EE515/IS523
Think Like an Adversary
Lecture 1 Introduction

Yongdae Kim

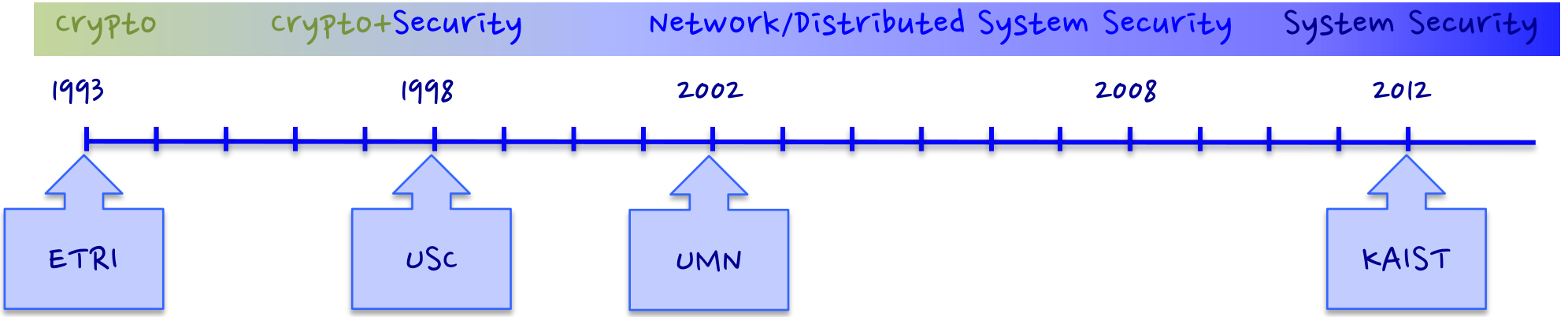
KAIST

Offense vs. Defense

- “Know your enemy.” – Sun Tzu
- "the only real defense is active defense” - Mao Zedong
- “security involves **thinking like an attacker, an adversary or a criminal**. If you don’t see the world that way, you’ll never notice most security problems.” - Bruce Schneier

Instructor, TA, Office Hours

- Instructor
  - Yongdae Kim
    - » 8th time teaching EE515/IS523
    - » 30th time teaching a security class
  - Email: yongdaek (at) kaist. ac. Kr
    yongdaek (at) gmail. com
    - » Please include ee515 or is523 in the subject of your mail
  - Office: N26 201
  - Office Hours: TBD
- TA
  - EE TA: Dohyun Kim dohyunjk (at) kaist.ac.kr
    Micheol Son mcson (at) kaist.ac.kr
  - GSIS TA: Minjung Kim (mjkim9334 (at) kaist.ac.kr)
  - security101_ta (at) syssec.kaist.ac.kr
  - Office hours: by appointment only



- 25+ year career in security research
  - Applied Cryptography, Group key agreement, Storage, P2P, Mobile/Sensor/Ad-hoc/Cellular Networks, Social networks, Internet, Anonymity, Censorship

- Published about 80 papers (+6,400 Google scholar citations)

Class web page, e-mail

- http://security101.kr
  - Read the page carefully and regularly!
  - Read the Syllabus carefully.
  - Check calendar.

- E-mail policy
  - Include [ee515] or [is523] in the subject of your e-mail

Textbook

- Required: Papers!

- Optional
  - Handbook of Applied Cryptography by Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone (Editor), CRC Press, ISBN 0849385237, (October 16, 1996) Available on-line at http://www.cacr.math.uwaterloo.ca/hac/
  - Security Engineering by Ross Anderson, Available at http://www.cl.cam.ac.uk/~rja14/book.html.

Goals

- To discover new attacks in emerging systems
- The main objective of this course is to learn how to think like an adversary.
- Review various ingenuous attacks and discuss why and how such attacks were possible.
- Students who take this course will be able to analyze security of practical systems

No Goals

- In depth study of OS/Software/Network security and Cryptography
- Hands-on Hacking Tutorial on Android, Windows, Embedded Systems, etc.

Course Content

- Overview
  - Introduction
  - Attack Model, Security Economics, Legal Issues, Ethics
  - Cryptography and Key Management
- Frequent mistakes
  - User Interface and Psychological Failures
  - Software Engineering Failures and Malpractices
- Case Studies
  - Embedded Device Security
  - Automobiles and IoT Security
  - Internet Protocols
  - RF Security
  - Low Level Attacks
  - Cellular Network Security
  - Cryptographic Failures
  - Sensing Security
  - Critical Systems
  - Medical Device Security
  - De-anonymization

Evaluation (IMPORTANT!)

- Approximately,
  - Lecture (20%)
  - Reading Report (14 x 3% = 42%)
  - Project (38%)

Group Projects

- Each project should have some "research" aspect.
- Group size
  - Min 1 Max 5
- Important dates
  - Pre-proposal: Sep 25, 11:59 PM.
  - Full Proposal: Oct 9, 11:59 PM.
  - Midterm report: Nov 4, 11:59 PM
  - Final report: Dec 11, 11:59 PM.
- Project examples
  - Attack, attack, attack!
  - Analysis
  - Measurement

Grading

- Absolute (i.e. not on a curve)
  - But flexible ;-)

- Grading will be as follows
  - 93.0% or above yields an A, 90.0% an A-
  - 85% = B+, 80% = B, 75% = B-
  - 70% = C+, 65% = C, 60% = C-
  - 55% = D+, 50% = D, and less than 50% yields an F.

Reading Report (Precise and Concise)

- Target System
- Target Service
- Vulnerability
- Exploitation (Attacks)
- Evaluation
- Defense
- Future Work: After reading this paper, what could be the next step?
  - Any problem in evaluation?
  - Other targets?
  - Other vulnerabilities?

And…

- Incompletes (or make up exams) will in general not be given.
  - Exception: a provably serious family or personal emergency arises with proof and the student has already completed all but a small portion of the work.

- Scholastic conduct must be acceptable. Specifically, you must do your assignments, quizzes and examinations yourself, on your own.

The Telegraph

HOME | NEWS | WORLD | SPORT | FINANCE | COMMENT | BLOGS | CULTURE | TRAVEL | LIFE

Politics | Obits | Education | Earth | Science | Defence | Health | Scotland | Royal | Celebrities

HOME » NEWS » UK NEWS » CRIME

Thieves placed bugs and hacked onboard computers of luxury cars

The leader of a gang that hacked into the onboard computers of luxury cars and bugged them with GPS tracking devices before stealing them is facing jail.

Bloomberg Our Company | Professional | Anywhere

HOME | QUICK | NEWS | OPINION | MARKET DATA | PERSONAL FINANCE | TECH | POLITICS

McAfee Hacker Says Medtronic Insulin Pumps Vulnerable To Attack

Confirmed: US and Israel created Stuxnet, lost control of it

Stuxnet was never meant to propagate in the wild.

by **Nate Anderson** - June 1 2012, 6:00am EDT

HACKING | NATIONAL SECURITY | 277

KrebsonSecurity

In-depth security news and investigation

FBI: Smart Meter Hacks Likely to Spread

Iran's Flying Saucer Downed U.S. Drone, Engineer Claims

By Spencer Ackerman and Noah Shachtman ✉ January 10, 2012 | 1:00 pm |
Categories: Tinfoil Tuesday

Most CCTV systems are easily accessible to attackers

Andy Greenberg, Forbes Staff

Covering the worlds of data security, privacy and hacker culture.

+ Follow (512)

SPONSORED BY SAS

SECURITY | 7/23/2012 @ 12:17PM | 218,082 views

Hacker Will Expose Potential Security Flaw In Four Million Hotel Room Keycard Locks

The cyberweapon that could take down the internet

› 13:30 11 February 2011 by **Jacob Aron**
› For similar stories, visit the **Computer crime** Topic Guide

27th Chaos Communication Congress

We come in peace

Wideband GSM Sniffing

The Telegraph

HOME | NEWS | WORLD | SPORT | FINANCE | COMMENT | BLOGS | CULTURE | TRAVEL | LIFE | FASHI

Politics | Obits | Education | Earth | Science | Defence | Health | Scotland | Royal | Celebrities

HOME » NEWS

Marie Colvin: Syria regime accused of murder in besieged Homs

Security Engineering

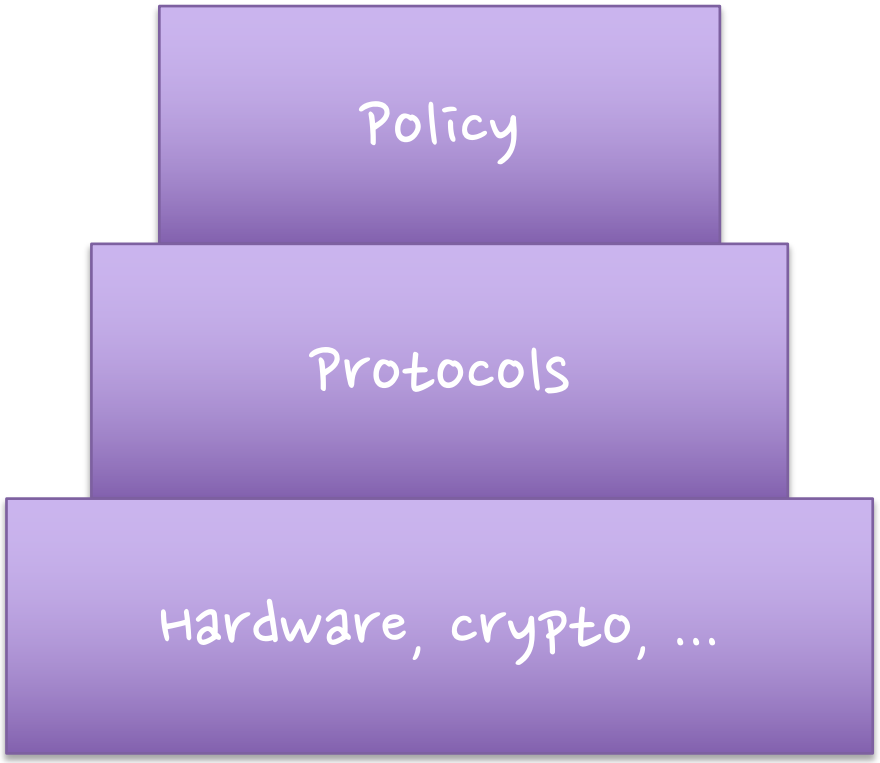
- Building a systems to remain dependable in the face of malice, error or mischance

System	Service	Attack Deny Service, Degrade QoS, Misuse	Security Prevent Attacks
Communication	Send message	Eavesdrop	Encryption
Web server	Serving web page	DoS	CDN?
Computer	;-)	Botnet	Destroy
SMS	Send SMS	Shutdown Cellular Network	Rate Control, Channel separation
Pacemaker	Heartbeat Control	Remote programming and eavesdropping	Distance bounding?
Nike+iPod	Music + Pedometer	Tracking	Don't use it?
Recommendation system	Collaborative filtering	Control rating using Ballot stuffing	?

TSA Body Scanner

Design Hierarchy

- What are we trying to do?
- How?
- With what?
- Considerations
  - Top-down vs. Bottom-up
  - Iterative
  - Convergence
  - environment change



Goals: Confidentiality

- Confidentiality of information means that it is accessible only by authorized entities
  - Contents, Existence, Availability, Origin, Destination, Ownership, Timing, etc… of:
  - Memory, processing, files, packets, devices, fields, programs, instructions, strings...

Goals: Integrity

- Integrity means that information can only be modified by authorized entities
  - e.g. Contents, Existence, Availability, Origin, Destination, Ownership, Timing, etc… of:
  - Memory, processing, files, packets, devices, fields, programs, instructions, strings...

Goals: Availability

- Availability means that authorized entities can access a system or service.

- A failure of availability is often called Denial of Service:
  - Packet dropping
  - Account freezing
  - Jamming
  - Queue filling

Goals: Accountability

- Every action can be traced to "the responsible party."

- Example attacks:
  - Microsoft cert
  - Guest account
  - Stepping stones

Goals: Dependability

- A system can be relied on to correctly deliver service
- Dependability failures:
  - Therac-25: a radiation therapy machine
    - » whose patients were given massive overdoses (100 times) of radiation
    - » bad software design and development practices: impossible to test it in a clean automated way
  - Ariane 5: expendable launch system
    - » the rocket self-destructing 37 seconds after launch because of a malfunction in the control software
    - » A data conversion from 64-bit floating point value to 16-bit signed integer value

Interacting Goals

- Failures of one kind can lead to failures of another, e.g.:
  - Integrity failure can cause Confidentiality failure
  - Availability failure can cause integrity, confidentiality failure
  - Etc…

Threat Model

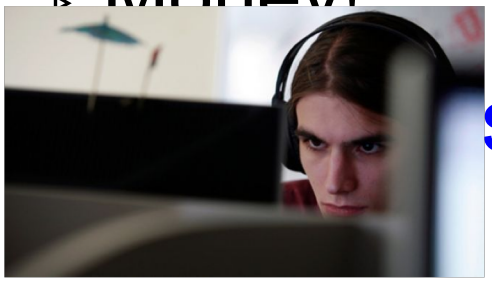
- What property do we want to ensure against what adversary?

- Who is the adversary?
- What is his goal?
- What are his resources?
  - e.g. Computational, Physical, Monetary…
- What is his motive?
- What attacks are out of scope?

Terminologies

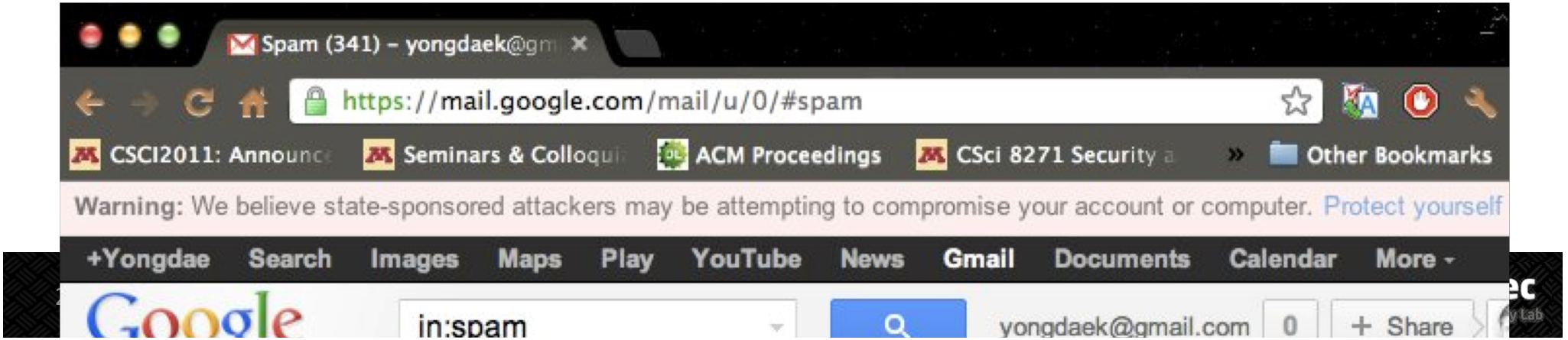
- Attack (Exploit): attempt to breach system security (DDoS)
- Threat: a scenario that can harm a system (System unavailable)
- Vulnerability: the “hole” that allows an attack to succeed (TCP)
- Security goal: “claimed” objective; failure implies insecurity

Who are the attackers?

- No more script-kiddies
  - sore
    - a n
  - 
  - 
  - 
  - 
  - 
  - 
  - Use of computers and computer networks as a
    - f prote
    - te po
  - Orga
    - inal
    - Money!
  - 
  - 
  - 
    - s

State-Sponsored Attackers

- 2012. 6: Google starts warning users who may be targets of government-sponsored hackers
- 2010 ~: Stuxnet, Duqu, Flame, Gauss, …
  - Mikko (2011. 6): A Pandora's Box We Will Regret Opening
- 2010 ~: Cyber Espionage from China
  - Exxon, Shell, BP, Marathon Oil, ConocoPhillips, Baker Hughes
  - Canada/France Commerce Department, EU parliament
  - RSA Security Inc. SecurID
  - Lockheed Martin, Northrop Grumman, Mitsubushi



Hacktivists

- promoting expressive politics, free speech, human rights, and information ethics
- Anonymous
  - To protest against SOPA, DDoS against MPAA, RIAA, FBI, DoJ, Universal music
  - Attack Church of Scientology
  - Support Occupy Wall Street

- LulzSec
  - Hacking Sony Pictures (PSP jailbreaking)
  - Hacking Pornography web sites
  - DDoSing CIA web site (3 hour shutdown)

Security Researchers

- They tried to save the world by introducing new attacks on systems

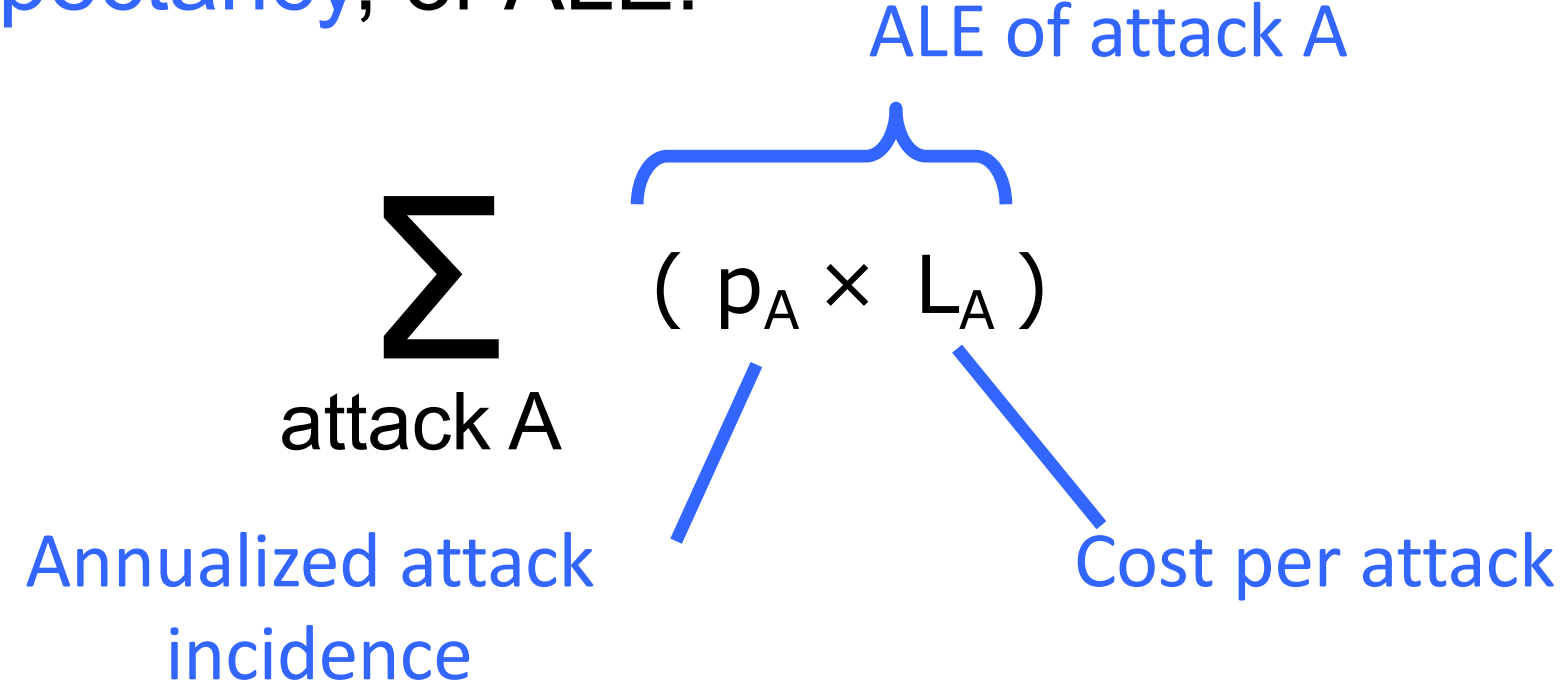
- Examples
  - Diebold AccuVote-TS Voting Machine
  - APCO Project 25 Two-Way Radio System
  - Kad Network
  - GSM network
  - Pacemakers and Implantable Cardiac Defibrillators
  - Automobiles, …

Rules of Thumb

- Be conservative: evaluate security under the best conditions for the adversary
- A system is as secure as the weakest link.
- It is best to plan for unknown attacks.

Security & Risk

- The risk due to a set of attacks is the expected (or average) cost per unit of time.
- One measure of risk is Annualized Loss Expectancy, or ALE:



Risk Reduction

- A defense mechanism may reduce the risk of a set of attacks by reducing L_A or p_A. This is the gross risk reduction (GRR):

$$\sum_{\text{attack A}} (p_A \times L_A - p'_A \times L'_A)$$

- The mechanism also has a cost. The net risk reduction (NRR) is GRR – cost.

Bug Bounty Program

- Evans (Google): “Seeing a fairly sustained drop-off for the Chromium”
- McGeehan (Facebook): The bounty program has actually outperformed the consultants they hire.
- Google: Patching serious or critical bugs within 60 days
- Google, Facebook, Microsoft, Mozilla, Samsung, …

Nations as a Bug Buyer

- ReVuln, Vupen, Netragard: Earning money by selling bugs
- “All over the world, from South Africa to South Korea, business is booming in what hackers call zero days”
- “No more free bugs.”
- ‘In order to best protect my country, I need to find vulnerabilities in other countries’
- Examples
  - Critical MS Windows bug: $150,000
  - a zero-day in iOS system sold for $500,000
  - Vupen charges $100,000/year for catalog and bug is sold separately
  - Brokers get 15%.

Sony vs. Hackers

do whatever to protect

Sony

Reimburse

PS3 Hack

settled

Hacke

2011. 3 $36.27 per share

2011. 6 $24.97 per share

recover

if PI leaked

encrypted

by 4.5%

Card on-line

Hacked

Outage cost $171M

Fired security staff

Posted Unreleased Michael Jackson video

Patco Construction vs. Ocean Bank

- Hacker stole ~$600K from Patco through Zeus
- The transfer alarmed the bank, but ignored

- “commercially unreasonable”
  - Out-of-Band Authentication
  - User-Selected Picture
  - Tokens
  - Monitoring of Risk-Scoring Reports

Cost of Data Breach

Ponemon Cost of Data Breach Study: 12th year in measuring cost of data breach

Company	Year	Data	Cost (USD)
Anthem	2015	80 M patient and employee records	100M
Ashley Madison	2015	33 M user accounts	850M
Ebay	2014	145M customer accounts	200M
JPMorgan Chase	2014	Financial/Personal Info of 76 M Personal, 7M Small B	1000M
Home Depot	2014	56 M credit card and 53 M email addresses.	80 M
Sony Pictures	2014	Personal Information of 3,000 employees	35 M
Target	2013	40 M credit and debit card, 70 M customer	252 M
Global Payments	2012	1.5M card accounts	90 M
Tricare	2011	5 M Tricare Military Beneficiary	130 M
Citi Bank	2011	360,000 Credit Card	19 M
Hearland	2009	130M Card	2800 M

Auction vs. Customers

- Auction's fault
  - Unencrypted Personal Information
  - It did not know about the hacking for two days
  - Passwords
    - » 'auction62', 'auctionuser', 'auction'
  - Malwares and Trojan horse are found in the server.

- Not gulity, because
  - Hacker utilized new technology, and were well-organized.
  - Auctions have too many server.
  - AVs have false alarms.
  - For large company like auction, difficult to use.
  - Causes massive traffic.

Security theater is the practice of

- investing in countermeasures intended to provide the **feeling of improved security**
- while doing little or nothing to **actually achieve it**

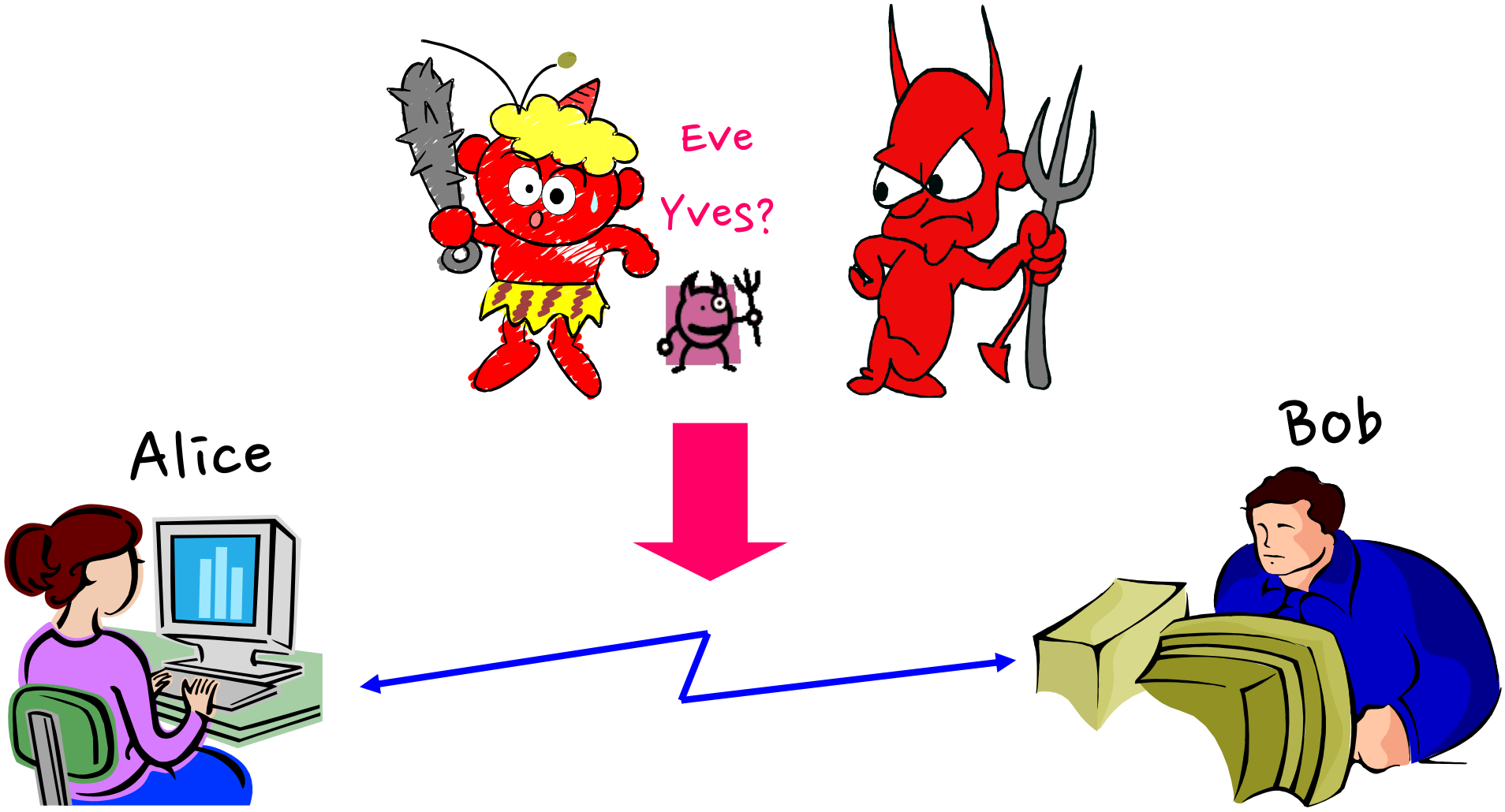
Security of New Technologies

- Most of the new technologies come with new and old vulnerabilities.
  - Old vulnerabilities: OS, Network, Software Security, …
  - Studying old vulnerabilities is important, yet less interesting.
  - e.g. Stealing Bitcoin wallet, Drone telematics channel snooping

- New Problems in New Technologies
  - Sensors in Self-Driving Cars and Drones
  - Security of Deep Learning
  - Block Chain Pool Mining Attacks
  - Brain Hacking

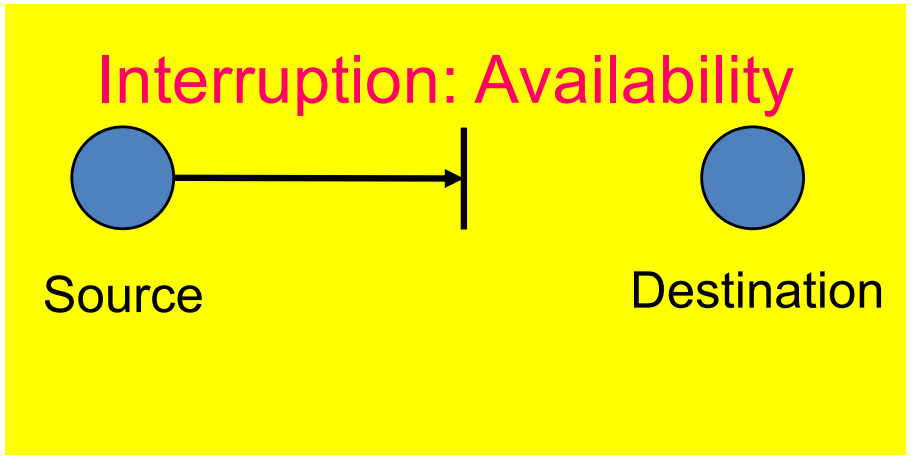
Basic Cryptography

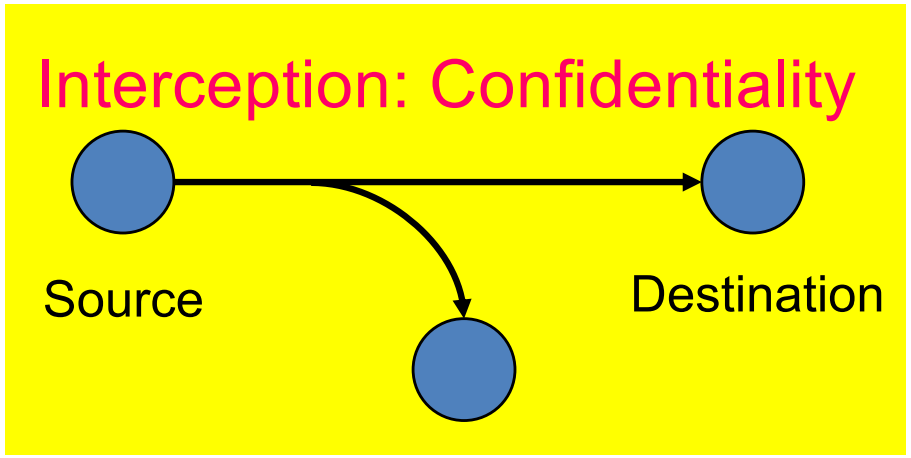
The Main Players

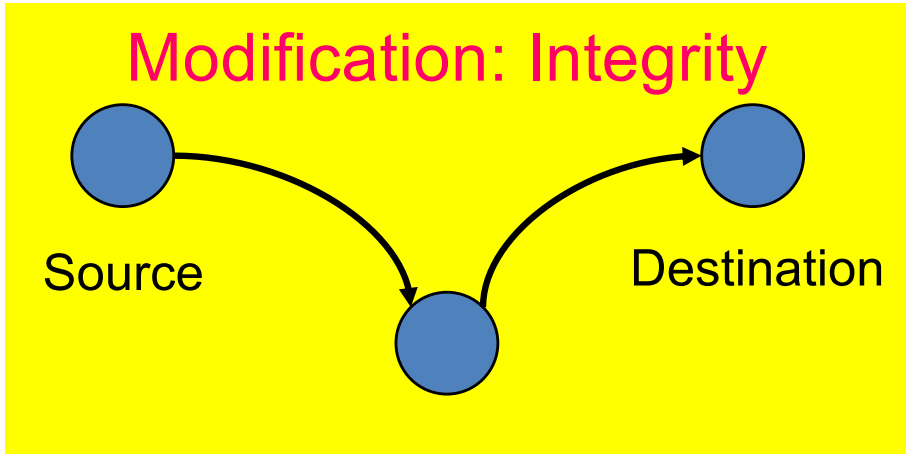


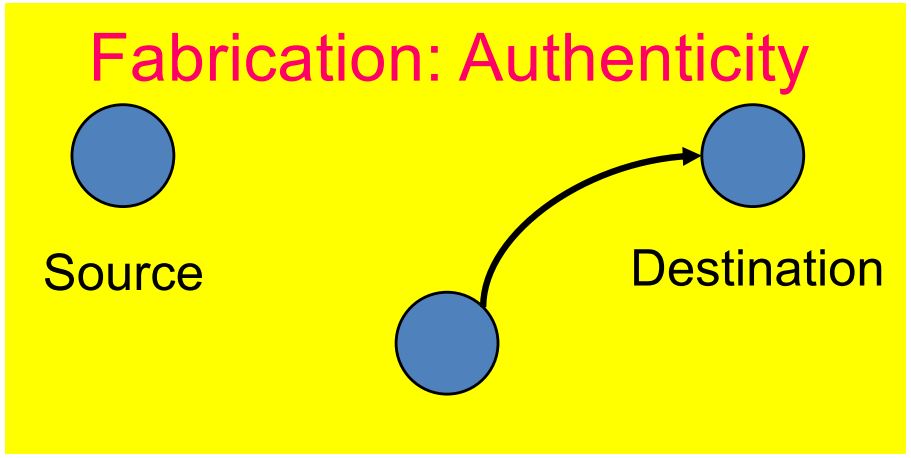
Attacks


Normal Flow
Source
Destination


Interruption: Availability
Source
Destination


Interception: Confidentiality
Source
Destination

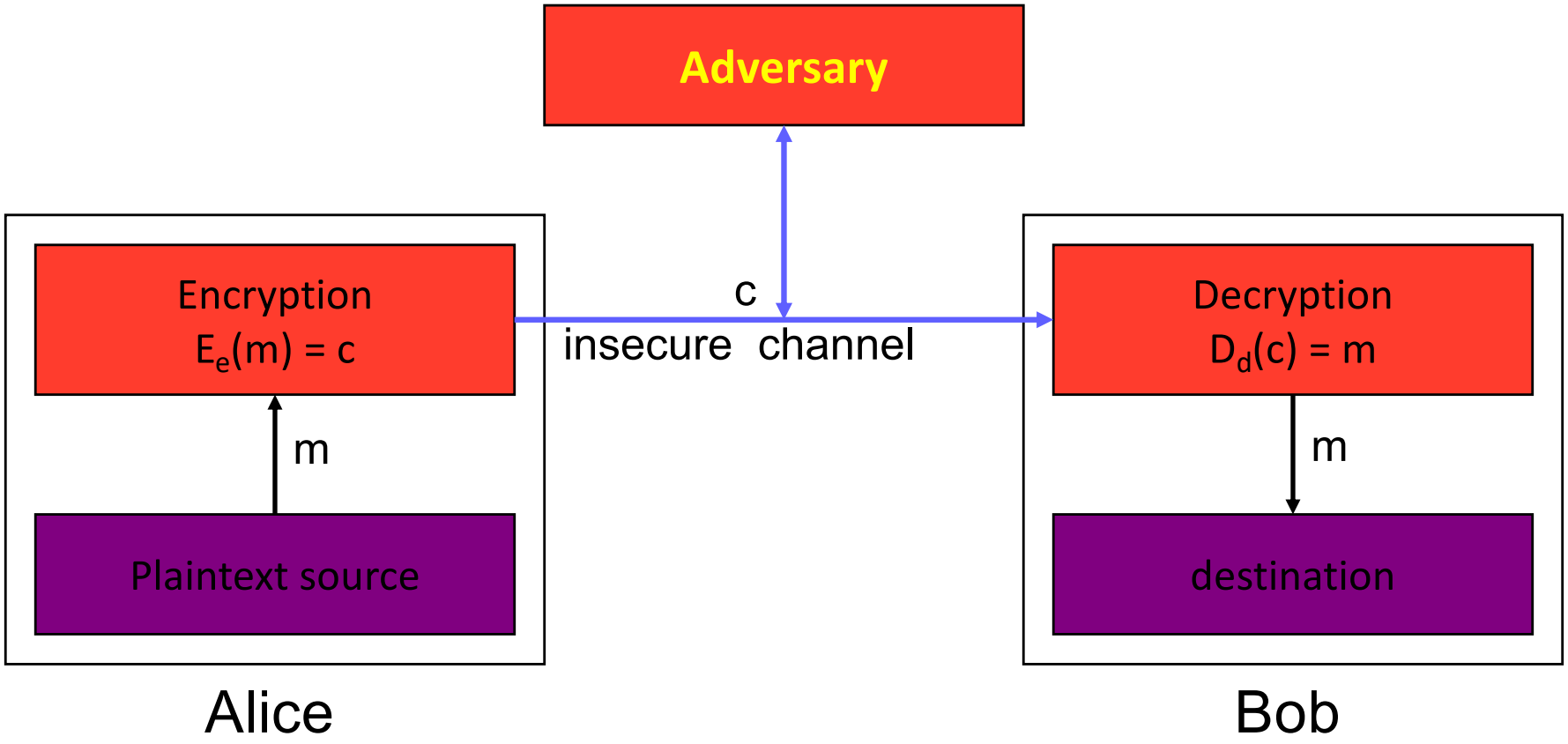

Modification: Integrity
Source
Destination


Fabrication: Authenticity
Source
Destination

Taxonomy of Attacks

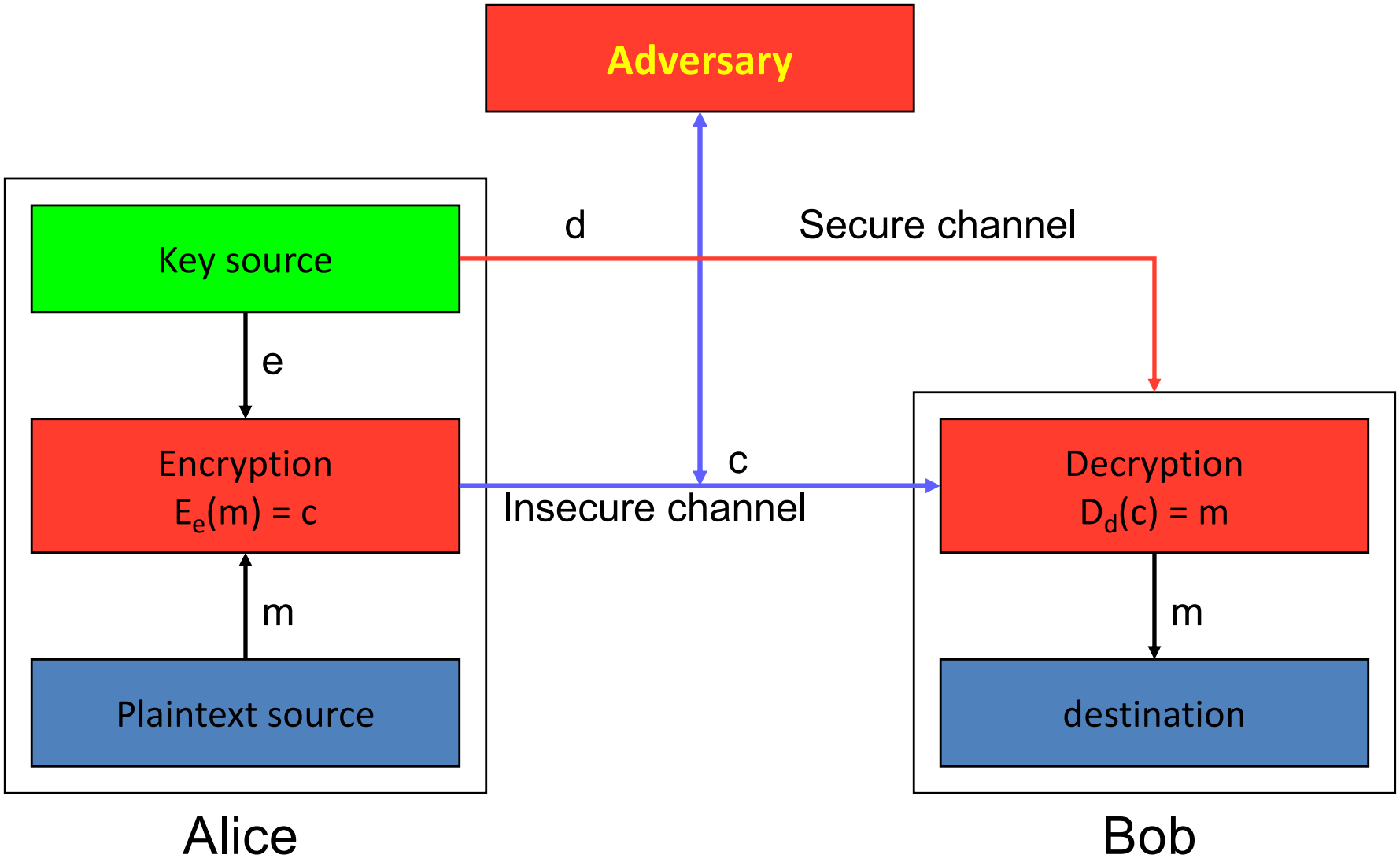
- Passive attacks
  - Eavesdropping
  - Traffic analysis
- Active attacks
  - Masquerade
  - Replay
  - Modification of message content
  - Denial of service

Encryption

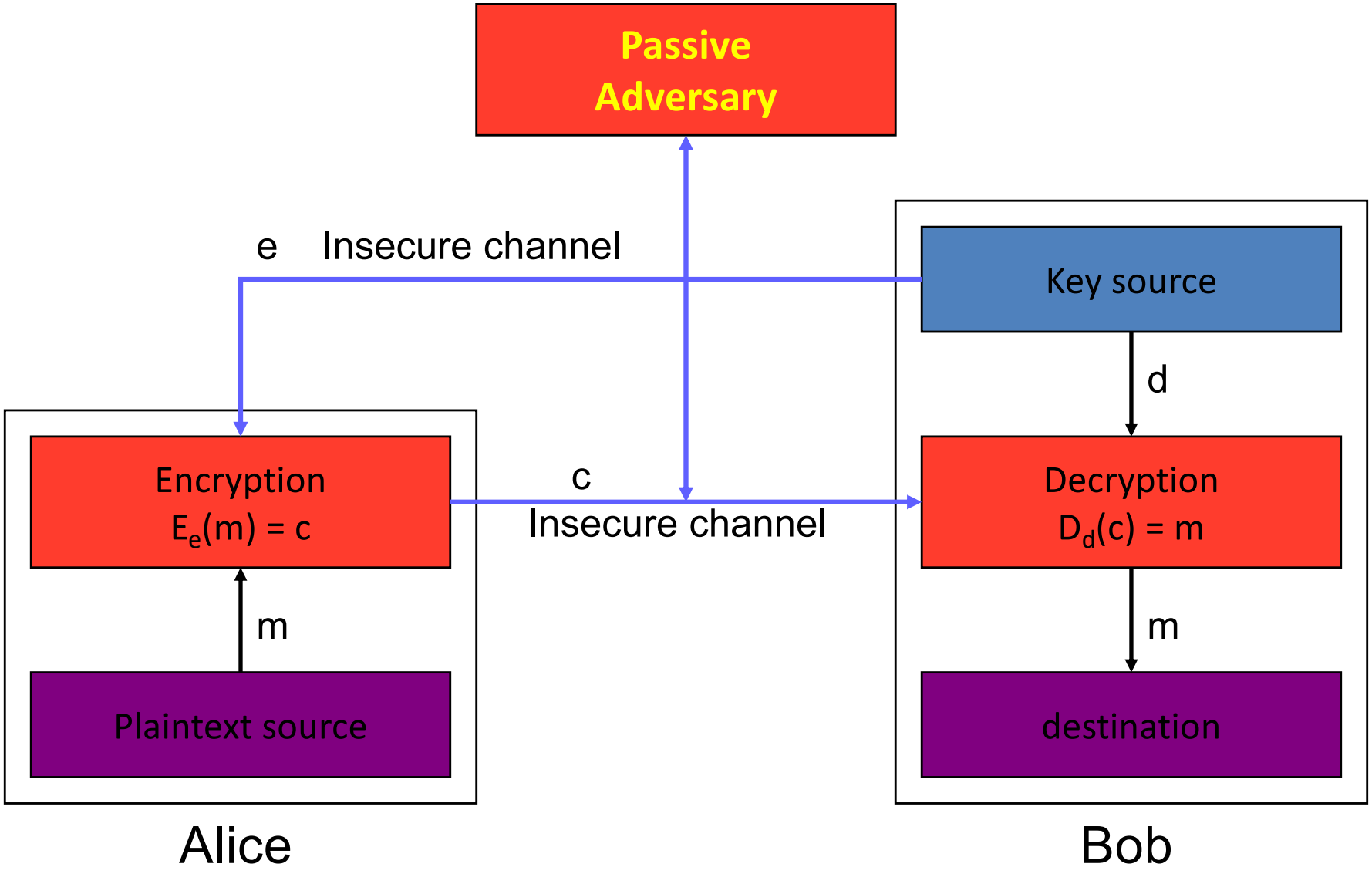


- Why do we use key?
  - Or why not use just a shared encryption function?

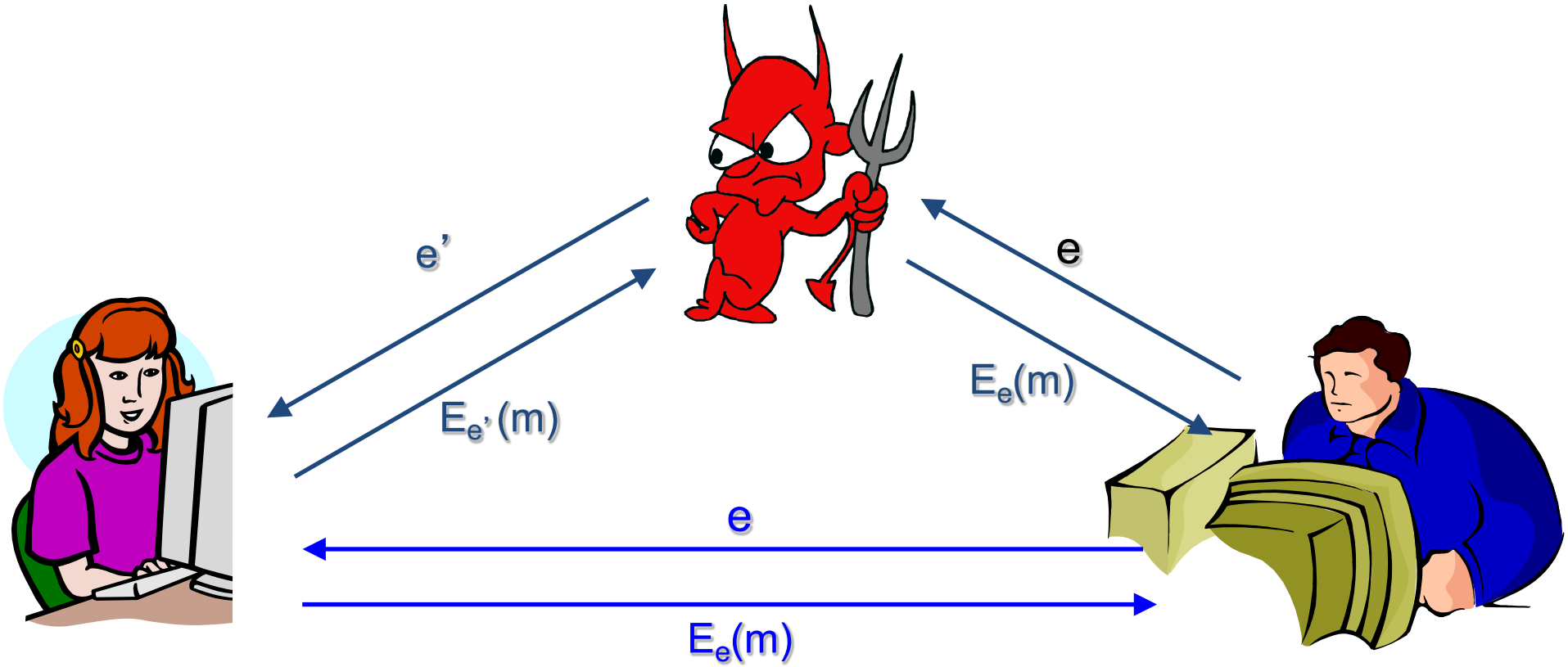
SKE with Secure channel



PKE with Insecure Channel



Public Key should be authentic!



Hash Function

- A hash function is a function h satisfying
  - $h:\{0, 1\}^* \rightarrow \{0, 1\}^k$ (Compression)
- A cryptographic hash function is a hash function satisfying
  - It is easy to compute y=h(x) (ease of computation)
  - For a given y, it is hard to find x' such that h(x')=y. (onewayness)
  - It is hard to find x and x' such that h(x)=h(x') (collision resistance)
- Examples: SHA-1, MD-5

Questions?

- Yongdae Kim
  - email: yongdaek@kaist.ac.kr
  - Home: http://syssec.kaist.ac.kr/~yongdaek
  - Facebook: https://www.facebook.com/y0ngdaek
  - Twitter: https://twitter.com/yongdaek
  - Google "Yongdae Kim"