SYSSEC: THREAT MODELLING

AARHUS
UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

26 JANUARY 2025

DIEGO F. ARANHA
ASSOCIATE PROFESSOR

LOGISTICS FOR THE LAB

Virtual Box with the latest Ubuntu LTS release (25.04) as a **reference** platform

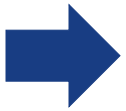
- Native environment is also fine, but you're supposed to know how to operate it

  Advantages: uniform CLI, packages, networking config
- We will announce package dependencies to be installed together with exercises
- Please try to come to class next week with it already preinstalled (we only need Python, but better to not delay)

WHO IS THE ADVERSARY?

1. The **spooks**:

- Governments and their surveillance programs (Five Eyes, PRISM, Tempora, Muscular against Google, XKeyscore, Bullrun)
- State-sponsored offensive operations (TAO division within NSA, Stuxnet/Flame malwares), investment in dual-use technology
- Advanced Persistent Threats (APTs) and espionage/information theft (China, North Korea)
- Control of non-trivial number of Internet nodes (global adversary)
- Disinformation campaigns and psychological operations (Russia and kompromat strategy)



Important: benefit a lot from **scale**, *attribution* can be **hard**.

WHO IS THE ADVERSARY?

2. The **crooks**:

- Cybercrime, botnet herders, malware developers
- Spam senders, data leakers, carders, ransomware campaigns
- Malicious insiders, CEOs, whistleblowers

3. The **geeks**: security researchers (academia and industry), activists, NGOs

4. The **swamp**: sex offenders, bullies, haters, abusive partners

WHAT IS THE ATTACKER GOAL?

- **S**poofing Identity: impersonate another person (user).
- **T**ampering: manipulate data without detection.
- **R**epudiation: deny doing something he actually did.
- **I**nformation Disclosure: access data he should not see.
- **D**enial of service: deny others access to a system.
- **E**levation of privilege: have more rights in a system than he/she was supposed to have.

One attack can achieve **multiple** goals.

WHERE IS THE ATTACKER?

- **E**xternal attackers: not users
- **I**nsiders: users with legitimate access or some privilege
- **N**etwork attacks: mounted remotely
- **O**ffline attacks: permanent data stored in disk, behind access control
- **O**nline attacks: in real time, by breaking defenses

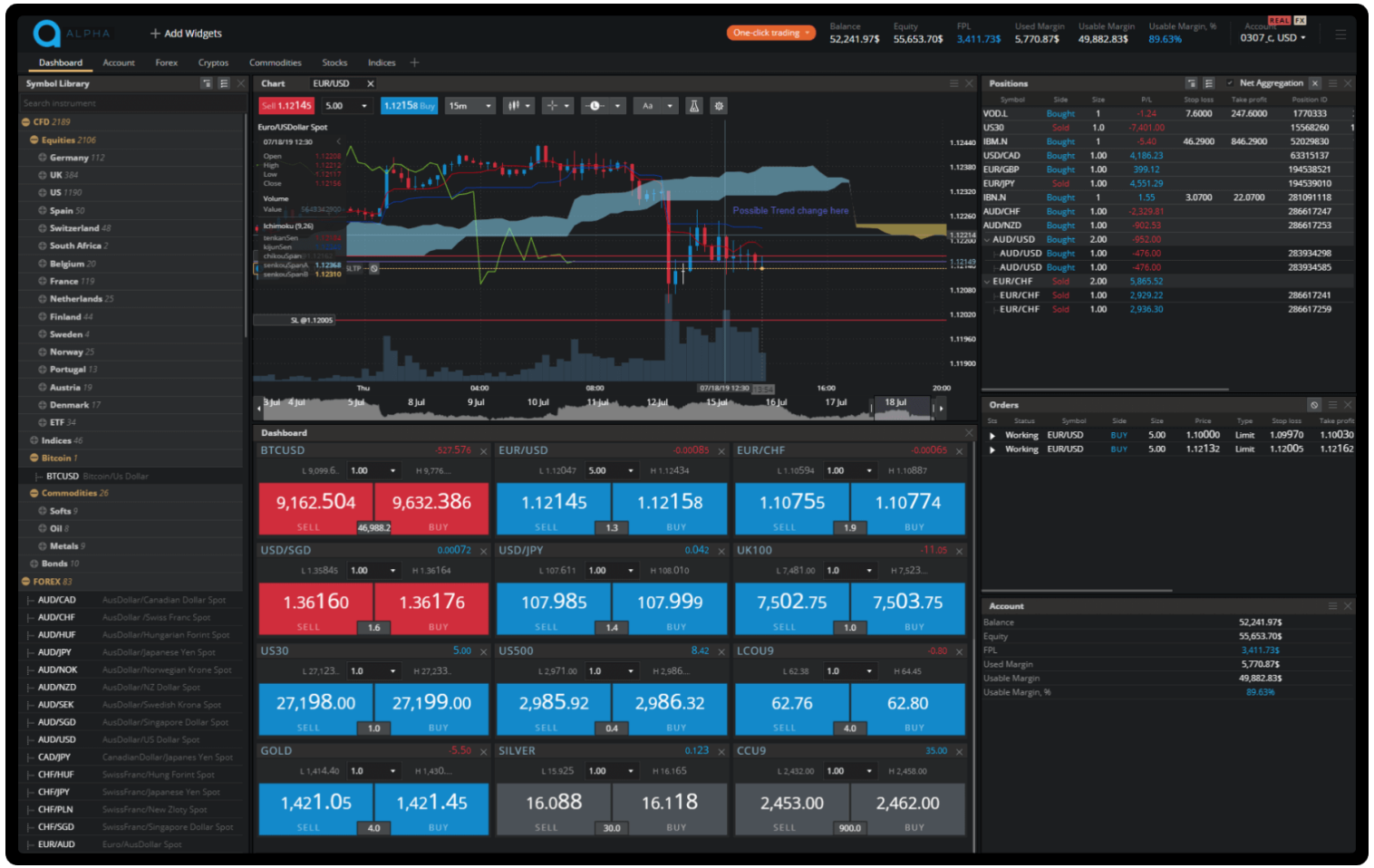
➡ Motivates the concept of *defense-in-depth*

THREAT MODELLING IS TRICKY

- Policies and mechanisms are as good as the model
- Can be flawed due to incomplete information, over-simplification, *lossy abstractions*
- Beware of **invalid** assumptions (e.g. misplaced trust)
- Beware of focus on the **wrong** threats
- Balance between pragmatism and paranoia

➡ *Important:* It should adapt to new threats.

EXAMPLE 1: ONLINE TRADING PLATFORM



EXAMPLE 1: ONLINE TRADING PLATFORM

Threat model (who, goal, where):

cybercriminals/crooks (remote, insider), spooks, geeks, swamp, with all the STRIDE goals

Attack surface: website, cloud infra, employeers, mobile app, broking info, network traffic, quality of assets

Policies: integrity (accountability), integrity of transactions, financial privacy, GDPR compliance, availability, authenticity and non-repudiation

Mechanisms: access control, logging, digital signatures, redundancy, backups, data encryption (rest and transit), TLS for network access, MFA

EXAMPLE 2: AN EMBASSY

EXAMPLE 2: AN EMBASSY

Threat model (who, goal, where):

Spooks, activists, swamp (terrorist)

Information disclosure, spoofing, DoS, tampering

Attack surface:

Employees, building, IT equipment, network, physical mail, documents, databases

Policies: authorization, confidentiality, integrity of data/personnel, availability

Mechanisms: access control, encryption (rest and in transit), digital signatures, physical security

THREAT MODELS CHANGE

Crisis in Kabul

This is the real story of the Afghan biometric databases abandoned to the Taliban

By capturing 40 pieces of data per person—from iris scans and family links to their favorite fruit—a system meant to cut fraud in the Afghan security forces may actually aid the Taliban.

by **Eileen Guo** and **Hikmat Noori** August 30, 2021

EXAMPLE 3: IOT PACEMAKER

EXAMPLE 3: IOT PACEMAKER

Threat model (who, goal, where):

Swamp (terrorism), crooks (ransom), spooks (target attack), security researcher

Information disclosure (wrt insurance), DoS, tampering, privilege escalation

Attack surface:

Bluetooth, hardware/device, cloud, mobile app, manufacturer/supply chain

Policies: data privacy, authentication, availability, integrity of data/firmware/device

Mechanisms: encryption, access control, lightweight consumption, firmware redundancy, monitoring platform, (trusted suppliers, couriers)

THREAT MODELS CHANGE

CRITICAL CONDITION —

Hospitals hamstrung by ransomware are turning away patients

The ransomware epidemic continues to grow.

DAN GOODIN - 8/16/2021, 9:26 PM

CASE STUDY I: PAPER ELECTIONS

PAPER ELECTIONS

Threat model (who, goal, where):

Spooks, crooks, activists, swamp

Politicians, other governments, companies, election officials, voters

Attack surface: ballot box, polling places, election officials, mail, social media, voter registration record

Policies: voter privacy, ballot integrity, accountability, transparency/observability/auditability, elligibility, availability

Mechanisms: physical security, voting booth, redundant counts, authentication of partial results, guidelines for votes, background checks on officials, government-issued credentials, biometrics, public place, ballot box shuffling

CASE STUDY II: ELECTRONIC ELECTIONS

AARHUS
UNIVERSITY