Threat analysis

Tuomas Aura

CS-C3130 Information security

Aalto University, 2021 course

Outline

- Security terminology
- Threat analysis
- Threat modeling example
- Systematic threat modeling

SECURITY TERMINOLOGY

What is security

- When talking about security, we are concerned about bad events caused with malicious intent
  - Security vs. reliability?
- Security is a non-functional property of a system
  - Comparable to quality; difficult to verify and measure
- Security is a moving target
  - The adversary is intelligent and creative; creates new threats
  - When will crime finally end?

Some security terminology

- Threat = bad event that might happen
- Attack = intentionally causing the bad thing to happen
- Vulnerability = weakness in an information system that enables attacks
- Exploit = implementation of an attack
- Risk = probability of an attack × damage in euros

Security Goals

- Confidentiality, Integrity, Availability "CIA"
  - Confidentiality — protection of secrets
  - Integrity — only authorized modifications
  - Availability —service works, business continuity
- Examples: web server, customer data
- Many security goals are not covered by CIA:
  - Access control — only authorized use of resources
  - Privacy — control of personal data and space

Some goals not covered by CIA

- Authentication for access control and accountability
- Correct accounting, fair payment
- Content protection
- Protection of services and infrastructure
  in a hostile environment (e.g. Internet)
- Anonymity, freedom of expression
- Control and monitoring

Who is the adversary?

- We divide the world into good and bad sides
  - Honest parties vs. attackers; red vs. blue; trusted vs. untrusted
  - Good ones follow the specification, bad ones do not
- Multilateral security: must consider all different partitions of the participating entities to good and bad
- Often, we only care about some attackers, not all
  - Who would you not want to see your Telegram messages?

Typical attackers

- Typical attackers:
  - Curious individuals
  - Friends and family
  - Dishonest people — for personal gain, making and saving money
  - Hackers, script kiddies — for challenge and reputation
  - Companies — for business intelligence and marketing, industrial espionage
  - Organized criminals, rogue countries — for money and power
  - Governments and security agencies — NSA, SVR RF, GCHQ, DGSE, etc.
  - Military SIGINT — strategic and tactical intelligence, cyber defense
- Insiders are often the greatest threat
  - Employee, administrator, service provider, customer, family member

THREAT ANALYSIS

Viewpoints to threat analysis

Different viewpoints to threat analysis:

- Assets
  - What has value and how could it be lost? !
  - What are the business objectives? What could put them at risk?
- Potential attackers and their motivation
  - Who could do something bad and why? !
  - Start by enumerating the actors and stakeholders the system
  - Insiders are often the greatest threat

Viewpoints to threat analysis

- Engineering
  - How does the system work? What are the system components and processes? How could they fail? !
  - Draw system architecture, data flow diagram, etc. Analyze potential vulnerabilities in each component
- Countermeasures
  - Are there known ways to prevent or mitigate attacks?
  - What security protections have been deployed or suggested? Why or why not?
  - Is the purpose of security mechanism understood? Are they effective?

Viewpoints to threat analysis

- Checklists, lessons learned, best practice guidelines
  - What can experience and past mistakes teach us?
- Compliance
  - Are there regulatory, contractual or standards compliance requirements?
- Risks analysis methodology
  - How likely are the threats and how much damage would they cause?

Threat analysis requires both security and domain expertise

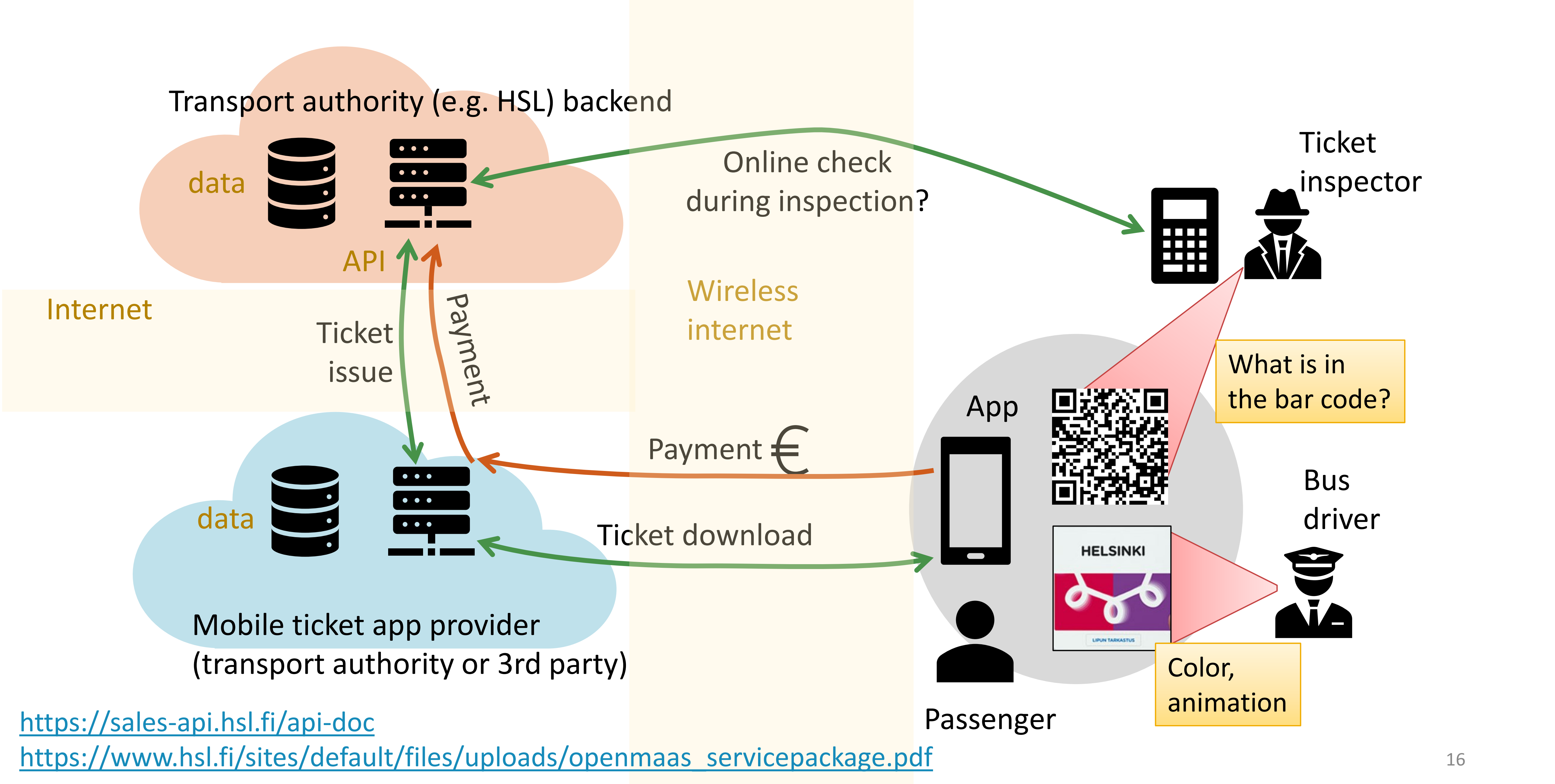
What I find most productive

- Given a system or product
  1. Understand the system architecture, operation, and business
  2. What assets are there that could be lost or damaged?
  3. Who are the actors in the system? Why might they break rules?
  4. What are the threats and potential attacks against the assets? What vulnerabilities might there be? Gather and organize ideas iteratively.
  5. Prioritize threats based on the risk and cost of mitigation

- Focus on understanding and intelligent analysis,
  not on a formal process or structure

THREAT MODELING EXAMPLE:
PUBLIC-TRANSPORT TICKET APP

Mobile ticket system architecture



https://sales-api.hsl.fi/api-doc
https://www.hsl.fi/sites/default/files/uploads/openmaas_servicepackage.pdf

Business model

- Fare structure and ticket types (pricing and product selection)
  - Based on zones, distance, time?
  - Influenced by political decisions
  - Poorly designed fare structure may lead to non-optimal resource usage
- Open vs. closed boarding
  - In closed boarding, a ticket gate or driver always checks the ticket
- Payment
  - For ticket app, payment is made just like in any online store
  - Public transport system typically require pre-payment

- Public subsidy: 50% ticket income, 50% public subsidies
- Purchaser-provider model (*tilaaja-tuottajamalli*)
  - EU Regulation on public passenger transport services (1370/2007)

Assets

- Money
  - Money paid or saved for tickets
  - Public subsidy
- Transport service
  - Right to travel
  - Transport capacity
  - Passenger numbers, customer satisfaction, reputation
- Personal information, business data
  - Passenger identity, travel history, location, statistical data
  - Credit card details and other payment information
- System components: the app, scanner, online services
- Data items: ticket, cryptographic secrets, messages

Actors

- Passenger
- Transport authority (HSL)

  = “competent authority responsible for organizing public transport on their service area”,
- Transport operator
- Ticket app provider
  - Either the transport authority itself or a Mobility as a Service (MaaS) provider
- Insiders:
  - Employees of transport authority, incl. ticket inspector
  - Driver and other employees of transport operator
  - Backend administrators, backend and app developers
- City and taxpayers
- Outsiders?

Potential attackers and their motivation

- Passengers: want free travel, cheaper travel
- Transport authority: trusted public servants?
  - Perhaps wants more funding and increased authority
- Transport operators: extra payment, subsidies, tax savings, transport data for competitive advantage
- Insider attackers: make money, get free travel
- Criminals, cybercriminals: make money
- Passengers’ family, police, stalkers, advertisers etc.: personal information
- Outsiders, vandals, hackers on the Internet

Threats / attacks by passengers 1

- Riding without a ticket in open ticketing (e.g., metro and bus 550)
- Fake ticket
  - – Edited screenshot
  - – Fake ticket app can replicate also animation and changing colors
    - HSL ticket is HTML generated by transport authority. What is in the bar code?
- Sharing authentic tickets
  - – Cloning the ticket (how strong is the binding to the phone or user ?)
  - – Passback = two people show the same ticket (and phone) to the inspector
  - – Timesharing: using the same monthly ticket (and phone) at different times
    - Was a problem with travel cards, but would anyone share their phone?
    - What information do inspectors have for identifying the passenger?
  - – Realtime relay of tickets from one phone to multiple passengers

Threats / attacks by passengers 2

- Misuse of discount tariffs (student, city resident)
  - App now checks student status and residence from online databases
- Misuse of failure recovery processes
  - Appealing to the bus driver's kindness on false grounds
  - If the phone battery is dead, inspectors may ask the phone number and check online → give someone else's number who has a ticket
  - If you forget a valid monthly ticket at home and get a penalty fee, it may be possible to cancel the fee afterwards → two people can share a ticket, let a friend borrow your ticket and have your penalty fees cancelled
  - Misuse of ticket refund or customer complaints
    - Better refund tickets only to the app or travel card and not in cash

Other threats / attacks to make or save money

- By mobile app provider:
  - Charging passengers for unissued tickets; selling intentionally invalid tickets
  - Not paying the transport authority for purchased tickets
- By insiders (driver, IT staff etc.):
  - Driver may let friends travel without a ticket
  - Staff may create free tickets for themselves and for friends
  - Misuse of refund policies (what policies are there?)
  - Limited financial damage unless it becomes a business
- By outsiders and hackers:
  - Hacking the backend system from the Internet (fake tickets, ransomware)
  - Any attacks against the app on the phone?

Probably not so significant threats

- By criminals:
  - Ticket theft or resale not a threat, unlike for physical tickets
  - Sale of fake ticket apps – could become serious organized crime
- By transport operators:
  - Limited opportunity for fraud. Subsidy fraud and tax fraud may not be possible in the purchaser-provider model
- Fraud against the payment systems:
  - Tickets are typically paid in advance; thus, no credit risk
  - Credit card fraud is possible
  - HSL already has 5% of unpaid passengers in open ticketing

Threats / attack that misuse authority

- By ticket inspectors:
  - Not easy to steal money from penalty fees because not paid in cash
  - Bonus system for ticket inspectors may lead to excessive issuing of penalty fees
- By transport authority:
  - Innovation by the authority always expands its power
  - Intentionally block private-sector competition (MaaS services), e.g., with API design or tariff structure

Threats / attacks against data

- Leaks of identity, addresses and payment information
- Misuse of individual travel data:
  - Tracking and stalking people by insiders, hackers (real-time or history)
  - Commercial use of location and travel history
  - Law-enforcement access to location and travel history
  - Storing identifiable travel history unnecessarily, sharing identifiable data
- Misuse of bulk travel data:
  - Travel data gives transport operator a competitive advantage in bidding processes: obtain it secretly, or refuse to share it

Summary

- Main threat is still passengers not paying for tickets
  - An old and well-understood problem
- Petty fraud by insiders is not a great financial risk but nevertheless unacceptable
- Cyber criminals may target any online service or data
- Need to keep an eye on unlikely but serious systemic threats:
  - Opportunities for criminals or insiders to make money
  - Systematic corruption of employees or organizations
  - Better not have any way to convert tickets back to cash

What next?

- Next steps in a professional threat analysis project:
  - Obtain full specifications and read them carefully
  - Interview the system designers
  - Reverse engineer components for which full documentation is not provided (e.g., APIs, QR code , ticket HTML)
  - Learn about relevant regulation, standards and similar specifications, which can give clues both to the system design and to the threats
    - EU Regulation on public passenger transport services (1370/2007), http://docs.maas-api.org/
  - Interview designers of similar systems (budget for travel!)
  - Analyze risk and business impact

Reporting

- Present the findings and get feedback from your customer a before finalizing the report
- Highlight high risks and new threats
  - Aim for balanced discussion, not scaremongering
- Recommend some action points even if it was not your task
  - More helpful and harder to ignore than a report that only lists threats
  - E.g., technical mitigations, risk monitoring and reduction
- Document even low-risk and out-of-scope threats

SYSTEMATIC THREAT MODELING

Basic security goals

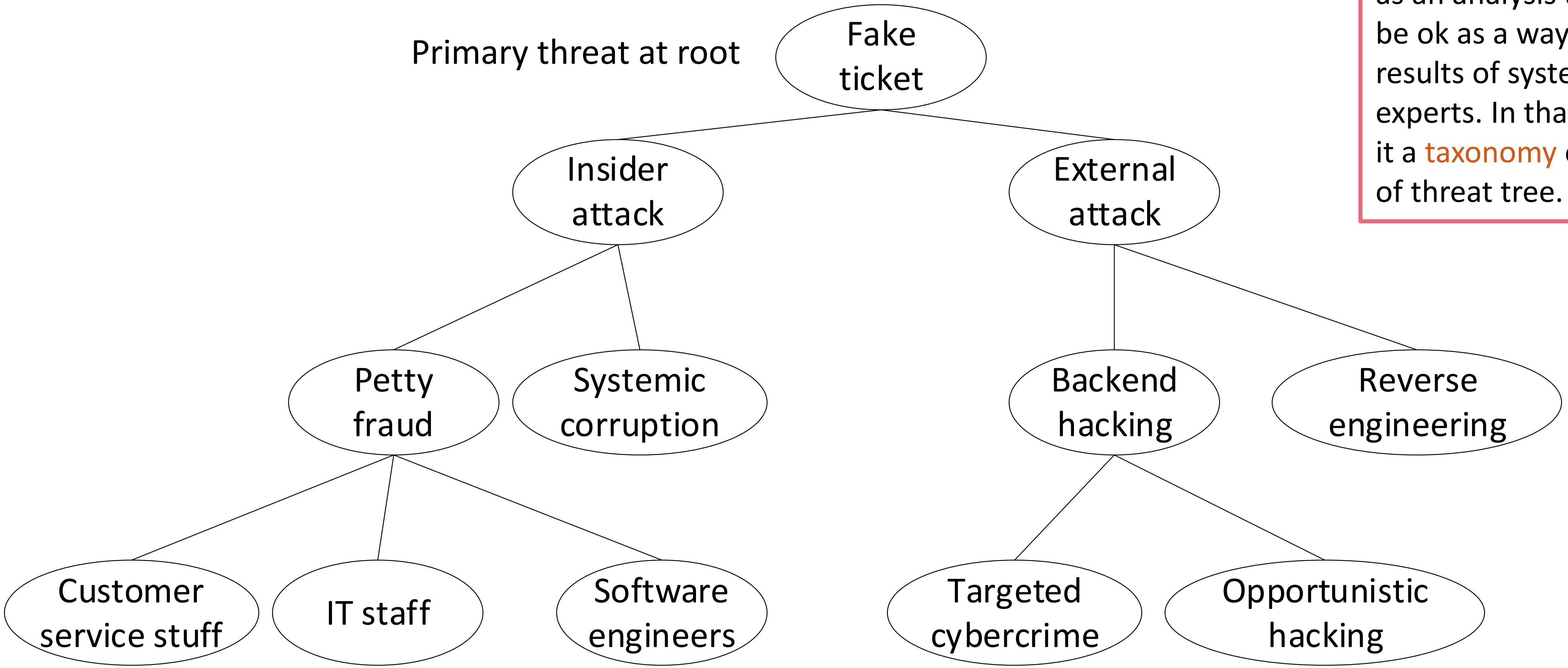
- Consider first well-known security goals:
  - **C**onfidentiality
  - **I**ntegrity
  - **A**vailability
  - Authentication
  - Authorization, access control
  - Non-repudiation
  - Fair payment
- Which goals apply to the system? How could they be violated?
- Look for more comprehensive checklists

Checklist: some threats to consider

- Typical crime motivated by money: theft, fraud, corruption
  - Corruption: tax evasion, misuse of public or company funds, bribery, theft by those in power
- Theft of business secrets, industrial espionage, dishonest ways to gain competitive advantage
- Threats to customer data and personal privacy
- Insider threats: employees, IT administrators, trusted entities misusing their position
  - Also: curiosity, pretty theft, mis-incentivized employees “doing their best”, power grabs within the organization
- Privilege escalation, steppingstones to further attacks
  - Threats to accounts, devices and administration; weaknesses in how authentication credentials are issued and verified
  - Bypassing controls, misuse of reputation systems
- Social-engineering threats
- Threats related to error handling and failure recovery: misuse of recovery processes
- Threats to business continuity: denial-of-service attacks, crisis management processes, business risks
- Public safety threats: critical infrastructure, vehicles, food safety, false alarms
- Threats against brands and reputation
- Misinformation: fake news, rumors, social media, drowning true information into noise, information warfare
- Political and military threats: nation-state actors, terrorism, authoritarian governments, dependence on hostile powers, disruption of energy supply or financial systems, physical attacks on information infrastructure

Threat trees

Primary threat at root



Lecturer’s opinion:
Threat threes are pretty useless as an analysis tool, but they can be ok as a way to present the results of systematic analysis by experts. In that case, maybe call it a taxonomy of threats instead of threat tree.

Each leaf is a secondary threat that needs to be analyzed separately

STRIDE

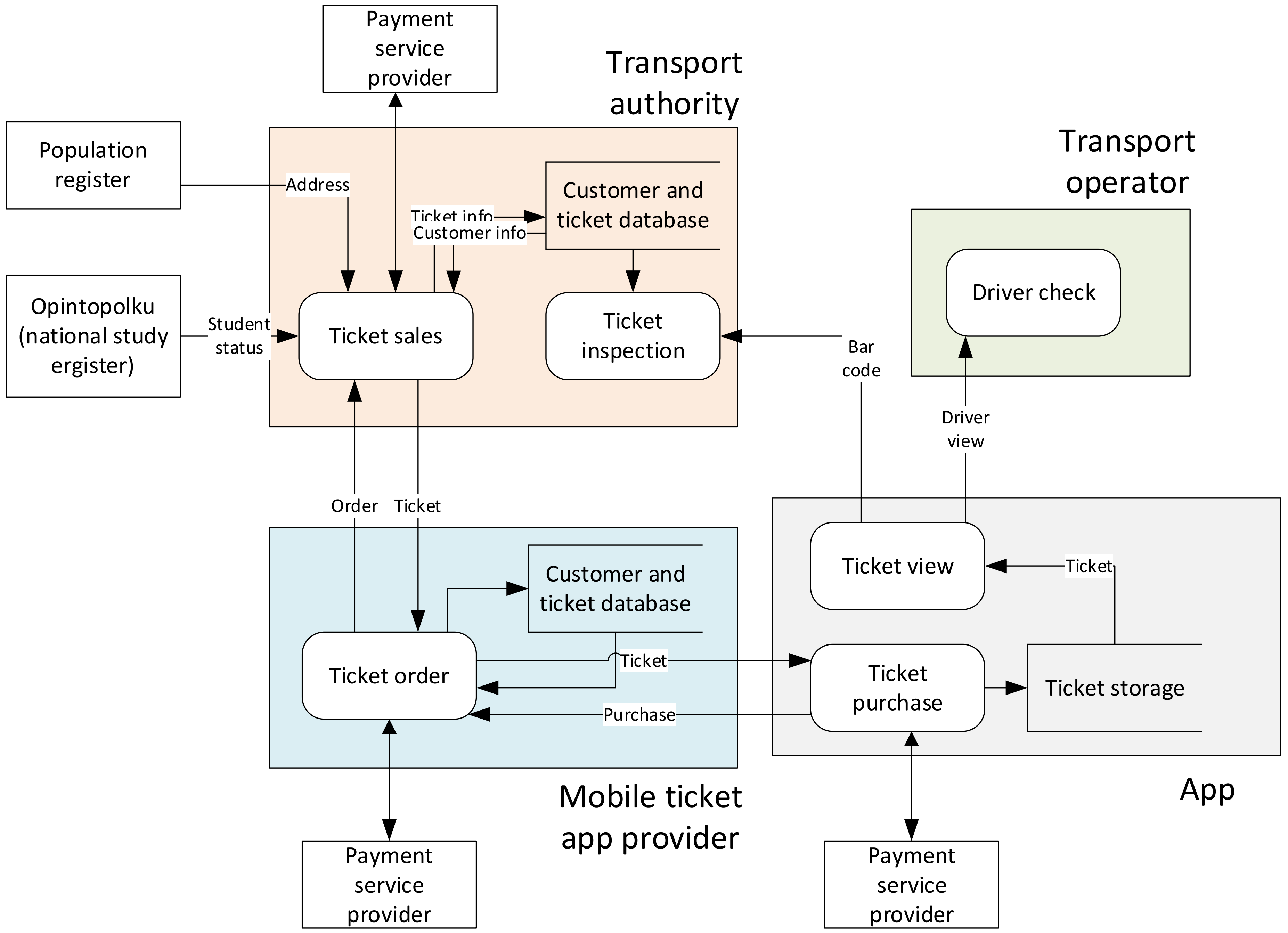
- Idea: model the system as data flow diagram (DFD) and analyze each component separately
- Threats considered in STRIDE:
  - Spoofing vs. authentication
  - Tampering vs. integrity
  - Repudiation vs. non-repudiation, accountability
  - Information disclosure vs. confidentiality
  - Denial of service vs. availability
  - Elevation of privilege vs. authorization, access control

Note: security of components is necessary but not sufficient for the security of the system

STRIDE

- Model the software system as a data flow diagram (DFD)
  - Data flows: network connections, RPC
  - Data stores: files, databases
  - Processes: programs, services
  - Interactors: users, clients, services etc. connected to the system
- Also mark the trust boundaries in the DFD
- Consider the following threats:

	Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
Data flow		x		x	x	
Data store		x		x	x	
Process	x	x	x	x	x	x
Interactor	x		x			



High-level DFD for the transport ticket app

- For example, are there tampering or information disclosure threats in data flows that cross trust boundaries?

Notes about STRIDE

- STRIDE was developed at Microsoft from 1999
- Originally designed for threat modeling in PC and application server software
  - Often used as a generic threat modeling framework, but that requires creative thinking
- Some limitations:
  - DFD does not capture the complexity of cloud, virtualization, or distributed computing
  - DFD models only data flows, not human or cyber-physical interaction, or money flows
  - Intended for software engineers; does not focus attention to business objectives or risks to them

Risk assessment

- Risk assessment is very subjective; many definitions:

  Risk = probability of attack × damage in euros

  Risk $\in$ { low, medium, high } × { low, medium, high }

  $0 < \text{Risk} < 1$

- Numerical risk values tend to be meaningless:
  - What does risk level 0.4 mean in practice?
- Usually difficult to assess absolute risk but easier to prioritize threats

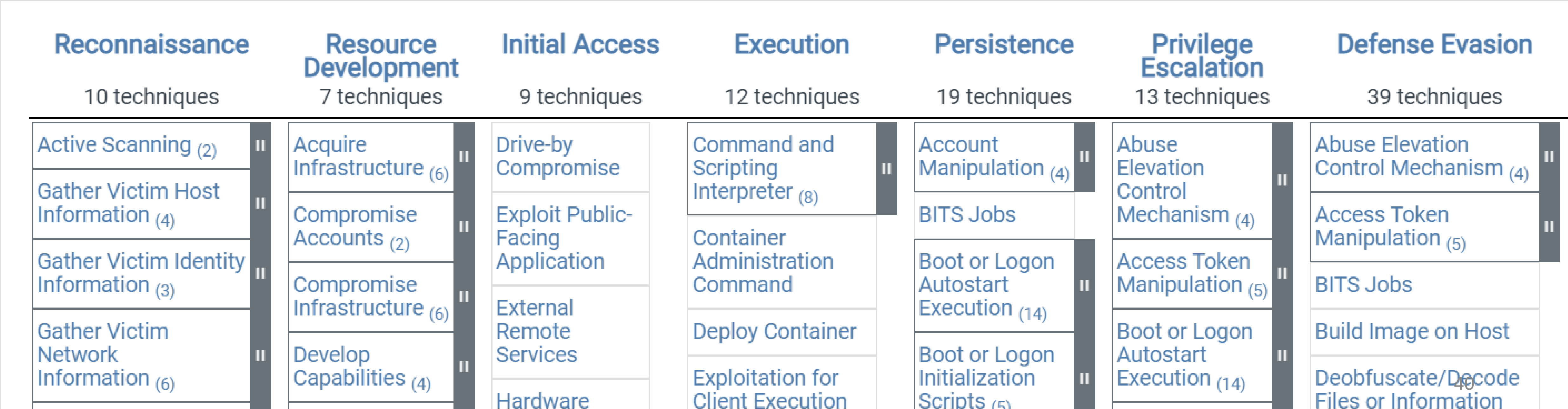
DREAD risk assessment model

- Designed to complement STRIDE, no longer widely used
- In DREAD, risk has many dimensions:
  - Damage: how much does the attack cost to defender?
  - Reproducibility: how reliable is the attack
  - Exploitability: how much work to implement the attack?
  - Affected users: how many people impacted?
  - Discoverability: how likely are attackers to discover the vulnerability?

Also suffers from the use of arbitrary numerical scales

MITRE ATTA&CK

- Conceptual framework for threats against enterprise information systems: https://attack.mitre.org/
  - Separate matrices for industrial control systems and mobile apps
  - Tactics (attack phases), which consists of techniques
- Common vocabulary for discussion threats and attacks



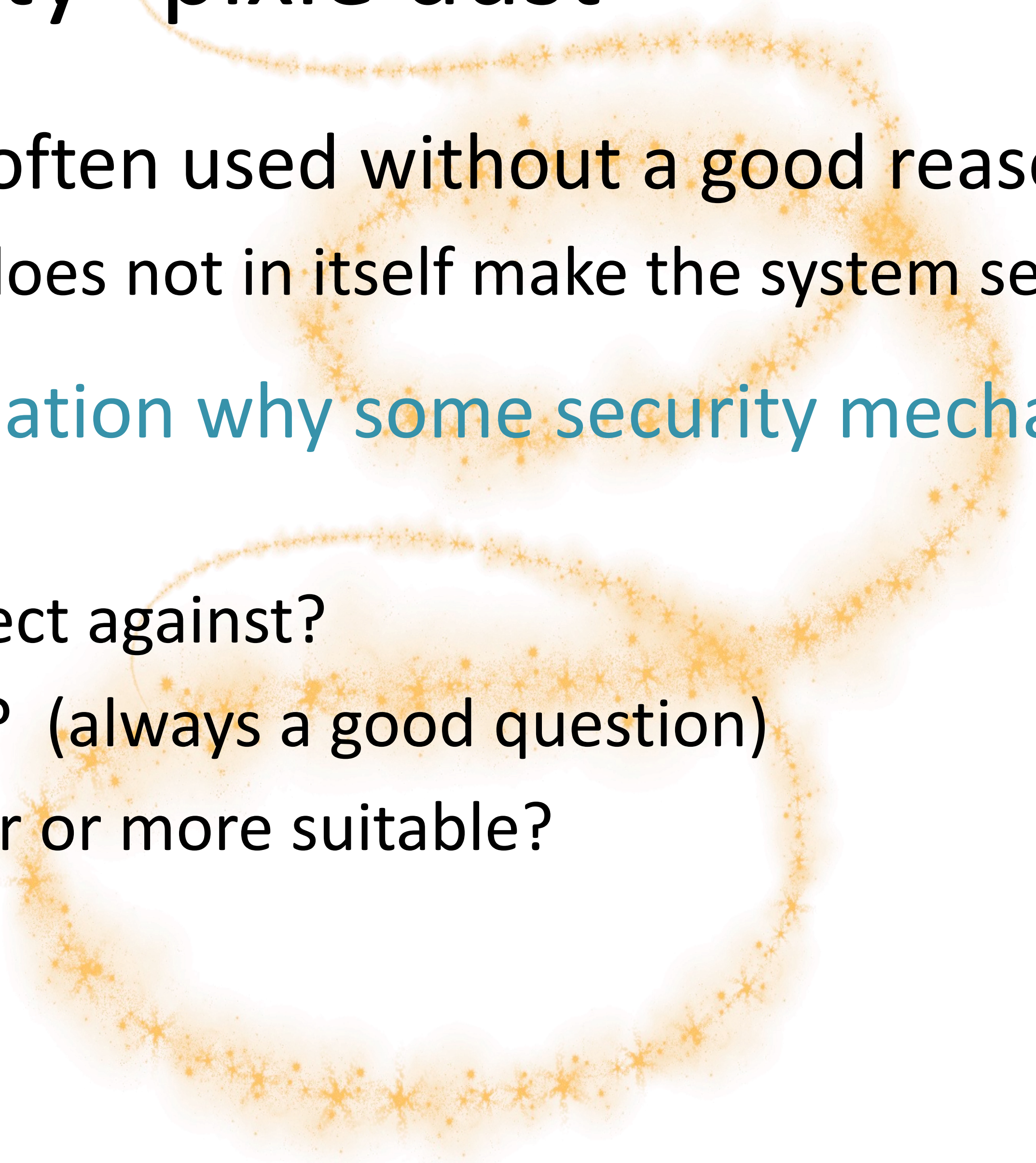
Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)		Build Image on Host
						Deobfuscate/Decode Files or Information

Pitfalls in threat and risk assessment

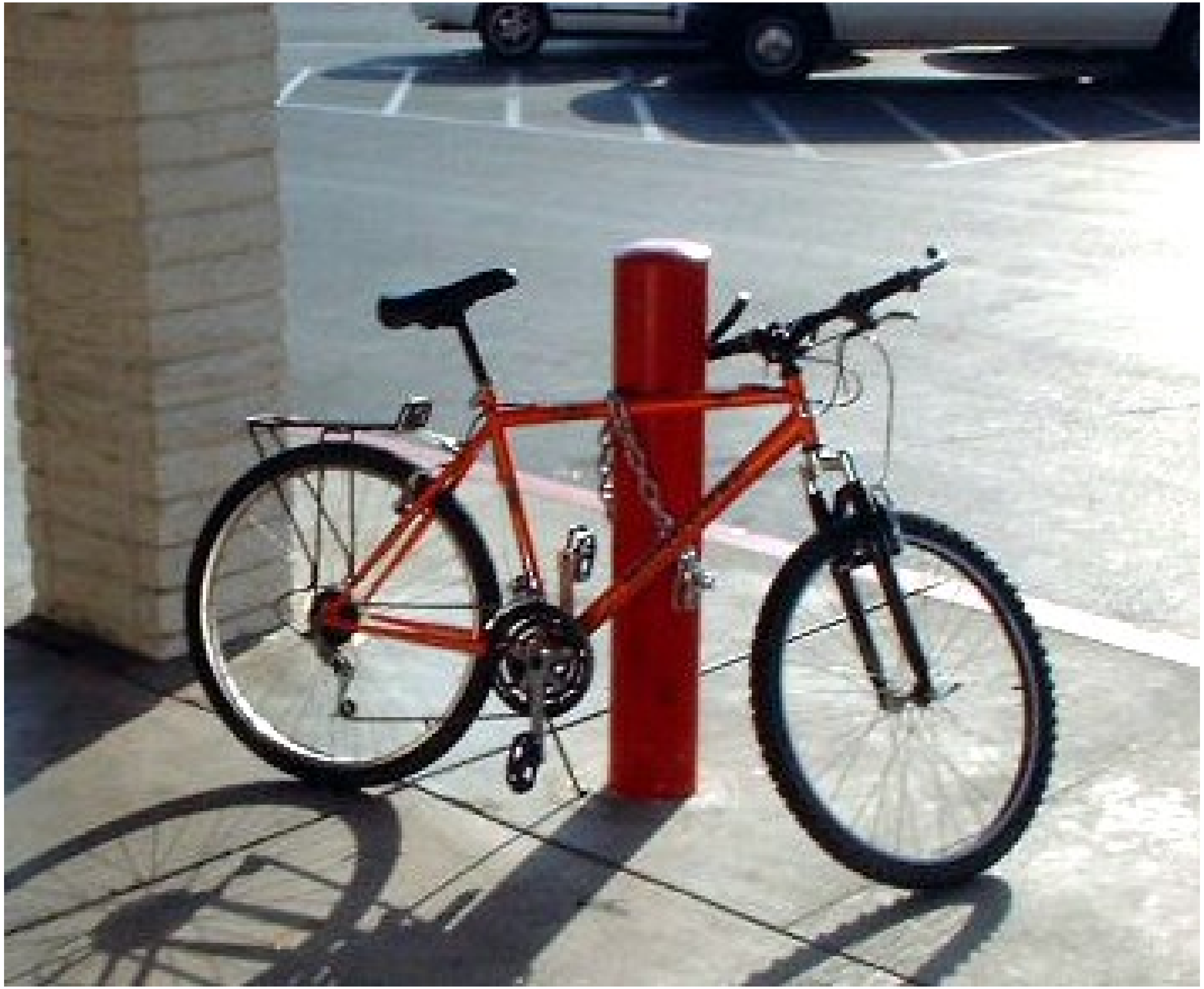
- The systematic threat analysis methods help but there is no guarantee of finding all or even the most important threats
- You need to understand the system: technology, architecture, stakeholders and business model
- Attackers are clever and invent new threats; systematic threat analysis often enumerates old threats
- Always start by considering assets and potential attackers, not system implementation details or security mechanisms

SUMMARY

Security "pixie dust"



- Security mechanism are often used without a good reason
  - For example, encryption does not in itself make the system secure
- If there is no clear explanation why some security mechanism is used, ask questions:
  - What threats does it protect against?
  - What if we just remove it? (always a good question)
  - Is there something simpler or more suitable?



[Photo: Internet, original source unknown]

List of key concepts

- Security, threat, attack, vulnerability, exploit, risk, countermeasure
- Confidentiality, integrity, availability
- Asset, attacker, insider
- Checklists, threat trees, DFD, STRIDE, DREAD, MITRE ATTA&CK
- Security pixie dust

Reading material

- Ross Anderson: Security Engineering, 2nd ed., chapter 25
- Swiderski and Snyder, Threat modeling, 2004
- Stallings, Brown: Computer Security: Principles and Practice, 4th ed., chapter 1

- Online resources:
  - OWASP, Application Threat Modeling, https://www.owasp.org/index.php/Application_Threat_Modeling
  - MSDN, Uncover Security Design Flaws Using The STRIDE Approach, MSDN Magazine 2016/11 (search for copies)
  - MSDN, Improving Web Application Security: Threats and Countermeasures, Chapter 3 http://msdn.microsoft.com/en-us/library/ff648644.aspx

Exercises

- Analyze the threats in the following systems:
  - Sisu student register
  - MyCourses
  - Remotely read electricity meter
  - University card keys
  - Contactless smartcard bus tickets
  - Traffic light priority control for public transportation
- What are the assets and potential attackers?
- What are the high-priority threats?
- Apply the STRIDE model to a system that you know well; this will you required to create a DFD first