Designing Deception Operations for Computer Network Defense

Jim Yuill
North Carolina State University
jimyuill-at-pobox.com

Fred Feer
consultant; CIA, RAND, ret.
ffeer-at-comcast.net

Dorothy Denning
Naval Postgraduate School
dedennin-at-nps.edu
Abstract: Deception is an appealing means for computer network defense (CND), as it pits the defender's strengths against the hacker's weaknesses.

This presentation explains how deception operations can be designed and developed for CND. Deception processes, principles and techniques are presented.

The presentation focuses on enduring principles that are of use for conducting deception operations. Applications to honeypot systems are also provided.
Outline

I. Introduction
II. Current deception technology
III. An overview of deception operations
IV. Deception planning
V. Developing the deception story
VI. Conclusion
I.A. The Opportunity for Using Deception

- Deception can pit the defender’s strengths against the hacker’s (e.g., adversary’s) weaknesses

- Hacker’s weaknesses:
  - hackers often rely on a single source of information:
  - the data is easily manipulated
  - the hacker is highly vulnerable to deception

- Defender’s strengths:
  - has physical control of the network
  - knows the network well

- Deception provides an offensive security-measure:
  - it can be used to attack hackers’ decision-making processes
I.B. Deception Principles

• Effectively deceiving an adversary is a job skill

• Presenting processes and principles applicable to all deception operations
  – technology changes, but
  – the principles of reinforcing the desires and perceptions of the deceived will not change
I.C. What is Computer-Security Deception?

• Computer-security deception:
  – actions taken to deliberately mislead hackers and to thereby cause them to take (or not take) specific actions that aid computer security

• Deception aims to:
  – mislead the hacker into a predictable course of action or inaction that can be exploited

• Tricking the hacker, or making him think a certain way,
  – is only a means to an end
I.D. Our Research

• Developed a how-to manual for deception operations
  – Abridged manual distributed for conference
  – Full manual available to DoD personnel (contact Jim Yuill)

• Deception systems R&D
  – two novel honeypot-like systems
  – used honeynet for testing
Outline

I. Introduction
II. *Current deception technology*
III. An overview of deception operations
IV. Deception planning
V. Developing the deception story
VI. Conclusion
II.A. Tools and Techniques

• Honeypots: computers whose purpose is for hackers to break into them

• Honeynet: a network of honeypots

• Honeypot purposes:
  – prevention, detection, response, intelligence

• Other uses of deception
  – firewall stealth
  – steganography, etc.
II.B. Honeynet Example--as seen by hacker
(maintenance backdoor for mainframe network)

Implemented Deceptions, accessible to target

Internet

Intranet

Notional Systems (i.e., non-existent)
Honeynet Example--actual implementation
II.C. Building Honeypots

- **Hacker surveillance:**
  - external to honeypot:
    - firewall logging, traffic sniffing
  - inside honeypot:
    - keystroke logging: sebek
    - shell logging
    - send log records to another computer

- **Hacker containment:**
  - external firewall
  - to be safe: allow connections in, but not out

- **False content:** can be very expensive and difficult
II.D. The *honeyd* Honeypot

- honeyd impersonates computers
  - at unused IP addresses

- can have many fake computers
  - thousands (e.g., by using 10.0.0.0)
  - many more fake computers than real computers

- promising security device, for:
  - prevention: thwart scanning
  - detect scanning
Honeyd’s Impersonations

router

Ethernet switch

honeyd server

real

fake
II.E. Honeyfiles

• Bait files, on network file server
  – e.g., passwords.txt
• Decentralized deployment
• Centralized alarm
II.E. Further Reading

• Honeynet Project
  – http://www.honeynet.org
  – book: *Know Your Enemy*, 2\textsuperscript{nd} edition (not 1\textsuperscript{st})

• Lance Spitzner’s book: *Honeypots*
Outline

I. Introduction
II. Current deception technology
III. An overview of deception operations
IV. Deception planning
V. Developing the deception story
VI. Conclusion
III.A. The Deception-Operation Process

- **Planning**
- **Build the Deception**
- **Prepare to Engage the Target**

**Deception-Operation Development**

**Deploy Deception-Story**

- **Target Engaged**
  - **Target Deceived**
  - **Feedback**
  - **Exploit Target's Response**

**Continuation Decision**

- **modify deception operation**
- **continue deception-operation as is**

**Termination**
III.B. Deception-Operation Development

**Planning**
- Goals and objectives
- Target identification & analysis
- Risk analysis
- Operations security

**Build the Deception**
- Deception story
- Feedback
- Termination plan
- Event-schedule

**Prepare to Engage the Target**
- Exploit for target actions
- Response for problems
- Coordination with network ops
The Deception Story

• *deception story*: induces the target to take the intended action

• presented to the target in his *observation arenas*

• the most effective observation arenas are the target’s intelligence sources
III.C. Engaging the Target

Target Engaged

- Target Deceived
  - story received
  - story accepted
  - intended-action taken

Feedback

- Exploit Target's Response
  - feedback collected and analyzed
  - target's-action exploited
III.D. Deception-Operation Termination

• preparing for the various termination conditions
  – success, failure

• the target often discovers the ruse
  – when his response to the ruse is exploited

• control exposure of the deception operation
  – so it can be used again
  – a cover story may be needed
Outline

I. Introduction
II. Current deception technology
III. An overview of deception operations
IV. Deception planning
V. Developing the deception story
VI. Conclusion
IV. Deception planning

IV.A. Deception opportunity analysis

IV.B. The deception objective

IV.C. Target identification and analysis

IV.D. The target’s intelligence process
IV.A. Deception Opportunity Analysis

• Extend and support the achievement of friendly objectives

• The deception operation should be fully integrated with the overall CND effort

• Compatible with, and coordinated with, the network’s security and production operations
Security Models Reveal Opportunities

Hacking process, from *Hacking Exposed*

1) **Footprinting**
   - Identify area of operation, e.g., network-address ranges

2) **Scanning**
   - Identify computers, OSs, servers

3) **Enumeration**
   - Identify user accounts, file shares, make and type of servers

4) **Gaining Access**
   - Attempt unauthorized access

5) **Escalating Privilege**
   - If only user-access, gain full control

6) **Pilfering:**
   - Search system for clear-text passwords, and trust-relationships

7) **Covering Tracks**
   - Hide tools, clear logs, and remove other evidence

8) **Creating Back Doors**
   - Ensure continued access
IV.B. The Deception Objective

• GEN Dudley Clarke, WWII deception planner
  – ...it became a creed [among deception planners] to ask a General, “What do you want the enemy to do,” and never, “What do you want him to think?”

• The *deception objective* is the desired result of the deception operation; it consists of:
  1. the intended *target action*, and
  2. the *deception exploit*
The Target Action

• The *target-action* is a statement of what the hacker is to do (or not do) at some time and location

• It is always stated in terms of specific actions,
  – “cause the targets’ attacks against our server to be performed, instead, against the honeypot server”

• “have the hacker think that the honeypot server is the real server”
  – is not a target-action, rather, it is a *desired perception*
The Deception Exploit

• The *deception exploit* is a statement of how the target-action will benefit CND
  – e.g., through attack detection, prevention, or response

• **ALWAYS** a positive action
  – what will friendly side do when the target takes the intended action?

• May, or may not, involve a response against the target
  – attack detection that initiates a response, or
  – attack prevention, e.g., deceptively hide network assets
The Deception Operation’s Ultimate Goal

• The deception operation’s ultimate goal:
  – successful completion of the deception exploit

• The deception-story and ruses:
  – just the means for inducing the target-action

• The deception planner can easily be captivated by the ruse’s intrigue,
  – and lose sight of the deception objective
IV.C. Target Identification and Analysis

• *It was so important to the deception work to be able to put oneself completely in the mind of the enemy, to think as they would think on their information, and decide what they would do.*
  – WWII deception planner

• Deception attacks the target’s perception and his thinking process, so

• Deception is more effective with intel on the target:
  – who he is, how he works, and how he thinks
IV.D. The Target’s Intelligence Process

• For the deception operation to work, the target must:
  – receive the deception story, AND
  – interpret it as intended, AND
  – take the target action

• Highly uncertain!
  – but we need certain outcomes, for deception to be useful

• The target’s intel collection:
  – he actively and eagerly seeks info
  – provides a predictable channel for deception story
Exploiting the Target’s Intel Process

• Hacker intel processes and tools are well known, e.g.,
  – port scans (e.g., nmap) and vulnerability scans (e.g., nesus)
  – *footprinting*, social engineering

• Vulnerabilities to deception, in target’s intel process:
  – single sources of information (no cross-validation)
  – info that is superficial and easily misrepresented (e.g., ping)
  – times when target is naïve (e.g., during his initial recon)
  – intel processing by dumb automated agents (e.g., worms)
I. Introduction
II. Current deception technology
III. An overview of deception operations
IV. Deception planning
V. Developing the deception story
VI. Conclusion
V.A. The Deception Story

• \textit{deception objective}: induce a specific target-action that benefits CND

• \textit{deception story}: induces the target action
  – implemented using various ruses

• \textit{desired perception}: a perception, if held by the target,
  – that will cause him to take the intended action

• deception story is an outline of:
  – how the computer system will be portrayed,
  – to cause the target to adopt the desired perception
V.B. The Deception Story’s Essential Design-Criteria

- **plausible**; must appear to the target as:
  - *appropriate*, from engineering and operations perspectives
  - something the defender is *capable* of doing
  - *consistent* with real systems and operations

- **receivable**, by target’s intel
- **verifiable**, if target uses multiple intel sources
- **efficacious**:
  - induces desired perception and target-action.
- **implementable**, by the deception planner
V.C. Design Principles for the Deception Story

Design Principles #1 and #2

1. Inducing the target-action

2. Making the story believable:
   – persuade the target to believe something he expects
   – show things that are normally concealed
3. Preventing the target from uncovering deception

- Minimize falsehood
  - make the story simple
  - weave the story into the truth (powerful verification)
  - show things that are normally concealed
    - by displaying expected indicators

- Minimize the target’s scrutiny of deceptions
Design Principles #4 and #5

4. Ensure the target receives the story
   – use the target’s intelligence sources to communicate the deception story to him

5. Revealing the story:
   – let the target piece the story together by inference
6. Implementing the deception story

• Parts of the story to be implemented, based on:
  – how the target receives the deception story
  – what the target expects to see

• Some parts don’t have to be implemented:
  – parts of the story are tied to the truth
  – parts of the story can be notional
7. Realism in the deception story

• The degree of realism needed is a function of:
  – the target’s intelligence capabilities, and
  – the target’s time available

• Design the story so needed realism is minimized
Outline

I. Introduction
II. Current deception technology
III. An overview of deception operations
IV. Deception planning
V. Developing the deception story
VI. Conclusion
Deception-Operation Development

Planning

Build the Deception

Prepare to Engage the Target

Deploy Deception-Story

Target Engaged

Target Deceived

Feedback

Exploit Target's Response

Continuation Decision

modify deception operation

continue deception-operation as is

Termination

VII. Conclusion
Deception: Ends vs. Means

• Computer-security deception:
  – actions taken to deliberately mislead hackers and to thereby cause them to take (or not take) specific actions that aid computer security

• The \textit{deception objective} is the desired result of the deception operation:
  – the intended \textit{target action}, and the \textit{deception exploit}

• \textit{The deception story}: creates \textit{desired perception}

• Communicate deception-story via target’s intelligence process
Current and Future Research

• Completed
  – How deceptive hiding works (for CND, also OP-SEC)
  – Psychological vulnerabilities to deception
  – Deception bibliography for computer security

• Jim Yuill
  – Battlefield intel process (IPB) applied to network security
  – R&D to extend honeyd deception
  – Managing data collected during investigation: intel, computer security, etc.
  – Problems in academic computer-science research methods
Authors

• **Jim Yuill** is a senior PhD student in the Computer Science Department at North Carolina State University. This paper is part of his dissertation. Jim previously worked at IBM in operating systems development. *jimyuill-at-pobox.com*

• **Fred Feer** is retired from a career with the U.S. Army counterintelligence, CIA, RAND and independent consulting. Deception has been an interest and area of professional specialization for over 40 years. *ffeer-at-comcast.net*

• **Dr. Dorothy Denning** is a Professor in the Department of Defense Analysis at the Naval Postgraduate School. She is an ACM Fellow, and the recipient of several awards, including the National Computer Systems Security Award. *dedennin-at-nps.edu*
Survival in a Sea of Deception
Part One

Deception: Why
Darwinian Deception

As a species, our ability to adapt to changes in the environment, avoid threats and outwit competition has been the key to our survival and dominance.

The realities of the universe we inhabit insure that witting adaptability remains at the heart of survival.

Who deceives may not always win but the chances are better and the losses will be lower.
Uncertainty Prevails

- Time
- Randomness
- Parallelism
- Interactivity
- Uncertainty
- Necessity of Action
Example #2
Ancient Wisdom

It is well to hurt the enemy by deceit, by raids or by hunger and never be enticed into a pitched battle, which is a demonstration more of luck than of bravery.

Maurice, The Strategikon, 6th century

Battle should only be offered if there is no other turn of fortune to hope for, as from its nature the fate of battle is always dubious.

Napoleon Bonaparte, 1809
Current Wisdom

“…the empirical fact of nonlinear dynamics, when coupled with the unavoidable mismatches between reality and our representations of it, reveal fundamental limits to prediction, no matter how much information and processing power technological advances may one day place in human hands.”

Why Do Deception?

Good: to survive

Better: to control/reduce uncertainty

Best: to seize and exploit an advantage
So, Why Isn’t Everyone Doing it?

✦ First, everyone who can does
✦ To do it poorly may be worse than not trying at all.
✦ It requires competence at all levels
✦ It means acceptance of risk and responsibility
The wages of Deception

Chances of a Successful Battle
With and Without Deception

<table>
<thead>
<tr>
<th></th>
<th>All Battles</th>
<th>No Deception</th>
<th>Deception Tried</th>
<th>Successful Deception</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Battles</td>
<td>104</td>
<td>64</td>
<td>38</td>
<td>13</td>
</tr>
<tr>
<td>Successful Battles</td>
<td>19</td>
<td>8</td>
<td>11</td>
<td>9</td>
</tr>
<tr>
<td>% Success</td>
<td>18.3%</td>
<td>12.5%</td>
<td>28.9%</td>
<td>69.2%</td>
</tr>
</tbody>
</table>
The Three Kinds of Knowledge

- **Type I:** Facts--things known
- **Type II:** Unknown facts--things not known, but knowable, i.e., somebody knows
- **Type III:** Facts Unknowable--because no one does or can know them because they don’t exist or are contingent.
Examples & Lessons

_mob D-Day
_mob Ticket Sales
_mob The Left Hook/Hail Mary
_mob The Bottom Line
Part Two

Deception: what to think about
Contemporary Military View

The profundity and exactness of the commander’s foresight in a battle directly depends on a degree of creativity demonstrated by the sides and their use of stratagems, camouflage and disinformation.

MGEN I. Vorobyov. Tactics as the Art of Command and Control in Military Thought, v 12 n 1, 2003, p 58. (English edition published by East View Publications, Minneapolis MN)
WW II Deciever’s View

Provided the enemy has an efficient intelligence service, provided he is capable of reacting to what he sees, or thinks he sees, he can apparently be taken in again and again.

Sherman on His March

“I must have alternates, else, being confined to one route, the enemy might so oppose that delay and want would trouble me, but, having alternates, I can take so eccentric a course that no general can guess at my objective. Therefore, when you hear I am off have lookouts at Morris Island, S.C., Ossabaw Sound, Ga., Pensacola and Mobile Bays. I will turn up somewhere.”

Sherman’s Alternates
What Do You Need to Know

- Who is the target
- What do you know and not know about him
  - Is he alert for deception
  - Has he practiced deception
- What has his record been
  - re: deception--use, results
  - re: success of his enterprise
- What do you need to know to present a credible story
- If we go ahead on what path does that put us?
Hackers, Attackers, Intruders, Crooks, Thieves and Terrorists

What do we know about them?

Some intruders are more threatening than others. Can we sort them out?

Defense should be proportional to the threat.

Until we know enough to sort them along a spectrum, we’re throwing mud at a wall.
Ethics

Clean house first--major security problem is internal personnel, training and admin

Is it OK to lie to liars?

Responsibility
Lying

Deception necessarily involves manipulation of the Truth

Is that always lying?

What justifies lying to the public?
Wanted: Real Damsel

"It’s no use... We’ve just got to get ourselves a real damsel."