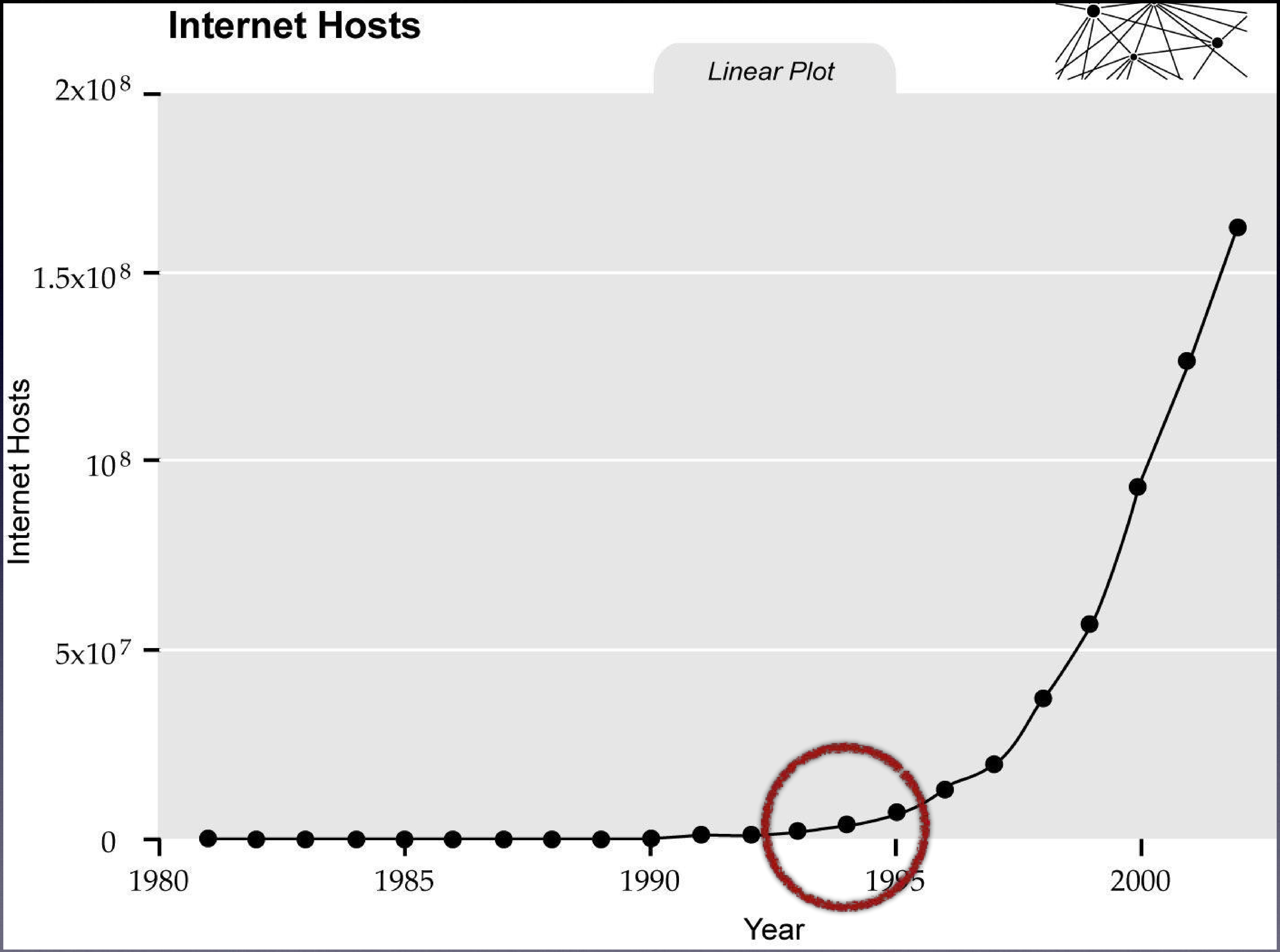
White Hats, Black Hats and STRIDE

An Introduction to Threat Modeling


Internet Hosts
Linear Plot
2x10^8
1.5x10^8
10^8
5x10^7
0
Internet Hosts
1980
1985
1990
1995
2000
Year

Threat Modeling

Risk

Vulnerability

Attack

Threat Modeling

Threat modeling is a process by which a system is methodically analyzed from an attacker’s perspective, to identify attack goals, evaluate the risks they pose and mitigate their vulnerabilities.

Threat Modeling

Threat modeling is a **process**
by which a **system** is **methodically analyzed**
from an **attacker's perspective,**
to **identify attack goals,**
evaluate the risks they pose
and **mitigate their vulnerabilities.**

Threat Modeling

Threat modeling is a **process**
by which a **system** is **methodically analyzed**
from an **attacker’s perspective**,
to **identify attack goals**,
evaluate the risks they pose
and **mitigate their vulnerabilities**.

Threat Modeling

Threat modeling is a **process**
by which a system is **methodically analyzed**
from an **attacker’s perspective**,
to **identify attack goals**,
evaluate the risks they pose
and **mitigate their vulnerabilities**.

Threat Modeling

Threat modeling is a **process**
by which a **system** is methodically analyzed
from an **attacker's perspective**,
to **identify attack goals**,
evaluate the risks they pose
and **mitigate their vulnerabilities**.

Threat Modeling

Threat modeling is a **process**
by which a **system** is **methodically analyzed**
from an attacker’s perspective,
to **identify attack goals**,
evaluate the risks they pose
and **mitigate their vulnerabilities**.

Threat Modeling

Threat modeling is a **process**
by which a **system** is **methodically analyzed**
from an **attacker's perspective,**
to **identify attack goals**,
evaluate the risks they pose
and **mitigate their vulnerabilities.**

Threat Modeling

Threat modeling is a **process**
by which a **system** is **methodically analyzed**
from an **attacker's perspective**,
to **identify attack goals**,
evaluate the risks they pose
and **mitigate their vulnerabilities**.

Threat Modeling

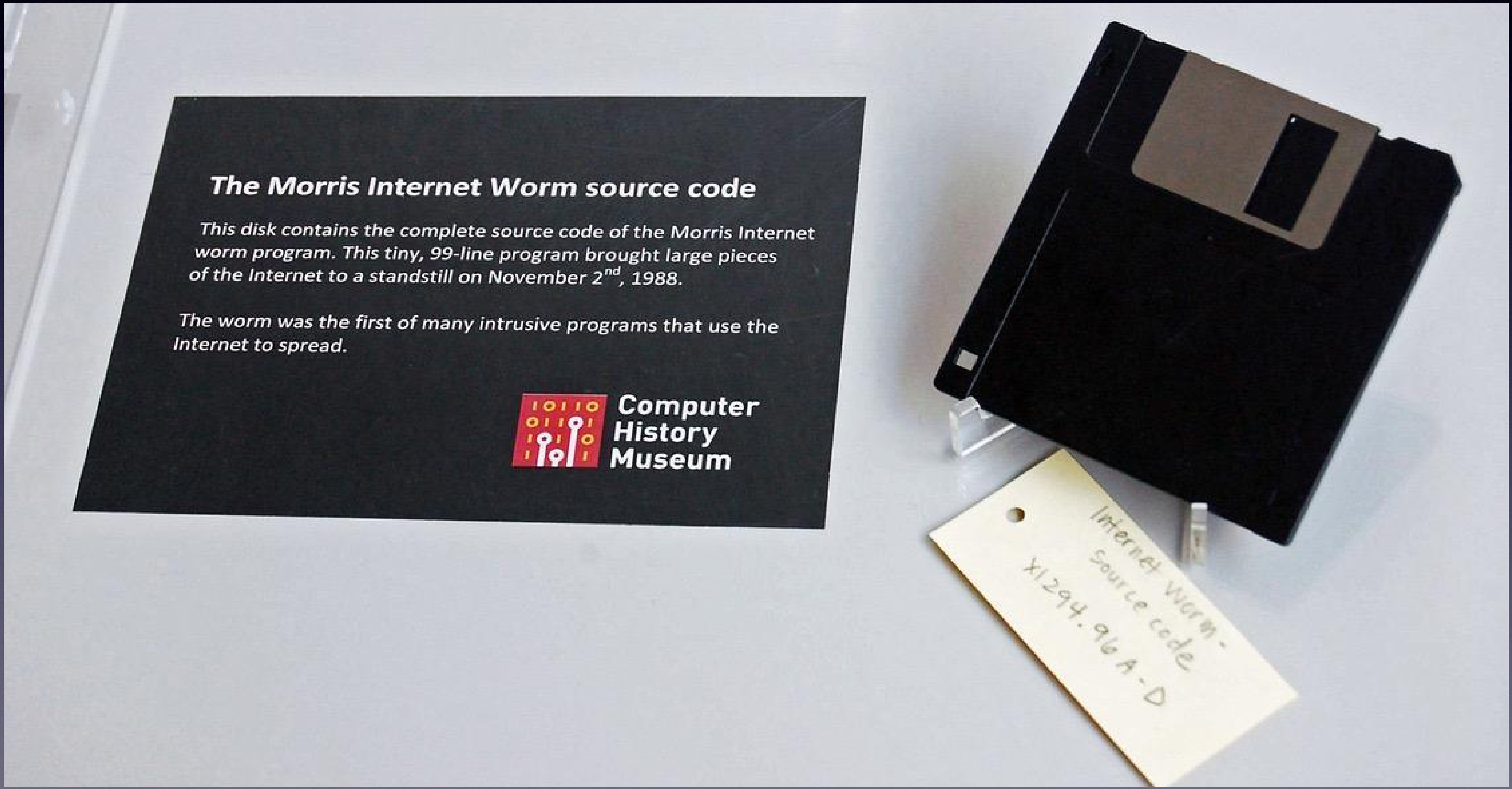
Threat modeling is a **process**
by which a **system** is **methodically analyzed**
from an **attacker’s perspective**,
to **identify attack goals**,
evaluate the risks they pose
and mitigate their vulnerabilities.

Threat Modeling

Threat modeling is *looking at your system the way an attacker does.*

Attackers

“Zero-Days”



The Morris Internet Worm source code

This disk contains the complete source code of the Morris Internet worm program. This tiny, 99-line program brought large pieces of the Internet to a standstill on November 2nd, 1988.

The worm was the first of many intrusive programs that use the Internet to spread.

Computer History Museum

White Hats

notify vendors before public

- Security Researchers
  - ★ Prestige, learning, public service
- Penetration Testers
  - ★ Payment
- Bug-Bounty Hunters
  - ★ Payment, reputation

Black Hats

no public release

- State Actors
    - ★ Intelligence, sabotage, zombies
- Hacktivists
    - ★ Retribution, publicity, zombies
- Vulnerability Brokers
    - ★ Money, reputation

Gray Hats

notify public first

- Insiders
  - ★ Vengeance, whistle-blowing
- Hobbyists
  - ★ Self-education, thrills, prestige…
    …sometimes extortion

A$$hats

use, not create, exploits

- Cybercriminals
  - ★ Credit cards, identity theft, extortion
- Script Kiddies
  - ★ Thrills, attention, vengeance

Threat Actors

“The Bad Guys”

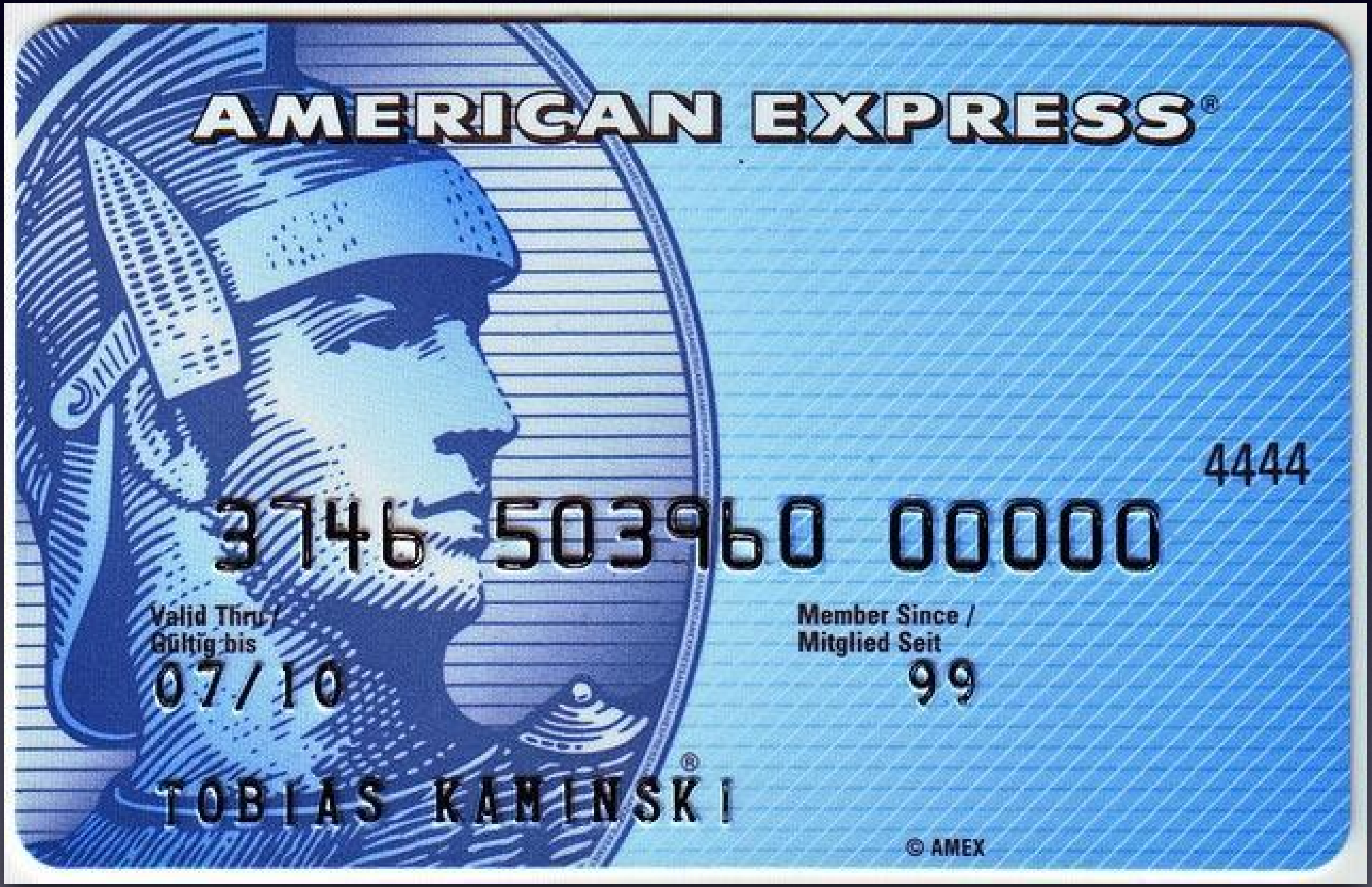
- Cybercriminals
  - ★ Credit cards, identity theft, extortion
- Script Kiddies
  - ★ Thrills, attention, vengeance

Attacks

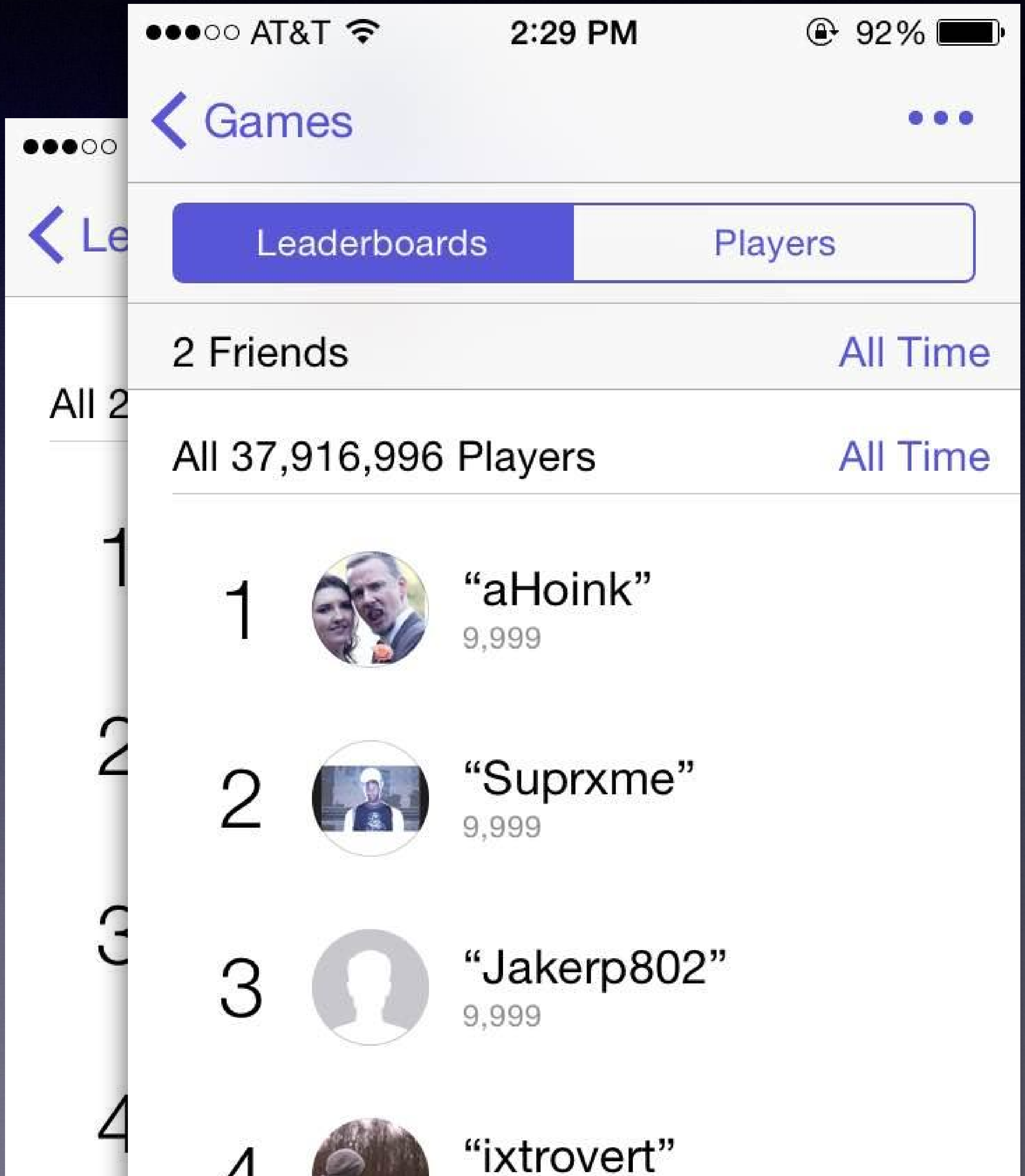
STRIDE

- Spoofing: Pretending to be another user
- Tampering: Modifying data outside of normal usage
- Repudiation: Erasing the history of an action
- Information disclosure: Reading secrets
- Denial of service: Preventing normal operation
- Elevation of privilege: Performing forbidden actions

Spoofing


AMERICAN EXPRESS
4444
3746 503960 00000
Valid Thru / Gültig bis
07/10
Member Since / Mitglied Seit
99
TOBIAS KAMINSKI
© AMEX

Tampering



●●●○○ AT&T 2:29 PM 92%

Games •••

Leaderboards | Players

2 Friends All Time

All 37,916,996 Players All Time

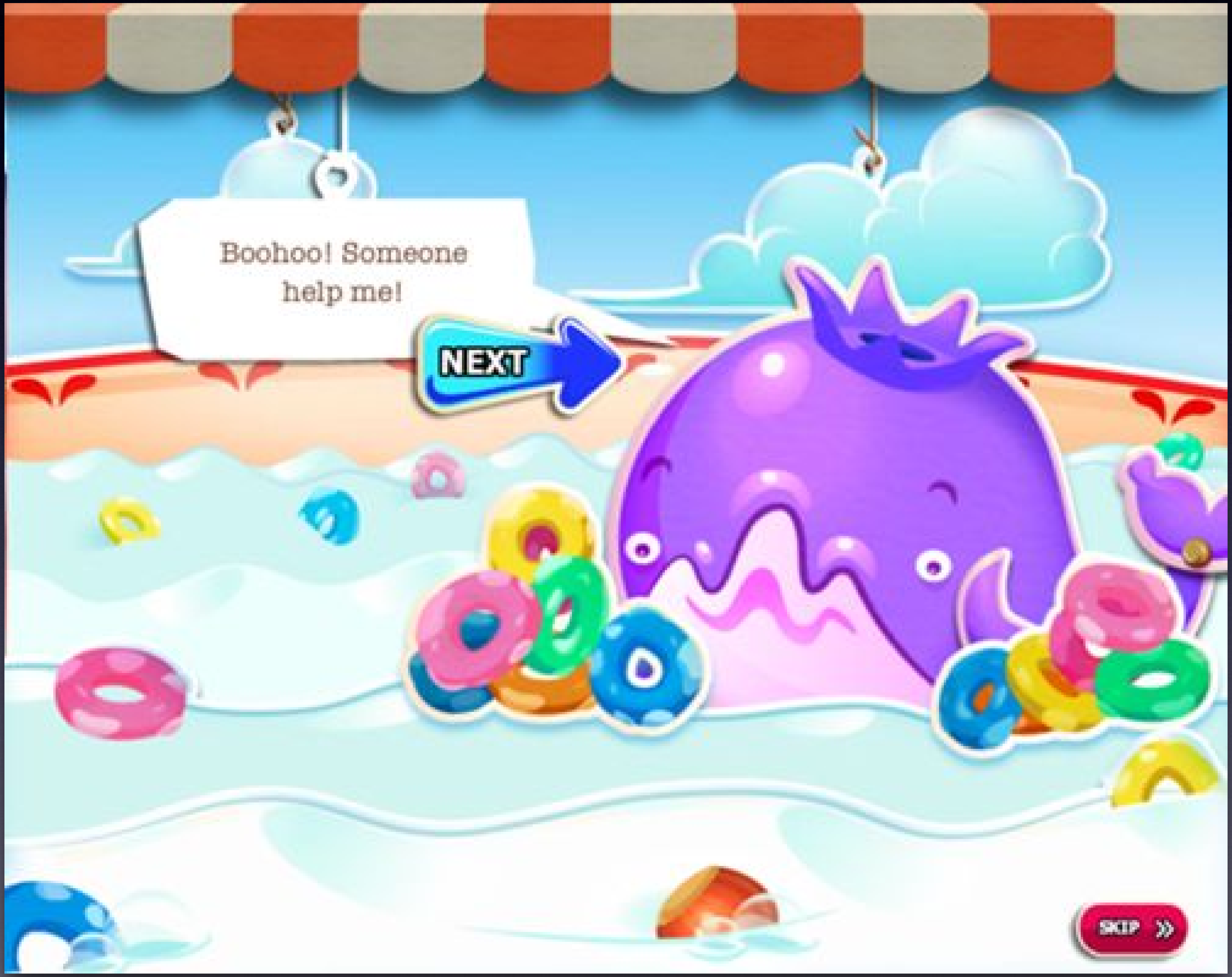
1 “aHoink” 9,999

2 “Suprxme” 9,999

3 “Jakerp802” 9,999

4 “ixtrovert”

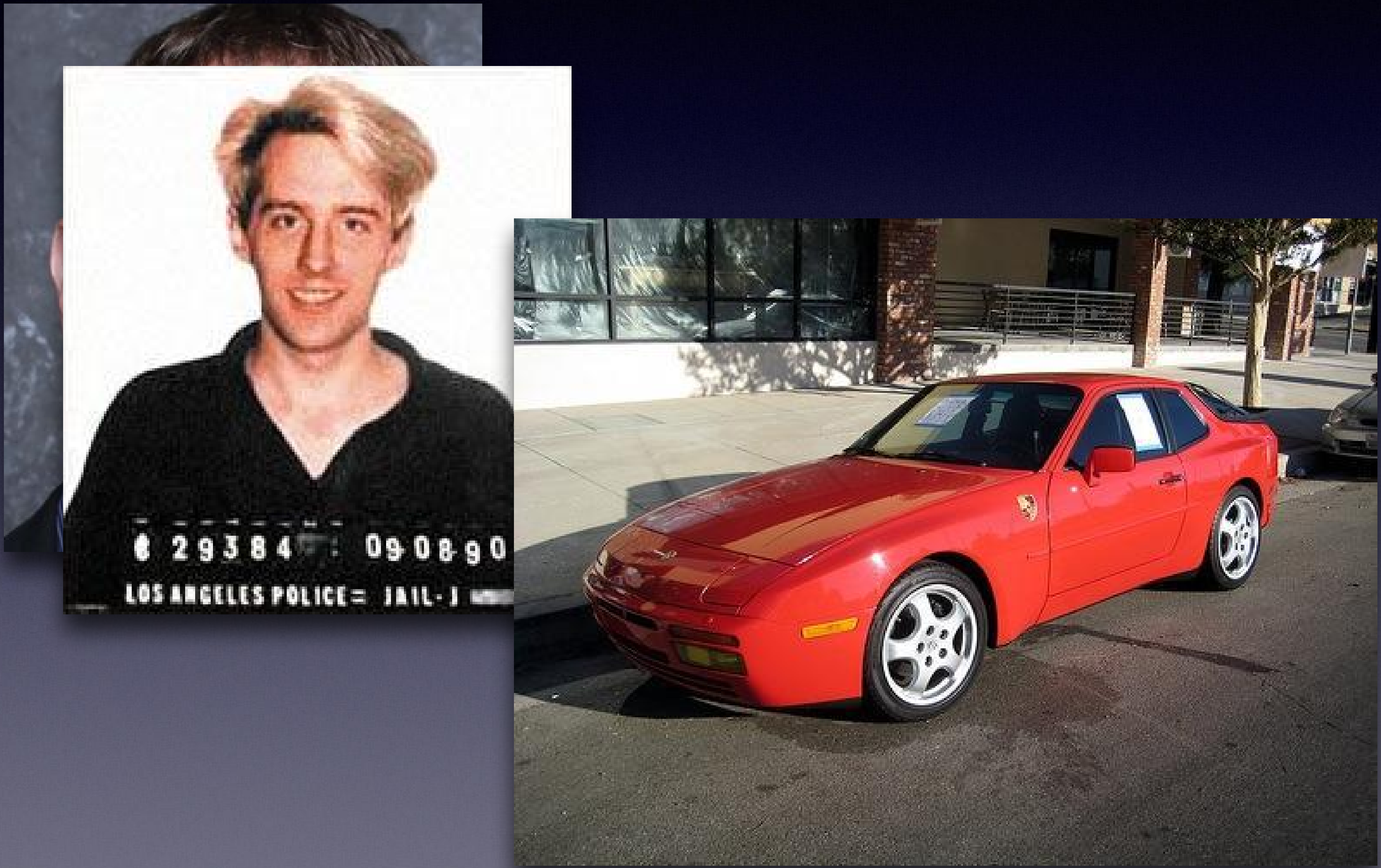
Repudiation



Boohoo! Someone help me!

Information Disclosure

Denial of Service



Elevation of Privilege

- Threat modeling looks at your system the way an attacker does.
- Attackers have goals and motivations.
- Classifying attacks into categories helps us maintain focus and be methodical.