

Mudge aka Peiter Mudge Zatko

BBN Technologies



BLACK HAT BRIEFINGS

Economics, Physics, Psychology and How They Relate to Technical Aspects of Counter Intelligence/Counter Espionage Within Information Security

The computer and network security fields have made little progress in the past decade. The rhetoric that the field is in an arms race; attacks are becoming more complicated and thus defenses are always in a keep-up situation makes little sense when 10 year old root kits, BGP and DNS attacks that have been widely publicized for years, and plain-text communications streams are still being taken advantage of. This talk looks at the environment without being skewed by currently marketed solutions. It then presents corollaries for environments in different disciplines, such as economics and physics, talks to certain psychological situations that prohibit researchers and organizations from being able to correctly address the problems, maps these solutions into Counter Intelligence and Counter Espionage models and finally applies them to low level network and systems communications. This presentation involves audience participation to point out ways of breaking the helplessness cycle (for the defensive side) or to better target areas for exploitation (for the offensive side).

"Mudge" Peiter Mudge Zatko

Better known as Mudge, the hacker who testified to the Senate that he could "take the Internet down in 30 minutes", Zatko has been a pioneer of the commercial information security and warfare sector since the 1980s. The leader of the hacker think-tank "LOpht", he founded @stake and Intrusic and currently works as a Division Scientist for BBN Technologies (the company that designed and built the Internet).

Mudge is the creator of LOphtCrack - the premier MS password auditor, SLINT - the first source code vulnerability auditing system, AntiSniff - the first commercial promiscuous system network detection tool, and Zepho - Intrusic's flagship product focused on Counter Intelligence / Counter Espionage for corporate Insider-Threat. His other software works are now included in several distributions of commercial and public domain operating systems.

As a lecturer and advisor Mudge has contributed to the CIA's critical National security mission, was recognized as a vital contributor to the success of the President's Scholarship for Service Program by the NSC, has briefed Senators, the former Vice President and President of the United States, and has provided testimony to the US Senate multiple times.

An honorary plank owner of the USS McCampbell and referenced as part of 'U.S. History' in Trivial Pursuit, his mission remains constant to "make a dent in the universe".

*Physics, Psychology, and
Economics as applied to
Counter Intelligence / Counter
Espionage InfoSec*

Mudge

Division Scientist BBN Technologies
{mudge@bbn.com, mudge@uidzero.org}

Background

L0pht

EOP
Executive Office of the President

Georgetown University

DoD

OST/P
Office of Science and Technology

CIA

@stake

DPC
Democratic Policy Committee

Dept. of the Air Force

Dept. of Commerce

M.I.T.

PCIP
Partnership for Critical Infrastructure Protection

NSA

NSA

BBN

Dept. of the Navy

U.S. Senate

Intrusic

Dept. of the Army

U.S. House of Representatives

FBI

JCS

Contributions to the Field

- L0phtCrack (aka LC4)
- AntiSniff
- L0phtWatch
- NFR (IDA)
- Zephon
- SLINT
- First explanations and public presentation of how to write buffer-overflows
- MonKEY
- DragonBallz
- Kerb4 - Kerberos Auditing tool
- Sculpting of MS security response organization
- Forced Intel to create security response procedures and channels
- Considered one of the fathers of 'Advisories'
- Crontab local root Advisory
- Modstat local kmem advisory
- Sendmail 8.7.5 advisory
- Test-cgi remote inventory advisory
- Imapd local shadowed password file retrieval advisory
- Solaris getopt(3) Elevated Privileges advisory
- RedHat 6.1 Init Scripts Race Condition advisory
- Cactus Software Shell-lock cipher to plain-text retrieval
- Security Analysis of the Palm Operating System and its Weaknesses Against Malicious Code Threats
- Initial Cryptanalysis of the RSA SecurID Algorithm
- Cryptanalysis of Microsoft's PPTP Authentication Extensions
- Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol
- Etc.
- Etc.

•Recognized as a vital contributor to the success of the President's Scholarship for Service Program by the National Security Council, Executive Office of the President

Psychology (1)

Functional Fixation and Learned Helplessness



Answering Machines



Cell Phones
(scanners, tracking,
clocks, capabilities)



Lo-Jack



Coins

Who {was,is} Mudge?

Psychology (2)

The Finality of Initial Spin
(implied biased interpretation)

- Advisories and Tools
 - L0phtCrack - LC4 - John the Ripper
 - Bo2k - PC Anywhere - VNC
 - ISS - Virus/Worms
- Presentations semantics
 - Passive vs active voice
 - Vendor security warnings

How important is Functional Fixation again?



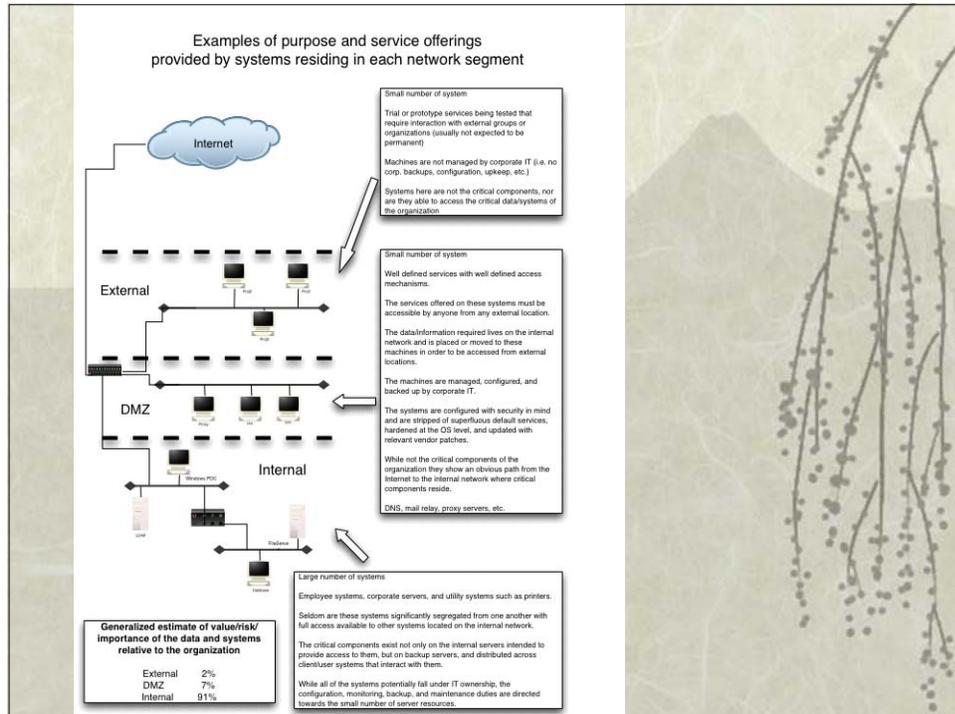
How Serious is Functional Fixation?



Intrusion v Attack v Compromise

Attacks draw unwanted attention. It is, and always has been, preferable in most situations to use credentials that are permitted on a system - however those credentials are obtained. This way, there is no actual “attack” as far as IDS would classify it.

Like a mole in a government agency, the greatest value is achieved through unnoticed longevity in the target environment. The expected movement and characteristics of information and it’s handling related to business functions must change in these cases and provides us the ability to identify such covert activities. Profiling the business functions and their information flows on the internal network is the important component, not profiling the people.



Misperceptions

Corrections

Entry to critical (ie Internal) environments is accomplished through overt and directed attacks.	Greater than 90% of illicit entry is opportunistic and accomplished through "piggy-backing" through authentication mechanisms and subsequently hiding of internal presence. [no attack takes place and activity is not abnormal]
Detection is accomplished through identification of attack while in progress.	[see above -- additional ref phys laws] Even overused FBI/CSI reports show internal compromise as the majority of problem... even if attack potentially is the method employed, it is a fraction of the duration posed by the risk and compromise.
Systems are the critical components at risk.	data and/or information, along with active or passive uses of it are the critical components at risk.
Profiling - anomaly detection is based upon mapping and/or modeling users and alarming when inappropriate behavior is seen.	network and system data movement and handling follow standard information theory - this highlights problems which are easily mapped back to actors/agents.
Once inside, further access to systems is achieved via subsequent attacks.	Once inside, further access is granted and requires little to no effort.
The attacker has the advantage, the defender is at a disadvantage.	In almost all segmented deployments, the defender is at a tremendous advantage. [CI/CE/Art of War/etc models correct]

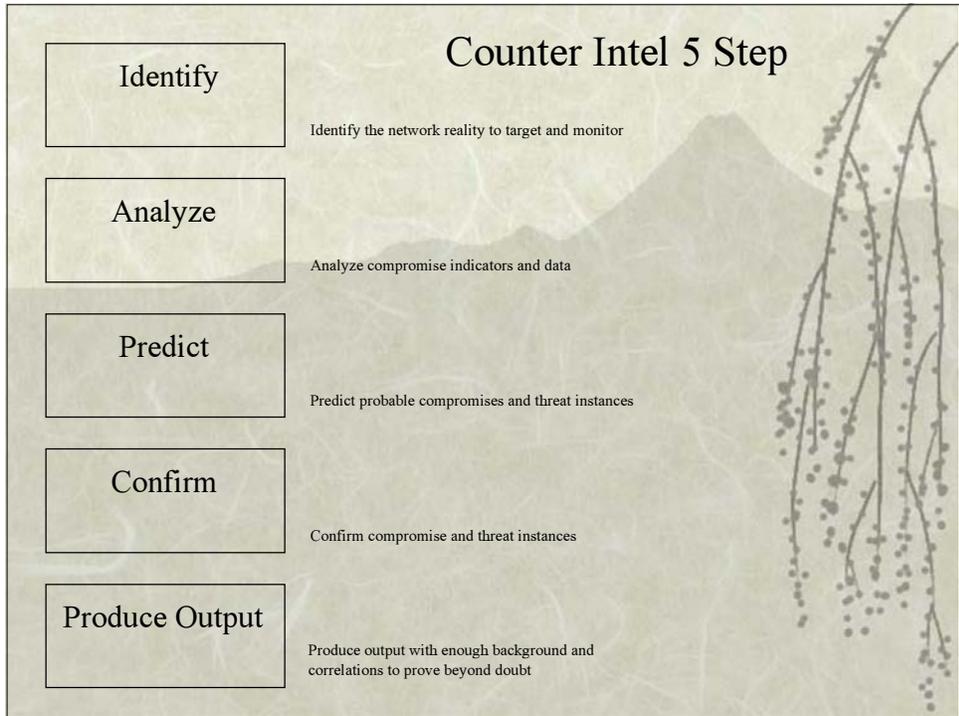
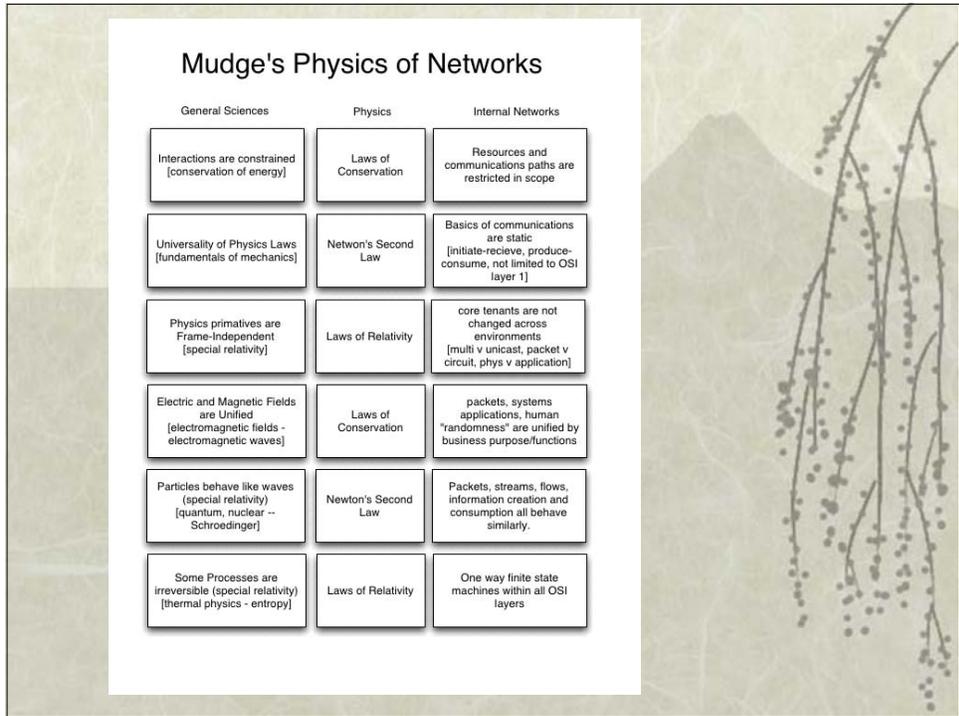
Current Environment

Intruders are already inside most corporations often sitting on key components of critical infrastructure usually without knowledge of exactly what they are in control of
accidental catastrophic failure is possible
intentional catastrophic failure is possible

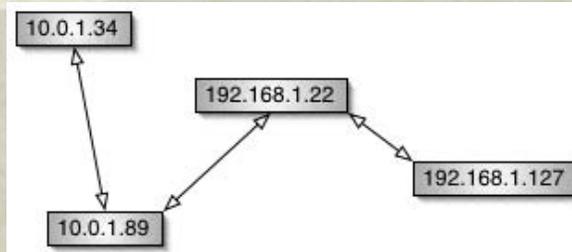
Passive control of systems is much more desirable than disruption or damage without purpose

Target selection is opportunistic
The selection is often acquired from within a large selection of systems, usernames, and passwords of already compromised systems
vpn - scanning DSL/Cable/Dialup - [also known as Island Hopping] [sniffed credentials of corporate accounts accessed from schools/universities [Fluffy Bunny demonstrated and documented this in his compromise of Akkamai, and other substantial environments]
shell systems or other large user-base machines through trojan'd binaries/applications
sniffed credentials obtained via compromised systems at ISPs

Passive control and tools have not changed much since pre 96
Cloaking tools have not changed much since pre 96



Stepping Stones



Interactive vs Non-Interactive

Small data packets making up most of the “server’s” data

Large deviations / variances in the time span between packets

Both large and small data packets making up the “client’s” data stream where there are distinct groupings of large vs small.

Conversational Statistical Analysis

- Only useful anomaly detection
- Based on subset of protocol(s)
- Can include non-critical violations as acceptable
- Maps real world communication syntax as opposed to theoretical RFC violations
- Basis of real world cryptanalysis

Relative Frequencies of Letters in General English Plain text
From Cryptographical Mathematics, by Robert Edward Lowand

Letter	Frequency	Letter	Frequency
a	0.08167	m	0.06749
b	0.01492	n	0.07107
c	0.02782	o	0.19219
d	0.04253	p	0.00095
e	0.12702	q	0.01987
f	0.02228	r	0.06327
g	0.02015	s	0.09058
h	0.06084	t	0.07758
i	0.05966	u	0.00978
j	0.00153	v	0.02160
k	0.00772	w	0.03150
l	0.04025	x	0.01974
m	0.02406	y	0.00074

Tom's Letter Frequencies (in order)

By analyzing roughly 15000 characters, or roughly 2700 words from three separate sources, Tom came up with the statistics below. The three sources were:

- The license agreement from Sun for JDK 1.2.1
- The teaching philosophy of a computer science professor from a liberal arts college in Minnesota.
- A letter of recommendation for a national competition for innovative uses of technology in collegiate teaching.

General Letter Frequencies

a	0.124187	m	0.0281775
b	0.0002215	n	0.0211895
c	0.0229031	o	0.0283121
d	0.0788932	p	0.0182182
e	0.0740951	q	0.0111888
f	0.0714095	r	0.0332251
g	0.0700789	s	0.0214827
h	0.0608112	t	0.0189181
i	0.0488308	u	0.00320319
j	0.0018709	v	0.00218684
k	0.0110386	w	0.0019984
l	0.0344391	x	0.0009237
m	0.028777	y	0.000199

The top ten letters with frequencies, which occur at the beginning of words:

Start of Word Letter Frequencies

Letter	t	a	i	s	c	d	e	m	f	p	w
freq	0.1394	0.1535	0.0821	0.0725	0.0712	0.0597	0.0426	0.0409	0.0401	0.0382	

The top ten letters with frequencies, which occur at the end of words:

Letter	e	i	o	u	a	r	l	t	f
freq	0.1917	0.1435	0.0923	0.0884	0.0786	0.0730	0.0693	0.0487	0.0450

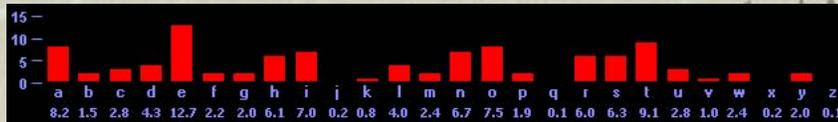
The most common digrams (in order):

th, he, in, en, nt, re, er, an, ti, es, on, at, se, nd, or, ar, al, te, co, de, to, ra, et, ed, ll, sa, em, ro,

The most common trigrams (in order):

the, and, tha, ent, ing, om, in, for, nde, has, nce, ebt, ll, uR, th, men

Source <http://www.central.edu/homepages/Lint.txt/classes/spring01/cryptography/letterfreq.html>

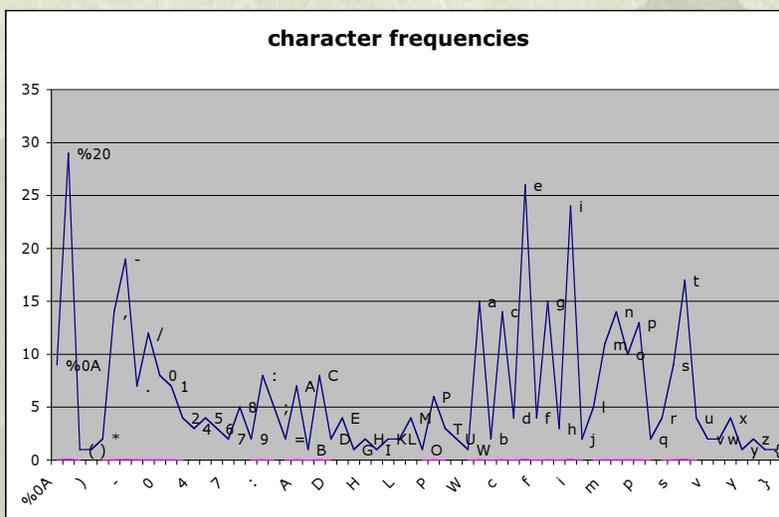


Source http://www.simonsingh.net/The_Black_Chamber/frequencyanalysis.html

Headers (Conversational Analysis)

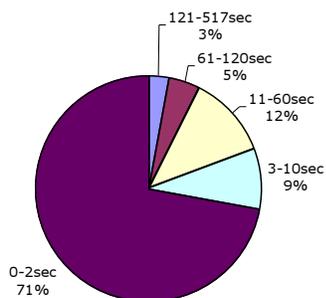
```
GET / HTTP/1.0
Connection: Keep-Alive
User-Agent: Mozilla/4.75C-CCK-MCD {C-
  UDP; EBM-APPLE} (Macintosh; I; PPC)
  OmniWeb v496
Host: 127.0.0.1:8080
Accept: image/gif, image/x-xbitmap,
  image/jpeg, image/pjpeg, image/png,
  image/tiff, multipart/x-mixed-replace, /;q=0.1
Accept-Encoding: gzip, identity
Accept-Charset: iso-8859-1, utf-8, iso-10646-
  ucs-2, macintosh, windows-1252, *
Accept-Language: en, *;q=0.5
```

Protocol Headers / Constants



Session Durations

HTTP Session Durations (from 7543 total sessions)



Some a-priori beliefs...

System	Initial a-priori beliefs (selected)
Generic System	<ul style="list-style-type: none"> Does not change MAC address Does not fragment local packets Does not send or receive packets out of order Consistently sets initial TTL value Client ports are allocated above 1023 Does not run well-known services on ports other than their assigned number Predominantly does not send bad TCP cksums Used for well-defined purposes that are persistent over time OS fingerprints do not change Etc.
Client System	<ul style="list-style-type: none"> Initiates network requests Is primarily a data consumer Repeatedly accesses the same servers / services Predominantly uses non-interactive services Does not engage servers simultaneously for small to medium size transfers Consumes data in bursts Acts as a client (or peer) Does not access other clients as servers Etc.
Microsoft Clients	<ul style="list-style-type: none"> Use MS services like Netbios, SMB, etc. Etc.
Unix Desktop	<ul style="list-style-type: none"> Does not use MS services except for SMB/CIFS Uses Unix services and protocols (IP printing, NIS, unix RPC, etc.)
Server	<ul style="list-style-type: none"> Does not access clients as servers Is a limited client (DNS, Etc.) Does not use DHCP Etc.
Users	<ul style="list-style-type: none"> Do not perform system administrator functions, eg: mount IPC\$ shares, reset passwords for others, etc. Etc.
System Administrators	<ul style="list-style-type: none"> Do not perform user functions, e.g.: engage in workflows, access certain databases, etc. Do not perform sys-admin functions from remote machines Etc.
Data Objects/Flows	<ul style="list-style-type: none"> Almost always direct transfers (no "stepping stones") Almost always immediate (not store and forward) Almost always non-interactive Almost always accessed as sub-elements (exception: full backups)

Why Security As We Know It Does Not Exist

Vulnerability Scanning - Keeping up to date on Patches
Host Based Intrusion Detection -Network Based Intrusion
Detection

...
Who cares???

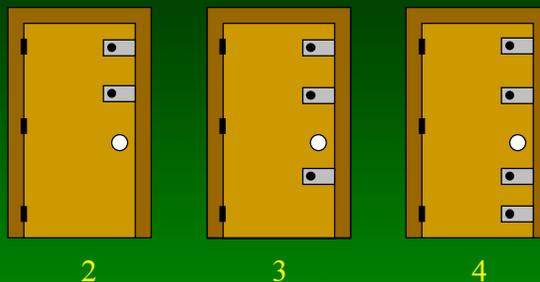
Why Security As We Know It Does Not Exist (cont)

Try this:

- ◆ No Foreign
- ◆ NNPI
- ◆ NOCONTRACT
- ◆ NRWAN
- ◆ SIPRNET
- ◆ WINTEL
- ◆ BETIS
- ◆ SECRET
- ◆ CONFIDENTIAL
- ◆ ATDT
- ◆ [0-9][0-9][0-9]-[0-9][0-9][0-9]
- ◆ Modem
- ◆ Password
- Login
- Username
- Dialup
- PPP
- .pwl
- Sam files
- Sdi files
- Config files
 - Systems
 - Routers
- INPO

Examples: NY power outage,
Telco, DoE/NERC/NRC, etc.

Problem Solving Basics: Locksmithing-101 Opening a Door That has Spring Latches



Solution:

- Pull on door knob and hold tension on it
- Unlatch L#1 and release
- Unlatch L#2 and release
- Repeat: going through all latches until door opens

Mudge's example to the FBI-QuanticoHQ / NSA - 2000

