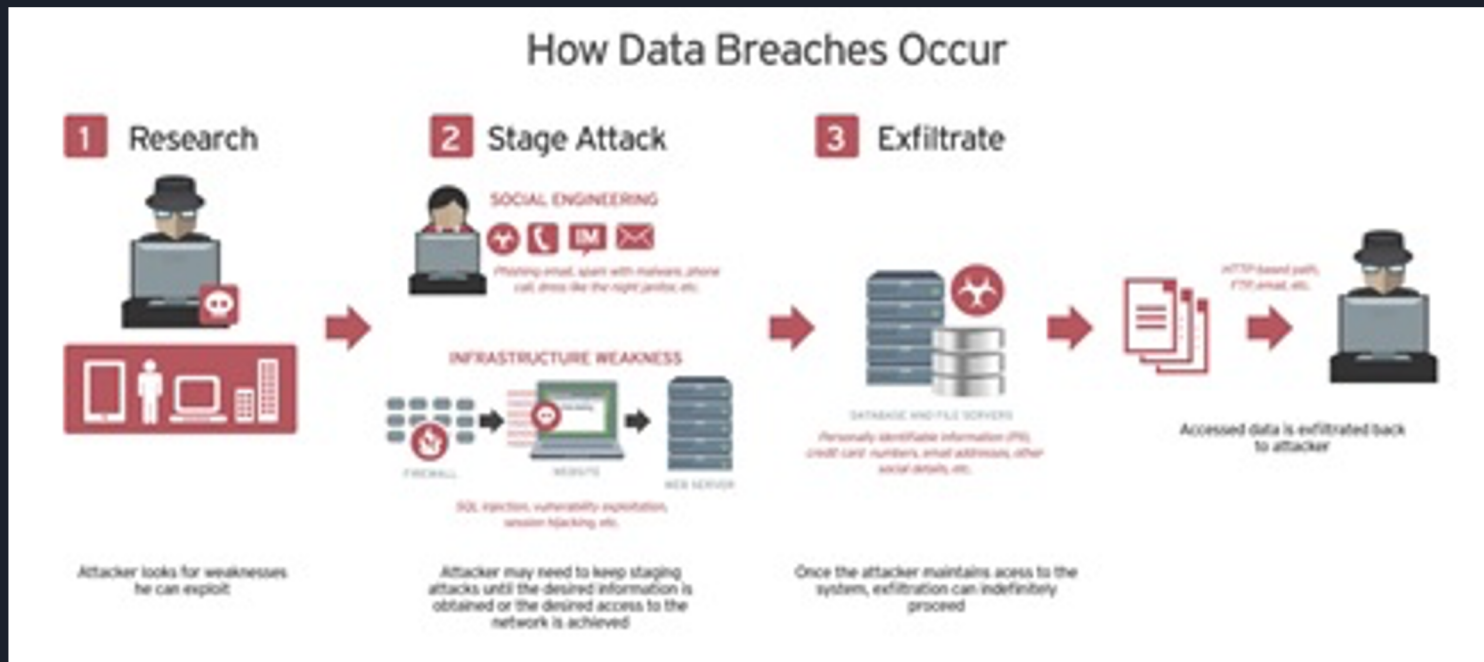
- 01 Security breach - unauthorized access to the computer data, application, network or device.
- 02 Business impact of security breach - Facebook's usage dropped 20% after the security breach in 2019
- 03 Yahoo experienced security breach in 2013, 2014 affecting 3 million records
Facebook experienced security breach in 2019 affecting 540 million records

Security Breach Methods



● Hacking or malware	25.0%
● Portable device loss	24.0%
● Unintended disclosure	17.4%
● Insider leak	12.0%
● Physical loss	11.6%
● Stationary device loss	5.4%
● Payment card fraud	1.4%
● Unknown	3.2%

Security Breach Phase

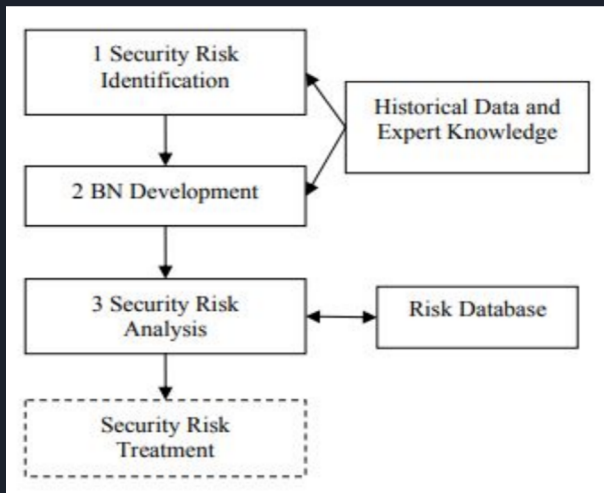




Current Status

- MIT built a new platform Computer Science and Artificial Intelligence Laboratory
- CSAIL quantify a companies' security risk without disclosing sensitive data.
- CSAIL will quantify
 - how secure they are
 - how their security is in comparison to their peers,
 - spending the right amount of money on security
- Vulnerabilities which had the largest losses (more than 1 million dollars each)
 - Failure to prevent Malware Attacks
 - Communication over unauthorized ports
 - Failures in log management for security incidents

Recent Developments



01 Security Risk Identification and Bayesian Network Development using Historical Data

02 Security Risk Analysis using Risk Database

03 Security Risk Treatment

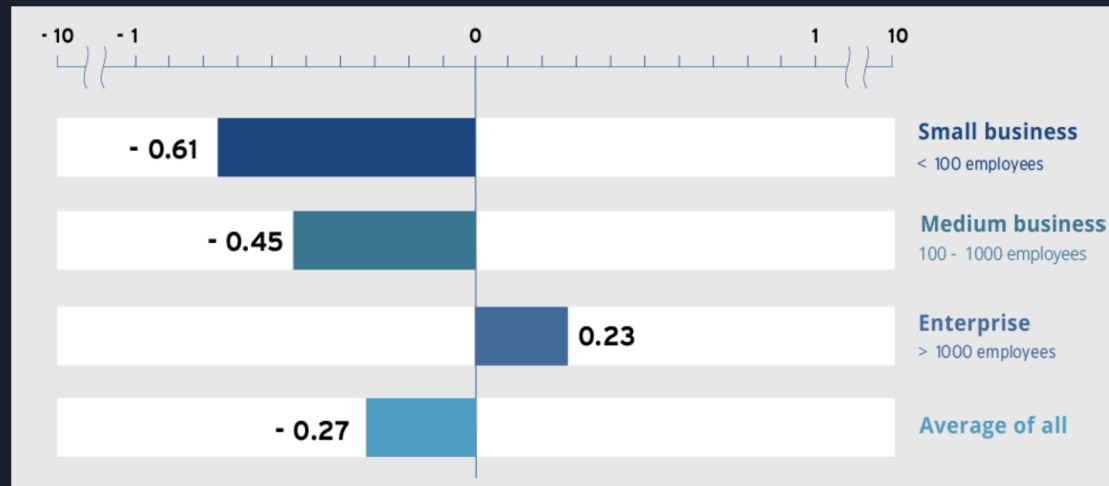
Current Products and Technology

Trend Micro - Cyber Risk Index

CRI is a comprehensive measure of the gap between an organization's current security posture and its likelihood of being attacked.

index is based on a numerical scale of -10 to 10, with -10 representing the highest level of risk.

[Link to CRI Calculator](#)





Industry, research labs or academic

- 01 IBM - report showing direct possible correlation of COVID-19 pandemic to increase in cost of security breaches
- 02 Trend Micro
- 03 MIT - platform, quantifying a companies' security risk without disclosing sensitive data