Deception

CSC 790

Spring 2014

Deception

- The general idea is – *"Hiding things from an adversary"*
  - Conceal or obscure an entity's existence or attributes that intentionally misleads the adversary

    Denial == mislead? Examples?

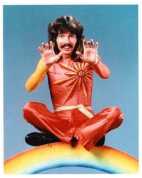
  - Disrupt adversary's discovery process (observation, investigation, and learning)

  Some deception techniques used for computer security? Real life examples (parking tickets)?

- Deception can be applied in several situations

Historical Perspective

- Homer's Iliad provides the example of the Trojan horse
  - Achaeans presented the Trojans a gift to mark their withdrawal
- British *Magic Gang* during WWII
  - Jasper Maskelyne was a British stage magician (*and member of AOFB*), developed deception for British Army
  - Used fake tanks (AKA French), jeeps, and smoke and mirrors




- Operation Fortitude, Operation Jael, and Operation Copperhead

More Recent Examples

- Kosovo War in 1999, which involved NATO and Serbia
  - Largely an air campaign from NATO's perspective
- NATO claimed it destroyed 40-60% of Serbian forces

> *"78-day aerial bombardment that had not cost the life of a single NATO soldier or airman, Defense Secretary William Cohen declared, "We severely crippled the [Serb] military forces in Kosovo by destroying more than 50 percent of the artillery and one third of the armored vehicles." Chairman of the Joint Chiefs Gen. Henry Shelton claimed that NATO's air forces had killed "around 120 tanks," "about 220 armored personnel carriers" and "up to 450 artillery and mortar pieces." "*

- However Serbia used several deception techniques...

Serbian Deception

- Serbian forces used deception
  - Several of the techniques were also used in WWII
  - Fake tanks, missiles, runways, business hugs ... crazy

- Results (*not verified by me... take with a grain of salt*)
  - Destroyed tanks, 14 not 120; Armored personnel carriers, 18 not 220 Artillery pieces, 20 not 450
  - Out of the 744 confirmed strikes by NATO pilots during the war, there is evidence of just 58

- War ended when NATO focused more on infrastructure?
  - Again, I'll let you decide

> *"In time of war, the truth is so precious, it must be attended by a bodyguard of lies." – Sir Winston Churchill*

- *Yeah so what, deception can work in different situations*
  - Consider the cost in these cases... attacker and defender

    At what cost does deception make sense?

Soviet K-129 + USS Swordfish + Hawaii == ?

Reasons for Using Deception

- Increase the freedom of action for the defender
- Persuade attacker to take a less optimal course of action
- Gain a surprise, Surprise!
- Preserve defender's resources

  What about the resources of the attacker?

Types of Deception

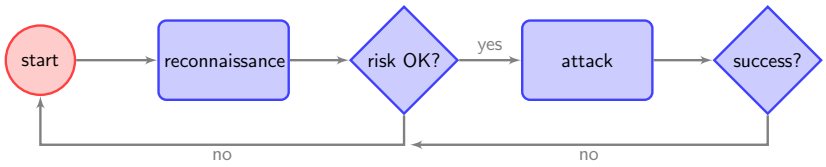
- Bell and Whaley[a] categorize into hiding and showing
  - **Deceptive hiding** conceals or obscures an entities existence or attributes to intentionally to mislead (not the same as denial...) *Deceptive hiding example?*
  - **Deceptive showing** make something that does not exist appear as if it does *Deception showing example?*
- Hiding and showing are present in any form of deception, one maybe explicit while the other is implicit...

[a] "Cheating and Deception," Transaction Publishers, 1982.

- Bell and Whaley taxonomy, (*three ways of hiding*)
  - Masking, repackaging, and dazzling (Chukar's favourite)
- Bell and Whaley taxonomy, (*three ways of showing*)
  - Mimicking, inventing, and decoying (Hobo's favorite)

Deception Applied to Cyber

Abbreviated attack process



- Reconnaissance is a vital step for any attack
  - Passive and active techniques to gather information
  - 70% time/energy devoted to this stage
  - Remainder of attack dependent on this information
- Deception seeks to nullify the reconnaissance stage

Cyber Examples of Deception

- Masking (hiding in the background) occurs with "low and slow" attacks that are accomplished over a long period of time to avoid appearing suspicious.
- Repackaging (hiding as something else) occurs with Trojan horses that to do some concealed function in addition to their avowed purpose.
- Dazzling occurs with denial-of-service attacks that flood a target with a large volume of information at once.
- Mimicking occurs with phishing that uses fake Web sites to steal personal data.
- Inventing occurs with honeypots, machines that invite attacks to collect data about attackers.
- Decoying occurs with scams of the "Nigerian letter" type where victims are decoyed by the promise of future money.

Consistent or Inconsistent Deception

- Another aspect of deception is consistency
  - Deception that is consistent if it creates an appearance that the system behaves normally
  - Inconsistent deception, the system acts unpredictably, crazy
- Neagoe and Bishop[a] described deception further
  - *"Consistent deception builds a fiction that functions under the rules of reality, so the attacker does not perceive the deception"*
  - *"Inconsistent deception ... is to discombobulate and disorient the adversary. The adversary will realize that something is wrong, possibly even realize that there is a deliberate attempt to deceive them, but not know which perceptions are of fiction and which are of reality. Thus, they will be confused."*
  - The efficacy of consistent deception deteriorates upon detection.

[a] V. Neagoe and M. Bishop "Inconsistency in Deception for Defense"

There simply cannot be any discrepancy in the deception, a difficult task in any complex system.

  - Inconsistency, on the other hand, is easier to implement as any discrepancy further leads to inconsistency
- An early example of inconsistent deception was done by Cliff Stoll
  - Keep an intruder on an international telephone line for several hours, downloading a bogus but interesting file
  - The authorities traced the call, and broke up a spy ring
  - Stoll raises the issue of whether defenders should remain open to an intruder once they are detected...

Honeypot

- A honeypot fake computer server
  - The system is designed to detect unauthorized access
  - Mimics an actual server connected to a network
  - Effective only when the attacker thinks the server is legit
  - Attacker will attempt to exploit, defender can save/observe identity and actions
- An examples include honeyd (`http://www.honeyd.org/`) and honeynet (`http://www.honeynet.org/`)

Teergrube

- Tar pitting is the idea that *"network abuses such as spamming or broad scanning are less effective if they take too long"*
  - Services purposely delay responses to invalid or sensitive requests (impeding the attacker's progress)
- Implemented by Postfix, Sendmail, and other SMTP packages, LeBrea can tar pit an entire network

> *" The machine listens for ARP requests that go unanswered (indicating unused addresses), then replies to those requests, receives the initial SYN packet of the scanner and sends a SYN/ACK in response. It does not open a socket or prepare a connection... However, the remote host believes the 3-way-handshake is complete. Then it starts to send data, which never reaches a destination. The connection will time out after a while, but since the system believes it is dealing with a live, i.e. established connection, it is conservative in timing it out and will instead try to retransmit, back-off, retransmit, etc. for quite a while. "*

Fake Honeypot *(is this redundant?)*

- Normal system that attempts to disguise itself as a honeypot
  - There are *clues* associate with honeypot, slow I/O, unusual system calls, temptingly delicious obvious file names (e.g., "secret," "super-duper-secret," "scott-drivin-a-lumina," "mmmmmmm," or "passwords"), or data in memory
  - A fake honeypot exhibits one or more of the above clues
- Also referred to as a honeyfile

Another Reason Why BSD is Awesome

- OpenBSD's packet filtering (`pf`) can camouflage TCP/IP stack
  - Allows vulnerable systems to evade `nmap` TCP/IP fingerprinting
- How does `nmap` do this?

  > *"Nmap OS fingerprinting works by sending up to 16 TCP, UDP, and ICMP probes to known open and closed ports of the target machine. These probes are specially designed to exploit various ambiguities in the standard protocol RFCs. Then Nmap listens for responses. Dozens of attributes in those responses are analyzed and combined to generate a fingerprint."*

- Top reasons that `nmap` can do this
  - Determining vulnerability of target hosts
  - Tailoring exploits (similar to previous)
  - Network inventory and support (*OK, that could be legit...*)
  - Detecting unauthorized and dangerous devices
  - Social engineering (*Hello, our internal sales database shows...*)

Example `nmap` Usage

```
# nmap -O -v hobo.guitar.fr

Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown:  994 filtered ports
PORT STATE SERVICE
22/tcp open ssh
25/tcp closed smtp
53/tcp open domain
70/tcp closed gopher
80/tcp open http
113/tcp closed auth
Device type:  general purpose
Running:  Linux 2.6.X
OS details:  Linux 2.6.20-1 (Fedora Core 5)
Uptime guess:  11.433 days (since Thu Sep 18 13:13:01 2008)
TCP Sequence Prediction:  Difficulty=204 (Good luck!)
IP ID Sequence Generation:  All zeros
```


Address Hopping

- Periodically change the IP address assigned to a system
  - Makes network scanning/mapping useless to the attacker
    What? How do I know how to connect to a machine?

- A couple of solutions for address hopping
  - Run algorithms on the legitimate communicating machines that produce the hopping pattern
  - Rely on DHCP, if addresses change query DNS for new value
    OK, so the attacker will just use DNS... right?

Managing Deception

- An interesting objective is how to manage deception
  - There are costs and rewards associated with deception
  - *At what point is deception a viable option? Do the rewards have dimensioning returns?*
- Given firewalls, address-hopping, and honeypots
  - *How many of each do you need to perform deception?*
  - *Where should you place honeypots in the address space?*
- Consider deception methods as strategies, then can apply game theory

Title

- Item
- Item
- Item
- Item
- Item
- Item
- Item
- Item
- Item
- Item
- Item

This entire lecture was fake...

or was it?