Session 08

Checkpoint

CS 7349

Spring 2024

World Changers
Shaped Here

SMU

© Shaibal Chakrabarty

Contents

- Security News of the Week
- House Keeping
- Class Presentation
- Concepts: Quick review

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 02/14, 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 still in Progress

Sources: Meta AI

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

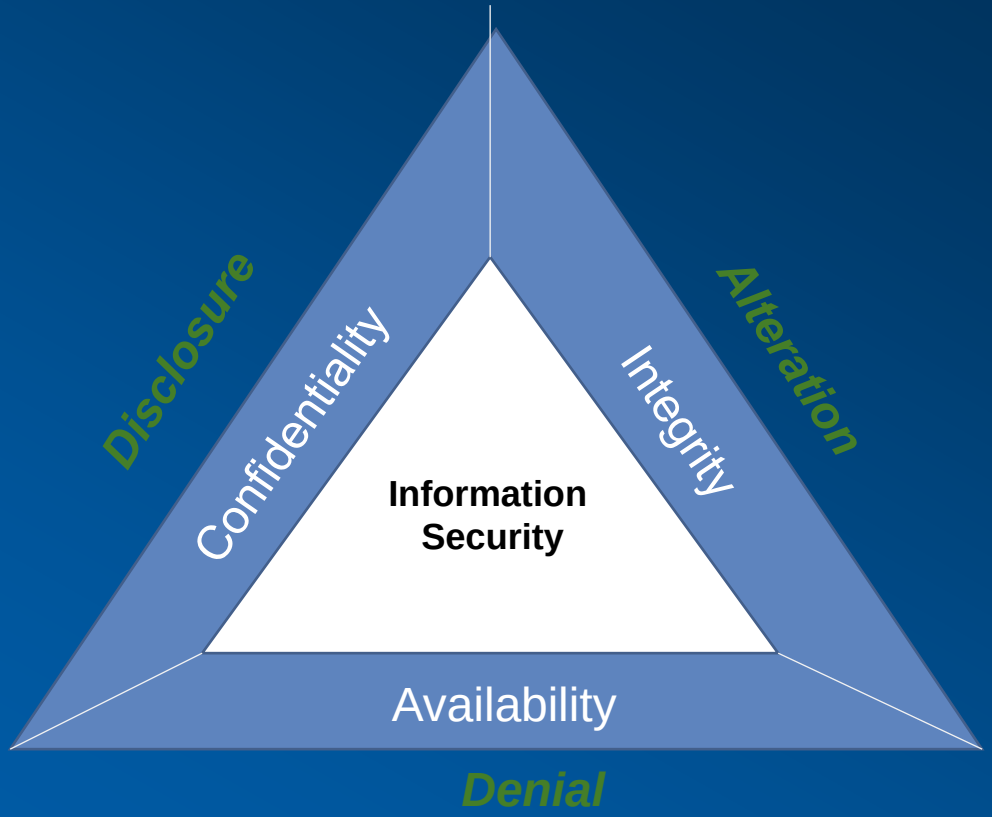
- Any topic of your interest: Work, ~~school~~, play
  - Can be a question/answer, wonderment, information
  - **Security related; NOT term paper related; NO course topic**
  - Strict time limits 5 mins + 3 mins Q&A
- Schedule – as per roster
  - ~~Adu, Aliliele~~, ~~Braden~~, ~~Cho~~, ~~Dominguez~~, ~~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

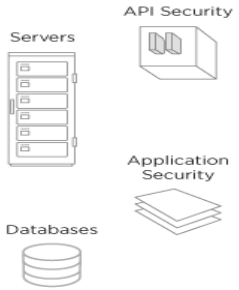
The IT Security Chain

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

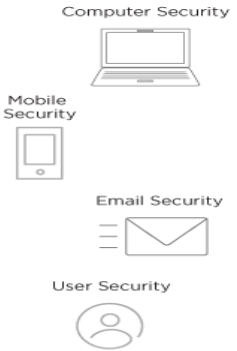
- HTTPS
- SSL Certificates
- OAuth 2.0

CLOUD SECURITY

- OAuth 2.0
- Web Sockets

WIRELESS SECURITY

END POINT SECURITY



- VPNs
- Encryption
- Anti-Malware

Source: Upwork Global, Inc

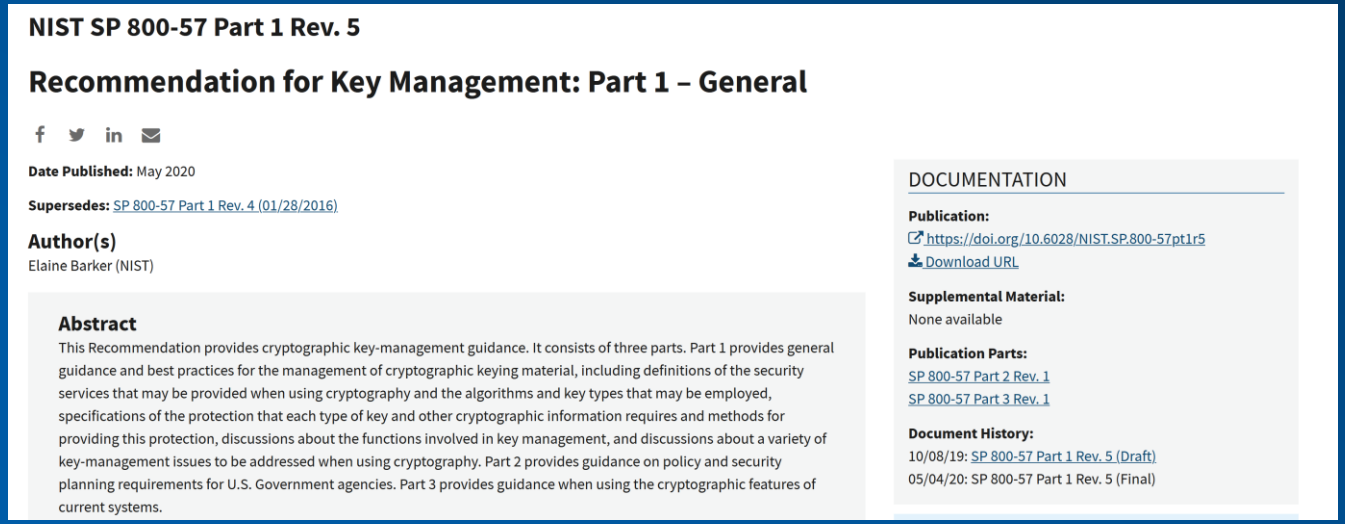
When in doubt – what must we do?

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**

Standards…

- https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final - NIST Management Recommendation



NIST SP 800-57 Part 1 Rev. 5

Recommendation for Key Management: Part 1 – General

Date Published: May 2020

Supersedes: SP 800-57 Part 1 Rev. 4 (01/28/2016)

Author(s)
Elaine Barker (NIST)

Abstract
This Recommendation provides cryptographic key-management guidance. It consists of three parts. Part 1 provides general guidance and best practices for the management of cryptographic keying material, including definitions of the security services that may be provided when using cryptography and the algorithms and key types that may be employed, specifications of the protection that each type of key and other cryptographic information requires and methods for providing this protection, discussions about the functions involved in key management, and discussions about a variety of key-management issues to be addressed when using cryptography. Part 2 provides guidance on policy and security planning requirements for U.S. Government agencies. Part 3 provides guidance when using the cryptographic features of current systems.

DOCUMENTATION

Publication:
https://doi.org/10.6028/NIST.SP.800-57pt1r5
Download URL

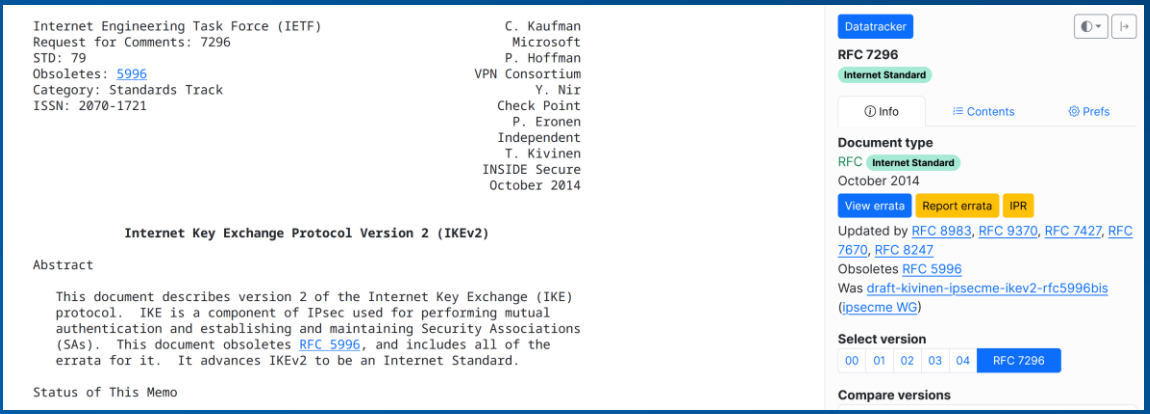
Supplemental Material:
None available

Publication Parts:
SP 800-57 Part 2 Rev. 1
SP 800-57 Part 3 Rev. 1

Document History:
10/08/19: SP 800-57 Part 1 Rev. 5 (Draft)
05/04/20: SP 800-57 Part 1 Rev. 5 (Final)

Source: nist.gov

Standards…cont



Internet Engineering Task Force (IETF)
Request for Comments: 7296
STD: 79
Obsoletes: 5996
Category: Standards Track
ISSN: 2070-1721

C. Kaufman
Microsoft
P. Hoffman
VPN Consortium
Y. Nir
Check Point
P. Eronen
Independent
T. Kivinen
INSIDE Secure
October 2014

Internet Key Exchange Protocol Version 2 (IKEv2)

Abstract

This document describes version 2 of the Internet Key Exchange (IKE) protocol. IKE is a component of IPsec used for performing mutual authentication and establishing and maintaining Security Associations (SAs). This document obsoletes RFC 5996, and includes all of the errata for it. It advances IKEv2 to be an Internet Standard.

Status of This Memo

Datatracker

RFC 7296

Internet Standard

ⓘ Info | Contents | Prefs

Document type

RFC Internet Standard
October 2014

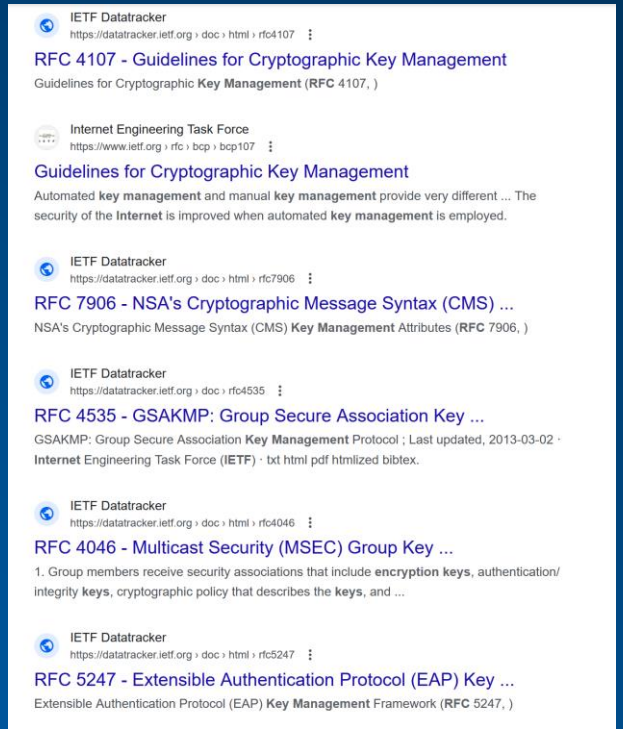
View errata | Report errata | IPR

Updated by RFC 8983, RFC 9370, RFC 7427, RFC 7670, RFC 8247
Obsoletes RFC 5996
Was draft-kivinen-ipsecme-ikev2-rfc5996bis (ipsecme WG)

Select version

00 | 01 | 02 | 03 | 04 | RFC 7296

Compare versions



IETF Datatracker
https://datatracker.ietf.org › doc › html › rfc4107

RFC 4107 - Guidelines for Cryptographic Key Management

Guidelines for Cryptographic **Key Management** (**RFC** 4107,)

Internet Engineering Task Force
https://www.ietf.org › rfc › bcp › bcp107

Guidelines for Cryptographic Key Management

Automated **key management** and manual **key management** provide very different ... The security of the **Internet** is improved when automated **key management** is employed.

IETF Datatracker
https://datatracker.ietf.org › doc › html › rfc7906

RFC 7906 - NSA's Cryptographic Message Syntax (CMS) ...

NSA's Cryptographic Message Syntax (CMS) **Key Management** Attributes (**RFC** 7906,)

IETF Datatracker
https://datatracker.ietf.org › doc › html › rfc4535

RFC 4535 - GSAKMP: Group Secure Association Key ...

GSAKMP: Group Secure Association **Key Management** Protocol ; Last updated, 2013-03-02 · **Internet** Engineering Task Force (**IETF**) · txt html pdf htmlized bibtex.

IETF Datatracker
https://datatracker.ietf.org › doc › html › rfc4046

RFC 4046 - Multicast Security (MSEC) Group Key ...

1. Group members receive security associations that include **encryption keys**, authentication/integrity **keys**, cryptographic policy that describes the **keys**, and ...

IETF Datatracker
https://datatracker.ietf.org › doc › html › rfc5247

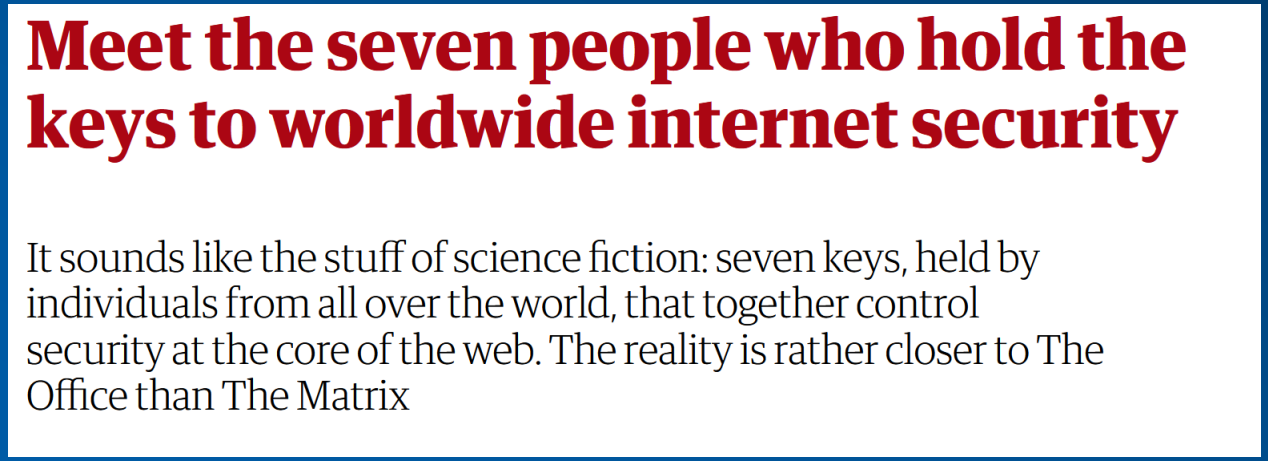
RFC 5247 - Extensible Authentication Protocol (EAP) Key ...

Extensible Authentication Protocol (EAP) **Key Management** Framework (**RFC** 5247,)

Source: ietf.org

Even Key Management! Hype vs Reality

- https://www.icann.org/en/blogs/details/the-problem-with-the-seven-keys-13-2-2017-en



Meet the seven people who hold the keys to worldwide internet security

It sounds like the stuff of science fiction: seven keys, held by individuals from all over the world, that together control security at the core of the web. The reality is rather closer to The Office than The Matrix

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.linkedin.com/advice/0/what-differences-similarities-between-x509-certificates-other - from LinkedIn

Thank You!

World Changers
Shaped Here

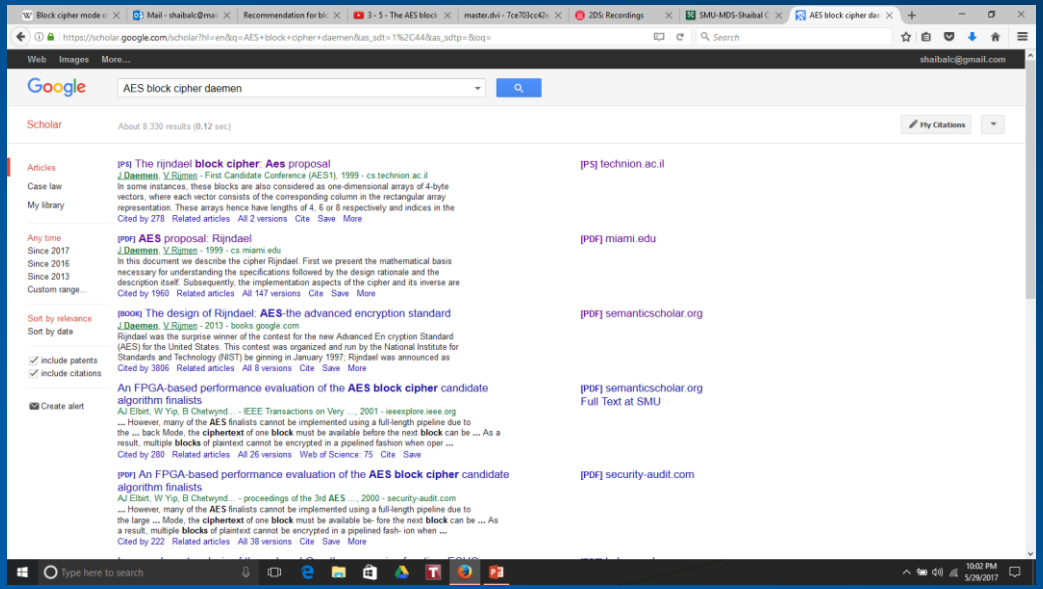
SMU®

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)



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