Security & Trust III — Part 1: Introduction

Peter-Michael Seidel

Fall 2018
Outline

Announcements

Motivation

Examples

Ideas
Outline

Announcements

Motivation

Examples

Ideas
Contact

- Peter-Michael Seidel
- email: pseidel@hawaii.edu
- office: POST 312B
- office hours: W 1030-1130 or email appointment
Course on the web

- slides and notes: asecolab.org and laulima
- homeworks and solutions: laulima
Books


What do you expect from the course?
Outline

Announcements

Motivation

Examples

Ideas
Question

Why study Security and Economics together?
Question

Is this a security problem or an economic problem?
Question

Whose problem is harder?
The troubles

- It is a trouble to not have.
- It is a trouble to have.
Security is the problem of having

J.K. Gallbraith:

- The poor man has always a precise view of his problem: he hasn’t enough and he needs more.

- The rich man [has] a much greater variety of ills and he [is] correspondingly less certain of their remedy.
Outline

Announcements

Motivation

Examples

Early security protocol

Security in E-commerce

Digital Rights Management

Tragedy of the Commons

Securing free market

Monetizing information
Example 1: Early security protocol

About 6000 years ago, Kain’s son Bob built a secure vault
Example 1: Early security protocol

and stored his goods in it.
Example 1: Early security protocol

and stored his goods in it. When Alice wanted to go for a vacation
Example 1: Early security protocol

and stored his goods in it. When Alice wanted to go for a vacation, she stored her goods there too.
Example 1: Early security protocol

As a receipt for her deposit in Bob’s vault, Alice got a secure token in a clay envelope.

Figure: Louvre, Paris
Example 1: Early security protocol

As a receipt for her deposit in Bob’s vault, Alice got a secure token in a clay envelope.

Figure: Louvre, Paris

To take the sheep, Alice must give the token.
Example 1: Early security protocol

As a receipt for her deposit in Bob’s vault, Alice got a secure token in a clay envelope.

Figure: Louvre, Paris

- To take the sheep, Alice must give the token.
- To give the sheep, Bob must take the token.
Example 1: Early security protocol

As a receipt for her deposit in Bob’s vault, Alice got a secure token in a clay envelope.

Figure: Louvre, Paris

- To take the sheep, Alice must give the token.
- To give the sheep, Bob must take the token.
- Anyone who gives the token can take the sheep.
Example 1: Early security protocol

- This protocol goes back to Uruk (Irak), 4000 B.C.
Example 1: Early security protocol

- This protocol goes back to Uruk (Irak), 4000 B.C.
- *Money* developed from *security* tokens.
Example 1: Early security protocol

- This protocol goes back to Uruk (Irak), 4000 B.C.
- *Money* developed from *security* tokens.
- Numbers developed from security annotations.
- Writing developed later.
Example 2: Security in E-commerce

Security seals convey trust
Example 2: Security in E-commerce

Adverse selection

<table>
<thead>
<tr>
<th></th>
<th>TRUSTE-certified</th>
<th>uncertified</th>
</tr>
</thead>
<tbody>
<tr>
<td>honest</td>
<td>94.6%</td>
<td>97.5%</td>
</tr>
<tr>
<td>malicious</td>
<td>5.4%</td>
<td>2.5%</td>
</tr>
</tbody>
</table>

Table: Trustworthiness of TRUSTE [Edelman 2007]
Example 2: Security in E-commerce

Adverse selection

<table>
<thead>
<tr>
<th></th>
<th>Google</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>sponsored</td>
</tr>
<tr>
<td>top</td>
<td>4.44%</td>
</tr>
<tr>
<td>top 3</td>
<td>5.33%</td>
</tr>
<tr>
<td>top 10</td>
<td>5.89%</td>
</tr>
<tr>
<td>top 50</td>
<td>5.93%</td>
</tr>
</tbody>
</table>

Table: Malicious search engine placements [Edelman 2007]
Example 2: Security in E-commerce

Adverse selection

<table>
<thead>
<tr>
<th></th>
<th>sponsored</th>
<th>organic</th>
</tr>
</thead>
<tbody>
<tr>
<td>top</td>
<td>6.35%</td>
<td>0.00%</td>
</tr>
<tr>
<td>top 3</td>
<td>5.72%</td>
<td>0.35%</td>
</tr>
<tr>
<td>top 10</td>
<td>5.14%</td>
<td>1.47%</td>
</tr>
<tr>
<td>top 50</td>
<td>5.40%</td>
<td>1.55%</td>
</tr>
</tbody>
</table>

Table: Malicious search engine placements [Edelman 2007]
Example 2: Security in E-commerce

Adverse selection

<table>
<thead>
<tr>
<th>Ask</th>
<th>sponsored</th>
<th>organic</th>
</tr>
</thead>
<tbody>
<tr>
<td>top</td>
<td>7.99%</td>
<td>3.23%</td>
</tr>
<tr>
<td>top 3</td>
<td>7.99%</td>
<td>3.24%</td>
</tr>
<tr>
<td>top 10</td>
<td>8.31%</td>
<td>2.94%</td>
</tr>
<tr>
<td>top 50</td>
<td>8.20%</td>
<td>3.12%</td>
</tr>
</tbody>
</table>

Table: Malicious search engine placements [Edelman 2007]
Example 2: Security in E-commerce

Questions

- Why does adverse selection happen?
- How can it be avoided?
Example 2: Security in E-commerce

Questions

- Why does adverse selection happen?
- How can it be avoided?

Answers

- Reputation
- Trust
Example 3: Digital rights management (DRM)

Economic art history

- art used to be bound to the artist
  - music was available only from a musician
  - a story from a storyteller
  - a painting could only be seen in the cave, church...
Example 3: Digital rights management (DRM)

Economic art history

- mass reproduction bound art to copiable media
  - copying technologies led to copyright-based markets
  - artists could sell lots of books and records
- Copyright Management: branding, celebrities
Example 3: Digital rights management (DRM)

Economic art history

- digital networks freed art (science, religion...) from physical tokens (books, CDs...)
  - copying of digital content is essentially costless
  - Copyright Management becomes unviable
  - **Digital Rights Management**: seeks to
    - prevent (sandboxing...)
    - detect (watermarking...)
    - deter (lawyers...)

unauthorized copying of digital content
Example 3: Digital rights management (DRM)

Art economy as a security problem

In DRM, economics and security cannot be separated
Example 3: Digital rights management (DRM)

Art economy as a security problem

In DRM, economics and security cannot be separated:

- unauthorized copying of digital content cannot be prevented
Example 3: Digital rights management (DRM)

Art economy as a security problem

In DRM, economics and security cannot be separated:

- unauthorized copying of digital content cannot be prevented
- the cost and the risk of copying needs to be made greater than the price of the downloads
Example 3: Digital rights management (DRM)

OR should art be a common resource, like air, or the Internet?
Example 4: Tragedy of the Commons

Commons: publicly shared resources

For centuries, Alice, Bob and Charlie have been sharing an open field system.
Example 4: Tragedy of the Commons

Commons: publicly shared resources

For centuries, Alice, Bob and Charlie have been sharing an open field system.
Example 4: Tragedy of the Commons

Commons: publicly shared resources

In England, such open fields were called *Commons*.

Alice, Bob and Charlie alternated different crops with grazing, and maintained the land together.
Example 4: Tragedy of the Commons

Commons: publicly shared resources

In England, such open fields were called *Commons*.

Alice, Bob and Charlie alternated different crops with grazing, and maintained the land together.

Two remarkable social processes ensued:

- Tragedy of the Commons, and
- Enclosure Movement
Example 4: Tragedy of the Commons

Charlie realized that it was *rational* for him to invest
  - all effort into exploiting the public resource, and
  - no effort into maintaining it.

Charlie became a *free rider*.
Example 4: Tragedy of the Commons

- Charlie realized that it was *rational* for him to invest
  - all effort into exploiting the public resource, and
  - no effort into maintaining it.

  Charlie became a *free rider*.

- Alice and Bob realized that it was *rational* for them
  - to stop maintaining the resource for Charlie, and
  - to hurry to exploit the resource too.
Example 4: Tragedy of the Commons

- Charlie realized that it was *rational* for him to invest
  - all effort into exploiting the public resource, and
  - no effort into maintaining it.

  Charlie became a free rider.

- Alice and Bob realized that it was *rational* for them
  - to stop maintaining the resource for Charlie, and
  - to hurry to exploit the resource too.

- A race to the bottom ensued.
Example 4: Tragedy of the Commons

- Charlie realized that it was *rational* for him to invest
  - all effort into exploiting the public resource, and
  - no effort into maintaining it.

Charlie became a *free rider*.

- Alice and Bob realized that it was *rational* for them
  - to stop maintaining the resource for Charlie, and
  - to hurry to exploit the resource too.

- A *race to the bottom* ensued.

- The resource got depleted.
Example 4: Tragedy of the Commons

Common resources cause the race to the bottom.
Example 4: Tragedy of the Commons

Fair sharing of public resources is a security problem.
Example 4: Tragedy of the Commons

- the Internet is a common resource
- spam is an instance of the Tragedy of the Commons
- it is an economic & security problem
Example 4: Tragedy of the Commons

Solution: The Enclosure Movement

- Charlie *enclosed* the Commons from Alice and Bob.
- In England, this happened in XV–XVII centuries.
Example 4: Tragedy of the Commons

Market economy: private vice → public benefit

"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 self-interest. We address ourselves not to their humanity but to their self-love, and never talk to them of our own necessities, but of their advantages"

Adam Smith
Example 4: Tragedy of the Commons

Second Enclosure

Verizon: net neutrality violates our free speech rights
Company argues FCC regulations run afoul of Fifth Amendment property rights too.

by Timothy B. Lee - July 3 2012, 6:15pm CEST

"Can you hear me now?"
Aurich Lawson

Verizon pressed its argument against the Federal Communications Commission's new network.
Example 5: Free market protocol
Example 5: Free market protocol

Based on trust
Example 5: Free market protocol

supply -> demand
Example 5: Free market protocol

advertising

supply

demand
Example 5: Free market protocol
Example 5: Free market protocol
Example 5: Free market protocol

Based on influence
Example 5: Free market protocol

Information asymmetry: "Market of lemons"
Example 5: Free market protocol

Information asymmetry: "Financial derivative"
Example 5: Free market protocol

Upshot

- **security goal**: equilibrium of supply and demand
- **security protocol**: free exchange
- "*attacks above*": advertising, information asymmetry
  - security protocol correctly executed
  - security goal shifted
Example 6: Monetizing information

Problem of the Web: Semistructured data

- no global declarations
- semantics vary from node to node
Example 6: Monetizing information

Problem of the Web: Semistructured data

- no global declarations
- semantics vary from node to node

Proposed solutions

- *Semantic Web:*
  - standardize formats for global declarations (ontologies)
- *search:*
  - do not standardize
  - extract the meaning from the documents
Example 6: Monetizing information

Demise of Web 1.0

- keyword search
  - crawling and indexing

- stealing the meaning is easy and blatant
  - keyword stuffing, keyword spam, spamdexing

- race to the bottom
  - costless advertising overruns all information
Example 6: Monetizing information
Web 2.0 solution: Reputation ranking

Reputation as a fixed point (PageRank, HITS)
Example 6: Monetizing information

Monetizing search: Ad Words
Example 6: Monetizing information

Monetizing semantics: Ad Sense
Example 6: Monetizing information

Google protocol
Example 6: Monetizing information

Search engine protocol
Example 6: Monetizing information

Search engine protocol

User → SE

query?

index
Example 6: Monetizing information

Search engine protocol

User --> SE

query?

index

query!
Example 6: Monetizing information

Search engine protocol
Example 6: Monetizing information

Search engine protocol

User → SE → Advertiser

- User queries "index" to SE
- SE searches for "index" and returns a list of advertisers
- Advertiser "advertises" a query
- SE returns a list of advertisers to User

User queries "index" to SE

User queries "index" to SE

User queries "index" to SE
Example 6: Monetizing information

Search engine protocol

User \(\xrightarrow{\text{query?}}\) SE \(\xrightarrow{\text{index}}\) Advertiser

SE \(\xrightarrow{\text{advertise?}}\) Advertiser

Advertiser \(\xrightarrow{\text{advertise!}}\) SE

SE \(\xrightarrow{\text{monetize!}}\) User
Example 6: Monetizing information

Upshot

Search protocol participants have **different security goals**:

- **surfer**: acquire information
- **search engine**: monetize information
- **sponsors**: influence information
Example 6: Monetizing information

Upshot

Search protocol has **different executions**: 

- *surfer*: information retrieval
- *search engine*: man-in-the-middle
- *sponsors*: user tracking and profiling
Example 6: Monetizing information

Upshot

...And these security problems arise before fraud...
Claim 1

Networks open up **social problems** like

1. trust and reputation
2. digital property rights
3. commons and the environment
4. free market
5. information economy

...
Claim 2

Such social problems open up to *technical solutions* that combine

- security methodologies and
- economic modeling
Outline

Announcements

Motivation

Examples

Ideas

Why Economics & Security?

Conceptual roots of network economy

Structure of the course
What are Economics & Security?

- What is economics?
- What is security?
What are Economics & Security?

- Economics is concerned with production of wealth.
- Security is concerned with protection of assets.
What links Economics & Security?

- Economics $\subseteq$ Security
  - economics studies the market
  - the market is a security protocol
  - market economy is a security process
What links Economics & Security?

- Security $\subseteq$ Economics
  - security protects assets
  - security costs $\leq$ asset value
  - security is an economic process
"The efforts of men are utilized in two different ways:

- they are directed to the production or transformation of economic goods,
- or else to the appropriation of goods produced by others.

Vilfrido Pareto
A race is won by moving fast
... or by tripping up the opponent
Economy of production and predation
Economy of production and predation

Bacteria have a security problem to protect their assets.
Economy of production and predation

- Production increases wealth.
- Predation redistributes it.
- Redistribution leads to new forms of production.
  - network servers: banks, real estate agents...
Dynamics of production and predation

The rich get richer.

Vilfrido Pareto
Structure of the course

Part I: Methods of economics in security
Lecture 2: Security Investment Analysis
Lecture 3: Interdependency and Gaming

Part II: Methods of security in economics
Lecture 4: Information economy
Lecture 5: Trust and reputation
Teaching outcomes of the course

Part I: Market aspects of security
Lecture 2: Tools for CIO
Lecture 3: Security and competition

Part II: Security aspects of market
Lecture 4: Pricing and market mechanisms
Lecture 5: Monetizing information
Employment outcomes the course

Part I: Chief Information Officer
Lecture 2: "How much is this firewall worth to me?"
Lecture 3: "Can I secure this transaction?"

Part II: Monetizing guru
Lecture 4: "Where is the revenue on this network?"
Lecture 5: "How can I monetize this free transaction?"