Security I: Introduction & Threat Model

Suman Jana

Columbia University

*some slides are borrowed from Vitaly Shmatikov and Ari Juels

1

Course goals

- Understand the fundamental principles of security
  - What are the common security mechanisms? Why they often go wrong?
  - What are the underlying principles behind building secure systems?
  - Why building secure systems is hard?

Logistics

- No text book but assigned readings from different sources

- Grading
  - Three programming assignments in C/C++ (60%)
  - Midterm (20%)
  - Non-cumulative final (20%)

- Class webpage:
  http://sumanj.info/security_1_2021.html

The art of adversarial thinking

What's adversarial thinking?

"Security requires a particular mindset. Security professionals -- at least the good ones -- see the world differently. They can't walk into a store without noticing how they might shoplift. They can't use a computer without wondering about the security vulnerabilities. They can't vote without trying to figure out how to vote twice. They just can't help it."

- Bruce Schneier

Adversarial thinking disclaimer

Hopefully, you will learn to think like a criminal mastermind but behave like a gentleman/woman!

Adversarial thinking: key questions

- Security goal: what security policy to enforce?

- Threat model: who is the adversary? What actions can the adversary perform?

- Mechanisms: What security mechanisms can be used to achieve the security goals given the adversarial model

Key security goals

- Confidentiality: Data not leaked

- Integrity: Data not modified

- Availability: Data is accessible when needed

- Authenticity: Data origin cannot be spoofed

You can apply adversarial thinking anywhere

- Columbia ID cards
  - Can you fake an ID card?
- ATM machine
  - How does the service person gets access to refill it with cash?
- MTA metrocard
  - Can you increase the card balance without paying?

Example: air travel

Print boarding pass at home

ID check by TSA

Boarding pass check at the gate

Adversarial thinking example: air travel

- Security goal: Ensure that each person getting inside an airport has a valid boarding pass and is authorized to fly (i.e., not on the no-fly list)
- Mechanisms
  - TSA checks validity of the ID (e.g., driver's license) and the boarding pass   How?
  - TSA matches name in the ID against the name in the boarding pass
  - TSA ensures that the name is not on the no-fly list
  - Gate agent checks whether the boarding pass is valid and has been checked by TSA   How?

Can an attacker who is on the no-fly list fly?

What is the threat model?

- Can an attacker create a fake boarding pass?

- Can an attacker fake a driver's license?

13

Security under different threat models

- Security goal: Ensure that each person getting inside an airport has a valid boarding pass and is authorized to fly (i.e., not on the no-fly list)

  - What are the minimum requirements for someone to violate this goal in the current TSA system?

  - The current TSA system is secure under which threat models?

Not all threat models are equal

- Which one is harder and why?
  - Creating a fake boarding pass
  - Creating a fake driver's license

Security measures in a driver's license?

Security measures in a boarding pass?

Can the barcode be faked?

Air travel revisited: a different security goal

Print boarding pass at home

ID check by TSA

Boarding pass check at the gate

Security goal: everybody boarding an aircraft must pass through TSA security check

Everybody must go through TSA checks

- How does the current TSA system ensure this?

- What is an example threat model where this goal can be violated by an attacker?

Yet another security goal

- Only authorized travelers should be allowed to enter premium lounges
  - How will the receptionist at the lounge know who is authorized?

What is the threat model for this attack?

ANDY GREENBERG   SECURITY   08.05.16   10:47 AM

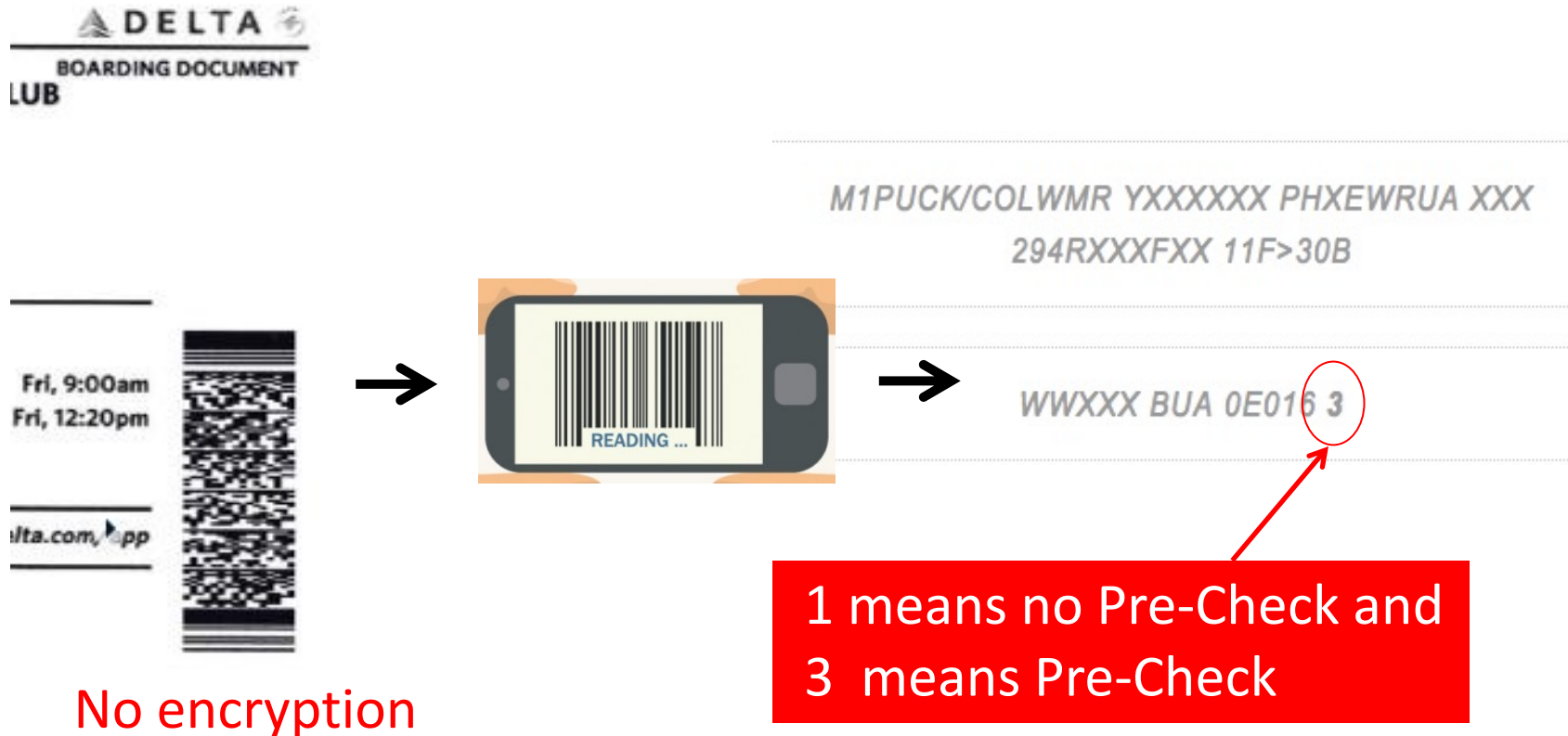# FAKE BOARDING PASS APP GETS HACKER INTO FANCY AIRLINE LOUNGES

As the head of Poland's Computer Emergency Response Team, Przemek Jaroszewski flies 50 to 80 times a year, and so has become something of a connoisseur of airlines' premium status lounges. (He's a particular fan of the Turkish Airlines lounge in

How will you fix it?

What about TSA Pre-Check?

- How does TSA Pre-Check work?
  - Passengers apply for Pre-Check
  - TSA decide whether the passenger is eligible for Pre-Check or not and sends the information back to the Airline.
  - The Airline encodes that information in a barcode that is on the issued boarding pass.
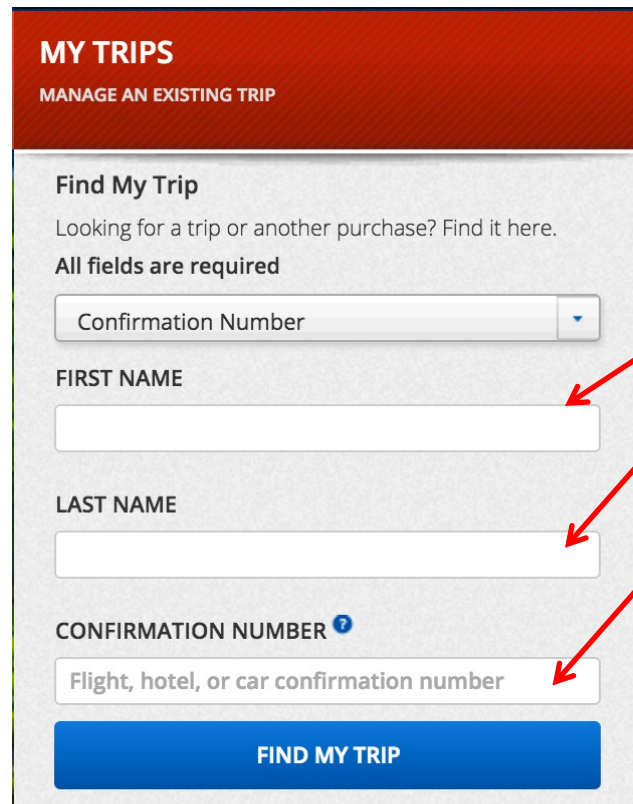
Hacking TSA Pre-Check

DELTA
BOARDING DOCUMENT
LUB

Fri, 9:00am
Fri, 12:20pm

elta.com/app

No encryption

M1PUCK/COLWMR YXXXXXX PHXEWRUA XXX
294RXXXFXX 11F>30B

WWXXX BUA 0E016 3

1 means no Pre-Check and 3 means Pre-Check

Unintended side-effects of the boarding-pass design

- What happens if someone else gets hold of your boarding pass?

MY TRIPS
MANAGE AN EXISTING TRIP

Find My Trip
Looking for a trip or another purchase? Find it here.
All fields are required

Confirmation Number

FIRST NAME

LAST NAME

CONFIRMATION NUMBER ?
Flight, hotel, or car confirmation number

FIND MY TRIP

All this information is in the boarding pass in cleartext

A different setting: money

- Counting tokens must be kept in a safe place to prevent tampering
  - In a temple or in clay envelopes on shipping routes
- How to make counting tokens completely portable for trade?

A different setting: money

- Security goals
  - Tokens can only be created by a trusted authority
  - Authenticity of tokens should be easily verifiable by anyone
- Threat model
  - Attackers can forge or modify tokens
- Clay tokens can be easily forged!

A different setting: money

- Coins were introduced around 6/7th century BCE
  - Make tokens out of scarce resources(gold and silvers)
  - Apply a signature that is hard to copy (depends on the skills of the engravers)
  - Harsh penalty for forgers

Modern crypto-currencies

- Same principles!
  - Scarce resource: computation
  - Hard-to-forge data: cryptography

Who is the adversary?
depends on who you are

Hackers

- Evgeniy Mikhailovich Bogachev
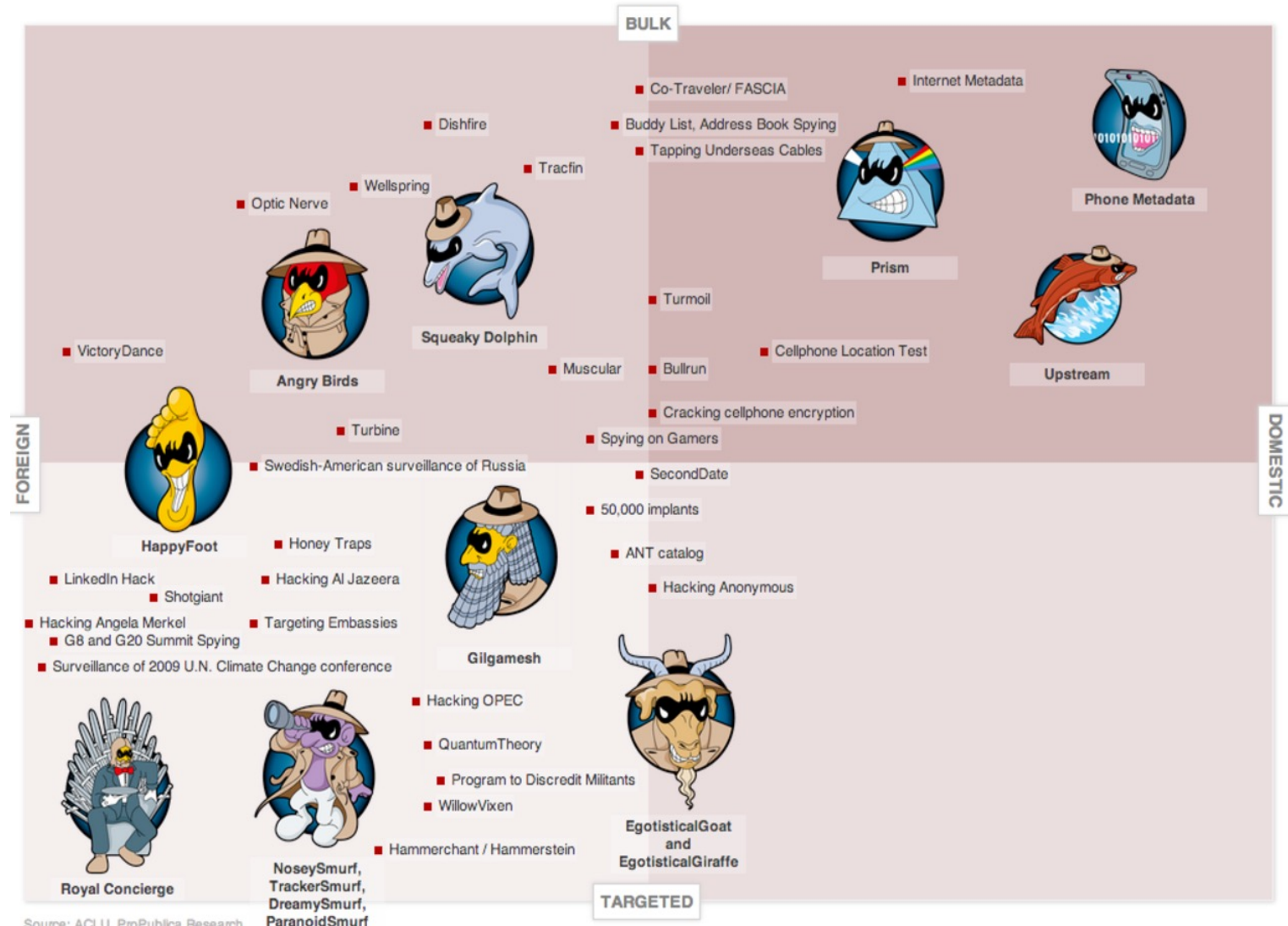 - Gameover Zeus botnet: banking fraud and ransomware distribution

Chinese government

- Censorship of materials critical to the current regime
- Monitoring dissidents

National Security Agency (NSA)

Source: ACLU, ProPublica Research