



Session 06

HMAC, Digital Signatures

CS 7349

Spring 2024

World Changers
Shaped Here



SMU®



Shaibal Chakrabarty

Contents

- Security News of the Week
- House Keeping
- Class Presentation
- Concepts: Quick review
- HMACs
- Authenticated Encryption Associated Data (AEAD)
- Digital Signatures



House Keeping

- Status of Teams for Term Paper? Topic?
- Research Paper submit Jan deliverables now;
- Checkpoint on 02/15, 02/19
- Submit Quiz 2 and start on Quiz 3; Case Study published
- Submit HW1 and start Case Study
- Quiz 2, 1 week; Case Study, 2 weeks
- **RED ALERT** on Research Paper! Teams & Topic NOW!!



Are we waiting to START the Case Study?



Sources: Meta AI



Security News of the Week – Spring 2024

- https://www.wired.com/story/27-year-old-codebreaker-busted-myth-bitcoins-anonymity/#intcid=wired-tag-right-rail_5368081e-380a-4ef5-adc6-53949cb77cb3_popular4-1
 - Cloudflare breach: Sensational Headline vs Reality (Mis/Dis/Information)
- <https://www.securityweek.com/schneider-electric-division-responding-to-ransomware-attack-data-breach/>
 - Schneider Electric division reported a ransomware attack started ~01/17
- https://www.wsj.com/articles/intelligence-researchers-to-study-computer-code-for-clues-to-hackers-identities-e1d594a4?mod=cybersecurity_more_article_pos1
 - Research: How to find hacker identity?



CS 7349 – Tying it all together

INTRODUCTION TO CS7349 AND THE
THREAT LANDSCAPE

INTRODUCTION TO NETWORKS

SYMMETRIC KEY CRYPTO

USING SYMMETRIC KEY CIPHERS

RANDOMNESS AND PSEUDORANDOM
NUMBERS

PUBLIC KEY CRYPTO/Team Paper

HASH FUNCTIONS

MESSAGE AUTHENTICATION CODES

KEY MANAGEMENT

IDENTITY AND ACCESS MANAGEMENT

NETWORK SECURITY

SECURITY – CLOUD, WIRELESS/5G, DDoS,
SASE, IoT, SDN, Smart Cities

FRAMEWORKS, STANDARDS, OPERATIONS,
Governance/Risk/Compliance

REVIEW/ADDITIONAL TOPICS

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

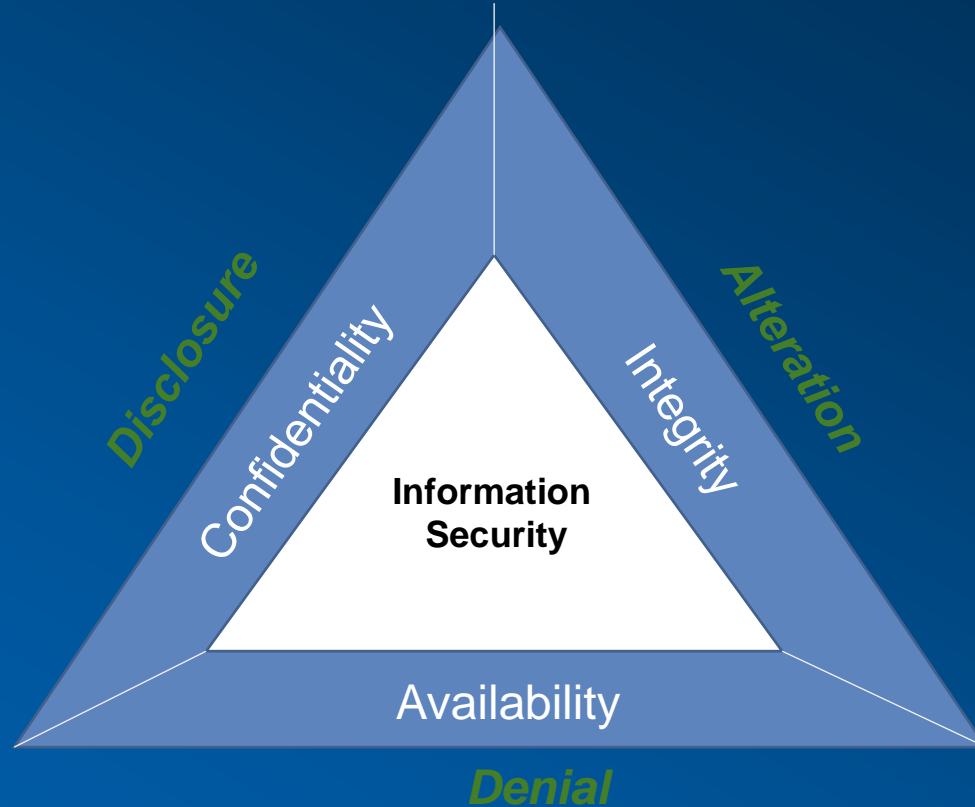


Project – 1st deliverable

- 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



InfoSec, CIA, Threats

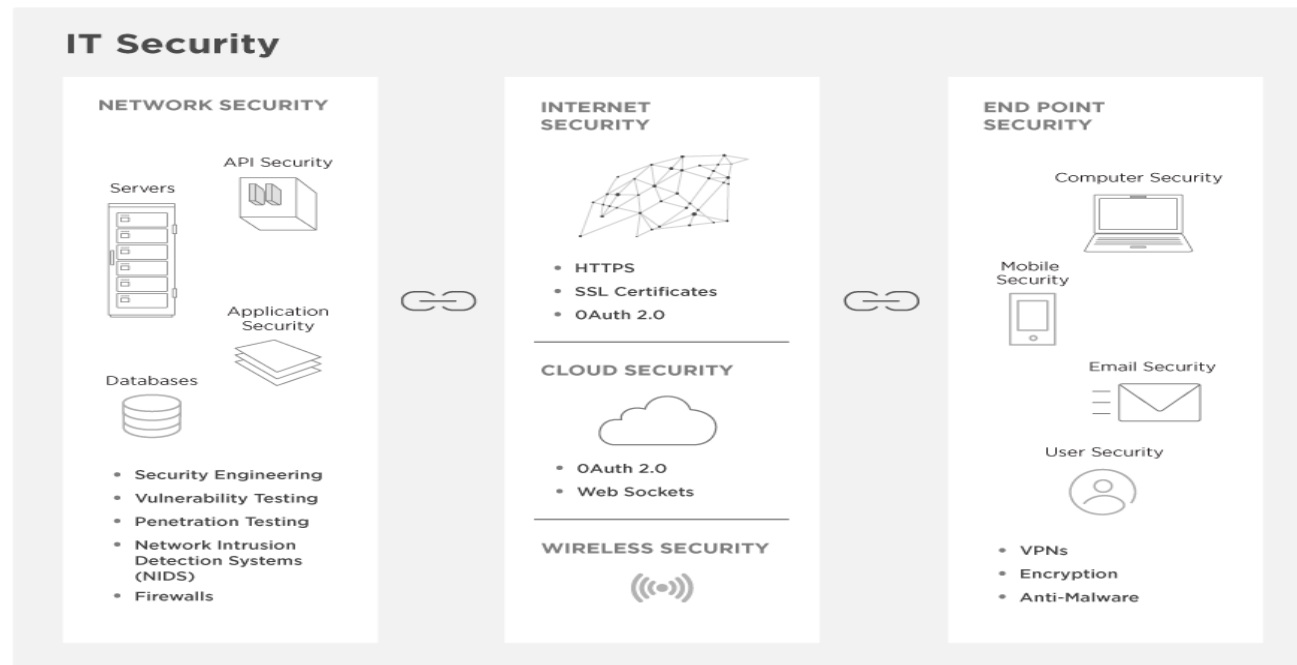


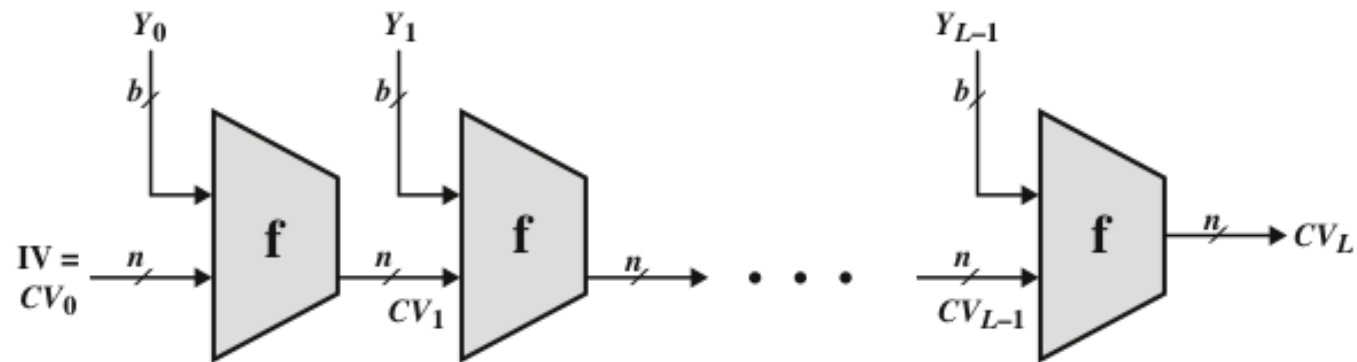
Network Security Basics

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.





IV = Initial value
 CV_i = chaining variable
 Y_i = i th input block
 f = compression algorithm

L = number of input blocks
 n = length of hash code
 b = length of input block

Figure 11.8 General Structure of Secure Hash Code



Hash Functions Based on Block Ciphers

Cipher Block Chaining (CBC mode)

- Can use block ciphers as hash functions
 - Using $H_0=0$ and zero-pad of final block
 - Compute: $H_i = E(M_i H_{i-1})$
 - Use final block as the hash value
 - Similar to CBC but without a key
- Resulting hash is too small (64-bit)
 - Both due to direct birthday attack
 - And “meet-in-the-middle” attack
- Other variants also susceptible to attack




Secure Hash Algorithm (SHA)

- SHA was originally designed by the National Institute of Standards and Technology (NIST) and published as a federal information processing standard (FIPS 180) in 1993
- Was revised in 1995 as SHA-1
- Based on the hash function MD4. Design closely models MD4
- Produces 160-bit hash values
- In 2002 NIST produced a revised version of the standard that defined three new versions of SHA with hash value lengths of 256, 384, and 512
 - Collectively known as SHA-2



Comparison of SHA Parameters

<https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html>



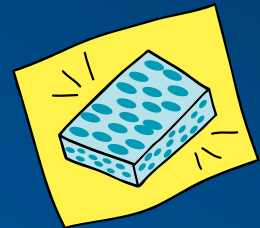
	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Message Digest Size	160	224	256	384	512
Message Size	$< 2^{64}$	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Block Size	512	512	512	1024	1024
Word Size	32	32	32	64	64
Number of Steps	80	64	64	80	80

Note: All sizes are measured in bits.



The Sponge Construction

- Underlying structure of SHA-3 is a scheme referred to by its designers as a *sponge construction*
- Takes an input message and partitions it into fixed-size blocks
- Each block is processed in turn with the output of each iteration fed into the next iteration, finally producing an output block
- The sponge function is defined by three parameters:
 - f = the internal function used to process each input block
 - r = the size in bits of the input blocks, called the *bitrate*
 - pad = the padding algorithm



SHA-3 Parameters

Message Digest Size	224	256	384	512
Message Size	no maximum	no maximum	no maximum	no maximum
Block Size (bitrate r)	1152	1088	832	576
Word Size	64	64	64	64
Number of Rounds	24	24	24	24
Capacity c	448	512	768	1024
Collision resistance	2^{112}	2^{128}	2^{192}	2^{256}
Second preimage resistance	2^{224}	2^{256}	2^{384}	2^{512}



Unit Overview – MAC

- Burning questions?
- Message Integrity, no confidentiality
 - Windows 10 system files on disk, integrity, but no confidentiality
 - Web page banner ads
- MAC: pair of signing and verification algorithms. Signing produces a tag/digest; verification takes in the message, the key and the tag, and generates a Y or a N.
- Needs a secret key
- CRC can be defeated, does not require a key. And designed for random errors, not malicious errors.
- Tags cannot be too short: 64, 96 (TLS), 128 bits



Message Authentication Code (MAC) and Medium Access Control (MAC at the Data Link Layer)

Octets:2	1	0/2	0/2/8	0/2	0/2/8	variable	2
Frame control	Sequence number	Destination PAN identifier	Destination address	Source PAN identifier	Source address	Frame payload	Frame check sequence
		Addressing fields					
MAC header						MAC payload	MAC footer

- IEEE 802.15.4 MAC Frame Format
- Frame Check Sequence is a CRC – used to detect and correct random bit errors in transmission



MAC Requirements

- Protect against:

- Disclosure
- Traffic Analysis

Confidentiality

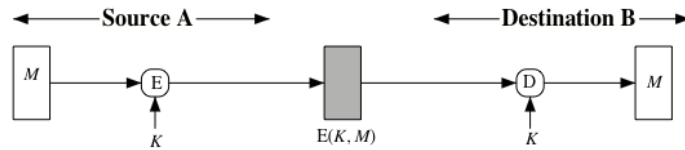
- Masquerade
- Content Modification
- Sequence Modification

Integrity

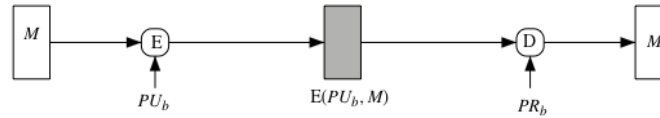
- Timing Modification
- Source Repudiation
- Destination Repudiation

Authentication

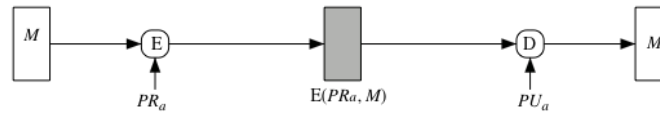




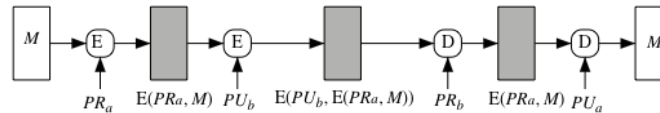
(a) Symmetric encryption: confidentiality and authentication



(b) Public-key encryption: confidentiality



(c) Public-key encryption: authentication and signature



(d) Public-key encryption: confidentiality, authentication, and signature

Figure 12.1 Basic Uses of Message Encryption

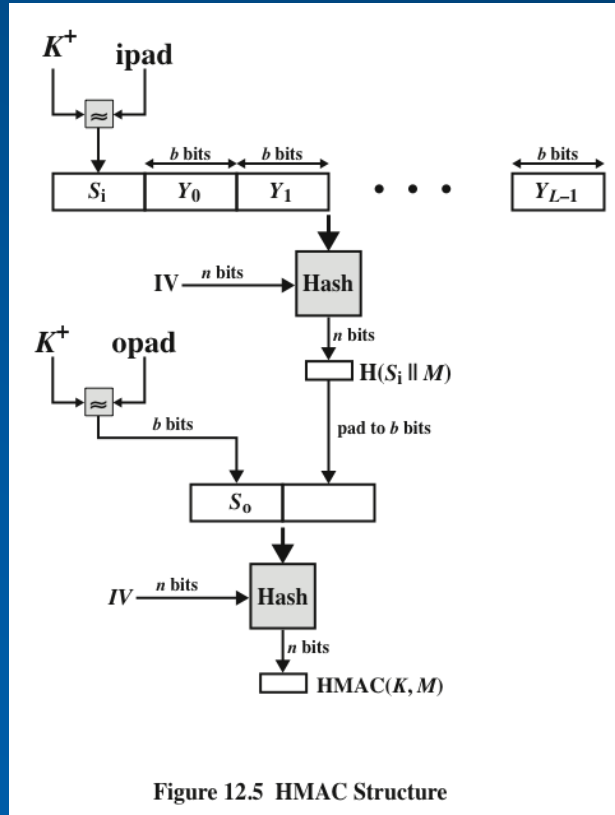


keyed-Hash MAC: HMAC

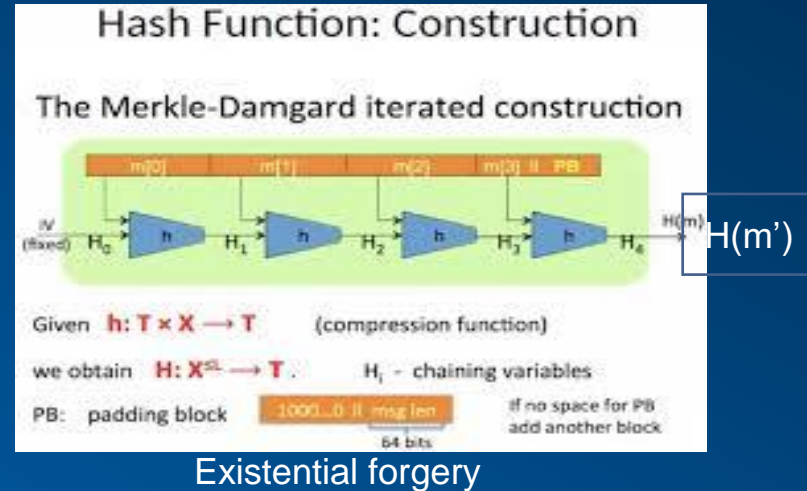
- There has been increased interest in developing a MAC derived from a cryptographic hash function
- Motivations:
 - Cryptographic hash functions such as MD5 and SHA generally execute faster in software than symmetric block ciphers such as DES
 - Library code for cryptographic hash functions is widely available
- HMAC has been chosen as the mandatory-to-implement MAC for IP security (RFC 2104) IETF (www.ietf.org)
- Issued as a NIST standard (FIPS 198)



HMAC Structure



Why can't we simply use a hash function?
i.e. $S(k, m) = H(k || m)$




$$S(k, m) = H(k(XOR)opad, H(k(xor)ipad || m))$$

<https://www.youtube.com/watch?v=xoMadIbWP1k>



Authenticated Encryption (AE)

- A term used to describe encryption systems that simultaneously protect confidentiality and authenticity of communications
- Approaches:
 - Hash-then-encrypt: $E(K, (M \parallel h))$ (single key)
 - MAC-then-encrypt: $T = \text{MAC}(K_1, M)$, $E(K_2, [M \parallel T])$ (SSL/TLS)
 - **Encrypt-then-MAC: $C = E(K_2, M)$, $T = \text{MAC}(K_1, C)$ (IPSec)**
 - Encrypt-and-MAC: $C = E(K_2, M)$, $T = \text{MAC}(K_1, M)$ (SSH)
- Both decryption and verification are straightforward for each approach
- There are security vulnerabilities with all of these approaches 

MAC with (CTR-CBC = CCM)

- Was standardized by NIST specifically to support the security requirements of IEEE 802.11 WiFi wireless local area networks
- Variation of the encrypt-and-MAC approach to authenticated encryption
 - Defined in NIST SP 800-38C
- Key algorithmic ingredients:
 - AES encryption algorithm
 - CTR mode of operation
 - CMAC authentication algorithm
- Single key K is used for both encryption and MAC algorithms
- <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf>



CCM Encryption

- The input to the CCM encryption process consists of three elements:

Data that will be both authenticated and encrypted

This is the plaintext message P of the data block

Associated data A that will be authenticated but not encrypted

An example is a protocol header that must be transmitted in the clear for proper protocol operation but which needs to be authenticated

A nonce N that is assigned to the payload and the associated data

This is a unique value that is different for every instance during the lifetime of a protocol association and is intended to prevent replay attacks and certain other types of attacks

<http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/ccm-ad1.pdf>

security proof for CCM mode



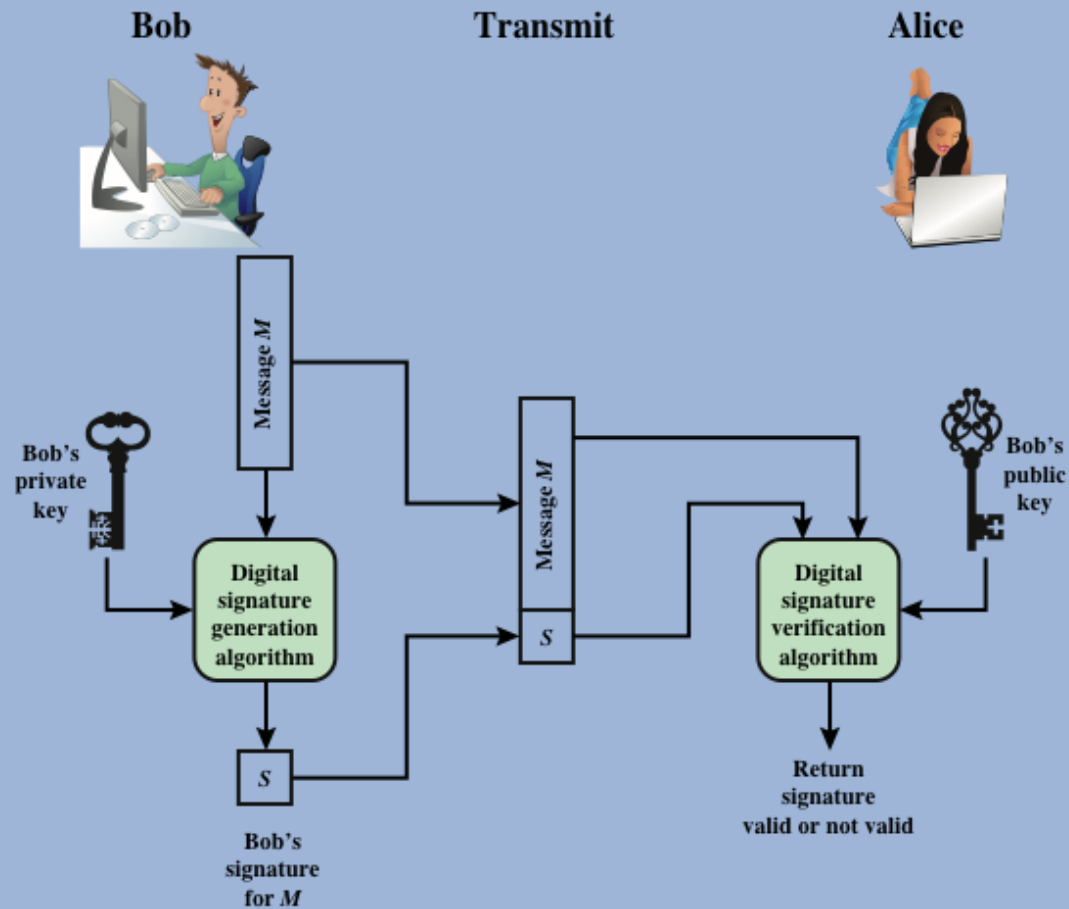
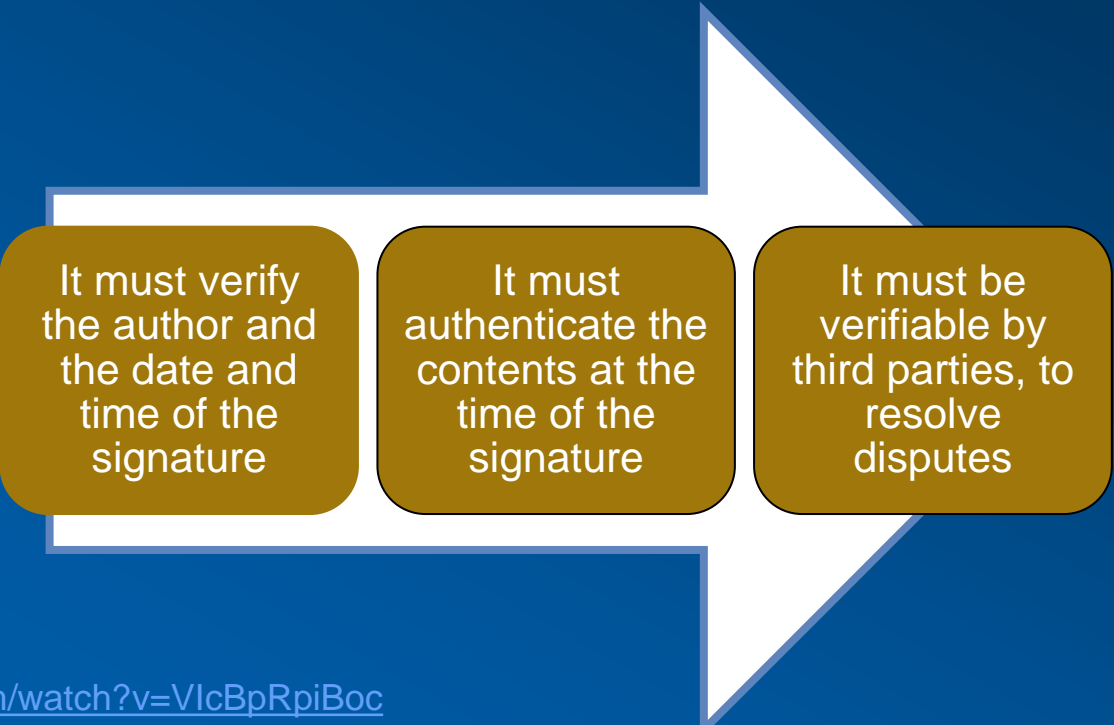


Figure 13.1 Generic Model of Digital Signature Process



Digital Signature Properties



It must verify
the author and
the date and
time of the
signature

It must
authenticate the
contents at the
time of the
signature

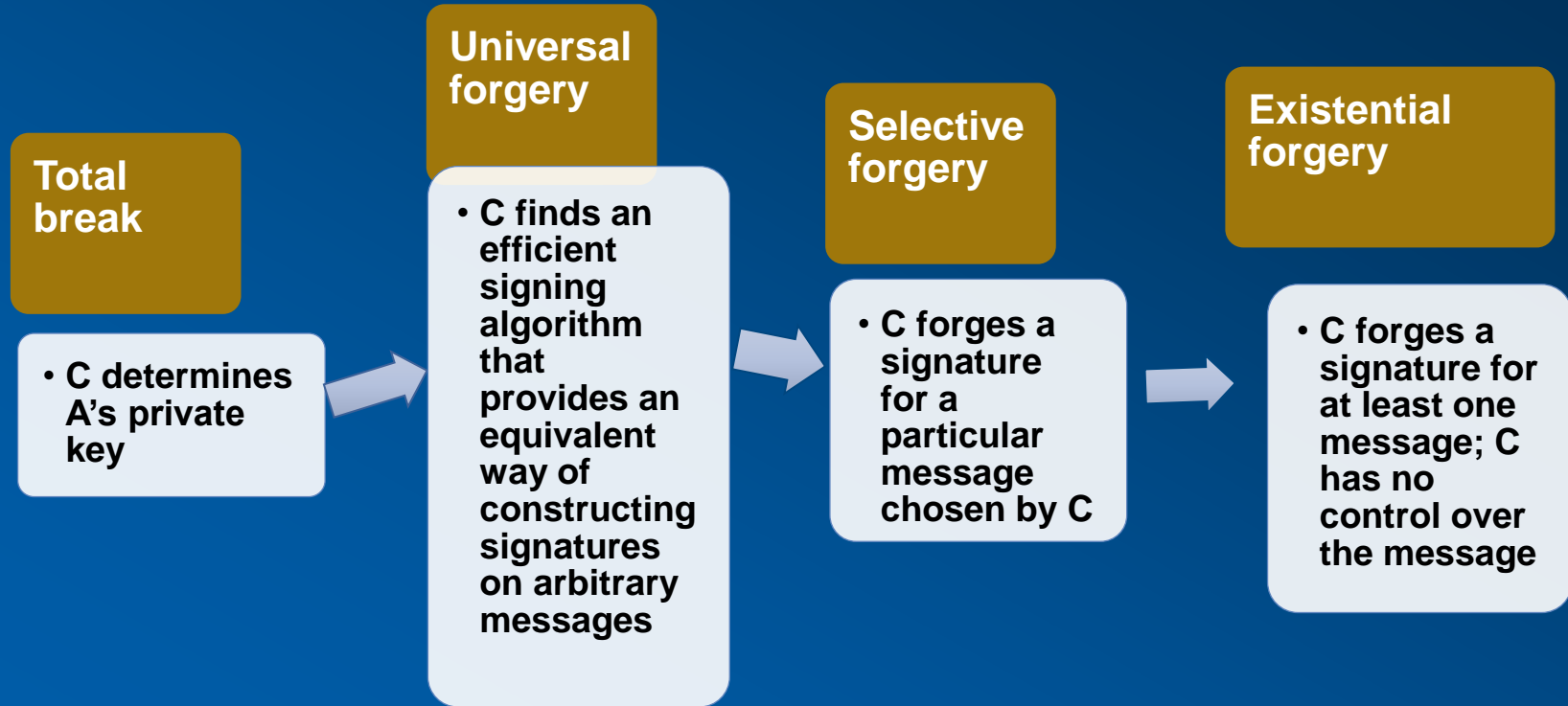
It must be
verifiable by
third parties, to
resolve
disputes

<https://www.youtube.com/watch?v=VlcBpRpiBoc>

High Level practical view of the uptake in digital signatures in Europe



Forgeries



Digital Signature Requirements

- The signature must be a bit pattern that depends on the message being signed
- The signature must use some information unique to the sender to prevent both forgery and denial
- It must be relatively easy to produce the digital signature
- It must be relatively easy to recognize and verify the digital signature
- It must be computationally infeasible to forge a digital signature, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message
- It must be practical to retain a copy of the digital signature in storage



Direct Digital Signature

- Refers to a digital signature scheme that involves only the communicating parties => no 3rd party involved.
 - It is assumed that the destination knows the public key of the source
- Confidentiality can be provided by encrypting the entire message plus signature with a shared secret key
 - It is important to perform the signature function first and then an outer confidentiality function
 - In case of dispute some third party must view the message and its signature
- The validity of the scheme depends on the security of the sender's private key
 - If a sender later wishes to deny sending a particular message, the sender can claim that the private key was lost or stolen and that someone else forged his or her signature
 - One way to thwart or at least weaken this ploy is to require every signed message to include a timestamp and to require prompt reporting of compromised keys to a central authority



Thank You!

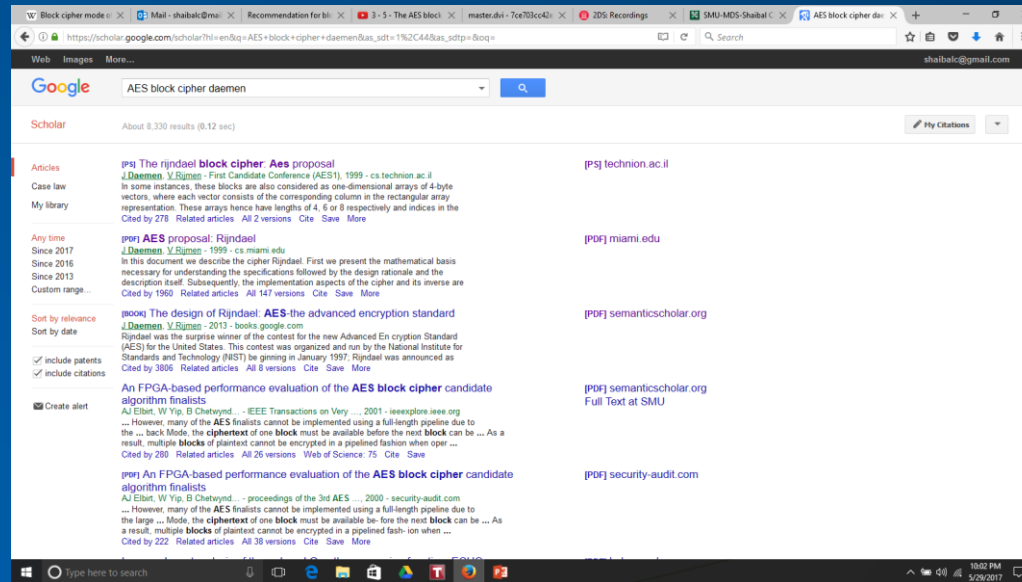
World Changers
Shaped Here



SMU®

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 be 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 Assessment 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

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,

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.

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

