Conditional Entropy for Deception Analysis

E. John Custy
Neil C. Rowe
Center for Information Security Research
U.S. Naval Postgraduate School
ncrowe@nps.edu

Overview

- Definition of Deception
- A Channel Model for Deception
- The Symmetric Complement of a Deception
- Examples of Deceptions Mapped to Channel Models
- Conditional Entropy
- So What?
  - Conditional Entropy is Concave
  - General Counter Deception Opportunities Exist
  - Deception Can Be Interpreted Geometrically
  - Deception-Based Computer Security
- A spoofing channel implementation with a honeypot

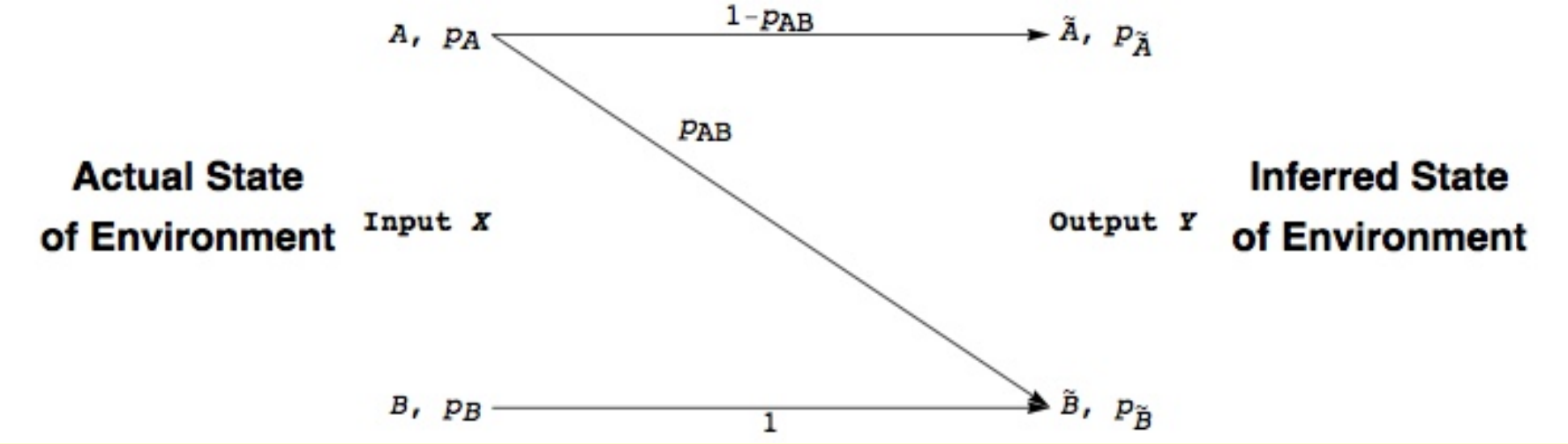
A Definition of Deception

Deception is the presentation of a specific false version of reality by a deceiver to a target for the purpose of changing the target's actions in a specific way that benefits the deceiver.

The deception target's decision is binary: there is only one correct version of reality, and one incorrect version of reality.

A Channel Model for Deception

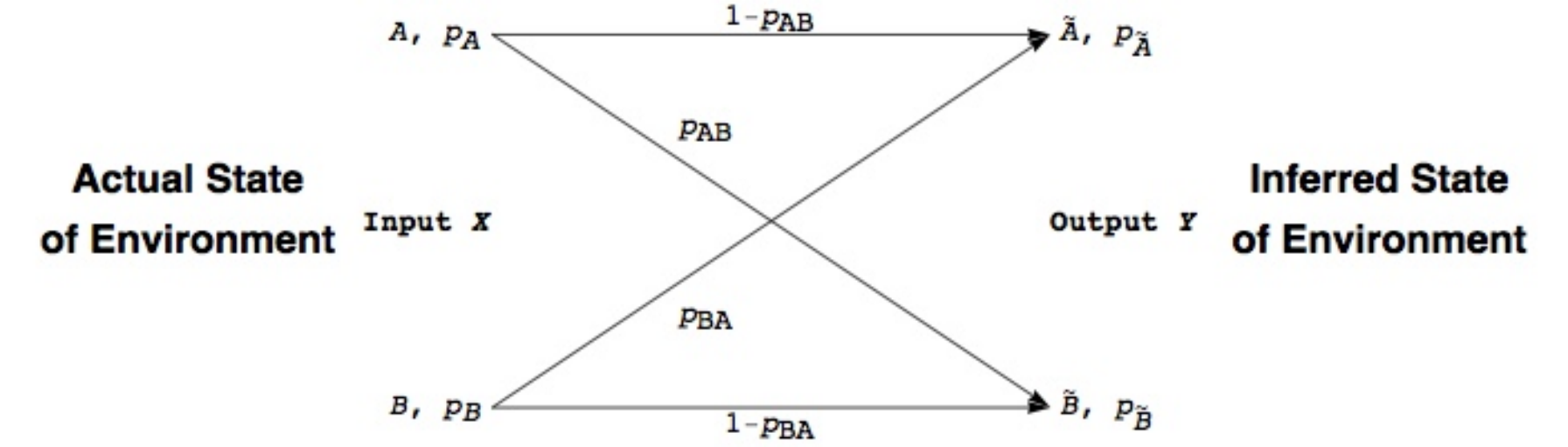
- Deception causes the actual state of the environment to differ, on occasion, from the inferred state of the environment.
- The deceiver acts as noise: without deception, the target will correctly infer the state of nature.



The deception target is vulnerable to only one type of error

The Symmetric Complement

- The symmetric complement of a deception makes the channel model symmetric
- Terminology: A two-sided deception is a deception deployed along with its symmetric complement



Here the deception target is vulnerable to <u>two</u> types of error

Examples (1/2)

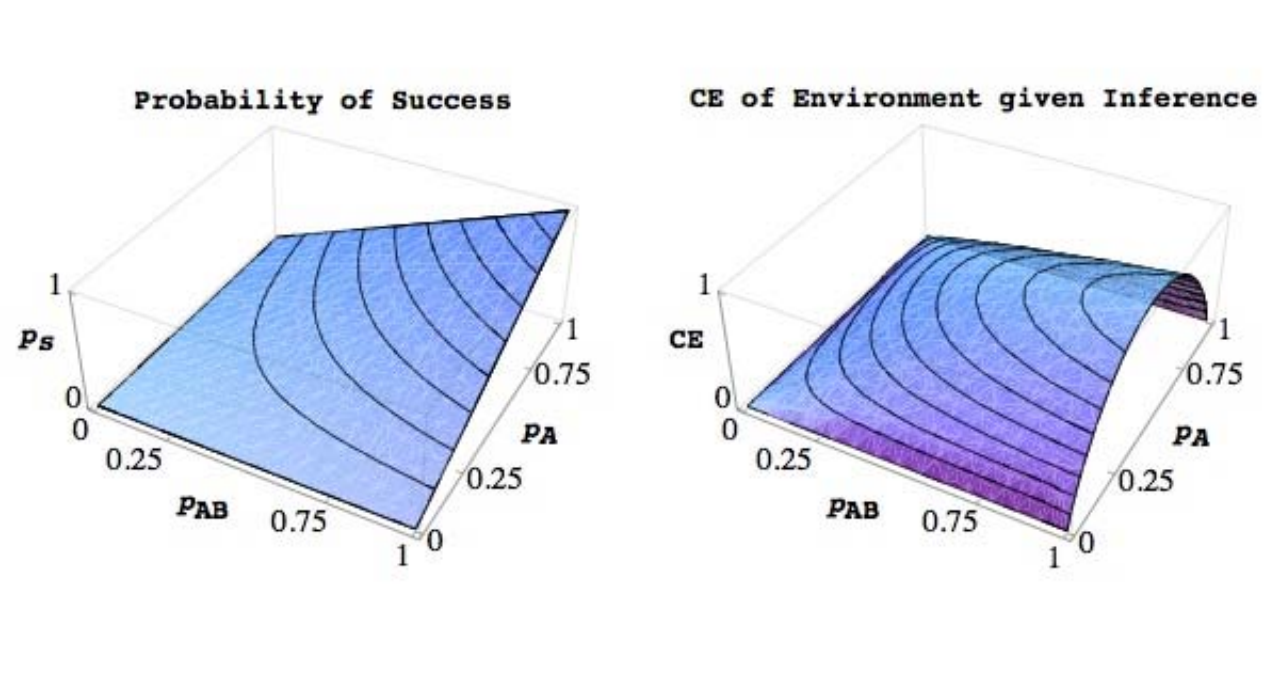
- One-Sided Deceptions
  - Sale of Low Quality Items
    - False Version of Reality: Product is High Quality
    - Actual Version of Reality: Product is Low Quality
  - Camouflage
    - False Version of Reality: No intruders are present
    - Actual Version of Reality: An intruder is present
  - Phishing
    - False Version of Reality: Web site is valid
    - Actual Version of Reality: Web site is in valid
  - Social Engineering
    - False Version of Reality: Person claiming authority has author.
    - Actual Version of Reality: Person claiming authority has none

Examples (2/2)

- Two-Sided Deception
  - Feints
    - False Version of Reality: An attack is in progress
    - Actual Version of Reality: No attack is in progress
  - Dummy Aircraft & Tanks
    - False Version of Reality: Dummies are valuable
    - Actual Version of Reality: Dummies are worthless
  - Runway Strafing
    - False Version of Reality: Runway is usable
    - Actual Version of Reality: Runway is useless

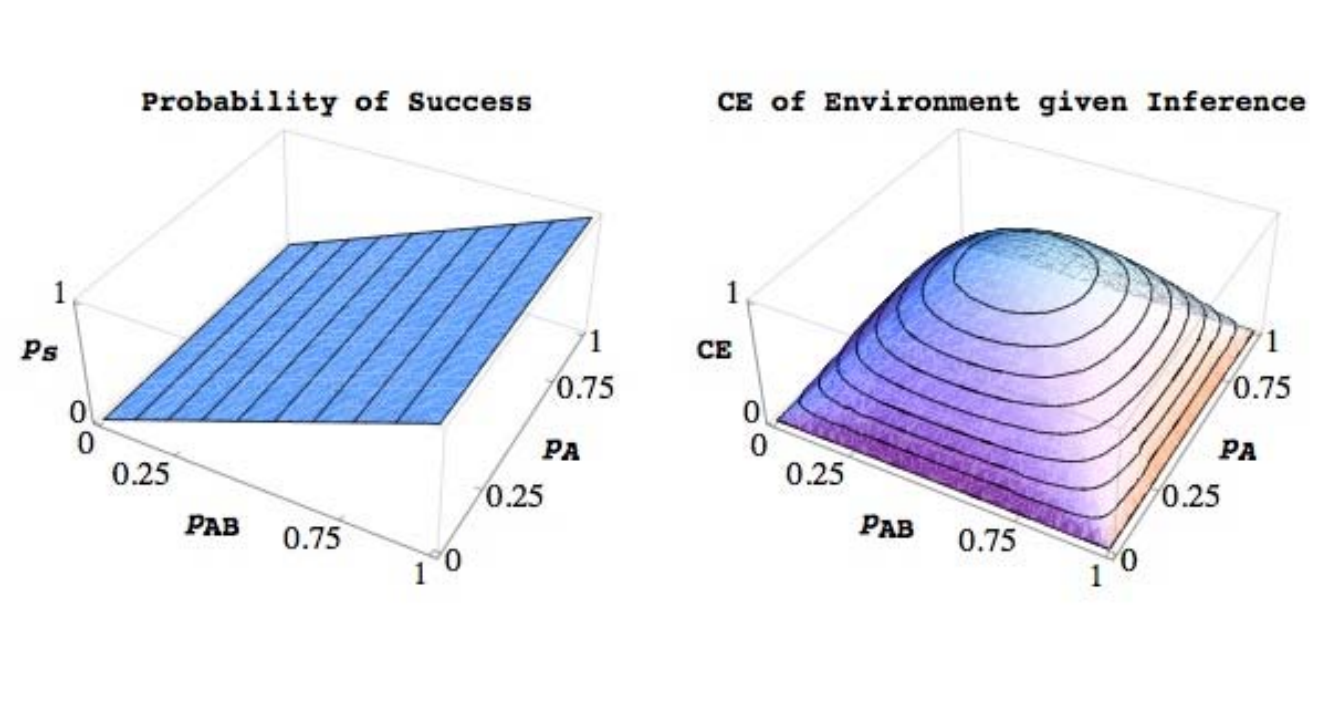
Conditional Entropy (1/2)

- Conditional Entropy of One-Sided Deceptions
  - An effective one-sided deception makes the target's observations worthless
  - But this situation is fragile: failures by deceiver can be exploited by target



Conditional Entropy (2/2)

- Conditional Entropy of Two-Sided Deceptions
  - Target's observations can be *worse* than worthless...
  - But counter-deception opportunities are available...
  - However, deceiver can "back-off" to make observations worthless in a non-fragile manner...



So What? (1/2)

We have done nothing more than reinterpret standard results from information theory in terms of deception

Answer 1: Conditional entropy is a concave function... (√)

Answer 2: Signal space concepts suggest a geometric interpretation of this work... (Work in progress)

Answer 3: Counter-deception based on a negative correlation between observed & actual state of environment (√)

So What? (2/2)

Answer 3: Computer Security Tools that burden attackers with uncertainty:

- A *Fake Honeypot* is the symmetric complement of the honeypot deception (√)
- *Spoofing Channels* provide intruders with data that has the same statistical structure as the original, but is otherwise arbitrary (√)

Experiments with a spoofing channel

- We are modifying honeypot computer systems into "intrusion-response systems" that frustrate attackers by confusing them.
- We used a honeypot on the Internet outside our School's firewall.
- We installed Snort Inline and used it to modify single bits in packets (TCP and UDP protocols only) sent to it.
- Since attacks commands are sensitive to errors, this might make the attack ineffective and confuse the attacker.
- Here’s an example Snort Inline rule we used. It says to change the 50th byte of the incoming data portion of a TCP-protocol packet to an upper-case X.

```
alert tcp $EXTERNAL_NET any -> $HONEYNET any
(msg:"Exp2-TCP-offset-50"; content:"|00|"; offset:50; flags:P+;
replace:"X";classtype:exp2; priority:10; sid:9002001;rev:1;)
```

Experimental results (1)

- Attack durations increased on the average with packet bit modifications.
- Much of the increase was in the form of retries of the same commands.
- There was not much variation in effect with location in the packet.
- We conclude then that rare random bit modifications are a good delaying tactic against attacks, while preserving most of the information content in the channel.
- Our deceptions also changed the frequencies of attacks we saw.

Experimental results (2)

- The table shows counts of Snort attack classes with first a control experiment (no packet modifications) and then changes to packets at offsets into the packet of 10, 20, 100, 20, and 20 respectively.
- The last two experiments changed the bytes to "W" rather than "X", and the last ignored the flags, to see if this made a difference.
- Each experiment was run for two days.
- ICMP Ping and MS-SQL traffic was not affected.
- FTP attacks (generally password guessing) are quite sporadic and not significant.
- NETBIOS and SHELLCODE attacks show effects in Exps. 1, 3, and 5.

	Control	**Exp.1**	**Exp.2**	**Exp.3**	**Exp.4**	**Exp.5**
FTP	**0**	**0**	**0**	**68794**	**0**	**3735**
ICMP Ping	**155**	**162**	**198**	**239**	**194**	**186**
MS-SQL	**48**	**32**	**34**	**50**	**44**	**30**
NETBIOS	**76**	**19**	**15**	**96**	**22**	**173**
POLICY	**0**	**2**	**1**	**0**	**0**	**1**
SHELLCODE	**74**	**57**	**33**	**38**	**65**	**148**
WEB	**0**	**0**	**0**	**1**	**35**	**0**