Quantitative Cyber-Security

Colorado State University

Yashwant K Malaiya

CS559

L28: Presentations

CSU Cybersecurity Center
Computer Science Dept

Presentations Evaluations, Report Reviews

- Everyone: fill the peer-review form for presentations and submit through canvas (Due Dec 10 Th). Evaluate
  a. Significance & originality
  b. Thoroughness & timeliness of research
  c. Depth of understanding displayed
  d. Organization & Presentation
  e. Overall

Evaluation	Score
Top 25%	10
Next 25%	9
Next 25%	8
Lowest 25%	7

- Final: is two part
  - Final A: critical 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 8, 2020

- Zhao, Qingyi. Quantitative examination of phishing
- Petkar, Jayesh Umesh. Smartphone Security Model and Vulnerabilities
- Alqurashi, Saja. Statical analysis of Mitre ATT&CK for Industrial Control System
- Li, Jacinda. Security Performance Analysis of Electronic Payment Systems
- Dubois, Alexandre. Economic tradeoffs due to security issues
- Chen, Sirius. Secure container Technologies

Th Dec 10 (participation required)

- Shang, Tony. Detection DDOS attack based on deep neural networks (will be moved)

Quantitative Examination of Phishing

Qingyi Zhao

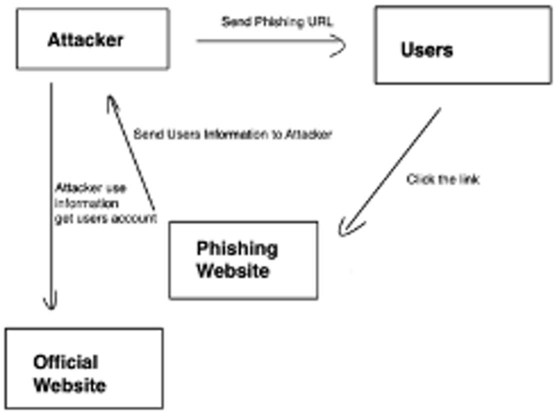
Colorado State University

Outline

- Introduction & Motivation
- Background Research
- Research Result & Future Research
- References

Introduction

What is phishing? Take a phishing website as an example: the attacker prepares a webpage that imitates the official website in advance and fails to send it to the server to make the webpage accessible, and sets up a channel for transmitting user information. Induce users to phishing web pages through emails, text messages, or hiding links in other web pages. After the user fills in the personal information and clicks the "Submit" button, the data is sent to the location designated by the attacker for storage. The following figure shows the flow of this series of attacks.


Attacker
Send Phishing URL
Users
Send Users Information to Attacker
Click the link
Attacker use information get users account
Phishing Website
Official Website

The more tired the phishing attack the more common.

This kind of attack is getting worse and causing great losses.

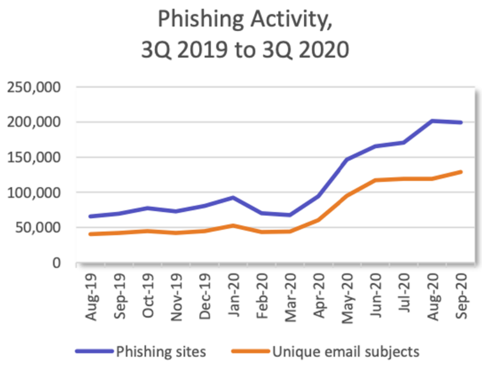
My personal experience.

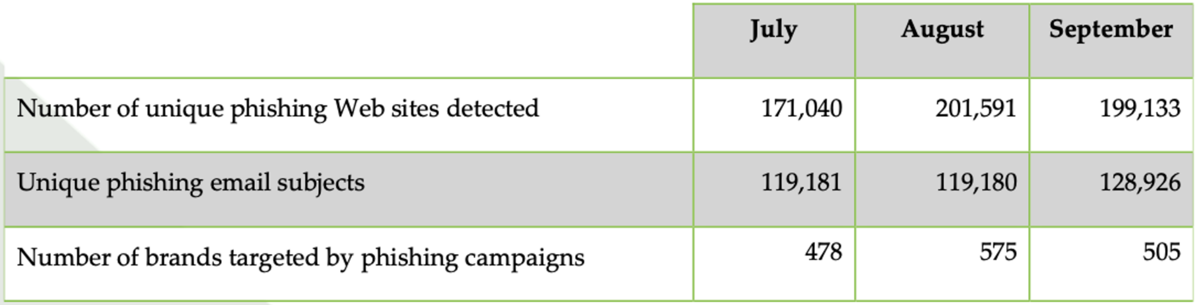
Report of Phishing

Phishing Activity Trends Summary

The more tired the phishing attack the more common.

Phishing Attacks Rise in the Third Quarter of 2020



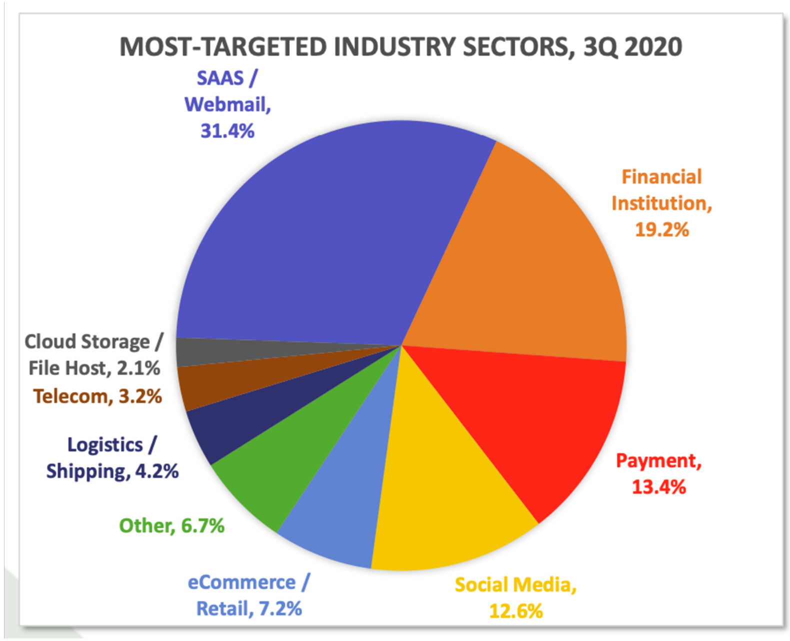


	July	August	September
Number of unique phishing Web sites detected	171,040	201,591	199,133
Unique phishing email subjects	119,181	119,180	128,926
Number of brands targeted by phishing campaigns	478	575	505

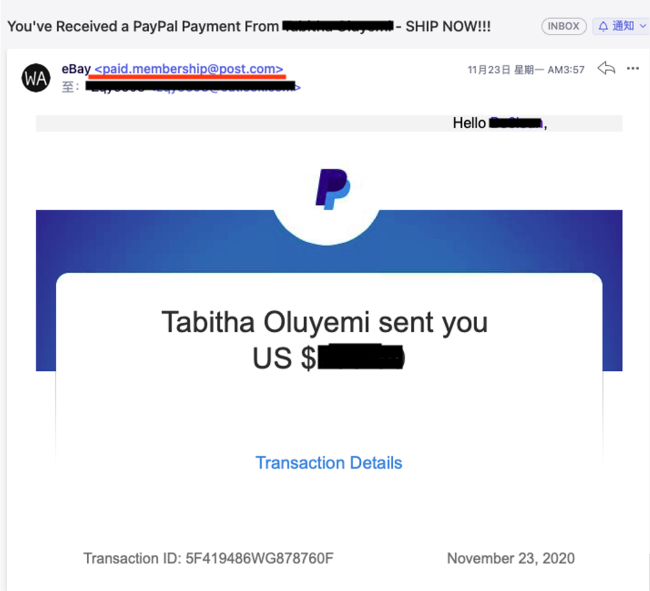
Report of Phishing (Cont.)

SaaS and webmail sites remained the most frequent targets of phishing.

Phishing against social media companies crept up from 10.8 to 12.6 percent.



Phishing attacks I encountered



You've Received a PayPal Payment From [redacted] - SHIP NOW!!!

eBay <paid.membership@post.com>

至： [redacted]

11月23日 星期一 AM3:57

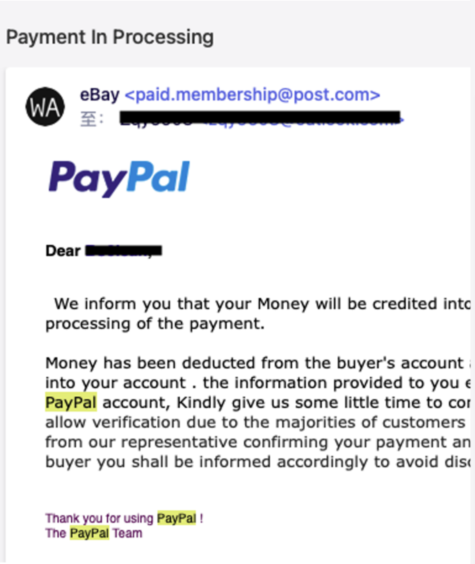
Hello [redacted],

Tabitha Oluyemi sent you US $[redacted]

Transaction Details

Transaction ID: 5F419486WG878760F

November 23, 2020



Payment In Processing

eBay <paid.membership@post.com>

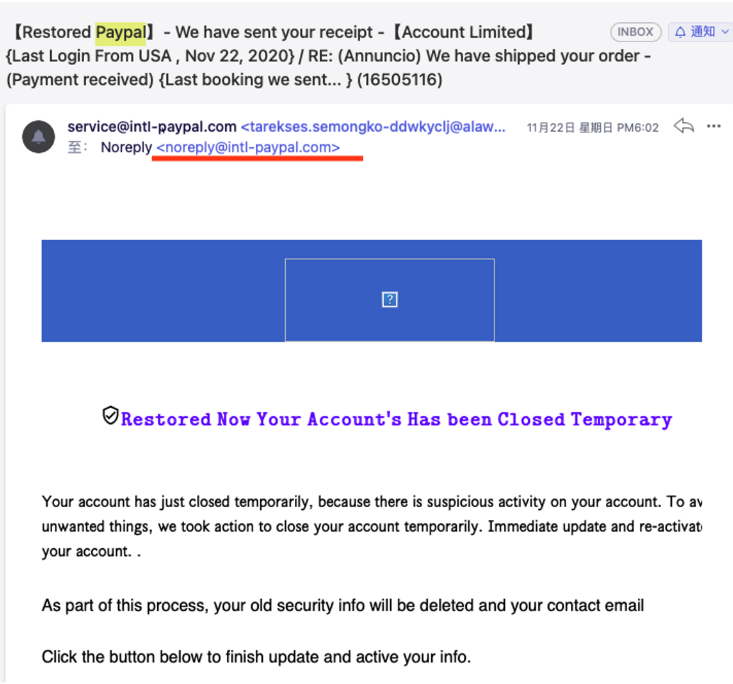
至： [redacted]

Dear [redacted]

We inform you that your Money will be credited into processing of the payment.

Money has been deducted from the buyer's account into your account . the information provided to you e PayPal account, Kindly give us some little time to cor allow verification due to the majorities of customers from our representative confirming your payment an buyer you shall be informed accordingly to avoid disc

Thank you for using PayPal !
The PayPal Team



【Restored Paypal】 - We have sent your receipt - 【Account Limited】 {Last Login From USA , Nov 22, 2020} / RE: (Annuncio) We have shipped your order - (Payment received) {Last booking we sent... } (16505116)

service@intl-paypal.com <tarekses.semongko-ddwkyclj@alaw...

至： Noreply <noreply@intl-paypal.com>

11月22日 星期日 PM6:02

Restored Now Your Account's Has been Closed Temporary

Your account has just closed temporarily, because there is suspicious activity on your account. To av unwanted things, we took action to close your account temporarily. Immediate update and re-activat your account. .

As part of this process, your old security info will be deleted and your contact email

Click the button below to finish update and active your info.

Academic research on anti-phishing

Su, K., Wu, K., Lee, H. and Wei, T, identify phishing URLs based on linear regression.

Afroz, S. And Greenstadt, R. designed a detection method called PhishZoo.

Sahingoz, O., Buber, E., Demir, O. and Diri, B., 2019. Machine learning based phishing detection from URLs.

There are many other studies.

Identifying that it is a phishing website

1. The browser compares the currently visited URL and database to match the page of the suspected phishing website.

2. Page text and picture feature recognition.

3. Identification of domain name registration information.

4. The website is registered and recognized by the government.

5. PageRank level recognition based on page change frequency.

Identify phishing URLs based on linear regression

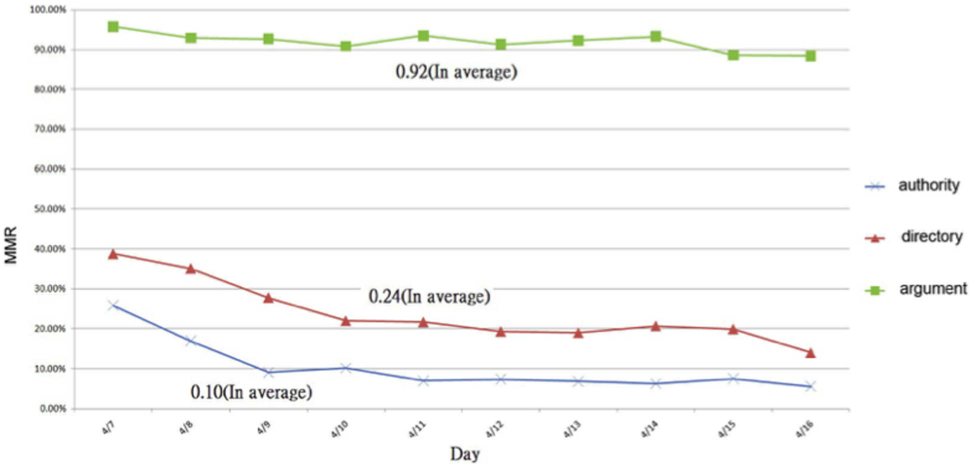
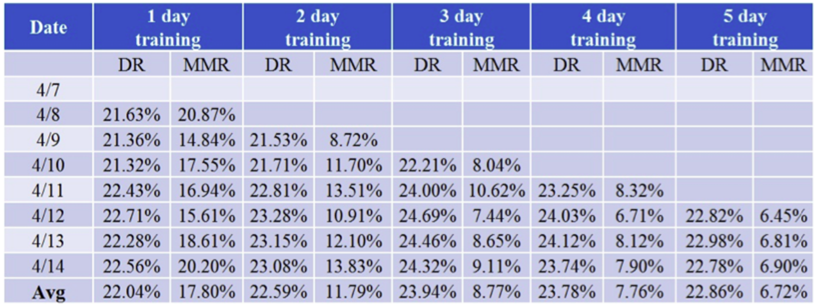


Figure 1. The malicious missing rate in different views.

Su, K., Wu, K., Lee, H. and Wei, T., 2013. Suspicious URL Filtering Based on Logistic Regression with Multi-view Analysis. 2013 Eighth Asia Joint Conference on Information Security.



Date	1 day training		2 day training		3 day training		4 day training		5 day training	
	DR	MMR	DR	MMR	DR	MMR	DR	MMR	DR	MMR
4/7										
4/8	21.63%	20.87%								
4/9	21.36%	14.84%	21.53%	8.72%						
4/10	21.32%	17.55%	21.71%	11.70%	22.21%	8.04%				
4/11	22.43%	16.94%	22.81%	13.51%	24.00%	10.62%	23.25%	8.32%		
4/12	22.71%	15.61%	23.28%	10.91%	24.69%	7.44%	24.03%	6.71%	22.82%	6.45%
4/13	22.28%	18.61%	23.15%	12.10%	24.46%	8.65%	24.12%	8.12%	22.98%	6.81%
4/14	22.56%	20.20%	23.08%	13.83%	24.32%	9.11%	23.74%	7.90%	22.78%	6.90%
Avg	22.04%	17.80%	22.59%	11.79%	23.94%	8.77%	23.78%	7.76%	22.86%	6.72%

Figure 2. The result with T. Co. request experiments. It shows the result that our process can satisfy the DR and MMR requests.

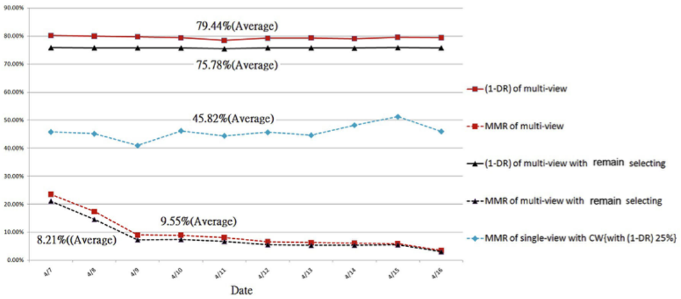
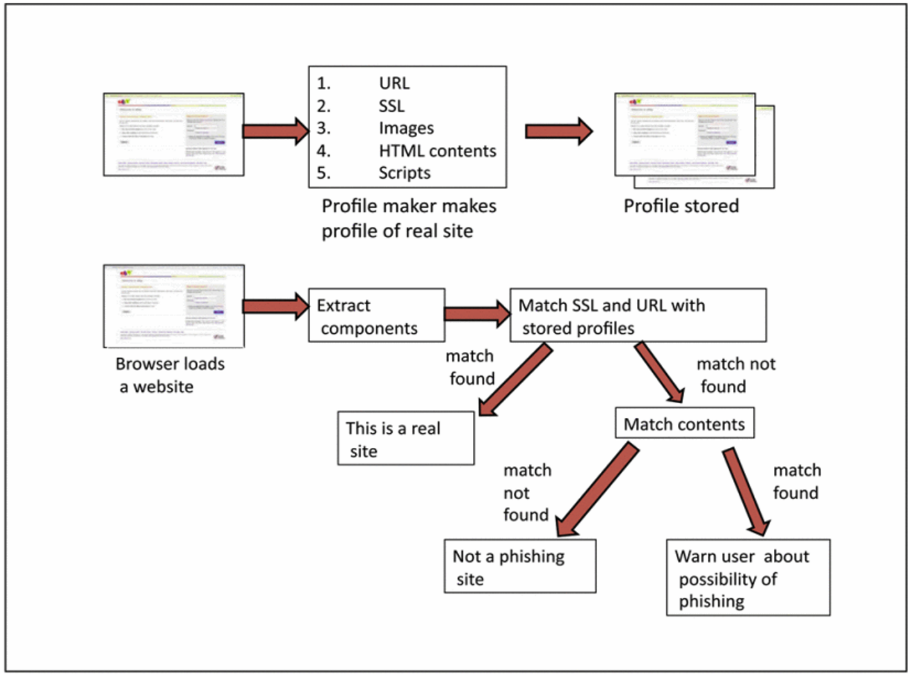


Figure 3. The results with continuous learning. It include multi-view, multi-view with remain selecting and single-view with confidence weighted.

Afroz, S. And Greenstadt, R. designed a detection method called PhishZoo.

Afroz, S. and Greenstadt, R., 2011. PhishZoo: Detecting Phishing Websites by Looking at Them. 2011 IEEE Fifth International Conference on Semantic Computing.



1. URL
2. SSL
3. Images
4. HTML contents
5. Scripts

Profile maker makes profile of real site

Profile stored

Browser loads a website

Extract components

Match SSL and URL with stored profiles

match found

This is a real site

match not found

Match contents

match not found

Not a phishing site

match found

Warn user about possibility of phishing

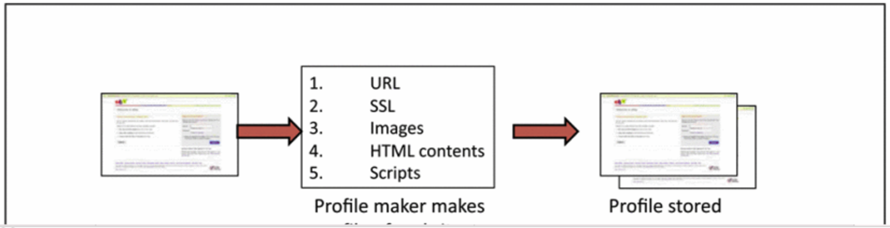
Afroz, S. And Greenstadt, R. designed a detection method called PhishZoo.

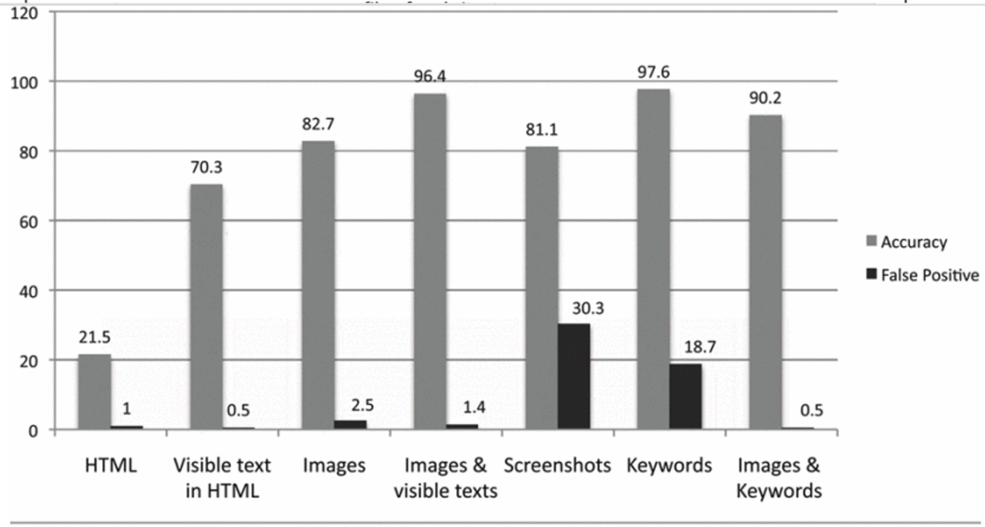
90.2% of phishing sites were detected through keyword and image matching.

PhishZoo will detect 97.6% of phishing sites.

21.5% of phishing sites directly reuse elements of the actual site and can be detected through HTML code matching.

By considering only the visible text of the website instead of the entire HTML, 70.3% of phishing can be detected.

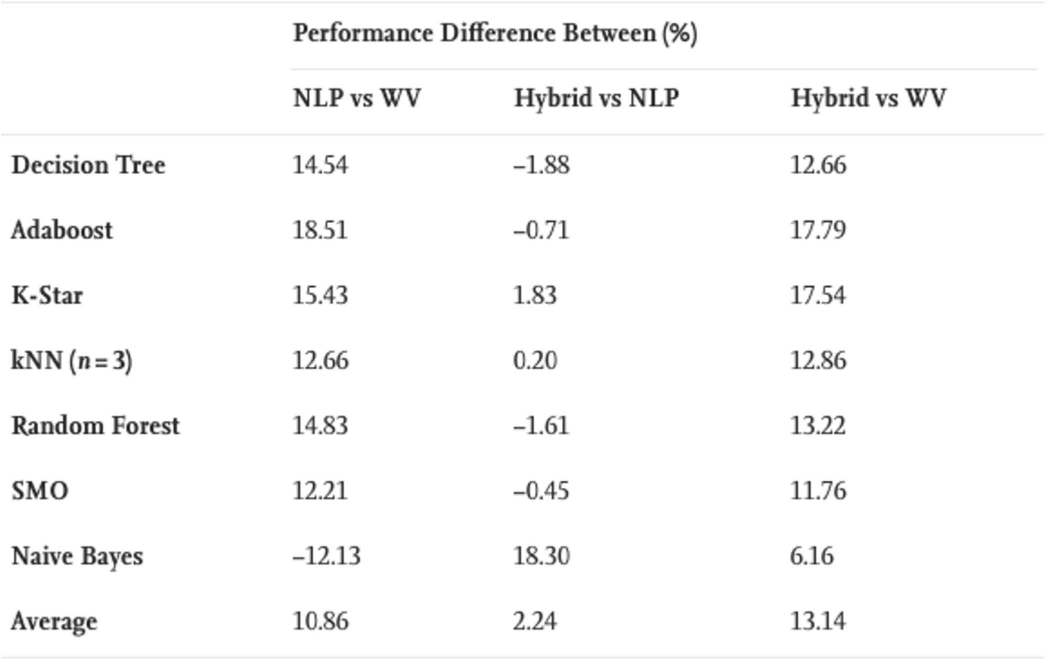




Machine learning based phishing detection from URLs.

According to the experimental results, it can be clearly seen that NLP-based functions have better performance than word vectors, with an average rate of 10.86%. In addition, using NLP-based features and word vectors together can also improve the performance of the phishing detection system. According to NLP-based features, the ratio is 2.24%, and for word vectors, it is 13.14%.

Sahingoz, O., Buber, E., Demir, O. and Diri, B., 2019. Machine learning based phishing detection from URLs.



	Performance Difference Between (%)		
	NLP vs WV	Hybrid vs NLP	Hybrid vs WV
Decision Tree	14.54	–1.88	12.66
Adaboost	18.51	–0.71	17.79
K-Star	15.43	1.83	17.54
kNN (*n* = 3)	12.66	0.20	12.86
Random Forest	14.83	–1.61	13.22
SMO	12.21	–0.45	11.76
Naive Bayes	–12.13	18.30	6.16
Average	10.86	2.24	13.14

Conclusion

Based on previous surveys, combined with reports issued by professional organizations. Phishing attacks are becoming more and more common. Among them, email phishing attacks are a very common form of attack by attackers. Because this attack method is more proactive. Actively send phishing emails to users to trick users into clicking links to enter the website. Compared with this method, the method of creating phishing websites and hiding links in other websites is not very effective. The attacker obtains the user's recent activities through public information on the Internet or in some way, and then sends targeted phishing emails. Since users have had the same activity recently, they are more likely to be deceived. Using machine learning to identify and classify phishing websites is a very efficient way. Many researchers are using this method to design a fan fishing system.

References

[1] Apwg.org. 2020. APWG — Unifying The Global Response To Cybercrime. [online] Available at: ¡https://apwg.org¿ [Accessed 7 September 2020].

[2] Su, K., Wu, K., Lee, H. and Wei, T., 2013. Suspicious URL Filtering Based on Logistic Regression with Multi-view Analysis. 2013 Eighth Asia Joint Conference on Information Security.

[3] Afroz, S. and Greenstadt, R., 2011. PhishZoo: Detecting Phishing Websites by Looking at Them. 2011 IEEE Fifth International Conference on Semantic Computing.

[4] Layton, R., Brown, S. and Watters, P., 2009. Using Differencing to Increase Distinctiveness for Phishing Website Clustering. 2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing,.

[5] Shirazi, H., Haefner, K. and Ray, I., 2017. Fresh-Phish: A Framework for Auto-Detection of Phishing Websites. 2017 IEEE International Conference on Information Reuse and Integration (IRI),.

References (Cont.)

[6] Shahriar, H. and Zulkernine, M., 2011. Information Source-Based Classification of Automatic Phishing Website Detectors. 2011 IEEE/IPSJ International Symposium on Applications and the Internet,.

[7] Sjouwerman, S., 2020. This Year, Phishing Causes Losses Of 17, 700PerMinuteAndRansomwareAttacksWillCost22,184 Per Minute. [online] Blog.knowbe4.com. Available at: ¡https://blog.knowbe4.com/this-year-phishing-causes-losses-of-17700per-minute-and-ransomware-attacks-will-cost-22184-per-minute¿ [Accessed 10 October 2020].

[8] Sahingoz, O., Buber, E., Demir, O. and Diri, B., 2019. Machine learning based phishing detection from URLs. Expert Systems with Applications, 117, pp.345-357.

Thank you

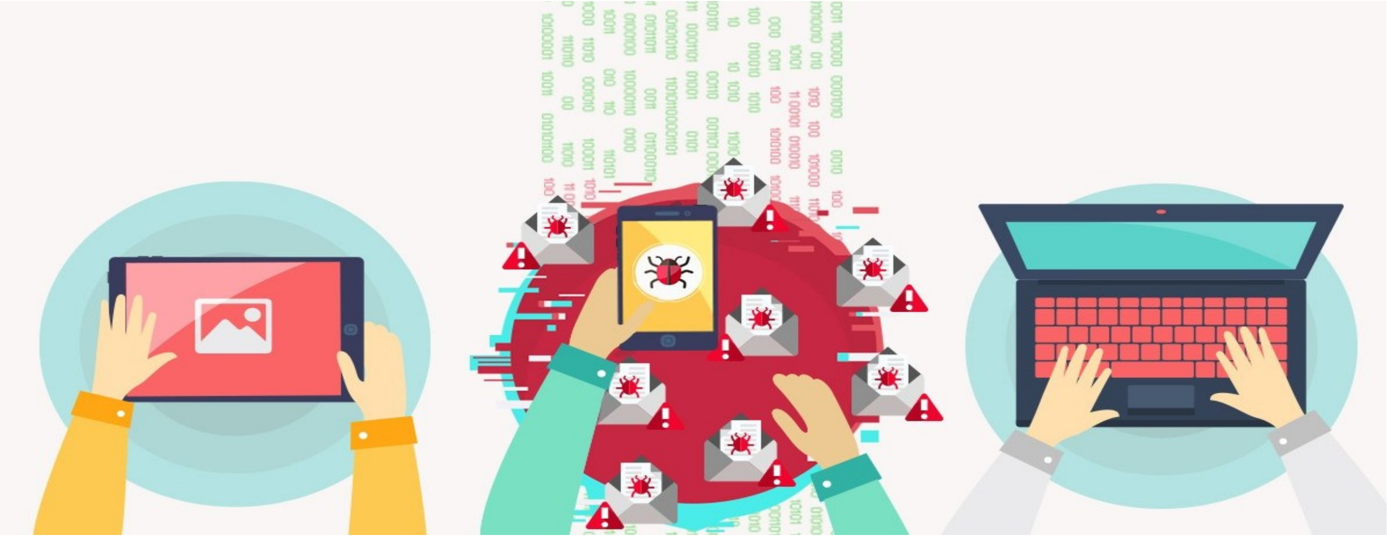
Colorado State University

SMARTPHONE SECURITY AND VULNERABILITIES

Jayesh Umesh Petkar
CS 559

INTRODUCTION

Why pay attention to mobile security?



RELATED WORK

- **Android smartphone vulnerabilities: A survey [1]**
- **A survey on security issues, vulnerabilities and attacks in Android based smartphone [2]**
- **A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks [3]**
- **A Markov adversary model to detect vulnerable iOS devices and vulnerabilities in iOS apps [4]**

TOP SECURITY THREATS FOR APPS

Improper Platform Usage: Maltreat of features of the phone or OS like giving app permissions to access contacts, gallery etc., beyond a need.

- **Superfluous Data Storage:** Storing unwanted data in the app.

Exposed Authentication: Failing to identify the user, failing to maintain the user’s identity and failing to maintain the user session.

- **Insecure Communication:** Failing to keep a correct SSL session.

Malicious Third-Party Code: Writing a third-party code which is not needed or not removing unnecessary code.

- **Failure to apply server-side controls:** The server should authorize what data needs to be shown in the app?

Client-Side injection: This results in the injection of malicious code in the app.

- **Lack of data protection in transit:** Failure to encrypt the data when sending or receiving via web service etc.

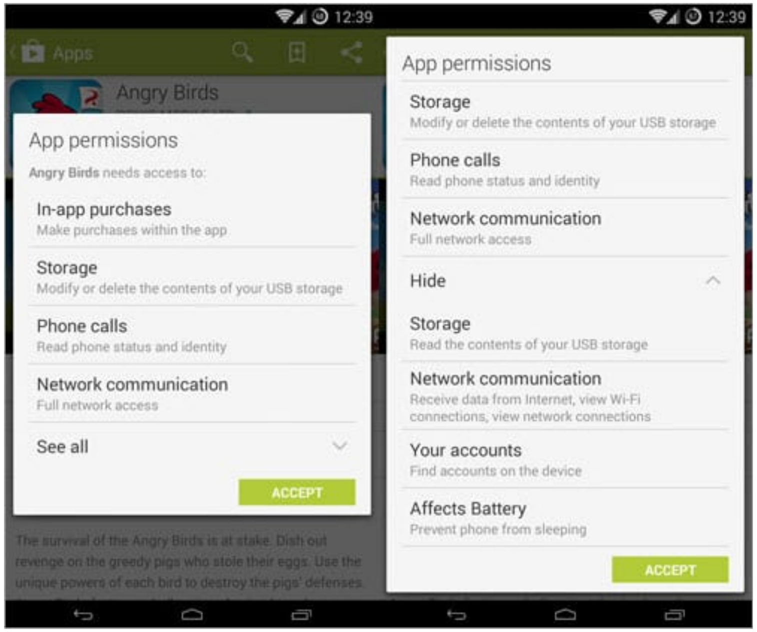
SECURITY THREAT FROM ROOTED AND JAILBROKEN PHONES

The installation of some extra applications on the phone.

The code used to root or jailbreak may have unsafe code, posing a threat of getting hacked.

These rooted/jailbreak phones are never tested by the manufacturers and hence they can behave in unpredictable ways.

SECURITY THREAT FROM APP PERMISSIONS



12:39

Apps

Angry Birds

App permissions

Angry Birds needs access to:

In-app purchases
Make purchases within the app

Storage
Modify or delete the contents of your USB storage

Phone calls
Read phone status and identity

Network communication
Full network access

See all

ACCEPT

The survival of the Angry Birds is at stake. Dish out revenge on the greedy pigs who stole their eggs. Use the unique powers of each bird to destroy the pigs' defenses.

12:39

App permissions

Storage
Modify or delete the contents of your USB storage

Phone calls
Read phone status and identity

Network communication
Full network access

Hide

Storage
Read the contents of your USB storage

Network communication
Receive data from Internet, view Wi-Fi connections, view network connections

Your accounts
Find accounts on the device

Affects Battery
Prevent phone from sleeping

ACCEPT

Network-based Location

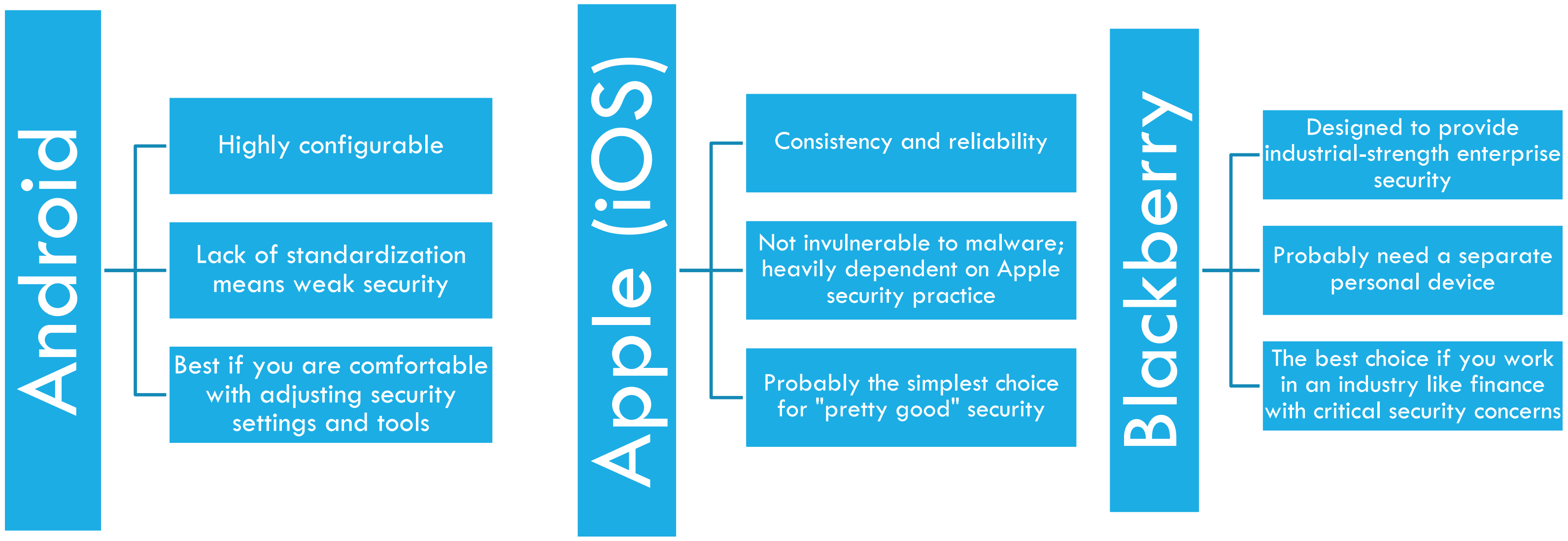
View the Wi-Fi state

Retrieving Running Apps

Full Internet Access

Automatically start on boot

ANDROID VS APPLE(IOS) VS BLACKBERRY



Android

- Highly configurable
- Lack of standardization means weak security
- Best if you are comfortable with adjusting security settings and tools

Apple (iOS)

- Consistency and reliability
- Not invulnerable to malware; heavily dependent on Apple security practice
- Probably the simplest choice for "pretty good" security

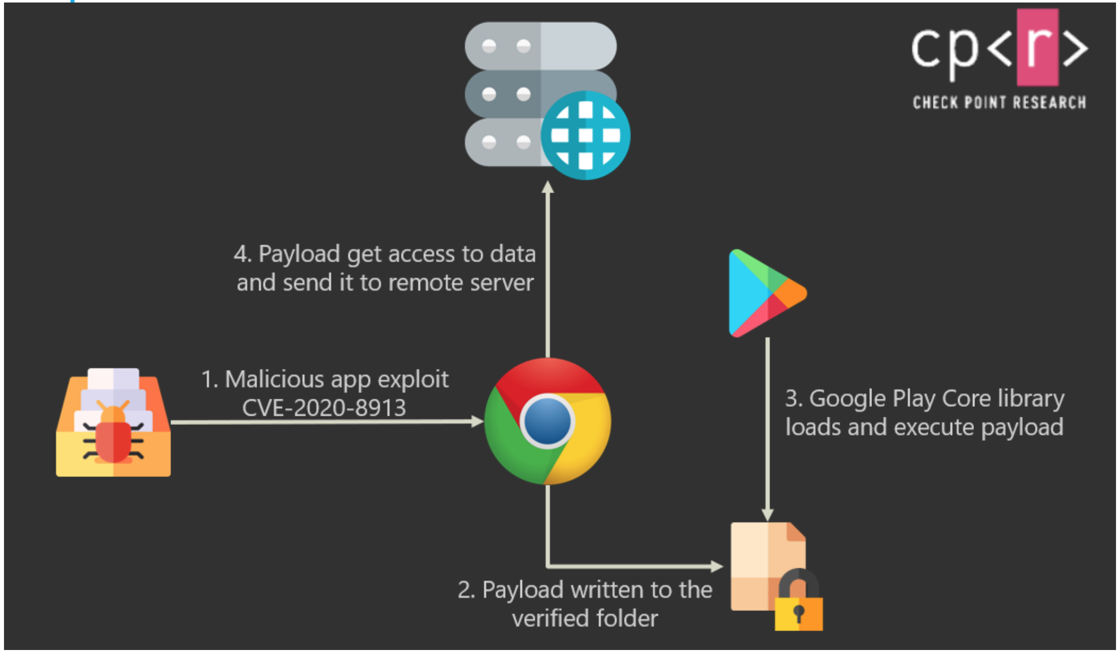
Blackberry

- Designed to provide industrial-strength enterprise security
- Probably need a separate personal device
- The best choice if you work in an industry like finance with critical security concerns

‘Scariest iPhone Hack Ever’ Illustrates Importance of Protecting Mobile Devices

CVE-2020-3848

- Discovered by Ian Beer.
- Causes memory corruption bug in iOS kernel.
- Gives remote access over Wi-Fi with no user interaction.
- Exploits were wormable.


cp<r>
CHECK POINT RESEARCH
4. Payload get access to data and send it to remote server
1. Malicious app exploit CVE-2020-8913
3. Google Play Core library loads and execute payload
2. Payload written to the verified folder

CVE-2020-8913

- Android Playstore Code Execution Flaw.
- Permits apps to interact with Google Playstore services
- Attackers can inject malicious code to steal bank credentials, two-factor authentication, spy on victims, steal messages, etc
- October 13th – 26643(about 8%) still vulnerable.

CONCLUDING REMARKS

- iOS is less susceptible to security threat when compared to Android.
- Apple iOS is a closed system and has very strict rules for app distribution on the iTunes store. Thus, the risk of malware or malicious apps reaching the iStore is reduced.
- Android is an open system with no strict rules or regulations of posting the app on the Google Play store.
- The apps are not verified before being posted.
- It takes a perfectly designed iOS malware to cause damage as much as 100 Android malware.

REFERENCES

[1]. Dataportal.com

[2]. Billions of devices vulnerable to new 'BLESA' Bluetooth security flaw. https://www.zdnet.com/article/billions-ofdevices-vulnerable-to-new-blesa-bluetoothsecurity-flaw/

[3]. Apple Patches Two iOS Zero-Days Abused for Years https://threatpost.com/apple-patches-two-ioszero-days-abused-for-years/155042/

[4]. The state of mobile app security in 2020 https://www.intertrust.com/blog/the-state-ofmobile-app-security-in-2020/

[5]. Mobile Security Vulnerabilities Are Creating Big Problems – Sean Cunningham. https://www.rsaconference.com/industrytopics/blog/mobile-security-vulnerabilities-arecreating-big-problems

[1] J. Joshi and C. Parekh, "Android smartphone vulnerabilities: A survey," *2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring)*, Dehradun, 2016, pp. 1-5, doi: 10.1109/ICACCA.2016.7578857

[2] J. B. Hur and J. A. Shamsi, "A survey on security issues, vulnerabilities and attacks in Android based smartphone," *2017 International Conference on Information and Communication Technologies (ICICT)*, Karachi, 2017, pp. 40-46, doi: 10.1109/ICICT.2017.8320163.

[3] arXiv:2001.09406

[4] Christian J. D'Orazio, Rongxing Lu, Kim-Kwang Raymond Choo, Athanasios V. Vasilakos, A Markov adversary model to detect vulnerable iOS devices and vulnerabilities in iOS apps, Applied Mathematics and Computation, Volume 293, 2017, Pages 523-544, ISSN 0096-3003

[5] Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret “Verkijika, Silas Formunyuy, Elsevier BV, Computers & security, 2018, Vol.77, p.860-870”

[6] Breitinger, Frank & Tully-Doyle, Ryan & Hassenfeldt, Courtney. (2019). A survey on smartphone user’s security choices, awareness and education. Computers & Security. 88. 101647.

[7] Yuan H, Tang Y, Sun W, Liu L (2020) A detection method for android application security based on TF-IDF and machine learning. PLoS ONE 15(9): e0238694.

[8] Amro, Belal. (2017). Malware Detection Techniques for Mobile Devices. nternational Journal of Mobile Network Communications & Telematics. 7.

[9] Mi, Tianyue & Gou, Mengke & Zhou, Guangyu & Gan, Yiqun & Schwarzer, Ralf. (2020). Effects of Planning and Action Control on Smartphone Security Behavior. Computers & Security. 97. 101954. 10.1016/j.cose.2020.101954.

Statistical Analysis of MITRE ATT&CK for Industrial Control Systems

Saja Alqurashi

CS559 Quantitative Security

Colorado State University

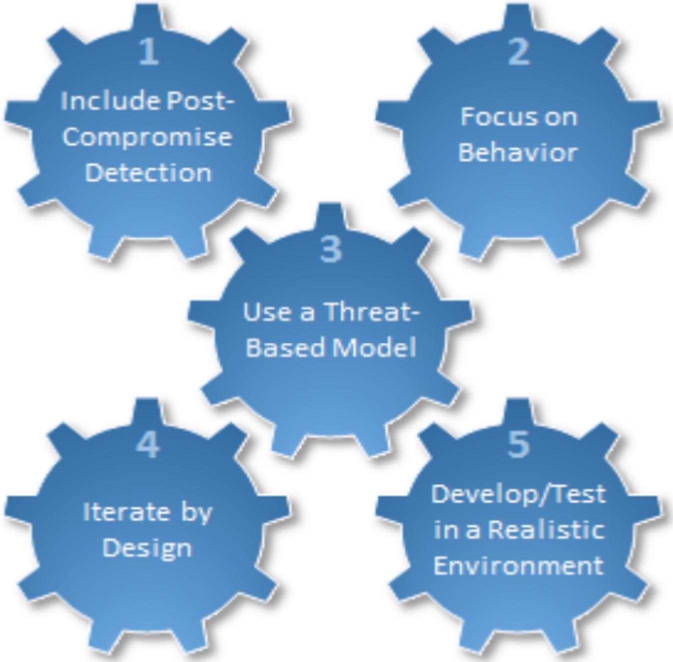
The Problem Statement

Studying how attackers can implement a technique using chains of tactics to accomplish their attack. Knowing the variety of ways (tactics) to complete malicious behavior helps security managers, such as those working in a security operation center (SOC) to apply appropriate defense mechanisms against each specific attack behavior

MITRE Approaches to Detect Advanced Persistent Threats APT

- **Threat-Based Security Approach**
- **ATT&CK Framework**

Threat-Based Security Approach


1
Include Post-Compromise Detection
2
Focus on Behavior
3
Use a Threat-Based Model
4
Iterate by Design
5
Develop/Test in a Realistic Environment

ATT&CK Framework

Mitre ATT&CK Matrices

1. Tactics
2. Techniques
3. Mitigation
4. Groups

Tactics

- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- **Execution**
- Collection
- Exfiltration
- Command and Control

Literature Review

Paper	The proposed Approach
Finding Cyber Threats with ATT&CK-Based Analytics [5]	proposed an approach that use MITRE ATT&CK framework to find related defensive sensors and build, test, and refine behavioral-based analytic detection capabilities using adversary emulation
Cyber Threat Dictionary Using MITRE ATT CK Matrix and NIST Cybersecurity Framework Mapping [12]	Proposed a tool called cyber thread dictionary. The main idea of this work is mapping Mitre ATT&CK with NIST framework
Automated Threat Report Classification over Multi-Source Data.[11]	proposed an approach that maps between attackers behaviors and APT in Mitre ATT&CK tactics and techniques

Contributions

- Analyzing the relation between chains of tactics and techniques.
- Creating a dataset contains chains tactics and many corresponding techniques that can be used for anomaly detection system in ICS.

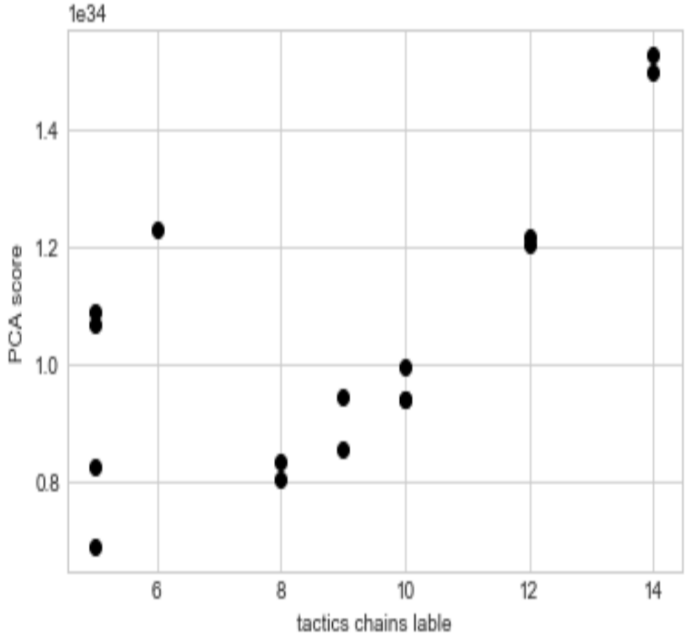
The proposed Approach

- The main objective in this research is studying the statistical correlation of chain of tactics and techniques using Principal Component Analysis (PCA)

Methodology

- PCA Algorithm
- Preparing Dataset

RESULTS AND DISCUSSION



- When Score are greater than 0.75 that means “strong correlation,
- When Socre are from 0.50-0.75 that means “moderate”,
- When Socre are range from 0.30-0.49 that means “weak”
- As shown in figure 5 most of chains of tactics have value more than .75 which means there is a strong correlation.

- **Evaluation:**
- ROC=1
-

Example

- **For example the malicious behavior “Packet capture” can be achieved by this chains of tactics : ['credential-access', 'collection'], ['defense-evasion', 'persistence', 'command-and-control'] and ['command-and-control']**

Conclusion

- In this paper, we analyzed tactics, techniques and procedures for ICS attack behavior techniques in MITRE ATT&CK. We proposed a machine learning principal component analysis to analyze the correlation tactics, techniques and procedures. We found that there is a strong correlation between some chains of tactics and techniques.

References

[1] L. Rosa, M. Freitas, S. Mazo, E. Monteiro, T. Cruz, and P. Simões, “A Comprehensive Security Analysis of a SCADA Protocol: From OSINT to Mitigation,” *IEEE Access*, vol. 7, pp. 42156–42168, 2019, doi: 10.1109/ACCESS.2019.2906926.

[2] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, “A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics,” *IEEE Commun. Surv. Tutor.*, pp. 1–1, 2020, doi: 10.1109/COMST.2020.2987688.

[3] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, “A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics,” *IEEE Commun. Surv. Tutor.*, vol. 22, no. 3, pp. 1942–1976, thirdquarter 2020, doi: 10.1109/COMST.2020.2987688.

[4] M. Att, “MP180360 MITRE PRODUCT,” p. 37.

[5] E. E. Bloedorn, L. M. Talbot, and D. D. DeBarr, “Data Mining Applied to Intrusion Detection: MITRE Experiences,” in *Machine Learning and Data Mining for Computer Security: Methods and Applications*, M. A. Maloof, Ed. London: Springer, 2006, pp. 65–88.

[6] S. Choi, J. Choi, J.-H. Yun, B.-G. Min, and H. Kim, “Expansion of {ICS} Testbed for Security Validation based on {MITRE} ATT&CK Techniques,” presented at the 13th {USENIX} Workshop on Cyber Security Experimentation and Test ({CSET} 20), 2020, Accessed: Oct. 07, 2020. [Online]. Available: https://www.usenix.org/conference/cset20/presentation/choi.

[7] U. Noor, Z. Anwar, T. Amjad, and K.-K. R. Choo, “A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise,” *Future Gener. Comput. Syst.*, vol. 96, pp. 227–242, Jul. 2019, doi: 10.1016/j.future.2019.02.013.

[8] G. Ayoade, S. Chandra, L. Khan, K. Hamlen, and B. Thuraisingham, *Automated Threat Report Classification over Multi-Source Data*. 2018.

References

[9] R. Kwon, T. Ashley, J. Castleberry, P. Mckenzie, and S. N. G. Gourisetti, “Cyber Threat Dictionary Using MITRE ATT CK Matrix and NIST Cybersecurity Framework Mapping,” in *2020 Resilience Week (RWS)*, Oct. 2020, pp. 106–112, doi: 10.1109/RWS50334.2020.9241271.

[10] P. Maynard and K. McLaughlin, “Big Fish, Little Fish, Critical Infrastructure: An Analysis of Phineas Fisher and the ‘Hacktivist’ Threat to Critical Infrastructure,” *ArXiv200414360 Cs*, Apr. 2020, Accessed: Nov. 23, 2020. [Online]. Available: http://arxiv.org/abs/2004.14360.

[11] V. Legoy, M. Caselli, C. Seifert, and A. Peter, “Automated Retrieval of ATT&CK Tactics and Techniques for Cyber Threat Reports,” *ArXiv200414322 Cs*, Apr. 2020, Accessed: Nov. 23, 2020. [Online]. Available: http://arxiv.org/abs/2004.14322.

[12] Z. Gniazdowski, “New Interpretation of Principal Components Analysis,” *Zesz. Nauk. Warsz. Wyższej Szk. Inform.*, vol. 11, no. 16, pp. 43–65, Aug. 2017, doi: 10.26348/znwwsi.16.43.

[13] M. Li, “Application of CART decision tree combined with PCA algorithm in intrusion detection,” in *2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, Nov. 2017, pp. 38–41, doi: 10.1109/ICSESS.2017.8342859.

[14] N. Wang, N. N. Zeng, and W. Zhu, “Sensitivity, Specificity, Accuracy, Associated Confidence Interval And ROC Analysis With Practical SAS Implementations,” p. 9, 2010.

Thank you

Colorado State University

Security Performance Analysis of Electronic Payment Systems

CS559—Final report, Jacinda Li

Catalogue

01

Electronic Commerce

02

Electronic Payment

03

Tools and Methods

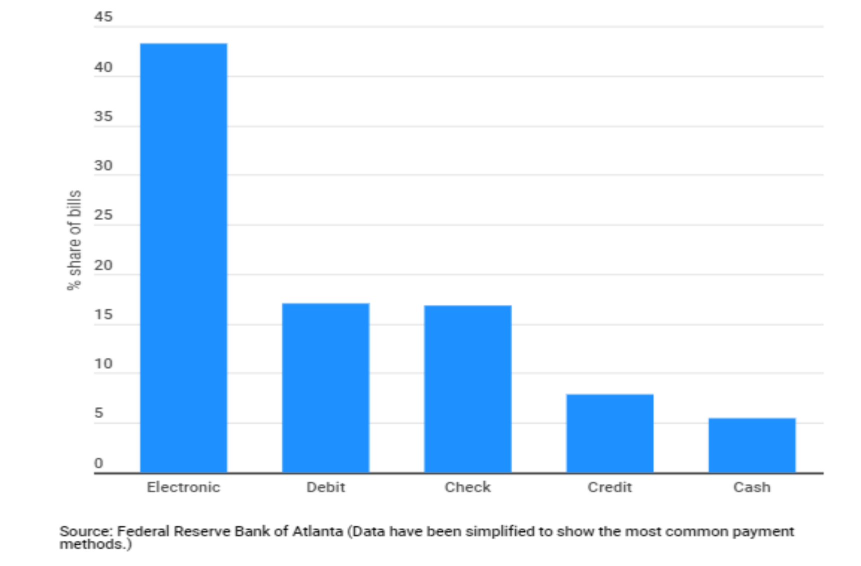
04

Conclusion

Electronic Commerce

- *Business to Employee*
- *Business-to-business electronic commerce(B2B)(Fig.2)*
- *Business-to-consumer electronic commerce(B2C)*
- Example: Apple official web, Nike official web.

- *Consumer -to- consumer electronic commerce(C2C)*
- Example: eBay.



Source: Federal Reserve Bank of Atlanta (Data have been simplified to show the most common payment methods.)

Figure 1. The data comes from at the Federal Reserve Bank of Atlanta about how consumers spent in 2018, with electronic payments accounting for the largest share.

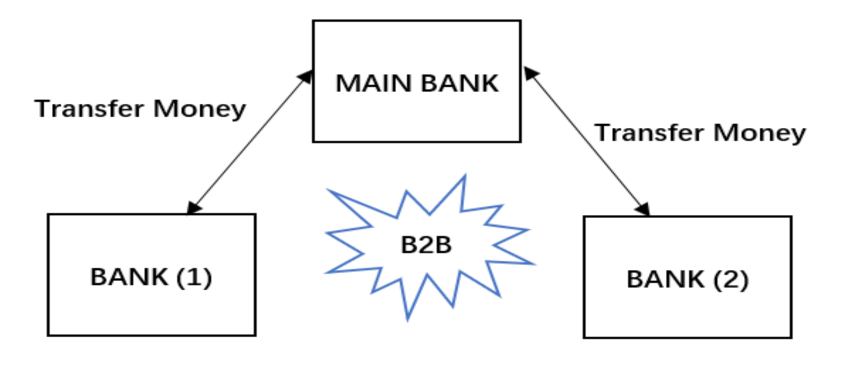


Figure 2. Between different banks, if a customer needs to transfer funds from the bank (1) to the bank (2), the funds need to be transferred through the B2B e-commerce model, first to the main bank (Settlement channels), and then to the bank where the target account is located.

Electronic Commerce

- *Advantage:*
  - High communication speed
  - 24-hour service
  - Low-cost
  - Convenient communication between customers and businesses
  - Businesses can improve their work on time
  - Better service quality

- *The characteristics of electronic commerce*
  - *Business and Service*
  - *Integration, Coordination and Extensibility*
  - *Security*

Electronic Payment Systems

Traditional Payment System(Fig.3)

V.S.

Electronic Payment System(Fig.4)

- ***Payment Risk***
  - *Information Risk*
  - *Transaction Risk*
  - *Operation Risk*
  - *Some risks about computer virus*
- ***Security Requirement***
  - *Integrity and confidentiality of information*
  - *Ensure the timeliness and controllability of transactions*
  - *Low-cost*

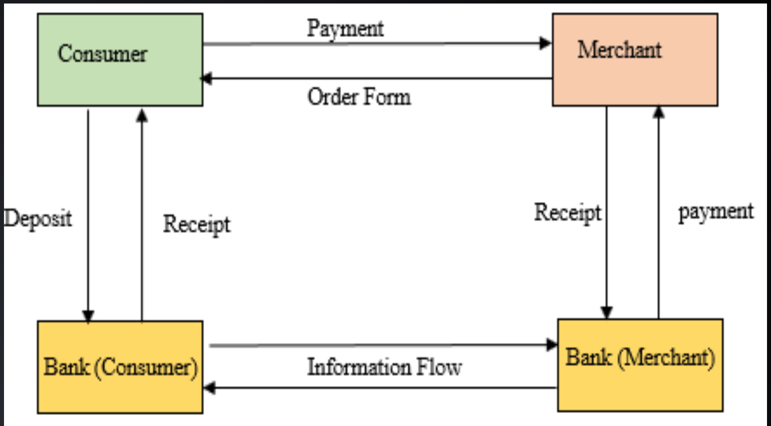


Figure 3. A schematic diagram of the transaction process.

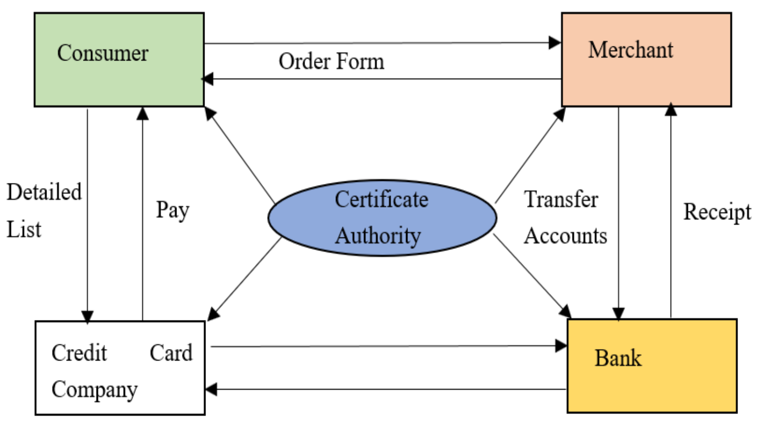


Figure 4. A schematic diagram of the electronic payment process.

Tools and Methods

Some common security protocols for electronic payment systems:

TCP/IP

- Process
- Advantage
- Disadvantage

SET

- Process
- Advantage
- Disadvantage

SSL

- Process
- Advantage
- Disadvantage

3D-Secure

- Process
- Advantage
- Disadvantage

TCP/IP

1) TCP/IP protocol is a standard protocol for network communication.

2) It is a combination of multiple protocols at different levels.

3) Using the socket to create a connection

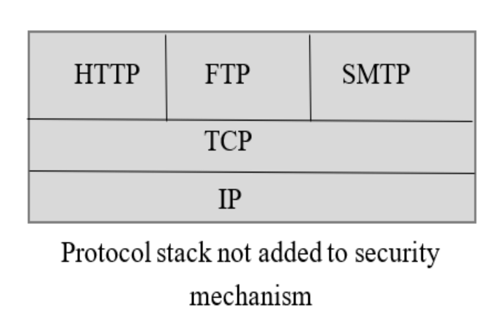


Figure 5.Protocol stack not added to security mechanism.

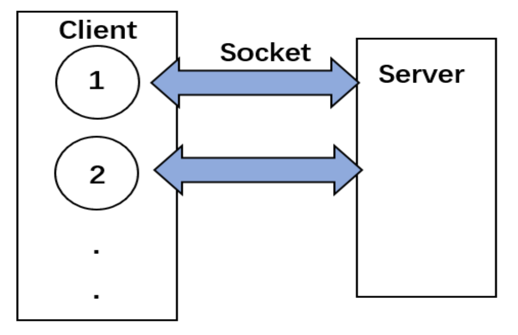


Figure 6. A diagram of the TCP transaction .

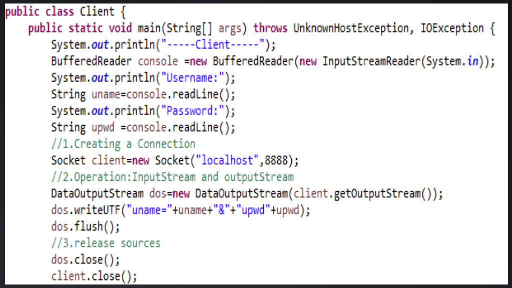
TCP/IP

Advantage:

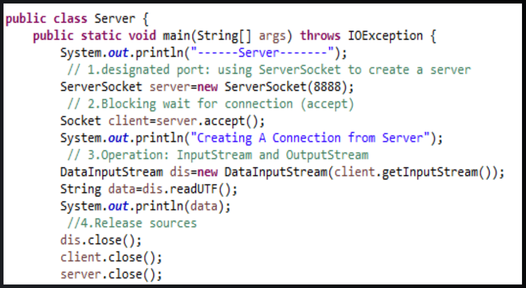
1) Reliability
2) Stability

Disadvantage:

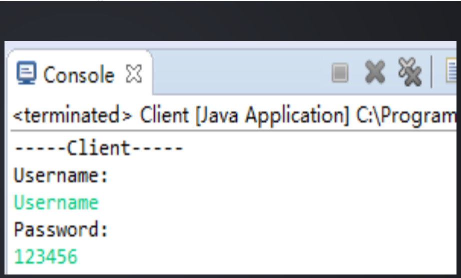
1) Slow
2) Low efficiency
3) High system resource occupancy
4) Vulnerable to attack: during transmission, vulnerable to Denial of Service (DOS), Distributed Denial of Service (DDOS), etc.



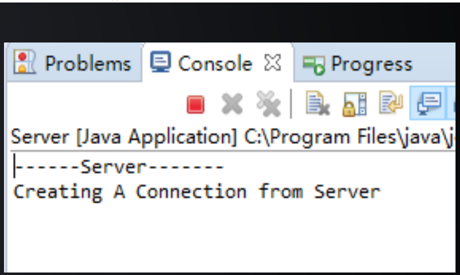
```java
public class Client {
    public static void main(String[] args) throws UnknownHostException, IOException {
        System.out.println("-----Client-----");
        BufferedReader console =new BufferedReader(new InputStreamReader(System.in));
        System.out.println("Username:");
        String uname=console.readLine();
        System.out.println("Password:");
        String upwd =console.readLine();
        //1.Creating a Connection
        Socket client=new Socket("localhost",8888);
        //2.Operation:InputStream and outputStream
        DataOutputStream dos=new DataOutputStream(client.getOutputStream());
        dos.writeUTF("uname="+uname+"&"+"upwd"+upwd);
        dos.flush();
        //3.release sources
        dos.close();
        client.close();
```



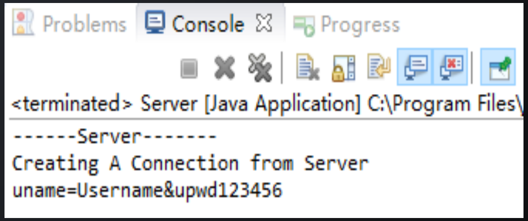
```java
public class Server {
    public static void main(String[] args) throws IOException {
        System.out.println("------Server-------");
         // 1.designated port: using ServerSocket to create a server
        ServerSocket server=new ServerSocket(8888);
         // 2.Blocking wait for connection (accept)
        Socket client=server.accept();
        System.out.println("Creating A Connection from Server");
         // 3.Operation: InputStream and OutputStream
        DataInputStream dis=new DataInputStream(client.getInputStream());
        String data=dis.readUTF();
        System.out.println(data);
         //4.Release sources
        dis.close();
        client.close();
        server.close();
```



```
<terminated> Client [Java Application] C:\Program
-----Client-----
Username:
Username
Password:
123456
```



```
Server [Java Application] C:\Program Files\java\j
------Server-------
Creating A Connection from Server
```



```
<terminated> Server [Java Application] C:\Program Files\
------Server-------
Creating A Connection from Server
uname=Username&upwd123456
```

SET

1) A Connection between consumers, manufacturers, and Banks.
2) The confidentiality of the information and the integrity of the payment process
3) It only encrypts sensitive and risky information.

Advantage:

- High confidentiality of information
- Ensure the integrity of information transmission
- By using two-way signatures, participants are guaranteed to be isolated from each other
- Real-time online payment
- High safety

Disadvantage

- Complex implementation process
- High requirements on the system
- High costs

SSL

1) SSL is a secure communication protocol introduced by Netscape.

2) Based on the Transport Layer Protocol (TCP) (Fig.7)

3) It is independent of the application layer protocol.

4) It uses encryption algorithms, communication protocols, and server authentication to reliably encrypt the data [9].

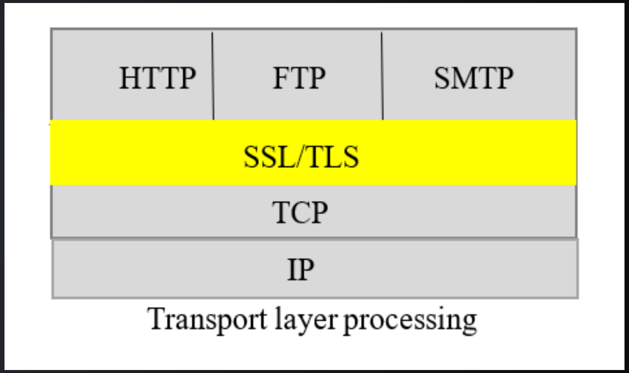


Figure 7.Transport layer processing.

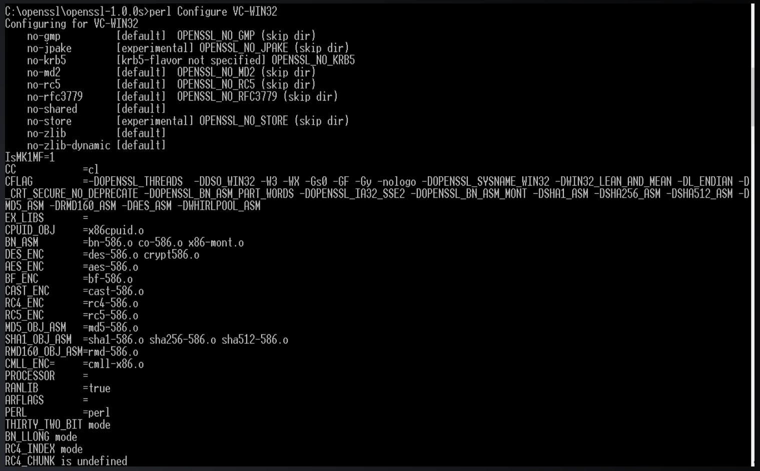
SSL

Advantage

- A relatively perfect transmission protocol,
- Low-cost
- Low requirements for the system
- The confidentiality and integrity of the data

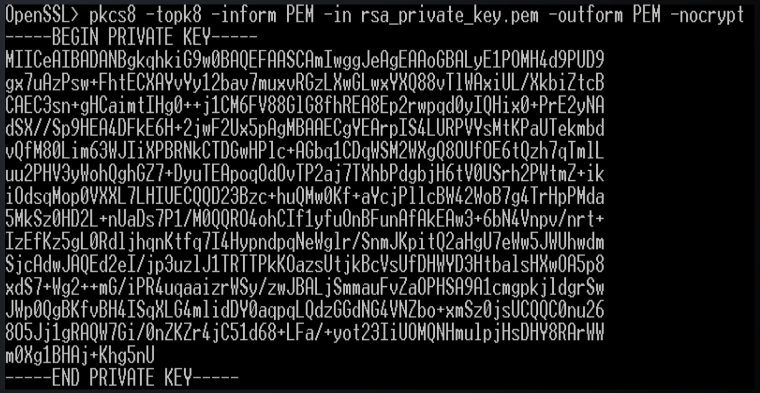
Disadvantage

- SSL provides only the identification of the browser and the server, not the identification of the customer or merchant.
- Encryption strength is not enough, security performance is not strong.
- Some risks about key management
- Vulnerable to attack



```
C:\openssl\openssl-1.0.0s>perl Configure VC-WIN32
Configuring for VC-WIN32
    no-gmp          [default]  OPENSSL_NO_GMP (skip dir)
    no-jpake        [experimental] OPENSSL_NO_JPAKE (skip dir)
    no-krb5         [krb5-flavor not specified] OPENSSL_NO_KRB5
    no-md2          [default]  OPENSSL_NO_MD2 (skip dir)
    no-rc5          [default]  OPENSSL_NO_RC5 (skip dir)
    no-rfc3779      [default]  OPENSSL_NO_RFC3779 (skip dir)
    no-shared       [default]
    no-store        [experimental] OPENSSL_NO_STORE (skip dir)
    no-zlib         [default]
    no-zlib-dynamic [default]
IsMK1MF=1
CC            =cl
CFLAG         =-DOPENSSL_THREADS  -DDSO_WIN32 -W3 -WX -Gs0 -GF -Gy -nologo -DOPENSSL_SYSNAME_WIN32 -DWIN32_LEAN_AND_MEAN -DL_ENDIAN -D
_CRT_SECURE_NO_DEPRECATE -DOPENSSL_BN_ASM_PART_WORDS -DOPENSSL_IA32_SSE2 -DOPENSSL_BN_ASM_MONT -DSHA1_ASM -DSHA256_ASM -DSHA512_ASM -D
MD5_ASM -DRMD160_ASM -DAES_ASM -DWHIRLPOOL_ASM
EX_LIBS       =
CPUID_OBJ     =x86cpuid.o
BN_ASM        =bn-586.o co-586.o x86-mont.o
DES_ENC       =des-586.o crypt586.o
AES_ENC       =aes-586.o
BF_ENC        =bf-586.o
CAST_ENC      =cast-586.o
RC4_ENC       =rc4-586.o
RC5_ENC       =rc5-586.o
MD5_OBJ_ASM   =md5-586.o
SHA1_OBJ_ASM  =sha1-586.o sha256-586.o sha512-586.o
RMD160_OBJ_ASM=rmd-586.o
CMLL_ENC=     =cmll-x86.o
PROCESSOR     =
RANLIB        =true
ARFLAGS       =
PERL          =perl
THIRTY_TWO_BIT mode
BN_LLONG mode
RC4_INDEX mode
RC4_CHUNK is undefined
```

Figure 8.Install the Perl and OpenSSL.



```
OpenSSL> pkcs8 -topk8 -inform PEM -in rsa_private_key.pem -outform PEM -nocrypt
-----BEGIN PRIVATE KEY-----
MIICeAIBADANBgkqhkiG9w0BAQEFAASCAmIwggJeAgEAAoGBALyE1POMH4d9PUD9
gx7uAzPsw+FhtECXAYvYy12bav7muxvRGzLXwGLwxYXQ88vTlWAxiUL/XkbiZtcB
CAEC3sn+gHCaimtIHg0++j1CM6FV88G1G8fhREA8Ep2rwpqd0yIQHix0+PrE2yNA
dSX//Sp9HEA4DFkE6H+2jwF2Ux5pAgMBAAECgYEArpIS4LURPVYsMtKPaUTekmbd
vQfM80Lim63WJIiXPBRNkCTDGwHPlc+AGbq1CDqWSM2WXgQ80Uf0E6tQzh7qTmlL
uu2PHV3yWohQghGZ7+DyuTEApoqOdOvTP2aj7TXhbPdgbjH6tV0USrh2PWtmZ+ik
iOdsqMop0VXXL7LHIUECQQD23Bzc+huQMw0Kf+aYcjPllcBW42WoB7g4TrHpPMda
5MkSz0HD2L+nUaDs7P1/M0QQRO4ohCIf1yfuOnBFunAfAkEAw3+6bN4Vnpv/nrt+
IzEfKz5gL0RdljhqnKtfq7I4HypndpqNeWglr/SnmJKpitQ2aHgU7eWw5JWUhwdm
SjcAdwJAQEd2eI/jp3uzlJ1TRTTPkKOazsUtjkBcVsUfDHWYD3HtbalsHXw0A5p8
xdS7+Wg2++mG/iPR4uqaaizrWSy/zwJBALjSmmauFvZaOPHSA9A1cmgpkjldgrSw
JWp0QgBKfvBH4ISqXLG4mlidDY0aqpqLQdzGGdNG4VNZbo+xmSz0jsUCQQC0nu26
805Jj1gRAQW7Gi/0nZKZr4jC51d68+LFa/+yot23IiUOMQNHmulpjHsDHY8RArWW
m0Xg1BHAj+Khg5nU
-----END PRIVATE KEY-----
```

Figure 9.RSD Private key.

3D-Secure

1) A new type of security verification service

2) It can make personalized information.

3) It can ensure the authenticity and reliability of the shopping website.

4) Double verification (Like SET)

Advantage

- Convenient and quick
- High security
- Low-cost

Disadvantage

- Large demand for data
- Difficult to popularize

Comprehensive model

- Combine the observations with the functions of the security protocols to create a payment transaction model that is applicable to the current situation.

- Based on SET, SSL, and 3D-Secure, we can use different protocols according to the identity of the participants.

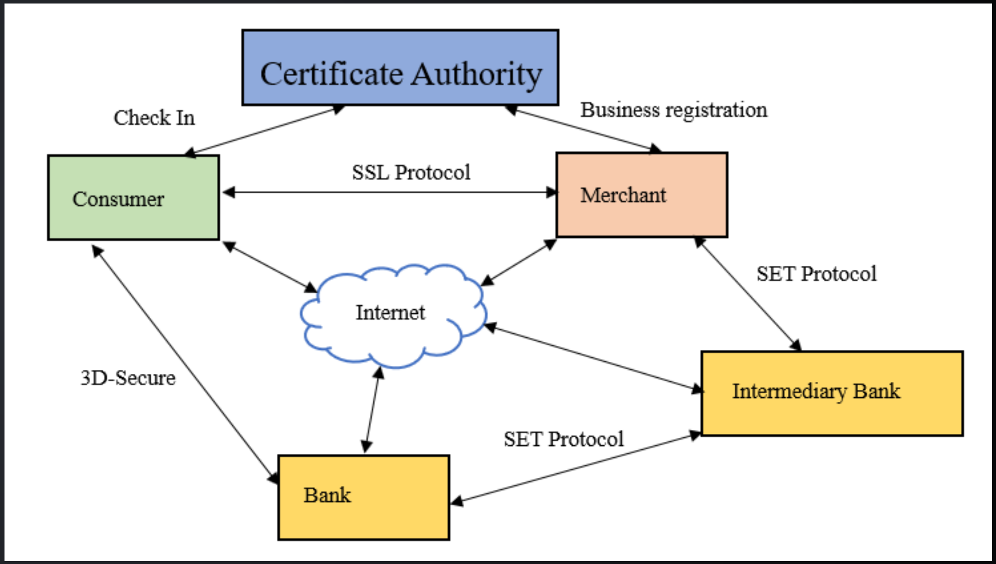


Figure 10. A diagram about comprehensive model.

Conclusion and Future work

- Understand electronic commerce, electronic payment and other information.
- Understand the advantage and disadvantages of security protocols.
- Created a comprehensive model for the complex trading environment.

- Security, cost, and complexity have always been major concerns in the establishment of security protocols.
- The promotion of 3D-SerCue can make electronic payment transactions more perfect.
- However, with the increasing complexity of the participants in the transaction, a single protocol sometimes cannot meet all the requirements.

Reference

[1] J. Kalbande, “Ecommerce Transactions: Secure Gateway in Payment System,”. International Research Journal of Engineering and Technology[J] vol. 6, pp. 421-427, 2019. Issue:06

[2] B. Narwal, “Security Analysis and Verification of Authenticated Mobile Payment Protocols,”. Conf. 2019 4th International Conference on Information Systems and Computer Networks (ISCON). Nov 21-22 2019. Available: https://ieeexplore.ieee.org/abstract/document/9036151

[3] J.T. Graves, A. Acquisti, N. Christin, “Should Credit Card Issuers Reissue Cards in Response to a Data Breach? Uncertainty and Transparency in Metrics for Data Security Policymaking,”. ACM Transactions on Internet Technology. vol. 18, pp. 1-19, 2018.

[4] P. Aigbe, J. Akpojaro, “Analysis of Security Issues in Electronic Payment Systems,”. International Journal Of Computer Applications[J] vol. 108, pp. 10-14, 2014.

[5] S. Saxena, S. Vyas, B.S. Kumar, S. Gupta,” Survey on Online Electronic Paymentss Security,”vol.6, pp. 746-751, 2019.

[6] C. Vinton. "Social, Technical and Economic Consequences of the Internet Evolution." Ensemble video, 01:39:21. 9-27, 2007.

[7] S. Sumanjeet, “EMERGENCE OF PAYMENT SYSTEMS IN THE AGE OF ELECTRONIC COMMERCE: THE STATE OF ART,”. Global Journal of International Business Research [J] vol. 2, pp. 17-36, 2009.

[8] T. Tsiakis, G. Sthephanides,” The concept of security and trust in electronic payments,”. vol. 24, pp. 10-59, 2005.

[9] H.El Ismaili , H. Houmani , H. Madroumi,” A Secure Electronic Transaction Payment Protocol Design and Implementation,” International Journal of Advanced Computer Science and Applications. Vol. 5, pp. 172-180, 2014. Available: https://thesai.org/Publications/IJACSA

[10] Y. Xu, J. Liu,” Electronic payment system design based on SET and TTP ,” 2010 International Conference on E-Business and E-Government, IEEE Access, Vol. 10, pp. 275-278, 2010.

[11] T. A. Hemphill, P. Longstreet,” Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards ,” Technology in Society, Vol. 44, pp. 30-38, 2016.

[12] S. Solat,” Security of Electronic Payment Systems: A Comprehensive Survey,” Sorbonne Universités, UPMC University of Paris VI, French National Centre for Scientific Research CNRS, Computer Laboratory , pp. 1-29, 2017.

[13] M. H. Sherif, A. Serhrouchni, A. Y. Gaid and F. Farazmandnia, "SET and SSL: electronic payments on the Internet," Proceedings Third IEEE Symposium on Computers and Communications. ISCC'98. (Cat. No.98EX166), Athens, Greece, 1998, pp. 353-358, doi: 10.1109/ISCC.1998.702546.

[14] Y. Zhao, L. Yuan, “A Study on Electronic Payment Protocols and their Evolution,” Journal of Information, vol. 11, pp. 1-16, 2006.

[15] G. Hua, , X. Fei, “An implementation of SET Protoeol based on SSL Protocol,” Computer engineering and design, vol. 24, No.9, pp.80-96, 2003

THANK YOU

THANK FOR YOU WATCHING

Review of the tradeoffs models due to cyber-security issues

Alexandre Dubois

Plan

1. Introduction
2. Motivating example
3. Prevention strategy
    a. Cybersecurity good practices and training
    b. Insurances
4. Response strategy
    a. Confidentiality shock and focus
    b. Confidentiality shock and availability focus
5. Conclusion
6. References

Introduction

Companies / Institutions need to take into considerations different aspects of cybersecurity:

1. Prevention to reduce the chances of occurrences
2. Insurance to cover the potential economic loss
3. Palliation that is how to answer to a vulnerability

Companies / Institutions have to choose how to invest their money in those areas knowing that:

1. Prevention is never enough alone
2. Insurance cannot cover risks that are not economical
3. Quick and efficient palliation needs to set up high priorities and is a last resort

This class project reviews existing models and recommendations in those three areas.

Prevention

Prevention consists on:

1. Training workers and sensibilizing them to cybersecurity issues
   - Initial training for new hired
   - Short regular updates on the training to keep everyone aware
   - Dummy attacks to sensibilize workers to the risk
2. Following good practices of the field [16]
3. Monitoring the evolution of the field and investing in research
   - Internally with specific teams
   - Through counseling companies
   - By keeping in touch with cybersecurity governmental institutions (https://www.ssi.gouv.fr/)

Prevention

Table from [16]

List of the vulnerabilities prevention practices and the percentage of companies respecting them.

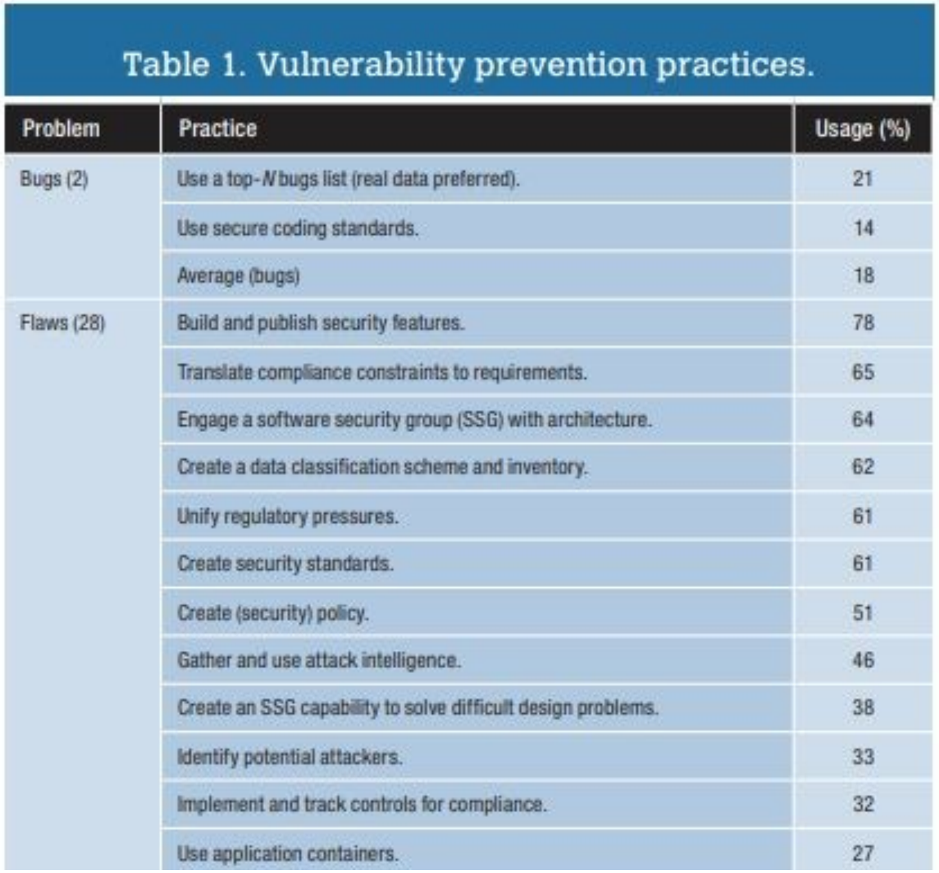


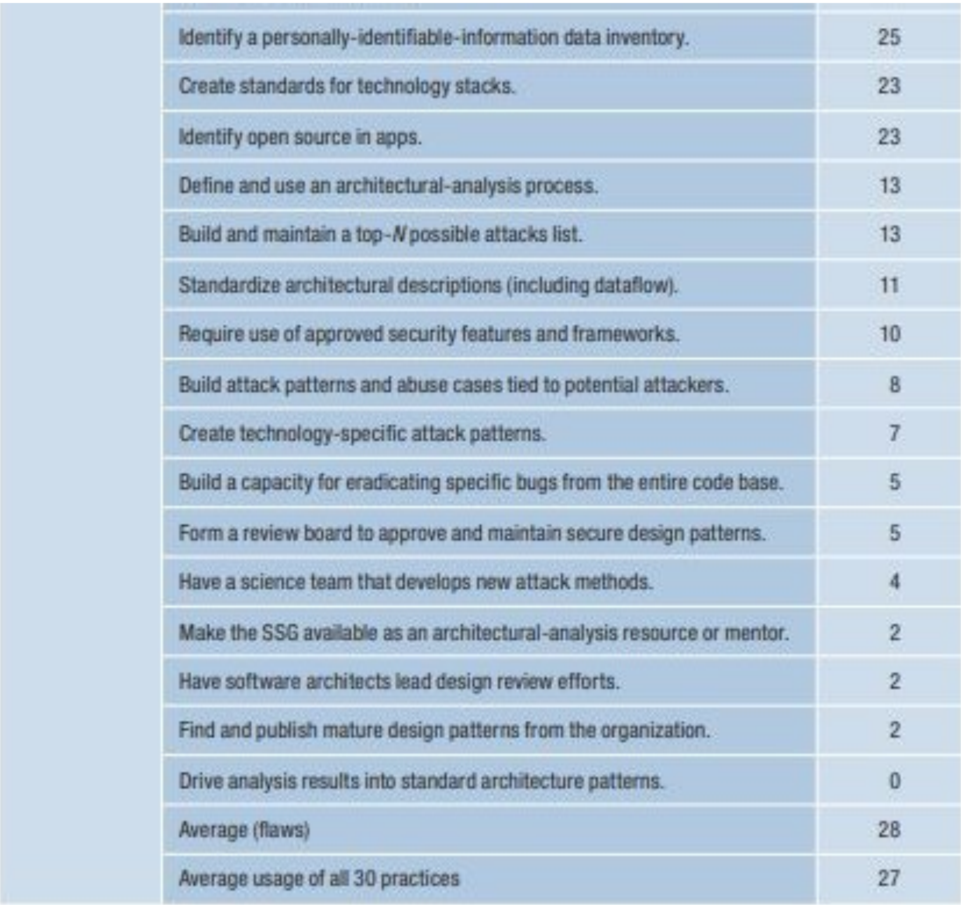
Table 1. Vulnerability prevention practices.

Problem	Practice	Usage (%)
Bugs (2)	Use a top-*N* bugs list (real data preferred).	21
	Use secure coding standards.	14
	Average (bugs)	18
Flaws (28)	Build and publish security features.	78
	Translate compliance constraints to requirements.	65
	Engage a software security group (SSG) with architecture.	64
	Create a data classification scheme and inventory.	62
	Unify regulatory pressures.	61
	Create security standards.	61
	Create (security) policy.	51
	Gather and use attack intelligence.	46
	Create an SSG capability to solve difficult design problems.	38
	Identify potential attackers.	33
	Implement and track controls for compliance.	32
	Use application containers.	27

Prevention

Table from [16]

List of the vulnerabilities prevention practices and the percentage of companies respecting them.



Identify a personally-identifiable-information data inventory.	25
Create standards for technology stacks.	23
Identify open source in apps.	23
Define and use an architectural-analysis process.	13
Build and maintain a top-*N* possible attacks list.	13
Standardize architectural descriptions (including dataflow).	11
Require use of approved security features and frameworks.	10
Build attack patterns and abuse cases tied to potential attackers.	8
Create technology-specific attack patterns.	7
Build a capacity for eradicating specific bugs from the entire code base.	5
Form a review board to approve and maintain secure design patterns.	5
Have a science team that develops new attack methods.	4
Make the SSG available as an architectural-analysis resource or mentor.	2
Have software architects lead design review efforts.	2
Find and publish mature design patterns from the organization.	2
Drive analysis results into standard architecture patterns.	0
Average (flaws)	28
Average usage of all 30 practices	27

Cyber-Risk Insurances

- The company / Institution subscribe to an insurance that mitigate losses in case of cyber-incidents
- The Cyber-Risk Insurance market is currently growing quickly
- Once established, that market will be able to make companies improve their prevention by giving rewards such as (https://www.cisa.gov/cybersecurity-insurance)
  - Giving more coverage
  - Reducing their cost based on risks models

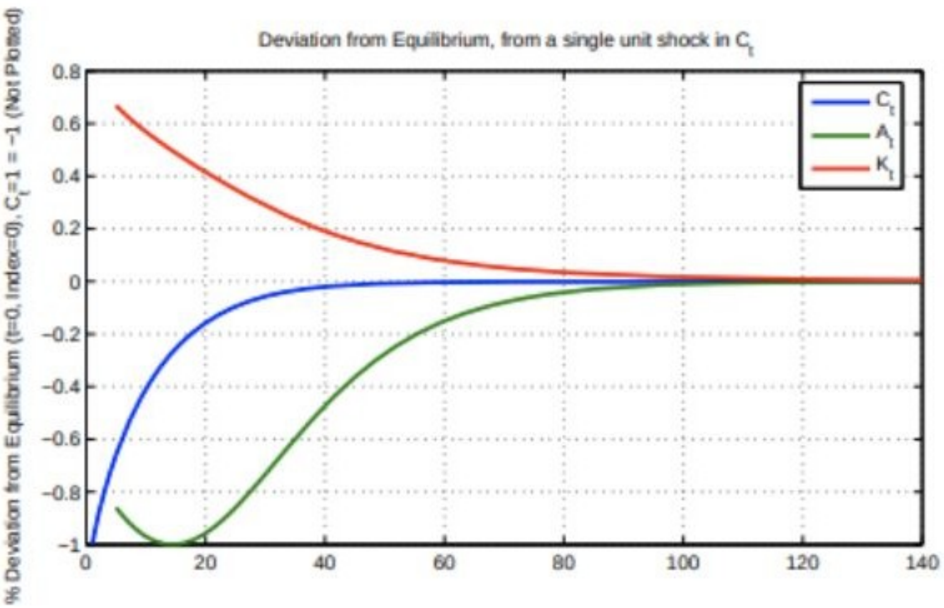
Response strategies [18]

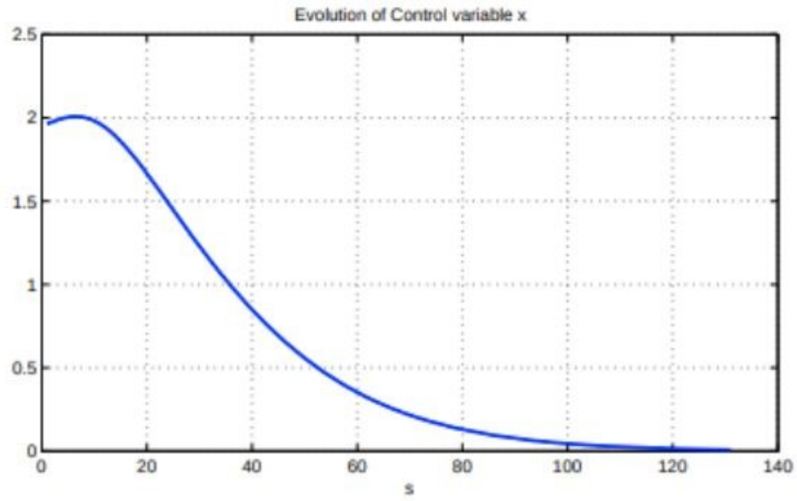
- A successful attack compromises the CIA (Confidentiality, Integrity, Availability)
- The institution/company victim put money on the table to solve the problem
- The victim can choose to restore the CIA by prioritizing differently

To be efficient in the response, procedures need to be in place, or at least the focus of the response need to be set to optimize response time.

Patching policies and timelines must also have been thought about to reduce the global loss.

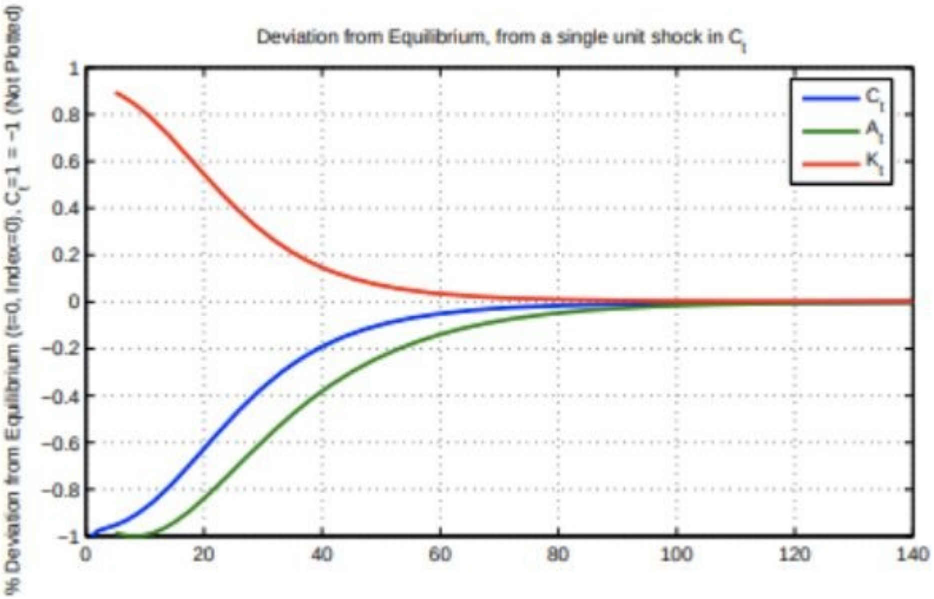
Confidentiality shock and focus

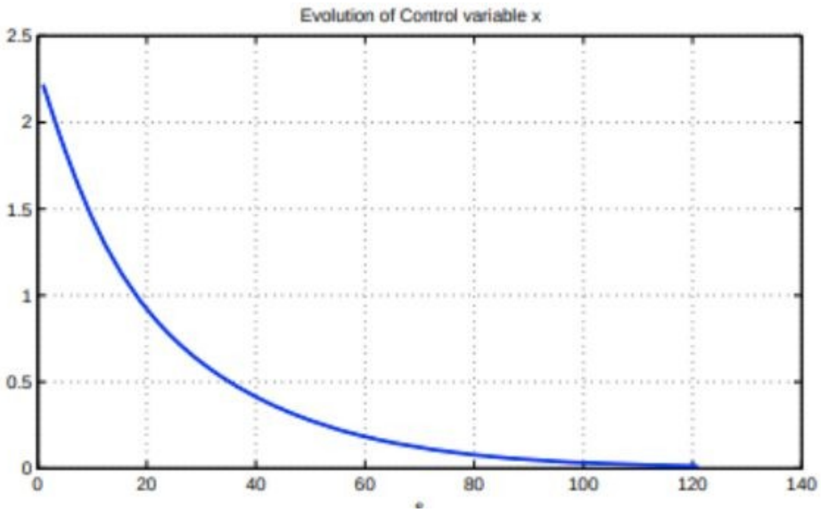




Graphs from [18]

Confidentiality shock and availability focus





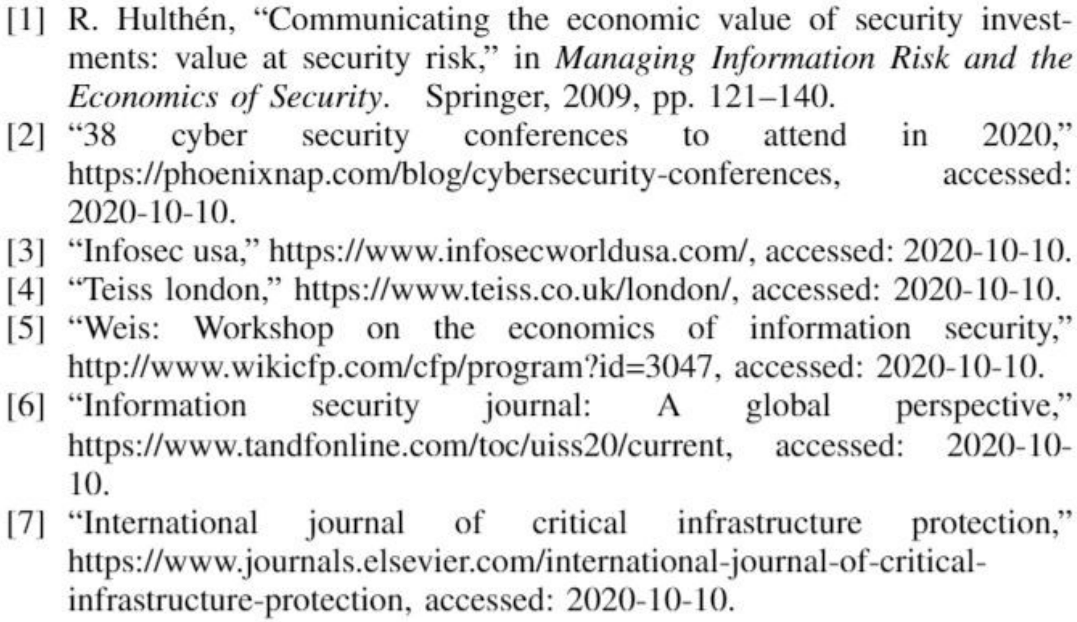
Graphs from [18]

Conclusion: drawbacks to consider

- Prevention
  - Training and counseling are expensive
  - Hard to quantify the impact of prevention as it is something not happening
- Insurance
  - Only impact financial losses
  - Tend to give the impression that the responsibility of the company has disappeared
- Palliation
  - Needs to have palliation procedures in place to be efficient
  - Is a last resort

This project has taken the point of view of harsh consequences for the victim (for example an attack disabling a company production for a vital product [13])

References



[1] R. Hulthén, "Communicating the economic value of security investments: value at security risk," in *Managing Information Risk and the Economics of Security*. Springer, 2009, pp. 121–140.

[2] "38 cyber security conferences to attend in 2020," https://phoenixnap.com/blog/cybersecurity-conferences, accessed: 2020-10-10.

[3] "Infosec usa," https://www.infosecworldusa.com/, accessed: 2020-10-10.

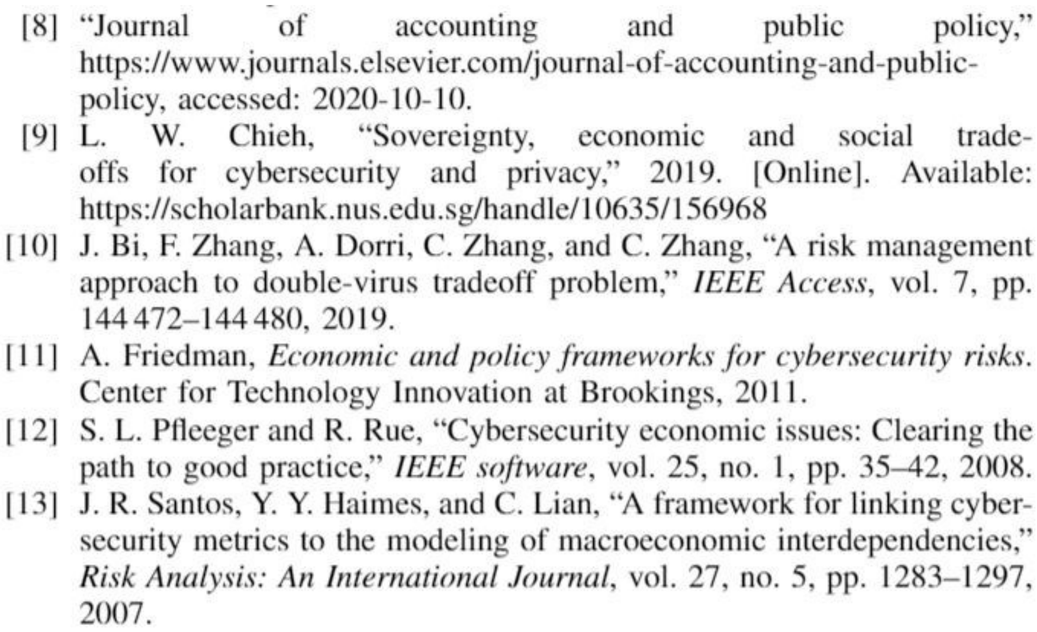
[4] "Teiss london," https://www.teiss.co.uk/london/, accessed: 2020-10-10.

[5] "Weis: Workshop on the economics of information security," http://www.wikicfp.com/cfp/program?id=3047, accessed: 2020-10-10.

[6] "Information security journal: A global perspective," https://www.tandfonline.com/toc/uiss20/current, accessed: 2020-10-10.

[7] "International journal of critical infrastructure protection," https://www.journals.elsevier.com/international-journal-of-critical-infrastructure-protection, accessed: 2020-10-10.

References



[8] "Journal of accounting and public policy," https://www.journals.elsevier.com/journal-of-accounting-and-public-policy, accessed: 2020-10-10.

[9] L. W. Chieh, "Sovereignty, economic and social trade-offs for cybersecurity and privacy," 2019. [Online]. Available: https://scholarbank.nus.edu.sg/handle/10635/156968

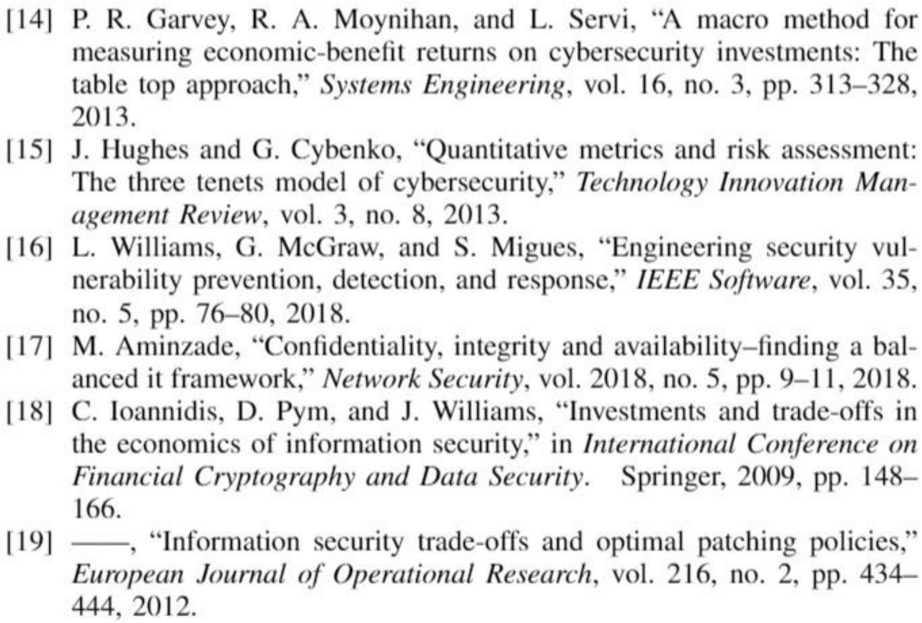
[10] J. Bi, F. Zhang, A. Dorri, C. Zhang, and C. Zhang, "A risk management approach to double-virus tradeoff problem," *IEEE Access*, vol. 7, pp. 144 472–144 480, 2019.

[11] A. Friedman, *Economic and policy frameworks for cybersecurity risks*. Center for Technology Innovation at Brookings, 2011.

[12] S. L. Pfleeger and R. Rue, "Cybersecurity economic issues: Clearing the path to good practice," *IEEE software*, vol. 25, no. 1, pp. 35–42, 2008.

[13] J. R. Santos, Y. Y. Haimes, and C. Lian, "A framework for linking cyber-security metrics to the modeling of macroeconomic interdependencies," *Risk Analysis: An International Journal*, vol. 27, no. 5, pp. 1283–1297, 2007.

References



[14] P. R. Garvey, R. A. Moynihan, and L. Servi, “A macro method for measuring economic-benefit returns on cybersecurity investments: The table top approach,” *Systems Engineering*, vol. 16, no. 3, pp. 313–328, 2013.

[15] J. Hughes and G. Cybenko, “Quantitative metrics and risk assessment: The three tenets model of cybersecurity,” *Technology Innovation Management Review*, vol. 3, no. 8, 2013.

[16] L. Williams, G. McGraw, and S. Migues, “Engineering security vulnerability prevention, detection, and response,” *IEEE Software*, vol. 35, no. 5, pp. 76–80, 2018.

[17] M. Aminzade, “Confidentiality, integrity and availability–finding a balanced it framework,” *Network Security*, vol. 2018, no. 5, pp. 9–11, 2018.

[18] C. Ioannidis, D. Pym, and J. Williams, “Investments and trade-offs in the economics of information security,” in *International Conference on Financial Cryptography and Data Security*. Springer, 2009, pp. 148–166.

[19] ——, “Information security trade-offs and optimal patching policies,” *European Journal of Operational Research*, vol. 216, no. 2, pp. 434–444, 2012.

CS559-Final Project

Advances on virtualization technology of cloud computing

Wei Chen
12/08/2020

content

1

2 Virtualization technology

Docker container and virtual machine comparison

3 The impact of Docker Container

4 Prospects for the development trend of containers

PART ONE

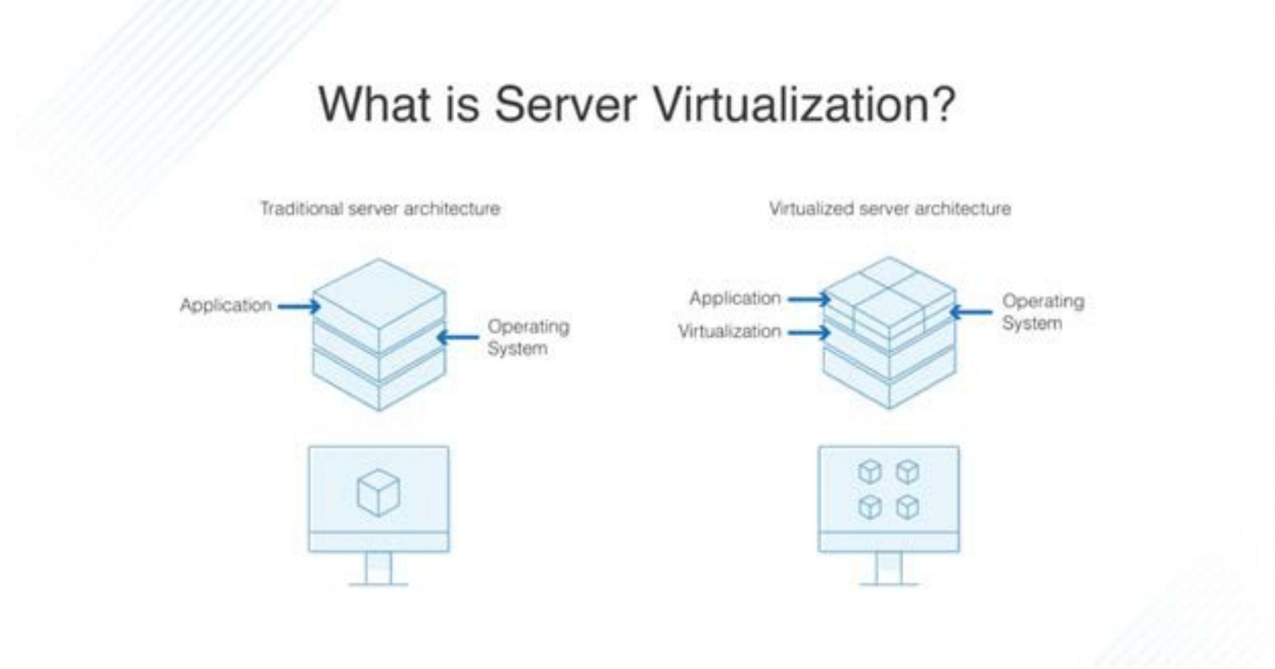
Virtualization technology

ADD YOUR TITLE HERE

Server virtualization

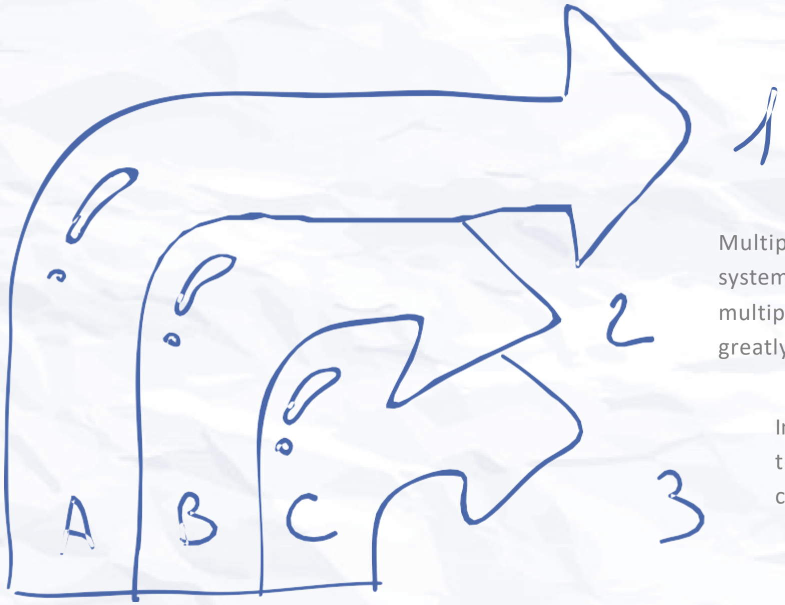
Server virtualization refers to virtualizing a computer into multiple logical computers through virtualization technology.

The virtualization of the server is realized by introducing a virtualization layer between the hardware and the operating system to realize the decoupling of the hardware and the operating system.


What is Server Virtualization?
Traditional server architecture
Application
Operating System
Virtualized server architecture
Application
Virtualization
Operating System

单击此处添加标题 Docker container technology

•Docker is a container platform that can simplify and standardize application deployment in different environments. There are already many ecosystem software related to distributed container management.



The container can provide an isolated operating space for the application, including the complete user environment space; changes in one container will not affect the operating environment of other containers

Multiple containers can share the kernel of the same operating system, so that when the same system library is used by multiple containers, the efficiency of memory usage will be greatly improved

In recent years, with the emergence of Docker, container technology has had a huge impact on the development of cloud computing.

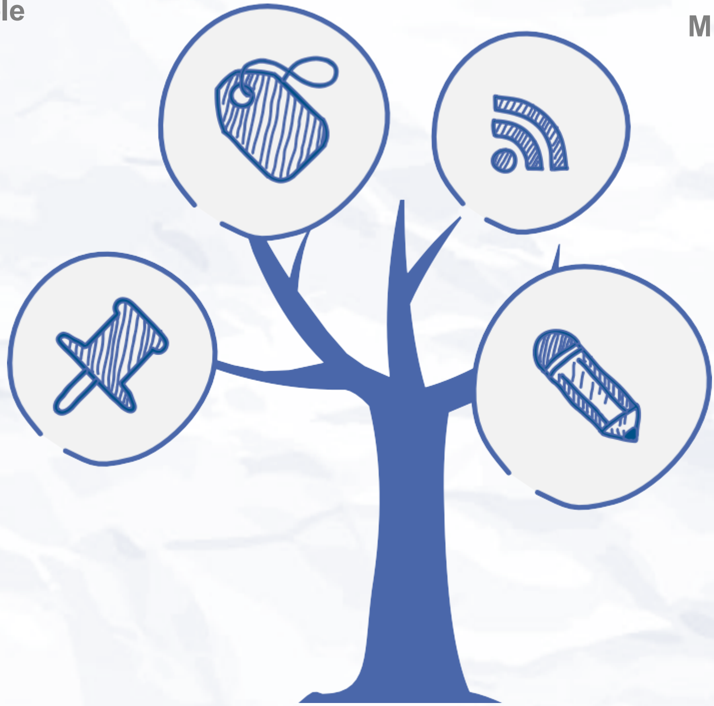
PART TWO

Docker container and virtual machine comparison

Advantages of Docker

Quickly available

More efficient virtualization



Simplify deployment

Microservices

Disadvantages of Docker

1) Resource isolation problem
2) Security issues
3) Container management needs to be strengthened

4) Compatibility issues
5) Windows containers are not yet mature
6) The container orchestration engine is not yet mature

PART Three

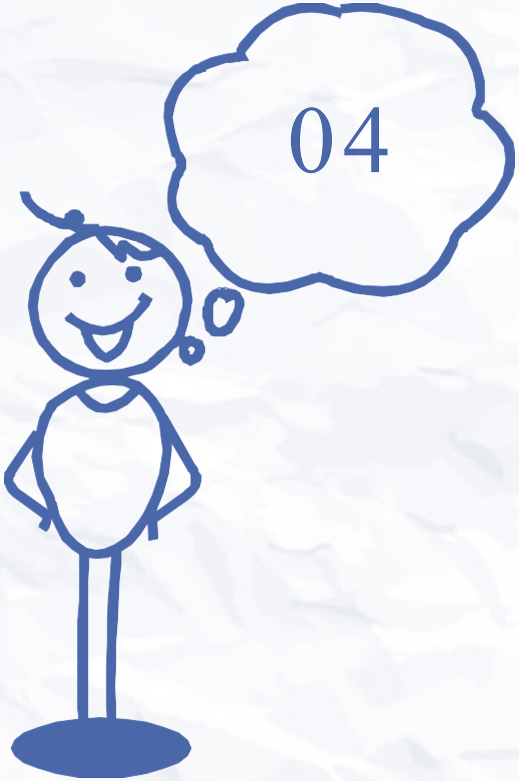
The impact of Docker Container

Container as a service

Docker container uses cgroups technology to greatly reduce the granularity of control system resources, thereby greatly improving the utilization of system resources.

Now public cloud service providers can completely migrate these applications to containers, which can not only reduce resource overhead, but also provide better portability.

Another advantage that the CaaS model brings to enterprises is that CaaS enables enterprises to easily and dynamically migrate services between different public cloud platforms without worrying about platform lock-in issues.



PART Four

Prospects for the development trend of containers

单击此处添加标题

1

Containers and virtualization technologies will coexist

2

Running containers in virtual machines will become a trend

3

The era of container-centric cloud computing is about to begin

Reference

The development track of modern cloud computing from the perspec-tive of container and Kubernetes technology [EB/OL]. [2016-10-16]. http://dockone.io/article/140. (The development track of modern cloud computing from container and Kubernetes Technology[EB/OL].[2016-10-16]. http://dockone.io/article/140.)

Wu Zhixue. Introduction to Cloud Computing: Concepts Frameworks and Applications[M]. Beijing: People’s Posts and Telecommunications Press, 2016: 43 -52. (WU Z X. Introduction to Cloud Computing: Concepts Frameworks and Applications[M]. Beijing : Posts and Telecom Press, 2016: 43 -52.)

IBM virtualization and cloud computing group. Virtualization and cloud computing[M]. Beijing: Publishing House of Electronics Industry, 2010. (IBM virtualization and cloud computing group. Virtualization and Cloud Computing[M]. Beijing: Publishing House of Electronics Industry, 2010.)

PRATT I, FRASER K, HAND S, et al. Xen 3.0 and the art of virtualization[J]. Proceedings of the Ottawa Linux Symposium, 2005, 36 (5): 164-177.

Ma Bofeng. VMware, Citrix and Microsoft Virtualization Technology Explanation and Application Practice[M]. Beijing: Mechanical Industry Press, 2013. (MA B F. VMware, Citrix and Microsoft Virtualization Technology Explanation and Application Practice[M]. Beijing: China Machine Press, 2013.)

KIVITY A, KAMAY Y, LAOR D, et al. KVM: the Linux virtual machine monitor[EB/OL].[2016-03-10]. https://www.kernel.org/doc/ols/ 2007/ols2007v1-pages-225-230.pdf.

ROSEN R. Linux Kernel Networking: Implementation and Theory[M]. Berkeley: Apress, 2014: 405 -482.
Wang Kai, Zhang Gongxuan, Zhou Xiumin. Research on Virtualization Technology Based on Containers [J]. Computer

Thanks For Listening

Leave Questions on Discussion