CSc 466/566

Computer Security

6 : Terminology II

Version: 2019/09/16 13:10:29

Department of Computer Science
University of Arizona

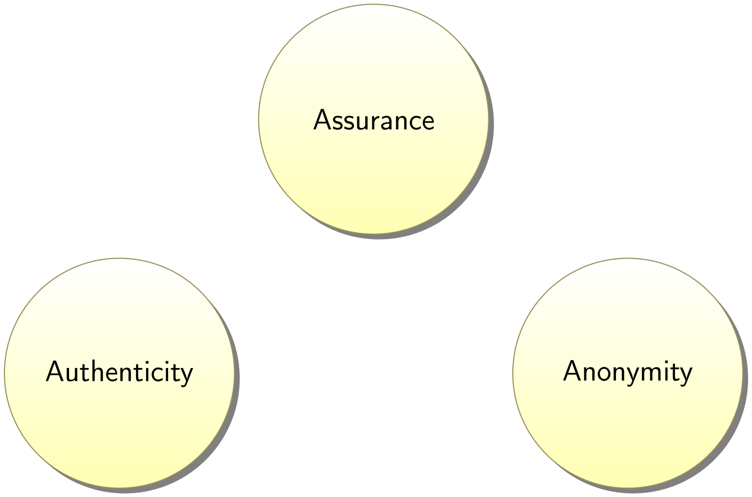
collberg@gmail.com

Christian Collberg

Outline

1. Security Goals—AAA
   - Assurance
   - Authenticity
   - Anonymity
2. Summary

Assurance, Authenticity, Anonymity



Assurance

Authenticity

Anonymity

Assurance, Authenticity, Anonymity

- Assurance — can we trust systems/people to behave as expected?
- Authenticity — is an issued statement/permission/policy/. . . genuine?
- Anonymity — can records/transactions not be tied to a particular individual?

Assurance

Definition (Assurance)

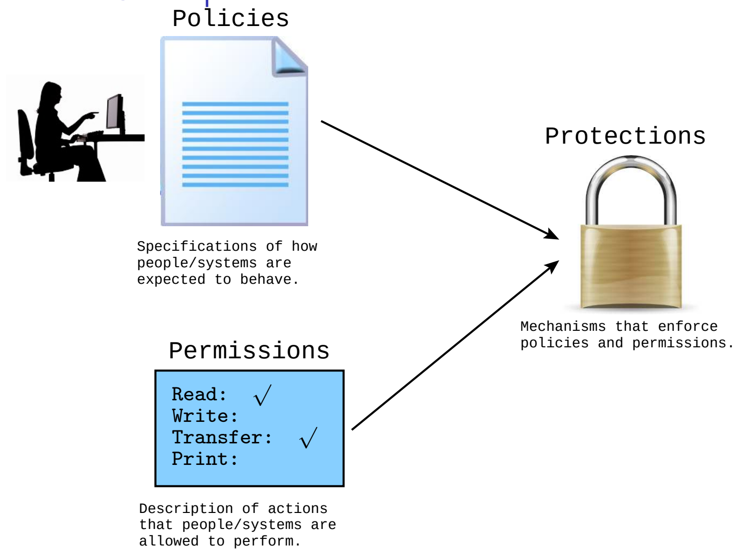
The way in which trust is provided and managed in a computer system.

Definition (Trust)

The degree to which we expect people and systems to behave as expected.

- Many other definitions of trust!

Assurance: Concepts



Policies

Specifications of how people/systems are expected to behave.

Permissions

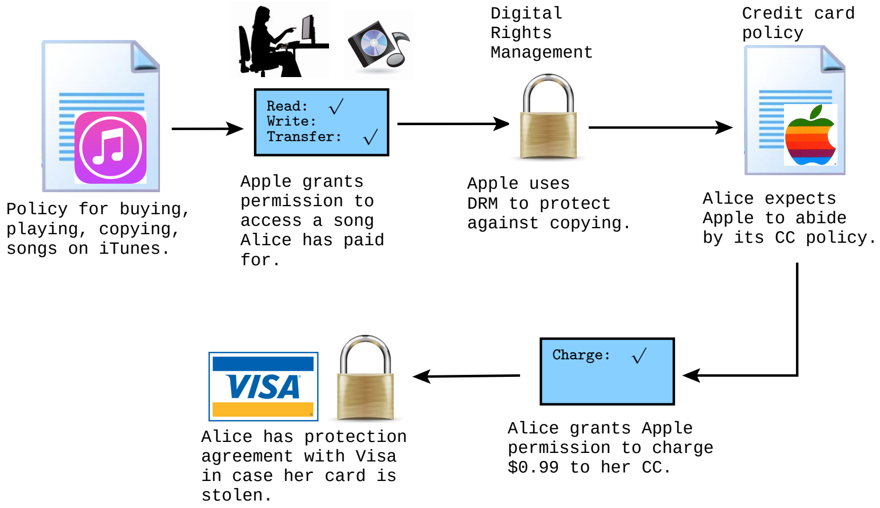
Read: √
Write:
Transfer: √
Print:

Description of actions that people/systems are allowed to perform.

Protections

Mechanisms that enforce policies and permissions.

Assurance: Apple iTunes



Policy for buying, playing, copying, songs on iTunes.

Read: √
Write:
Transfer: √

Apple grants permission to access a song Alice has paid for.

Digital Rights Management

Apple uses DRM to protect against copying.

Credit card policy

Alice expects Apple to abide by its CC policy.

Charge: √

Alice grants Apple permission to charge $0.99 to her CC.

Alice has protection agreement with Visa in case her card is stolen.

Assurance: Examples — Computer Usage

- Bob is enrolled in 466/566.
- The department has a policy in place saying students can use department computers for homework assignments only.
- Bob is granted permission by the department to use lectura.cs.arizona.edu according to the policy.
- The department uses passwords/groups/file modes/monitoring/... to protect against unauthorized use of CPU/memory/storage resources.

Authenticity

Definition (Authenticity)

The ability to determine that statements, policies, permissions issued by persons or systems are genuine.

- We need to be able to enforce contracts.
- We cannot enfore the contract unless we know it's genuine.

Authenticity: Nonrepudiation

Definition (Nonrepudiation)

The property that authentic statements issued by a person or system cannot be denied.

- A person could claim they didn't sign a contract, or say it was signed by someone else.

Authenticity: Mechanisms

- Blue-ink signatures — achieves nonrepudiation by allowing a person to commit to the authenticity of a document, by signing their name on it.
- Digital signatures — achieves nonrepudiation for digital documents, using cryptography.

Attack on Authenticity: Masquerading

Definition (Masquerading)

Create information that appears to be from someone who isn't the author.

- An attack on authenticity.
- Examples:
  1. Phishing: `BankOfAmerica.com` looks like `BankOfAmerica.com`, but isn't, and is used to gather username/passwords.
  2. Spoofing: Send a network packet with the wrong return IP address.

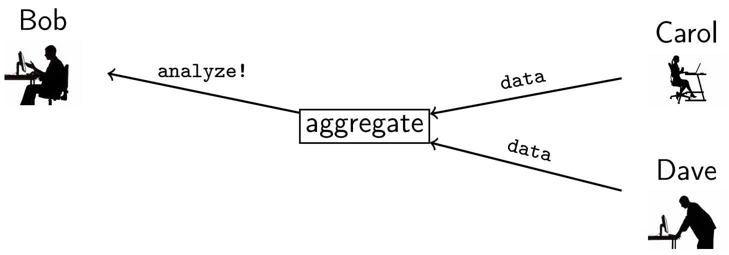
Anonymity

Definition (Anonymity)

Records or transactions cannot be attributed to any individual.

- Our identity is tied to the online transactions we perform:
  - medical records
  - purchases
  - legal records
  - email
  - browsing history

Anonymity Mechanisms: Aggregation



- Aggregation — merging data from many people, but only when sums/averages can't be mined for an individual's information.

Attack on Anonymity: Correlation/Traceback

Definition (Correlation/Traceback)

Merging several sources of information to determine a particular piece of information, or the source of the information.

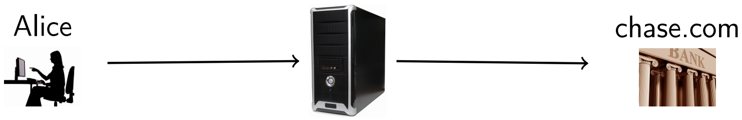
Aggregation Example: U.S. Census

- The Census publishes data (race, ethnicity, gender, age, salary) by zip-code.
- They won't publish the information if it would expose details about an individual.

Aggregation Example: Target

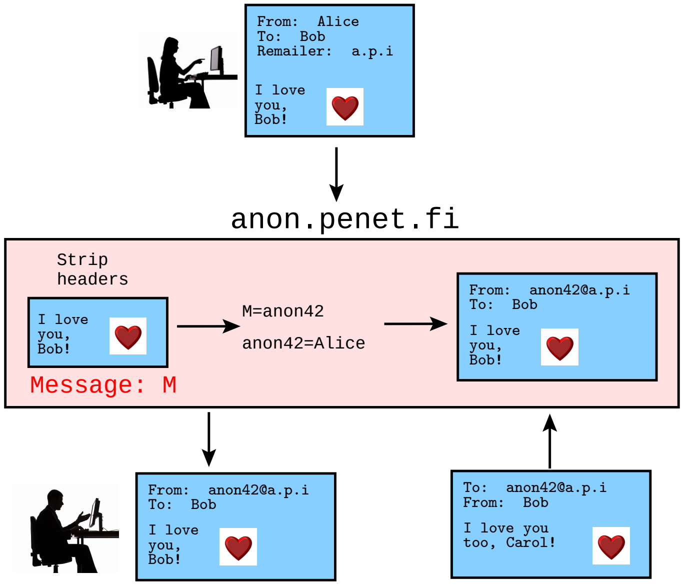
- The Colbert report: *The Word - Surrender to a Buyer Power*, http://www.cc.com/video-clips/dv9iqc/the-colbert-report-the-word---surrender-to-a-buyer-power

Anonymity Mechanisms: Proxies



- Proxies — trusted agents performing actions on behalf of a person, such that it can't be traced back to that individual.

Proxies Example: Pseduo-Anonymous Remailers



From: Alice
To: Bob
Remailer: a.p.i

I love you, Bob!

anon.penet.fi

Strip headers

I love you, Bob!

Message: M

M=anon42

anon42=Alice

From: anon42@a.p.i
To: Bob

I love you, Bob!

From: anon42@a.p.i
To: Bob

I love you, Bob!

To: anon42@a.p.i
From: Bob

I love you too, Carol!

Proxies Example: Pseduo-Anonymous Remailers. . .

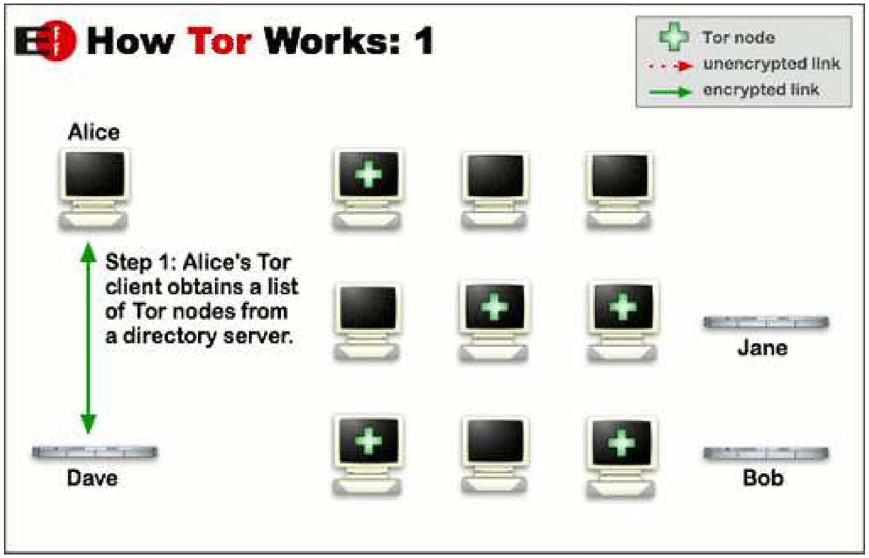
- In 1995 The Church of Scientology made a legal attack on anon.penet.fi to reveal the identity behind an144108@anon.penet.fi.

Proxies Example: Tor

- Data in the Tor network takes a random pathway through several relays.
- No observer can tell where the data came from or where it's going.
- Individuals use Tor to keep web sites from tracking them
- Journalists use Tor to communicate more safely with whistleblowers and dissidents.
- Law enforcement uses Tor for visiting web sites without revealing government IP addresses, and for security during sting operations.

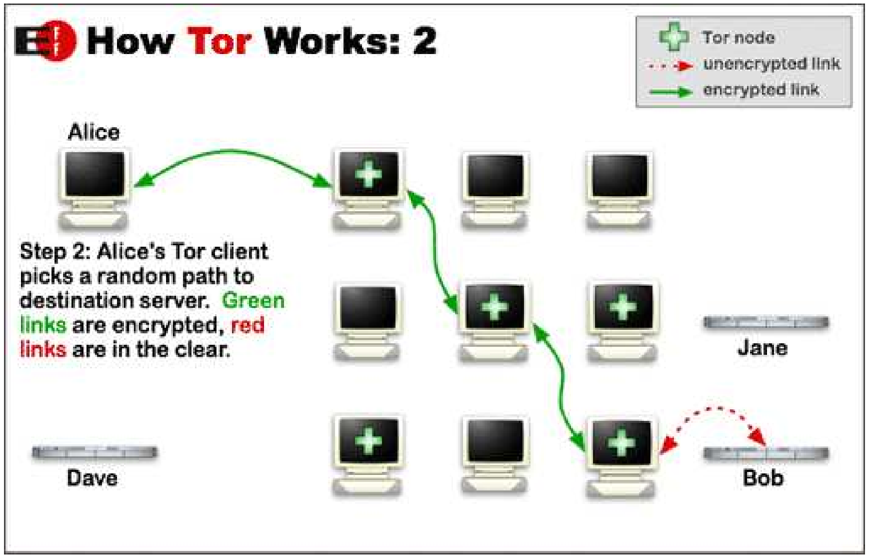
Proxies Example: Tor. . .

- See https://www.torproject.org
- The next 3 slides are from https://www.torproject.org/about/overview



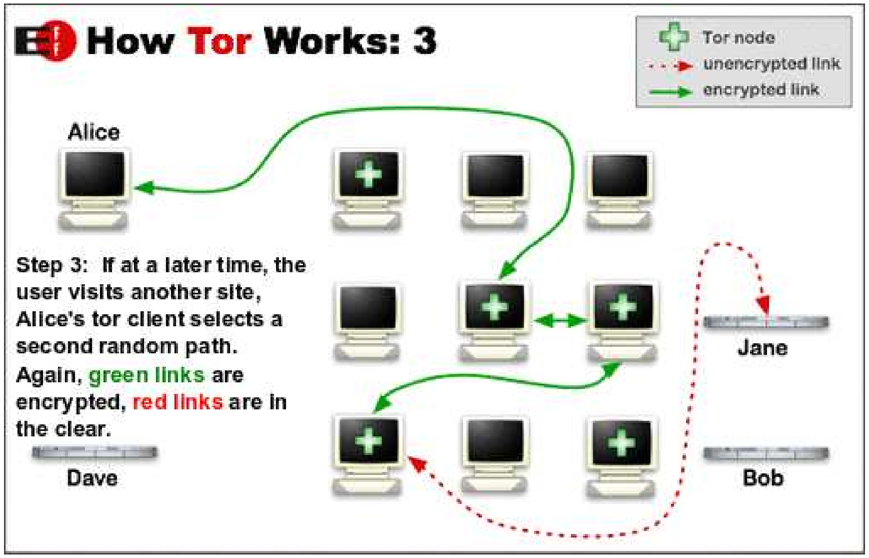
How Tor Works: 1

Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.



How Tor Works: 2

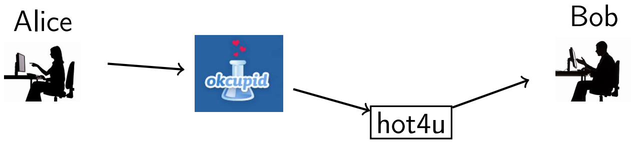
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.



How Tor Works: 3

Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

Anonymity Mechanisms: Pseudonyms



- Pseudonyms — fake identities used in online communication, such that only a trusted party knows the connection to the real identity.

Outline

1. Security Goals—AAA
   - Assurance
   - Authenticity
   - Anonymity
2. Summary

Readings

- Chapter 1 in *Introduction to Computer Security*, by Goodrich and Tamassia.

Acknowledgments I

Material and exercises have also been collected from these sources:

1. Roger G. Johnston, *Being Vulnerable to the Threat of Confusing Threats with Vulnerabilities*, `jps.anl.gov/Volume4_iss2/Paper3-RGJohnston.pdf`.
2. Bruce Schneier, *Attack Trees*, Dr. Dobb's Journal December 1999, `http://www.schneier.com/paper-attacktrees-ddj-ft.html`.
3. Bishop, *Introduction to Computer Security*.
4. Michael S. Pallos, `http://www.bizforum.org/whitepapers/candle-4.htm`.