Nicolas Christin
nicolasc@cmu.edu

Usable Privacy and Security

Security, privacy and behavioral biases

Motivation: Security analysis

- Who/What is the target?
- What are the desired security properties?
- **Understand defenders resources**
  - **Economic, technological, behavioral**

- Who are the adversaries?
  - Identify attackers
  - Probability of attack (risk assessment) and damages
- **Estimate attackers resources**
  - **Economic, technological, behavioral**

Research question

How can we better model attackers and defenders?

- Defenders *have been* assumed knowledgeable, interested in security, and altruistic
  - But in practice, generally self-interested
  - Rarely fully informed
  - Not even really rational: behavioral biases
- Attackers *have been* assumed omnipotent
  - But in practice very often financially motivated
  - Tend to be economically rational
  - May not lead us to devise effective defenses (see Anderson, 1993)
- Economics can tell us which intervention strategies most likely to succeed…
  - **… but for that we need sound economic models of all parties' behavior…**

This lecture's agenda

- Outline
  - Motivation
    - Why security economics?
    - Why selfishness?
  - Discussion
    - Limitations of classical game theory
    - Further challenges in security and privacy
- Objective
  - Learn techniques to model externalities
  - Learn how economics-inspired techniques can help discover incentive misalignment
  - Get an exposure to behavioral economics

Trivial observation 1

- Why are security-compromising and privacy-invasive technologies abundant?
  - Examples: Spyware, Malware, Targeted Advertisment, Phishing…
  - Answer: Financial incentives
  - Historical perspective is different

Trivial observation 2

- Why and how should users protect?
  - Examples of protective measures: PETs, security software, different behaviors online and offline (i.e., use shredders, use curtains)
  - Motivation: Financial and other incentives (e.g., feeling of safety)

Homo economicus

- Assuming a rational, self-interested agent
  - Rational: Individuals are able to estimate the benefits and costs of a particular action (i.e., are able to estimate the net benefit)
  - Self-interested: Agents engage in an activity if the benefit is greater than or equal to the cost (i.e., the net benefit is greater than or equal to zero)

"It is not from the benevolence of the butcher, the brewer, or the baker that we expect our dinner, but from their regard to their own interest." (Adam Smith, The Wealth of Nations, 1776)

Network effects and externalities

- Terms often used interchangeably
  - Effects: Benefit, or cost, that an agent derives from a good when the number of other agents consuming the same kind of good changes
  - Externality: Participants in the market fail to internalize these effects
- Relationship to public goods
  - An externality occurs when a decision causes costs or benefits to third party stakeholders, often, although not necessarily, from the use of a public good
  - E.g., is identifying information and shopping data a public good?

Networking, security and economics

- Problem well known in economics and game theory

Economics	Networks	Security
Rational players competing in a market	Selfish nodes competing for network resources	Selfish agents whose security impacts others

- Can use game theory as a tool
  - to determine likely user (nodes) strategies given the context (network topology, network protocols, policies)
  - to design mechanisms (network topology, protocols, policies) which yield desirable strategies

Toward building a model

- Model can be mathematical, or merely describe dependencies or behaviors etc.
- Defining models is a process
  - Getting ideas
  - Evaluate usefulness of ideas
  - Work out examples
  - Generalize and simplify: Distill essence of phenomenon under investigation
  - Study literature

Game-theoretic model overview

- Set of players in a network
- Utility function: value each player extracts from the network
  - Given by a cost model
- Strategies: Actions each player can take
- Equilibrium concept: situation where all players are content with their utility and don't change their strategy

Important equilibria concepts

- **Social optimum**: set of strategies that maximizes total $U = \sum_{i=1}^{N} U_i$ network utility
  - Ideal configuration for the community
  - What a benevolent government would want
- **Nash equilibrium**: set of strategies in which no individual player can increase their individual utility U_i by changing their strategy
  - Selfish equilibrium
  - Best response to others' actions

Limitations in a security context

- Asymmetric games: attackers vs. targets
  - Different motivations, utility functions…
- Incomplete information: Are parameters of model known to agents?
  - Can attackers infer defense posture?
  - Can defenders predict likelihood of attack?
- Information asymmetry: Does one party know more about parameters of interaction?
  - Lemons market: Are security products of high or low quality?

Rationality in practice

- Can researchers formulate a complete model?
- Can consumers act according to model?

Free Giveaway!

Name: _____

Address: _____

City: _____ State: _____ Zip: _____

Home Phone: _____

Work Phone: _____

❑ Single ❑ Married

Age: _____ Occupation: _____

Spouses Age: _____ Occupation: _____

Combined Income:

❑ Under $30,000 ❑ Over $30,000 ❑ Over $50,000

DO YOU: ❑ RENT OR ❑ OWN YOUR HOME?

❑ VISA ❑ MASTERCARD ❑ AMERICAN EXPRESS

Would you like info on special events & promotions at Pier 39?

❑ Yes ❑ No

E-mail address: _____

Details of Participation and Eligibility Requirements

- Only one Entry per Family.
- Winner allows the use of his or her name, photo, and statements for future promotional use without further compensation.
- Winner must be 18 or over. I.D. required. Winner must provide all necessary federal and state tax reporting information before receiving prizes.
- Drawing held February 23, 2003. Last date to enter drawing is February 16, 2003.
- Winner need not be present to win. Winner will be notified by phone.
- Drawing will be conducted by a Certified Public Accounting Firm at the corporate office of Grand Pacific Resorts, 5900 Pasteur Ct., #200, Carlsbad, CA 92008. To request winner information, correspondence may be forwarded to Grand Pacific Resorts, Promotions Dept. P.O. Box 4068, Carlsbad, CA 92018.
- All local, state, and federal taxes, fees and licenses are the winner's responsibility. Acceptance of the prizes constitutes a release of Facility Management, it's agents and employees from all responsibility to the winner.
- Odds are based on number of entries received, approximately 1 in 700,000.
- No purchase or attendance is necessary to be entered into the drawing. Entrants may be invited to attend a sales presentation about the Red Wolf Lodge at Squaw Valley.
- Entries become the property of PNR Marketing Inc.
- The annual "Grand Prize" Giveaway consists of any vehicle with a retail value not to exceed $25,000 or a three year lease (value to $25,000) on a luxury car; or any prize (or similar) displayed in a Grand Pacific Resorts Promotion February 25, 2002 - February 23, 2003 (valued up to $15,000), or the winner may choose cash in the amount of $15,000.

What can the individual infer?

- Benefits:
  - Non-monetary benefit (e.g., excitement of participation)
  - Expected monetary benefit:
    - *1/700000 * $15000 = 2 cent*
- Costs:
  - Promotions, unsolicited mailing, sales contacts (cannot exclude further use and consequences)
  - Expected monetary cost:
    - *?*
- *What behavioral variables are missing?*

Psychological biases

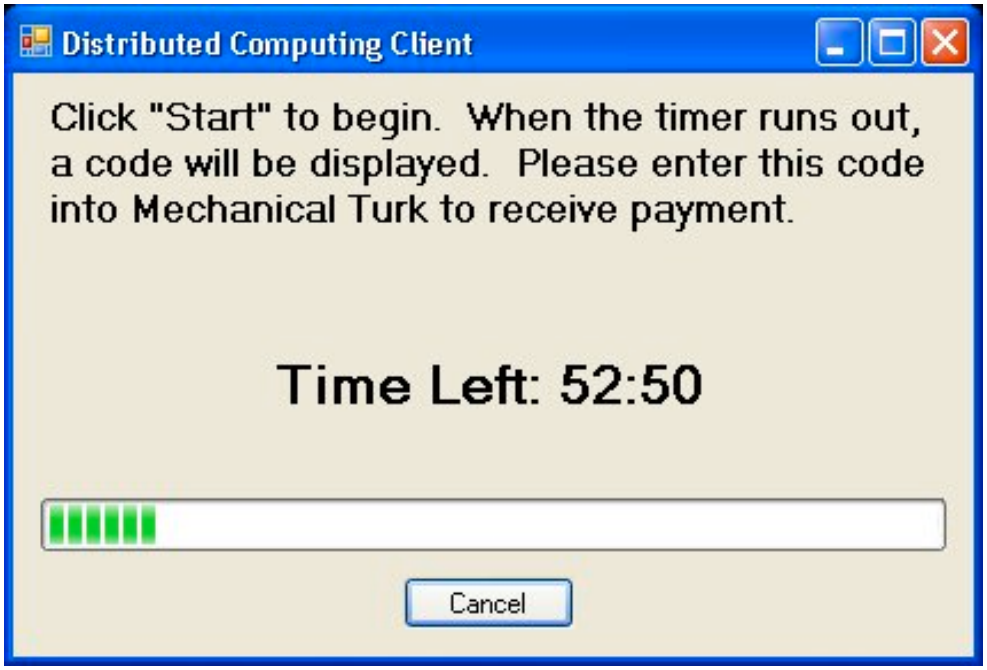
- We react differently depending on framing of messages
- We make time-inconsistent decisions
- We seek immediate gratification
- We are susceptible to strong biases with ambiguous and unknown information

Paying people to install malware
[Christin, Egelman, Vidas, Grossklags, FC 2011]

- We paid people to download and run an unknown executable
- Payment was increased every week
  - Log scale
  - $0.01/$0.05/$0.10/$0.50/$1.00
- Mechanical Turk as experimental platform
  - Measured views vs. downloads vs. runs

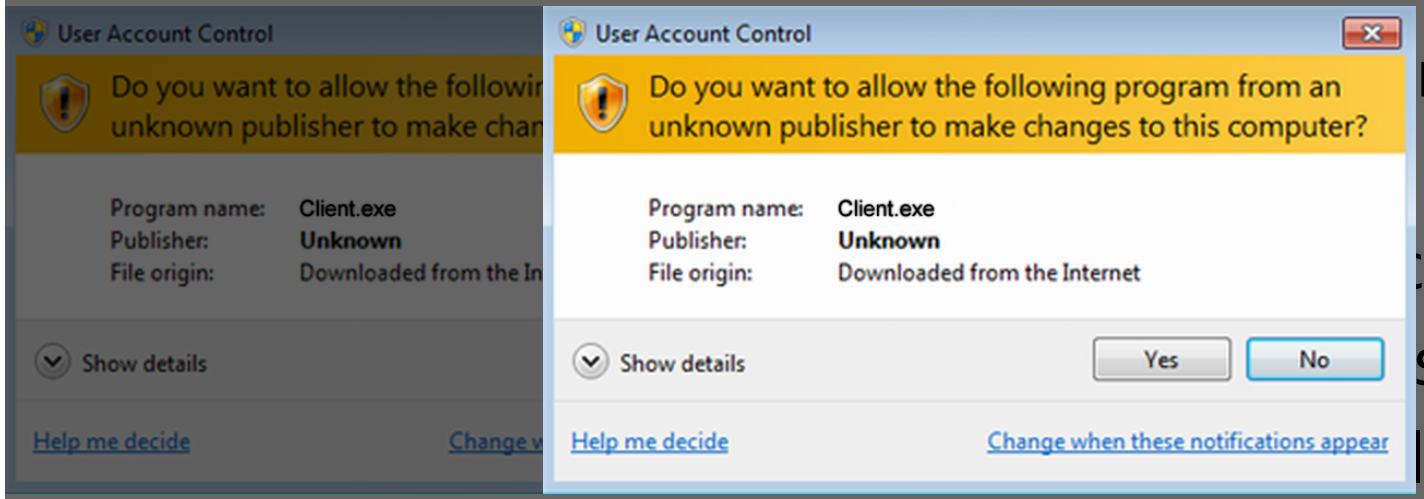
Experimental environment

- CMU Distributed Computing Project
  - No such project exists
  - All code was hosted on a third-party domain
  - No connection to us or our institutions



Experimental Environment

- Are current mitigations effective?



mpt for 50% data:

ontrol

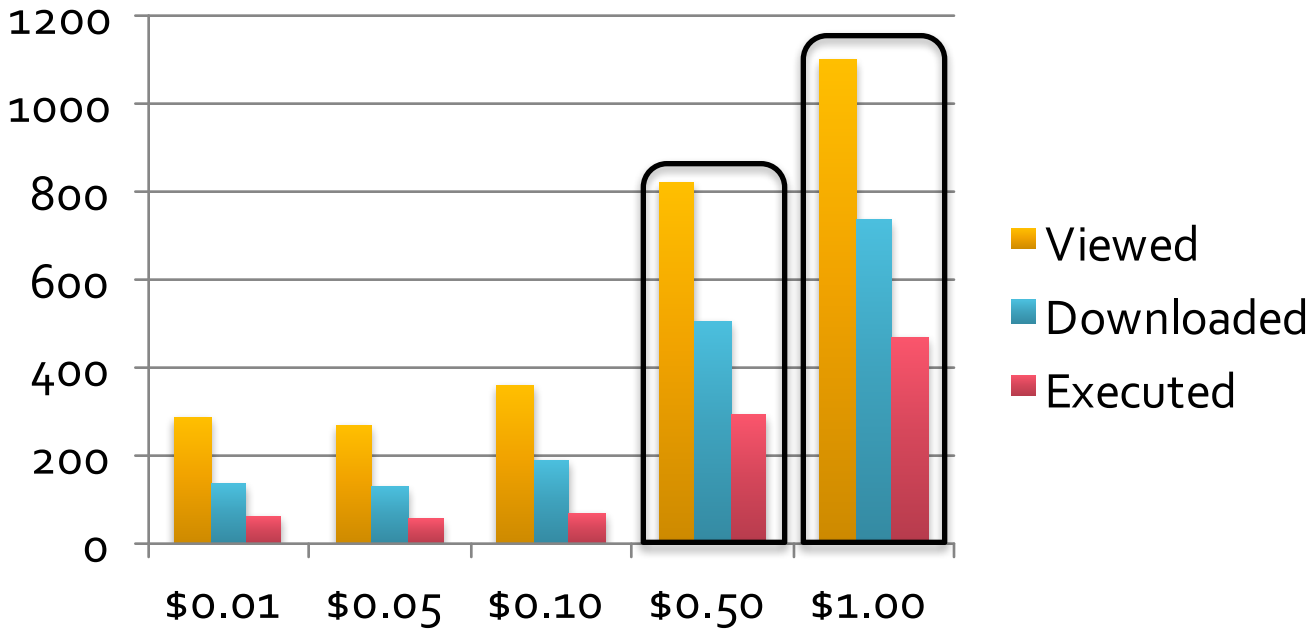
s version

list

  - VM detection
- Displayed payment code
- Sent an exit survey

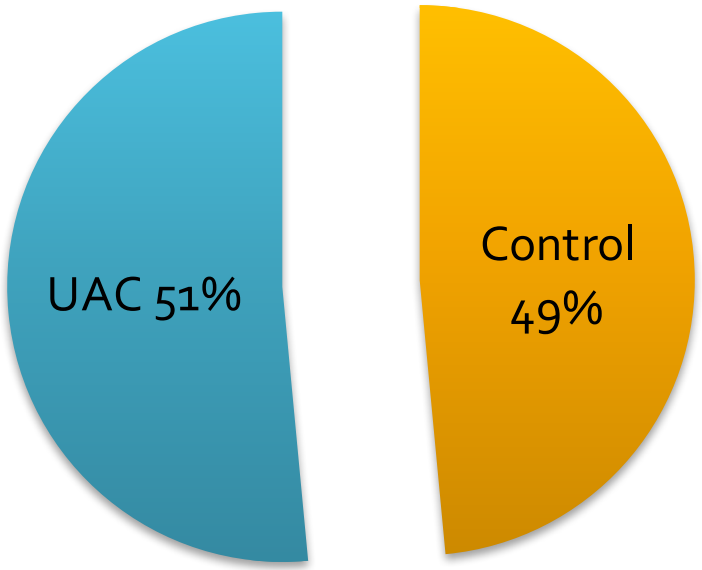
Results

	$0.01		$0.05		$0.10		$0.50		$1.00	
Viewed	291		272		363		823		1,105	
Downloaded	141	49%	135	50%	190	52%	**510**	**62%**	**738**	**67%**
Executed	64	22%	60	22%	73	20%	**294**	**36%**	**474**	**43%**



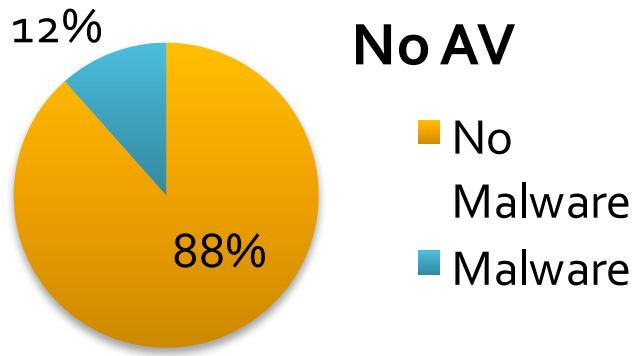
UAC Was ineffective

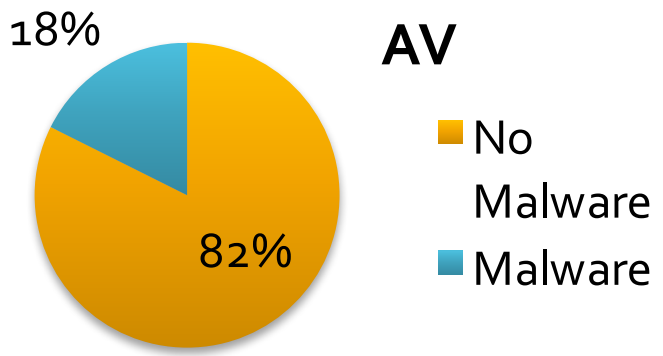
- 501 users had either Vista or Windows 7
- Conditions randomly assigned
  - $X^2_1=0.449$, $p<0.503$



Security behaviors

- 17 participants used a VM (1.8% of 965)
- We categorized 3,110 unique processes
  - 16.4% had malware
  - 79.4% had security software
  - Correlation between malware/security software
    - $\Phi=0.066,\ p<0.039$





Price and behavior

- Significant increase in patched software as payment increased:
  - $0.50-$1.00: 69.3%
  - $0.01-$0.10: 54.3%
- Cheating (invalid codes) decreased significantly as payment increased:
  - $1.00: 14.8%
  - $0.01: 46.5%
- Correlation between payment and run time:
  - $r=0.210$, $p<0.0005$

Validating behaviors

- Exit survey for a $0.50 bonus payment
- 513 people responded
  - 40% from India
  - 30% from US/Canada
  - Percentage from the developed world increased with price, 9.4% to 23.4%

Unpatched systems explained

- Significant correlation between developing world and unpatched systems
  - $\Phi = 0.241$, $p < 0.0005$
  - Windows Genuine Advantage?
- This does not explain security software
  - Not correlated with demographics or price

Security perceptions

- Danger of running code from MTurk on a 5-point scale
  - $F_{4,508} = 3.165$, $p < 0.014$
  - People who *should* have known better participated once the price was right
- 70% of participants knew it was dangerous to download unknown programs
  - All of them did so anyway

What is rational?

- Peltzman effect
  - Availability of seatbelts leads to more risky driving
- Same effect observed here
  - Installation of security software does not limit risky behaviors, far from it!

In their own words

- *It's a virus carrying HIT that I runned in to my lap top corrupted all my datas and suffered* [sic]
- *Do you think it is safe to run?*
  - *Yeah, a few of us ran it last time and had no complaints. Pretty sure it's just a port scanner.*
- *FYI I just got paid today for the shady looking software one…he's good people.*

Take away slide

- Modeling rational choice extremely valuable
  - Important conclusions about market processes and behavior of economic agents
  - Identification of incentive misalignment
- Careful investigation into characteristics of situation necessary
  - E.g., incommensurate resources
- Models can include aspects of limited rationality
  - E.g., near-rational agents
- Behavioral biases can and should be tested through experimentation