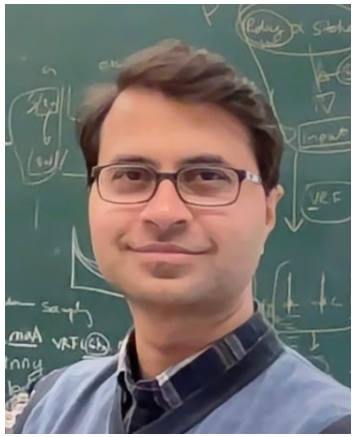
CSEC-10/11 Admin

- 3 Lectures per week: Monday, Wednesday, Friday @ 10:00-10:50am

- 8 tutorials or labs: Weeks 3-10 (CSEC-10)
- 7 tutorials or labs: Weeks 4-10 (CSEC-11)

Myrto Arapinis
CO CSEC-10



Tariq Elahi

Marc Juarez
CO CSEC-11

Assessment

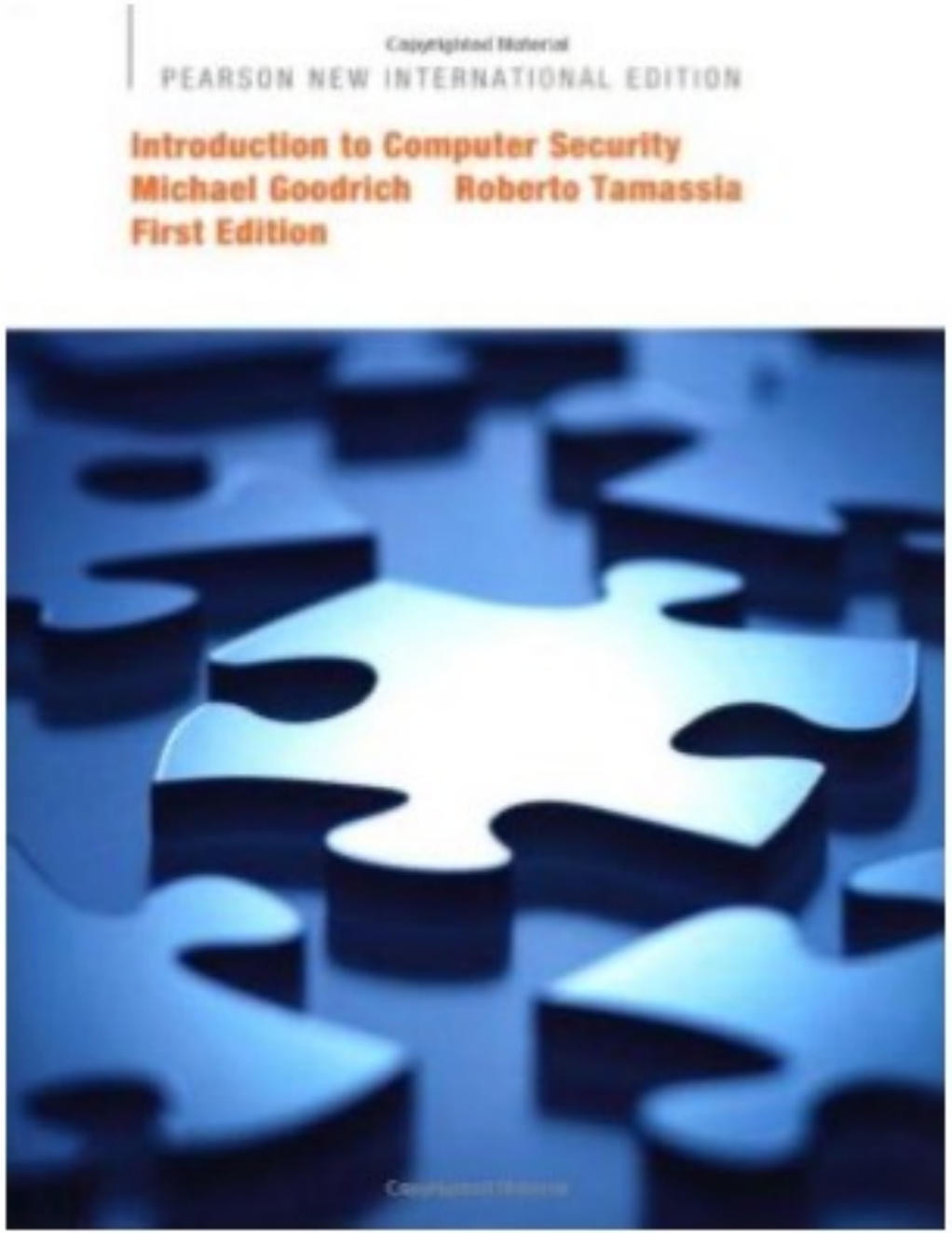
CSEC-10

- CW1 (formative)
  - Friday 13 October 12pm
- CW2 (12.5% of total)
  - Friday 3 November 12pm
- CW3 (12.5% of total)
  - Friday 24 November 12pm
- Final exam (75% of total)
  - December Exam Period

CSEC-11

- CW1 (15% of total)
  - Friday 3 November 12pm
- CW2 (15% of total)
  - Friday 24 November 12pm
- Final exam (70% of total)
  - December Exam Period

Textbook


Copyrighted Material
PEARSON NEW INTERNATIONAL EDITION
Introduction to Computer Security
Michael Goodrich Roberto Tamassia
First Edition

Where to find information

- Course Learn page
  - Schedule
    - Week 1-5 RAAC arrangements
    - Assignment, tutorial sheets, tutorial solutions
  - Lecture recordings
  - Online lecture links
  - Assignment submission links
  - Piazza (student discussions)
    - Office hours
      - Myrto: Wednesday’s 11am-12pm IF5.27
      - Tariq: Friday’s 11am-12pm IF4.04A

Course overview

- What are our goals in this course?
- What is trust?
- What is security?
- What is privacy?
- Who are the adversaries?
- Terminology
- Common defence methods

What are our goals in this course?

- To be able to identify security, privacy, and trust issues in various aspects of computing, such as:
  - Programs
  - Operating systems
  - Networks
  - Distributed systems
  - Internet applications
- The awareness of how security, privacy, and trust can be achieved in practice

The landscape

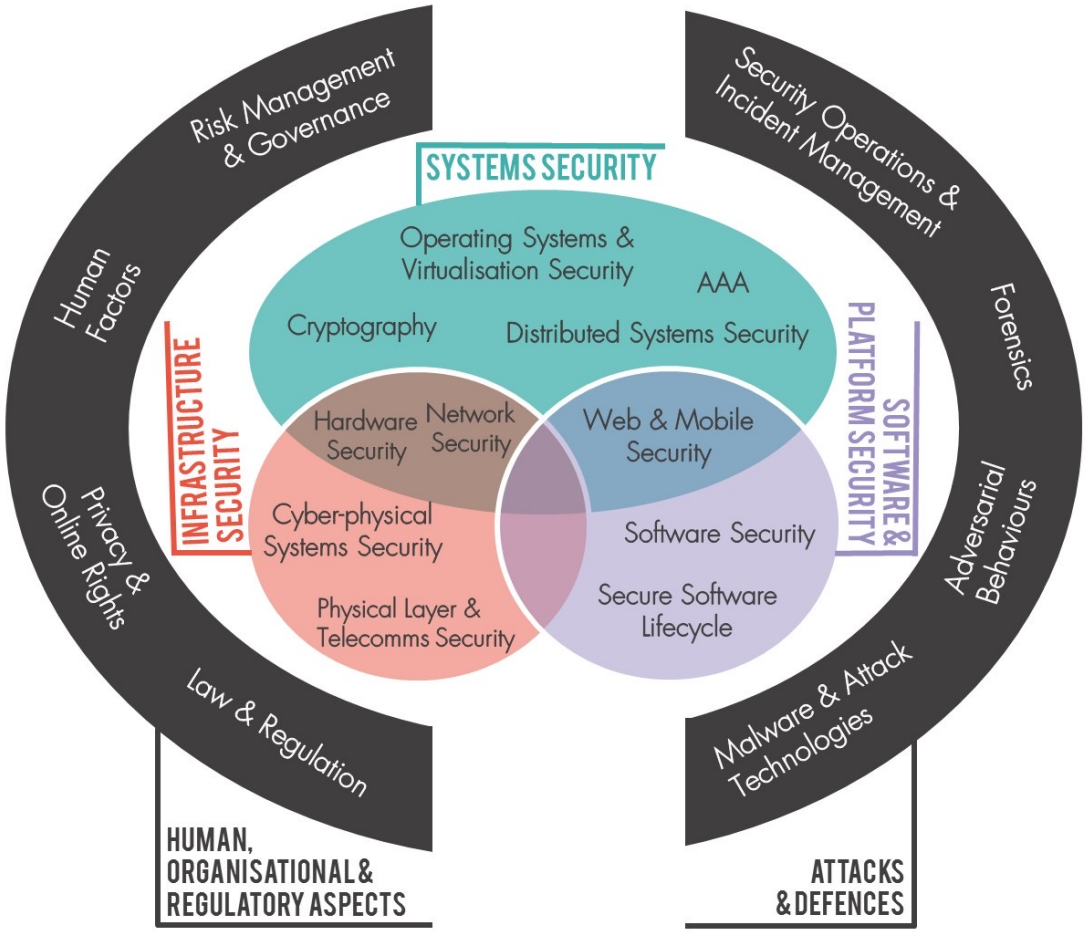


Image: CyBOK

What do we want?

What do the we mean when we say…?

- Authentic
- Safe
- Common language/sense → (more) Formal language/models
  - Based on definitions
  - Properties of the system, the data, usage, and abilities of the participants
  - Wide-spread agreement (in some areas; still evolving)

Who is we?

- Ordinary citizen
- Whistle blower
- Corporate worker
- Dissident activist
- Secret agent

What is security?

- The main general properties are:
  - Confidentiality
    - Information access to only authorized entities
  - Integrity
    - The data is untampered and uncorrupted
  - Availability
    - Both the data and the system that provides access to it are there when you need them
- Are these enough? What can still go wrong?

Failure of Security: Apple Security Cert Validation Bug

- The bug occurs in code that is used to check the validity of the server's signature on a key used in an SSL/TLS connection.
- An active attacker (a “malfactor-in-the-middle”) could potentially exploit this aw to get a user to accept a counterfeit key that was chosen by the attacker.

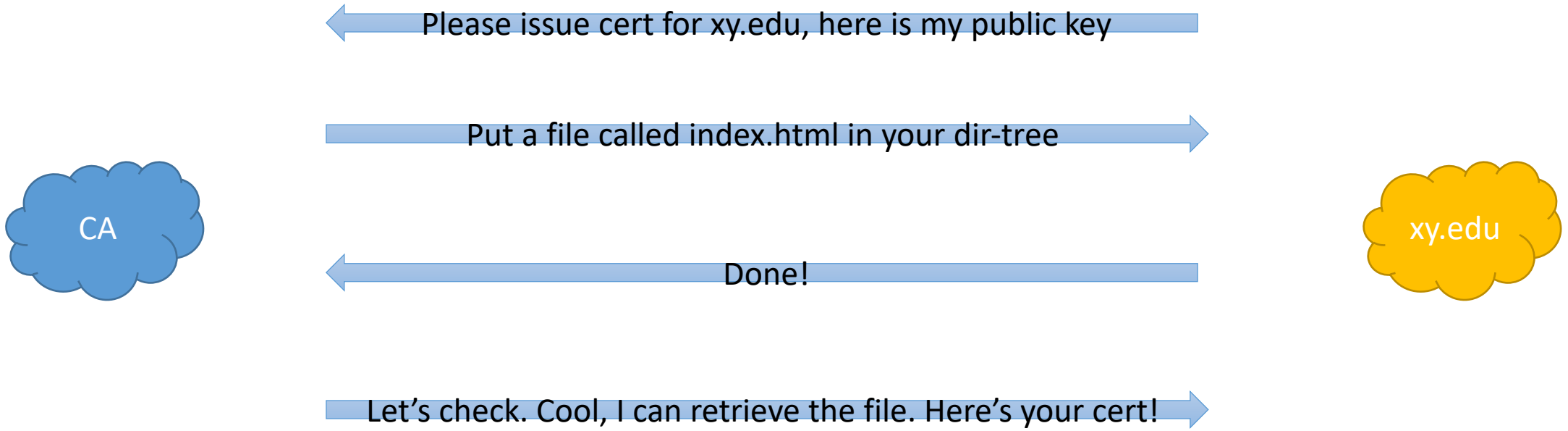
```
static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParams,
                                 uint8_t *signature, UInt16 signatureLen)
{
        OSStatus        err;
        ...

        if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
                goto fail;
        if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
                goto fail;
                goto fail;
        if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
                goto fail;
        ...

fail:
        SSLFreeBuffer(&signedHashes);
        SSLFreeBuffer(&hashCtx);
        return err;
}
```

What is trust?

- Generally, we trust when we have:
  - Assurance
    - The means to know that the system is secure
  - Reliability/Resilience
    - To operate intact in the face of natural disasters and human-launched attacks
  - Accountability
    - The means to verify that the system is operating as designed (i.e. securely)

NB: There is a difference between trustworthy and trusted

Failure of Trust:
CA Domain Control Validation



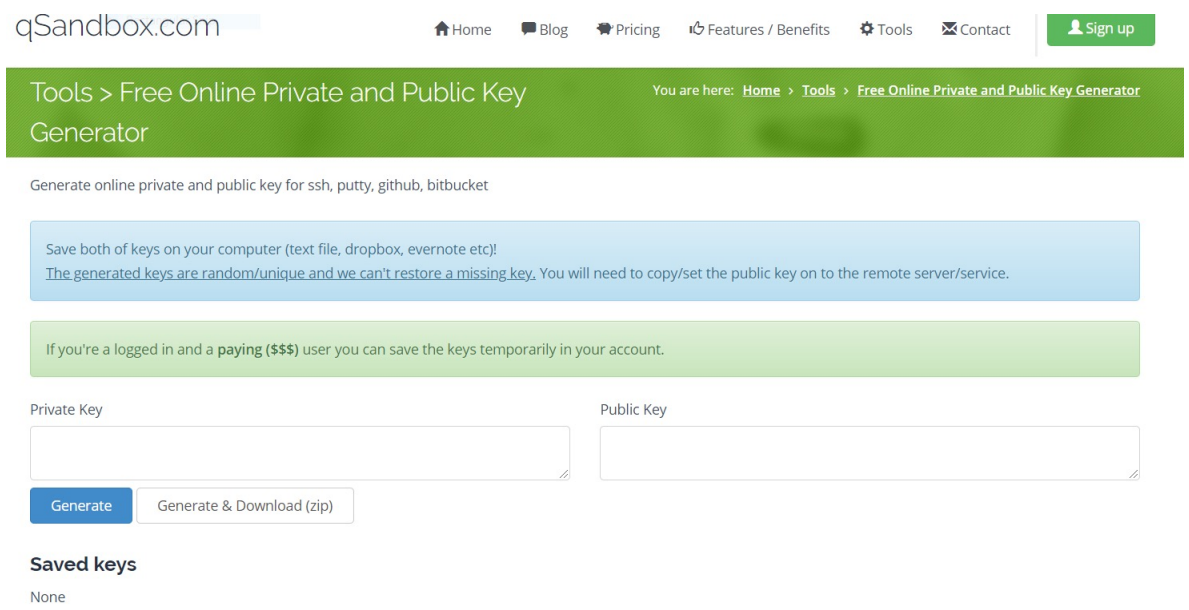
Failure of Trust:
Operational security of digital certs

- Symantec has a track record of fumbling certificate issuance, once even wrongly issuing one for google.com
- Google chrome, among other browsers removes Symantec as a root CA
- Trustico (Symantec reseller) emails 23,000 private keys for certs they issued, thus invalidating them (how did they get them?)
- All 23,000 certs are revoked within 24 hours

*Logo from Trustico website

Convenient insecurity

- Offer a service to generate public/private key pairs
- Do not delete the keys afterwards
- ???
- Profit



What is privacy?

- Concerns individuals and their expectations on how their data, behaviours, and interactions are recorded, utilized, and spread

- A useful definition: “Information self-determination”
  - A person gets to control information about themselves

  - Controls can include:
    - Who gets to see it
    - Who gets to use it
    - What they can use it for
    - Who they can give it to

Failure of Privacy: New York Taxi Database

- Database released for research
- Taxi numbers and licence numbers pseudonymized
  - MD5 hash
  - Same input = Same result
- Taxi/Lic. numbers have structure
  - Results in reduced number of possible values
  - Brute force is feasible on 24 million numbers

https://www.theguardian.com/technology/2014/jun/27/new-york-taxi-details-anonymised-data-researchers-warn

Failure of Privacy:
New York Taxi Database

Taxi #	Lic. #
3A3D444BB	01001EDFD
…	…
…	…
ADE034523	B0BB321AA

DATABASE

1. Enumerate all values with structures:
5X55, XX555, XXX555, 5XXXXXX, 5XXXXXXX

2. Hash all values above with MD5

3. Compare results with database on left

How could we have prevented this?

- Was the problem lack of education?
- Could some processes have helped?
- Were the problems obvious?
- Were the right stakeholders involved?

Who are the adversaries?

- All systems are vulnerable to all manner of threats

- Adversary types:
  - Nature
  - Script kiddies
  - Crackers/Hackers
  - Organised Crime
  - Governments
  - Terrorists

- Who should we worry about most? Can we ignore anyone?

Threat Modelling

- Who is the adversary (the system may protect against many types)?
- What are they allowed to do? Or, what can't we prevent them from doing?
  - The adversary need not be malicious, he could merely be curious
- What do we want to prevent the adversary from doing or learning?
  - What is the adversary's aim, or, when does he win?
- The set of threats we want to protect against given this (set of) adversaries
  - When do we win?
  - When does the adversary win?

Terminology

- Assets: Things we want to protect, like:
  - Hardware
  - Software
  - Information

- Vulnerabilities
  - Weaknesses in a system that may be exploited
    - Example: Public facing email server without spam protection

Terminology

- Threats
  - Loss or damage to the system, its users, or operators
    - E.g. Proprietary source code being stolen and sold
  - The six major categories of threats:
    - Interception
    - Interruption
    - Modification
    - Fabrication
    - Repudiation
    - Epistemic

Terminology

- Attack
  - An action that exploits a vulnerability to carry out a threat
    - E.g. Hacking the company public facing email server to read emails to steal company trade-secrets
- Controls
  - Mitigating or removing a vulnerability
  - The control mitigates a vulnerability to prevent an attack and that defends against a threat
  - No system is perfect: Control vulnerabilities when discovered

Security Principles (pp. 15-18)

- Economy of mechanism: easy to understand, verify, and maintain
- Fail-safe defaults: conservative permissions and functionality
- Complete mediation: every access should be checked (again)
- Open design: no security by obscurity
- Separation of privilege: cooperation required to act, no single point of failure
- Least privilege: programs and users on bare minimum of access
- Least common mechanism: minimize shared means of access to resources
- Psychological acceptability: well designed UI that are intuitive and clear
- Work factor: comparable effort for the value of the resource
- Compromise recording: record failures and breaches

Common defence methods

- There are 5 common defence patterns:
  - Prevent
  - Deter
  - Deflect
  - Detect
  - Recover

  NB: Not all attacks can be prevented!

- Best practice to employ some form of all to get “defence in depth”

Defence tools of the trade

- Protect assets that can be
  - Hardware, software, data (PII, social graph, confidential information, etc.)

- Many forms of control
  - Cryptography
  - Software controls
  - Hardware controls
  - Physical controls
  - Policies and procedures

Cryptography

- Protects the data, making it unreadable by anyone without keys
- Authenticating users with digital signatures
- Authenticating transactions with cryptographic protocols
- Ensures the integrity of data against unauthorized modification

Software controls

- Passwords
- Sandboxes
- Virus scanners
- Source code versioning systems
- Software Firewalls
- Privacy enhancing technologies (PETs)

KeePass

Hardware controls

- Fingerprint readers
- Smart tokens
- Firewalls
- Intrusion detection systems

Physical controls

- Protecting against unauthorized physical access to hardware
- Locks
- Guards
- Off-site backups
- Not placing critical systems in natural disaster zones

Policies and procedures

- Non-technical means to protect against some type of attacks
- Disallow personal hotspot within work place
- Password rules
- Security training against social engineering attacks

Recap

- What is our goal in this course?
  - Identify security and privacy issues
  - Design systems that are more protective of security and privacy
- What is Security?
  - Confidentiality, Integrity, Availability, Authenticity
- What is Trust?
  - Assurance, Reliability/Resilience, Accountability
- What is Privacy?
  - Informational self-determination

Recap

- Who are the adversaries?
  - Threat modelling
  - Learn to think like an attacker
- Trade-offs
  - Security, Privacy, Performance, Cost
- Assets, vulnerabilities, threats, attacks and controls
  - You control a vulnerability to prevent an attack and block a threat
- Methods of defence
  - Cryptography, software controls, hardware controls, physical controls, policies and procedures