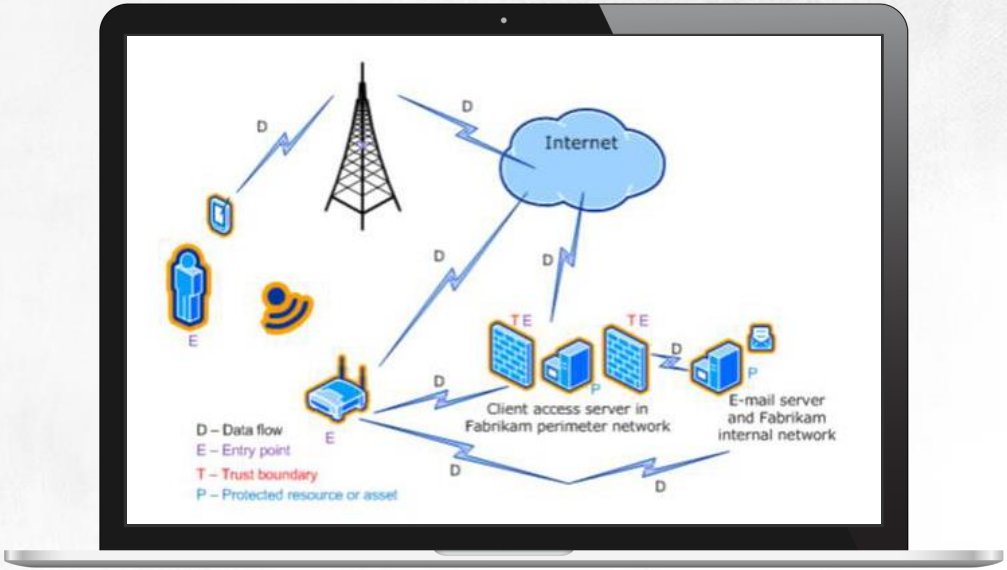

THREAT
MODELLING
AND
CLASSIFICATION

THREAT MODELLING

THREAT MODELLING COMPRISES OF THE IDENTIFICATION, EVALUATION AND DOCUMENTATION OF THREATS THAT APPLY TO A COMPUTER SYSTEM

To identify the attacker's possible goals, you need to approach threat modelling from an attacker's POV:
Establish:

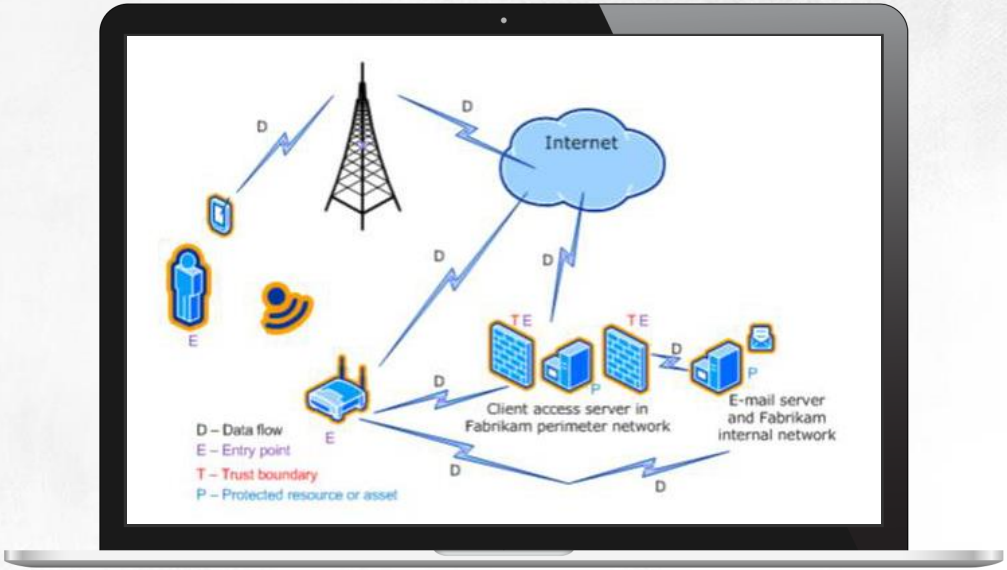
- Potential Entry Points (E)
- Protected Resources or Assets (P)
- Data Flows between the system's parts (D)
- Trust Boundaries in the system (T)



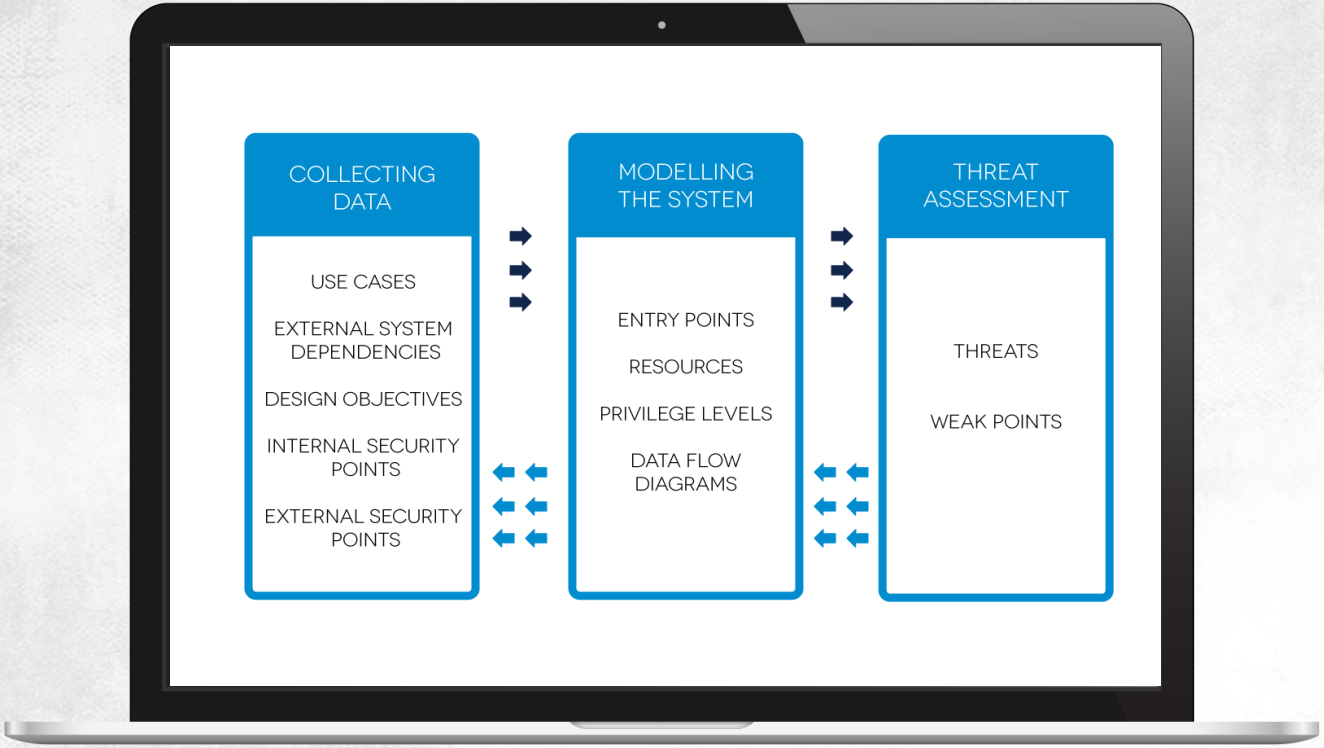
THREAT MODELLING

The level of detail in a diagram has to be broad enough to cover all protected resources and reflect all scopes of potential threats

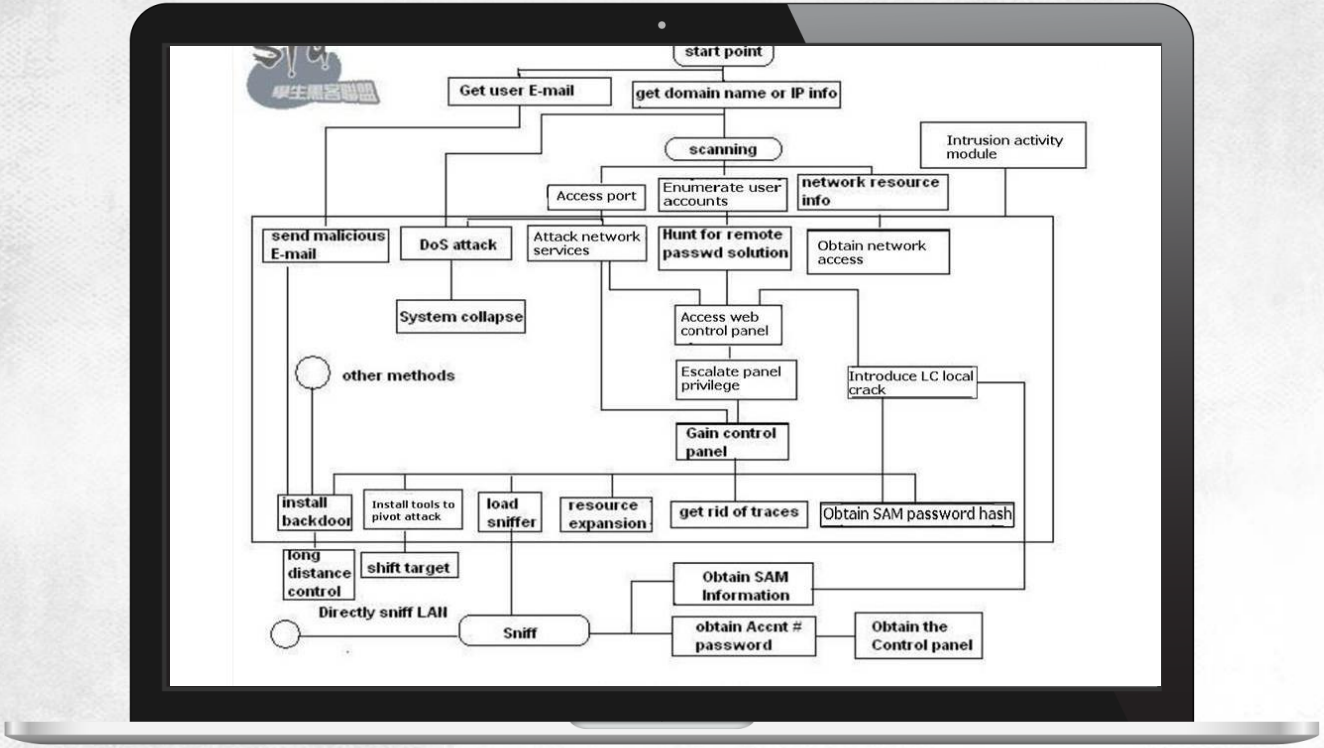
EACH RESOURCE TAKES AN AGREED NUMBER STARTING FROM 0 (NEGLIGIBLE) TO 4 (CRUCIAL)



THREAT MODELLING



THREAT MODELLING

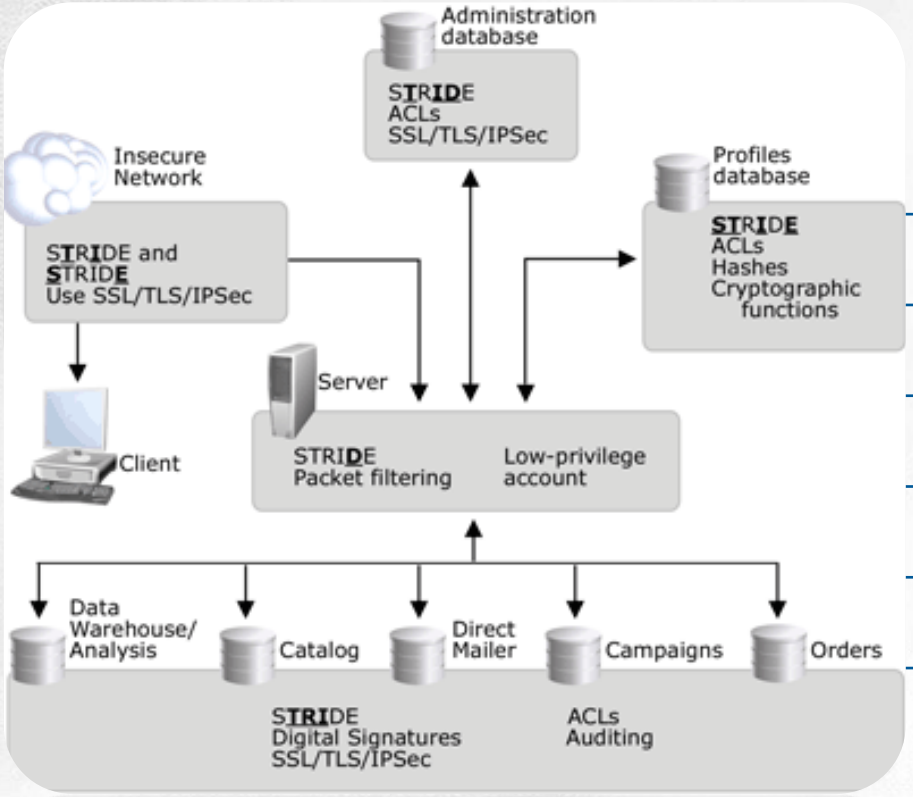


THREAT MODELLING

WHILE IT IS RELATIVELY EASY TO IDENTIFY RESOURCES, MODELLING SPECIFIC THREATS PRESUPPOSES A DEEP KNOWLEDGE OF THE MODERN ATTACK PATHS AND TECHNIQUES

The assumption for threat modelling is that the attacker will not target a system that doesn't store some attractive resources. Because of that, it's worth it to reverse the natural order in securing the system and start with presenting a classification of the results of a successful intrusion rather than with a risk assessment

STRIDE



SIX CATEGORIES OF THREATS:

- **S**poofing Identity
- **T**ampering with Data
- **R**epudiation, Deniability
- **I**nformation Disclosure
- **D**enial of Service
- **E**levation of Privilege

STRIDE **SPOOFING IDENTITY**

Occurs when user's or a service's identity is used illegally. Examples:

An attacker creates a rogue website made to look like a legitimate website and confirms its authenticity by establishing an SSL session as the website

Sending spoofed, digitally-signed emails that pretend to be sent from another user

Spoofing certificate-based authentication systems to get elevated privilege access to the system

Obtaining digital signatures for malware using Authenticode that says it was issued for a trusted company

CASE STUDY

Spoofing Identity

DURING A NATIONAL CENSUS

in a country in Europe, an application was shared to enable citizens to complete their census forms online.

It transpired it could leak the addresses and dates of birth of entrepreneurs or people who had their resident ID numbers published online

CASE STUDY

Spoofing Identity

ANYONE COULD IMPERSONATE THESE PERSONS AND COMPLETE A CENSUS FORM BY PROVIDING FAKE DATA ON THEIR BEHALF:
To create an account, you only needed to provide your resident ID and first and last name or your taxpayer ID or the place of birth or the birth name of your mother. Taxpayer IDs and resident IDs of entrepreneurs were public information

YOU CAN FIND A PERSON'S FIRST AND LAST NAME IN A SOCIAL ENGINEERING WEBSITE. They also can contain their addresses, years of birth and even the birth names of their mothers. Once you provided this info, the application automatically filled out the address field

USER PASSWORDS IN THE APPLICATION were provided in the plaintext. To discover them, you simply had to call a help line and submit the info you already knew (like the taxpayer ID) to have a consultant give you the password

STRIDE

Tampering with Data

THIS THREAT RELATES BOTH TO PERSISTENT DATA STORED ON HARD DRIVES AND DATA THAT IS PASSED OVER NETWORKS

It's the number one target for attackers since day one

TAMPERING WITH DATA MAY LEAD TO SERIOUS CONSEQUENCES:

- Malicious modification of websites to put up propaganda and spread misinformation
- Tampering with data used in a system can allow attackers to control these systems
- Changing business information may mean that parties reach a decision based on false data provided by an attacker

STRIDE

Repudiation, Deniability

REPUDIATION TAKES PLACE WHEN
you are unable to prove it that a person has performed a specific action or has sent a specific message

IT GREATLY RELEVANT FOR E-BUSINESS
as such and informs the ability or inability to identify and charge culprits responsible for launching an attack

STRIDE

Repudiation, Deniability

IN 2009 THE CHIEF IT ADMINISTRATOR of an employment centre was arrested on charges of illegally obtaining unemployment benefits by creating fictitious records. He created addresses and IDs for fictitious persons, entered the data into the centre's computer network and then received the benefits for non-existing people, gaining about 40 thousand dollars.

BECAUSE HE NEVER PLEAD GUILTY and the computer system used by the centre did not ensure non-repudiation, the prosecution case was based on circumstantial evidence

STRIDE

Information Disclosure

ALL TYPES OF THREAT THAT GIVE UNAUTHORIZED PERSONS THE ACCESS TO CONFIDENTIAL INFORMATION OR OTHER VALUABLE DATA

Information disclosure may also involve the obtaining of sensitive data which makes it possible to run a social engineering attack or impersonate another user. Between 17 and 19 April 2001 attackers broke into PlayStation Network and Qriocity, both Sony services, and sniffed out data like usernames, passwords, names, addresses and emails, birthdates and, likely, shopping credit card details belonging to more than 80 million customers

STRIDE

Information Disclosure

INFORMATION DISCLOSURE COVERS ALSO ALL threats related to unauthorized persons obtaining data that makes running an attack easier. The virus that crept into computers in the Creech Air Force Base was found out to register every operation logged by operators of unmanned aircrafts like Predator and Reaper, both used by the US Army to conduct military operations in Libya, Afghanistan and Iraq

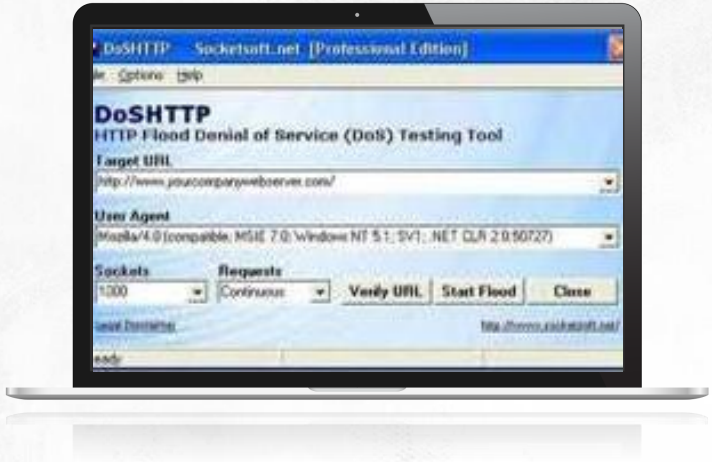
STRIDE

Denial of Service

THIS ATTACK TEMPORARILY DENIES VALID USERS THE USE OF A SERVICE PROVIDED BY A SERVER

Most cases of denial of service attacks lead to sever overload by flooding it with a high number of requests (if these requests come from a number of hosts controlled by attackers, we can speak of a distributed denial of service attack, DDOS)

Denials of service may also be launched through the use of specially-crafted incorrect requests

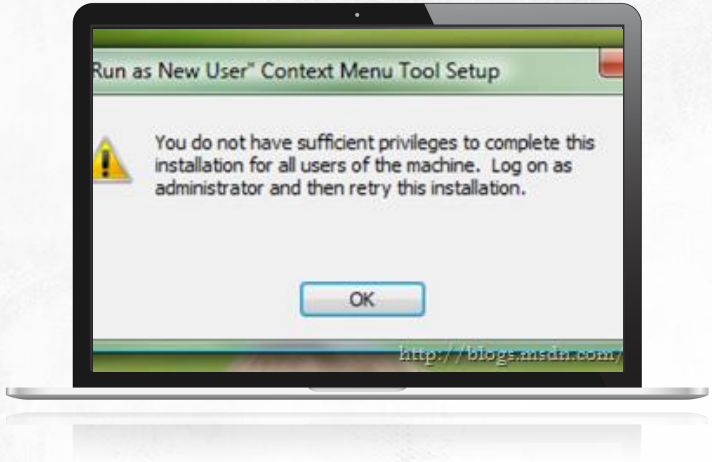


STRIDE

Evelation of Privilege

OCCURS WHEN UNAUTHORIZED PERSONS, WHO ALREADY HAVE OBTAINED ACCESS TO A TARGETED SYSTEM, NOW OBTAIN PERMISSIONS THEY ARE NOT PRIVILEGED TO HAVE

Attackers who run this type of attack usually exploit an existing vulnerability in a program or operating system or exploit system users' carelessness or ignorance



STRIDE

Security threats in a database server: A classification

THREAT	CATEGORY	RECOMMENDED COUNTERMEASURES
WEAK PASSWORDS	S	ENFORCING PASSWORD RULES
NOT AUDITING USER ACTIVITY	R	DDL, DML AND LOGON TRIGGERS, AUDIT SESSIONS, TRACE FILES
DISCLOSURE OF CONFIDENTIAL INFORMATION	I	ENCRYPTING DATA OR ENTIRE DATABASES
DISCLOSURE OF A DATABASE STRUCTURE	I	VIEW DEFINITION PRIVILEGE CONTROL
UNPRIVILEGED ACCESS TO OBJECTS OR DATA	E	SEPARATING SCHEMAS FROM USER ROLES, SIGNING CODE MODULES
RUNNING UNTRUSTED CODE	E	CHANGING THE CONTEXT OF A EXECUTING A MODULE
INTERCEPTING USERNAMES AND PASSWORDS	S	ENCRYPTING AUTHENTICATION DETAILS SENT OVER NETWORKS
UNAUTHORIZED DATA MODIFICATION	T	DENYING USERS TABLE PERMISSIONS, EXECUTING ALL MODIFICATIONS THROUGH STORED PROCEDURES
ESTABLISHING MULTIPLE SIMULTANEOUS SESSIONS	D	USING LOGON TRIGGERS TO LIMIT THE MAXIMUM NUMBER OF CONNECTIONS, AUTOMATICALLY CLOSING AN INACTIVE SESSION

THANKS