

Arbeitsgruppe 4

Applied Cryptography and Security Engineering

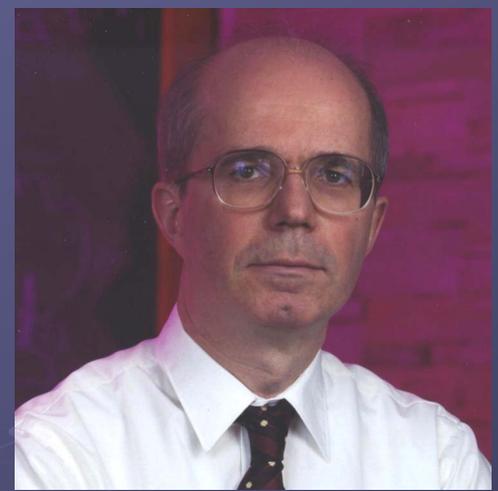
Economics, Psychology, and Sociology of Security

by Andrew Odlyzko

Überblick

1. Andrew Odlyzko
2. Paper 1: ***Economics, Psychology, and Sociology of Security***
3. Paper 2: ***Privacy, Economics and Price Discrimination on the Internet***

Andrew Odlyzko



- Professor an der mathematischen Fakultät der Universität von Minnesota
- Im Besitz eines **Ehrendokortitels** der Universität Marne la Vallee (France)
- Engagement in einer **Vielzahl von Projekten**
- Sein Schriftwerk umfasst über **150 Fachbeiträge**
- Übergang: theoretisch/ mathematisch → gesellschaftspolitisch
- **Kryptographie**: Advisory Board, Programm Komitee, Organisator zahlreicher Workshops, Schriftsteller und in der Redaktion

Warum ist Computer- und Kommunikationssicherheit nicht perfekt?

- Rolle von **nicht-technischen Aspekten** (oft wirtschaftliche Aspekte)
 - Kosten- und Nutzenabwägung
 - Absichten verschiedener Mitwirkender
- **Grundproblem:** „people and formal methods do not mix well“

Psychologische Aspekte: Unvereinbarkeit von formellen Methoden und der menschlichen Natur

- Sicherheit ↔ Flexibilität
- Interpretationsspielraum von Regeln
- Menschen vertrauen in eine „shared culture“
- Schwierigkeiten mit Sicherheitssystemen werden oft durch die Tatsache unterstützt, dass sie von Technologen entwickelt werden
- Illustratives Beispiel: Wason selection task

Wason selection task



BOB aus
Philadelphia

Er reist mit
dem Auto



ALICE aus
Philadelphia

Ihre Reise
führt sie nach
Baltimore



CHARLIE aus
Philadelphia

Er reist nach
Chicago



DAVE aus
Philadelphia

Er fliegt mit
dem
Flugzeug.

Wason selection task

Aufgabe:

Welche der Karten muss man umdrehen, um herauszufinden, ob sich die Personen nach einer bestimmten Regel verhalten. Die Rückseite der Karten enthält die fehlenden Informationen!

Die Regel ist vorgegeben:

Wenn eine Person von Philadelphia nach Chicago reist, fliegt sie.

Wason selection task- Solution



BOB

Er reist mit
dem Auto



CHARLIE

Er reist nach
Chicago

Wason selection task



BOB aus
Philadelphia

Schaut
Fernsehen
nach dem
Essen.



ALICE aus
Philadelphia

Isst Früchte
zur
Nachspeise.



CHARLIE aus
Philadelphia

Isst Eis zur
Nachspeise.



DAVE aus
Philadelphia

Spült nach
dem Essen.

Wason selection task

Regel:

**Wenn ein Kind als Nachspeise Eis isst,
muss es auch das Geschirr spülen.**

Wason selection task- Solution



BOB

**Schaut
Fernsehen
nach dem
Essen.**



CHARLIE

**Isst Eis zur
Nachspeise.**

Wirtschaftliche Aspekte

- „There is a context to most of electronic transactions that provides extra margin of safety.“

→ zum Beispiel Fax

- „Commercial, government and academic enterprises are typically based on social relations and unwritten rules.“

Definition der Sicherheit von A. O.

- „**Security is not an isolated good, but just one component of a complicated society.**“
- „**Security is not a way to provide ironclad protection, but is the equivalent of speed bumps, decreasing the velocity and impact of electronic attacks.**“

Unsicherheit im „realen“ Leben



Unsicherheit in der virtuellen Welt

Andrew Odlyzko:

„In information and communication technologies, we have also managed to live with insecurity.“

Hat sich unsere Gesellschaft mit der Unsicherheit wirklich bereits abgefunden?

Müssen wir uns wirklich mit Unsicherheit abfinden?

- Bilden?

- Vermeiden?

- ...

Privacy, Economics and Price Discrimination on the Internet

Andrew Odlyzko

July 27, 2003

Preis Diskriminierung

Preis Diskriminierung 1. Grades

- Individuelle Preise für gleiche Güter für verschiedene Kunden

Preis Diskriminierung 2. Grades

- Individuelle Preise für ein bestimmtes Kundensegment
- Der Kunde entscheidet selbst zu welchem Segment er gehört

Preis Diskriminierung 3. Grades

- Individuelle Preise für ein bestimmtes Kundensegment
- Kunde kann nicht entscheiden zu welchem Segment er gehört

Beispiele für Preisdiskriminierung

- **Senioren und Studentenvorteile**
- **Flugtickets:**
 - First Class, Business Class, Economy Class
 - Buchungszeitpunkt
- **Tankstellen in den USA**
- **Privatuniversitäten in den USA**
- **„Versioning“:** Verschiedene Produktversionen (meistens fast identisch) zu verschiedenen Preisen
 - Gebundenes Buch ↔ Taschenbuch

Entwicklung von Preisdiskriminierung

- Langbestehende Strategie:
Preissetzung im Zeitalter der Eisenbahnen
im 19. Jahrhundert
- Wurde als Zeichen für Monopole gesehen
- Spielt eine immer größere Rolle
2 Hauptgründe:
 - Hohe Fixkosten, niedrige Stückkosten
 - Moderne Technologie → Kundenanalyse
- Aber: Horrorszenarien unwahrscheinlich

Warum sind Horrorszenarien unwahrscheinlich?

- Arbitrage
- Gesetze müssten sich ändern
- Protest und Ablehnung der Öffentlichkeit
„Technology changes rapidly, but human nature does not.“
→ Vergleiche Reaktionen im 19. Jahrhundert
- Tools um Preisdiskriminierung aufzudecken

Preisdiskriminierung und Wirtschaft

● Preisdiskriminierung in der Öffentlichkeit nicht angesehen

→ Regierungen sollen reagieren

● Aber: Soziale Wohlfahrt kann durch Preisdiskriminierung gesteigert werden

- Größerer Wettbewerb
- Steigerung der wirtschaftlichen Aktivität
- Kann sich für alle Parteien auszahlen:

- Charlie ist Unternehmensberater, Alice und Bob wollen von ihm einen Bericht
- Alice würde 700\$ dafür zahlen, Bob 1000\$
- Charlies Kosten: 1500\$
- Würde Charlie den Bericht für den gleichen Preis verkaufen: 700\$
- Erlös 1400\$ → Charlie wäre nicht bereit den Bericht zu schreiben
- Preis zwischen 700\$ und 1000\$ → nur Bob Käufer
- Optimale Lösung: Preisdiskriminierung
- Alice: 650\$, Bob: 950\$, Gewinn für Charlie: 100\$

Privatsphäre ↔ Preisdiskriminierung

„Privacy intrusion serves to provide the information that allows sellers to determine buyers willingness to pay.“

- Größter Eingriff in Privatsphäre vom privaten Sektor!
- Interesse am Geld des Kunden, nicht an der Kontrolle seines Verhaltens
- Preisdiskriminierung zahlt sich mehr aus, als jede Marketingstrategie

Andrew Odlyzko: Privatsphäre

- Ausweitung von Preisdiskriminierung aufgrund von Anreizen und Möglichkeiten
- Inakzeptanz der Öffentlichkeit
→ Preisdiskriminierung verstecken oder in versteckter Form: z. B. Bundling
- Regierungen im Zwiespalt:
Druck der Öffentlichkeit ↔ Wohlfahrt generierende Wirkung der P. D.
- Fazit:
 - Verlust der Privatsphäre aufgrund von Preisdiskriminierung
 - Identifizierung mit dem Verlust der Privatsphäre

Verlust der Privatsphäre

- Datenschutz Grundrecht: Recht zur informationellen Selbstbestimmung
- ADAC ↔ Shell
- Kundenkarten
- Studivz, facebook
-

Diskussion

- Verlust der Privatsphäre akzeptieren?
- Welche Rolle übernimmt die Kryptographie?
- Welche Auswirkungen ergeben sich für unsere Gesellschaft?
- Sind Horrorszenarien wirklich so unwahrscheinlich?