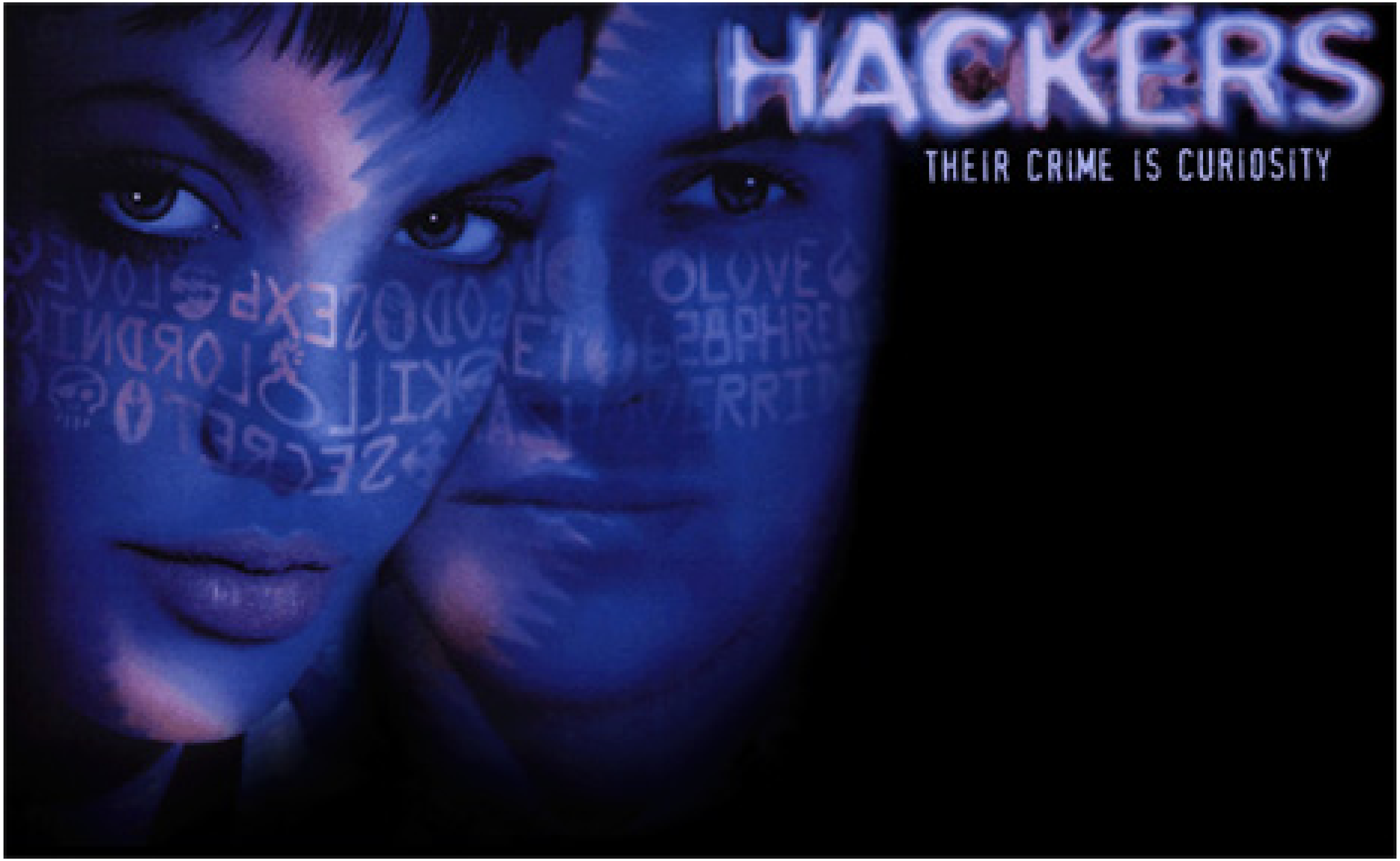
Exploitable Assumptions

Doktor Zoz, Dr. Foley, and Eric Schmiedl

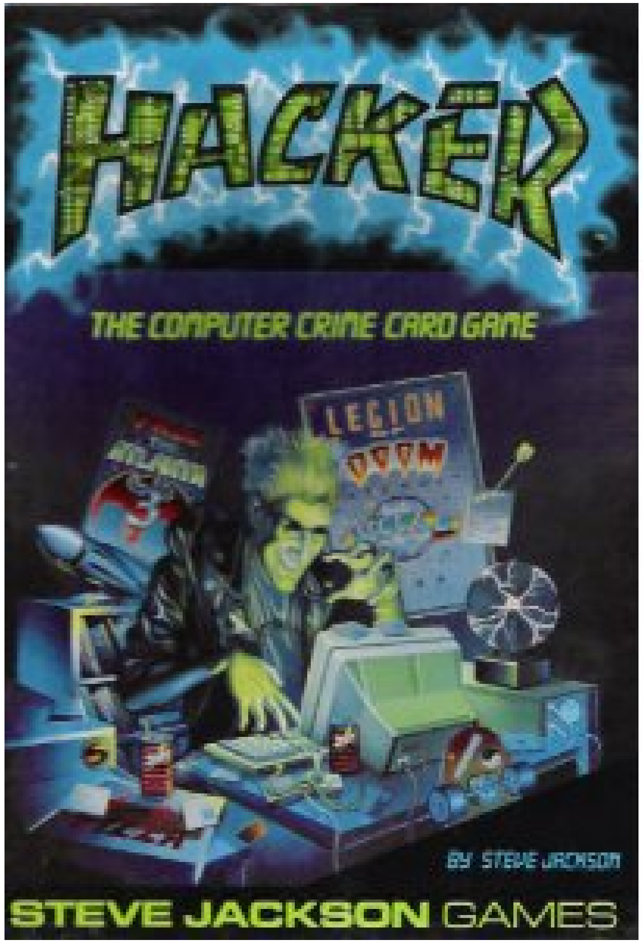
What the hell is a Hacker?



What the hell is a Hacker?

The movie does get a few things right

- Curiosity
- Assumptions and Authority!



Hacker Mindset

Good at spotting flaws, inefficiencies
Must know how things work at any cost
Boil things to most abstract level
Are stubborn, with bloody-mindedness
Constantly testing even if inconvenient
Intuition of what is interesting to verify
Willing to take risks and fail

}

Assumptions!

Доверяй, но проверяй

Trust but verify --Ronald Reagan 1987

Why do we care about those damned Assumptions?

When you assume...

KRB4 zero-seed encrypt

- everyone assumed working because output looked encrypted and worked

Buffer overruns

- Assumption that you will only write so much data

SQL injections

- Assume that variables cannot affect flow control

Assumptions Aplenty

Snake in the Peanut Brittle!

- No explanation needed

Good looking websites and evil web design

- Assumption of similarity to physical storefronts
- Exploits assumptions of "relevant info" and "not relevant" through misleading graphic design

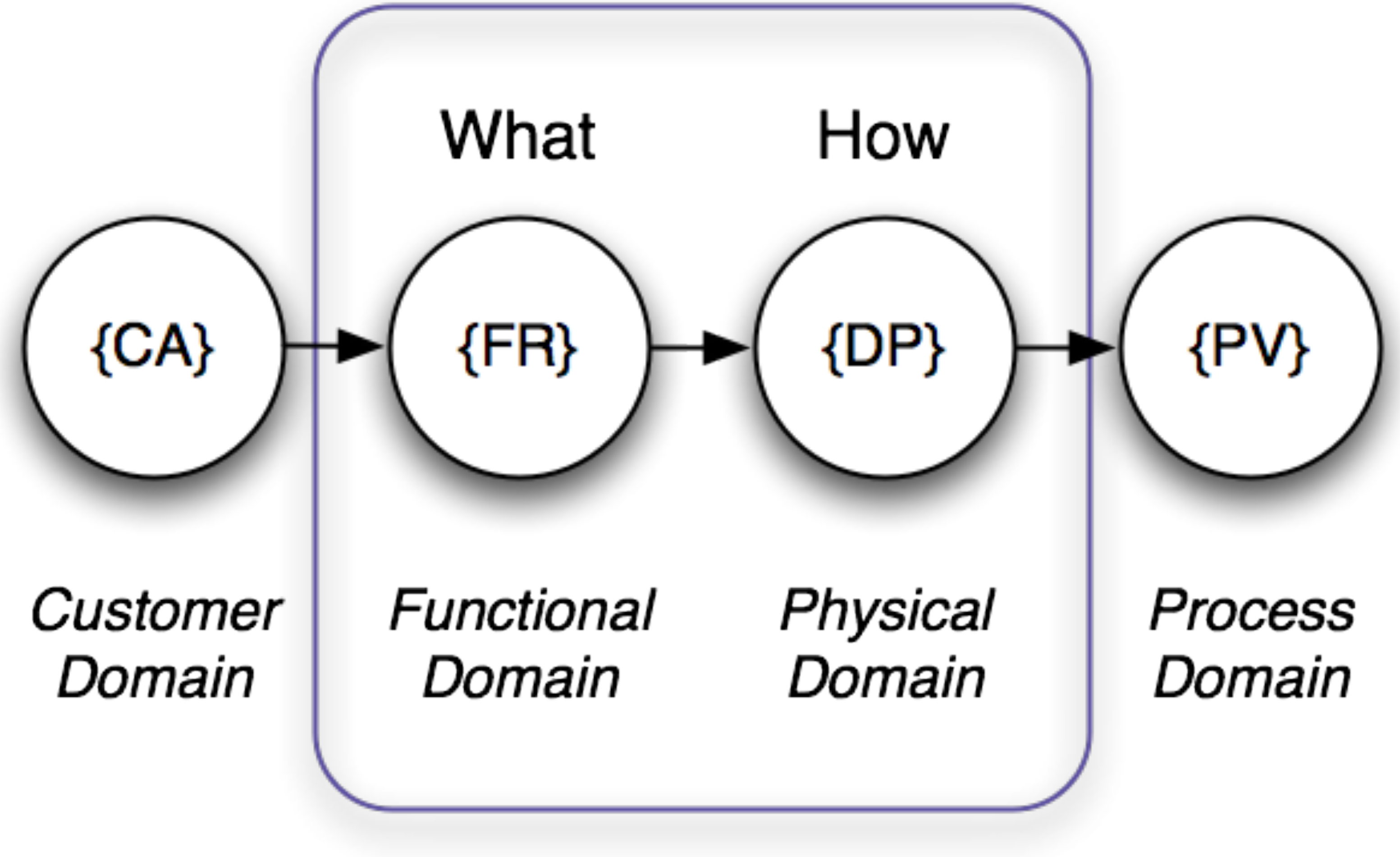
Fighting Assumptions: Axiomatic Design
aka WWNSD

MIT Mechanical Engineering &
KAIST: Design Methodology [Suh 2001]

- Solution neutral design process
- Excellent for discovering assumptions

Dr. Nam Suh says: "Assumptions make you stupid. No good! Y fail!"

Axiomatic Design Process



Axiom 1: Decouple

aka. Independence Axiom

Within domain, elements MUST be independent!

Problems arise when

- Customer needs assumed as functional requirements
- Functional requirements assumed as design parameters
- Contradictions lead to conflicts, lead to security holes

Axiom 2: Reduce complexity

aka Information Axiom

Designs with least information increase robustness

- complexity opens "arbitrage" opportunities
- complexity vs. user centered design
    - user workarounds create security holes

Beware time dependence

Some complexity is static, some is time dependent

- t-dependent combinatorial complexity -> chaos
- transform combinatorial into periodic
    - periodical, lossless "reboot"

Warm Up Problem: H.A.M.M.E.R.

Straight Hardened Metal Fastener Insertion Tool

Functional Requirements (Why)

1.
2.
3.
4.

Design Parameters (How)

1.
2.
3.
4.

Creating Assumption Exploits

- Confusing comparisons
  - aka. *Math is hard, let's go shopping*
- Jumping the Epic Level
  - spear phishing
  - generating pseudoauthority
  - using fantasy
- Misdirection
  - bait and switch
- Aesthetics cons
  - looks like a duck... must be a duck

Why do people gamble?

http://i64.photobucket.
com/albums/h190/Morphthecat/death
-clock.jpg

Odds of dying

- if you were alive 1939-1945: 1 in 221
- due to a home appliance: 1 in 1,500,000
- of terrorism in the USA: 1 in 3,500,000
- of terrorism in Canada: 1 in 3,800,000

Challenge: Develop more approachable statistics set by having comparisons of things people recognize

Vegas Odds

- Poker
- Roulette
- Craps

Mommy, I'm Scared...

"Unacceptable risk"
- normally 1 in 10,000 or 1 in 100,000

risks
- home appliances 1 in 1,500,000
- terrorism is 1 in 3,500,000

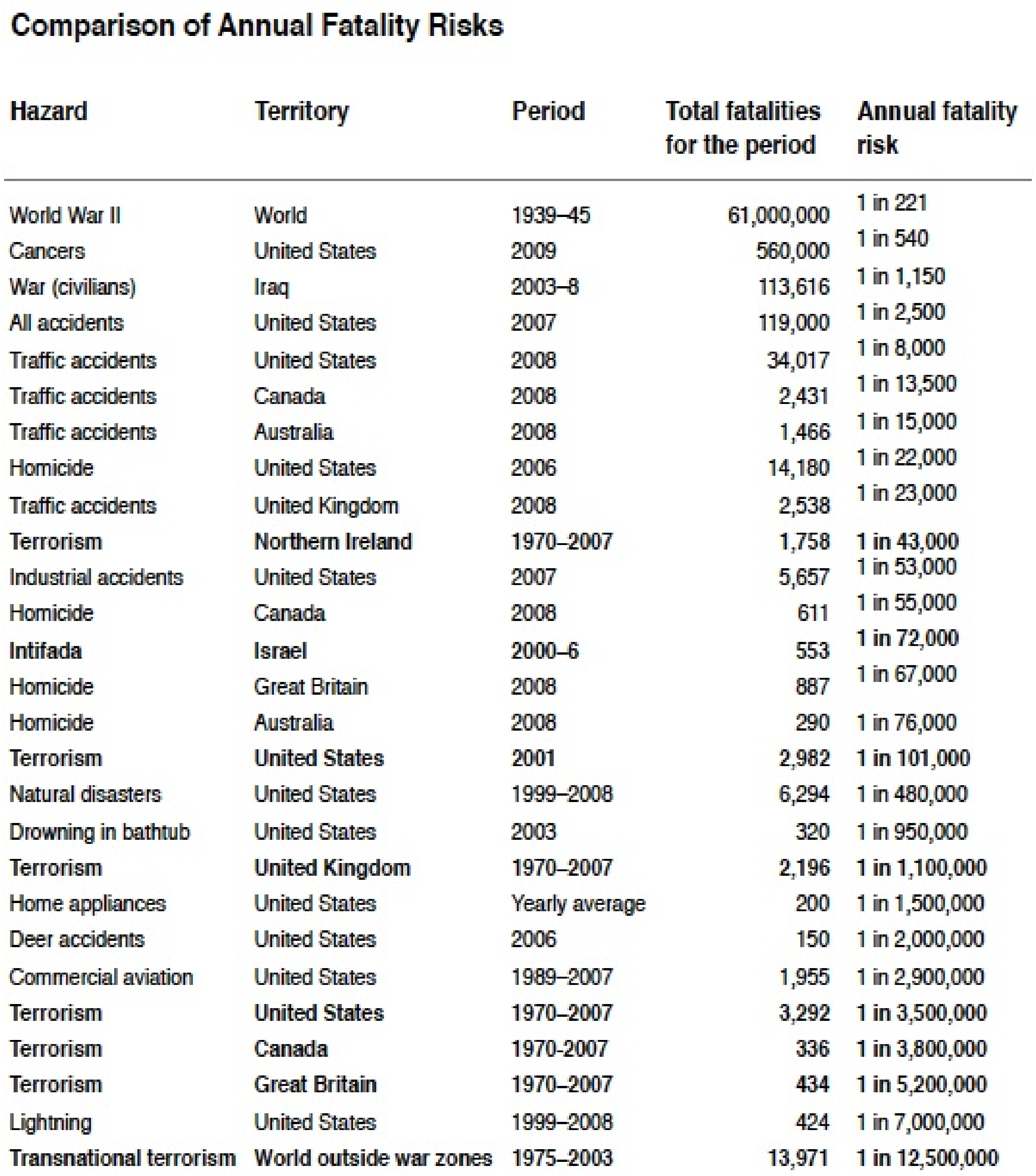
budgets
- CPSC [product safety] -- $100 million
- FBI counterterrorism -- **29x** higher, $2.9 billion
- DHS budget -- **440x** higher, $44 billion

Death in the USA 2001

Heart Disease	1:6
Cancer	1:7
Stroke	1:23
Motor Vehicle Accident	1:100
Suicide	1:121
Falling Down	1:246
Assault by Firearm	1:325
Fire or Smoke	1:1,116
Natural Forces (heat, cold, storms, quakes, etc.)	1:3,357
Electrocution	1:5,000

Drowning	1:8,942
Air Travel Accident*	1:20,000
Flood*	1:30,000
Legal Execution	1:57,618
Tornado*	1:60,000
Lighting Strike*	1:83,930
Venom (Bee, Snake, etc.)	1:100,000
Earthquake	1:131,890
Dog Attack	1:147,717
Asteroid Impact*	1:200,000 -- 1:500,000
Tsunami*	1:500,000
Fireworks Discharge	1:615,488

http://www.livescience.com/environment/050106_odds_of_dying.html



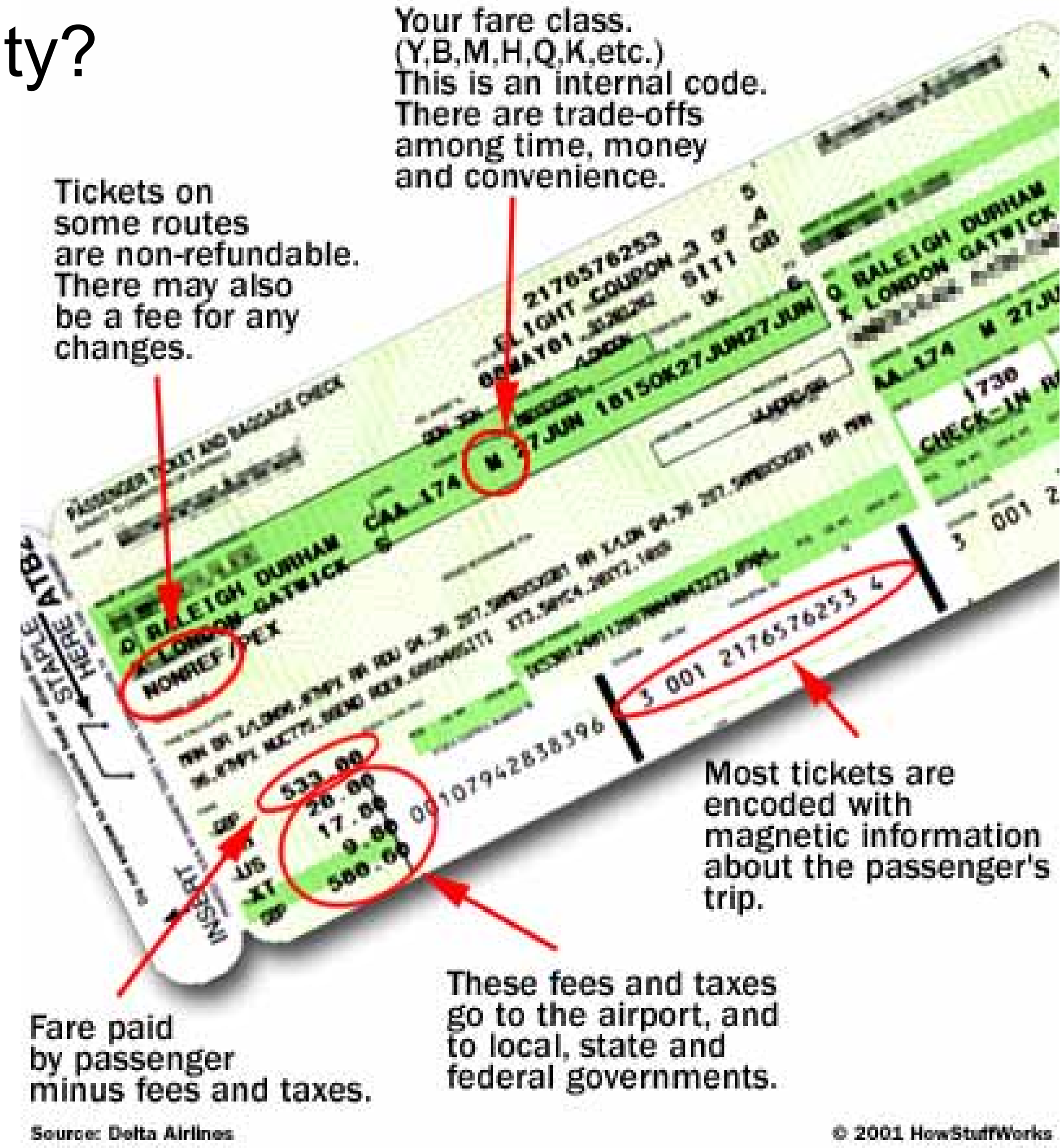
Comparison of Annual Fatality Risks

Hazard	Territory	Period	Total fatalities for the period	Annual fatality risk
World War II	World	1939–45	61,000,000	1 in 221
Cancers	United States	2009	560,000	1 in 540
War (civilians)	Iraq	2003–8	113,616	1 in 1,150
All accidents	United States	2007	119,000	1 in 2,500
Traffic accidents	United States	2008	34,017	1 in 8,000
Traffic accidents	Canada	2008	2,431	1 in 13,500
Traffic accidents	Australia	2008	1,466	1 in 15,000
Homicide	United States	2006	14,180	1 in 22,000
Traffic accidents	United Kingdom	2008	2,538	1 in 23,000
Terrorism	**Northern Ireland**	**1970–2007**	**1,758**	**1 in 43,000**
Industrial accidents	United States	2007	5,657	1 in 53,000
Homicide	Canada	2008	611	1 in 55,000
Intifada	**Israel**	**2000–6**	**553**	**1 in 72,000**
Homicide	Great Britain	2008	887	1 in 67,000
Homicide	Australia	2008	290	1 in 76,000
Terrorism	**United States**	**2001**	**2,982**	**1 in 101,000**
Natural disasters	United States	1999–2008	6,294	1 in 480,000
Drowning in bathtub	United States	2003	320	1 in 950,000
Terrorism	**United Kingdom**	**1970–2007**	**2,196**	**1 in 1,100,000**
Home appliances	United States	Yearly average	200	1 in 1,500,000
Deer accidents	United States	2006	150	1 in 2,000,000
Commercial aviation	United States	1989–2007	1,955	1 in 2,900,000
Terrorism	**United States**	**1970–2007**	**3,292**	**1 in 3,500,000**
Terrorism	**Canada**	**1970-2007**	**336**	**1 in 3,800,000**
Terrorism	**Great Britain**	**1970–2007**	**434**	**1 in 5,200,000**
Lightning	United States	1999–2008	424	1 in 7,000,000
Transnational terrorism	**World outside war zones**	**1975–2003**	**13,971**	**1 in 12,500,000**

Mueller and Stewart, "Hardly Existential: Thinking Rationally about Terrorism." Foreign Affairs, April 2, 2010.

Problem: Airport Security

What is the goal of Airport Security?



Your fare class. (Y,B,M,H,Q,K,etc.) This is an internal code. There are trade-offs among time, money and convenience.

Tickets on some routes are non-refundable. There may also be a fee for any changes.

Most tickets are encoded with magnetic information about the passenger's trip.

Fare paid by passenger minus fees and taxes.

These fees and taxes go to the airport, and to local, state and federal governments.

Source: Delta Airlines

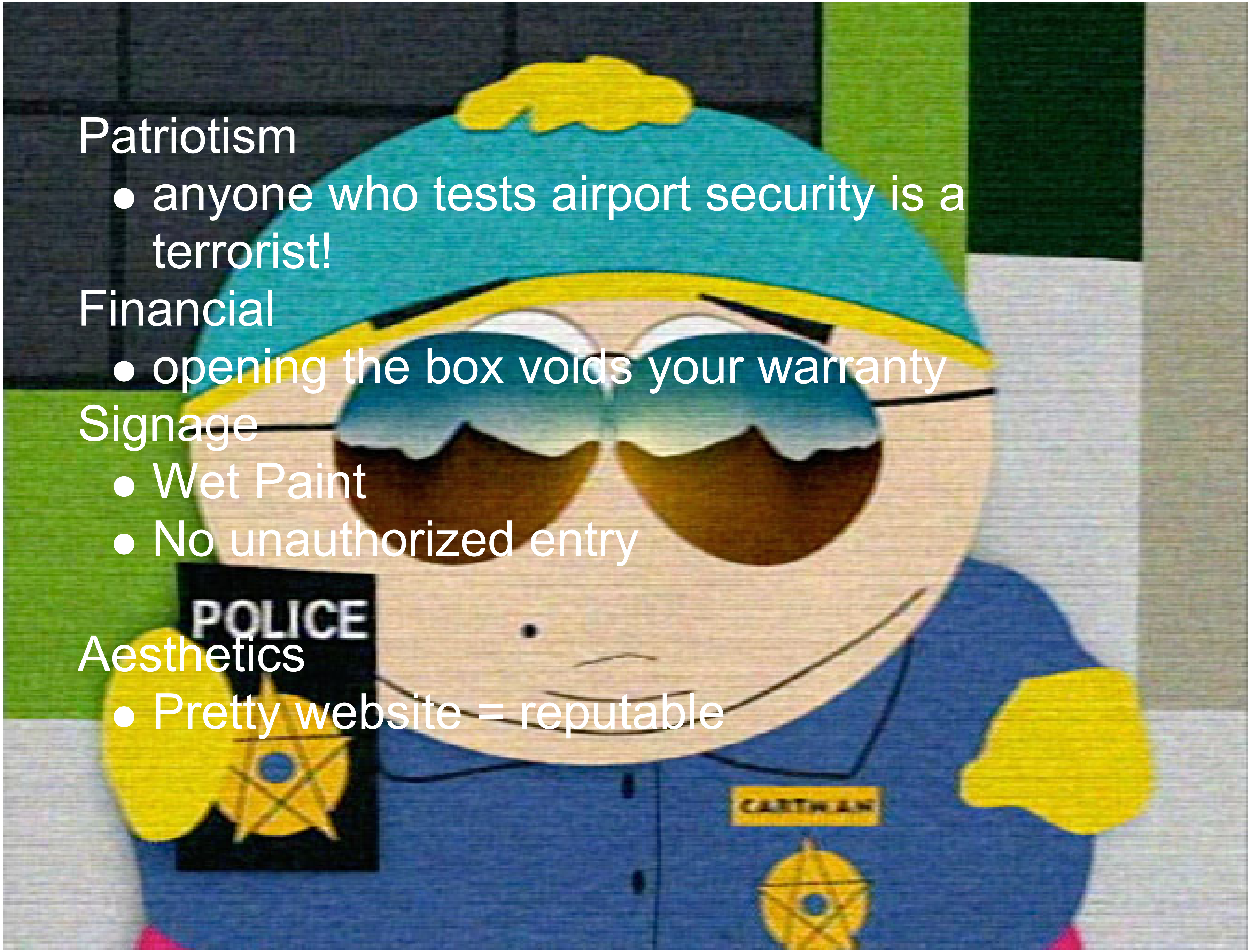
© 2001 HowStuffWorks

3 Card Monty Challenge

Design a simple con game where the target thinks they have an unfair advantage but also legitimate way to lose.

http://www.123opticalillusions.com/pages/dice_illusion.php

Assumptions of (pseudo)Authority



Patriotism

- anyone who tests airport security is a terrorist!

Financial

- opening the box voids your warranty

Signage

- Wet Paint
- No unauthorized entry

Aesthetics

- Pretty website = reputable

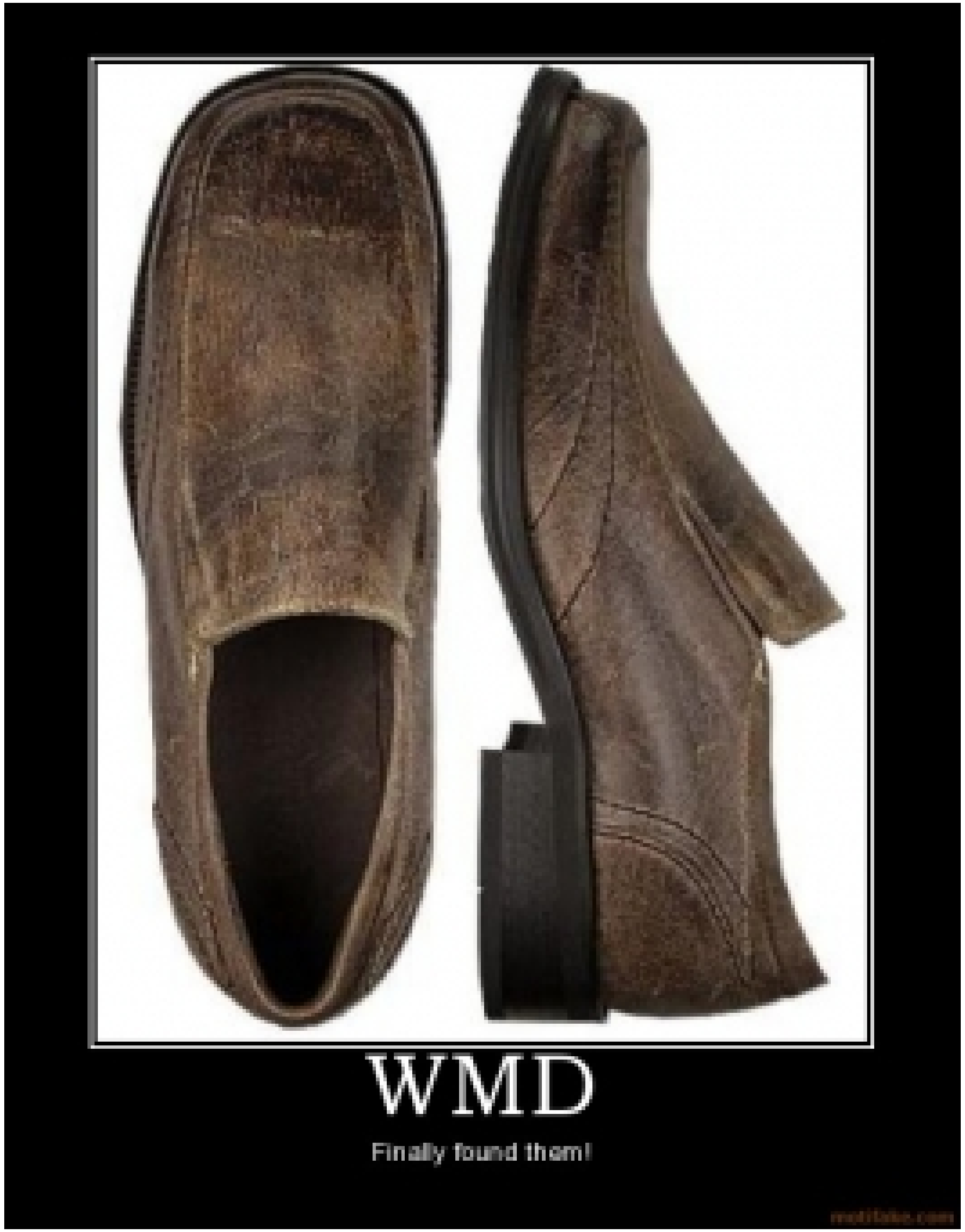
DEFCON Vendor Security Challenge

Defenders

- Step 1: define attackers, operating needs
- Step 2: develop defenses

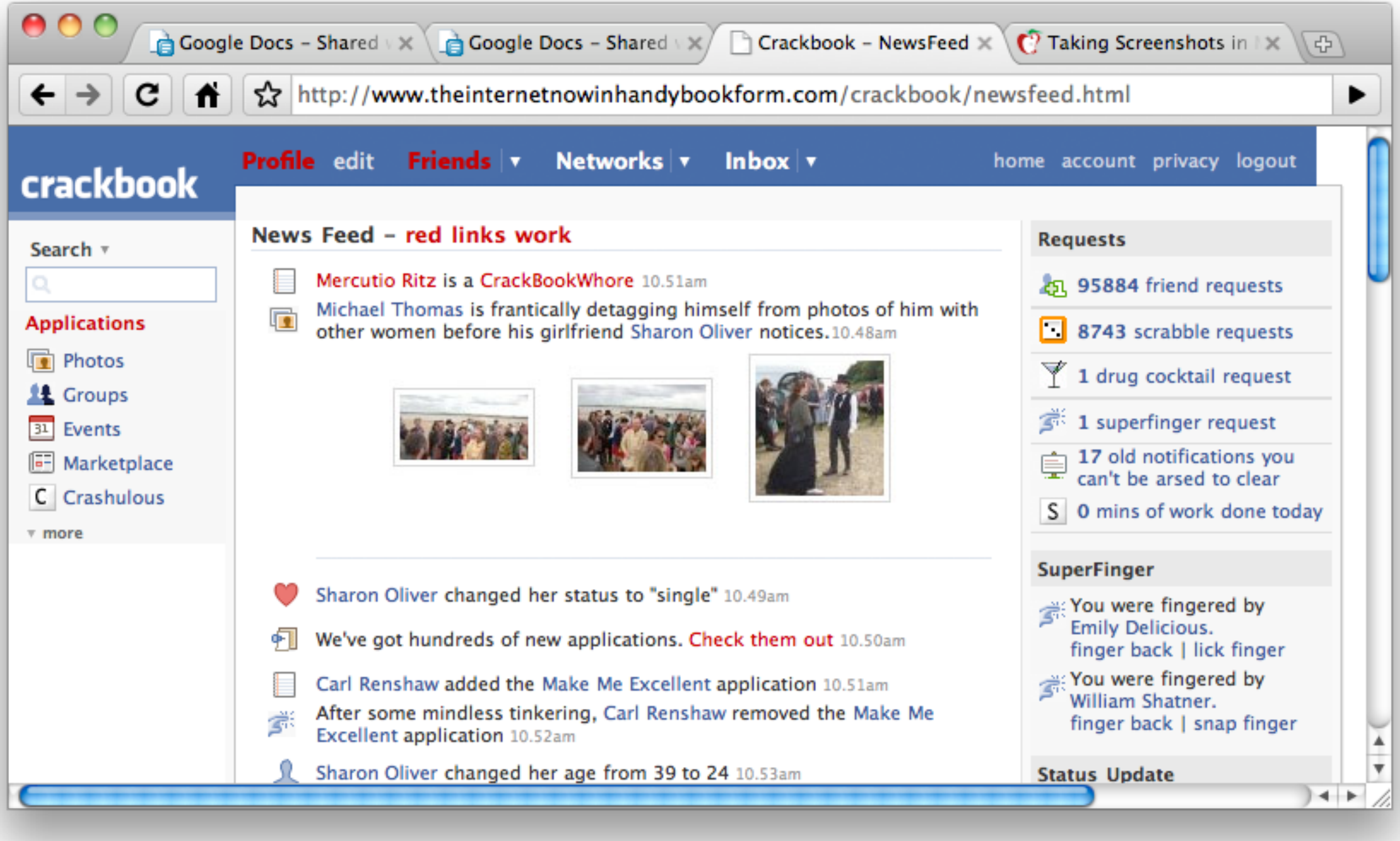
Attackers

- Step 1: define attackers, desired exploit outcomes
- Step 2: develop countermeasures



www.motifake.com

Problem: Compromised Account Value



News Feed – red links work

Mercutio Ritz is a CrackBookWhore 10.51am

Michael Thomas is frantically detagging himself from photos of him with other women before his girlfriend Sharon Oliver notices. 10.48am

Sharon Oliver changed her status to "single" 10.49am

We've got hundreds of new applications. Check them out 10.50am

Carl Renshaw added the Make Me Excellent application 10.51am

After some mindless tinkering, Carl Renshaw removed the Make Me Excellent application 10.52am

Sharon Oliver changed her age from 39 to 24 10.53am

Requests

95884 friend requests

8743 scrabble requests

1 drug cocktail request

1 superfinger request

17 old notifications you can't be arsed to clear

0 mins of work done today

SuperFinger

You were fingered by Emily Delicious.
finger back | lick finger

You were fingered by William Shatner.
finger back | snap finger

Status Update

Problem: Social Authentication

Could you use social networking as an authentication mechanism? What does "friending" actually mean?

http://www.blacknbougie.com/2010/03/five-quick-ways-to-get-de-friended-on.html

Social Engineering Contest

Best comp from the casino you are **not** staying in
(the Riv is out no matter what)

Deadline Saturday 2PM

Fantasy Hacking

Marketing people want to use fantasy/symbols to sell you stuff

- Coke gives you life!
- Redbull gives you wings.

Social assumptions in slogans are made evident during translation

- Coke brings your dead ancestors back!
- Ming's Market in Boston is actually "Cheap Good Grocer"

Let's look for fantasy probes and social assumptions that can be used to marketing-hack a particular group.

Summary

Assumptions are powerful

- Lesser mind control

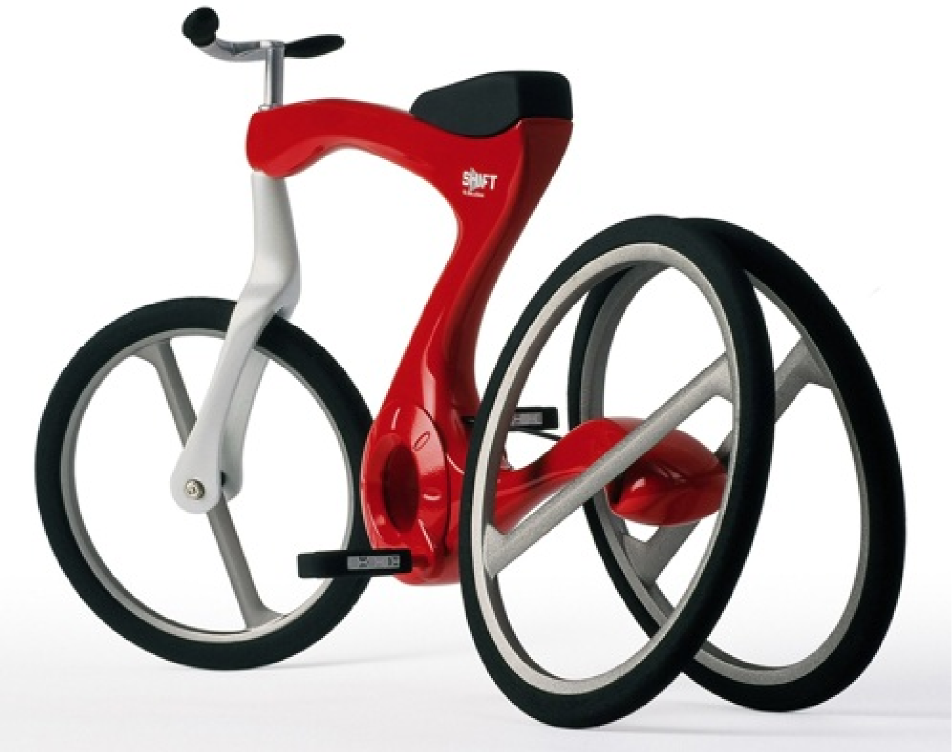
We need to be aware of these assumptions to avoid designing bad systems or exploit such systems

Axiomatic Design is a tool to identify these assumptions

Thanks for Playing!

assumptions@objid.net
Latest Version:
http://objid.net/assumption-defcon

Bicycles!



http://blog.makezine.com/archive/2006/03/the_modern_marvels_invent_4.html

Visualization: Gun

Are these guns?

Fabrique Nationale P90

Metal Storm

Steyr AUG A2

Steyr Match FP