SECURITY (COMP0141): LAST WEEK → THIS WEEK

SECURITY DESIGN

define

How to ~~design~~ a secure system?

SECURITY DESIGN

define

How to ~~design~~ a secure system?

one that meets a specific security policy

How to define a security policy?

WHAT SHOULD POLICY ADDRESS?

Threats (who is the adversary?)

WHAT SHOULD POLICY ADDRESS?

Threats

Vulnerabilities (where can system break?)

WHAT SHOULD POLICY ADDRESS?

Threats

Vulnerabilities

Likelihood (might this happen?)

WHAT SHOULD POLICY ADDRESS?

Threats

Vulnerabilities

Likelihood

Impact (what if bad things happen?)

WHAT SHOULD POLICY ADDRESS?

Threats

Vulnerabilities

Likelihood

Impact

Protection (what does it cost?)

SECURITY DESIGN

define

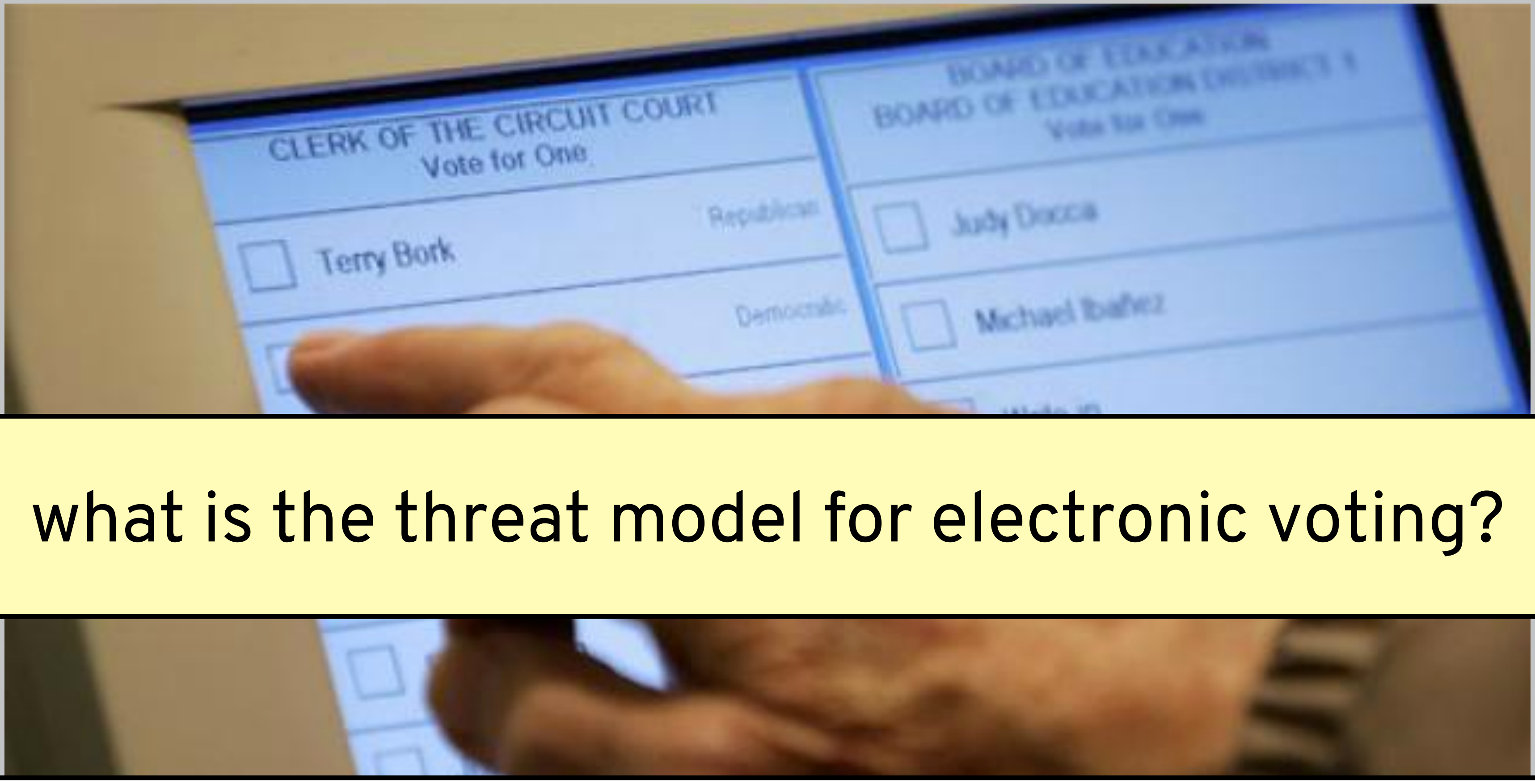
How to ~~design~~ a secure system?

one that meets a specific security policy

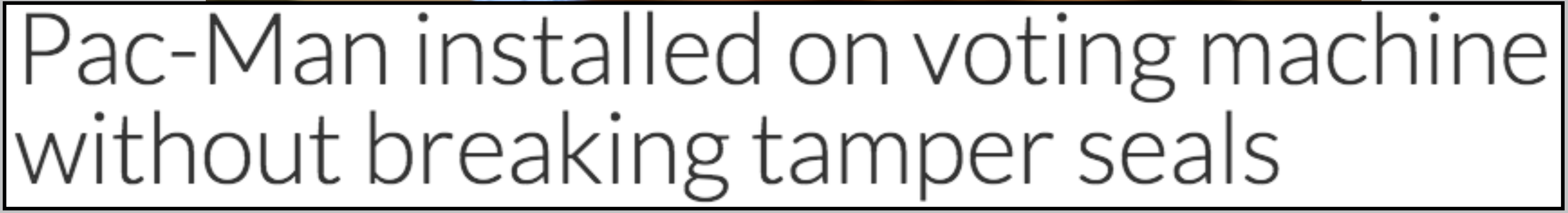
How to define a security policy?

threats, vulnerabilities, likelihood, impact, and cost used to create a **threat model**

EXAMPLE: ELECTRONIC VOTING

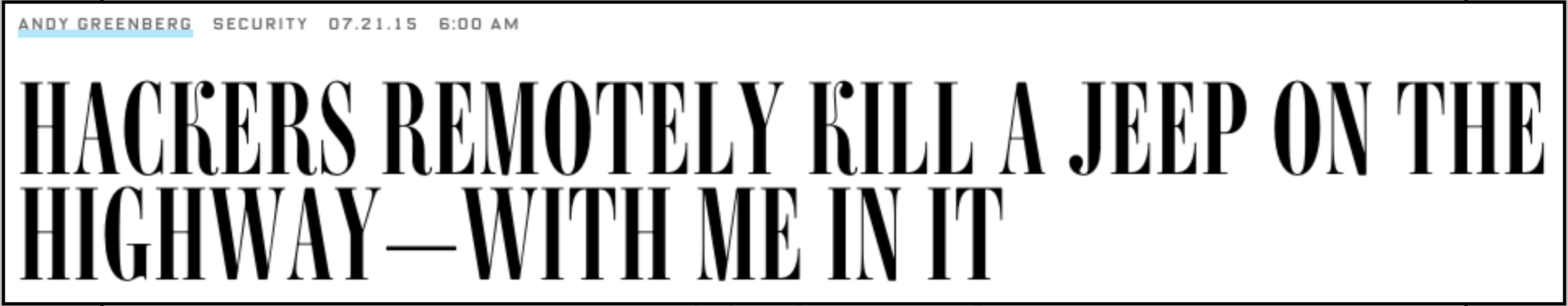


what is the threat model for electronic voting?


Pac-Man installed on voting machine without breaking tamper seals

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