Info2222
Security & Usability

Security Part Overview

Why Study Cybersecurity?

Why Study Cybersecurity?

Forbes / Leadership / #IfIOnlyKnew

MAR 16, 2017 @ 06:46 PM 25,452

The Little Black Book of

The Fast-Growing Job With A Huge Skills Gap: Cyber Security

Jeff Kauflin, FORBES STAFF

I cover leadership, management and careers. FULL BIO

NEWS

Cybersecurity job market to suffer severe workforce shortage

10 facts, figures and statistics summarize the cybersecurity labor market

Why Study Cybersecurity? More Reasons





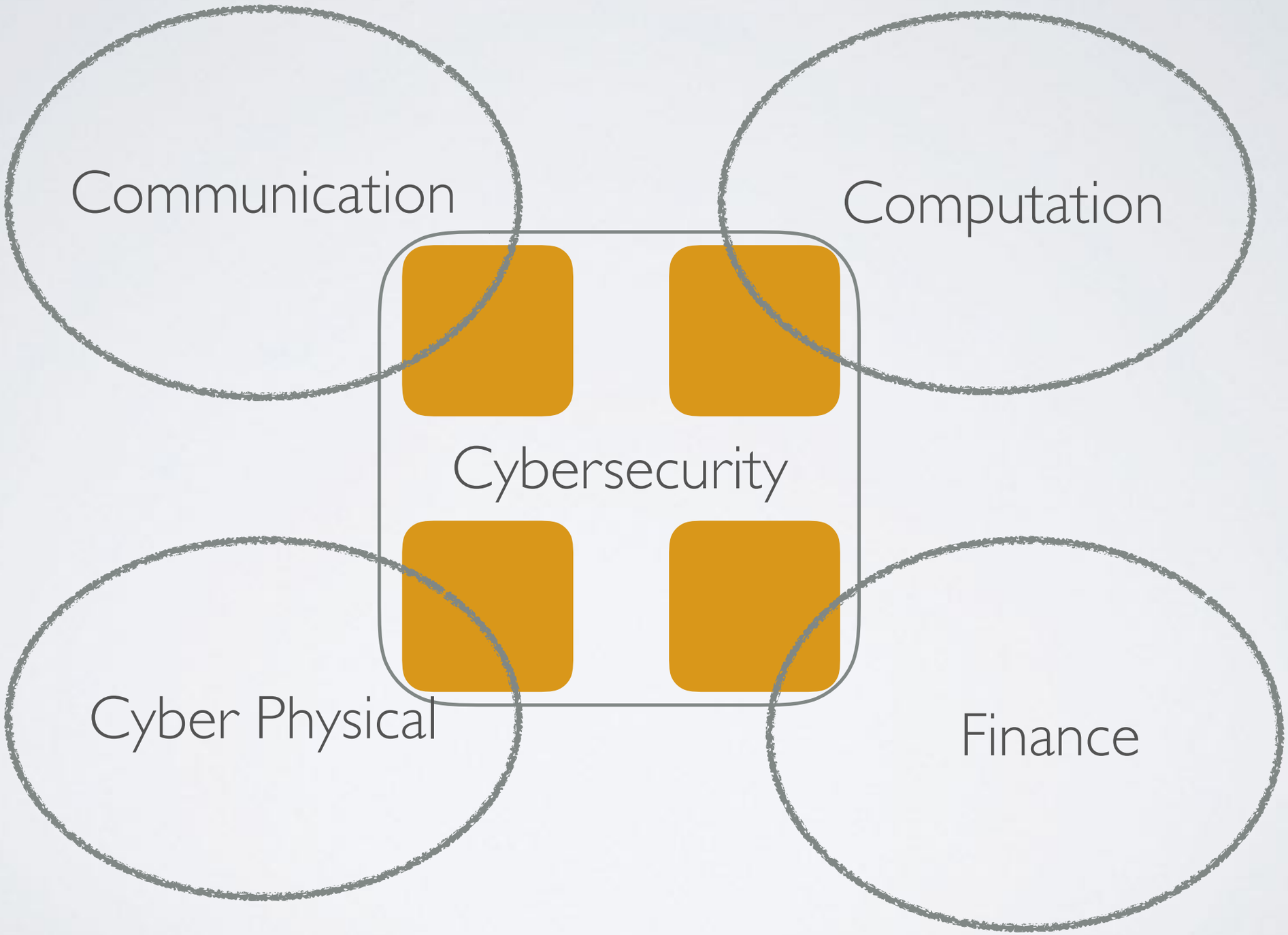

intellectually deep & intriguing

Why Study Cybersecurity? More Reasons

Why Study Cybersecurity? More Reasons

huge & direct practical impact

It Is Everywhere



Why Cyber?

Includes network, system, data, even physical objects

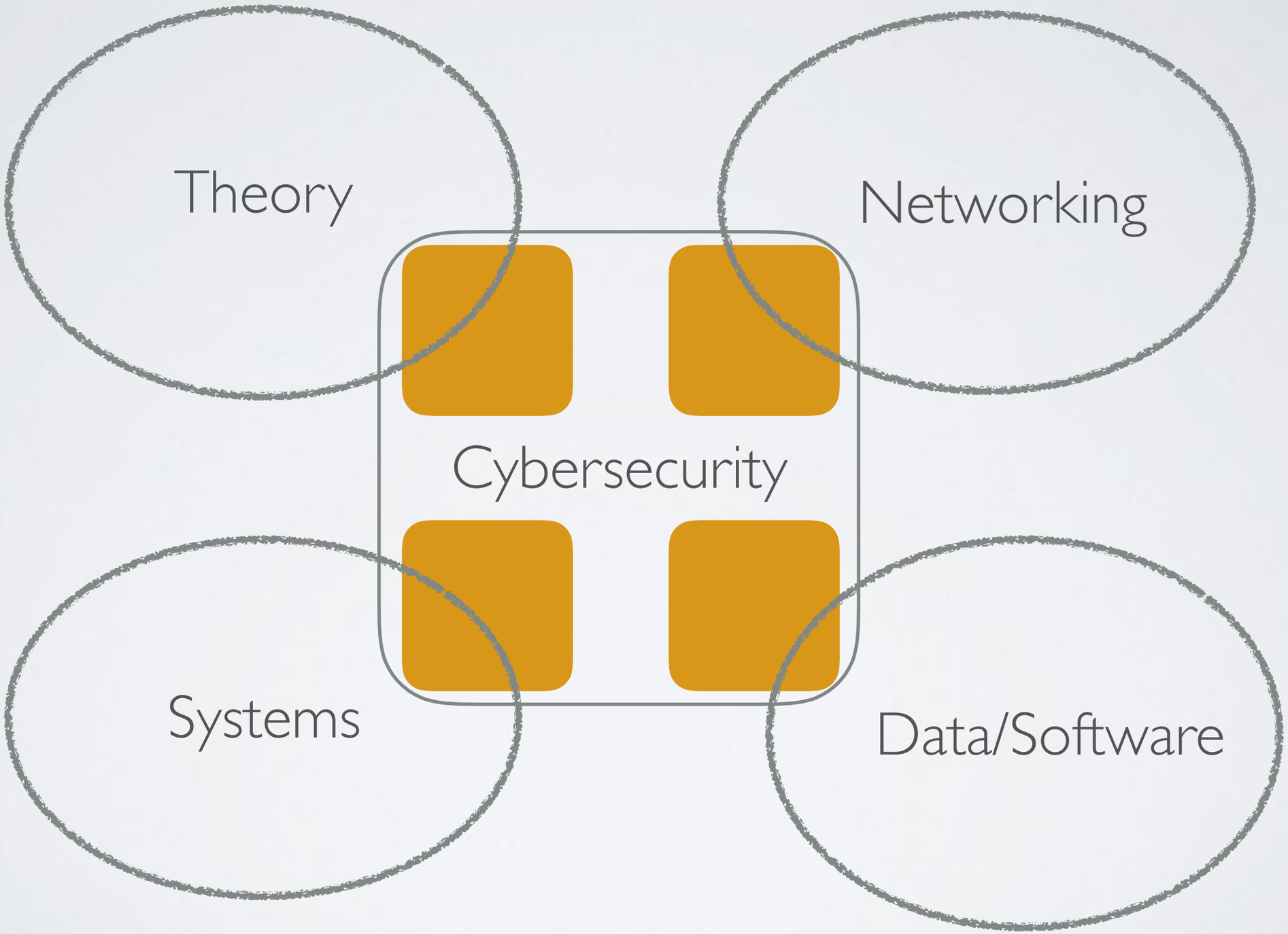
and many more…

Challenge

Name some areas having NO relationship to cybersecurity

It Relates to All CS

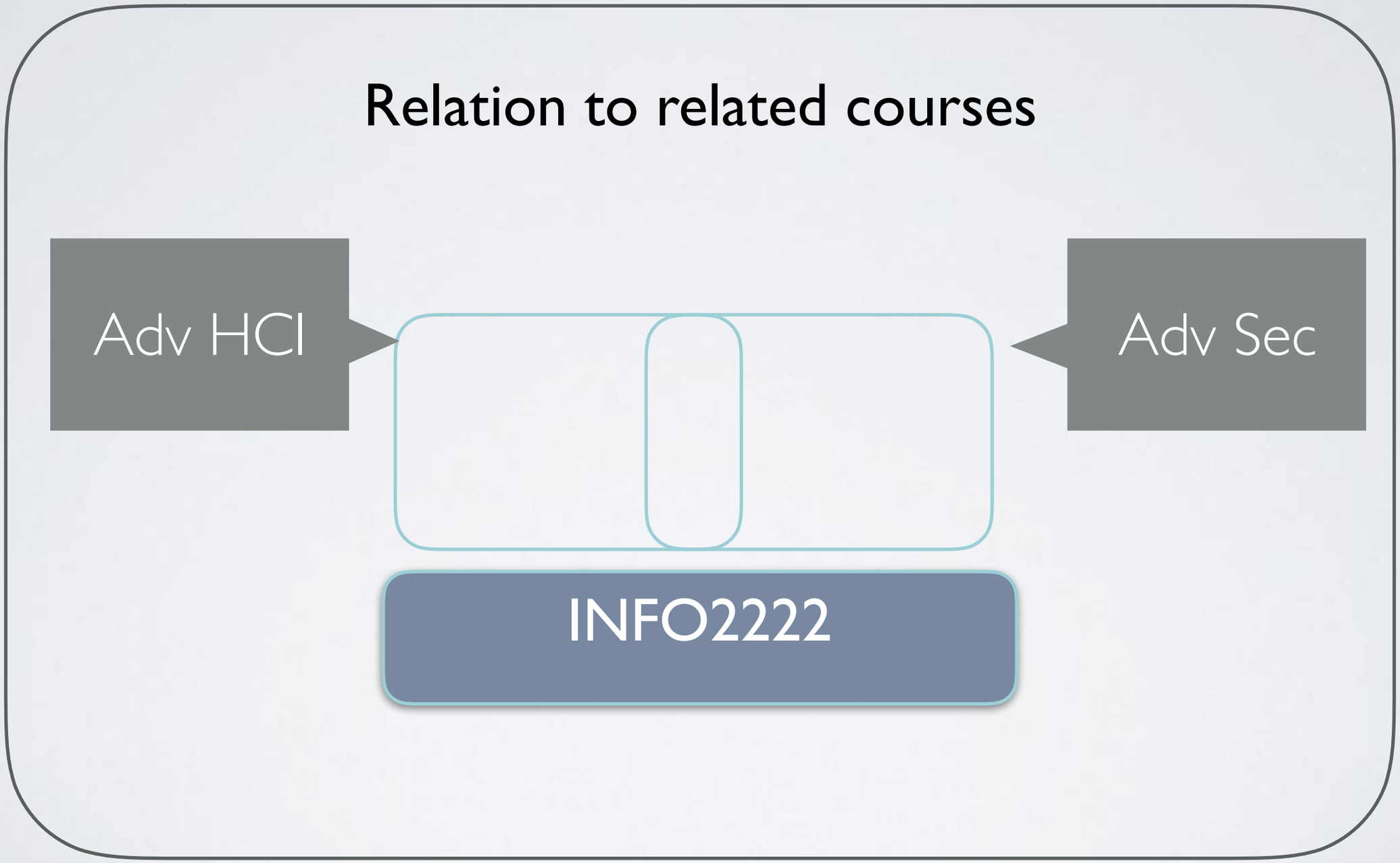
It Relates to All CS



Your Reason?

Other than being a “mandatory” course

General Background



The Goal of the Security Part

Provide broad fundamental concepts
and practical applications of cybersecurity.

won't be a trivial class,
but questions are
normally easy, if you
understand the concepts

No Goal of the Course

Hack anyone other than yourself

Ethics of Cybersecurity

- 1. Using virtue value always, not just concerning legal aspects
- 2. Consider downstream risks in security practice
- 3. Establish Chains of Ethical Responsibility and Accountability
- 4. Practice Cybersecurity Disaster Planning and Crisis Response
- 5. Promote Values of Transparency, Autonomy, and Trustworthiness
- 6. Design for Privacy and Security

Ethics of Cybersecurity

- 1. Using virtue value always, not just concerning legal aspects
- 2.

An Introduction to Cybersecurity Ethics
MODULE AUTHOR:
Shannon Vallor, Ph.D.
William J. Rewak, S.J. Professor of Philosophy, Santa Clara University

- 3. [illegible]y
- 4. Practice Cybersecurity Disaster Planning and Crisis Response
- 5. Promote Values of Transparency, Autonomy, and Trustworthiness
- 6. Design for Privacy and Security

What is Security

In physical world: safety, confidence etc

Security is a fuzzy/vague term

Example Scenarios in Banks

Example Scenarios in Banks

Scenarios I

Our Fantasy

Scenarios I

What is the design goal here?

Scenarios I

How to ensure you can access your account?

How to ensure you cannot access others' accounts?

Scenarios II

How to ensure your pin is not eavesdropped during transmission?

How to ensure when you login, the website is still on?

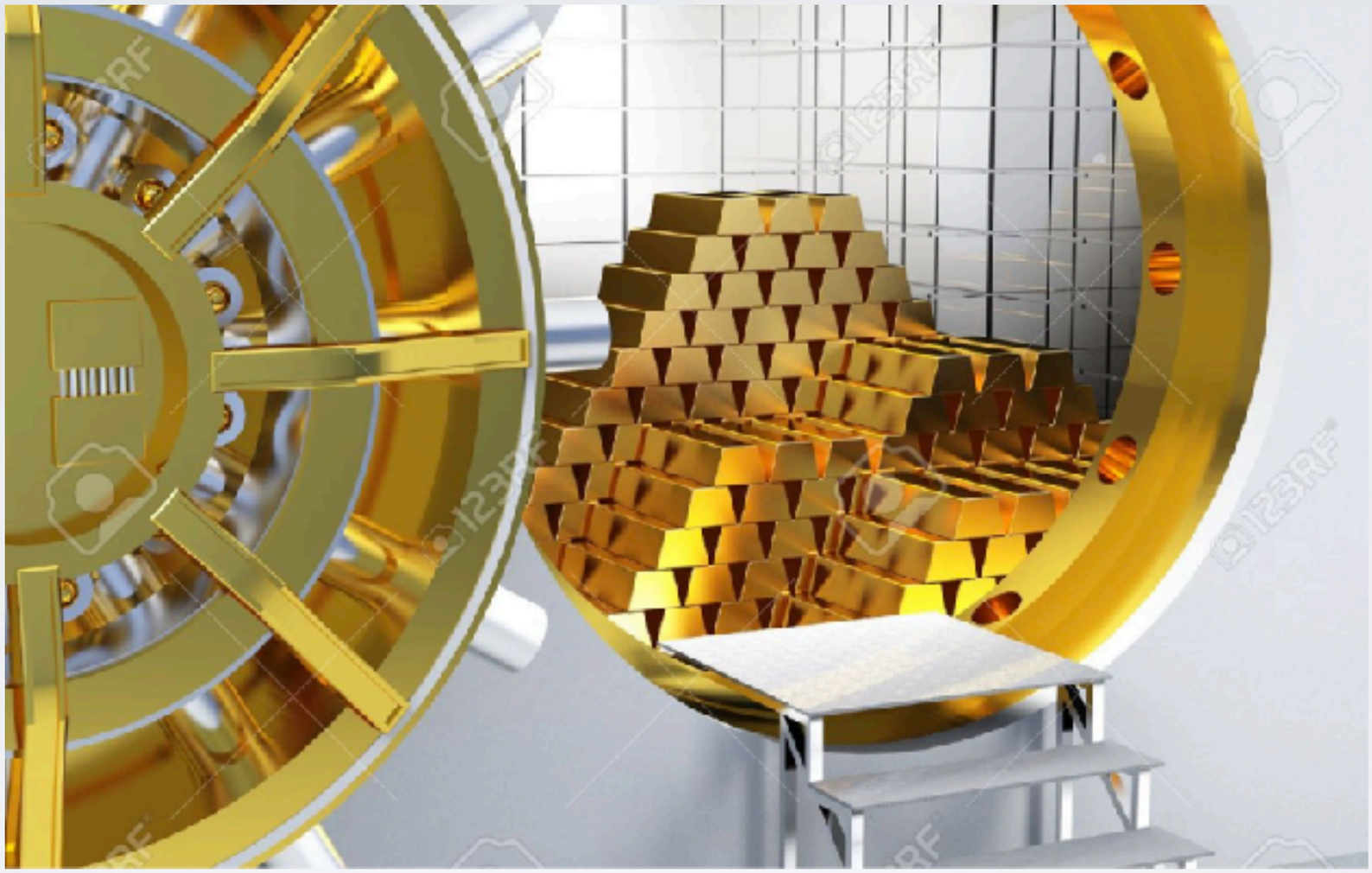
Scenarios III

Date	Description	Ref	Income	Expenses	Bank Balance	
1-Apr	Balance b/f				200.00	R
4-Apr	Folders and pens	1		15.00	185.00	R
15-Apr	Sale: Ms E Inkson	2	54.00		239.00	R
18-Apr	Sale: Mr R U Redy	3	30.00		269.00	R
19-Apr	Drawings	4		10.00	259.00	R
21-Apr	Envelopes & Stamps	5		20.00	239.00	R
24-Apr	Web host fees	6		40.00	199.00	R
27-Apr	Simply Chairs: Chair	7		127.00	72.00	
29-Apr	Sale: Mr J Mighty	8	30.00		102.00	R
30-Apr	Bank Fee	9		2.50	99.50	R
30-Apr	Sale: Ms T Real	10	54.00		153.50	
	Totals		168.00	214.50	153.50	C/f

BANK RECONCILIATION	
Cash Book Balance	153.50
Add: Unpresented check	127.00
Subtotal	280.50
Less: Deposit not yet showing	54.00
Bank Statement Balance	226.50

How to ensure bank insiders do not eliminate your record?

Scenarios IV



How to ensure a drunk key-holder not to open the gate arbitrarily?

Scenarios V

Scenarios V

How to make sure they are not printing all the time?

More Scenarios in a Bank

We probably did not mean the same requirement
In previous scenarios

What do they teach us?

**Security is a fuzzy/vague term, let's make
Is more precise**

Scenarios I

Identify the card owner — identification/user authentication

Not having access to other account — access control

Scenarios II

Secure transmission — confidentiality

The website is still on — availability

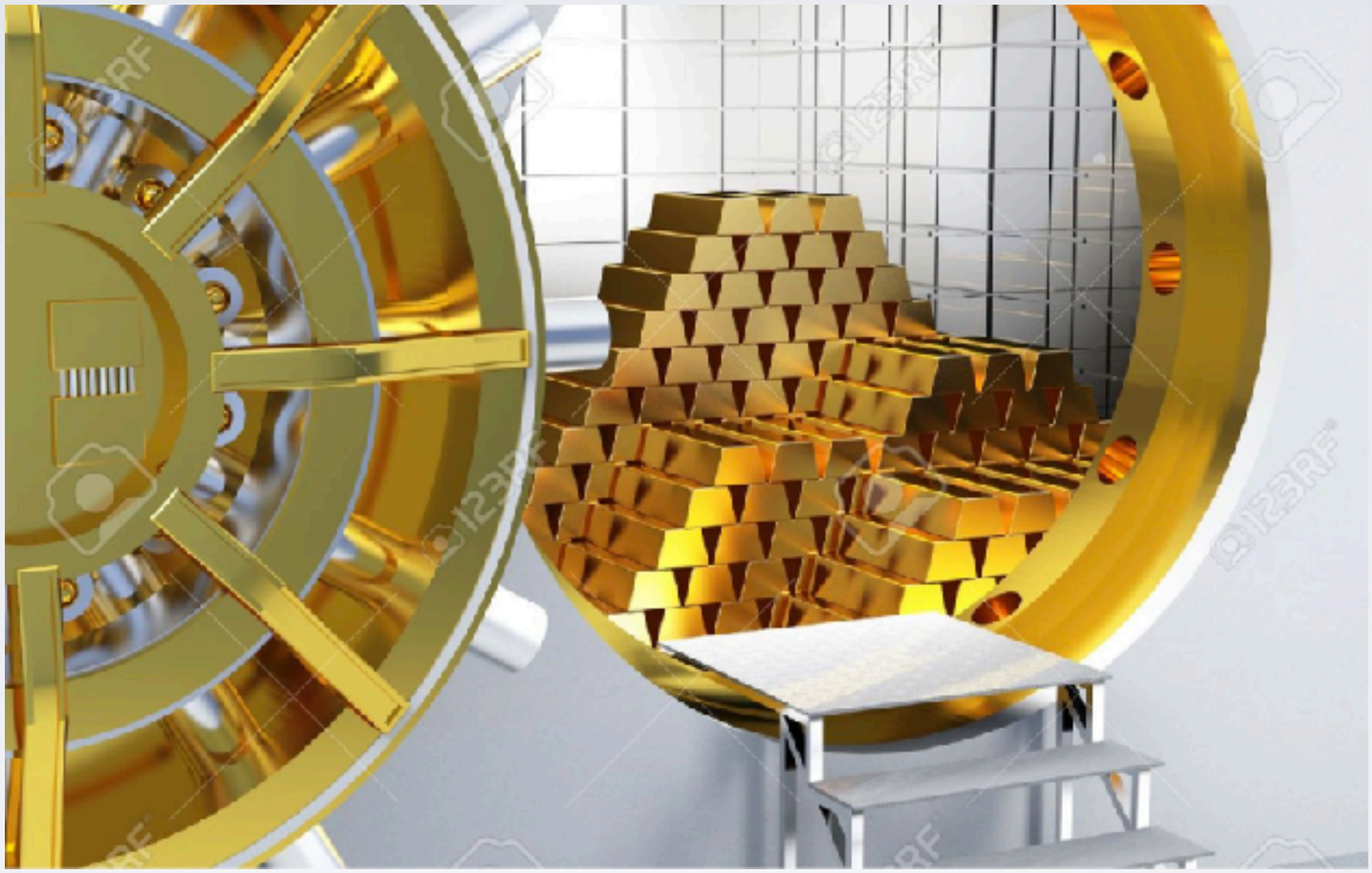
Scenarios III

Date	Description	Ref	Income	Expenses	Bank Balance	
1-Apr	Balance b/f				200.00	R
4-Apr	Folders and pens	1		15.00	185.00	R
15-Apr	Sale: Ms E Inkson	2	54.00		239.00	R
18-Apr	Sale: Mr R U Redy	3	30.00		269.00	R
19-Apr	Drawings	4		10.00	259.00	R
21-Apr	Envelopes & Stamps	5		20.00	239.00	R
24-Apr	Web host fees	6		40.00	199.00	R
27-Apr	Simply Chairs: Chair	7		127.00	72.00	
29-Apr	Sale: Mr J Mighty	8	30.00		102.00	R
30-Apr	Bank Fee	9		2.50	99.50	R
30-Apr	Sale: Ms T Real	10	54.00		153.50	
	Totals		168.00	214.50	153.50	C/f

BANK RECONCILIATION	
Cash Book Balance	153.50
Add: Unpresented check	127.00
Subtotal	280.50
Less: Deposit not yet showing	54.00
Bank Statement Balance	226.50

The intactness of the ledger —integrity/data authentication

Scenarios IV



Threshold access

Scenarios V

Accountability

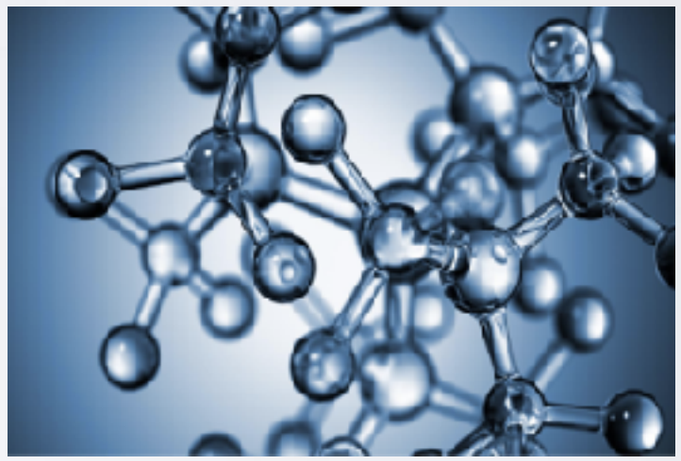
Decentralized system: cryptocurrency and blockchain

Are They Good Enough?

- Impersonation resistance, confidentiality, authenticity..

Still fuzzy/vague

Art v.s. Science



Art

- Mostly rely on artists inspiration — “the call from above”
- Hard to explain
- Hard to reproduce

Science

Understand the world following a systematic method based on evidence. a way of understanding the world through thought and experimentation. — wikipedia

Science

- Crisp definitions and models
- Rigorous argument and analysis
- Sound conclusions and theorems

The Danger

No one breaks it today does not mean it cannot be broken tomorrow — what exactly is the strength?

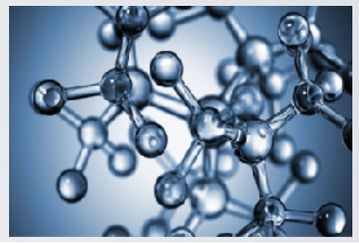
The Danger

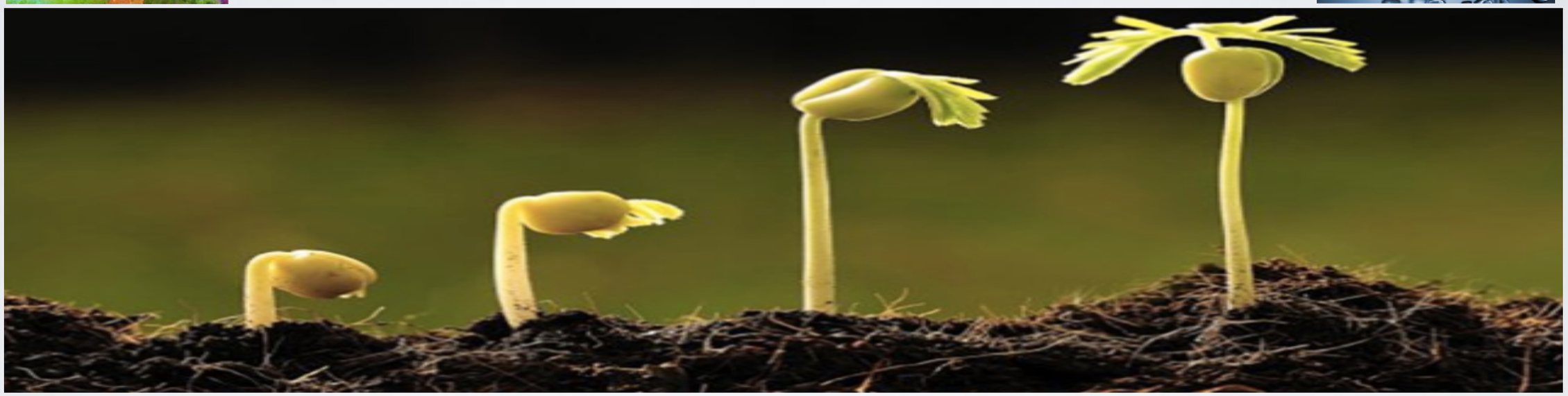
No one breal
broken tomo

Every system will be secure until it is broken

it cannot be
e strength?

Current Status





now

What is Security

Security is a fuzzy/vague term

To Model a Secure System

Think as an attacker

Think as a defender

Adversarial Thinking

Think as an attacker

What is attacker's capability?

What is attacker's goal?

Attacker Capability

Attacker can guess

Attacker can steal card

Attacker can peek

Attacker can destroy card

Attacker's Capability

Guess

Peek

Getting hold of the ATM?

Cut the electricity wire?

...

Attacker Goals

Attacker wants to withdraw money from your account

Attacker wants you not be able to withdraw money

.....

Attacker's Goal

Impersonate

Avoid card owner to use

Destroy bank reputation

...

Identification

PIN + Card solution defends against

Attacker who peeks but having no card

Attacker who guesses but having no card

Attacker who has card but only guesses

Not Attacker who steals card and also peeks

Not Attacker who destroys card

To Model the System

Think as a defender

Defender's Goal

Prevention

Detection

Response

Recovery

Deterrance

...

Defender's Capability/Cost

Secure Hardware

Secure Systems

Cryptographic Library

Isolated Network

Careful Employees?

...

Defender's Capability/Cost

Secure Hardware

Always have attacker in mind

Careful Employees?

...

Wooden Barrel Theory

Wooden Barrel Theory

Security of the system is determined by the weakest point

Next Lectures

Study some properties in more details