Session 07

Key Management and Distribution

CS 7349

Spring 2024

World Changers Shaped Here

SMU

© Shaibal Chakrabarty

Contents

- Security News of the Week
- House Keeping
- Class Presentation
- Concepts: Quick review
- Symmetric and Public Key Exchange
- Digital Certificates

Sources: YouTube/Dr. Dan Boneh, Cryptography 1; Cryptography and Network Security, William Stallings;

House Keeping

- Status of Teams for Term Paper? Topic?
- Research Paper submit Jan deliverables now;
- Checkpoint on 02/15, 02/19
- Quiz3/4 published; Case Study published
- Focus on Case Study and Research paper – 3 pages due
- RED ALERT on Research Paper! Track!!

Weekend Recovery in Progress

Sources: Meta AI, brenqtressa.pages.dev

Security News of the Week – Spring 2024

- Security researcher charged with defrauding Apple out of $2.5 million, company thanks him two weeks later | TechSpot
  - Timely communication is key….2 lessons
- 10 must-read cybersecurity books for 2024 - Help Net Security
  - George Finney's, Project Zero Trust is listed (SMU CSO)
- https://www.nbcnews.com/tech/security/chinese-hackers-cisa-cyber-5-years-us-infrastructure-attack-rcna137706
  - Read the Joint Cybersecurity Advisory for vulnerabilities in OT/IoT

Source: techspot.com; helpnetsecurity.com;nbc.com

CS 7349 – Tying it all together

INTRODUCTION TO DS7349 AND THE THREAT LANDSCAPE	HASH FUNCTIONS	NETWORK SECURITY
INTRODUCTION TO NETWORKS	MESSAGE AUTHENTICATION CODES	SECURITY – CLOUD, WIRELESS/5G, DDoS, SASE, IoT, SDN, Smart Cities
SYMMETRIC KEY CRYPTO	KEY MANAGEMENT	FRAMEWORKS, STANDARDS, OPERATIONS, Governance/Risk/Compliance
USING SYMMETRIC KEY CIPHERS	IDENTITY AND ACCESS MANAGEMENT	REVIEW/ADDITIONAL TOPICS
RANDOMNESS AND PSEUDORANDOM NUMBERS		
PUBLIC KEY CRYPTO/Team Paper		

Confidentiality **Integrity** **Availability** **Networks/Application**

Spring schedule

Date	Week/Unit	Learning Material	Assignment
01/17/2024	1/1	Intro to Data and Network Security	Stallings Ch 1; Quiz#1;Start project team, select project and inform instructor
Jan 22, 24	2/2	Intro to Computer Networks	Submit Quiz #2; Project team confirms problem with instructor/Homework 1 issued/Term paper checkpoint
Jan 29, 31	3/3	Symmetric Key Cryptography	Stallings Ch 2-3; Submit Quiz #3; First Project Draft (Title, authors, abstract and Intro)/
Feb 5, 7	4/4	Using Symmetric Key Ciphers	Stallings Ch 3-6; Submit Quiz#4 (ch03 and ch06); Homework #2 issued
Feb 12, 14	5/5	Randomness and Pseudorandom Numbers	Stallings Ch 7; Submit Quiz #5/Term Paper Checkpoint
Feb 19, 21	6/6	Public Key Cryptography	Stallings Ch 9-10; Submit Quiz #6/Case Study Due/
Feb 26, 28	7/7	Hash Functions/	Stallings Ch 11; Submit Quiz #7; Paper Interim Draft; Exam 1 issued
Mar 4, 6	8/8	Message Authentication Codes	Stallings Ch 12; Submit Quiz#8;
Mar 11, 13	9/9	SPRING BREAK!!!	
Mar 18, 20	03/10	Key Management and Key Distribution	Stallings Ch 14; Submit Quiz #10/Term paper checkpoint/Start on project presentation/Case Study
Mar 25, 27	04/11	User Authentication	Stallings Ch 15; Submit Quiz #11/
Apr 1, 3	12/12	Network Security	Stallings Ch 17; Submit Quiz #12; Presentation check/Exam #2
Apr 8, 10	13/13,14	Privacy, Security Ethics	
Apr 15, 17	14	Applications: AI and Quantum Computing	Submit Final Project Paper
Apr 22, 24	15	Open	Presentations of Term Project by class/
Apr 29		Wrap up and Review	
This schedule is subject to changes. All assignments are due by 11:59pm of the due date. Earlier submissions are encouraged and welcome. Do not wait till the last moment.			
You will have 2 weeks to complete most assignments.			

Book: Cryptography and Network Security by William Stallings, 8th edition

Class Presentation - Special Topic

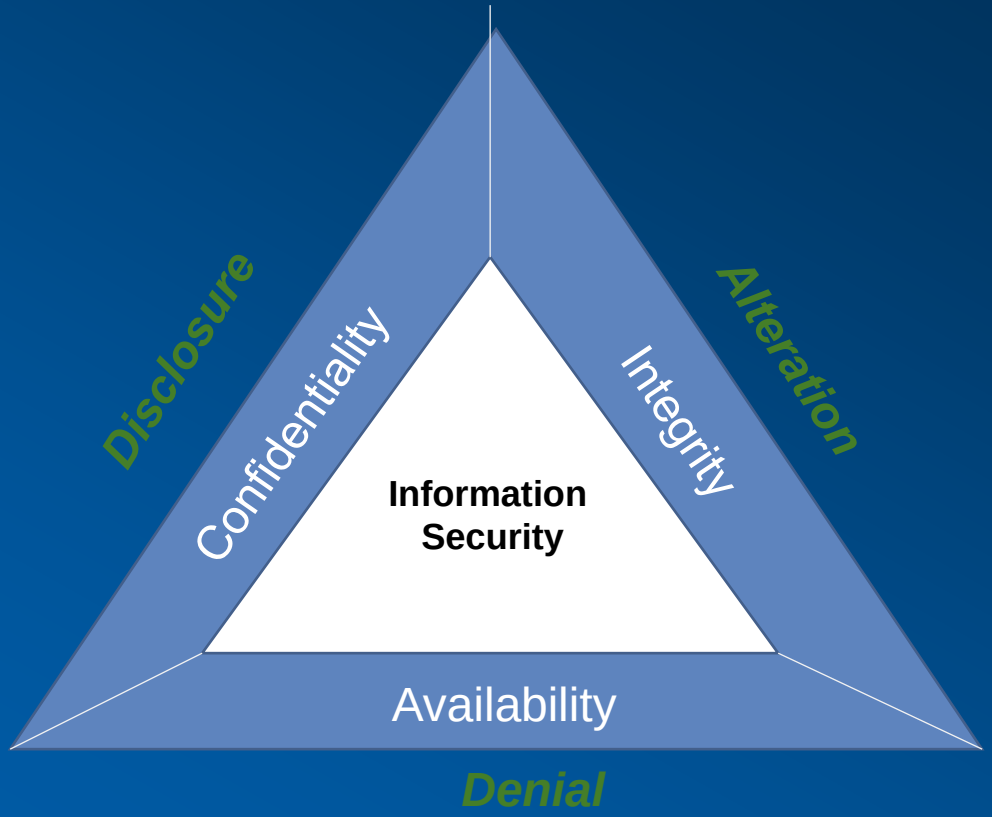
- Any topic of your interest: Work, ~~school~~, play
  - Can be a question/answer, wonderment, information
  - **Security related; NOT term paper related; NO course topic**
  - Strict time limits 5 mins + 3 mins Q&A
- Schedule – as per roster
  - ~~Adu, Aliliele~~, ~~Braden~~, ~~Cho~~, ~~Dominguez~~, ~~Garcia~~, Garza, Gibbs, Guo, Hennes, Jackson, Kharwadhkar, Kucera, Lei, Liang, Lim, Lin, Liu, Magee, Mandalaneni, Mathew, Miller, Nagamanickam, DPatel, PPatel, Pittman, Sanaboyina, Singh, Skochdopole, Swigart, Taghavi, Wang, Werth, Zhai

Project Timeline (For 9 page paper)

- Jan: First project draft 1 page, basically your Introduction section, plus title, authors and abstract, some references
- Feb: Interim draft 3 pages, basically your intro and related work, plus basic description of your solution
- Mar: Draft 6 pages. Detailed solution, analysis, references
- Apr: Final paper 9 pages. Submit, with presentation

A LaTex template and example paper will be provided

InfoSec, CIA, Threats



Source: “Information Security Illuminated”, Solomon and Chapple, 2005, Sudbury, MA:Jones and Bartlett.

Network Security Basics

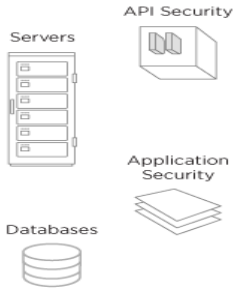
The IT Security Chain

upwork™

The more links in your network's chain—databases, cloud-based servers, APIs, and mobile applications—the more potential vulnerabilities you face. Here's an overview of areas of IT security to consider.

IT Security

NETWORK SECURITY



- Security Engineering
- Vulnerability Testing
- Penetration Testing
- Network Intrusion Detection Systems (NIDS)
- Firewalls

INTERNET SECURITY

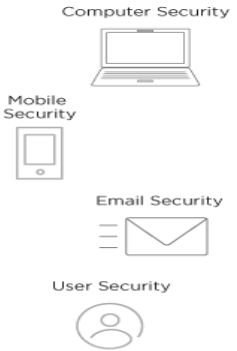
- HTTPS
- SSL Certificates
- OAuth 2.0

CLOUD SECURITY

- OAuth 2.0
- Web Sockets

WIRELESS SECURITY

END POINT SECURITY



- VPNs
- Encryption
- Anti-Malware

Source: Upwork Global, Inc

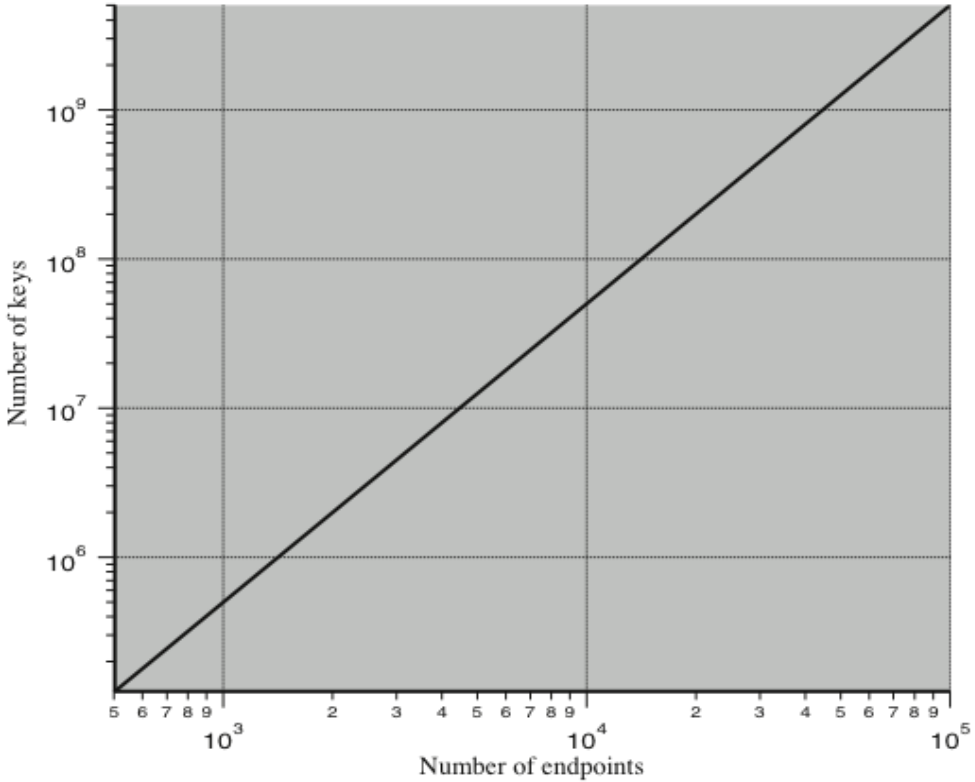
Overview – Key distribution

- Burning questions?
- Key Distribution
  - Symmetric KD using symmetric encryption
  - Symmetric key distribution using asymmetric encryption
  - Public Key Distribution

Symmetric Key Distribution

Given parties A and B, key distribution can be achieved in a number of ways:

- **A can select a key and physically deliver it to B**
- **A third party can select the key and physically deliver it to A and B**
- **If A and B have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key**
- **If A and B each has an encrypted connection to a third party C, C can deliver a key on the encrypted links to A and B**



N entities means N(N-1)/2 symmetric keys

Figure 14.1 Number of Keys Required to Support Arbitrary Connections Between Endpoints

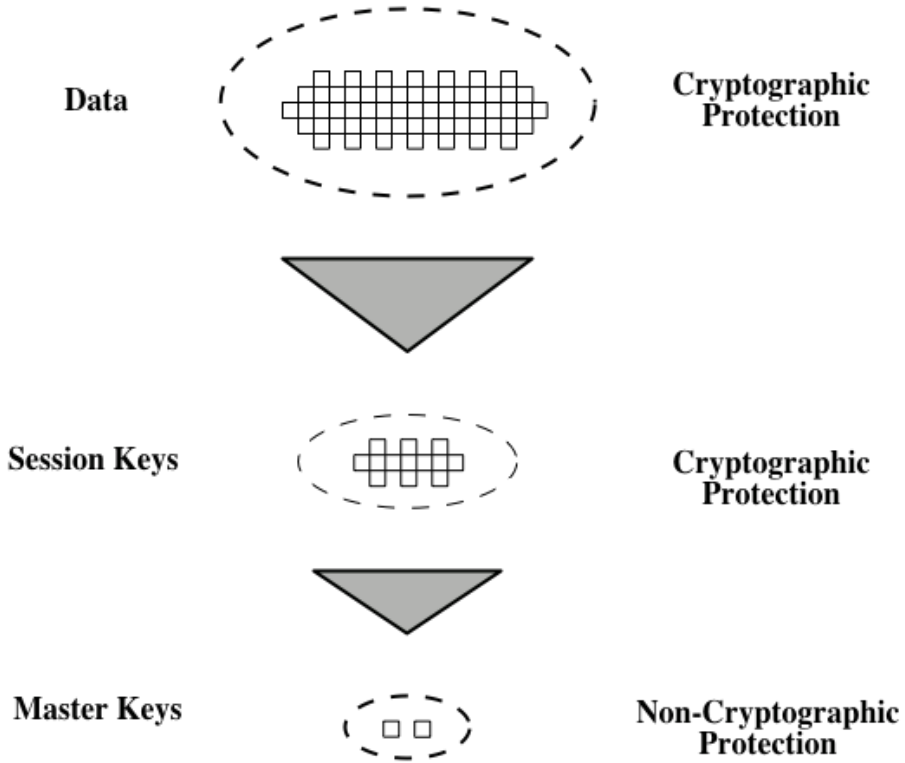


Figure 14.2 The Use of a Key Hierarchy

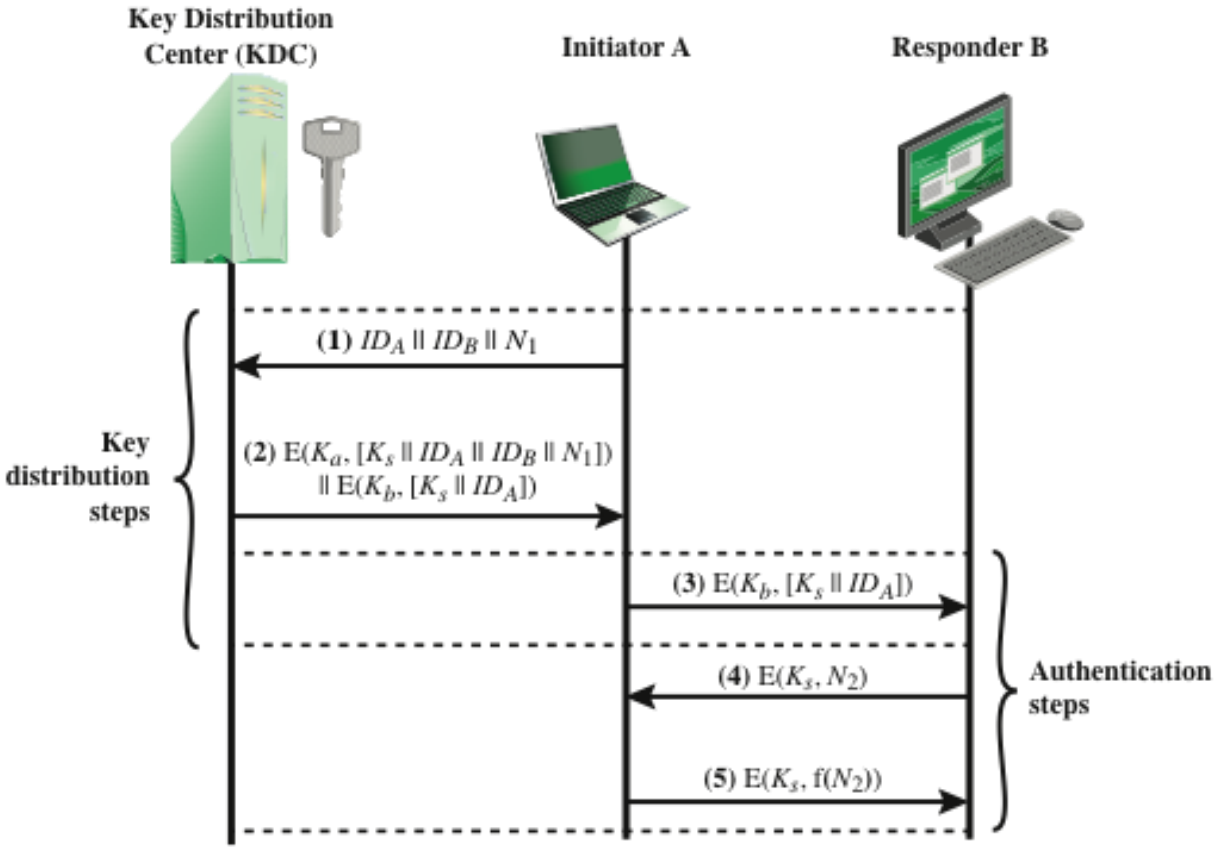


Figure 14.3 Key Distribution Scenario

KDC Other

- Hierarchical KDCs (local, regional, global)
- Key Lifetimes: per session, per transactions
  - Connection Oriented, Connectionless
- Categorizing key usage: Separation
  - Type: Master keys, Session Keys
  - Usage: Data Encryption key, Pin-encryption key; File encryption key

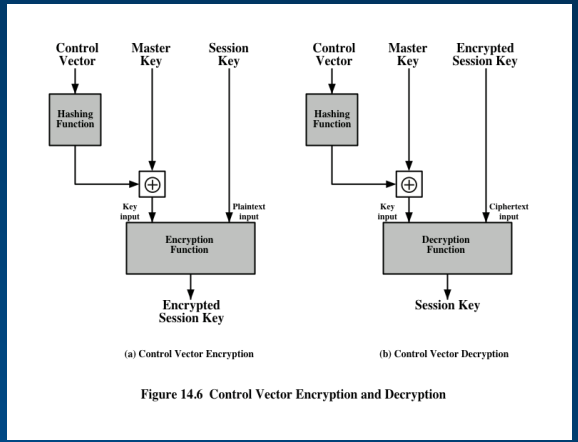


Figure 14.6 Control Vector Encryption and Decryption

Key Distribution using PKC

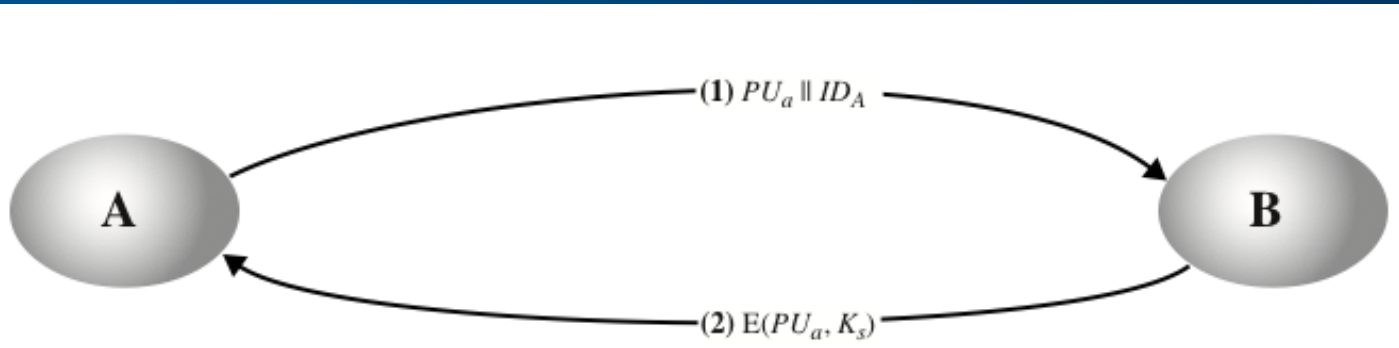


Figure 14.7 Simple Use of Public-Key Encryption to Establish a Session Key

Vulnerability

Meet-in-the-Middle Attack

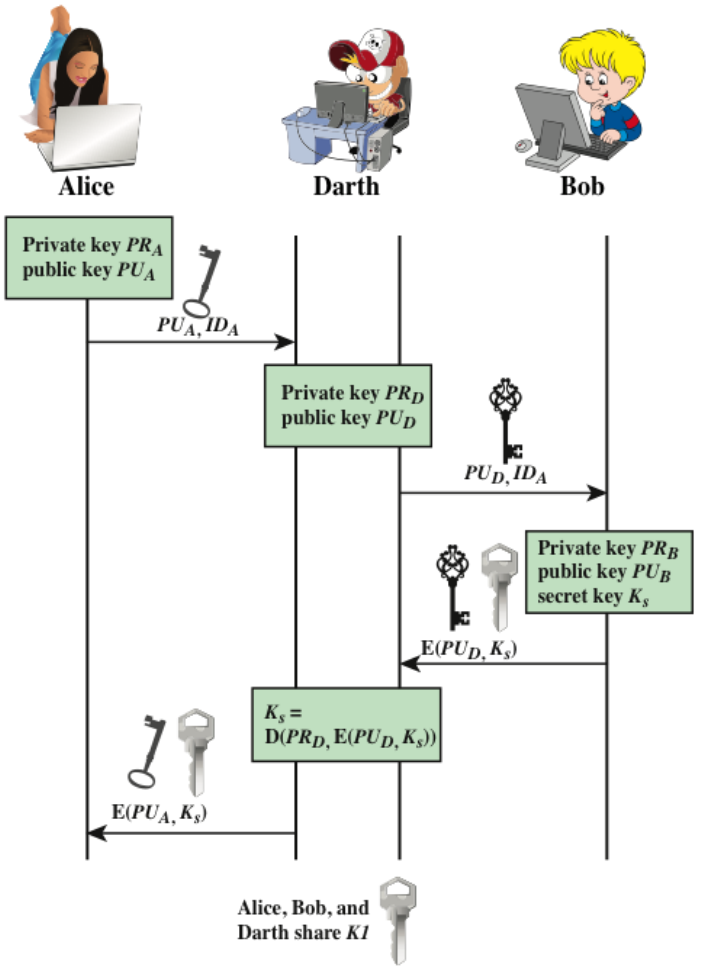
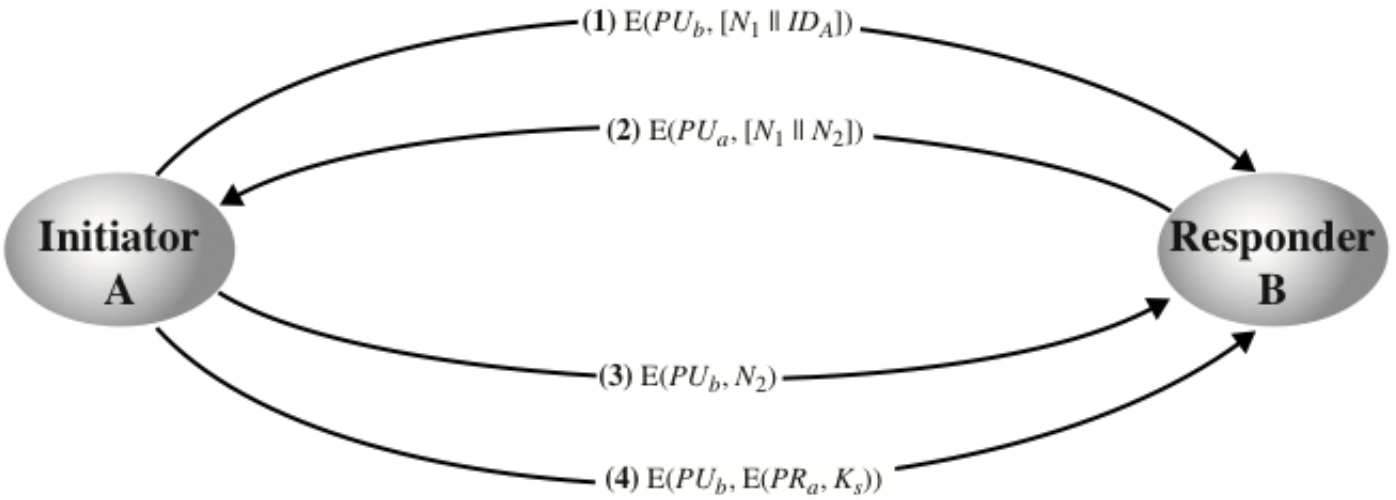


Figure 14.8 Another Man-in-the-Middle Attack

Secret Key Distribution with Confidentiality and Authentication



Confidentiality and Authentication with no TTP

Figure 14.9 Public-Key Distribution of Secret Keys

Distribution of Public Keys

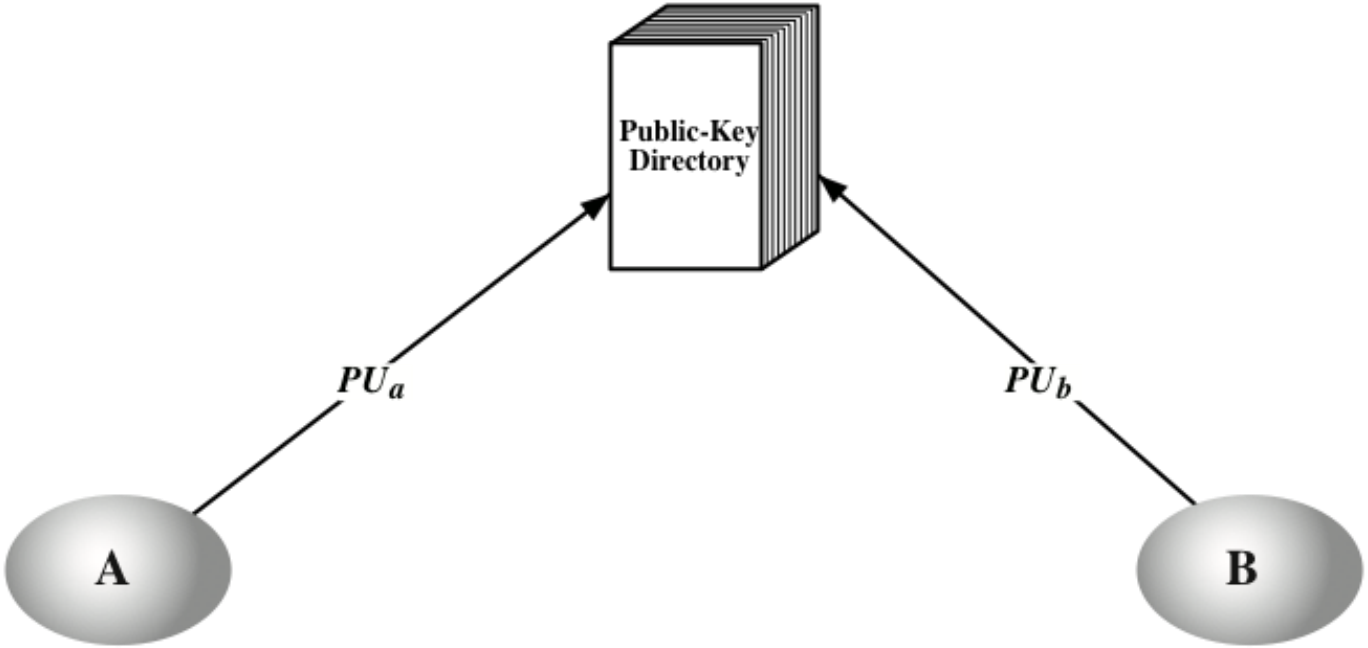
Public Key distribution can be grouped into the following schemes:

Public Announcement

Masquerade

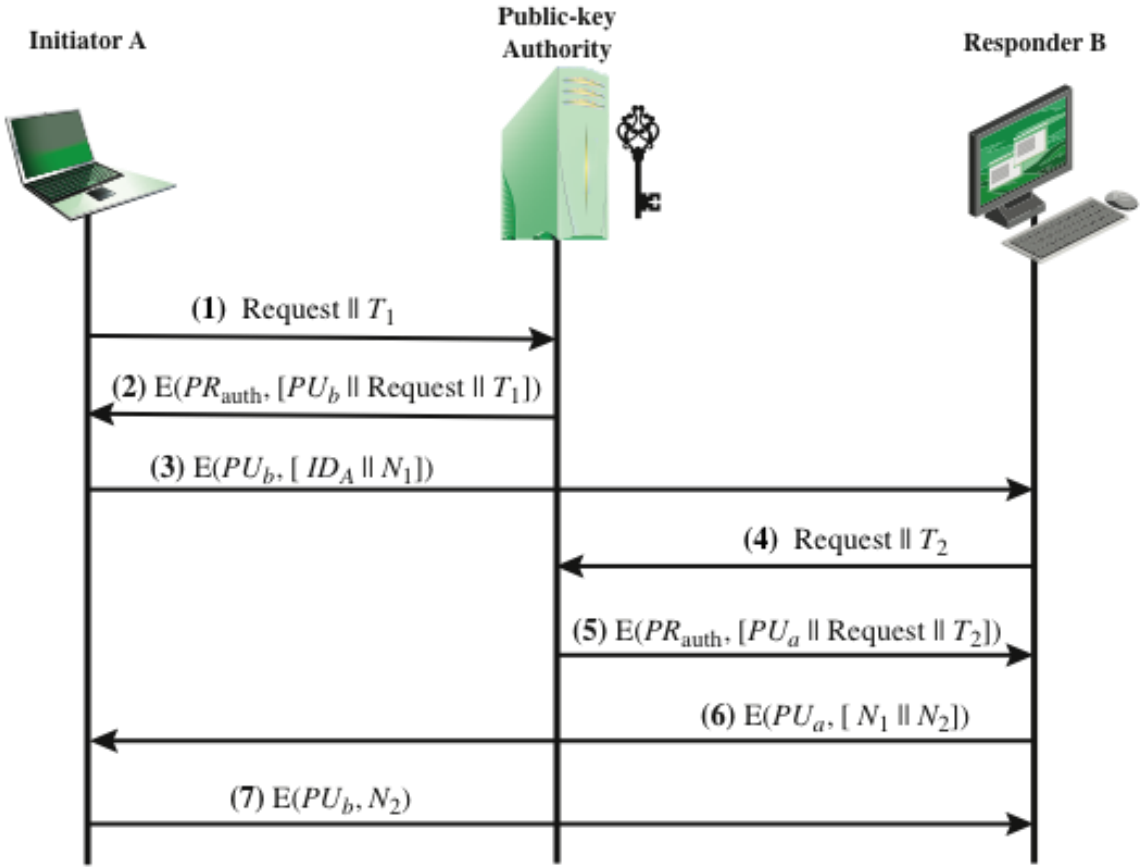
Figure 14.10 Uncontrolled Public Key Distribution

Publicly Available Directory



Single point of failure

Figure 14.11 Public Key Publication



Mitigates Masquerade attacks

Figure 14.12 Public-Key Distribution Scenario

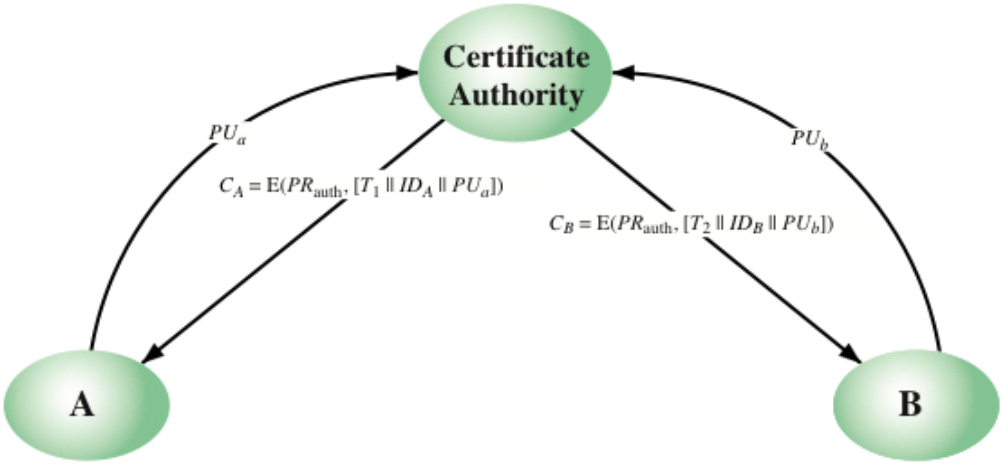
Digital Certificates

- ITU-T Recommendation X.509
  - http://www.itu.int/itu-t/recommendations/rec.aspx?rec=X.509
- Maintained and updated by SG-17 (Study Group 17)
- “Recommendation ITU-T X.509 | ISO/IEC 9594-8 defines frameworks for public-key infrastructure (PKI) and privilege management infrastructure (PMI). It introduces the basic concept of asymmetric cryptographic techniques. It specifies the following data types: public-key certificate, attribute certificate, certificate revocation list (CRL) and attribute certificate revocation list (ACRL). It also defines several certificates and CRL extensions, and it defines directory schema information allowing PKI and PMI related data to be stored in a directory. In addition, it defines entity types, such as certification authority (CA)……..”

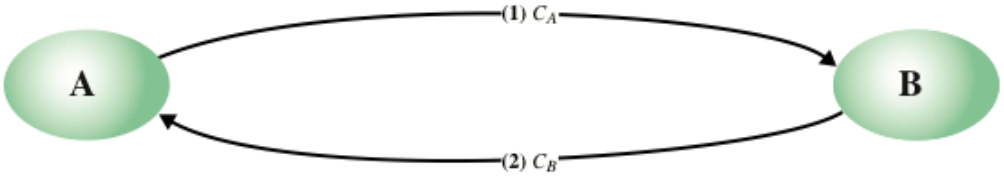
Digital Certificates

- Types of Digital Certificates
  - Secure Socket Layer certificate [SSL]
    - Server: mail, directory, LDAP or web
  - Software Signing [Code Signing certificate]
    - Authenticate software or downloaded code
  - Client Certificate
    - Digital IDs. Authenticate entity (bind entities: D2D)
  - Digital Signature
    - Authenticate documents, files and emails

- https://www.youtube.com/watch?v=hq56tXhTnLg



(a) Obtaining certificates from CA



(b) Exchanging certificates

Figure 14.13 Exchange of Public-Key Certificates

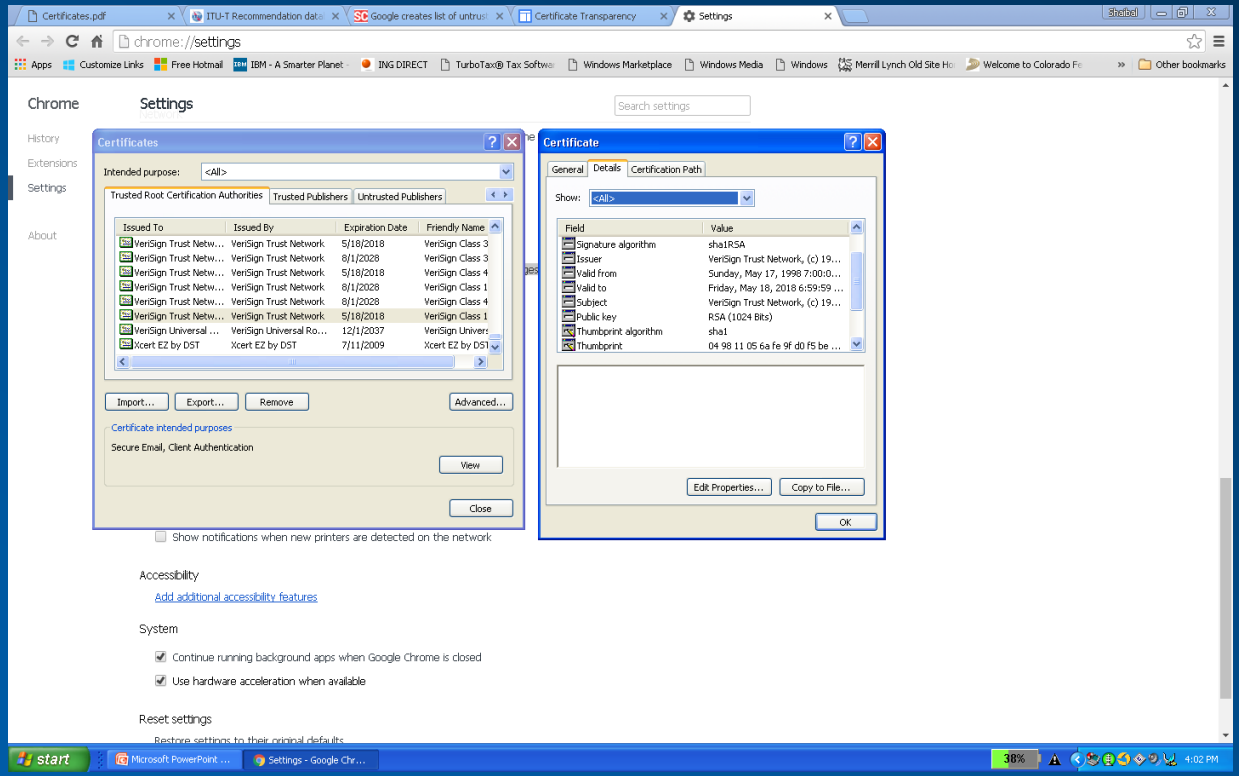
Certificate Authority

- Bad boys - Untrusted CA's
- https://www.certificate-transparency.org/what-is-ct
  - Opensource project creating a blacklist of untrusted CA's.
- No efficient auditing or monitoring SSL certificates in real time
  - Days, weeks or months to detect forged or improper certs
- DigiNotar was compromised and the hackers were able to use the CA's system to issue fake SSL certificates, allowing the entity to monitor traffic on networks.
- TrustWave admitted that it issued subordinate root certificates to one of its customers so the customer could monitor traffic on their internal network

Certificate Authority

- Worse – Improper implementation of Untrusted CA's
  - https://www.csoonline.com/article/3000574/security/the-sorry-state-of-certificate-revocation.html
- Cunning - Steal CA's and sign your malware
  - https://www.computerworld.com/article/3044728/security/cyberespionage-groups-are-stealing-digital-certificates-to-sign-malware.html

Example Digital Certificate



Public Key Infrastructure (PKI) – X.509

- **End entity**: A generic term used to denote end users, devices (e.g., servers, routers), or any other entity that can be identified in the subject field of a public-key certificate. End entities typically consume and/or support PKI-related services.

- **Certification authority (CA)**: The issuer of certificates and (usually) certificate revocation lists (CRLs). It may also support a variety of administrative functions, although these are often delegated to one or more Registration Authorities.

- **Registration authority (RA)**: An optional component that can assume a number of administrative functions from the CA. The RA is often associated with the end entity registration process but can assist in a number of other areas as well.

- **CRL issuer:** An optional component that a CA can delegate to publish CRLs.

- **Repository**: A generic term used to denote any method for storing certificates and CRLs so that they can be retrieved by end entities.

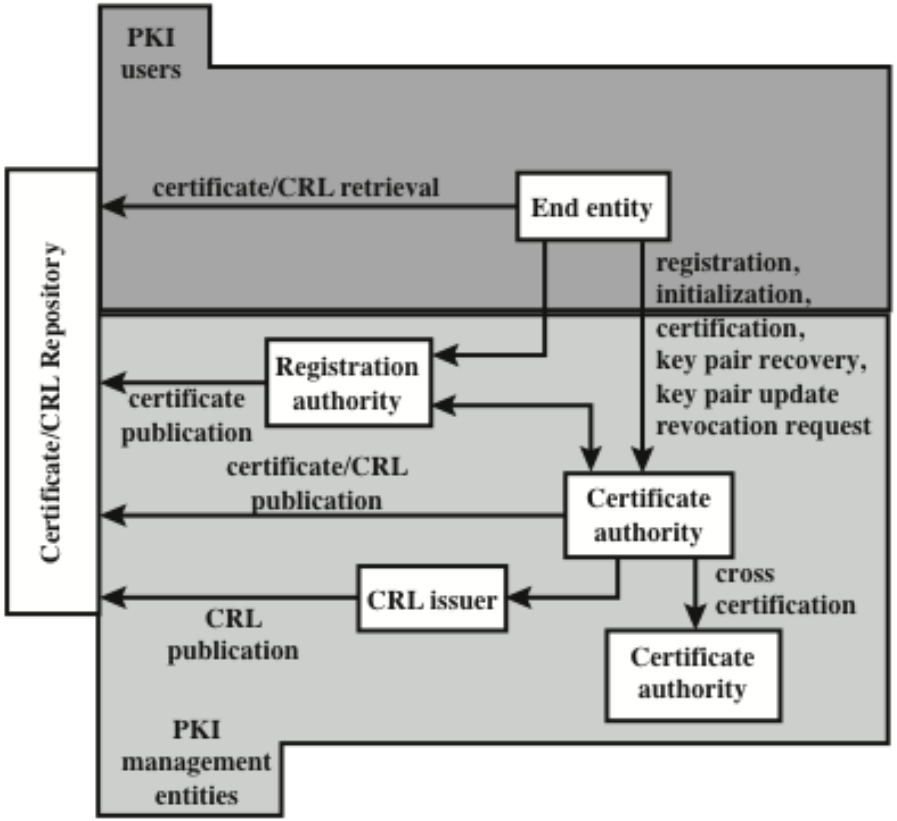


Figure 14.17 PKIX Architectural Model

PKIX Management Functions

- Registration
- Initialization
- Certification
- Key pair recovery
- Key pair update
- Revocation request
- Cross certification

Summary

- Key Management and Distribution is the most complex and intricate part of security networks and systems.
- Digital Certificates are essential to key distribution
- Key Management includes: Key Generation; Key Transfer; Key Verification; Key Usage; Key Updates; Key Storage; Key Backup; Compromised Keys; Key Expiry; Key Revocation

Thank You!

World Changers
Shaped Here

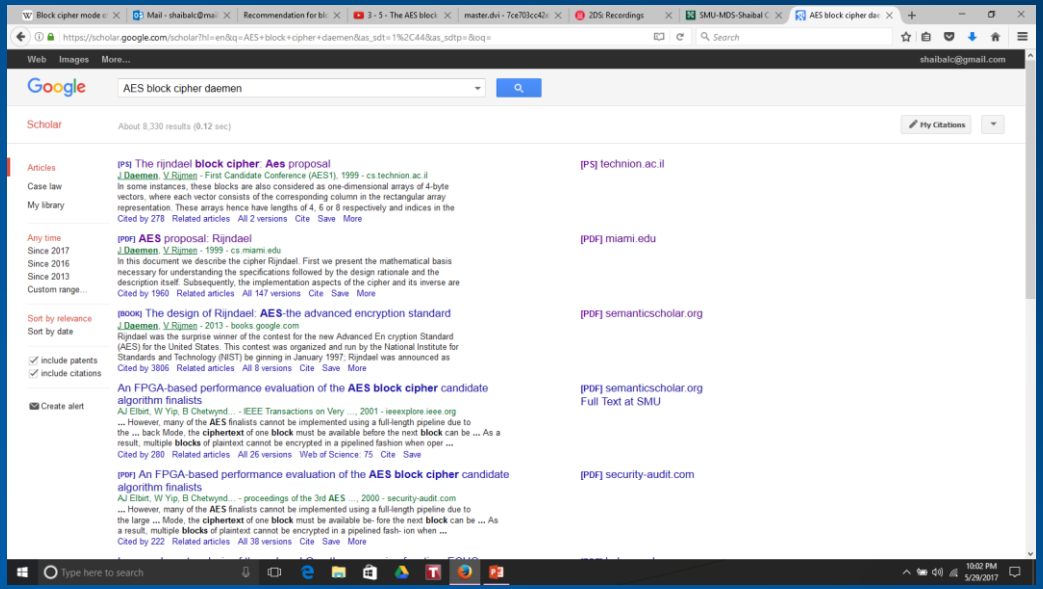
SMU®

Project – 1st deliverable

- Team projects (3 per team)
- Choose topic (from topic list or your own)*
- Within topic, identify problem to be addressed (no survey projects, only problem solving projects - survey is a part of your problem solution and is contained in the final paper)
- Confirm problem with professor

Peer reviewed publications

- https://scholar.google.com/
- Get your references from here, and download IEEE, ACM and other papers from CUL. (http://www.smu.edu/cul)



Example: Case Study

Following are the questions for Case Study 1. Your response expectations are outlined per question. Your reading is the Radware Global Application and Security Report for 2017-2018, and a review of the AT&T Cybersecurity Insights Report (Vol 6) online. Please find these reports using google. (https://www.business.att.com/solutions/Portfolio/cybersecurity/cybersecurity-resources/page=addl-info/?gc=cybersecurity-report/v6/index.html#resource)

1. What are the differences AND similarities between these reports? Understand that the two companies are different domains but both are in the business of IT Security. Please outline your responses CLEARLY, in your own words, in a MINIMUM of 1 page. This will help you compare and contrast multiple cybersecurity reports.

2. In the Radware report, please identify 3 emerging cybersecurity trends (either attacks and/or defense) in 2017. What was the business impact, and projected business impact of these trends? (business impact can include loss in $; loss in reputation; restructuring and new investments; executive departures, brand and reputation loss). A MINIMUM of 1 page is expected. This will help you look for business impact in general if you were a CIO or CSO, and put forth policies to mitigate loss.

3. From the Radware report, please summarize four (4) 2017 incidents and their impact. These are specific attacks and their business impact. (a) what was the incident (b) how did the incident occur? (what vulnerability was exploited) (c) how was the vulnerability fixed (if at all, or if a fix was in place and not put in) (d) what was the impact? ($ loss, reputation, restructuring, etc). A MINIMUM of 1 page is expected. This will bring you up to speed on the top cybersecurity incidents of 2017.

4. What do the Radware report and the AT&T report outline as next steps, forward looking trends and expectations for 2018. 2 trends from Radware and 2 trends from AT&T are requested. The goal is to compare the focus from 2 different companies, in different domains, looking at the same problem of how to secure IT in enterprises. A MINIMUM of 1 page is expected.

4. What do the Radware report and the AT&T report outline as next steps, forward looking trends and expectations for 2018. 2 trends from Radware and 2 trends from AT&T are requested. The goal is to compare the focus from 2 different companies, in different domains, looking at the same problem of how to secure IT in enterprises.

According to the report Radware 2 Trends:

1. Blockchain:
   With AI weaponizing and automated social engineering efforts, Blockchain can help with the additional level of security. Blockchain can help make cloud computing more secure
- Ensure that services and applications are less centralized in DNS and other public services
- Will be more secure and resistant with censorship and governance, since blockchain provides additional level of security which can prove difficult to infiltrate.
- Can ensure about 51% security with cryptocurrencies transactions with the number of networks that blockchain is specialized in

2. FaaS- Serverless Computing:
- Serverless tends to more secure than traditional architecture
- Eliminates server poisoning
- Makes the attack surface significantly larger which reduces the chances of being infected.
- Making the outdated legacy security solutions irrelevant which makes brute force or social engineering threats irrelevant
- Chances of DDoS attacks to be affected tends to zero

According to At&T report, the 2 trends:

1. Expand CyberRisk Assesment program
- Organizations to implement feedback loop between cybersecurity and a risk management strategy
- Gather information about daily threat activity and response
- Evaluate cybersecurity situation of third party consultant
- Investment in cyber-insurance and cybersecurity separately
- Testing the methods and analyzing the flaws can help with the assessment and suggest improvement strategies to increase security

2. Invest Strategically:
- Apt defense tools and adapt apt mitigation plans and invest in
- Undertake CyberInsurance
- Create right balance between prevention, detection and remediation
- Keep up with current technologies- adapt to threat analytics, cloud cybersecurity solutions and machine learning
- Constantly fine tune investment strategies and try to fill in gaps for your organization
- As much as inhouse training of the employees or team is essential, so is investing smartly in third party tools and consultancy services.
- Mandate Awareness training can reduce the manual error probability

Example: Case Study

Following are the questions for Case Study 1. Your response expectations are outlined per question. Your reading is the Radware Global Application and Security Report for 2017-2018, and a review of the AT&T Cybersecurity Insights Report (Vol 6) online. Please find these reports using google. (https://www.business.att.com/solutions/Portfolio/cybersecurity/cybersecurity-resources/page=addl-info/?gc=cybersecurity-report/v6/index.html#resource)

1. What are the differences AND similarities between these reports? Understand that the two companies are different domains but both are in the business of IT Security. Please outline your responses CLEARLY, in your own words, in a MINIMUM of 1 page. This will help you compare and contrast multiple cybersecurity reports.

2. In the Radware report, please identify 3 emerging cybersecurity trends (either attacks and/or defense) in 2017. What was the business impact, and projected business impact of these trends? (business impact can include loss in $; loss in reputation; restructuring and new investments; executive departures, brand and reputation loss). A MINIMUM of 1 page is expected. This will help you look for business impact in general if you were a CIO or CSO, and put forth policies to mitigate loss.

3. From the Radware report, please summarize four (4) 2017 incidents and their impact. These are specific attacks and their business impact. (a) what was the incident (b) how did the incident occur? (what vulnerability was exploited) (c) how was the vulnerability fixed (if at all, or if a fix was in place and not put in) (d) what was the impact? ($ loss, reputation, restructuring, etc). A MINIMUM of 1 page is expected. This will bring you up to speed on the top cybersecurity incidents of 2017.

4. What do the Radware report and the AT&T report outline as next steps, forward looking trends and expectations for 2018. 2 trends from Radware and 2 trends from AT&T are requested. The goal is to compare the focus from 2 different companies, in different domains, looking at the same problem of how to secure IT in enterprises. A MINIMUM of 1 page is expected.

QUESTION #4 - What do the Radware report and the AT&T report outline as next steps, forward looking trends and expectations for 2018.

With its technically astute target audience in mind, the Radware report focuses more heavily on the leading technological aspects of which to be aware. From Radware's perspective, automation is the central theme heading into 2018, with automated technology processes centered in the crosshairs. 2017 yielded strikingly new attack methods. For instance, the Brickerbot botnet coming to light demonstrated the reality of permanent denial of service attacks (PDoS) in which a "software-based botnet" can raze an IoT device's firmware and even wreck its core system functionality, thereby permanently disabling the physical device. Sooner rather than later, the pairing of PDoS with automation will mature well beyond the rudimentary use of automation by the WannaCry and NotPetya ransom attacks in 2017. Two of the four areas that Radware urges the reader to pay particular attention to and prepare for are AI weaponization and automated social engineering. AI is discussed in the Radware report as a new type of weapons race that, in essence, fights AI with AI. It is also a race characterized by striving to be the first to find one's own vulnerabilities (i.e. as a company, nation, etc.) and those of one's adversaries, using AI to thwart incoming AI-based attacks, and even achieving major AI breakthroughs. The Radware report also expects that the automation of cyber-based social engineering attacks will only become more prevalent. Social engineering-based assaults, which essentially employ psychological manipulation techniques, based on the typical tendencies of human nature, to deceive a target into sharing private information or into doing something on the trickster's behalf, are nothing new. With automation though, the well-known, lower-tech versions, such as phone calls by impersonators and phishing email campaigns, can be executed much more rapidly and on a much larger scale. Radware leaves the reader with food for thought as questions to keep in mind as organizations endeavor to thwart, manage and recover from cyber attacks. The reader is invited to think about what new types of attacks could surface as a result of the increasing use of automation, along with what tools and methodologies organizations could create to offer protection. The threat of automated attacks cannot be underestimated in a climate where it is not uncommon for IoT devices to be implemented in insecure modes, thereby facilitating automated attacks.

Based on the AT&T survey, the ongoing or "persistent" threats that respondents were chiefly still concerned about were corporate data being accessed and vulnerability to malware. The AT&T report identifies emerging threats, about which its survey participants were most concerned, as the increasing risks related to the following: IoT, mobile device vulnerability, successful malware attacks inflicting irreversible damage to customers and the firm, and ransomware. In fact, ransomware ranked first as the number one concern for the healthcare sector. Looking forward in terms of industry preparation, nearly half of AT&T survey respondents were already planning to increase their cyber security headcount in the upcoming year. At the same time, the report acknowledges the overall global trend toward using automation coupled with the cyber intelligence necessary for threat detection and alerting that goes beyond human capabilities. The AT&T report predicts that automation will ultimately support attack response and recovery functions. Without going into technical details, AT&T's risk-themed report focuses on the need for organizations to re-evaluate their cyber strategies on a regular basis in order to keep up with the ever-changing threats lurking in the cyber world, as well as highlights gaps (e.g. risk,

Project Reports

- **Use the LaTex template** provided for your project paper submissions.
- **Read** the Sample paper and **follow** its directions as appropriate in writing your paper.
- Your paper is expected to be publishable
  - High quality research, well written, reproducible results based on paper contents.
- https://scholar.google.com/ for references (NOT cnn.com, foxnews.com, cnbc.com; YES ietf.org, ieee.org,…itu-t)

Project Abstract and Intro

- **Abstract** structure (125-150 word limit for 9 pages)
  - start with statement of what is presented (2 sentences)
  - motivate the problem (2-3 sentences)
  - discuss details of what is done at a high level (1-2 sentences)
  - state the main conclusions (1-2 sentences)
- **Introduction** basic structure (the rest of page 1):
  - motivate the problem further
  - state the problem in detail
  - state the basic work done/approach taken
  - State the contributions of your paper (2nd last paragraph)
  - state the outline for the rest of the paper (final paragraph)
    - Conclusions are not stated in the introduction.

Project Paper

- **Use the LaTex template** provided for all of your project paper submissions.
- Your paper is expected to be publishable
  - High quality research, well written, reproducible results based on paper contents. 9 pages exactly. No more, no less
  - https://scholar.google.com/ for references (NOT cnn.com, foxnews.com, cnbc.com; YES ietf.org, ieee.org,…itu-t)
  - https://www.overleaf.com/read/brpdfvsxsjww#8886a4 ←Paper template