Network Security

Dr. Haojin Zhu
Zhu-hj@cs.sjtu.edu.cn
https://nsec.sjtu.edu.cn/

About Instructor

- Dr. Haojin Zhu, Professor of Computer Science and Engineering Department
  - https://nsec.sjtu.edu.cn/
  - zhu-hj@cs.sjtu.edu.cn
  - Office: SEIEE 3-509
  - Office hours:
    - by appointment
    - TA: shaofeng li
      shaofengli2013@gmail.com

Course Objectives

- Learn some fundamental and advanced issues, concepts, principles, and mechanisms in network security
- Learn recent research advances in network security
- Prepare for graduate research in network security

Text

- No required textbook
- Research papers listed on the course website

Grading

- Attendance (20%)
- In-class paper presentation (40%)
- Course research project (2~3 persons a group) (40%)
  - A survey on a topic (normally related to your presentation) (30%)
  - 1~2 pages on your findings from this survey (10%)
    - Improvement of existing works (protocol/algorithm design)
    - Or System Implementation with a better performance

Grading (Cont'd)

- The final grades are computed according to the following criteria:
  - In-class paper presentation: your score is determined by peer-evaluation (will be discussed later)
  - Survey (please indicate each person's contribution in the survey paper)
  - Research findings (evaluation based on your novelty, and contribution)

Course Outline

- Topic 1: Network Security Basics
- Topic 2: Link Layer security
- Topic 3: Network Layer Security
- Topic 4: Transport-layer security and privacy
- Topic 5: Application-layer security and privacy

Course Outline

- Topic 6: Emerging research topics
  - Present later

Research Paper

- Small team -- at most 3 students per group
- Important Dates
  - Team Proposal due: April 5 (The first will have the priority)
  - Presentation Schedule fixed: April 4 (6rd week)
  - First Presentation: April 11 (7th week)
  - Report submission due: one week after last week's class
- The instructor will be available to discuss your topic via email or face-to-face discussion (by appointment)
- You should start thinking about team and topic now
  - How to select topic: introduce later

Paper Presentation

- Each group presents 3 papers depending on the technical difficulty of the presented papers (two persons on a paper).

- We have 6 papers to discuss.

Presenter's Preparation

- Please prepare your presentation slides.
- You have 25-30 minutes for your presentation. Please expect questions after one person's presentation. Your presentation will be graded based on the criteria in the grading form, which can be downloaded from our course website.

Peer Evaluation

- Your participation in grading is required.
- Your presentation score will be determined by the evaluations from the instructor (50%), the peer evaluation from the audience (50%)
- Your participation in grading other students' presentations (Attendance 20%).
- Please print the evaluation form and hand in the form after the class. All your evaluations will be kept as confidential.

Peer Evaluation (Cont'd)

- The highest and lowest peer evaluation scores will be deleted and the average of the remaining scores will be used as your final peer evaluation score.
- For example, if your peer evaluation scores from audience are 100, 99, 15, 87, 85, 77, 90. The highest score 100 is discarded and the lowest score 15 is also discarded. Your peer evaluation final score is the average of the remaining scores, which is 87.6
- If you have multiple identical highest/lowest scores, only one will be deleted.

Security Conferences

- 1st tier (Big 4)
- IEEE S&P(Oakland), ACM CCS, USENIX Security, NDSS

- 2nd tier
- ACSAC, ESORICS, WiSec, AsiaCCS, CT-RSA, and etc

Cryto Conferences

- 1st Tier
- Crypto, EUROCRYPT

- 2nd Tier
- ASIACRYPT, PKC, TCC, Financial Crypto and etc

Networking Conferences

- 1st Tier
- SIGCOMM, MOBICOM

- 2nd Tier
- INFOCOM, Mobihoc, SIGMETRICS, CONEXT, ICNP, ICDCS and etc

Presentation Topic 1
Electrical Cash

- **Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. 24 May 2009**
- Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing, Usenix Security'16
- TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub, NDSS'17

Presentation Topic 2
Smart Phone Security

- **Adrienne Porter Felt, Erika Chin, Android permissions demystified, Steve Hanna, Dawn Song, David Wagner. CCS 2011.**
- Tracking Mobile Web Users Through Motion Sensors: Attacks and Defenses, NDSS'16
- Life after App Uninstallation: Are the Data Still Alive? Data Residue Attacks on Android, NDSS'16
- Automated Analysis of Privacy Requirements for Mobile Apps, NDSS'17
- How They Did It: An Analysis of Emission Defeat Devices in Modern Automobiles, IEEE Oakland'17
- LUNA: Quantifying and Leveraging Uncertainty in Android Malware Analysis through Bayesian Machine Learning , Euro S&P 2017

Presentation Topic 3
IoT Security

- **Hidden Voice Commands, Usenix Security'16**
- **DolphinAttack: Inaudible Voice Commands, ACM CCS'17**
- Speechless: Analyzing the Threat to Speech Privacy from Smartphone Motion Sensors , IEEE Oakland'18
- Wi-Fly?: Detecting Privacy Invasion Attacks by Consumer Drones, NDSS'17
- Fingerprinting WiFi Devices using Software Defined Radios, wisec'16

Presentation Topic 4
Adversarial ML/ ML Privacy

- MagNet: a Two-Pronged Defense against Adversarial Examples, ACM CCS' 2017
- Membership Inference Attacks against Machine Learning Models , IEEE Oakland'2017.
- Tracing Information Flows Between Ad Exchanges Using Retargeted Ads, Usenix Security'16
- Stealing Machine Learning Models via Prediction APIs, Usenix Security'16
- Deep Learning with Differential Privacy, CCS'16

Presentation Topic 5
Social Network Security

- IVD: Automatic Learning and Enforcement of Authorization Rules in Online Social Networks, oakland'17
- Automated Crowdturfing Attacks and Defenses in Online Review Systems, ACM CCS'17
- Smoke Screener or Straight Shooter: Detecting Elite Sybil Attacks in User-Review Social Networks, NDSS'18, 2018.

Presentation Topic 6
Mobile Advertisement Security

- Investigating Ad Transparency Mechanisms in Social Media: A Case Study of Facebooks Explanations, NDSS'18, 2018
- Are these Ads Safe: Detecting Hidden Attacks through the Mobile App-Web Interfaces, NDSS 2016
- The Price of Free: Privacy Leakage in Personalized Mobile In-Apps Ads, NDSS'16
- What Mobile Ads Know About Mobile Users, NDSS'16
- Tracing Information Flows Between Ad Exchanges Using Retargeted Ads, Usenix Security'16

Presentation Topic 7
Cloud Security

- **CryptDB: Protecting Confidentiality with Encrypted Query Processing. In Proceedings of the 23rd ACM Symposium on Operating Systems Principles (SOSP), 2011.**

- Reduced Cooling Redundancy: A New Security Vulnerability in a Hot Data Center. NDSS'18

- SoK: Cryptographically Protected Database Search, Oakland'17

- TenantGuard: Scalable Runtime Verification of Cloud-Wide VM-Level Network Isolation, NDSS'17

Presentation Topic 8
TLS/SSL security

- Analyzing Forged SSL Certificates in the Wild , IEEE S&P 2014
  Lin-Shung Huang (Carnegie Mellon University), Alex Rice and Erling Ellingsen (Facebook), and Collin Jackson (Carnegie Mellon University)
- Triple Handshakes and Cookie Cutters: Breaking and Fixing Authentication over TLS
  Karthikeyan Bhargavan and Antoine Delignat-Lavaud (INRIA Paris-Rocquencourt), Cédric Fournet (Microsoft Research), Alfredo Pironti (INRIA Paris-Rocquencourt), and Pierre-Yves Strub (IMDEA Software Institute)
- Using Frankencerts for Automated Adversarial Testing of Certificate Validation in SSL/TLS Implementations
  Chad Brubaker and Suman Jana (University of Texas at Austin), Baishakhi Ray (University Of California Davis), and Sarfraz

Presentation Topic 9
Side Channel

- Leave Your Phone at the Door: Side Channels that Reveal Factory Floor Secrets, CCS'16
- Inferring User Routes and Locations using Zero-Permission Mobile Sensors, Oakland’16
- Privacy Threats through Ultrasonic Side Channels on Mobile Device, EURO S&P’17
- EyeTell: Video-Assisted Touchscreen Keystroke Inference from Eye Movements , Oakland’18

How to Determine Your Presentation Paper

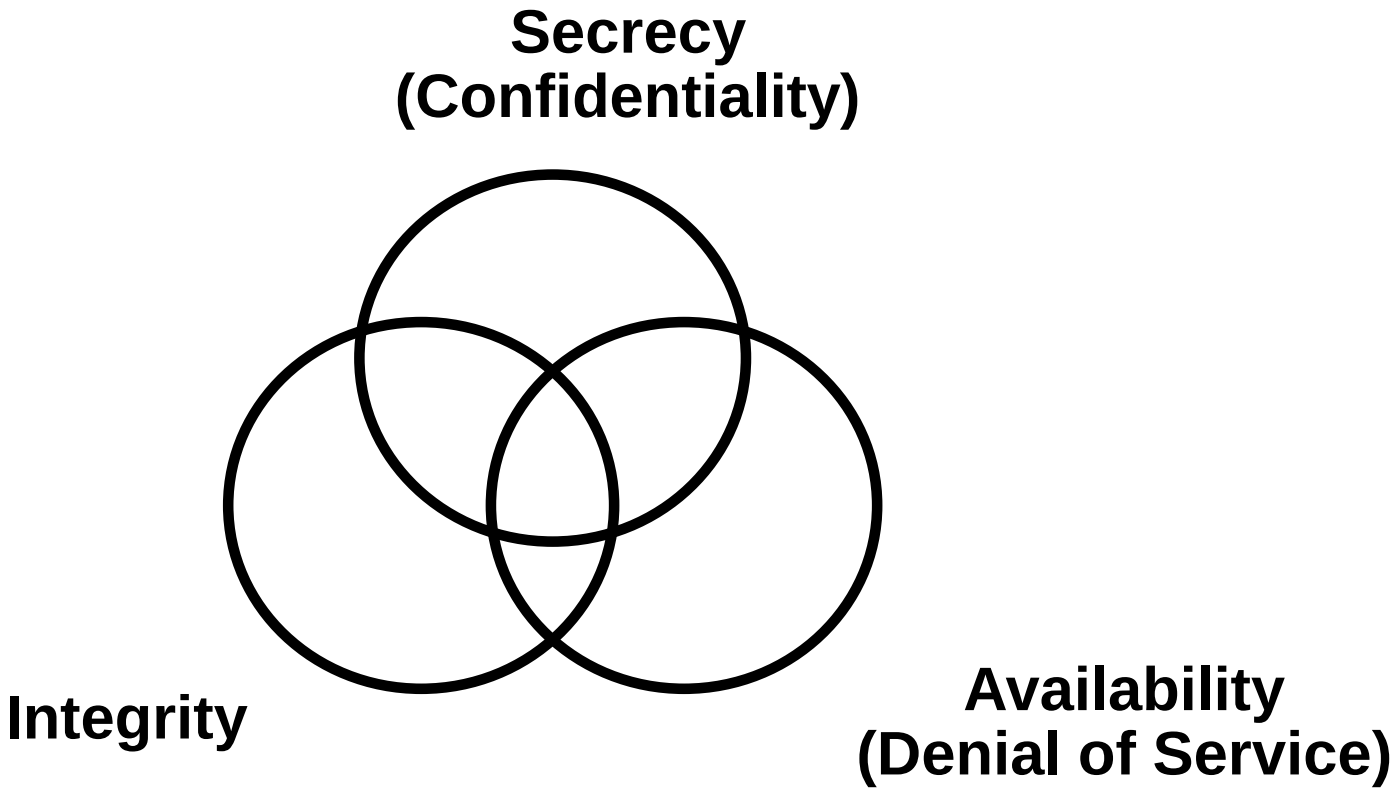
- Form Your Group First (2~3 persons)
- Send your team member names and the preferred topics via email

How to Determine Your Presentation Paper Cont’

- If no suitable topics for you, please discuss with me for an alternative choice.

A Brief Review of Basic Security Concepts

Security Objectives



Security Objectives

- Secrecy — Prevent/detect/deter improper disclosure of information
- Integrity — Prevent/detect/deter improper modification of information
- Availability — Prevent/detect/deter improper denial of access to services provided by the system

Commercial Example

- Secrecy — An employee should not know the salary of his manager
- Integrity — An employee should not be able to modify the employee's own salary
- Availability — Paychecks should be printed on time as stipulated by law

Military Example

- Secrecy — The target coordinates of a missile should not be improperly disclosed
- Integrity — The target coordinates of a missile should not be improperly modified
- Availability — When the proper command is issued the missile should fire

A Fourth Objective

- Securing computing resources — Prevent/detect/deter improper use of computing resources including
  - Hardware Resources
  - Software resources
  - Data resources
  - Network resources

Security Mechanisms

- In general three types
  - Prevention
  - Detection
  - Tolerance

Good prevention and detection both require good authentication as a foundation

Security Services

- Security functions are typically made available to users as a set of security services through APIs or integrated interfaces
- Confidentiality: protection of any information from being exposed to unintended entities.
  - Information content.
  - Parties involved.
  - how they communicate, how often, etc.
- Authentication: assurance that an entity of concern or the origin of a communication is authentic - it's what it claims to be or from
- Integrity: assurance that the information has not been tampered with

Security Services (Cont'd)

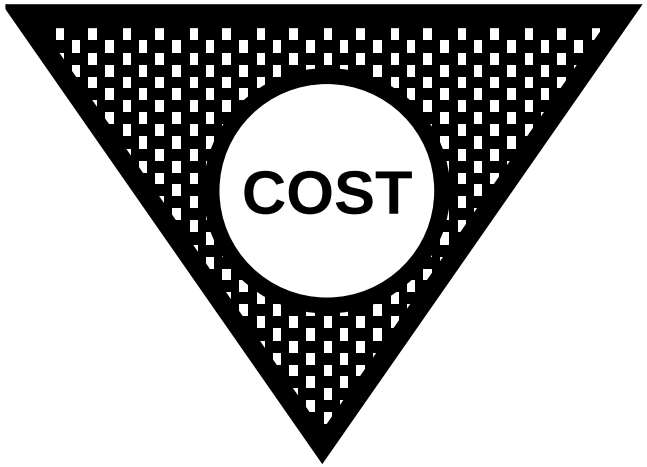
- Non-repudiation: offer of evidence that a party is indeed the sender or a receiver of certain information
- Access control: facilities to determine and enforce who is allowed access to what resources, hosts, software, network connections
- Monitor & response: facilities for monitoring security attacks, generating indications, surviving (tolerating) and recovering from attacks

Security Assurance

- How well your security mechanisms guarantee your security policy
- Everyone wants high assurance
- High assurance implies high cost
  - May not be possible
- Trade-off is needed

Security Tradeoffs

Security **Functionality**



Ease of Use

Security by Obscurity

- Security by obscurity
  - If we hide the inner workings of a system it will be secure
- More and more applications open their standards (e.g., TCP/IP, 802.11)
- Widespread computer knowledge and expertise

Security by Legislation

- Security by legislation says that if we instruct our users on how to behave we can secure our systems
- For example
  - Users should not share passwords
  - Users should not write down passwords
  - Users should not type in their password when someone is looking over their shoulder
- User awareness and cooperation is important, but cannot be the principal focus for achieving security

Threat-Vulnerability

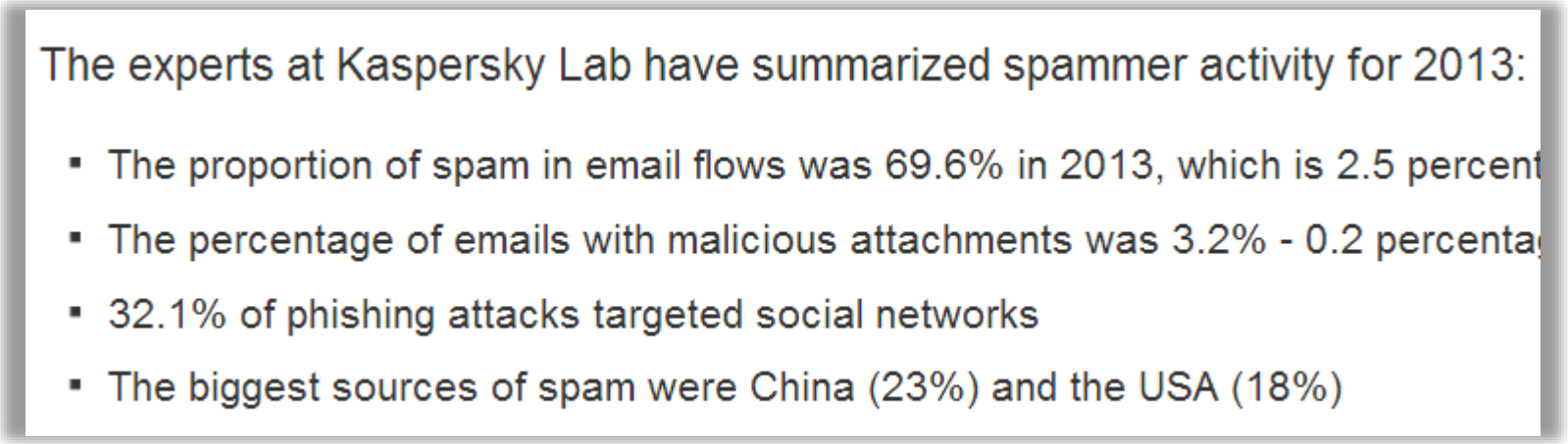
- Threats — *Possible* attacks on the system
- Vulnerabilities — Weaknesses that may be exploited to cause loss or harm

Threat Model and Attack Model

- Threat model and attack model need to be clarified before any security mechanism is developed
- Threat model
  - Assumptions about potential attackers
  - Describes the attacker's capabilities
- Attack model
  - Assumptions about the attacks
  - Describe how attacks are launched

Introduction to Network Security

- Security Breaches
  - http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
- Symantec Threat Explorer
  - http://us.norton.com/security_response/threatexplorer/index.jsp
- Email Spam



Introduction to Network Security

- Security threats
  - Malware: Virus, worm, spyware
  - Spam
  - Botnet
  - DDoS attacks
  - Phishing
  - Cross-site scripting (XSS)
  - …

Contributing Factors

- Lack of awareness of threats and risks of information systems
  - Security measures are often not considered until an Enterprise has been penetrated by malicious users
- Wide-open network policies
  - Many Internet sites allow wide-open Internet access
- Lack of security in TCP/IP protocol suite
  - Most TCP/IP protocols not built with security in mind
- Complexity of security management and administration
- Software vulnerabilities
  - Example: buffer overflow vulnerabilities
- Cracker skills keep improving

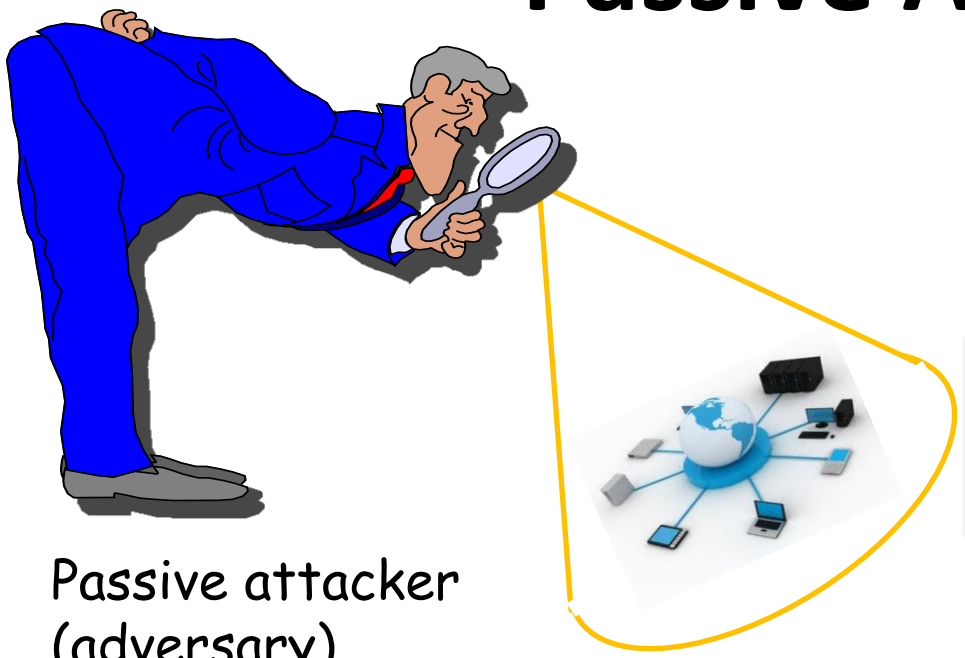
OSI Security Architecture

- ITU-T X.800 “Security Architecture for OSI”
- Defines a systematic way of defining and providing security requirements
- It provides a useful, if abstract, overview of concepts we will study

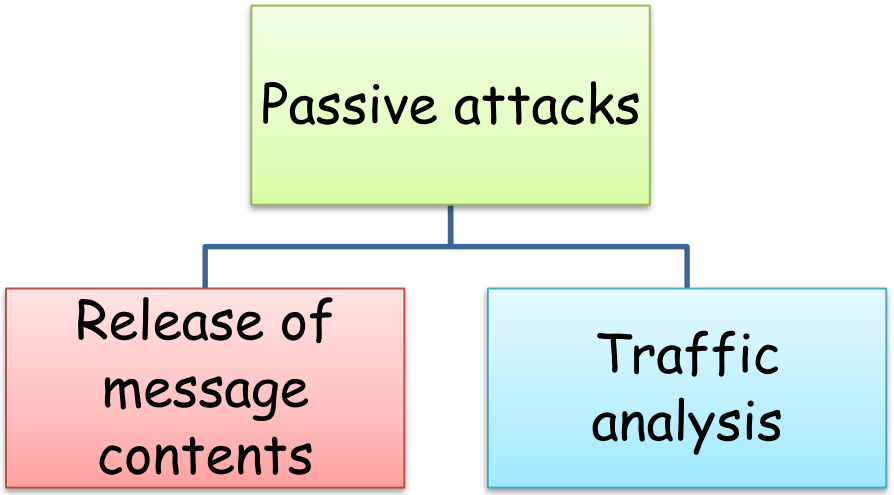
Aspects of Security

- 3 aspects of security:
  - **security attack**
    - Any action that compromises the security of information owned by an organization
  - **security mechanism**
    - A process that is designed to detect, prevent, or recover from a security attack
  - **security service**
    - Counter security attacks: make use of one or more security mechanisms to provide the service

Passive Attacks

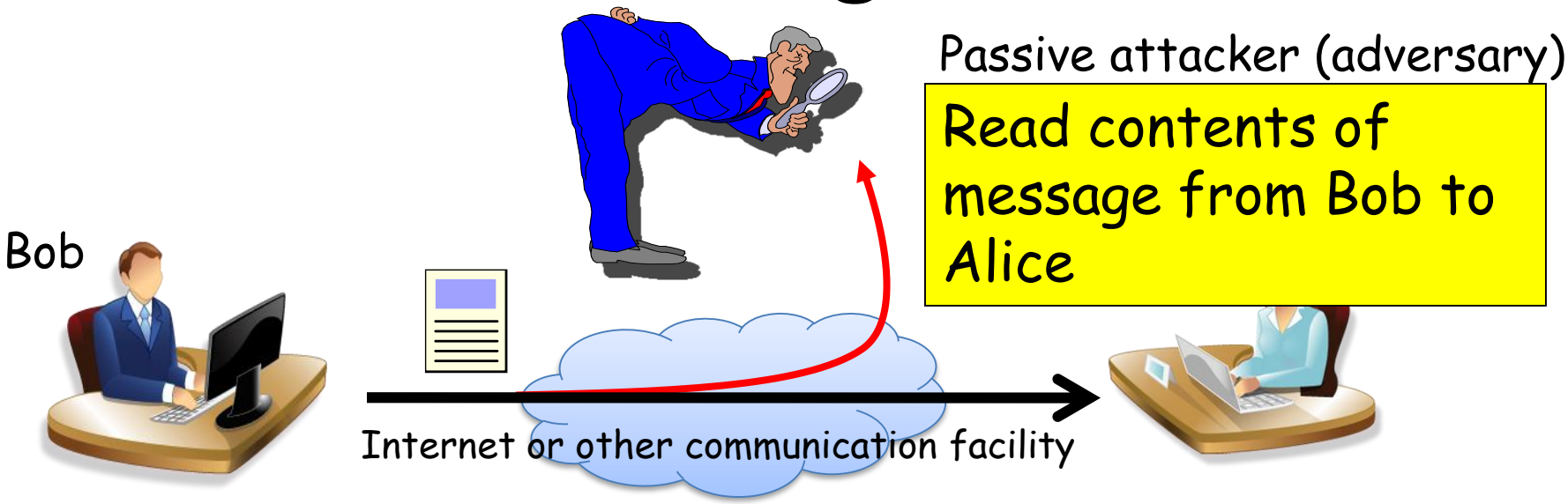


Passive attacker (adversary)



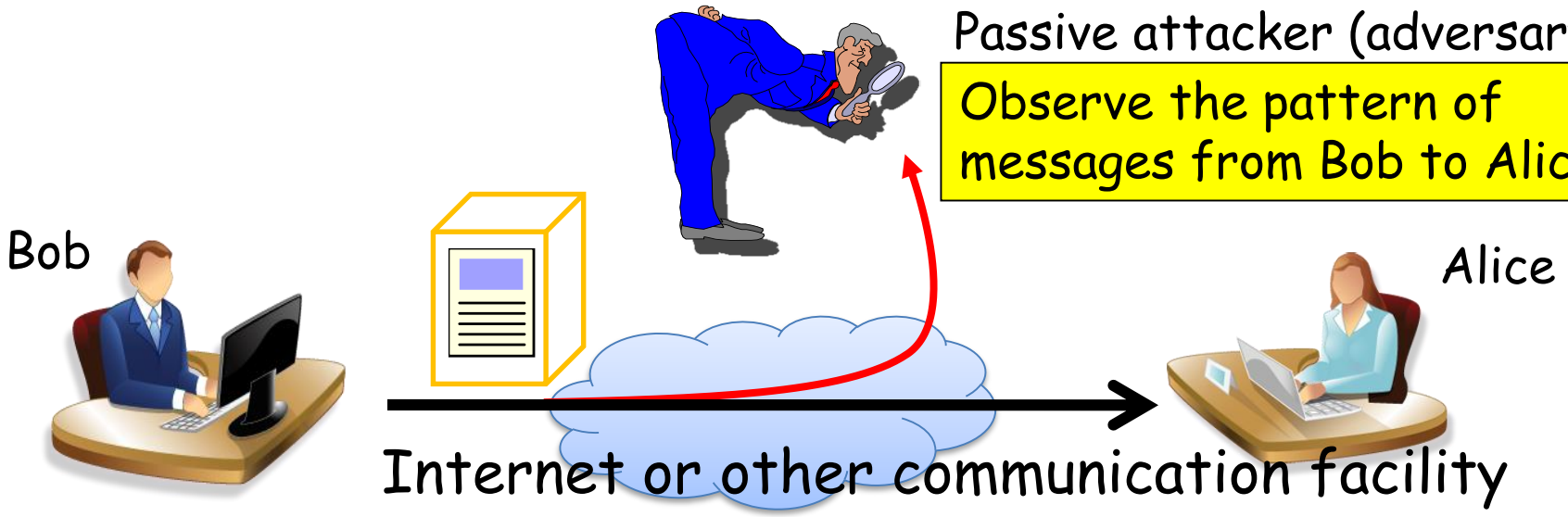
- **Passive attacks**
  - in the nature of eavesdropping on, or monitoring of, transmissions.
  - the goal is to obtain information that is being transmitted.
- Two types of passive attacks
  - release of message contents
  - traffic analysis.

Release of Message Contents

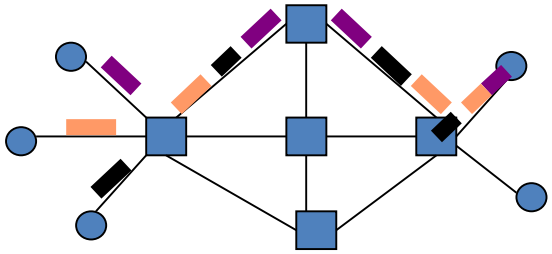


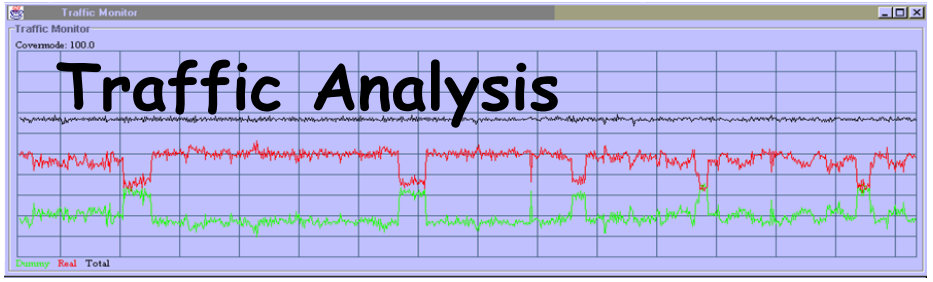
- **The release of message contents:**
  - A telephone conversation, an e-mail message, and a transferred file may contain sensitive or confidential information.
  - The attacker: identify the sensitive or confidential information.

Release of Message Contents Traffic Analysis

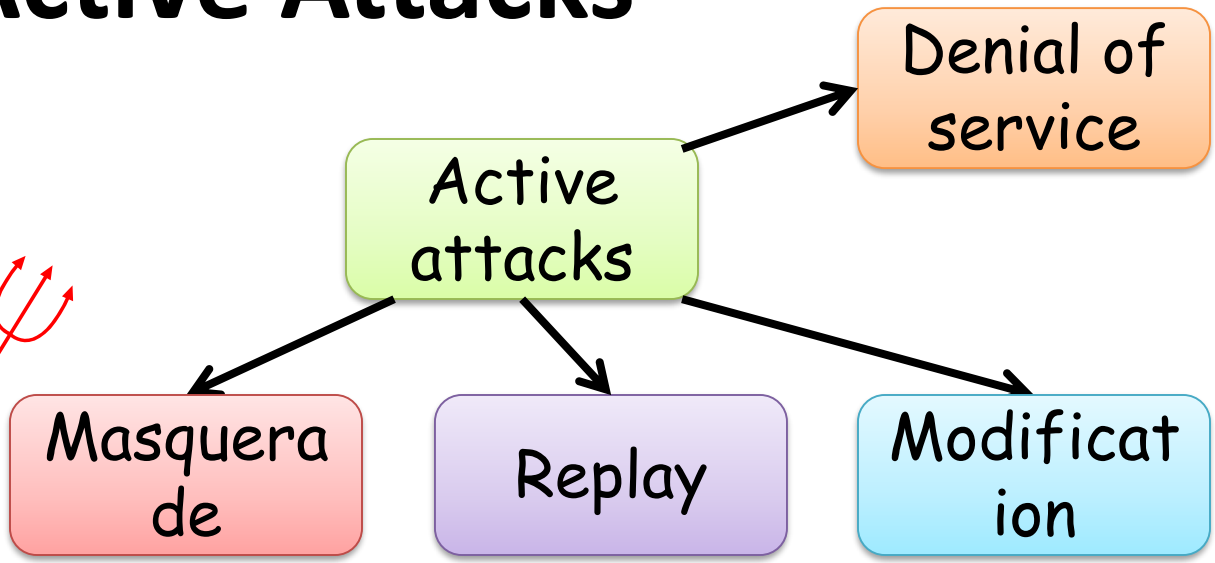


- **Traffic Analysis:** the goal of an attacker is to
  - observe the pattern of these messages, e.g.,frequency
  - determine the location and identity of communicating hosts





Active Attacks



Active attacker (adversary)

- **Active attacks**
  - involve some malicious actions on the transmission
  - can be subdivided into four categories:
    - ✓ masquerade,
    - ✓ replay,
    - ✓ modification of messages,
    - ✓ denial of service.

Masquerade

CNET › News › Personal Tech

November 8, 1999 6:55 PM PST

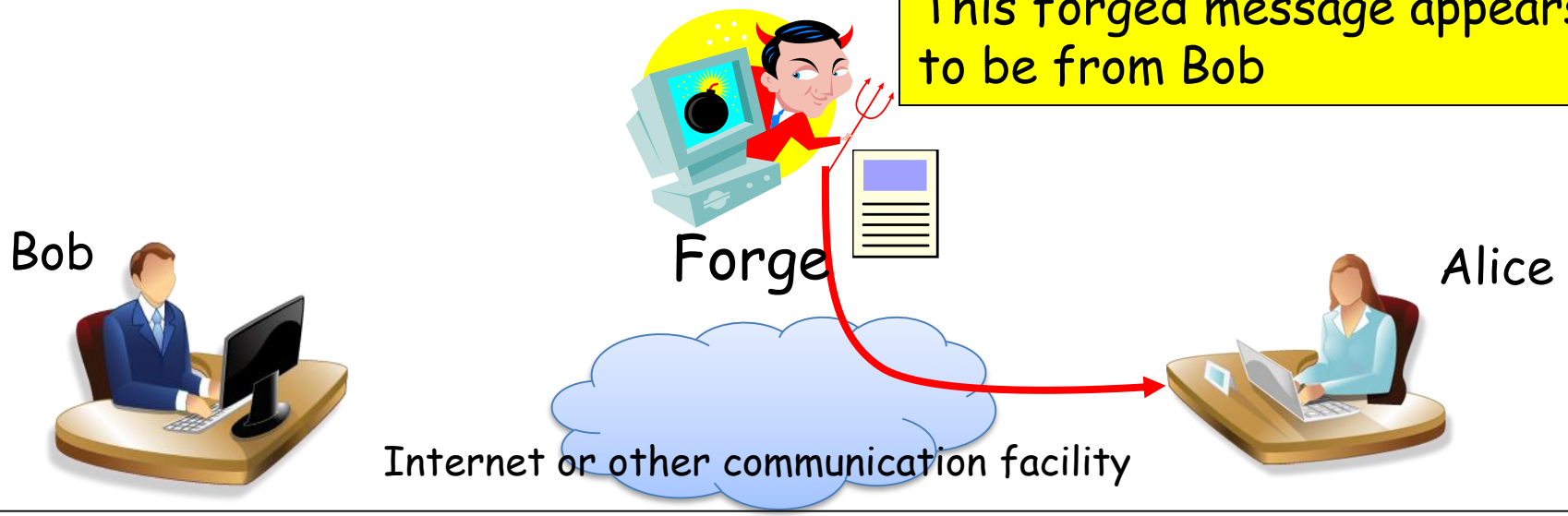
Outlook vulnerable to masquerade attack

By Stephen Shankland
Staff Writer, CNET News

http://news.cnet.com/Outlook-vulnerable-to-masquerade-attack/2100-1040_3-232656.html

Active attacker (adversary)

This forged message appears to be from Bob



- **Masquerade:**
  - one entity pretends to be a different entity
  - in order to gain unauthorized access or malicious goal

Replay

Gmail hacking through Cookie replay by using GX cookie value

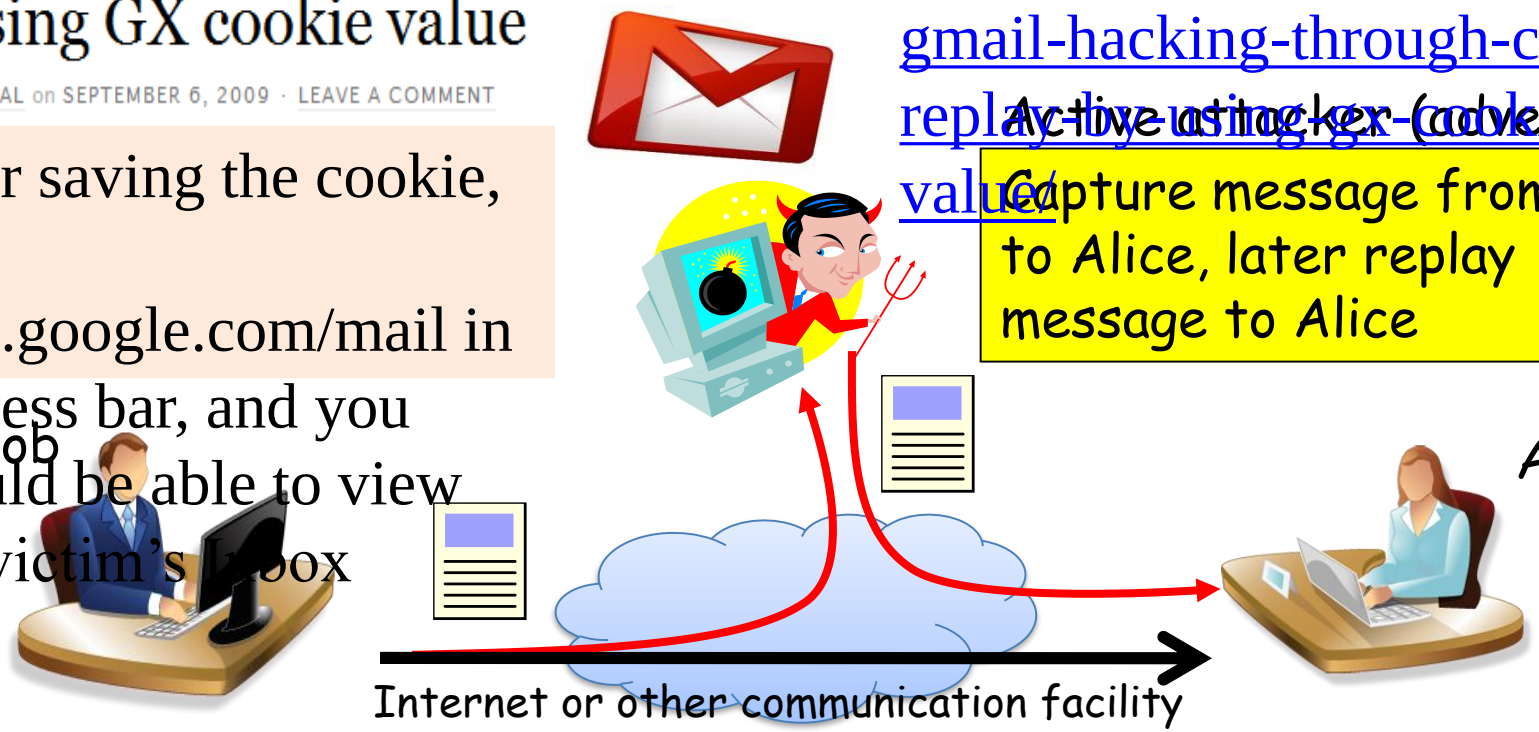
by RAVI GOPAL on SEPTEMBER 6, 2009 · LEAVE A COMMENT

After saving the cookie, type mail.google.com/mail in address bar, and you should be able to view the victim's Inbox

http://www.ravigopal.com/blog/gmail-hacking-through-cookie-replay-by-using-gx-cookie-value/

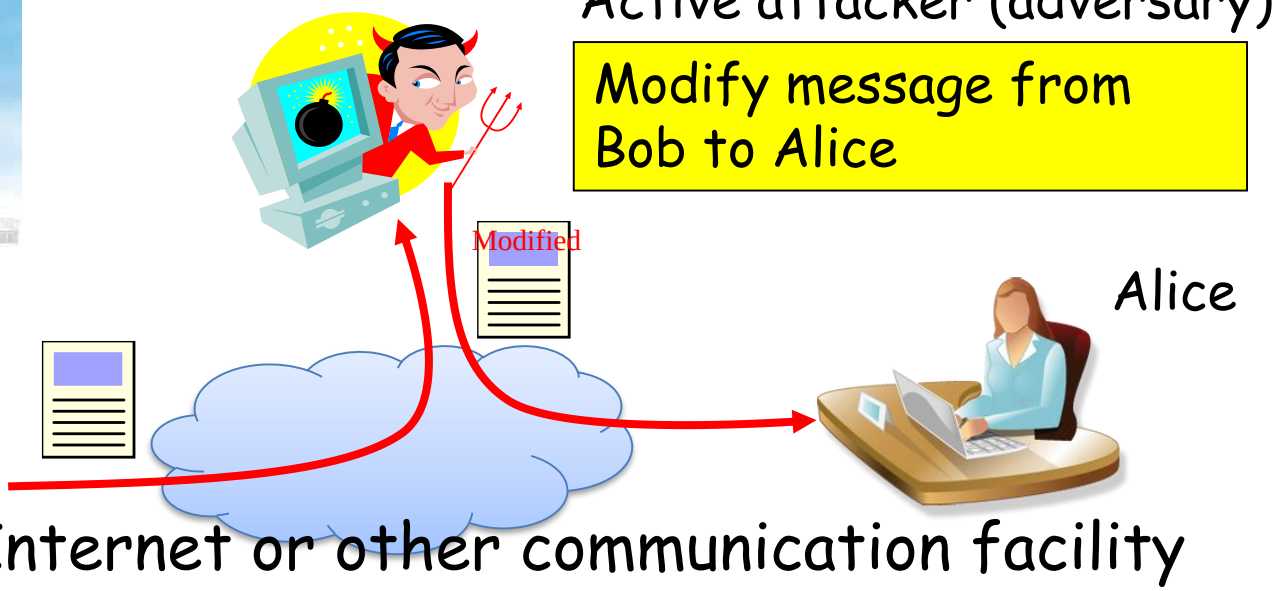
Active attacker (adversary)

Capture message from Bob to Alice, later replay message to Alice



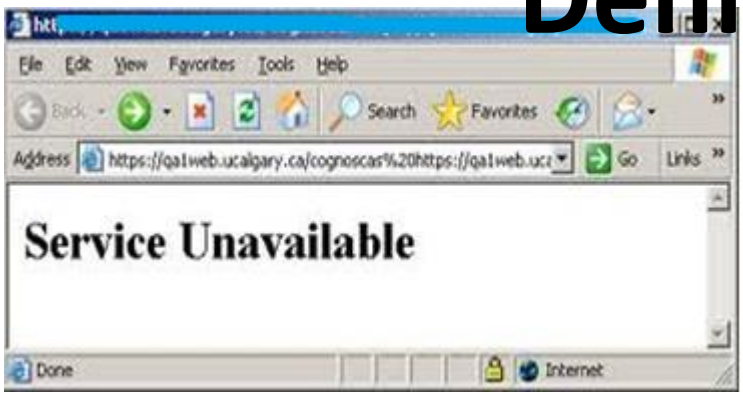
- **Replay:**
  - involves the passive capture of the transmitted data
  - subsequently replays it to produce an unauthorized effect

Modification



- **Modification:**
  - make some modification of the transmitted data
  - to produce an unauthorized effect.
- For example,
  - a message "Allow Alice to read confidential file accounts"
  - is modified to "Allow Alice to delete confidential file accounts."

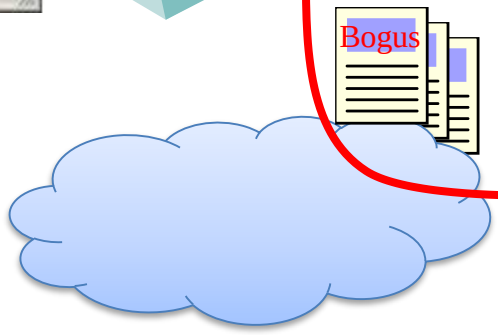
Denial of Service



Active attacker (adversary)

Disrupt service provided by server

Bob



Server

Internet or other communication facility

- **Denial of Service (DoS):** prevents the normal use or management of communication facilities.
  - by overloading it with messages so as to degrade its performance.

Security Mechanism (X.800)

- Specific security mechanisms:
  - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- Pervasive security mechanisms:
  - trusted functionality, security labels, event detection, security audit trails, security recovery