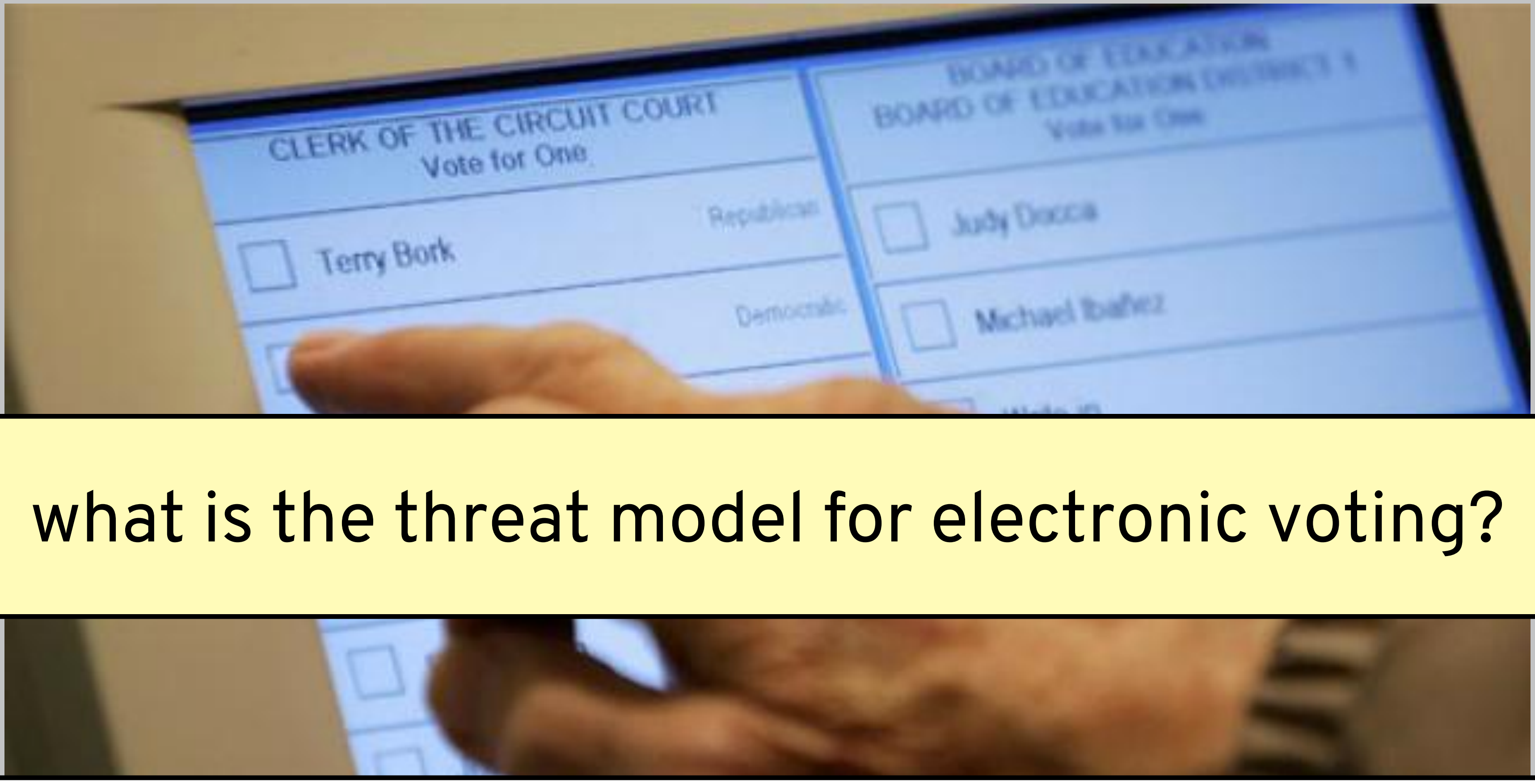
SECURITY (COMP0141): EXAMPLE THREAT MODELLING

EXAMPLE: ELECTRONIC VOTING



what is the threat model for electronic voting?

Pac-Man installed on voting machine without breaking tamper seals

ELECTRONIC VOTING: THREATS

Threats (who is the adversary?)

Capabilities?

Motivation?

ELECTRONIC VOTING: THREATS

Threats (who is the adversary?)

Capabilities?

Voter(s)

Election official

Manufacturer of EVM

Software engineer

Cleaner

Motivation?

ELECTRONIC VOTING: THREATS

Threats (who is the adversary?)

Capabilities?

Voter(s)

Election official

Manufacturer of EVM

Software engineer

Cleaner

Motivation?

Vote as someone else (S)

Rig the election (T)

Learn someone’s vote (I)

Prevent others from voting (D)

ELECTRONIC VOTING: VULNERABILITIES

Vulnerabilities (where can system break?)

Capabilities?

Voter(s)

Election official

Manufacturer of EVM

Software engineer

Cleaner

ELECTRONIC VOTING: VULNERABILITIES

Vulnerabilities (where can system break?)

Capabilities?

Voter(s)

Election official

Manufacturer of EVM

Software engineer

Cleaner

Vulnerabilities

Weak cryptography/design

Software/hardware defects

Hardware defects

Software defects

Machine access before/after election

ELECTRONIC VOTING: LIKELIHOOD

Likelihood (might this happen?)

Motivation	Capabilities	Vulnerabilities

ELECTRONIC VOTING: LIKELIHOOD

Likelihood (might this happen?)

Motivation	Capabilities	Vulnerabilities
Rig the election yes!	Manufacturer of EVM Janitor	Hardware defects Access to machines
Vote as someone yes!	Voter Software engineer	Weak cryptography
Rig the election no!	Election official	Hardware defects

ELECTRONIC VOTING: IMPACT

Impact (what if bad things happen?)

Motivation?

Vote as someone else (S)

Rig the election (T)

Learn someone’s vote (I)

Prevent others from voting (D)

ELECTRONIC VOTING: IMPACT

Impact (what if bad things happen?)

Scale	Motivation?
Small group	Vote as someone else (S)
Huge!	Rig the election (T)
Small to large group	Learn someone's vote (I)
Small to large group	Prevent others from voting (D)

ELECTRONIC VOTING: PROTECTION

Protection (what does it cost?)

Vulnerabilities

Weak cryptography/design

Software/hardware defects

Hardware defects

Software defects

Machine access before/after election

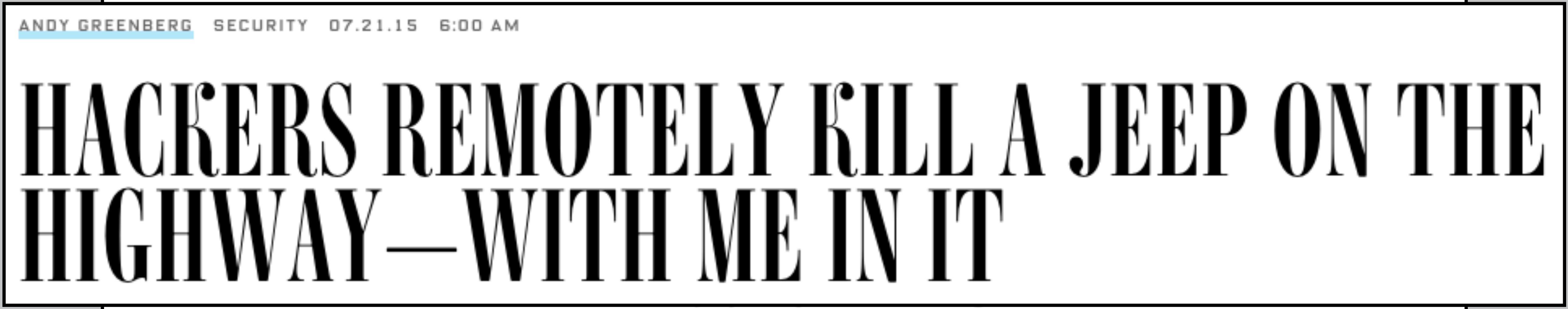
ELECTRONIC VOTING: PROTECTION

Protection (what does it cost?)

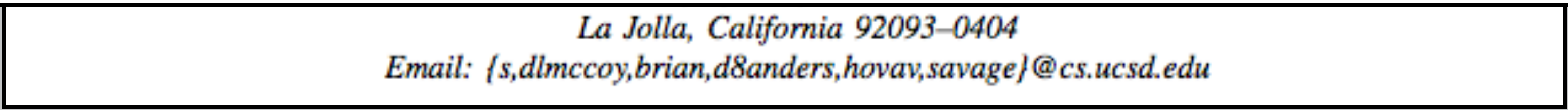
Cost	Vulnerabilities
Expensive (binary)	Weak cryptography/design
Cheap - expensive	Software/hardware defects
Expensive	Hardware defects
Cheap - expensive	Software defects
Cheap (risk management)	Machine access before/after election

EXAMPLE: HACKING CARS

what is the threat model for driving a car?


ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT


La Jolla, California 92093–0404
Email: {s,dlmccoy,brian,d8anders,hovav,savage}@cs.ucsd.edu

DRIVING A CAR: THREATS

Threats (who is the adversary?)

Capabilities?

Passenger(s)

Manufacturer

Hacker

Other driver(s)

???

Motivation?

Crash the car! (T)

DRIVING A CAR: VULNERABILITIES

Vulnerabilities (where can system break?)

Capabilities?

Passenger(s)

Manufacturer

Hacker

Other driver(s)

???

Vulnerabilities

DRIVING A CAR: LIKELIHOOD

Likelihood (might this happen?)

Motivation	Capabilities	Vulnerabilities

DRIVING A CAR: IMPACT

Impact (what if bad things happen?)

Scale

Motivation?

Crash the car! (T)

DRIVING A CAR: PROTECTION

Protection (what does it cost?)

Cost

Vulnerabilities