

Why Security Through Obscurity Isn't

A primer on saving your sanity while trying to save somebody else's butt.

“The only defense against the world is a thorough knowledge of it.”

-- John Locke

treachery
unlimited



Where Are We Going...and Why Am I in This Handbasket?

“Without disclosure, there is no truth. Without truth, there is no accountability.”

-- Richard Thieme

treachery
unlimited



Where are we going & why am I in this handbasket?

- **Target Audience**

- Newly-Ordained System Administrators
- Experienced Admins whose so-called superiors “just don’t get it”
- Any hacker who doesn’t want to see their livelihood and liberty destroyed by their elected representatives who “just don’t get it” either

treachery
unlimited



Where are we going & why am I in this handbasket?

- **The Problem**

- Computer security types held to grim double-standard
 - If there are no intrusions, you're superfluous
 - If there are numerous intrusions, you're incompetent
 - Regardless of outcome, you're eventually seen as a waste of resources
- Consequence: exceedingly difficult to get support for genuine security practices and the notion of Security Through Obscurity (STO) gains acceptance.

treachery
unlimited



Where are we going & why am I in this handbasket?

- **Definition of Security-Through-Obscurity**

“...[T]he notion that the opponent will always be less intelligent than the defender; and that said opponent who otherwise follows a criminal lifestyle will suddenly become a law-abiding citizen whenever a new law is passed.

“This isn’t a security policy; it’s institutional hubris.”

from the [in]famous “Okay, Joke’s Over” memo - 1998

treachery
unlimited



Where are we going & why am I in this handbasket?

- **Examples of Security-Through-Obscurity**

- Service banner alterations & non-standard port use
- Singular reliance on firewalls, proxies and NATs
- Juvenile belief of immortality
- Opposition to full disclosure and Open Source
- Carnivore and other “Black Box” technologies
- Digital Millennium Copyright Act (DMCA)
- Security Systems Standards and Certification Act (SSSCA)

treachery
unlimited



Where are we going & why am I in this handbasket?

- **How Do Most People Cope?**

- Fear, Uncertainty and Doubt (FUD)

- Claim a threat to National Security
- Insist that penetration testing tools are disasters in waiting
- Outlaw reverse engineering and decompiling

- Reactive (rather than proactive) security measures

- “Law enforcement will protect us.”
- “If it ain’t broke, don’t fix it. ...and it’s not broken unless I say it’s broken!”
- Snake oil “security solutions”

treachery
unlimited



Up Close and Critical

Recognizing and Rebuking STO Practices

“It will not follow that everything must be suppressed which may be abused... If all those useful inventions that are liable to abuse should therefore be concealed, there is not any Art or Science which may be lawfully professed.”

-- Bishop John Wilkins, 1641

treachery
unlimited



Up Close and Critical

- **What STO is and why it doesn't work**

- Service banner alterations & non-standard port use

- Ill-begotten notion that if you rename or relocate your service, the potential intruder will get confused and go away
- Obscurity is typically used in lieu of a robust security solution. This in itself compromises the security model more than any other factor.
- Doesn't do squat with automated intrusion agents (worms)
- Tools such as Nessus and Retina see right through the ruse
- OS fingerprints give away likely vectors of attack
- Scriptkiddies just blast away until something cries "Uncle"
- Skilled intruders look at obfuscation as a challenge

treachery
unlimited



Up Close and Critical

- **What STO is and why it doesn't work**

- Singular reliance on firewalls, proxies and NATs

- Operating under the Myth of the Maginot Line
- These technologies are great, but only when properly configured, used in concert with robust NIDS, and somebody's watching the logs regularly
- Proxies and NATs are just one more NIC in the loop when allowing services in; if it's reachable, it's breachable
- TCP scans may be blocked, but UDP typically sneaks through
- Every firewall ships with Port 53 TCP/UDP open; and loads of folks think their BIND DNS is "safe" because of the firewall

treachery
unlimited



(I'm sure these guys thought a firewall was "good enough"...)

OAKTREE

IF YOUR PASSWORD IS ON THIS
LIST YOU NEED TO CHANGE IT AND
STOP USING PLAINTEXT PASSWORD PROTOCOLS

!polpot	1999g4Ør76	%07048d
88fafa	nc5mnpvx	Mus!cals
D3mk165f	pclS132	
ab1234	sdf	
adfjk	Surfpw	
otacrew	vermin99	
bingo	yqzMZPJg	
bingo1999	cisco1	
cardedeu	mØsquitØ	
dkfjd	blahblah	
enrico	rafa-baw2	
hello	soogjksjka	
jik488	dances	
ju1cyb1ts	:Apf!	

treachery
unlimited



toorcon -- 09/2001

Up Close and Critical

- **What STO is and why it doesn't work**

- Juvenile belief of immortality

- By “juvenile,” I mean the bravery of the inexperienced
- Optimists are pessimists who haven't learned their lesson yet
- “We haven't been hacked in years. We're safe forever.” (No, you're due...if you haven't been quietly breached already.)
- “We're too small of a target to be interesting to an attacker.” (You don't have to be a big name...you just have to have big holes in your systems.)
- “Nobody knows enough about our system to attack it!” (Einstein once said, “Imagination is more important than knowledge.” This is absolutely true -- a skilled attacker can still breach your systems with little direct knowledge.)

treachery
unlimited



Up Close and Critical

- **What STO is and why it doesn't work**

- Opposition to full disclosure & Open Source

- Insistence that full disclosure is a threat to security (ridiculous, considering that nearly every vendor doesn't recognize a security problem until *after* proof-of-concept is released)
- Society should *never* limit its law-abiding citizens' rights based on what the maladjusted *might* do.
- Operating under the assumption that because something costs, it's worth more than something that's free (as evidenced by government sector COTS solutions rather than exploration of Open Source, no matter how superior the Open Source product may be)

treachery
unlimited



Up Close and Critical

- **What STO is and why it doesn't work**

- Carnivore and other “Black Box” technologies

- Even the “critical review” of Carnivore was a joke. The Bureau stipulated that the reviewers had to “assume proper usage” (and precisely *how* are problems supposed to be found when ignoring *improper* usage?).
- The FBI insisted that Carnivore was secure, yet was adamant that releasing its internals would leave it vulnerable to attack. (High indication that its “security” was a house of cards.)
- Even with the closed architecture, it only took a bit of ingenuity for Network ICE to write Altivore which probably does the same thing as Carnivore, but in a more secure manner

treachery
unlimited



Up Close and Critical

- **What STO is and why it doesn't work**

- Digital Millennium Copyright Act and the coming Security Systems Standards and Certification Act

- The bane of every Constitution- and technology-loving citizen!
- Criminalizes publication of research and proof-of-concept code which is deemed unflattering to snake oil “security solutions”
- Criminalizes decompiling, disassembly & reverse engineering
- Ewscray Ooyay Dobe-Ay (if they try to decipher that, someone please have them hauled into court under the same statute by which Dmitry was busted)
- As if that wasn't enough, Senator Hollings now proposes SSSCA which will do to PC hardware what the RIAA did to Napster...and, because of DMCA, no critical review of the “solution” will be possible

treachery
unlimited



Up Close and Critical

- **Dear God, that's some grim stuff**
 - So what can be done to overcome all this?
 - Thankfully, there *are* solutions!



treachery
unlimited



t o o r c o n - - 0 9 / 2 0 0 1

Rx: The Red Pill



(Or, “Do you want real security,
or a security policy on drugs?”)

treachery
unlimited



t o o r c o n - - 0 9 / 2 0 0 1

Rx: The Red Pill

- **Step 1: Wake Up!**

- False Class Consciousness --Marx, 1846

- The bourgeoisie perpetuate ideology so proletariat believe they're equal to those who run their lives. Similar story here.

- False Security Consciousness

- Industry perpetuates an ideology that they are blameless for their own mistakes (ever read a license agreement?)
- The users end up believing that industry is without fault and it's those "wily hackers" who are ruining everything
- Most importantly, we can no longer assume a quiet voice of reason will be heard; we have to register our objections loud enough for our reps to undeniably hear!

treachery
unlimited



t o o r c o n - - 0 9 / 2 0 0 1

Rx: The Red Pill

- **Step 2: Read Up!**

- **The brain, security, and liberty are like a muscles -- use them or lose them**

- Follow and support open source and full disclosure mail lists
- Your future is based on lessons from the past. Where possible, learn as much history as you can (and if you find that too dry, at least make a point of learning the history of warfare)
- Keep up on current technology events. People are making decisions for you in the U.S. government. Suffice it to say that they don't have your interests at heart; only their own.
- *Do something!* Lead, follow, or get out of the way.

treachery
unlimited



Rx: The Red Pill

- **Step 3: Speak Up!**

- **Aggressively insistent on fiat security over FUD**

To illustrate: Our economy is based on fiat currency. Money is not based on gold or silver, but on consumer faith. Counterfeiting is aggressively pursued not due to real damage to the economy by additional dollars, but because counterfeiting could precipitate a loss in consumer confidence

- **Security systems should function like a good cryptosystem:**

- Multilayered; redundant risk mitigation
- Not compromised when its internals are revealed

treachery
unlimited



Rx: The Red Pill

- **And finally...**

- **Fight the FUD**

For every person who insists that a hacker is just a potential criminal; for every person who insists that open source and open security models are a venue for criminal conduct, simply remind them of a few simple and inescapable truths:

- Every locksmith is a potential burglar
 - Every cop is a potential robber
 - Every soldier is a potential mercenary

...BUT HOW MANY ARE?

treachery
unlimited



Useful Links

- **Latest version of this presentation**
<http://www.treachery.net/~jdyson/toorcon2001/>
- **SecurityFocus (home of multiple security lists)**
<http://www.securityfocus.com/>
- **Nessus Vulnerability Scanner**
<http://www.nessus.org/>
- **eEye Retina Scanner**
<http://www.eeye.com/>
- **Cryptography List**
majordomo@wasabisystems.com (subscribe cryptography)

treachery
unlimited

