# Introduction

COMPUTER SECURITY

MARKULF KOHLWEISS

Some slides adapted from those by Myrto Arapinis, Kami Vaniea, and Roberto Tamassia

# Basic concepts



# What is Computer Security?

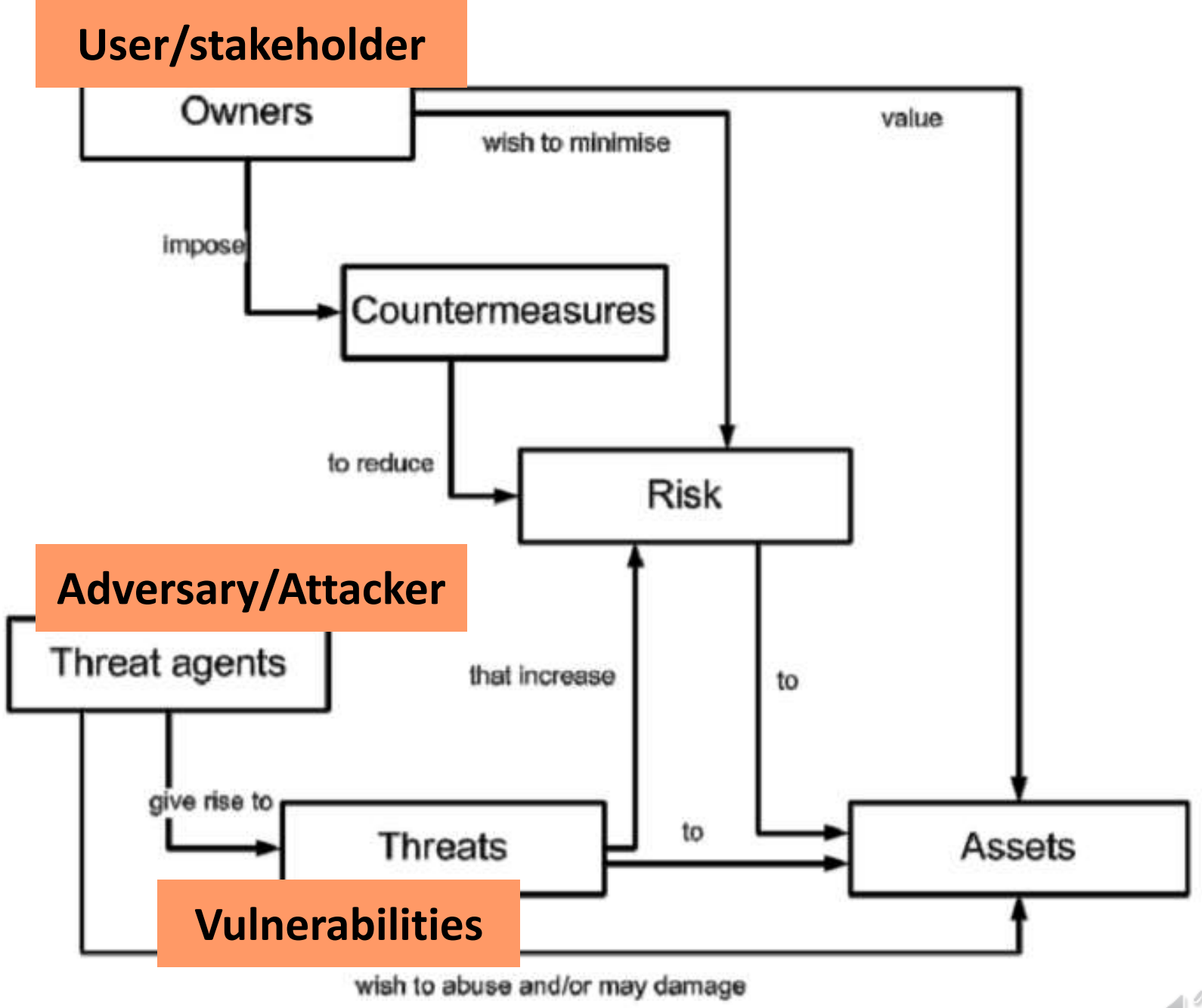
- **Security** is about protecting assets. **Privacy,** asset is your freedom and dignity.
- **Computer security** is the protection of assets on computer systems against adversarial environments
  - Allow intended use
  - Prevent unintended use

# Common Criteria for Information Technology Security Evaluation (CC)

- Security is about protecting assets from threats.
- Threats are the potential for abuse of assets.
- **Owners** value assets and want to protect them.
- **Threat agents** also value assets, and seek to abuse them.
- Owners analyze threats to decide which apply; these risks can be costed.
- This helps select countermeasures, which reduce vulnerabilities.
- Vulnerabilities may remain leaving some residual risk; owners seek to minimize that risk, within other constraints (feasibility, expense).

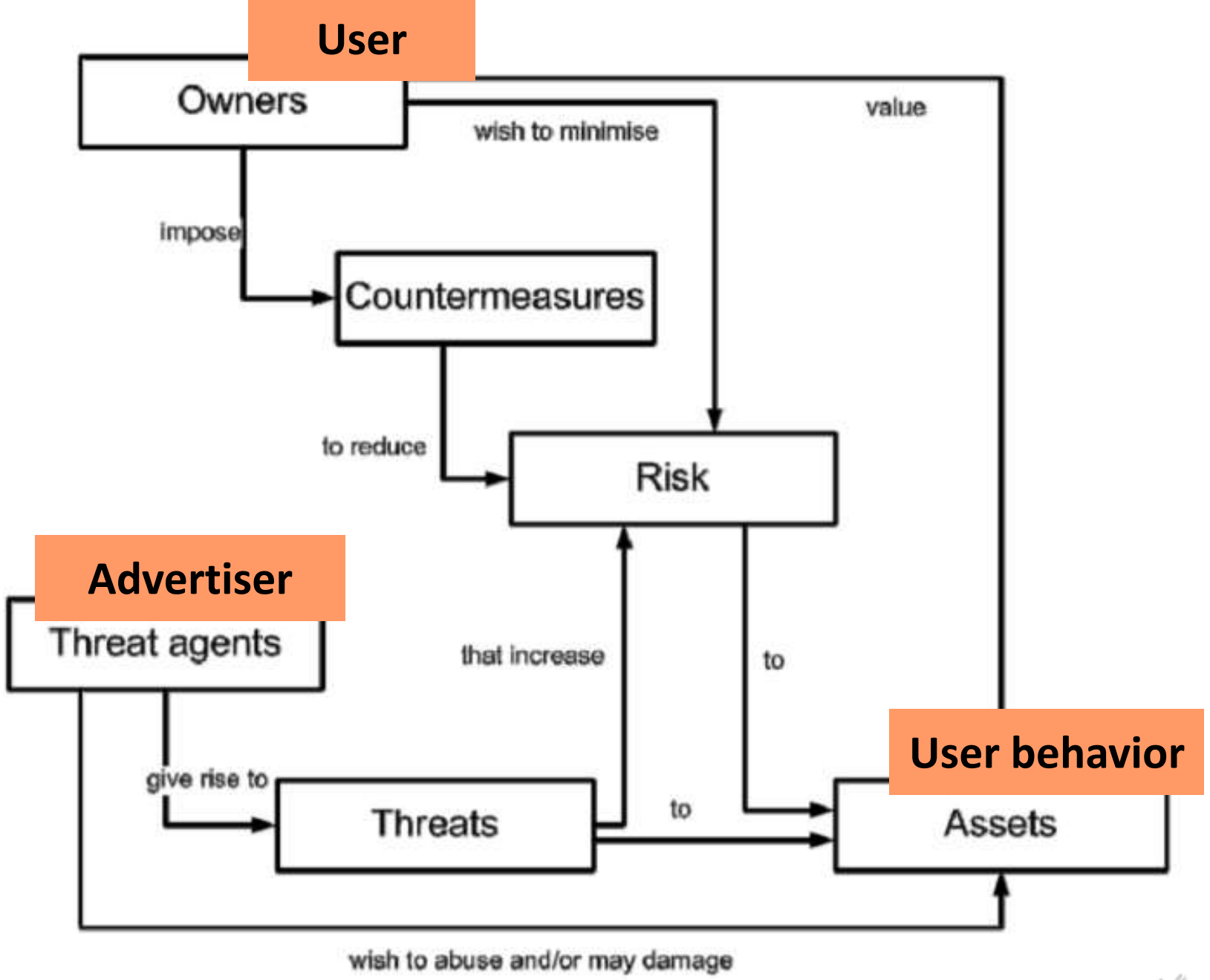
# Security concepts and relationships

-- CC V3.1 R4



# Example: Behavioral Advertising

- **Asset**: User behavior
- **Owner**: The user
- **Threat agent**: Advertisers
- Risks:
  - Tracking
  - Discriminatory pricing
  - Electoral manipulation

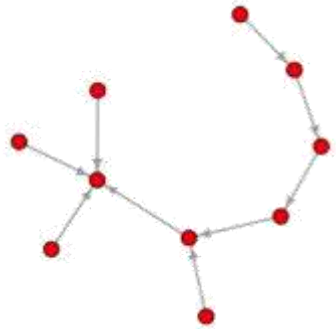


“A system which is unspecified can never be wrong, it can only be surprising.”

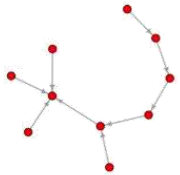


# The security problem

$|$



$\models \Phi$



computer system

attacker model, e.g, personal motivation (spouse or boss), financial motivation (pharmaceutical, credit card theft), political motivation (governments, activists), . . .

$\Phi$

security policy, security properties

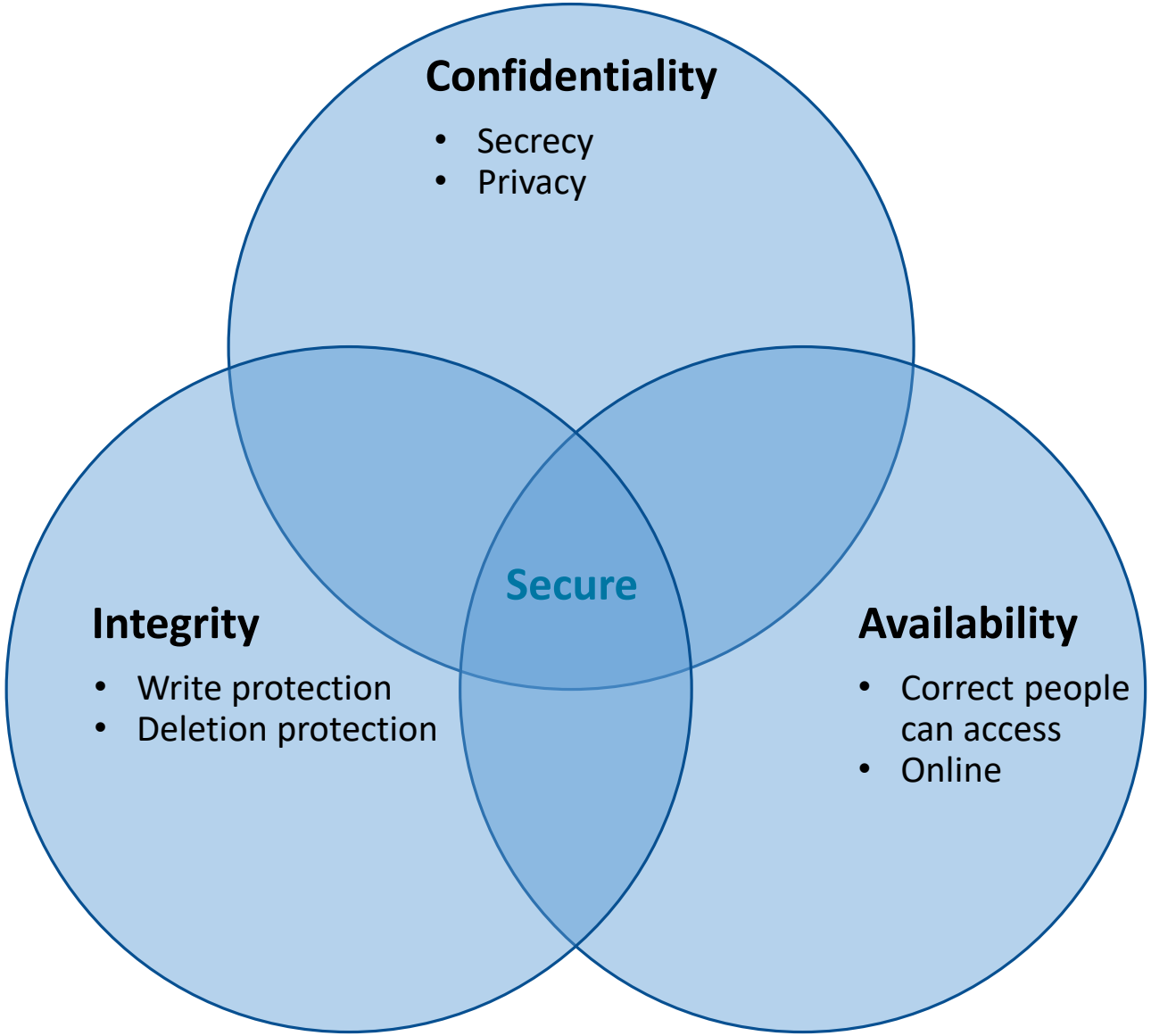
e.g. confidentiality, integrity, availability, authenticity, anonymity, . . .

# Security properties

## PROTECTION GOALS

# Defining Security

- Confidentiality
  - Ensures that computer-related assets are accessed only by authorized parties.
- Integrity
  - Assets can be modified only by authorized parties or only in authorized ways.
- Availability
  - Assets are accessible to authorized parties at appropriate times.



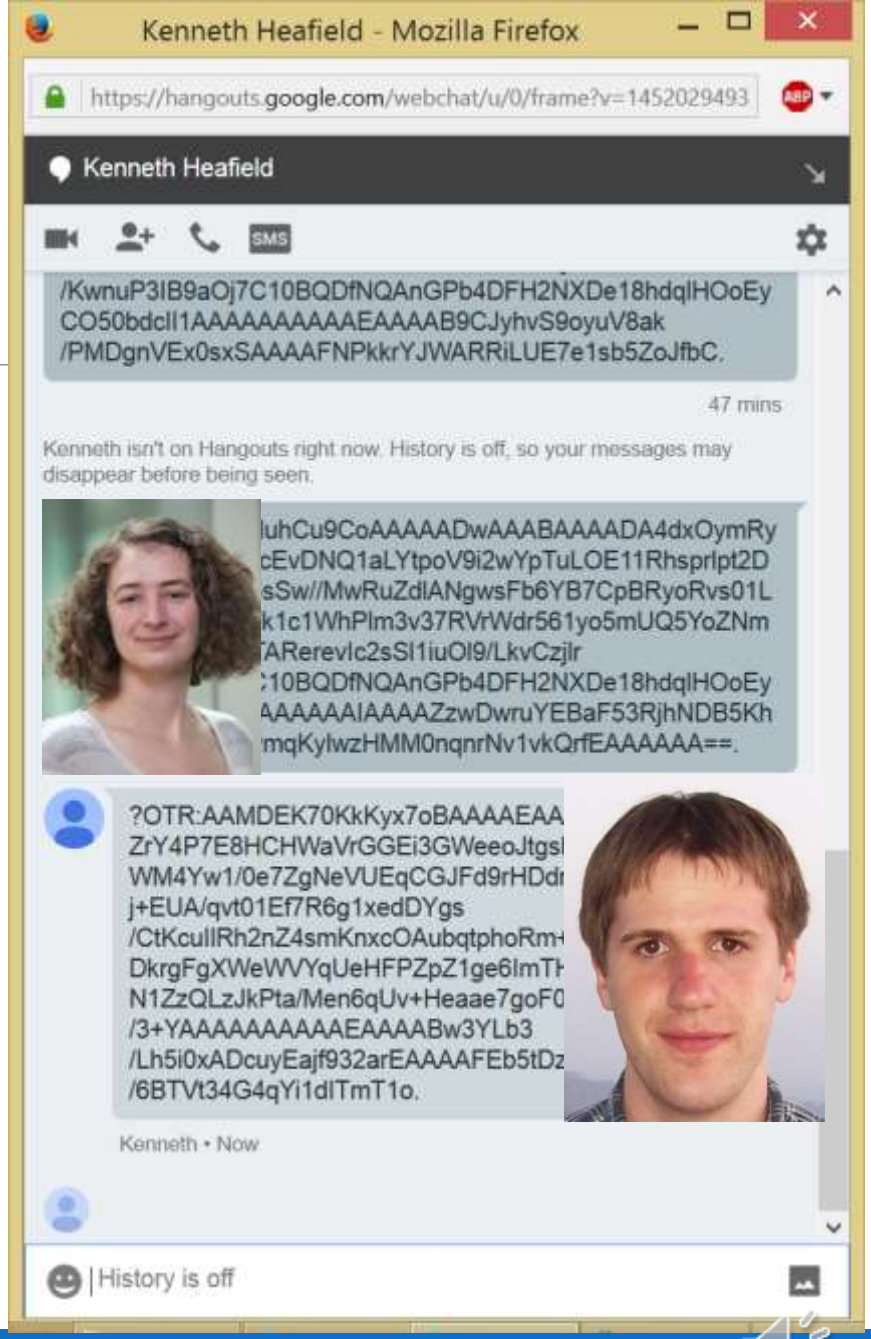
# Security is a whole system issue

- Software
- Hardware
- Physical environment
- Personnel
- Corporate and legal structures

| Security properties to ensure | |
|---|---|
| **Confidentiality** | No improper information gathering |
| **Integrity** | Data has not been (maliciously) altered |
| **Availability** | Data/services can be accessed as desired |
| **Accountability** | Actions are traceable to those responsible |
| **Authentication** | User or data origin accurately identifiable |
| **Anonymity** | User or data origin is not identifiable |

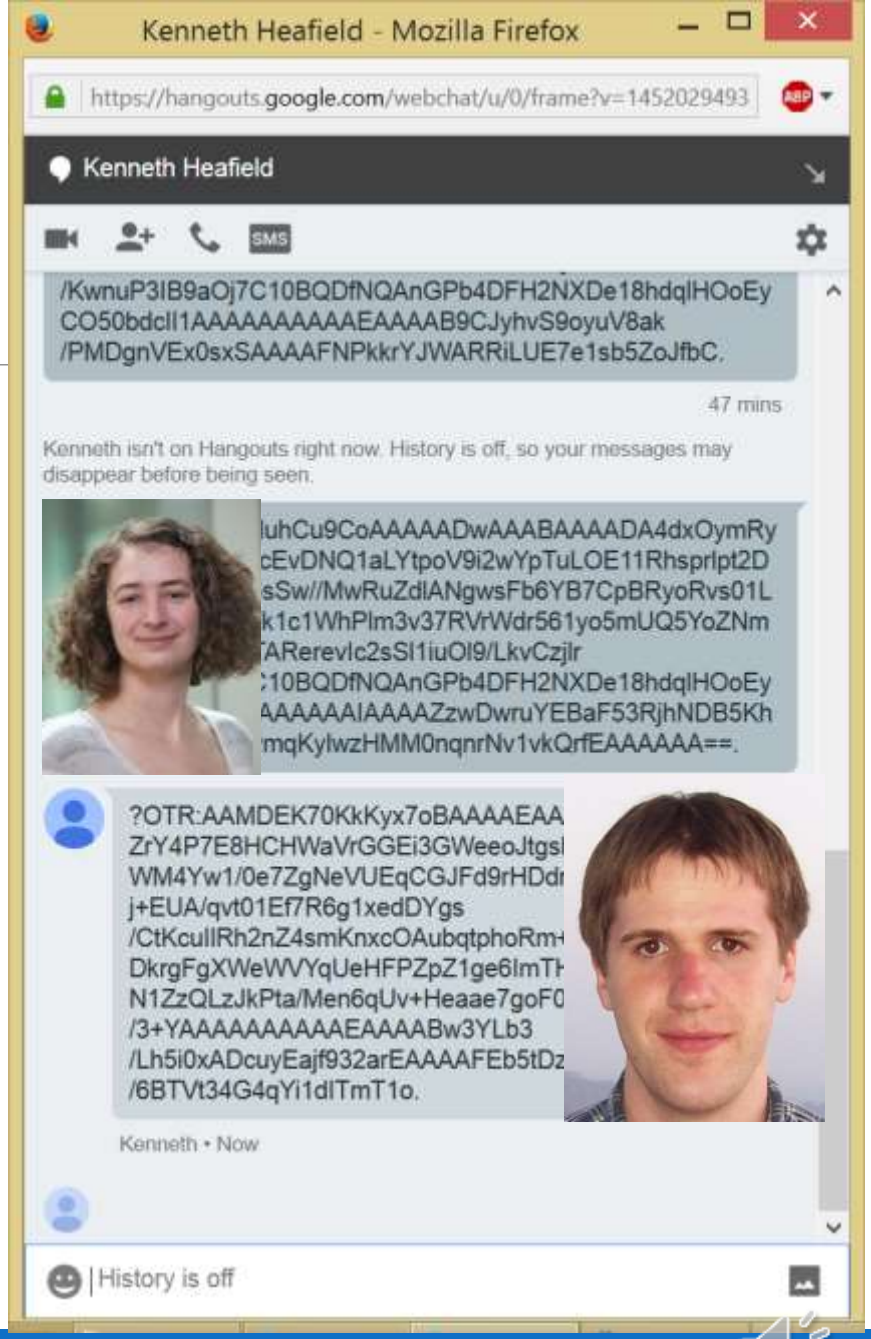
# Confidentiality, privacy, and secrecy

- Confidentiality is characterized as preventing the unauthorized reading of data, when considering access control systems. More generally, it implies unauthorized learning of information.
- The gchat on the right is encrypted. How much can you learn from it anyway?



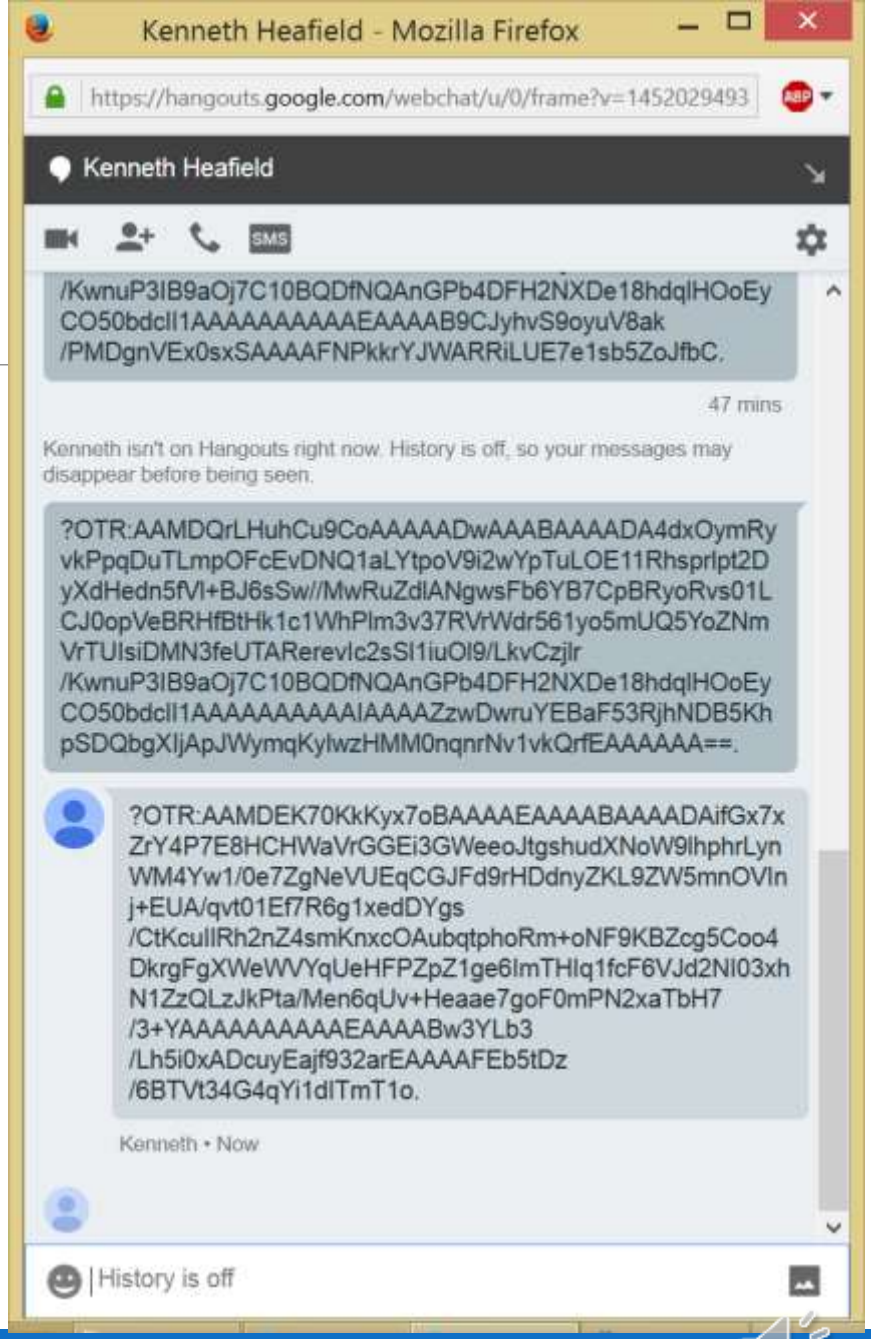
# Confidentiality, privacy, and secrecy

- Conf … s
  prev … ding of
  data … ontrol
  syste … es
  unau … ation.
- The … ed. How
  muc … vay?

# Integrity

- Data has not been maliciously altered.
- Integrity can have different meanings, in computer security we are primarily concerned with the unauthorized writing of data.
- Examples:
  - Removing a record from a system.
  - An on-line payment system alters an electronic check to read £10000 instead of £100.00



# Availability

- Data or services are accessible as expected.
- Threats to availability cover many kinds of external environmental events (e.g., fire, pulling the server plug) as well as accidental or malicious attacks in software (e.g., infection with a debilitating virus).
- Denial of Service (DOS) threats are the most common form of an Availability threat.

# Accountability

- Actions are recorded and can be traced to the party responsible.
- If prevention methods and access controls fail, we may fall back on detection: keeping a secure audit trail is important so that actions affecting security can be traced back.

# Authentication

- Data or services available only to authorized entities.
- Authentication is necessary for allowing access to some people but denying access to others.
- Authentication typically characterized as:
  - Something you **have** – an entry card, your phone
  - Something you **know** – a password, your mother's maiden name
  - Something you **are** – a signature, fingerprint, way of typing

# Anonymity and Deniability

- Somewhat dual to Accountability and Authentication

  *Alice may wants to say something very private to Bob. She wants that Bob believes it comes from her, but does not want Bob to be able to convince a third party that she said such a thing or that they spoke at all.*

  *Additionally, she may want to authenticate as a government official but keep her identity hidden.*

- Important property for Whistleblowing.