Quantitative Cyber-Security

Colorado State University

Yashwant K Malaiya

CS559

L26: Presentations

CSU Cybersecurity Center
Computer Science Dept

Presentations

- This is a research-oriented project. Please mention significant recent work and cite researchers and identify current trends challenges.
- Students with closely related presentations should coordinate among themselves to minimize overlap.
- Everyone: fill the peer-review form, and submit through canvas on
- Final: is two part
  - Final a: critial review of two specific project Final Reports
    - Assignment should be available Dec 10 and will be due on Dec 15.
  - Final b: proctored questions based (somewhat like midterm)
    - Dec 16 2-4 PM as scheduled. Perhaps 1 hour.

Presentations/Final Report

Tu Dec 1, 2020

1. Paudel, Upakar. **Security Posture of Various Android based IoT**
2. Gowdanakatte, Shwetha. **ATT&CK Framework and Vulnerability detection for Industrial Control System**
3. Eswaran, Suraj. **Cyber Risk and Cyber Insurance**
4. Cheng, YaHsin. **Severity of Cybercrime acts and Methods to Prevent them**
5. Weaver, Austen. **Cost and Cause of U.S. Government Security Breaches**
6. Ravichandran, Shree Harini. **Smartphone Security Model and Vulnerabilities**

Project

Final report (8-12 pages, submit using Canvas/Turnitin): It needs to be publication quality. It should include

- the title, name of the author(s), name of the class and professor,
- an abstract,
- description of what is your contribution and what is new in your report,
- introduction (modification, background and related work, objectives and methods),
- description of assumptions/schemes/models/problem-formulation,
- comparison/discussion/derivation etc. of the results,
- conclusions (findings and suggestions for improvements) and
- references.
- Report must include appropriate figures and must have some hard data (tables/plots/screen-shots/algorithms etc.).

- Evaluation: significance and originality, thoroughness of research, depth of understanding displayed and presentation.

Measuring Security Posture of Various Android Based IoT Applications

Upakar Paudel

Colorado State University

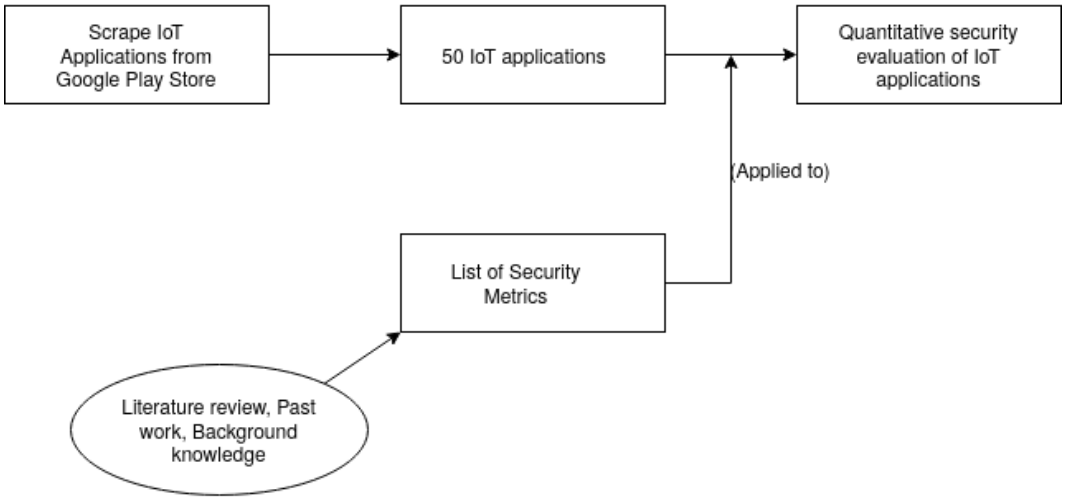
OVERVIEW

- IoT device rise in popularity opens up a lot of security and privacy issues
- IoT applications act as a bridge between IoT device and outer network
- IoT applications need to be secure to better protect IoT devices and network

CONTRIBUTION

- Devised various metrics to measure security health of IoT applications
- Measured the security health of 50 IoT applications based on devised metrics
- Understand the correlation between various metrics and security health of IoT applications

METHODOLOGY



Security Metrics	Tools
Strength of Password Policy	Crylogger
RiskInDroid Score	RiskInDroid
CVSS Score	MobSF
Malicious/Risky third party dependencies	MobSF
Number of ICC Leaks	IccTa / FlowDroid
App Rating	Application Detail
Use of expired/invalid certification	MobSF
Sensitive data to logs/third party	MobSF
Days Since last released update	Application Detail
Number of Cryptoguard violations	Cryptoguard
Number of Crylogger violations	Crylogger

SECURITY METRICS AND TOOLS USED

Application	RiskInDroid_Score	CVSS Score	Malicious/Risky 3rd Party Depencies	App Rating	# Invalid Certs	Sensitive Data to Logs	Days since release	FlowDroid # of l	# CryptoGuard violations	Crylogger Violations
castify.roku	20.00949004	6.2	No Severity	4.3	Severity (7.4)	Severity (7.5)	0	1	85	6
castwebbrowsertotv.castwebvideo.webvideocaster	16.87102103	6.3	No Severity	4.3	Severity (7.4)	Severity (7.5)	266	3	45	
cn.ubia.ubox	39.66391169	6.2	No Severity	3	Severity (7.4)	Severity (7.5)	1	55	50	2
co.bitfinder.awair	25.1147021	6.5	No Severity	3.5	Severity (7.4)	Severity (7.5)	19	4	20	
co.sonofy.smartroomsolutions	44.78844702	5.9	No Severity	3.5	No Severity (0)	Severity (7.5)	22	0	26	2
com.abb.energyviewer	27.80792497	5.6	No Severity	3	No Severity (0)	Severity (7.5)	25	0	19	2
com.adt.pulse	17.63325678	5.9	No Severity	4.5	No Severity (0)	Severity (7.5)	187	7	19	
com.alarm.alarmmobile.android.guardian	12.77713509	5.9	No Severity	4	No Severity (0)	Severity (7.5)	21	2	22	
com.allocacoc.smart	13.03858582	6.2	No Severity	4.1	No Severity (0)	Severity (7.5)	336	1	47	
com.angelcam	16.37759876	6	No Severity	4.3	No Severity (0)	Severity (7.5)	40	4	12	
com.bosch.indegoconnect	32.18617769	6	No Severity	2.8	No Severity (0)	Severity (7.5)	64	11	7	3
com.concept2.ergdata	23.78130006	5.8	No Severity	3	No Severity (0)	Severity (7.5)	174	8	5	3
com.customsolutions.android.alexa	13.77088834	6	No Severity	3.8	Severity (7.4)	Severity (7.5)	1	17	68	
com.datadudu.ubibot	83.55327179	6.1	No Severity	4	No Severity (0)	Severity (7.5)	14	16	10	
com.ezviz	26.49029453	6.2	No Severity	3.8	No Severity (0)	Severity (7.5)	4	6	53	3
com.fibaro.homecenter	25.48420798	5.9	No Severity	2.3	No Severity (0)	Severity (7.5)	45	10	14	
com.govee.home	15.4987491	6.3	No Severity	3.7	No Severity (0)	Severity (7.5)	26	5	29	3
com.hubble.care	23.65007916	6.2	No Severity	4	No Severity (0)	Severity (7.5)	1	1	34	
com.hunter.hunterWifiConnectAndroid	39.28325299	5.9	No Severity	1.9	No Severity (0)	Severity (7.5)	89	3	22	
com.ilifesmart.mslict_gp	50.22148724	6.2	No Severity	4.2	Severity (7.4)	Severity (7.5)	25	1	81	
com.iruleav.nebula.android.prod	62.88423324	6.2	No Severity	4.6	No Severity (0)	Severity (7.5)	223	0	9	2
com.jibo	17.53310785	6.1	No Severity	4.1	No Severity (0)	Severity (7.5)	867	7	27	
com.lgeha.nuts	18.20389998	6.3	No Severity	3.9	Severity (7.4)	Severity (7.5)	14	5	85	
com.mm.android.direct.AmcrestViewPro	16.44592273	5.8	No Severity	3.7	No Severity (0)	Severity (7.5)	125	15	6	
com.mm.android.yale	44.35523956	5.9	No Severity	3.6	No Severity (0)	Severity (7.5)	128	1	33	
com.mobics.kuna	32.14857018	6.2	No Severity	3.5	No Severity (0)	Severity (7.5)	202	6	31	2
com.netatmo.camera	38.70498726	5.7	No Severity	4.1	No Severity (0)	Severity (7.5)	7	3	17	2
com.northstar.connect	54.72970251	6.2	No Severity	3.6	No Severity (0)	Severity (7.5)	35	5	16	
com.safety1st.babymonitor	15.6002384	6.1	No Severity	2.2	No Severity (0)	Severity (7.5)	15	12	41	
com.schneider_electric.wiser2	26.55555704	5.8	No Severity	3.2	Severity (7.4)	Severity (7.5)	439	1	7	2
com.sensibo.app	40.91785054	5.8	No Severity	3.9	No Severity (0)	Severity (7.5)	21	18	11	2
com.seventwentysoftware.powerzoneplus	23.30521411	5.1	No Severity	4.7	No Severity (0)	Severity (7.5)	290	1	0	3
com.simplisafe.mobile	37.09232772	6.2	No Severity	4.7	No Severity (0)	Severity (7.5)	8	4	53	
com.smarthvac	11.55532989	5.7	No Severity	3.7	No Severity (0)	Severity (7.5)	53	7	17	2
com.smartroost.app	29.39379723	5.5	No Severity	2.7	No Severity (0)	Severity (7.5)	147	0	10	3
com.sonova.hansaton.rcapp	34.51833581	6	No Severity	2.6	No Severity (0)	Severity (7.5)	145	3	24	
com.specialyg.ippro	52.77745701	6.3	No Severity	3.1	Severity (7.4)	Severity (7.5)	55	40	90	
com.supremevue.ecobeewrap	13.05248864	6	No Severity	4.1	No Severity (0)	Severity (7.5)	25	8	29	3
com.tplink.tpm5	19.77756491	6.2	No Severity	4.7	No Severity (0)	Severity (7.5)	18	2	47	11
com.tuya.smart	15.73711562	6.1	No Severity	4.2	No Severity (0)	Severity (7.5)	24	0	37	2
com.velux.active	39.1415388	5.9	No Severity	3.5	No Severity (0)	Severity (7.5)	22	0	2	
com.vivitarsecurity.smart	16.14666676	6.2	No Severity	3.6	Severity (7.4)	Severity (7.5)	127	1	45	
com.vuebell	6.408135591	6	No Severity	2.9	Severity (7.4)	Severity (7.5)	4	6	51	
com.xvrview	75.35598769	6.2	No Severity	2.3	Severity (7.4)	Severity (7.5)	16	29	17	
de.twokit.video.tv.cast.browser.firetv	15.3456646	6.4	No Severity	3	Severity (7.4)	Severity (7.5)	34	1	44	3
eu.hoermann.ast.bluesecur	59.96070958	5.8	No Severity	2.8	No Severity (0)	Severity (7.5)	98	0	3	
io.fireboard.android	46.59954102	5.7	No Severity	4.2	No Severity (0)	Severity (7.5)	31	18	11	7
no.easee.apps.easee.users	21.54588838	6	No Severity	4.1	No Severity (0)	Severity (7.5)	7	16	4	2
xyz.angeldev.flux	24.58459827	5.8	No Severity	4.1	No Severity (0)	Severity (7.5)	38	0	5	1

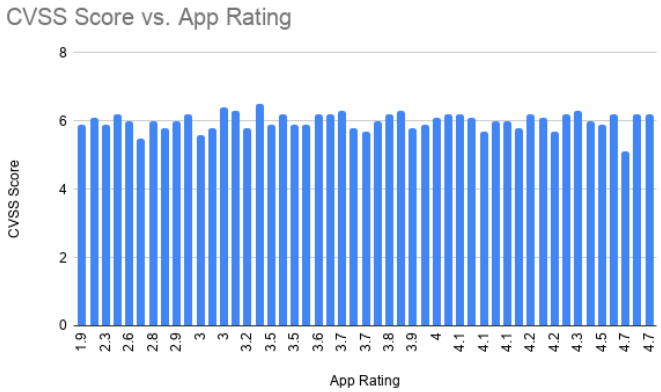
Measured Metrics

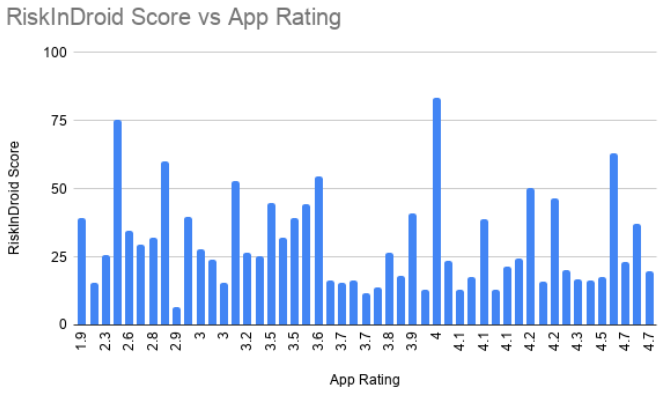
cryptoguard	crylogger
Rule 2: Found broken hash functions	R-01: Don't use broken hash functions (SHA1,MD2,MD5, ..)
Rule 1: Found broken crypto schemes	R-02: Don't use broken encryption alg. (RC2,DES,IDEA..)
	R-03: Don't use the operation modeECBwith>1 data block
	R-04: Don't use the operation modeCBC(client/server scenarios)
Rule 9: Found constant salts in code	R-10: Don't use a static (= constant) salt for key derivation
	R-11: Don't use a short salt (<64 bits) for key derivation
	R-12: Don't use the same salt for different purposes
Rule 3: Used constant keys in code	R-05: Don't use a static (= constant) key for encryption
	R-07: Don't use a static (= constant) initialization vector (IV)
Rule 10: Found constant IV in code	R-08: Don't use a "badly-derived" initialization vector (IV)
	R-09: Don't reuse the initialization vector (IV) and key pairs
Rule 8a: Used < 1000 iteration for PBE ***Constants: [1000]	R-13: Don't use<1000 iterations for key derivation
Rule 11: Found predictable seeds in code	R-17: Don't use a static (= constant) seed for PRNG
Rule 13: Untrusted PRNG	R-18: Don't use an unsafe PRNG (java.util.Random)
Rule 7: Used HTTP Protocol	R-22: Don't use HTTP URL connections (use HTTPS)
Rule 14: Used Predictable KeyStore Password	R-23: Don't use a static (= constant) password for store
Rule 12: Does not manually verify the hostname	R-26: Don't manually change the hostname verifier
Rule 6: Uses untrusted HostNameVerifier	R-24: Don't verify host names in SSL in trivial ways
Rule 4: Uses untrusted TrustManager	R-25: Don't verify certificates in SSL in trivial ways
Rule 5: Used export grade public Key	
	R-14: Don't use a weak password (score<3)
	R-15: Don't use a NIST-black-listed password
	R-16: Don't reuse a password multiple times
	R-19: Don't use a short key (<2048 bits) for RSA
	R-20: Don't use the textbook (raw) algorithm for RSA
	R-21: Don't use the paddingPKCS1-v1.5for RSA

Cryptoguard vs Crylogger rules

Application	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15	R16	R17	R18	R19	R20	R21	R22	R23	R24	R25	R26
castify.roku	V	V	R	V	S	R	S	R	V	S	R	R	R	R	R	S	S	V	R	R	R	V	S	R	R	R
castwebbrowsertotv.castwebvideo.webvideocaster	V	R	R	V	S	R	S	R	V	S	R	R	R	R	R	S	S	V	R	R	R	R	S	R	R	R
cn.ubia.ubox	V	R	R	R	S	R	S	R	R	S	R	R	R	R	R	S	S	V	R	R	R	R	S	R	R	R
co.bitfinder.awair	V	R	R	R	S	R	S	R	R	S	R	R	R	V	R	S	S	V	R	R	R	R	S	R	R	R
co.sonofy.smartroomsolutions	V	R	R	R	S	R	S	R	R	S	R	R	R	R	R	S	S	V	R	R	R	R	S	R	R	R
com.abb.energyviewer	V	R	R	R	S	R	S	R	R	S	R	R	R	R	R	S	S	V	R	R	R	R	S	R	R	R
com.alarm.alarmmobile.android.guardian	V	R	R	R	S	R	S	R	R	S	R	R	R	R	R	S	S	V	R	R	R	R	S	R	R	R
com.angelcam	V	R	R	R	S	R	S	R	R	S	R	R	R	R	R	S	S	V	R	R	R	R	S	R	R	R
com.bosch.indegoconnect	V	R	R	R	S	R	S	R	R	S	R	R	R	R	R	S	S	V	V	R	R	R	S	R	R	R
com.concept2.ergdata	V	R	R	R	S	R	S	R	R	S	R	R	R	R	R	S	S	V	V	R	R	R	S	R	R	R
com.customsolutions.android.alexa	V	R	R	V	S	R	S	R	R	S	R	R	R	R	R	S	S	V	V	R	R	R	S	R	R	R
com.datadudu.ubibot	V	R	R	V	S	R	S	R	V	S	R	R	R	R	R	S	S	V	R	R	R	R	S	R	R	R
com.ezviz	V	R	R	R	S	R	S	R	R	S	R	V	R	R	R	S	S	V	R	R	R	R	S	R	R	R
com.fibaro.homecenter	V	R	R	R	S	R	S	R	R	S	R	R	R	R	R	S	S	V	R	R	R	R	S	R	R	R
com.govee.home	V	R	R	V	S	R	S	R	R	S	R	R	R	R	R	S	S	V	R	R	R	R	S	R	R	R
com.iruleav.nebula.android.prod	V	R	R	R	S	R	S	R	R	S	R	R	R	R	R	S	S	V	R	R	R	R	S	R	R	R
com.jibo	V	R	R	R	S	R	S	R	R	S	R	R	R	R	R	S	S	V	R	R	R	R	S	R	R	R
com.mobics.kuna	V	R	R	R	S	R	S	R	R	S	R	R	R	R	R	S	S	V	R	R	R	R	S	R	R	R
com.netatmo.camera	V	R	R	R	S	R	S	R	R	S	R	R	R	R	R	S	S	V	R	R	R	R	S	R	R	R
com.safety1st.babymonitor	V	R	R	R	S	R	S	R	R	S	R	R	R	R	R	S	S	V	R	R	R	R	S	R	R	R
com.schneider_electric.wiser2	R	R	R	V	S	R	S	R	R	S	R	R	R	R	R	S	S	V	R	R	R	R	S	R	R	R
com.sensibo.app	V	R	R	R	S	R	S	R	R	S	R	R	R	R	R	S	S	V	R	R	R	R	S	R	R	R
com.seventwentysoftware.powerzoneplus	V	R	R	R	S	R	S	R	R	S	V	R	R	R	R	S	S	V	R	R	R	R	S	R	R	R
com.smarthvac	V	R	R	R	S	R	S	R	R	S	R	R	R	R	R	S	S	V	R	R	R	R	S	R	R	R
com.smartroost.app	V	R	R	R	S	R	S	R	R	S	R	R	R	R	R	S	S	V	V	R	R	R	S	R	R	R
com.supremevue.ecobeewrap	V	R	R	V	S	R	S	R	R	S	R	R	R	R	R	S	S	V	R	R	R	R	S	R	R	R
com.tplink.tpm5	V	V	V	V	S	R	S	R	V	S	V	R	V	R	R	S	S	V	R	R	V	R	S	R	V	V
com.tuya.smart	V	R	R	R	S	R	S	R	R	S	R	R	R	R	R	S	S	V	R	R	R	R	S	R	R	R
de.twokit.video.tv.cast.browser.firetv	V	R	R	R	S	R	S	R	R	S	R	R	R	R	R	S	S	V	R	R	R	V	S	R	R	R
io.fireboard.android	V	R	R	R	S	R	S	R	R	S	V	R	V	V	R	S	S	V	V	R	R	R	S	R	V	R
no.easee.apps.easee.users	V	R	R	R	S	R	S	R	R	S	R	R	R	R	R	S	S	V	R	R	R	R	S	R	R	R
xyz.angeldev.flux	R	R	R	R	S	R	S	R	R	S	R	R	R	R	R	S	S	V	R	R	R	R	S	R	R	R

Individual Crylogger Violations





Correlation across CVSS, RiskInDroid Score and App Rating

OBSERVATION

- All applications are vulnerable to sending sensitive data to logs/third party
- Applications don't usually communicate with bad host on the internet
- Applications show high vulnerability with regard to use of broken hash function and unsafe random number generator
- No correlation between App Rating and CVSS score / RiskInDroid score

CONCLUSION & FUTURE WORK

- **Conclusion:**
  - Measured the security health of 50 IoT applications
  - Pinpointed areas that need improvement and developers can address
- **Future Work:**
  - Extend current work with additional IoT applications
  - Devise other suitable metrics to measure security health of IoT applications
  - Perform thorough analysis

REFERENCES

- Daniel R. Thomas, Alastair R. Beresford, and An-drew Rice. 2015. Security Metrics for the Android Ecosystem. In Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smart-phones and Mobile Devices (SPSM '15). Association for Computing Machinery, New York, NY, USA, 87–98. DOI:https://doi.org/10.1145/2808117.2808118
- R. M. Savola, P. Savolainen, A. Evesti, H. Abie and M. Sihvonen, "Risk-driven security metrics development for an e-health IoT application," 2015 Information Security for South Africa (ISSA), Johannesburg, 2015, pp. 1-6, doi: 10.1109/ISSA.2015.7335061.T. Zheng, T. Jianwei, Q. Hong, L. Xi, Z. Hongyu, and
- Q. Wenhui, "Design of automated security assessment framework for mobile applications," in 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, Nov. 2017, pp. 778–781, doi: 10.1109/ICSESS.2017.8343028.
- L. Piccolboni, G. Di Guglielmo, L. P. Carloni, and S. Sethumadhavan, "CRYLOGGER: Detecting Crypto Misuses Dynamically," arXiv:2007.01061 [cs], Jul. 2020, doi: 10.1109/SP40001.2021.00010.

Quantitative Analysis of MITRE ATT&CK and Threat Modeling for Industrial Control Systems.

Author: Shwetha Gowdanakatte

Professor: Dr. Yashawant Malaiya

Computer Science
Colorado State University

Colorado State University

OVERVIEW

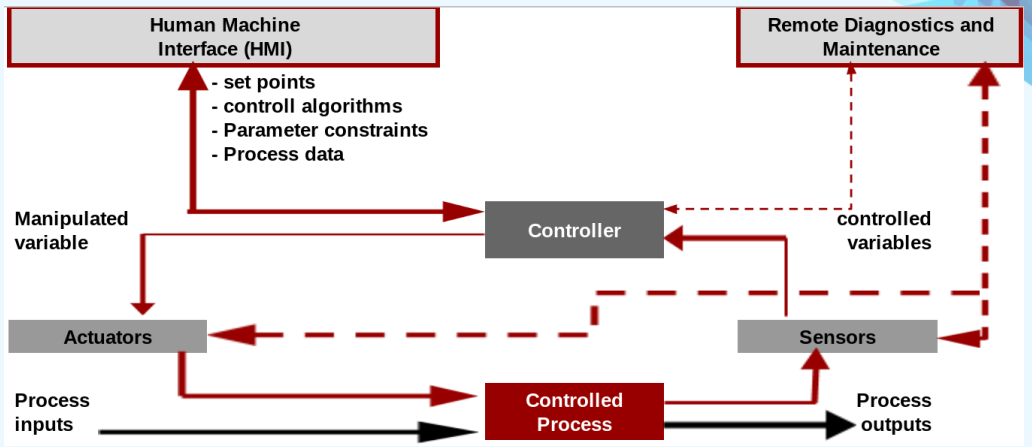
In this paper, I explore

- Current standards, procedures and technologies for vulnerability detection and threat modeling for Industrial Control Systems [ICS].
- Quantitative examination of MITRE ATT&CK for ICS.
- Recent research in threat modeling and vulnerability detection for ICS.
- Demonstrate manual threat modeling for ICS.
- Propose Automated threat modeling for ICS.

Index Terms: Cyber Security, Industrial Control Systems [ICS], Supervisory Control and Data Acquisition [SCADA], Human Machine Interface [HMI], Programmable Logic Controller [PLC], Information Technology [IT], Operation Technology [OT], Advanced Persistent Threats [APT], Industrial Internet Of Things [IIOT], Common Vulnerabilities and Exposures [CVE]

INTRODUCTION TO ICS

- ICS: Collective term used to describe the control systems and associated instrumentation used to automate the industrial process.
- Typically include Human Machine Interface [HMI], Programmable Logic Controller [PLC], sensor, network systems,
- Supervisory Control and Data Acquisition Systems [SCADA] are used to control and monitor ICS.

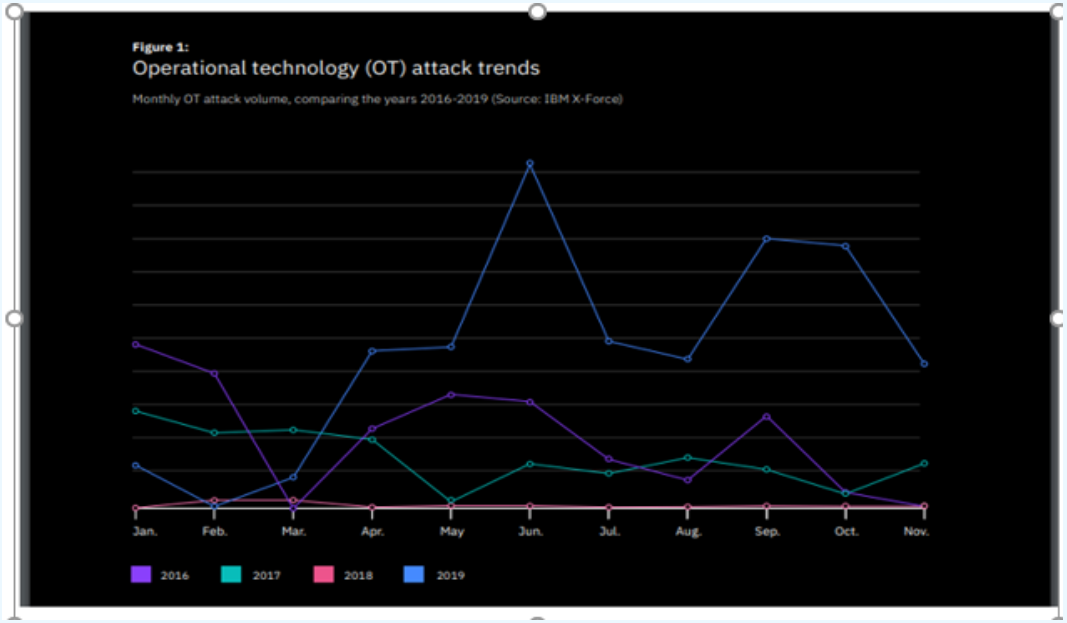


INTRODUCTION TO ICS

- Initial ICS systems were isolated from enterprise network and the internet, has hence been less vulnerable to cyber-attacks.
- Current day ICS systems are equipped with advanced communication protocols, such as TCP/IP, Modbus, Device-Net
- Vulnerable to cyber-attacks.

Years	Attacks
2019	Hydro Cyber Attack
	Hexane on Oil and Gas Industries
	Cyber attack on HOYA
	Nyrstar Ransomware attack
2018	Allanite
	Lyceum APT
	Ransomeware Attack on Manufacturing system
2017	DragonFly
	BadRabbit Rasomware
	Triton Attack
	Trisis: Saudi Arabia
	Merck's cyber attack
	APT33 US Aerospace and Energy sectors
	Xanotime
	Wannacry attack
	Crashoverride
	NotPetya
2016	Ukraine: Crash Override
	Attack on German Nuclear Power Plant
	APT33 US Aerospace and Energy sectors
	Kermuri Water Company
	Shamoon : Saudi Arabia
2015	Helmith: OilRig
	Dymalloy
	Black Engery on Ukranian Power Grids
2014	DragonFly
2013	Infiltration of Newyork Dam
	MAGNALLIUM Petrochemical Industry
	Havex
2012	Shamoon : Saudi Arabia
	Gas Pipe line cyber intrusion
2011	Dymalloy
	duqu
2010	Stuxnet
	Night Dragon: Oil and Gas
2009	Derail City Tran Systems
2008	Turkey Pipe line explosion

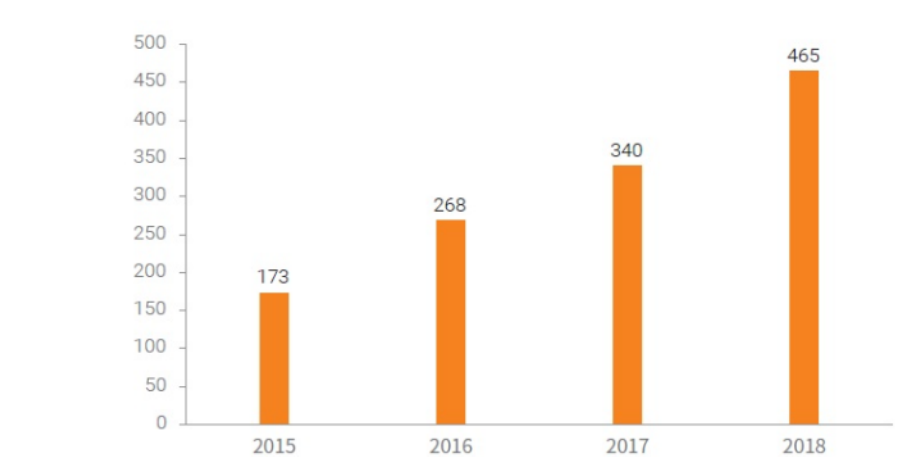
ICS: CYBER ATTACKS STATISTICS



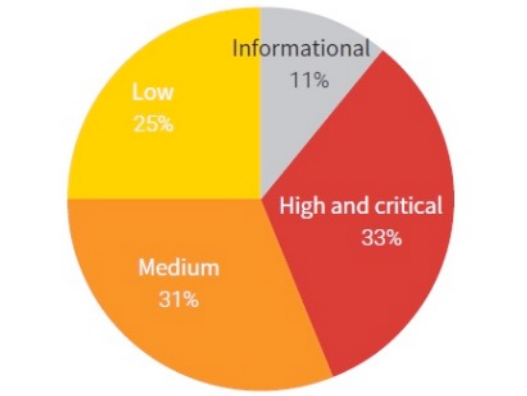
ICS Statistics 2016-2019: IBM-X-Force Report

ICS: CYBER ATTACKS STATISTICS

ICS Vulnerability trend from 2015-2018: [7]



Distribution of security issues by risk level: [7]



CURRENT STATE OF TECHNOLOGY

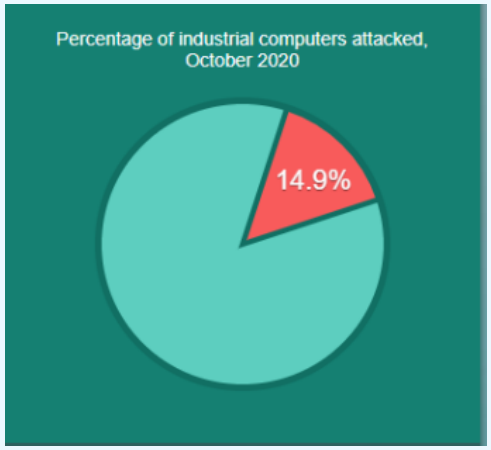
- 2002: Strategies for ICS security by DHS [Department of Homeland Security.
- 2006: A national infrastructure plan for ICS security.
- 2010: Industrial Control System Network Emergency Response Team (ICS-CERT).
- 2011: Standards for ICS security by NIST.
- ICS Kill Chain: Adapted from cyber kill chain created by Lockheed Martin.
- 2020: MITRE ATT&CK Framework for ICS.

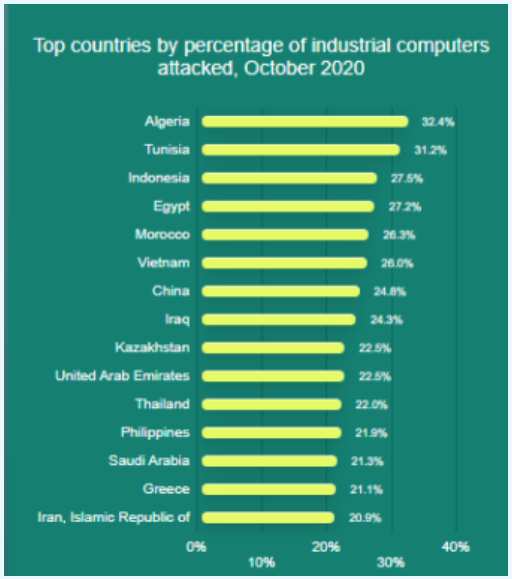
Dragos Inc. :

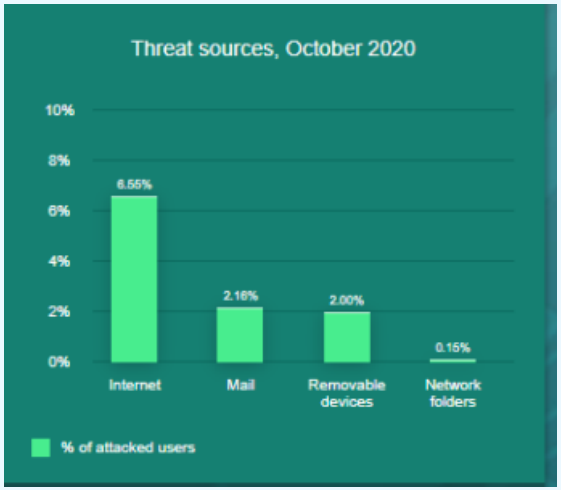
- Provides in-depth visibility of threats for ICS and provides recommendations.
- Regular reports, critical alerts, executive insight, webinars and more.
- Reported 438 ICS vulnerabilities, 3 new activity groups targeting ICS systems in 2019.

CURRENT STATE OF TECHNOLOGY

Kaspersky Lab: Reports on latest vulnerabilities, threats and recommendations.





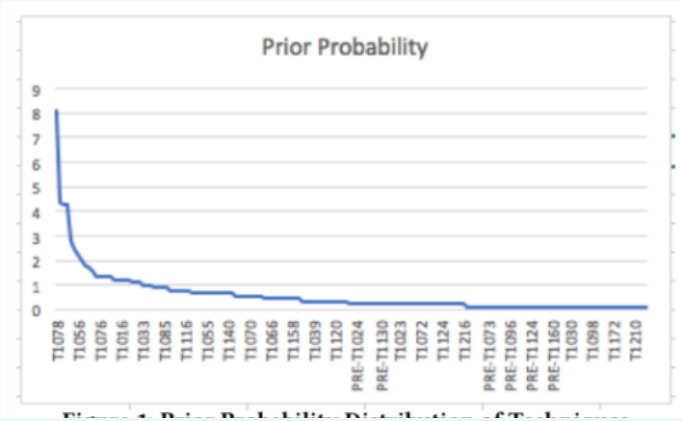


RELATED RESEARCH-1

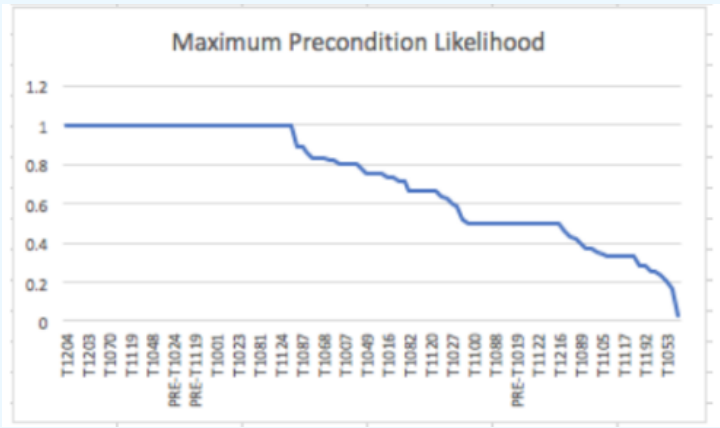
Al-Shaear. et.all[11]: Statistical analysis of APT TTP chains of MITRE ATT&CK.

Main Idea: Principal Component Analysis and prior distribution of techniques in reported ATP attacks.

Provides fundamental techniques the probability of techniques for a set of adversaries.



Prior probability distribution techniques [11]



Maximum Prediction Likelihood [11]

RELATED RESEARCH-2

Falco, et. All [5]: AI based attack planner for smart cities.

Incorporates MITRE and Cyber Kill Chain for attack tree generation.

Pros: Effective compared to manual attack trees.

Cons: Lack of data on Probabilistic results on possible techniques.

D. Cerotti et.all [2]: Bayesian network for monitoring and forecasting adversaries for power grid systems.

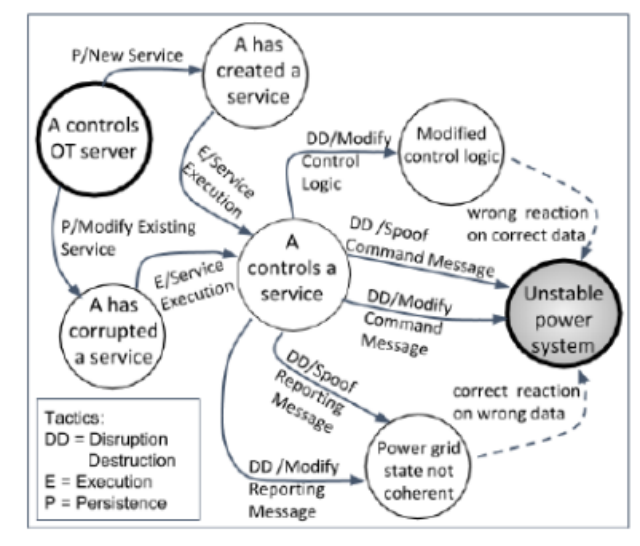
Analyzes attacks at DMZ between IT and OT networks.

Pros: Excellent method for prediction of techniques for ICS.

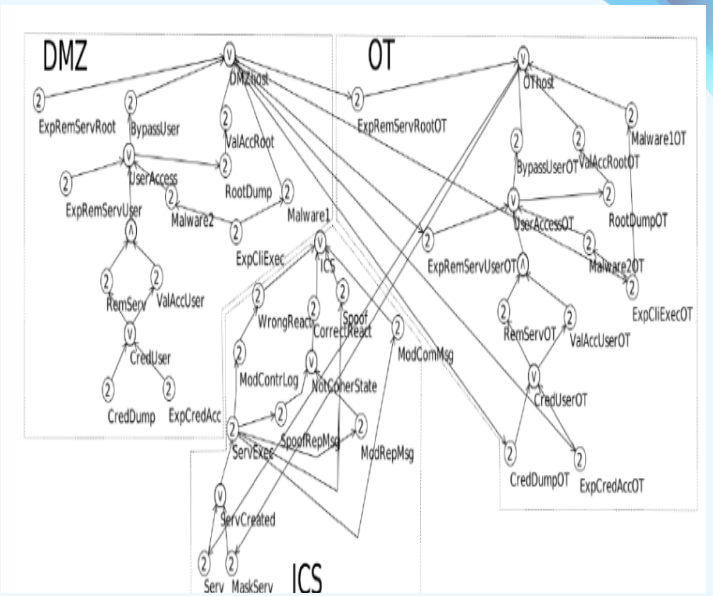
Cons: Does not provide details on implementation of Bayesian networks.

Technique	Prob.
BypassUser	0.021764
CredDump	0.0717119
ExpCredAcc	**0.342749**
ExpRemServRoot	0.0359553
ExpRemServUser	0.0057617
RemServ	0.0024305
RootDump	0.0364453
ValAccRoot	0.0019609
ValAccUser	0.010796

Probabilistic values for techniques from Bayesian Network. [2]



Bayesian Network Attack Graph [2]



Bayesian Network Model [2]

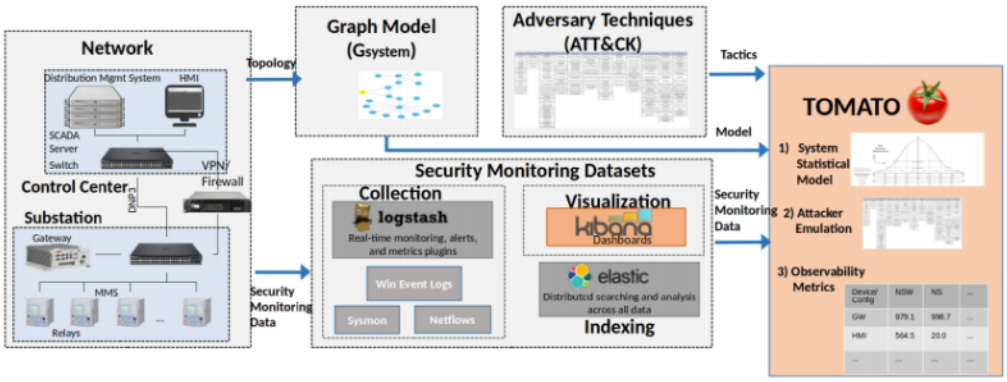
RELATED RESEARCH-3

Halvosen et.al. [6]: TOMATO [Threat Observability and Monitoring, Assessment Tool]

Measure the effectiveness of security monitoring. It evaluates a number of adversarial techniques and false alarms.

Pros: More advanced than the previous method.

Cons: Not address the detection of attacks and vulnerabilities at components level.



Architectural Overview of TOMATO

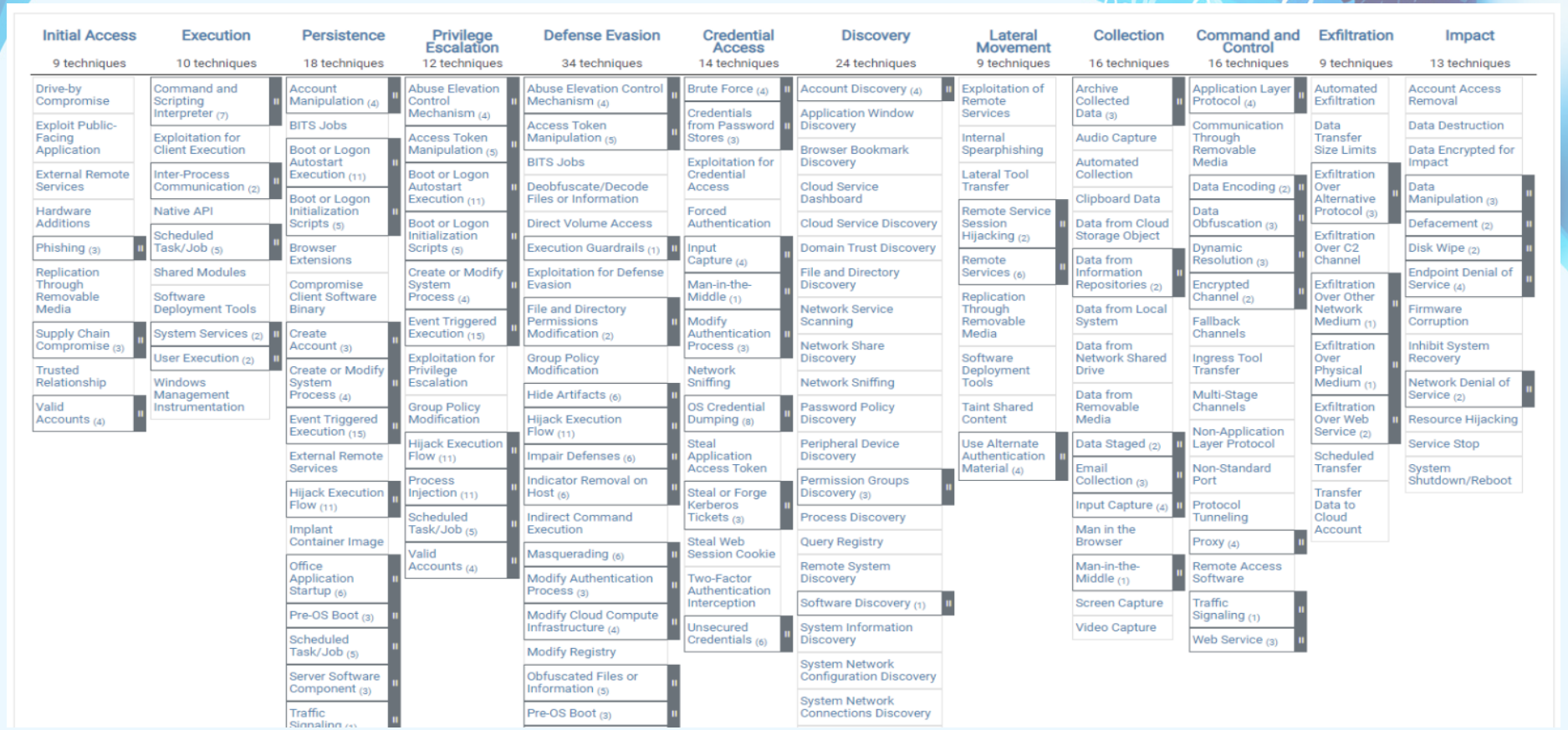
Event	Num Occurr.	Freq.	Anomalous Freq.
sc.exe	7	0.0026	0.2333
ipconfig.exe	6	0.0022	0.2000
rundll32.exe	4	0.0015	0.1333
cmd.exe	3	0.0011	0.1000
powershell.exe	3	0.0011	0.1000
reg.exe	2	0.0007	0.0666
net.exe stop	1	0.0004	0.0333
regsvr32.exe	1	0.0004	0.0333
sdbinst.exe	1	0.0004	0.0333
parent=taskeng.exe	1	0.0004	0.0333

Distribution of Anomalous Process Creation Events on the Gateway Device

Host	Tactic	$P(f_{tactic}\|Host)$
GW	Lateral Movement	0.2931
GW	Discovery	0.0022
GW	Execution	0.0052
GW	Privilege Escalation	0.0404
HMI	Lateral Movement	0.4549
HMI	Discovery	0
HMI	Execution	0
HMI	Privilege Escalation	0.0316

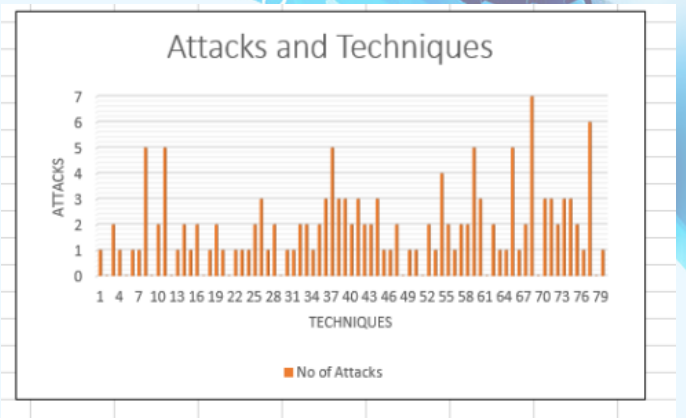
Probability Distribution of Finding Attack Tactics Using Host-Based Monitoring [6]

MITRE ATT&CK FRAMEWORK FOR ICS



MITRE ATT&CK FRAMEWORK FOR ICS

Attacks			Tactics and Techniques	
	Intial Access	Execution	Persistance	Evasion
Trition	Eng. Wrk Stattion	Change Program State	Program. Donwload	Exploitattion for Evasion
		Exec thrugh API	System Firmware	Indicator Removal on Host
		Scripting		
Industroyer or Crash ove	Data Historian Compromise	Command Line Interface		
Dragonfly Havox	sphearphishing attachement	User Execution		
	supply chain compromise			
Black Energy	sphearphishing attachement		Valid Account	
Bad Rabbit	Drive By Conpromise	User Execution		
	External Remote Services			
Conficker	Replication Through Removable Media			
Duqu				
Flame				
kill disc				Indicator Removal on Host



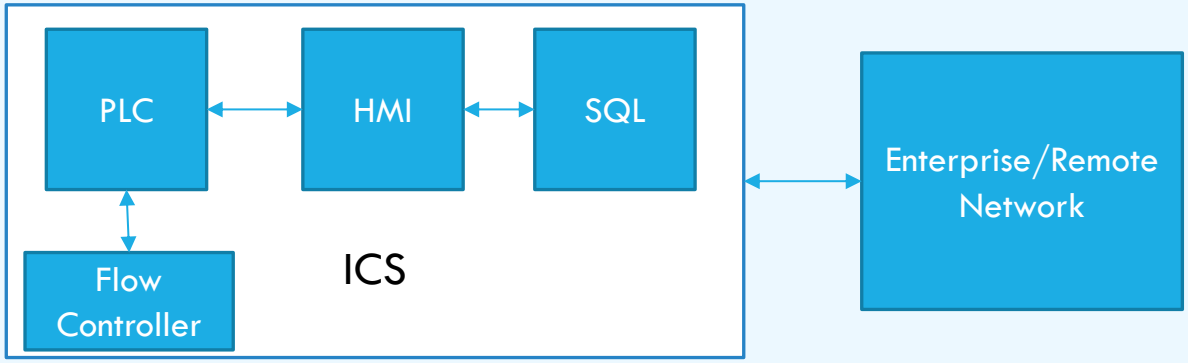
Techniques	Attacks
Spearphishing Attachment	7
Valid Accounts	6
Remote System Discovery	5
Change Program State	5
Scripting	5
Program Download	4

MANUAL THREAT MODELING FOR ICS

Example ICS system: Air Sampling and particle monitoring system.

- Monitors air particles in pharmaceutical clean rooms.
- Periodically samples air at a certain flow rate.

Critical Assets: PLC, HMI, SQL Server and Flow Controller with PID



MANUAL THREAT MODELING FOR ICS

Vulnerabilities released in 2019 for Rockwell Components

Component	vulnerability	Risk
Compact Logix 5370 PLC	Remote Exploiatbility	Denial Of Service
	cross site scripting	Denial Of Service
Panel View Plus 700-1500 HMI	Improper access control	Remote Attacker can access to the target system
Ethernet module:1756-ENBT	Remote Exploiatbility	Denial Of Service
	Buffer overflow	

Possible Adversaries and Techniques for this application

Adversaries	Techniques
Initial Access	Data Historian Compromise
	sphearphishing attachement
Execution	Change program state
	Man in the middle
Persistance	Program download
	Valid account
Discovery	Remote discovery
Inhibit Response Function	Modify control logic
	Service Stop
Impact	Denial of Service
	Loss of availability
	Loss of control

Based on the analysis, the possible attacks can be:

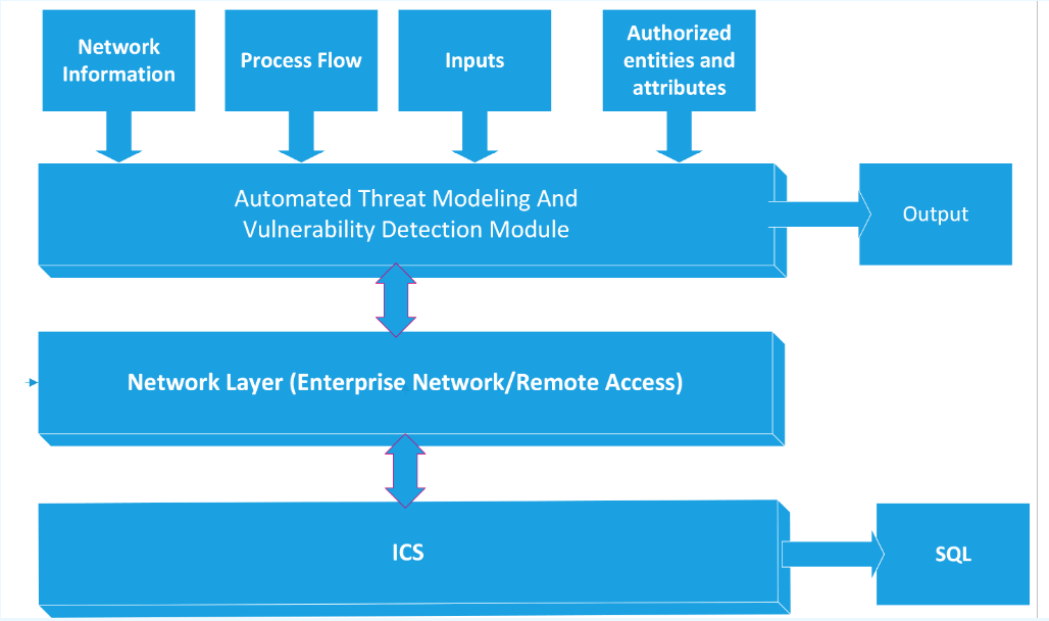
- Triton.
- Industroyer or Crashoverride.
- Dragonfly Havox.

Limitations:

- In this method, threats are analyzed manually based on the ICS architecture, MITRE ATT&CK framework, and the vulnerabilities that are disclosed to the public. This can be time consuming and tedious for complex ICS systems.
- Testing of techniques and adversaries can be done only by penetration and brute force method for each adversary.
- This method fails to detect vulnerabilities that are not discovered yet.

PROPOSED AUTOMATED THREAT MODELING

Proposed Architecture



- Takes the inputs, such as network information (IP addr, subnet mask, gateway), process flow, inputs and authorized entities and attributes.
- Performs various attacks with MITRE ATT&CK techniques on the given ICS systems.
- Analyzes probability of techniques that can be successfully used by possible adversaries, and detects vulnerabilities in the PLC and HMI.
- Produces the probabilistic results on techniques and vulnerabilities.

PROPOSED AUTOMATED THREAT MODELING

Hypothetical Output

Possible Techniques	Probability
Data Historian Compromise on the HMI	0.85
Denial Of Service	0.7
Unitended PLC Start/Stop	0.65
Unitended Program Modification	0.6
Unauthorized access	0.5
Loss of Availability	0.4

Detected Vulnerabilities
Crafted TCP/IP Packets
SQL injection attacks
Vulnerability in Remote Web Server

Overall Percentage Of Security Risk	70%

Implementation Discussion:

- Implementation of the AI algorithm to take the inputs and generate attack trees for various attacks.
- Apply MITRE ATT&CK techniques for each attack and test them against ICS
- Calculate the probabilities of possible techniques and detect vulnerabilities

Next Steps:

- Implementation of Automated Threat Modeling tool.
- Simulate the attacks and verify the effectiveness of the tool.

Conclusion

- ICS attacks are increasing every year as the automation industries and manufacturing facilities are incorporating advanced technology for their ICS.
- Many organizations are working towards implementing standards and providing security assessments for ICS.
- Current Research in the field of threat modeling and vulnerability demonstrates that we need to come up with effective automated threat modeling techniques.
- Proposed automated threat modeling can be useful if it can be demonstrated through implementation and simulation.
- Conclusively, I got to learn a lot about recent trends in ICS attacks, current state of technology and current research in the related field.

Acknowledgement

MANY THANKS TO DR. MALAIYA FOR PROVIDING AN OPPORTUNITY TO CONDUCT RESEARCH ON THIS TOPIC, FOR HIS GUIDANCE AND TIMELY SUPPORT. THANKS FOR THE CONSTRUCTIVE FEEDBACK ON THE PROGRESS REPORT.

REFERENCES

[1] Analysis of the cyber attack on the ukrainian power grid. https://ics.sans.org/media/E-ISAC SANS Ukraine DUC 5.pdf, 2016.

[2] D. Cerotti , D.Codetta-Raiteri1, and G.Dondossola. A bayesian networkapproach for the interpretation of cyber attacks to power systems. June 2019.

[3] T. M. Chen and S. Abu-Nimeh. Lessons from stuxnet. Computer,44(4):91–93, April 2011.

[4] etc.. Davide Cerotti, Daniele Codetta-Raiteri. Evidence-based analysis of cyber attacks to security monitored distributed energy resources. Applied Science, July 2020.

[5] G. Falco, A. Viswanathan, C. Caldera, and H. Shrobe. A master attack methodology for an ai-based automated attack planner for smart cities. IEEE Access, 6:48360–48373, 2018.

[6] James Halvorsen, Jesse Waite, and Adam Hahn. Evaluating the observability of network security monitoring strategies with tomato. IEEE Access.

[7] Mina hao. Ics information security assurance framework 10. https://nsfocusglobal.com/ics-information-security-assurance-framework-10/,2020.

[8] Zhang Jian, Yang Li, and Liao Haode. A security architecture model of oil and gas scada network based on multi-agent. International Journal of Security and Its Applications, 10:449–460, 01 2016.

[9] MITRE. ATTCK for Industrial Control Systems. https://collaboratemitre.org/attackics/index.php/Main Page, 2020.

[10] MITRE. Brute Force I/O. https://collaborate.mitre.org/attackics/index.php/Technique/T806, 2020.

[11] J. M. Spring R. Al-Shaer and E. Christou. Learning the associations of mitre att ck adversarial techniques. IEEE Conference, pages 1–9.

[12] T. Williams. The purdue enterprise reference architecture, 1993.

[13] Coffey Kyle etc. Zhou, Jianying. Vulnerability analysis of network scanning on scada systems. Computer, 2018.

[14] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain. Machine learning-based network vulnerability analysis of industrial internet of things. IEEE Internet of Things Journal, 6(4):6822–6834,2019.

CYBER RISK AND CYBER INSURANCE

CS559 QUANTITATIVE SECURITY

SURAJ ESWARAN

COLORADO STATE UNIVERSITY

INTRODUCTION

- **Cyber Risk**: Any risk form the **use of IT systems** that affects the **confidentiality**, **availability** or **integrity** of information (systems) caused by (non) criminal activity.
- A form of risk from the exposure resulting from a **cyber-attack** or **data breach**.
- Organizations tend to become more **vulnerable** to these kinds of threats due to their **high reliability** on **computers**, **networks**, and **information** in order to have a good relationship with the delivery of the services.
- In order to protect against these risk, many businesses have cyber insurance with their insurance policy.
- **Cyber Insurance:** A **financial policy** which helps the businesses to send the funds involving in recovery from cyber risk events.
- This paper deals with the understanding the **various views on cyber risk insurance** and its **challenges that arises in insurance markets** in the recent years.

CYBER RISK= CONSEQUENCE OF THE ATTACK x LIKELIHOOD OF THE ATTACK

THREATS FACED RECENTLY

Business Fraud

Government Fraud

Investment Fraud

Utility Fraud

Confidence Fraud

Auction Fraud

Credit/Debit Card Fraud

Technology Fraud

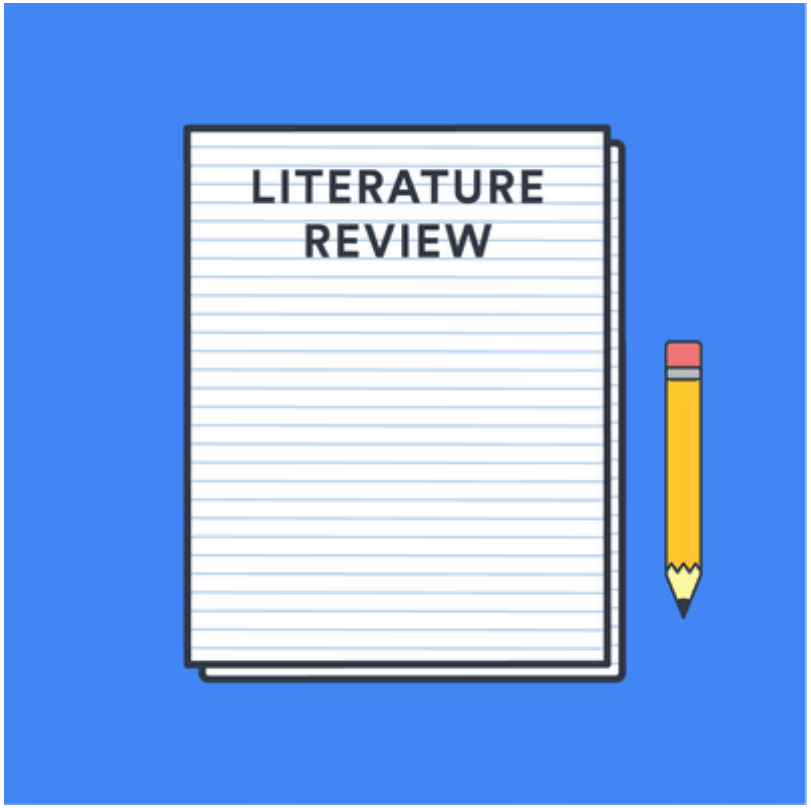
RESEARCH QUESTIONS

List of research questions were listed during this analysis:

1. RQ1: How **dangerous** is **Cyber Risk**?
2. RQ2: What were the several ways in handling **Cyber-Risk** by Insurers?
3. RQ3: What are the **challenges** faced in **insurance markets** in the recent years?

LITERATURE REVIEW

- Kokolakis et.al: Utilized **IT risk** with the help of **BPM(Business Process Modeling)**.
- Pernul et al.: Developing a **secured** business process based on security requirements.
- Halliday et al.: Conducted **risk analysis** with high level business strategy.
- Rodriguez et. al.: Elaborated the analysis of **Business Process Modelling Notation(BPMN)** with security requirements.
- Majuca et. al.: Explains the **evolution of cyber insurance** in **2005**.
- Mukhopadhyay et. al. : Developed **Utility Based Preferential Pricing(UBPP)** in distinguishing **cyber insurance pricing policy**.
- Ulrik Franke : Documented the **empirical study of cyber insurance market** in **Sweden**.



RQ1: HOW DANGEROUS IS CYBER RISK?

61% of **data breaches** are **malicious attacks**.

47% **increase in data breaches** due to **Social Engineering.**

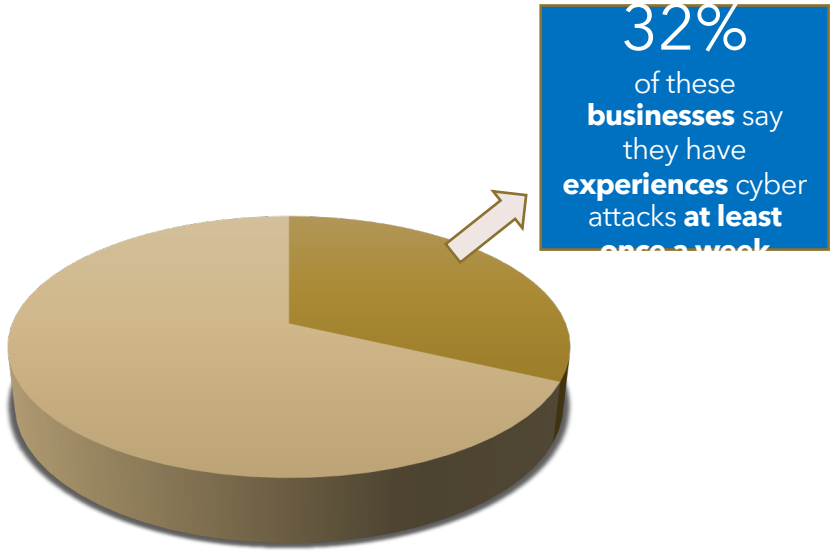
22% of notifications came from the **health sector**.

Motivation behind attack may be to **encrypt data**.

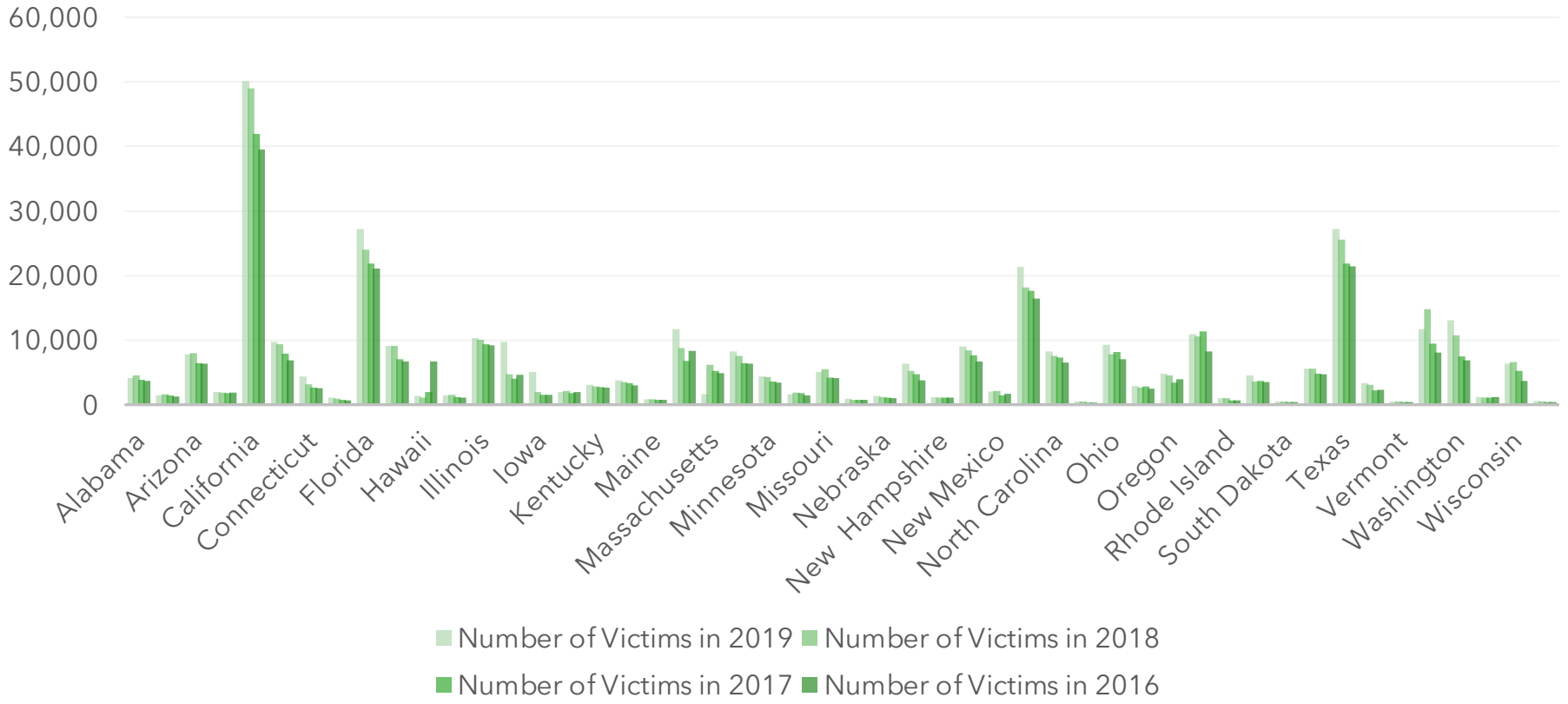
Many **businesses** are reportedly **paying attacks** to **recover data**.

$3846.48 - **Avg. amount** of cyber attacks of **businesses of all size**

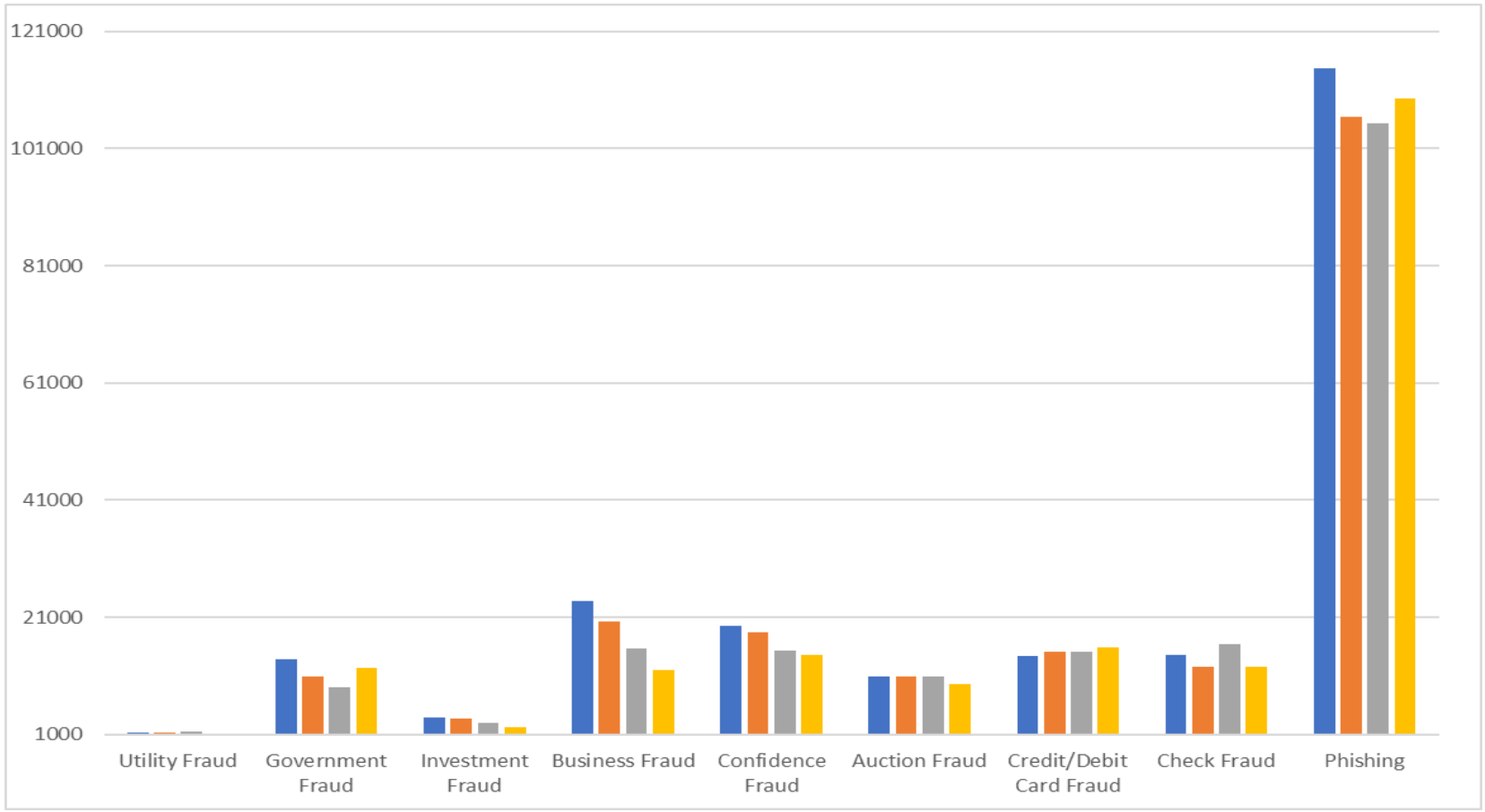
$6216.34 - **Avg. amount** of cyber attacks of **businesses of medium and large sizes**



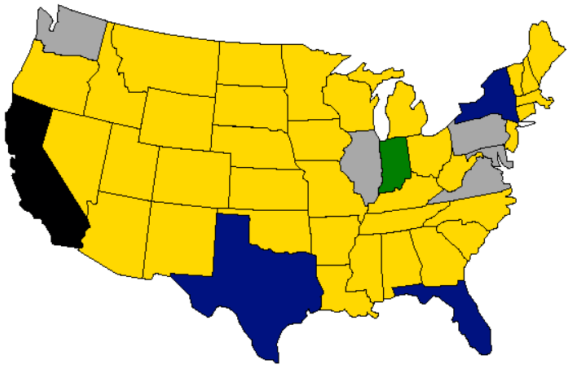
Number of victims



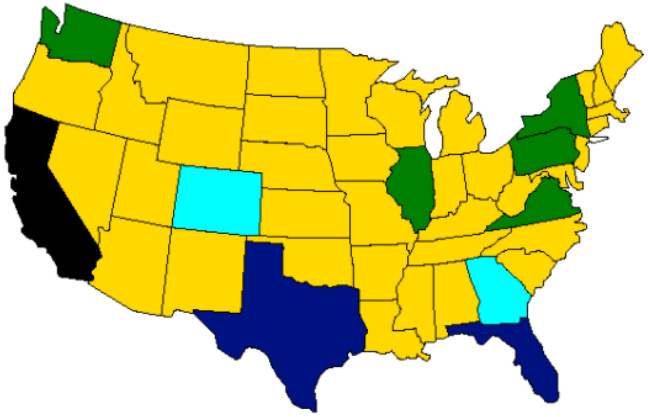
FIELDS AFFECTED DUE TO CYBER RISK FROM 2019 TO 2016



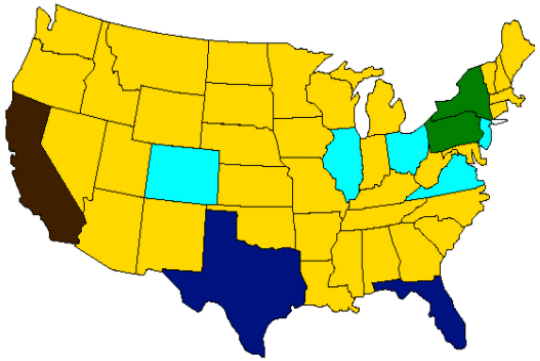
2019



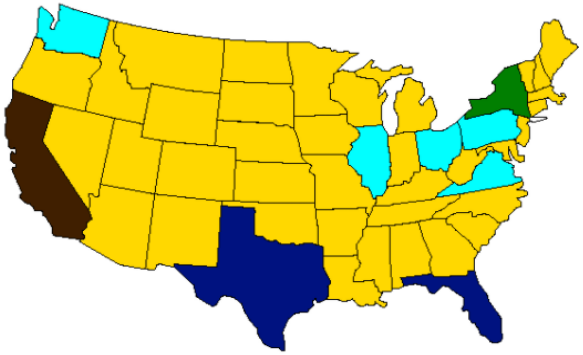
2018



2017



2016



CYBER RISK INSURANCE

- **Cyber Risk Insurance** is developed in such a way to reduce the losses from **various cyber incidents** like **data breaches**, or **network interruptions**.
- A **robust** cyber risk insurance involves:
  - **Improving** the **usage of preventative measures** for more **coverage**.
  - **Encouraging** the **usage of best practices** by premiums on **insurer's level of self protection**.

RQ2: WHAT WERE THE SEVERAL WAYS IN HANDLING CYBER RISK BY INSURERS?

- Cyber security insurance as a "**stand alone** " line if coverage.
- Coverages includes **1st party coverage**, **liability coverage** and **other benefits** includes security-audit, post- incident and criminal rewards.
- Annual gross premiums for cyber risk insurance in United States: **From $1.3 billion to $2.5 billion**.
- Thus, there is a **fledgling market** compared with others streamlines of insurance business.

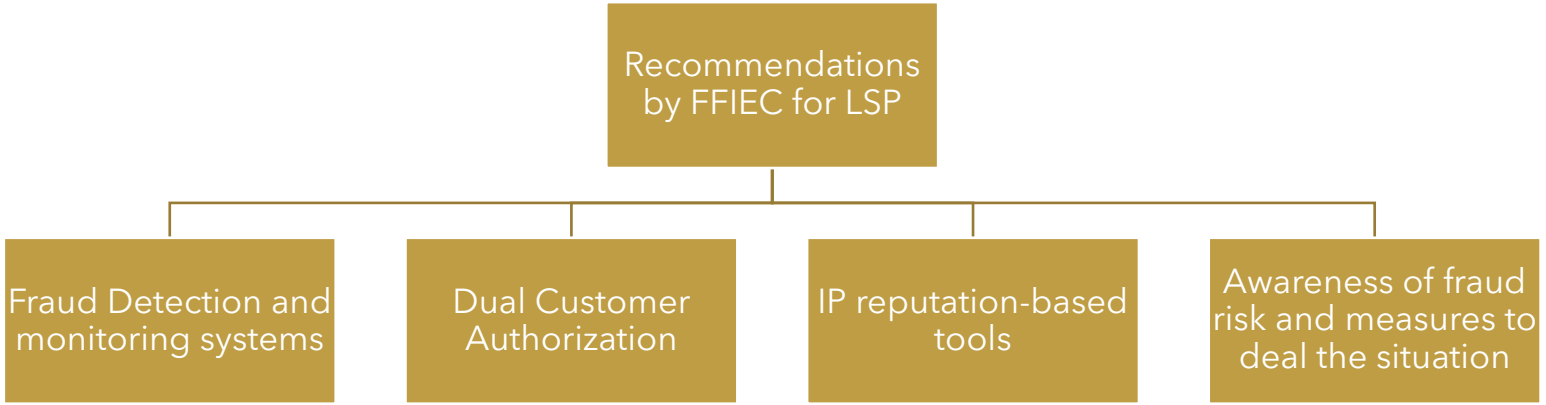
PERSPECTIVES ON CYBER RISK AND INSURANCE

- **Federal Financial Institutions Examination Council**
- Guidelines they follow: **Provide a risk management framework** for Internet based products to customers.

The 2005 Guidance provided a risk management framework for financial institutions offering Internet-based products and services to their customers. It stated that institutions should use effective methods to authenticate the identity of customers and that the techniques employed should be commensurate with the risks associated with the products and services offered and the protection of sensitive customer information.

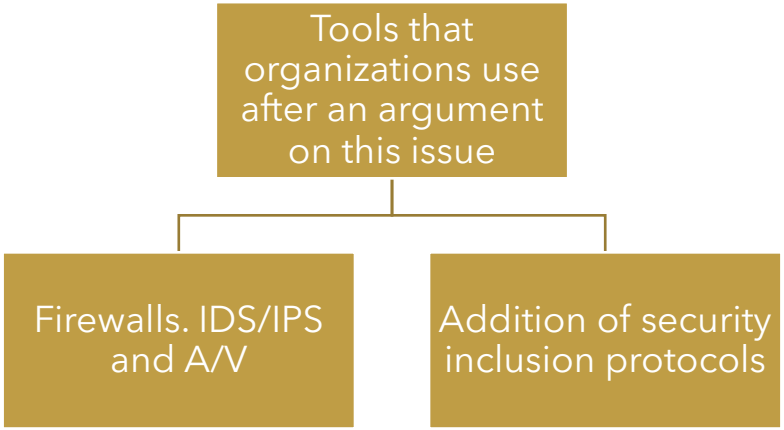
LAYERED SECURITY PROTOCOL(LSP) FOR CYBER RISK

- Use of **different scenario**s at different during a transaction process.
- Enhance **overall security** for **internet-based products** and **services**.



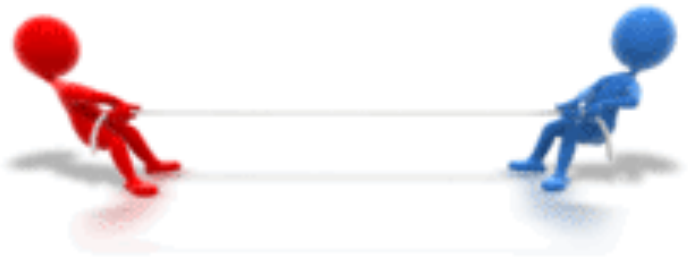
INDUSTRIAL PERSPECTIVES ON CYBER RISK AND REGULATIONS

- **RSA** mentioned in their report a term named **GAP** which explained an approach to assess, diagnose **vulnerabilities** between **IT fields** and **security fields**.
- **Risk managers** and **senior executives** are not interested to specify the kind to attack and vulnerability according to perspective of IT fields.
- Whereas **IT team** and **security team** do not focus on type of cyber breach that leads to high loss impacts.



RQ3:WHAT ARE THE CHALLENGES FACED IN INSURANCE MARKETS IN THE RECENT YEARS?

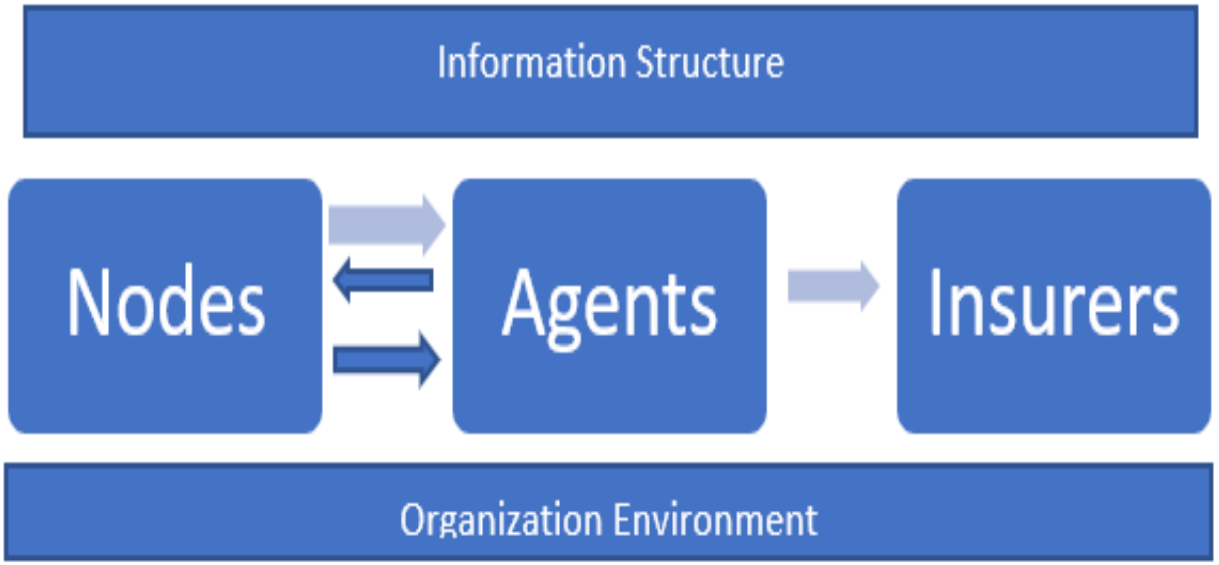
- **Reactionary strategies** are not designed well with affected process of the **business.**
- Not placing a **formal method** to collect and analyze data regarding cyber insurance market.
- **Business developments** are involved outside the **IT sphere** which only allows to see in loss point of view rather than the information point of view.
- **95%** of cyber risk happens due to misinterpretations by business team and IT team.
- By **2022**, there can be huge increase in **$140 billion** ,If they do not follow the regulations.



SOLUTION TO THESE CHALLENGES

- Organizations must look over interests of **both the groups**.
- Being **proactive**.
- **Educating your employees** on dealing with data

ANY REFINEMENTS OF THE PROPOSAL OBJECTIVES AS A RESULT OF THE PAST STUDY



REFERENCES

1. S. Kokolakis, A. Demopoulos and E. Kiountouzis, “The use of business process modeling in information systems security analysis and design,” Inf.Manag.&Comp. Security, 8, 2000, p. 107-116.
2. Herrmann, G., & Pernul, G. (1998, January). Towards security semantics in workflow management. In Proceedings of the Thirty-First Hawaii International Conference on System Sciences (Vol. 7, pp. 766-767). IEEE.
3. S. Roehrig and K. Knorr, “Security Analysis of Electronic Business Processes,” Electronic Commerce Research, vol. 4, 2004, P. 59-81.
4. C. Ribeiro and P. Guedes, “Verifying Workflow Processes against Organization Security Policies,” 8th IEEE International Workshops on Enabling Technologies, 1999, P. 190-191.
5. S. Halliday, K. Badenhorst and R. von Solms, “A business approach to effective information technology risk analysis and management“ Information Management&Computer Security, vol. 4/1, 1996, P. 19–31.
6. A. Rodriguez, E. Fernandez-Medina and M. Piattini, “A BPMN Extension for the Modeling of Security Requirements in Business Processes,” IEICE Trans. INF. & SYST., vol. E90–D, Apr. 2007.
7. B. Suh und I. Han, “The IS risk analysis based on a business model,” Information & Management, vol. 41, 2003, P. 149–158.
8. R.K. Rainer, C.A. Snyder and H.H. Carr, “Risk Analysis for Information Technology,” Journal of Management Information Systems, vol. 8, 1991, P. 129-147.
9. Böhme R, Schwartz G. Modeling cyber-insurance: towards a unifying framework. In: Workshop on the Economics of Information Security (WEIS). Cambridge, MA: Harvard University, 2010.
10. Marotta, A., Martinelli, F., Nanni, S., & Yautsiukhin, A. (2015). A survey on cyber-insurance. Technical Rep. IIT TR-17/2015. Istituto di Informatica e Telematica, Consiglio Nazionale delle Richerce, Pisa.
11. Majuca, R. P., Yurcik, W., & Kesan, J. P. (2006). The evolution of cyberinsurance. arXiv preprint cs/0601020.
12. Woods, D., Agrafiotis, I., Nurse, J. R., & Creese, S. (2017). Mapping the coverage of security controls in cyber insurance proposal forms. Journal of Internet Services and Applications, 8(1), 8.
13. Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2017). Content analysis of cyber insurance policies: How do carriers write policies and price cyber risk?. Available at SSRN 2929137.
14. Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not?. Decision Support Systems, 56, 11-26.
15. Herath, H., & Herath, T. (2011). Copula-based actuarial model for pricing cyber-insurance policies. Insurance markets and companies: analyses and actuarial computations, 2(1), 7-20.
16. Franke, U. (2017). The cyber insurance market in Sweden. Computers & Security, 68, 130-144.
17. Gartner Inc. (n.d.). Forecast Analysis: Information Security, Worldwide, 2Q18 Update. Retrieved November 08, 2020, from https://www.gartner.com/en/documents/3889055
18. Symantec Security Center. (n.d.). Retrieved November 08, 2020, from https://www.broadcom.com/support/security-center
19. Böhme, R., & Schwartz, G. (2010, June). Modeling Cyber-Insurance: Towards a Unifying Framework. In WEIS.\
20. Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: how do carriers price cyber risk?. Journal of Cybersecurity, 5(1), tyz002.
21. Falco, G., Eling, M., Jablanski, D., Miller, V., Gordon, L. A., Wang, S. S., ... & Donavan, E. (2019). A research agenda for cyber risk and cyber insurance. In Workshop on the Economics of Information Security (WEIS)..
22. Camillo, M. (2017). Cyber risk and the changing role of insurance. Journal of Cyber Policy, 2(1), 53-63.
23. Anon. Internet Crime Complaint Center(IC3): Home Page. Retrieved November 30, 2020 from https://www.ic3.gov/
24. Shetty, N., Schwartz, G., Felegyhazi, M., & Walrand, J. (2010). Competitive cyber-insurance and internet security. In *Economics of information security and privacy* (pp. 229-247). Springer, Boston, MA.
25. Podolak, G. D. (2014). Insurance for Cyber Risks: A Comprehensive Analysis of the Evolving Exposure, Today's Litigation, and Tomorrow's Challenges. *Quinnipiac L. Rev.*, *33*, 369.

The Severity of Cybercrimes and Methods to Prevent

Ya-Hsin Cheng

Colorado State University

Outline

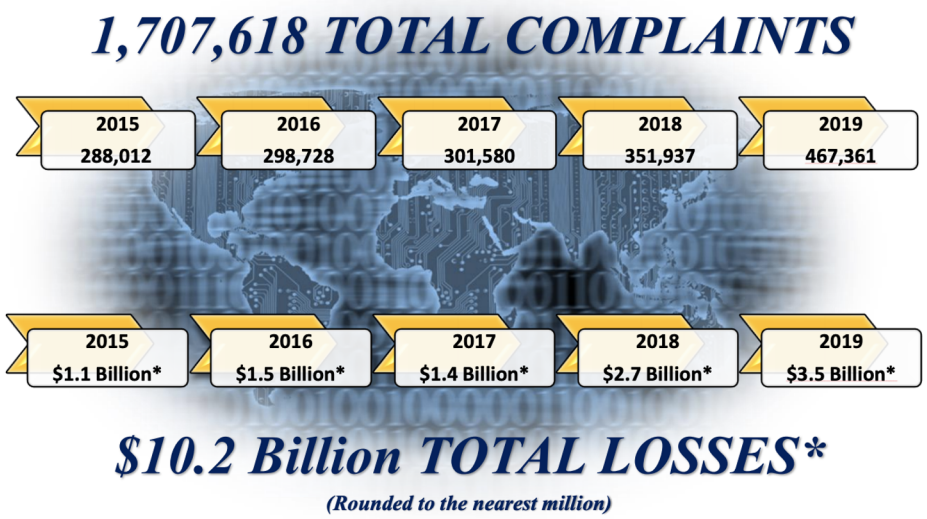
- Introduction
  - Cybercrimes
  - Cybercriminals
- Schemes and Models
  - Machine Learning
  - Data Mining
- Advantages and Disadvantages
- Conclusion

Introduction

- Cybercrimes
  - Cybercrime can be divided into several types: data theft, child pornography, cyber bullying, cyber hacking
    - Social media crimes
    - Data Theft
- Cybercriminals
  - Build by Social Ties as Base
  - Build by Forums as Base

IC3 Complaint Statistics

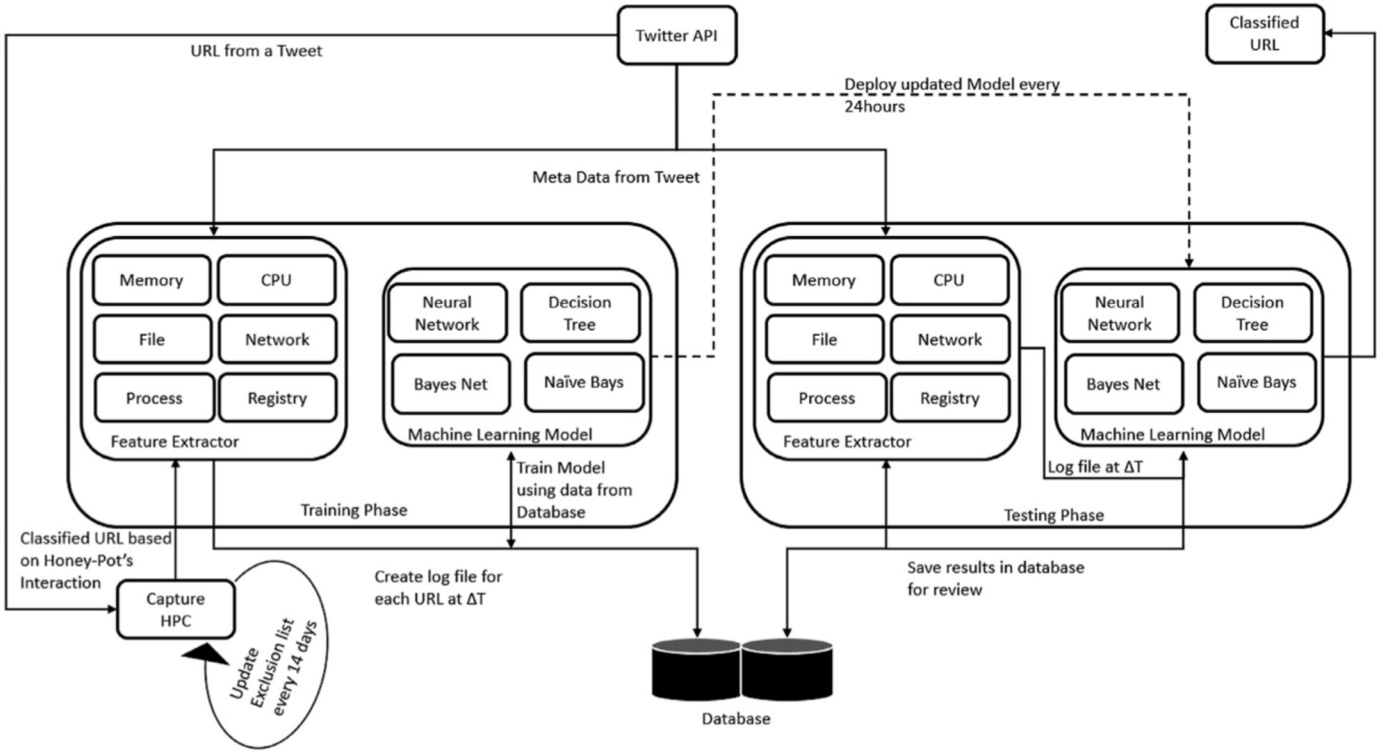
Last Five Years



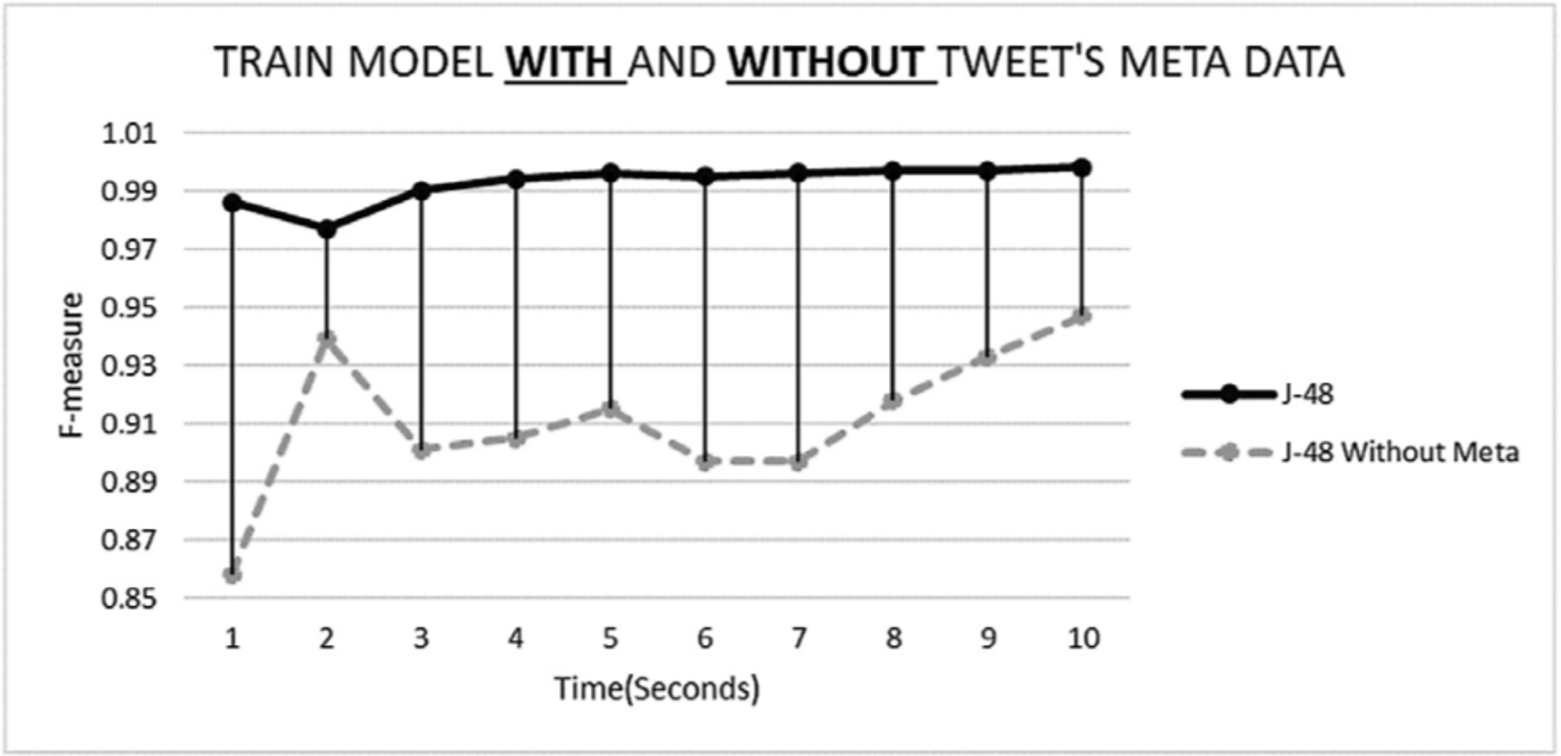
The statistical results from FBI's Internet Crime Complaint Center (IC3)

Schemes and Models

- Machine Learning
  - Malicious URLs from Twitter Posts
    - Metadata (username, user screen name, user id, follower count, friends count, and age of account, etc.)
  - Detect Data Breach from Underground Forums
- Data Mining
  - Hospital data leakage



Architecture of predictive model



F–Measure score (with or without metadata)

Advantages and Disadvantages

- Advantages
  - Machine Learning
    - Reduce the time to find
    - Predict the attack
  - Data Mining
    - Find the weak part of system and strengthen it
    - The collected data can use as the train set for machine learning

Advantages and Disadvantages

- Disadvantages
  - Machine Learning
    - Need a lot of data for training
    - Might exist the misjudgment
  - Data Mining
    - Need the time to analyze the reason
    - It can’t predict the attack

Conclusion

- Data mining can be helpful for finding the problem of data leaking
- Data mining can be a helper for machine learning
- If choose the suitable Machine learning model, it can be a powerful tool to prevent cybercrimes from happening

REFERENCES

[1] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq and M. K. Khan, ”Comprehensive Review of Cybercrime Detection Techniques,” in IEEE Access, vol. 8, pp. 137293-137311, 2020, doi: 10.1109/ACCESS.2020.3011259.[Online]. Available: https://ieeexplore.ieee.org/document/9146148/

[2] ”Cost of a Data Breach Report 2020,” IBM. [Online]. Available: https://www.ibm.com/security/digital-assets/cost-data-breach-report/. [Accessed: 11-Oct-2020].

[3] H. Landi, ”Average cost of healthcare data breach rises to $7.1M, according to IBM report,” FierceHealthcare, 29-Jul-2020. [Online]. Available: https://www.fiercehealthcare.com/tech/average- cost-healthcare-data-breach-rises-to-7-1m-according-to-ibm-report. [Accessed: 11-Oct-2020].

[4] T. Floyd, M. Grieco and E. F. Reid, ”Mining hospital data breach records: Cyber threats to U.S. hospitals,” 2016 IEEE Conference on Intelligence and Security Informatics (ISI), Tucson, AZ, 2016, pp. 43-48, doi: 10.1109/ISI.2016.7745441.[Online]. Available: https://ieeexplore.ieee.org/iel7/7739307/7745427/07745441.pdf[Accessed: 11-Oct-2020]

[5] M.Furdek,C.Natalino,F.Lipp,D.Hock,A.D.GiglioandM.Schiano, ”Machine Learning for Optical Network Security Monitoring: A Prac- tical Perspective,” in Journal of Lightwave Technology, vol. 38, no. 11, pp. 2860-2871, 1 June, 2020, doi: 10.1109/JLT.2020.2987032.[Online]. Available: http://ieeexplore.ieee.org/document/9064530[Accessed: 11- Oct-2020].

[6] R.Sabillon, J.Cano, V.Cavaller, J.Serra. ”Cybercrime and Cybercriminals: A Comprehensive Study,” International Journal of Computer Networks and Communications Security, vol. 4, no. 6, pp. 165–176, June 2016. [Online].Available: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/78507/1/p1 4- 6.pdf[Accessed: 11-Oct-2020].

[7] T. S. Sudha and C. Rupa, ”Analysis and Evaluation of Inte- grated Cyber Crime Offences,” 2019 Innovations in Power and Advanced Computing Technologies (i-PACT), Vellore, India, 2019, pp. 1-6, doi: 10.1109/i-PACT44901.2019.8960187.[Online]. Available: https://ieeexplore.ieee.org/document/8960187[Accessed: 11-Oct-2020].

[8] R.Ch, T.R.Gadekallu, M.H.Abidi, A.Al-Ahmari. ”Computational Sys- tem to Classify Cyber Crime Offenses using Machine Learning,” SUSTAINABILITY, vol. 12, no. 10, May 2020.[Online]. Available: https://www.mdpi.com/2071-1050/12/10/4087/pdf [Accessed: 11-Oct- 2020].

REFERENCES

[9] Z. Abbass, Z. Ali, M. Ali, B. Akbar and A. Saleem, ”A Framework to Predict Social Crime through Twitter Tweets By Using Machine Learning,” 2020 IEEE 14th International Conference on Semantic Computing (ICSC), San Diego, CA, USA, 2020, pp. 363-368, doi: 10.1109/ICSC.2020.00073.[Online]. Available: https://ieeexplore.ieee.org/iel7/9022806/9031442/09031496.pdf[Accessed: 11-Oct-2020].

[10] Y.Fang,Y.Guo,C.HuangandL.Liu,”AnalyzingandIdentifyingData Breaches in Underground Forums,” in IEEE Access, vol. 7, pp. 48770- 48777, 2019, doi: 10.1109/ACCESS.2019.2910229.[Online]. Available: https://ieeexplore.ieee.org/document/8686093[Accessed: 11-Oct-2020].

[11] A.Javed, P.Burnap, O.Rana, “Prediction of Drive-by Download Attacks on Twitter.” in Information processing management ,vol. 56, Issue 3, pp. 1133-1145, May 2019.[Online]. Available: https://www-sciencedirect- com.ezproxy2.library.colostate.edu/science/article/pii/S0306457317305824 [Accessed: 06-Nov-2020].

[12] E.R.Leukfeldt, E.R.Kleemans, W.P.Stol, ”Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties Within Phishing and Malware Networks”, in The British Journal of Criminology, vol. 57, Issue 3, pp. 704–722, 1 May 2017.[Online]. Available: https://academic-oup-com.ezproxy2.library.colostate.edu/bjc/article/57/3/704/2624001 [Accessed: 06-Nov-2020].

[13] E.R.Leukfeldt, E.R.Kleemans, W.P.Stol,”Origin, growth and criminal capabilities of cybercriminal networks. An international empirical anal- ysis”, in Crime Law Soc Change 67, 39–53 , Feb 2017.[Online]. Avail-

able: https://doi-org.ezproxy2.library.colostate.edu/10.1007/s10611-016-

9663-1 [Accessed: 06-Nov-2020].

[14] J.Davis, ”FBI: $3.5B Lost to Cybercrime in 2019, Led by Business

Email Compromise”, in HealthITSecurity.[Online]. Available: https://healthitsecurity.com/news/fbi-3.5b-lost-to-cybercrime-in-2019- led-by-business-email-compromise [Accessed: 06-Nov-2020].

[15] E.R.Leukfeldt, E.R.Kleemans, W.P.Stol,”A typology of cybercrimi- nal networks: from low-tech all-rounders to high-tech specialists” in Crime Law Soc Change 67, 21–37, Nov 2017.[Online]. Avail- able: https://doi-org.ezproxy2.library.colostate.edu/10.1007/s10611-016- 9662-2 [Accessed: 06-Nov-2020].

[16] ”Full Report: 2019 Internet Crime Report”, in FBI News, February, 2020.[Online]. Available: https://pdf.ic3.gov/2019 IC3Report.pdf [Ac- cessed: 06-Nov-2020].

ANALYSIS OF COST AND CAUSE OF U.S. GOVERNMENT SECURITY BREACHES

AUSTEN WEAVER

CS559

AUSTEN.WEAVER@COLOSTATE.EDU

INTRODUCTION

- Due to the nature of any government hard numbers were not found.
- Cost directly associated with dollar amounts.
- Cost associated with global standing.
  - Militarily
  - Economically
  - Politically
- Cause or weaknesses exploited
- Analysis compared to industry security standards

DIRECT COST

- R&D of military technology
  - Many military technologies take over a decade of R&D before becoming operational.
  - Data breaches of this technology help foreign adversaries leap forward without putting in the same time and resources.
  - C-17 took 14 years of development and $6+ billion. The Y-20 took ~8 years(05-13) and an unknown amount of money. (Su Bin hack 2009-2014)
- Man hours
  - Any private organization suffers a data breach they include the FBI and other government agencies in investigations.
- Legal fees & Damages
  - In the case of the OPM breach many lawsuits have been filed against the federal government.

Figure 1: U.S. C-17 on the left, Chinese Y-20 on the right

INDIRECT COST

- Military
- F-22 and J-20
  - $32 billion vs ~$4.5 billion
  - ~20 year development vs ~15 years
- F-35 and J-31
- $400 billion vs ~Unknown however china is marketing it for less than half the cost of a f-35.
- ~18 year development vs In development since ~2011

Figure 2: U.S. F-22

Figure 3: Chinese J-20

Figure 4: U.S. F-35

Figure 5: Chinese J-31

INDIRECT COST CONT.

- Economically
  - Technology stolen from private companies for foreign adversaries to copy and resale at a lower price.
  - Companies affected:
    - Apple – self driving car tech.
    - Micron Technologies - DRAM
    - T-Mobile – Cell phone tech.
    - American Superconductor Inc. (AMSC) – Wind turbine
    - And agricultural development companies – seed corn varieties
- Politically
  - Loss of influence on the global stage

GOVERNMENT PRACTICES

- Levels of Classification
  - All require security clearance
- Need to know
  - Mixture of connected and air gapped networks
- Secret
  - Air gapped networks situated in hardened rooms or buildings
  - No communication devices allowed
- Top-Secret
  - Restricted to those with top-secret security clearance
- Every branch is treated like independent companies
  - All must abide by security policies set at the top, but not all are enforced
- Contractors
  - Too often lowest bid receives contract
  - Priority Bias
- Due to cost of developing technology, projects are sourced out to allied countries thus spreading the data around.
- Underqualified personal managing these small networks

CAUSE

- Legacy Systems
  - "Security through antiquity"
  - Software written in languages that are hard to find skilled developers in.
- Social Engineering
- Phishing attempts
  - Cause of 2016 F-35 data breach
- Many government data breaches have not disclosed how adversaries were able to access their networks.

Table 1: The 10 Most Critical Federal Legacy Systems in Need of Modernization

Agency	System name[a]	System description[a]	Age of system, in years	Age of oldest hardware, in years	System criticality (according to agency)	Security risk (according to agency)
Department of Defense	System 1	A maintenance system that supports wartime readiness, among other things	14	3	Moderately high	Moderate
Department of Education	System 2	A system that contains student information	46	3	High	High
Department of Health and Human Services	System 3	An information system that supports clinical and patient administrative activities	50	Unknown[b]	High	High
Department of Homeland Security	System 4	A network that consists of routers, switches, and other network appliances	Between 8 and 11[c]	11	High	High
Department of the Interior	System 5	A system that supports the operation of certain dams and power plants	18	18	High	Moderately high
Department of the Treasury	System 6	A system that contains taxpayer information	51	4	High	Moderately low
Department of Transportation	System 7	A system that contains information on aircraft	35	7	High	Moderately high
Office of Personnel Management	System 8	Hardware, software, and service components that support information technology applications and services	34	14	High	Moderately low
Small Business Administration	System 9	A system that controls access to applications	17	10	High	Moderately high
Social Security Administration	System 10	A group of systems that contain information on Social Security beneficiaries	45	5	High	Moderate

Figure 6: GAO Analysis of government systems

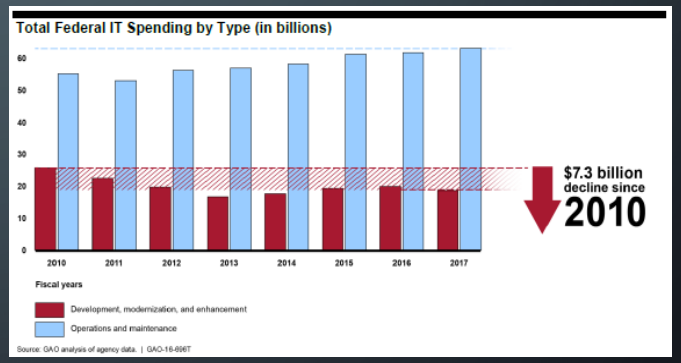


Figure 7: GAO Analysis of IT Spending

OFFICE OF PERSONAL MANAGEMENT(OPM) BREACH

- 21.5 million individuals Social Security Numbers, 19.7 million background reports of which 5.6 million contained fingerprints.
- Security failure on many levels
- Unqualified InfoSec Personnel
- Legacy System
  - Data was not encrypted
- No Two-factor Authentication
- Many systems had not renewed OTA
  - Failed to pass security renewal
- Untimely Patch Management
- Primary breach was through two contractors which allowed for a backdoor malware to be uploaded to the network.

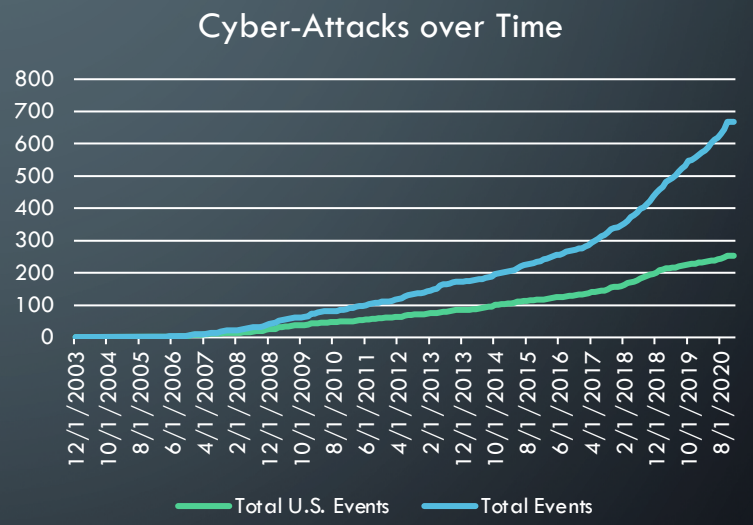


Figure 8: Significant Cyber-attacks tracked by CSIS

CURRENT COVID-19 OBSTACLES

- Any employee working on a classified project cannot work from home.
- No method of accessing air gapped networks
- Attempt to transition some air gapped networks to VPN access with 2FA

REQUIRED GOVERNMENT CHANGES

- Enforce existing security policies across the entire Federal government
- More stringent contractor vetting
- Consolidate data
- Modernize
- Implement modern security network analyzers

CONCLUSION

- Crucial to modernize all systems
- Implement a system of vetting contractors for security while also stipulating that a contractor must maintain a level of security competent staff.
- Cannot let departments fall behind in OTA approval

FUTURE WORK

- Investigate new government security breaches and revise analysis and solutions accordingly

REFERENCES

[1] J. Fruhlinger, "The OPM hack explained: Bad security practices meet China's Captain America," csoonline.com, 12 February 2020. [Online]. Available: https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html. [Accessed 20 November 2020].

[2] T. T. Pham, "OPM Security Audit: No Two-Factor Authentication," duo.com, 10 June 2015. [Online]. Available: https://duo.com/blog/opm-security-audit-no-two-factor-authentication. [Accessed 18 November 2020].

[3] U.S. Government Accountability Office, "Agencies Need to Develop Modernization Plans for Critical Legacy Systems," U.S. Government Accountability Office, Washington D.C., 2019.

[4] U.S. Government Accountability Office, "Federal Agencies Need to Address Aging Legacy Systems," U.S. Government Accountability Office, Washington D.C., 2016.

[5] The Council of Economic Advisers, "The Cost of Malicious Cyber Activity to the U.S. Economy," The Council of Economic Advisers, Washington D.C., 2018.

[6] J. Bambenek, "Nation-state attacks: the new normal," *Network Security,* pp. 8-10, 1 October 2017.

[7] P. Bischoff, "Government breaches - can you trust the US Government with your data?," 24 July 2019. [Online]. Available: https://www.comparitech.com/blog/vpn-privacy/us-government-breaches/. [Accessed 8 October 2020].

[8] H. T. Min-Seok Pang, "Strategic Roles of IT Modernization and Cloud Migration in Reducing Cybersecurity Risks of Organizations: The Case of U.S. Federal Government," *ssrn.com,* vol. 0, no. 0, pp. 1-39, 2019.

[9] J. Moore, "Here Are 10 of the Oldest IT Systems in the Federal Government," 25 May 2016. [Online]. Available: https://www.nextgov.com/cio-briefing/2016/05/10-oldest-it-systems-federal-government/128599/. [Accessed 8 10 2020].

[10] OPM, "Cybersecurity Incidents," opm.gov, [Online]. Available: https://www.opm.gov/cybersecurity/cybersecurity-incidents/. [Accessed 8 10 2020].

[11] S. Romanosky, "Examining the costs and causes of cyber incidents," *Journal of CyberSecurity,* vol. 0, no. 0, pp. 1-15, 2016.

[12] A. Haizler, "The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking," *Cyber, Intelligence, and Security,* vol. 1, no. 1, pp. 31-45, 2017.

[13] Center for Strategic & International Studies, "Significant Cyber Incidents Since 2006," 2020.

[14] Stilgherrian, "Secret F-35, P-8, C-130 data stolen in Australian defense contractor hack," zdnet.com, 11 October 2017. [Online]. Available: https://www.zdnet.com/article/secret-f-35-p-8-c-130-data-stolen-in-australian-defence-contractor-hack/. [Accessed 20 November 2020].

Smartphone Security Model and Vulnerabilities

CS559 : Quantitative Security

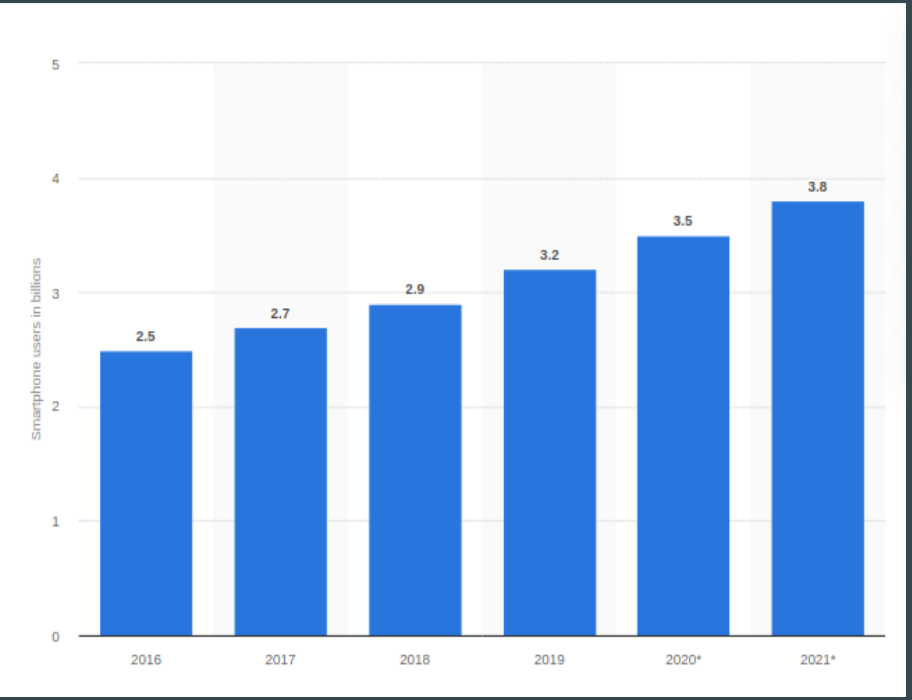
Shree Harini Ravichandran

Outline

- Introduction
- Literature Review
- Smartphone Security Threats
- Smartphone Security Model: iOS, Android, Windows, Blackberry
- Smartphone Market Share
- Smartphone Vulnerabilities

Introduction

- Improvement from a basic and feature phone
- Combines cellular features and computations
- Smartphone users in 2020 is 3.5 billion



Source: Statista

Literature Review

- Milad et al [7], review the security in different operating systems, threats and vulnerabilities in smartphones

- Chuanxiong Guo et al [8], in their paper discuss how smartphone attacks take place and how to defend them
  - Attacks: Compromise of smartphones and smartphone attacks against the telecommunication networks
  - Defense mechanisms: Smartphone hardening, protection features from the internet and protection services

- Mohamed et al [9], primarily discuss the factors influencing the security in Android and iOS devices
  - iOS reports more vulnerabilities than android
  - malware attacks are more in Android than in iOS

Smartphone Security Threats

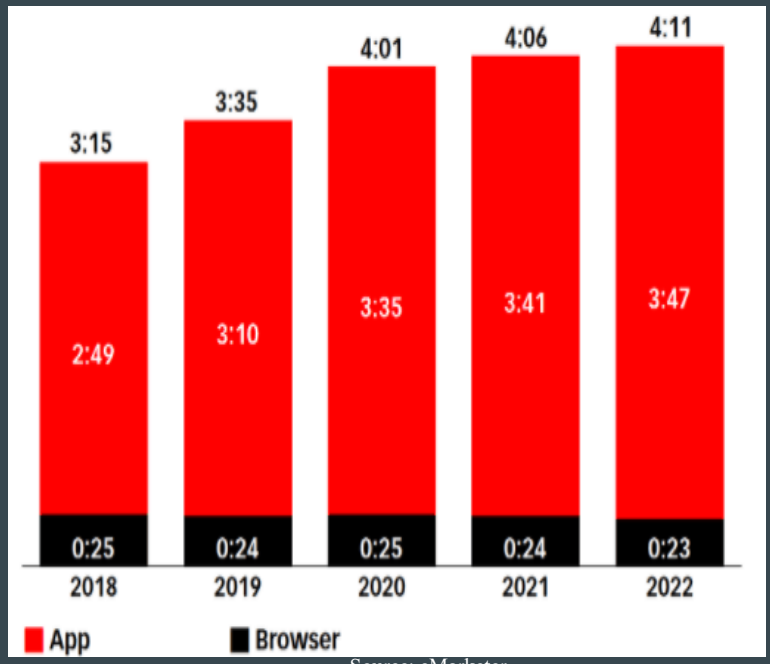
- User
- Applications
- Device
- Network

1. Users

- First point of security
- Attacks:
  - Phishing: Fraudulent attempt to obtain sensitive information or data
  - URL Obfustication: Legitimate web location is modified to conceal and obtain information
  - Homograph attack: Domain name is changed slightly and a malicious site is developed

2. Applications

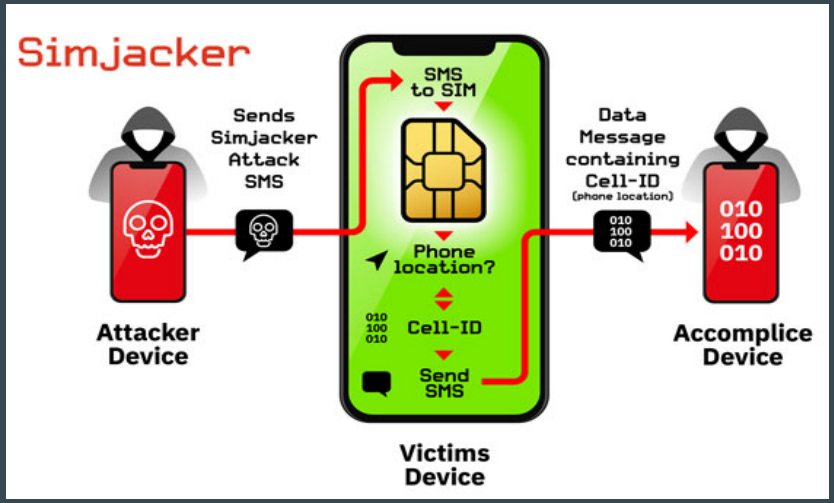
- Most widely used and spent time on everyday
- Attacks:
  - Malware: Hidden in applications
  - Sideloading: Happens when apps are installed from places other than official app store



Source: eMarketer

3. Devices

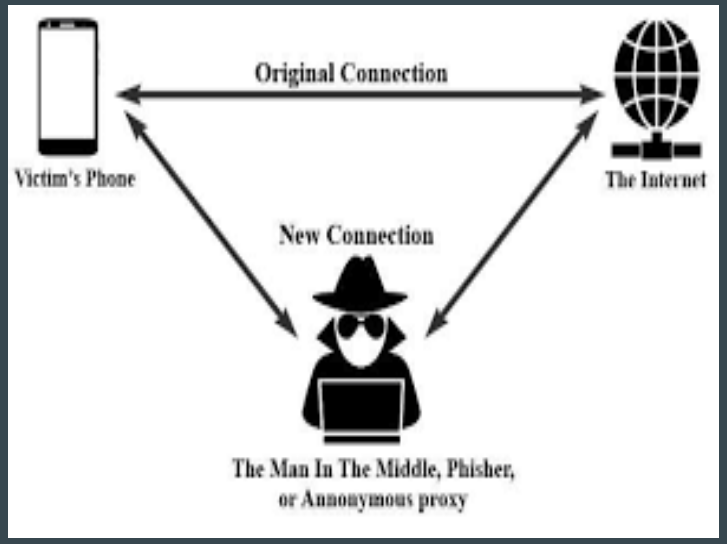
- Most of the attacks on devices do not require physical access to the devices
- Attacks:
    - SIM-jacking: Perpetrators get personal information from social media or persuade victims to tell



Source: thehackernews.com

4. Network

- Similar to attacks in IOT applications
- Attacks:
  - Man - in - the middle attack (MITM): Can happen through public WiFis
  - MITM Types: IP, DNS, ARP, Https Spoofing, SSL hijacking, stealing browser cookies and WiFi eavesdropping



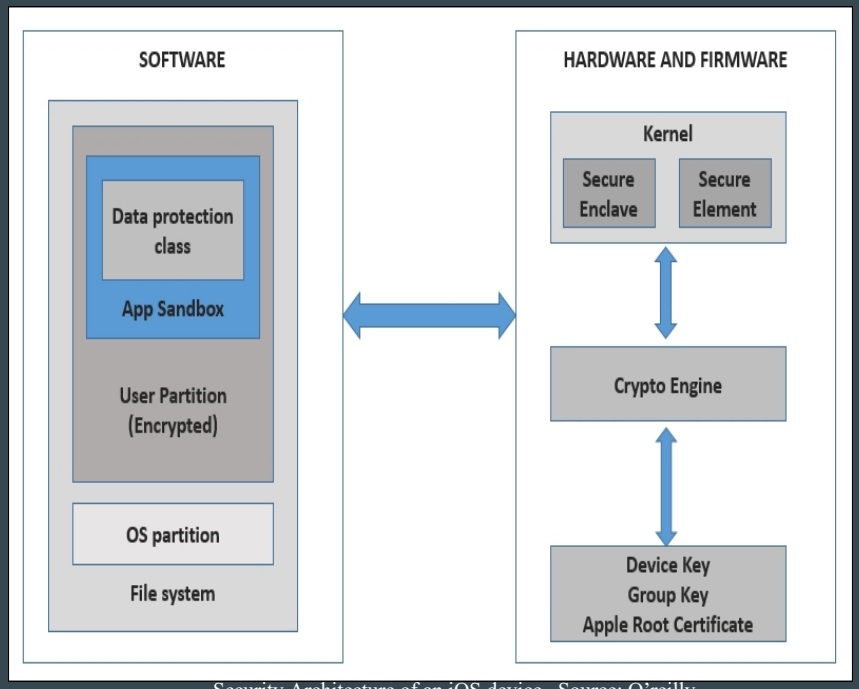
Source: Google Images

Smartphone Security Model

- iOS
- Android
- Windows
- Blackberry

iOS

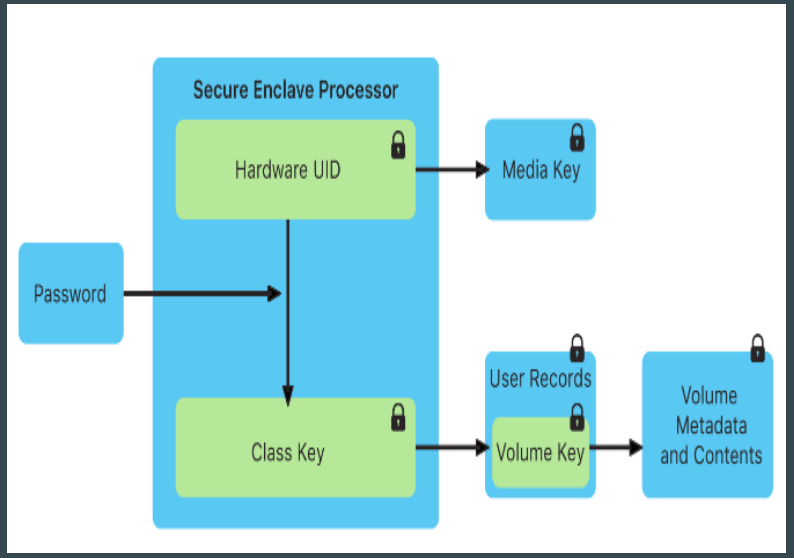
- Known for their security features and quality assurance
- Device security: Prevents unauthorized access to the device
- Data security: Protects the data present in the device Network security includes networking protocols and encryption techniques
- Application security: Includes many protective layers to protect from malware attacks



Security Architecture of an iOS device. Source: O'reilly

iOS

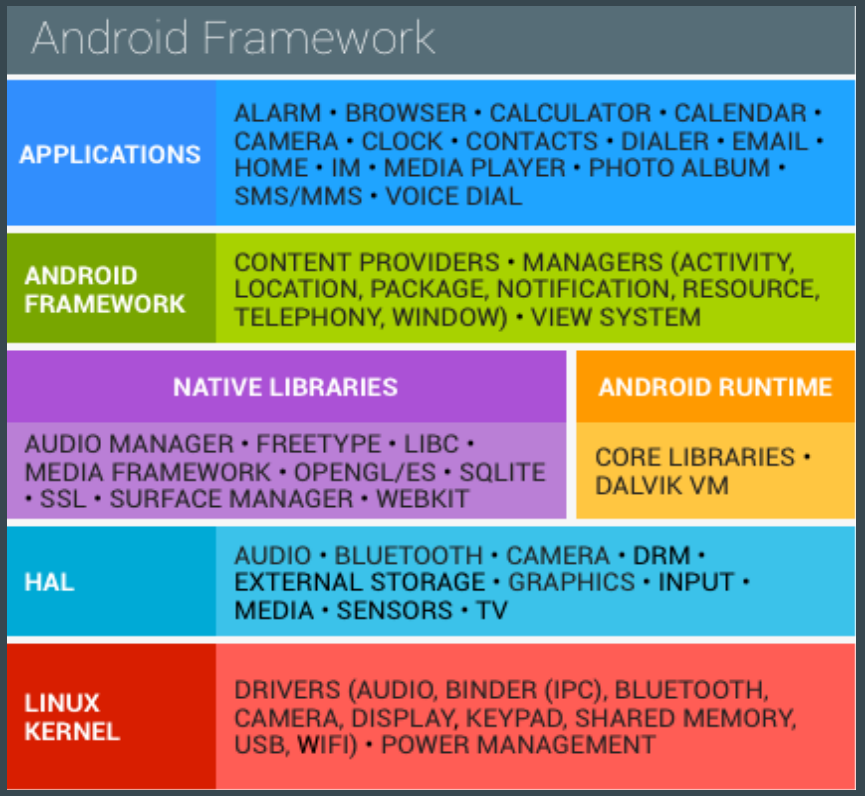
- T2 chip and an AES hardware engine to power encryption as files are written or read
- Special co-processor: Allows Touch and Face ID to provide secure authentication and keeps the biometric data secure
- iOS sandboxing: Protects the data and prevents accessing of this data from one application to another



Secure Enclave Processor on Apple Devices, Source: Apple

Android

- Open source
- Security components have to be considered for various levels in the android software stack
- Mainly based on permissions and sandbox



Android Software Stack, Source: Android.com

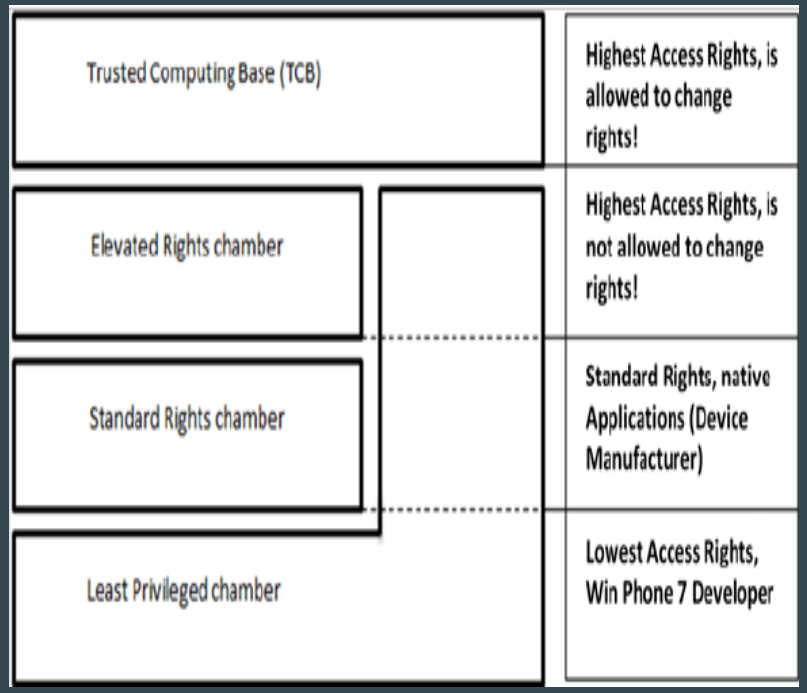
Android

Security Features:

- Linux kernel: Process isolation, user based permission model and interprocess communication
- Android sandboxing: Prevent interaction of malicious programs with applications that are protected
- Android OS: Implements user ID for application access control
- To secure the data: Includes security library that allows two classes of data encryption

Windows

- Four categories: chambers, capabilities, sandbox and application deployment
- Chambers: Trusted Computer Base (TCB), Elevated Rights Chamber(ERC), Standard Rights Chamber(SRC) and Least Privileged Chamber (LPC)
- Capabilities: GPS support, camera, microphone, WiFi and Bluetooth access
- Along with the chambers, applications also get sandboxed when it is running



Chambers of the Windows Phone 7 security model

Windows

Windows Phone 8.1 Security Features:

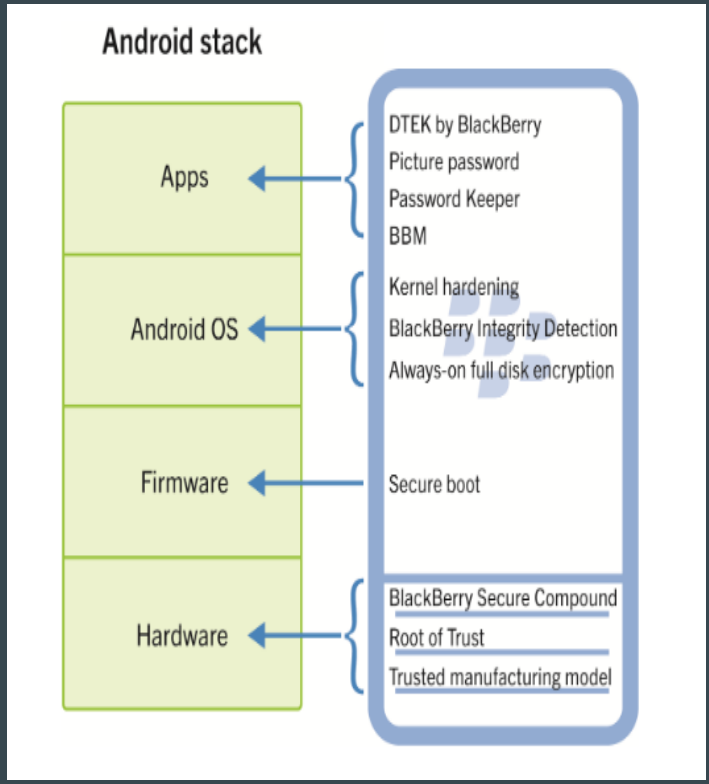
- Encryption of applications
- Malware resistance
- Address space layout randomization

Windows 10 Mobile Security Features::

- Identity access and control, Data protection, Malware resistance, Application platform security
- Windows Hello: Incorporates multi factor authentication
- Bitlocker technology for encryption purposes

Blackberry

- Blackberry Secure Integrated Manufacturing services, Blackberry Secure Identity Services
- Blackberry Integrity Detection monitors the events which could lead to compromise
- Address space layout randomization: Prevents exploitation of device memory corruption
- Linux kernel is hardered with security patches

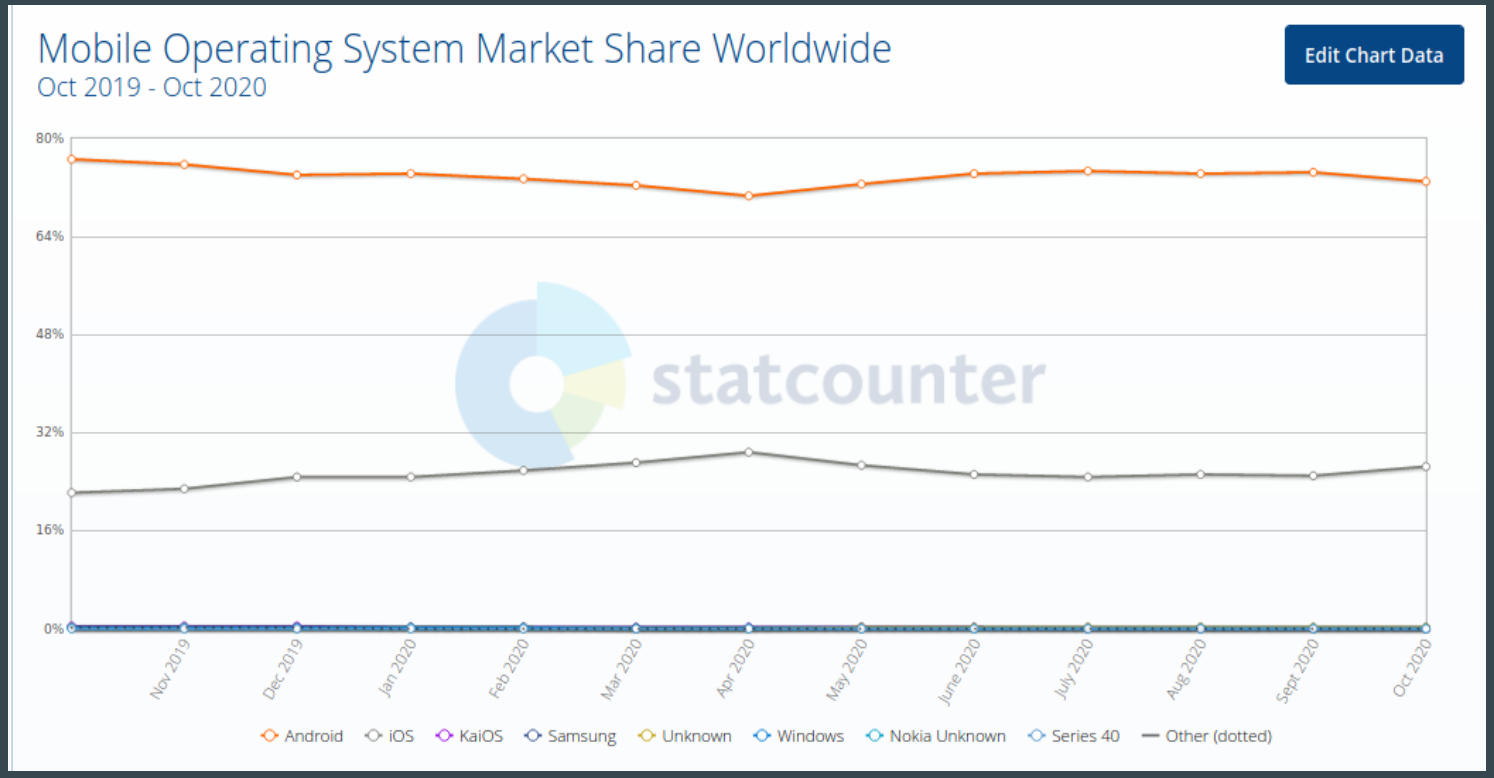


Blackberry Security Model

Blackberry

- Supports picture passwords - helps in addressing brute force attacks
- DTEK by Blackberry analyses and evaluates security features set up in the phone and assigns an overall security rating
- Password keeper feature stores passwords, usernames and security questions

Smartphone Market Share

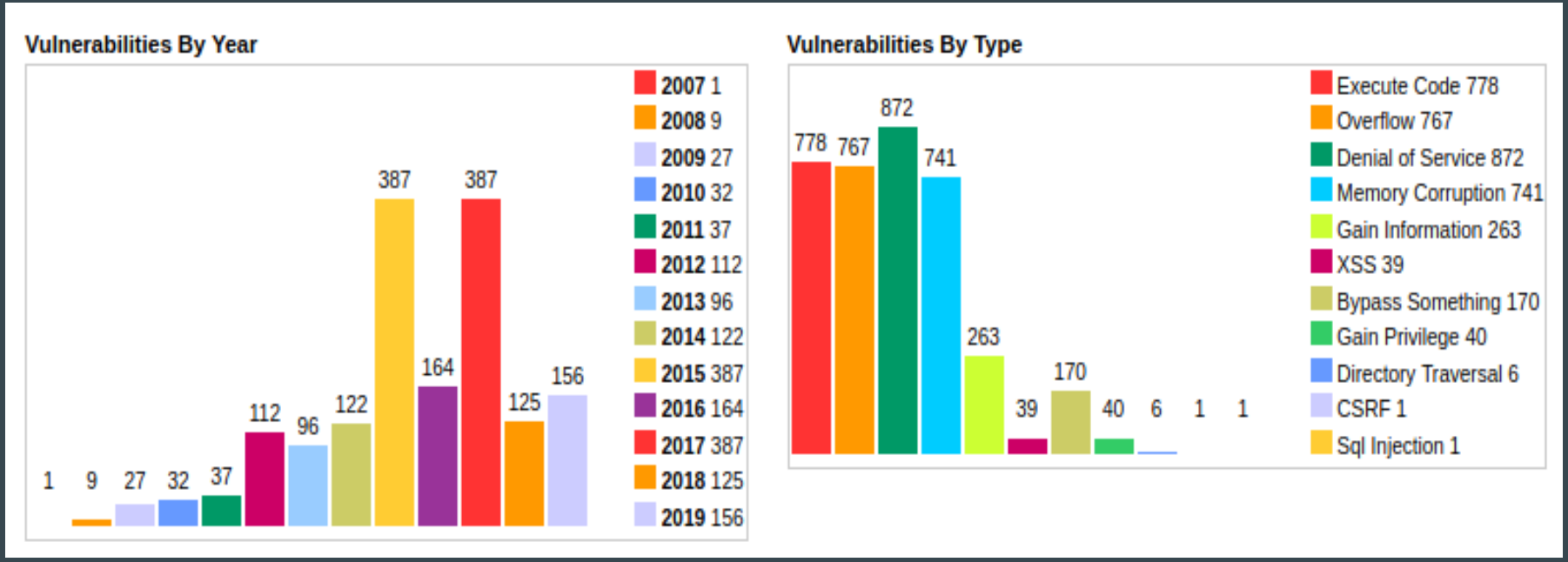


Source: Statcounter

Android VS iOS

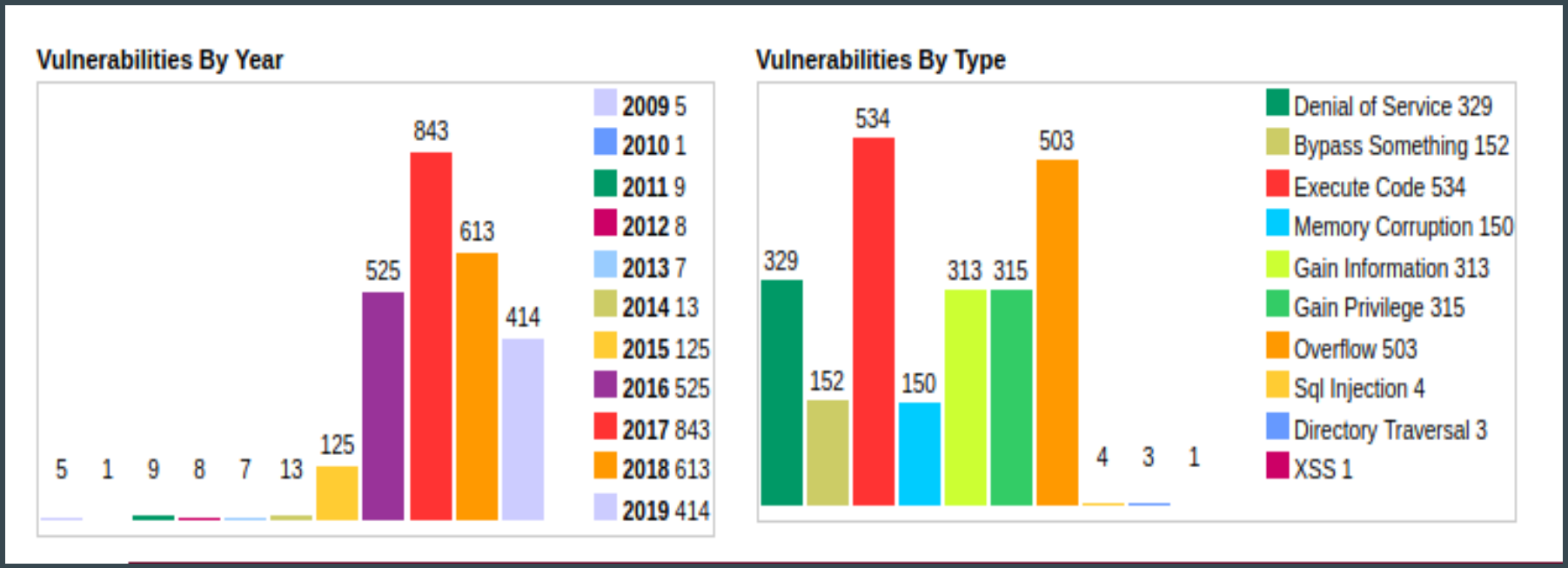
Region	Android	iOS
Africa	86.74%	10.66%
Asia	83.24%	16.17%
Europe	67.81%	31.77%
North America	46.06%	53.73%
South America	87.59%	12.14%
Oceania	48.13%	51.49%

Smartphone Vulnerabilities - iOS



Source: CVE details

Smartphone Vulnerabilities - Android



Source: CVE details

References

1. Accessed on: Oct, 09, 2020 [Online]. Available: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/
2. Y. Wang, K. Streff and S. Raman, "Smartphone Security Challenges," in Computer, vol. 45, no. 12, pp. 52-58, Dec. 2012, doi: 10.1109/MC.2012.288.
3. Y. Wang, C. Hahn and K. Sutrave, "Mobile payment security, threats, and challenges," 2016 Second International Conference on Mobile and Secure Services (MobiSecServ), Gainesville, FL, 2016, pp. 1-5, doi: 10.1109/MOBISECSERV.2016.7440226.
4. Debnath, Biswajit and Das, Sanchari and Das, Ankita, Study Exploring Security Threats in Waste Phones a Life Cycle Based Approach (August 19, 2019). In 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation. IEEE., Available at SSRN: https://ssrn.com/abstract=3443923
5. Accessed on: Nov, 06, 2020 [Online]. Available: https://usa.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store
1. Sharma K., Gupta B.B. (2018) Attack in Smartphone Wi-Fi Access Channel: State of the Art, Current Issues, and Challenges. In: Lobiyal D., Mansotra V., Singh U. (eds) Next-Generation Networks. Advances in Intelligent Systems and Computing, vol 638. Springer, Singapore. https://doi.org/10.1007/978-981-10-6005-2_56
2. Taleby Ahvanooey, Milad & Li, Qianmu & Rabbani, Mahdi & Rajput, Ahmed. (2017). A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks. International Journal of Advanced Computer Science and Applications. 8. 30-. 10.14569/IJACSA.2017.081005.
3. Guo, Chuanxiong, Helen J. Wang, and Wenwu Zhu. "Smart-phone attacks and defenses." In hotnets III. 2004.
4. I. Mohamed and D. Patel, "Android vs iOS Security: A Comparative Study," 2015 12th International Conference on Information Technology - New Generations, Las Vegas, NV, 2015, pp. 725-730, doi: 10.1109/ITNG.2015.123.
5. Shabtai, A. & Fledel, Y. & Kanonov, U. & Elovici, Yuval & Dolev, Shlomi. (2009). Google Android: A State-of-the-Art Review of Security Mechanisms. Neural Networks. abs/0912.5.
6. Accessed on: Nov 08, 2020 [Online]. Available: https://support.apple.com/guide/security/welcome/web
7. Accessed on: Nov 08, 2020 [Online]. Available: https://enterprise.verizon.com/resources/reports/mobile-security-index/
8. Haber, Morey J. "Attack Vectors." In Privileged Attack Vectors, pp. 65-85. Apress, Berkeley, CA, 2020.
9. Francis L., Hancke G., Mayes K., Markantonakis K. (2010) Practical NFC Peer-to-Peer Relay Attack Using Mobile Phones. In: Ors Yalcin S.B. (eds) Radio Frequency Identification: Security and Privacy Issues. RFIDSec 2010. Lecture Notes in Computer Science, vol 6370. Springer, Berlin, Heidelberg.