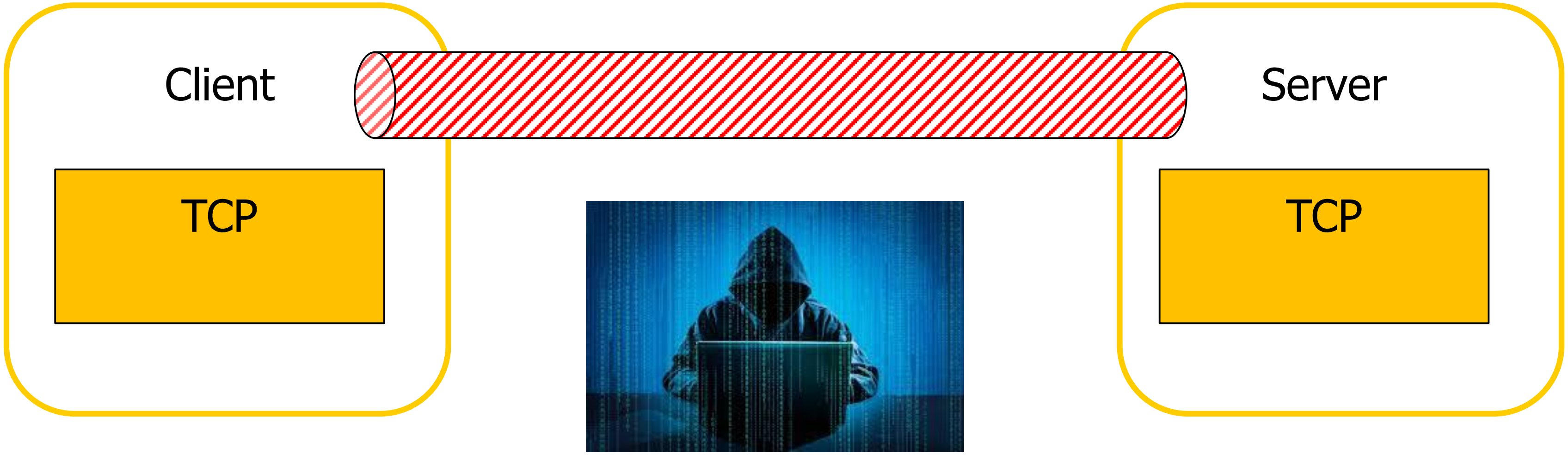
Threat Model

TCP: No Secrecy

No Secrecy



Client

TCP

Server

TCP

Network Attacker

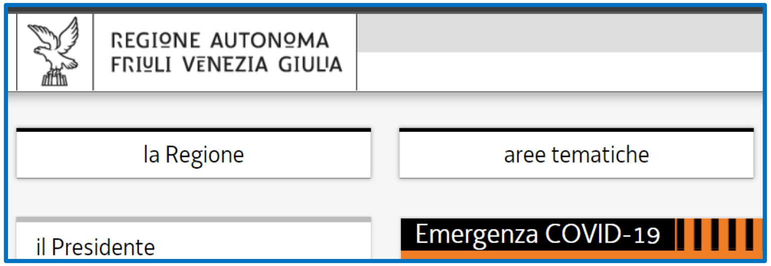
Can do "bad things" in the network

TCP: No Authentication

DNS

```
...
regione.fvg.it       A       IP-s
...
```

http://regione.fvg.it



TCP

IP-a

IP-s

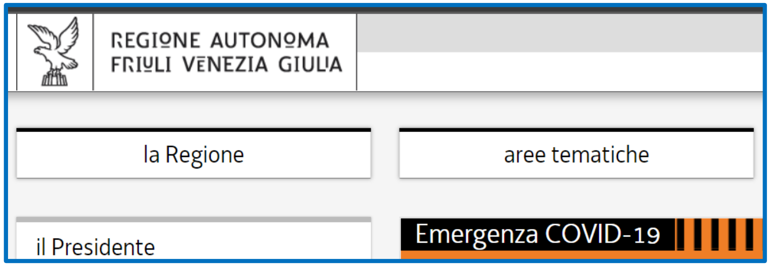
TCP

TCP: No Integrity

DNS

```
...
regione.fvg.it        A        IP-s
...
```

http://regione.fvg.it



REGIONE AUTONOMA FRIULI VENEZIA GIULIA

la Regione

aree tematiche

il Presidente

Emergenza COVID-19

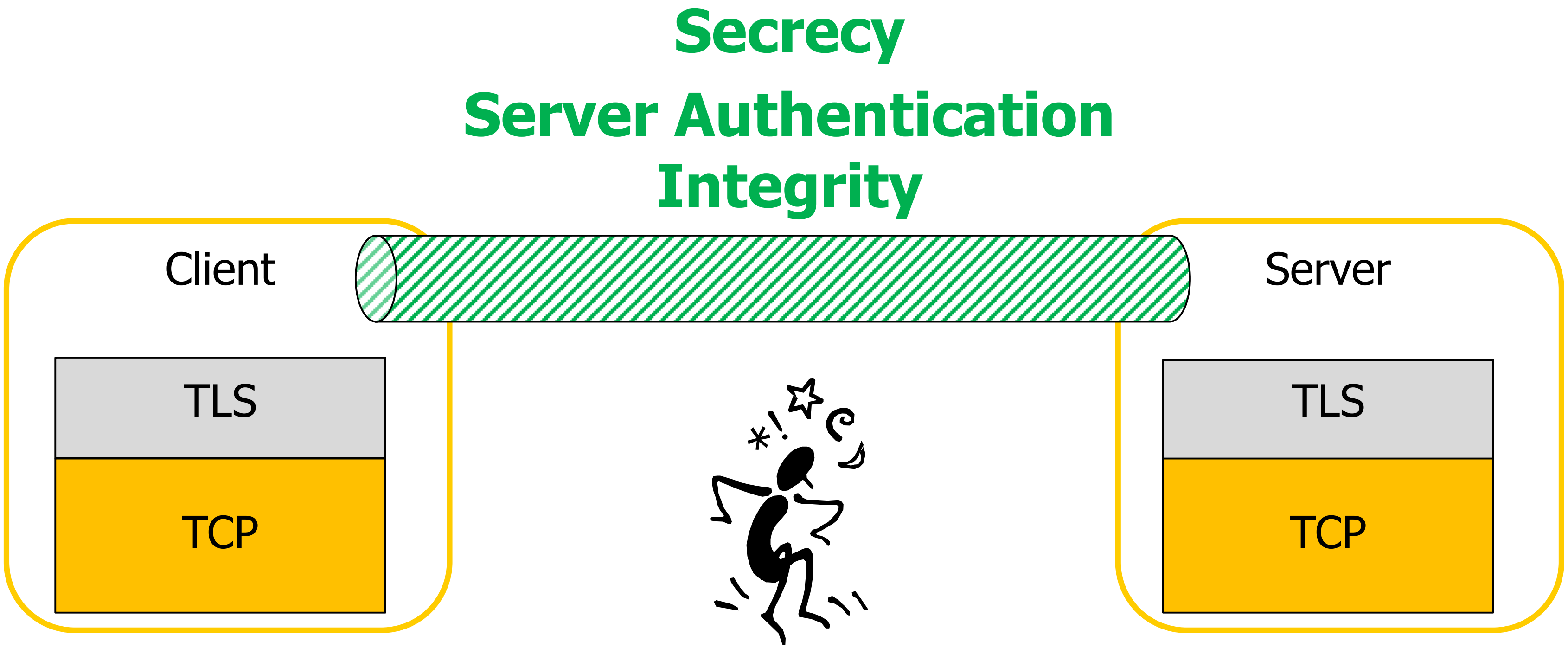
TCP

IP-a

IP-s

TCP

TLS: Security Properties



Secrecy

Server Authentication

Integrity

Client

TLS

TCP

Server

TLS

TCP

- **Cryptographic** techniques for “strengthening” TCP connection
- HTTPS : HTTP over TLS

Let's change scenario

- **Scenario 1**: Network Attacker

⇒ TLS guarantees Secrecy, Integrity, Authentication

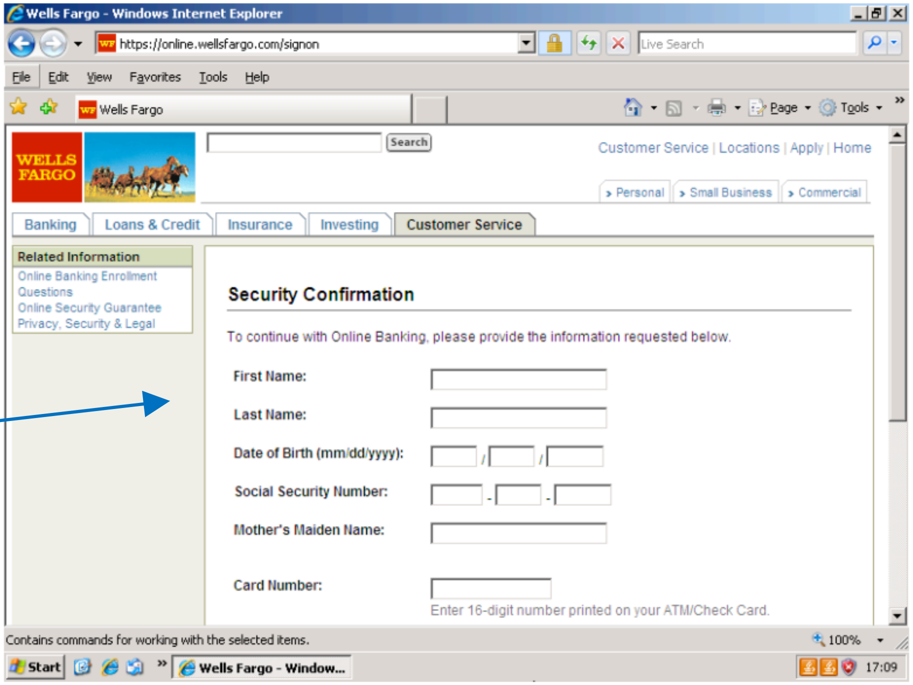
- **Scenario 2**: Attacker has installed **malware** in Client

…

Example

- **Malware** controllable and configurable from remote
- Can **modify** all web pages (HTTP or HTTPS)
- When on a configured banking site:
  - Fetches an HTML form from an attacker-controlled web site
  - Replaces the original form

Visually identical to the page sent by the banking site


Wells Fargo - Windows Internet Explorer
https://online.wellsfargo.com/signon
Live Search
File Edit View Favorites Tools Help
Wells Fargo
Page Tools
WELLS FARGO
Search
Customer Service | Locations | Apply | Home
Personal | Small Business | Commercial
Banking | Loans & Credit | Insurance | Investing | Customer Service
Related Information
Online Banking Enrollment
Questions
Online Security Guarantee
Privacy, Security & Legal
Contains commands for working with the selected items.
100%
Start
Wells Fargo - Window...
17:09

Security Confirmation

To continue with Online Banking, please provide the information requested below.

First Name:

Last Name:

Date of Birth (mm/dd/yyyy): / /

Social Security Number: - -

Mother's Maiden Name:

Card Number:

Enter 16-digit number printed on your ATM/Check Card.

Very important Question

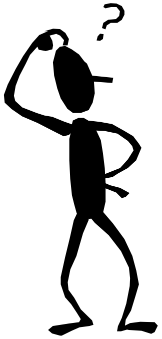
- **Scenario 1**: Network Attacker

⇒ TLS guarantees Secrecy, Integrity, Authentication

- **Scenario 2**: Attacker has installed **malware** in Client

⇒ TLS **does not** guarantee Secrecy, Integrity, Authentication

So, does TLS give me security guarantees or not????



It DEPENDS on the Threat Model

- **Threat Model**: Set of Attacker capabilities ("what the Attacker can do")
- FUNDAMENTAL Concept in cybersecurity

- **Threat Model**: Network Attacker

⇒ TLS guarantees Secrecy, Integrity, Authentication

- **Threat Model**: Attacker has installed **malware** in Client

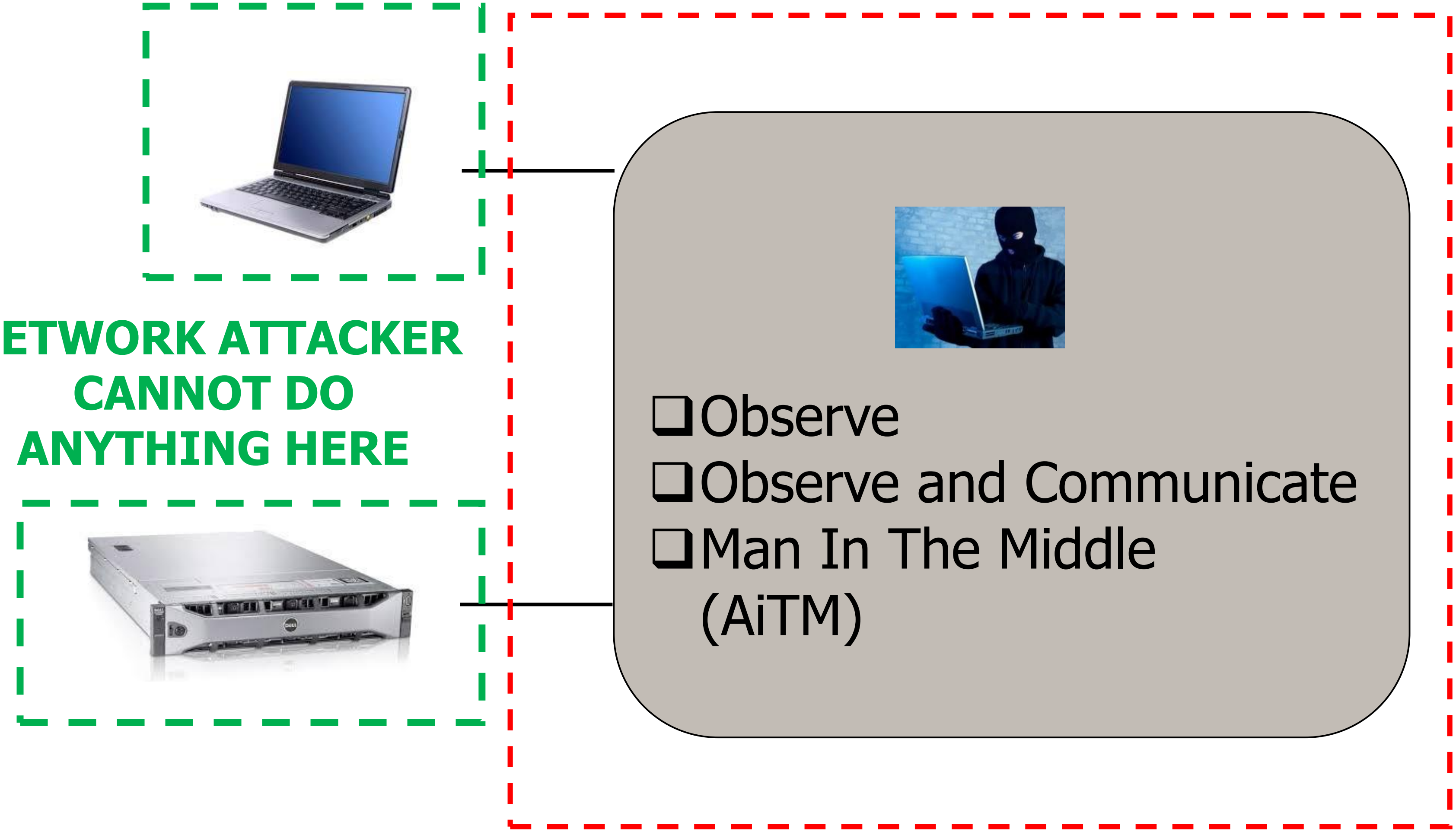
⇒ TLS **does not** guarantee Secrecy, Integrity, Authentication

ALWAYS specify the Threat Model!

- Reasoning about "security of a system" **does not make any sense**

- You must **always** reason in terms of "security of a system with a **specified** threat model"

Threat Model: Network Attacker

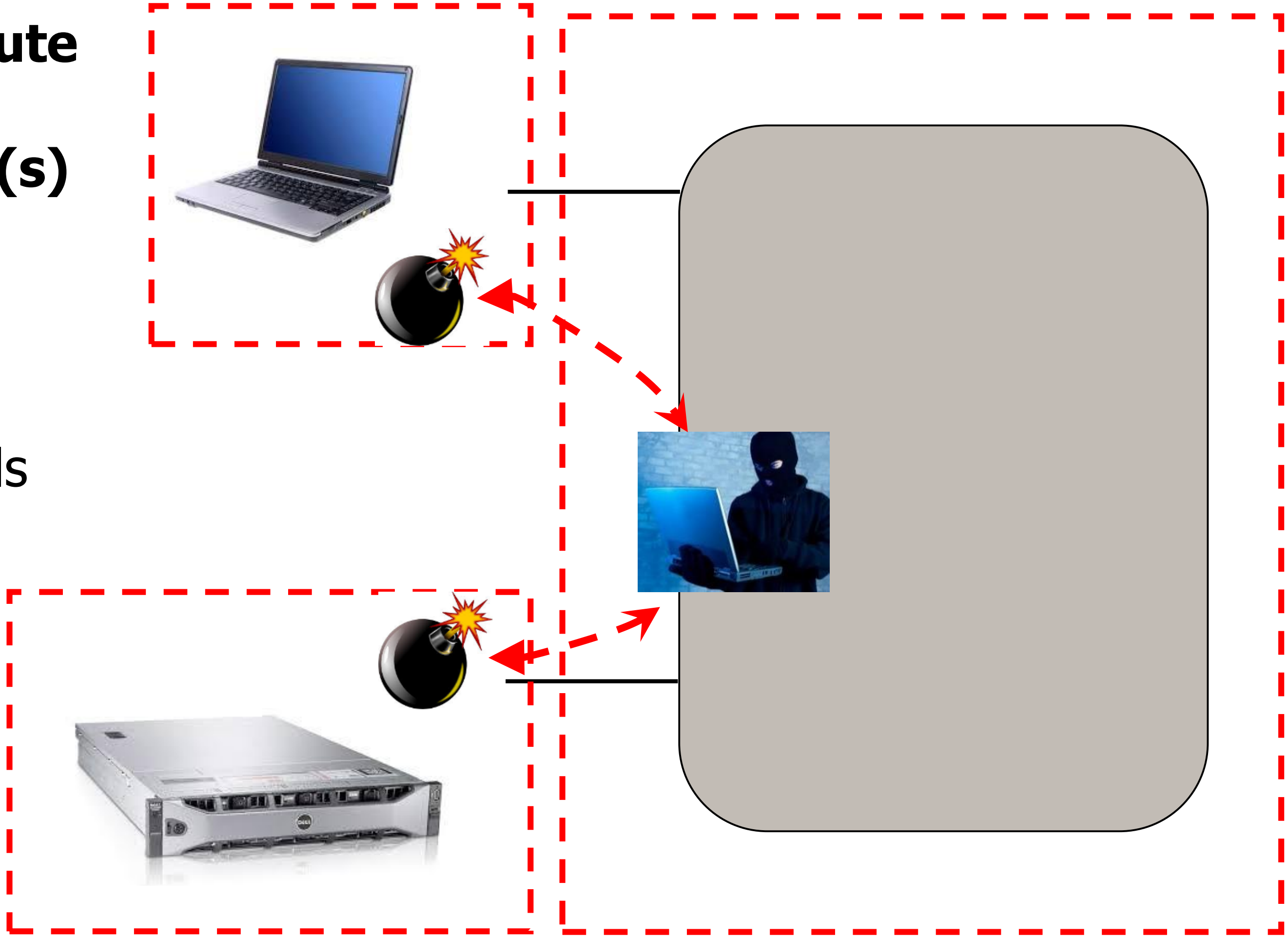


NETWORK ATTACKER CANNOT DO ANYTHING HERE

- □ Observe
- □ Observe and Communicate
- □ Man In The Middle (AiTM)

Threat Model: Compromised endpoint (I)

- **Attacker can execute some actions on some endpoint(s)**
- Realistic?
  - Vulnerabilities
  - Stolen credentials
  - …



Threat Model: Compromised endpoint (II)

- Attacker can:
  - Read **some** information
  - Read **every** information
  - **Execute** some existing procedure
  - **Execute arbitrary code**

Pessimism

Other Relevant Threat models

- **Physical access**
  - "If a bad guy has physical access to your computer, it is not your computer anymore"
- **Insider**
- **Supply chain compromise**

Every defensive tool has a Threat Model

- Whenever you have a **defensive tool, understand its threat model**

- From what attacks does this tool defend me?
- From which attacks does it **not** defend me?

Example: HTTPS (as most crypto defenses)

- Network attacker
  - Observe
  - Observe and Communicate
  - Man In The Middle

Secrecy
Integrity
Authentication

- Compromised endpoint
  - Malware

~~Secrecy~~
~~Integrity~~
~~Authentication~~

- Physical access

~~Secrecy~~
~~Integrity~~
~~Authentication~~

- Supply chain compromise
  - Software libraries (or a lot of other things)

~~Secrecy~~
~~Integrity~~
~~Authentication~~

Exams: Important suggestion

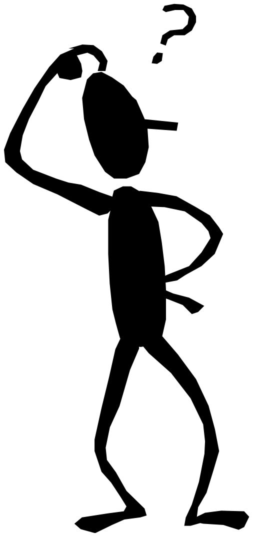
- *Discuss attack X*
- *Discuss defense Y*
- **Always describe the assumed threat model!**

- Phishing
  - The attacker needs the ability to send an email to the target and to control a website reachable by the target
- Kerberoasting
  - The attacker needs to have valid credentials and needs to be able to contact the domain controller

Understanding Threat Models

Naive question 1

- *How can I tell what Attackers can do?*
- *Maybe my threat model is too optimistic!*



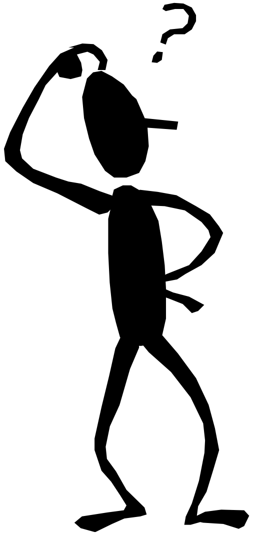
Threat MODEL

- It is a **model**
- You make some **hypotheses** about Attackers and then reason accordingly
- If the Attackers are more powerful than you assumed then your defenses will not work

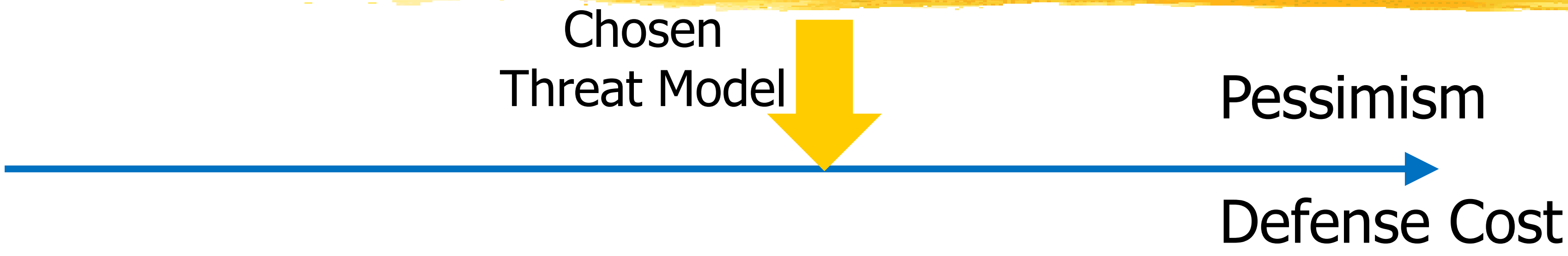
- It is **impossible** to guarantee that **real** Attackers will adhere to your **model**

Naive question 2

- *Why not choose the most pessimistic threat model?*



More pessimism implies More costs



Chosen
Threat Model

Pessimism

Defense Cost

- Who can afford to build everything with threat model Supply chain compromise?
- In practice:
  1. Choose a "reasonable" working point
  2. Cross your fingers

REMIND…

- To understand cybersecurity **never** think only in **technical** terms
- **Always** think in **economical** terms

- What is the cost?
  - Attack, Defense, Incident
- Who pays?

- **Money is what drives the world**
  - It may sound cynical…but thinking in these terms is very helpful

No predefined list to choose from

- Some threats are **general**
  - Modifying / Forging network messages
  - Stolen password
- Some others may depend on a **specific** environment
  - Frequent usage of external personnel on networking devices
  - Wide freedom in physical access
  - Low skilled staff can operate on key applications
  - ...
- No list (sort of "partial order")

Threat model for organizations

- **"Assume breach"**

  1. An attacker has **control of a computer** on the **internal** network

  +

  2. can access the **same resources** the **users who have recently logged on to that computer** have access to.

- **Only** realistic model for organizations today
  - It suffices to obtain 1 valid password / compromise 1 PC

- Lots of (bad)implications

Suggestion: Forget "how"

- You are assuming a certain threat model

⬇

- **Forget** about how the Attacker can arrive there
  - There are usually **a lot** of **complex** ways
  - You would get **confused** and **miss the focus**
  - Just **take it for granted**

Example

- **Network attacker**
  - Man In The Middle
- DNS spoofing
  (Windows environments with IPv6 enabled - "all of them")
- ARP spoofing
  (open WiFi, "single password" WiFi in promiscous places)
- BGP spoofing
- Vulnerabilities in network devices
- Dishonest administrators (access point, router, DNS server)
- Judicial authorities / Intelligence agencies
- ...

Consequence: "Think in modular steps"

- You are assuming a certain threat model
- You realize that the Attacker can increase capabilities (= more pessimistic threat model)
  - Network attacker with working exploit
  - Can inject the exploit → Compromised endpoint

⬇

- Assume the new threat model and **forget** about how you arrived there