Bulletproof IT Security: Unclassified Secrets of the NSA

by Gary S. Miliefsky,
Executive Producer,
CyberDefenseMagazine.com

Brought to you by NAISG.org
A moment of silence...

Terror Attack on the Boston Marathon
Innocent civilians murdered on April 15, 2013

“I laugh because I must not cry, that is all, that is all.”
- Abraham Lincoln, 16th POTUS
murdered on April 15, 1865
About Me

Executive Producer of Cyber Defense Magazine
Former Lead Cover Story Writer for Hakin9
Founder of NetClarity, a BYOD/NAC Company
Founding Member of US Department of Homeland Security

Board and Advisory Membership
National Information Security Group (NAISG.org)
Norwich.edu Cyber-war Research Labs
Informal Advisor to White House.gov PCIPB
MITRE’s CVE – Global standard for vulnerability information
Maybe I’m the NAISG April Fools Speaker?

Let’s get our definitions straight:

UNCLASSIFIED – ie in the public domain, accessible to the public. Not “DECLASSIFIED” and not “CLASSIFIED”, hence non-government access without the need for a FOIA request.

SECRETS of the NSA – hold on a sec! How can they be secrets if they are UNCLASSIFIED? But....

THE CATCHY TITLE GOT YOU HERE, DIDN’T IT? HE HE HE....

So to be fair, I will do my best to deliver (exactly what, thought?)
COMEDY IS MEANT TO OFFEND... THAT'S HOW MOST HUMOR WORKS.

LIFE IS SHORT AND HERE IN BOSTON WE EXPERIENCED A TERROR ATTACK THIS WEEK SO I HAVE CHOSEN TO LIGHTEN UP MY SLIDES AND MAKE THEM “DARK HUMOR”....

IF YOU FIND ANY OF THE FOLLOWING SLIDES TOO OFFENSIVE, THEN DO NOT VIEW THEM, DELETE YOUR ACCESS TO THIS SLIDESHOW AND MOVE ON, PLEASE.

“I laugh because I must not cry, that is all, that is all.”
- Abraham Lincoln, 16th POTUS murdered on April 15, 1865
So I won’t be telling you about these CLASSIFIED programs as you don’t have proper clearance:

THE S3 PROJECT:  
Squirrel Super Soldier

Genetically modified squirrels with an incredible I.Q. score, performing missions for the US government for two reasons:  
a) Love of Country and b) Free Nuts
So I won’t be telling you about these CLASSIFIED programs as you don’t have proper clearance (cont’):

THE UBP PROJECT: Underwater Border Patrol

Genetically modified Chihuahuas with an incredible I.Q. score, performing joint missions for both the Mexican and US governments to:
a) Ensure our waters are safe b) Befriend dolphins and other sea creatures

PROJECT CANCELED ON 3/1/2012 AS MANY OF THESE CHIHUAHUAS WENT AWOL AND ILLEGALLY CROSSED INTO CANADA THROUGH LAKE ONTARIO
Or how this CLASSIFIED NSA program failed miserably:

THE GAMMA RAY PROJECT:

Create a super soldier by dousing him with high amounts of Gamma Radiation. End results – uncontrollable rage, always chasing cars and then biting into their bumpers and then throwing them at least 50-100 yards. Highly dangerous. Project canceled.

PROJECT CANCELED ON 4/1/2013: LAST KNOWN SUPER SOLDIER WHEREABOUTS UNKNOWN
Or how NSA wiretapping helped capture this terrorist:

SHIEK BOOMBOOM ALMEEYOW:

Caught dining at the Whitehouse and the Pentagon. Location discovered through Wiretapping...POTUS authorized Drone attack! Collateral damage: 3 of his kittens were in his apartment when the Drone struck. There were no survivors.
Or how one of our top NSA agents went rogue:

Agent Smith:

Stole highly classified government secrets. Whereabouts: Last seen in Orlando. We usually hid top secret information in USB sticks that looked remarkably like cheese.

NEW USB Stick – redesigned on 4/1/2013 since the “Smith Incident”

Folio: see MIAC report, possible Tea Party member, formerly Patriotic decorated Veteran, potential domestic terrorist...be on the lookout for anyone who purchases CHEESE at Walmart – if you see something, say something.
Look at The Current Stats....

Cybercrime up by 6% through January 1, 2013
(Source: PONEMON INSTITUTE)  

WhiteHouse Hacked by China
(Sources: WHITEHOUSE.GOV and PENTAGON.MIL)

ADOBE UPDATE SERVER – RECENTLY HACKED
MICROSOFT INTERNET EXPLORER – RECENTLY HACKED
ORACLE – RELEASES OVER 110 SECURITY FIXES IN THE LAST QUARTER

Total Personally Identifiable Information Records Stolen (US): 607,472,154+
Total Common Vulnerabilities and Exposures (CVEs aka “holes”): ~56,000
Total MD5 Hash Entries in Top Anti-virus Databases: 120,000,000+ and growing
(Sources: CDM, Adobe, Microsoft, Oracle, MITRE, PrivacyRights.org, VirusBulletin)
Bulletproof IT Security Best Practices: NSA Recommends...

Here's the NSA best practice list, in order of importance:

1. Roll out corporate security policies
2. Deliver corporate security awareness and training
3. Run frequent information security self-assessments
4. Perform regulatory compliance self-assessments
5. Deploy corporate-wide encryption
6. Value, protect, track and manage all corporate assets
7. Test business continuity and disaster recovery planning
New Idea – Does Your Supply Chain Matter? The NSA believes so...

If you BUILD or even BUY IT Networking and Security Equipment, have you checked the supply chain?

• Walmart ships picture frames infected with zero-day malware from China
• Spyware found on Brand New ‘blank’ USB sticks built in China
• Microsoft uncovers Nitol botnet which shipped on “new” PCs from Distribution partners throughout USA who purchase their equipment from China in the last quarter of 2012
• Huawei and ZTE Equipment may ship with remote ‘eavesdropping’ technology from China – US House Intelligence Panel, Q4, 2012

In balance, the USA’s NSA.gov has admitted (through EPIC FOI requests) asking for similar capabilities through US telco and network equipment manufacturers, whether or not this has happened and to what extent... (google or bing “Carrier IQ”)

New Ideas – Should You Become a Big Brother, like the NSA?

• Create Employee Policy Agreements That All Must Accept
  • Proper use of resources
  • Behavior on the network and internet
  • Password rules and storage do matter
  • Best practices about NOT being socially engineered
  • BYOD and wireless devices must be managed and controlled

• Run Your Own HoneyPots on Your Own Employees and Consultants
  • To catch a thief you have to give them something to steal
  • Create a fake database of confidential information and make it easy to find and easy to hack
  • Log all activities and track the sources of the attacks

Visit [www.honeynet.org](http://www.honeynet.org) to learn more about Honey Pots
New Ideas – You Deploy BYOD Security like the NSA?

Do you allow employees to bring in their own equipment?

- What is the OS? What apps are running? Are they patched?
- What if it is lost or stolen with data leakage potential?
- Do you have the controls in place to remote wipe it?
- Can you find a stolen device? Lojack or similar software?
- What’s it doing on your network anyway?

It’s time to….

- Detect, Log, Alert, Block, Audit, Quarantine
- There are agentless and agent-based ways to do this...
- Google “BYOD” and “NAC” and evaluate, then deploy
New Ideas – Centralize and Frequently Review CybOX, used by the NSA:

CybOX stands for Cyber Observable Expressions...

- Threat assessment & characterization
  (detailed attack patterns)
- Malware characterization
- Operational event management
- Logging
- Cyber situational awareness
- Incident Response
- Digital Forensics
- Cyber Threat information sharing

Visit [http://cybox.mitre.org](http://cybox.mitre.org) to learn how to implement it.
NSA’s System Hardening 101

1. Understand your software development weaknesses: http://cwe.mitre.org
2. Understand your operating system weaknesses: http://oval.mitre.org
4. Remove these weaknesses by better software development processes, patching and reconfiguring operating systems and network systems. Repeat. Repeat. Repeat. Repeat. Repeat....yes...Repeat again...and again...
NSA’s System Hardening 101 (cont’)

Make sure you checkout [http://www.first.org/](http://www.first.org/) and find their local affiliate in your country or region... First offers a **FIRST Best Practice Guide Library (BPGL)**

**Also maintained by FIRST: the FIRST Security Reference Index**

It is a complicated, arduous, and time-consuming task for even experienced system administrators to know what a reasonable set of security settings is for any operating system. Thus, the FIRST Best Practice Guide Library intends to assist FIRST Team Members and public in general in configuring their systems securely by providing configuration templates and security guidelines.

Also, this initiative aims at recognizing FIRST members' work and promote it outside the FIRST community. *Note: The Best Practice Guides Library is based on documents and links submitted by FIRST members.*

**FIRST members are strongly encouraged to share their Best Practice guides or links to Web sites hosting Best Practice guides.**

The FIRST BPGL is found here: [http://www.first.org/resources/guides](http://www.first.org/resources/guides)
NSA’s System Hardening 101 (cont’)

Want to see all of the UNCLASSIFIED STIGS so you can harden just about anything?

Here is the entire list of STIGS:

http://iase.disa.mil/stigs/a-z.html

Say you are worried about a Windows 7 deployment.

How would you harden it when you finish the install?


Download the STIG...follow the instructions...
Leverage their UNCLASSIFIED recommendations...

For example...How would you harden a bluetooth network?  
www.nsa.gov/ia/_files/wireless/BlueToothDoc.pdf  

All their guides can be found here:  

What are the best checklists to follow to harden your systems?  
http://web.nvd.nist.gov/view/ncp/repository
NSA says the Root Cause of Exploitation is....?

Common Vulnerabilities and Exposures (CVEs)

1. Although there might be 120,000,000 signatures in your McAfee or Symantec anti-virus scanner database (and growing exponentially), there are only ~56,000 CVEs. If you close just one CVE, for example, you can block more than 110,000 variants of the W32 malware.

2. If you aren’t visiting http://nvd.nist.gov to see what kind of exploitable holes you have in your network, cyber criminals CERTAINLY are...

3. Everything with an IP address has a CVE, you need to figure out which ones are critical holes and how to patch, reconfigure and remove them—i.e. system hardening.
Some Best Practices Tools Used by the NSA’s INFOSEC Staff...

NETWORK-BASED VULNERABILITY TESTS:

http://www.openvas.org
(better than Nessus)

OPERATING SYSTEM-BASED VULNERABILITY TESTS:

http://oval.mitre.org

Try: http://threatguard.com/node/27 for a great OVAL tool that’s FREE ‘cause you don’t have the NSA budget, do you?
Some Best Practices Free Tools Used by the NSA (cont’)

COBIT 5 is the latest edition of ISACA’s globally accepted framework, providing an end-to-end business view of the governance of enterprise IT that reflects the central role of information and technology in creating value for enterprises. The principles, practices, analytical tools and models found in COBIT 5 embody thought leadership and guidance from business, IT and governance experts around the world.

http://www.isaca.org/COBIT/Pages/default.aspx
Some Best Practices Free Tools used by the NSA (cont’)

Stay on top of your CERTIFICATION...take some free online quizzes at CCCURE.org


Send an email to clement.dupuis@gmail.com mentioning you saw CCCURE.org in my Concise-Courses.com presentation and Clement will send you a copy of his Scenario Based questions practice test for FREE. This is a value of $59.99. The real exam contains many scenario based question, get ready for this special format, CCCURE.org is the only vendor providing such type of quizzes.
Some Best Practices Free Tools used by the NSA (cont’)

ENCRIPTION...  http://www.truecrypt.org

Main Features: Creates a virtual encrypted disk within a file and mounts it as a real disk. Encrypts an entire partition or storage device such as USB flash drive or hard drive. Encrypts a partition or drive where Windows is installed (pre-boot authentication). Encryption is automatic, real-time (on-the-fly) and transparent. Parallelization and pipelining allow data to be read and written as fast as if the drive was not encrypted. Encryption can be hardware-accelerated on modern processors. Provides plausible deniability, in case an adversary forces you to reveal the password: Hidden volume (steganography) and hidden operating system. More information about the features of TrueCrypt may be found in the documentation.
What Are The Best Ways the NSA Stops Malware from infecting their networks?

Checkout the VirusBulletin at http://www.virusbtn.com/vb100/index

Upload a suspicious file to VirusTotal: https://www.virustotal.com/

or try Jotti’s here: http://virusscan.jotti.org/en

or try VirScan here: http://virscan.org/

or try MetaScan from Opswat: http://www.metascan-online.com/
Speaking of VirusBulletin...

No one is at 100% x 100% are they? That’s right, malware WILL get in!
NSA Methods at Stopping Malware... Multi-pronged Approach

1. System Hardening is crucial. No CVEs. No holes. Almost nowhere to exploit.

2. Educating Employees to not be socially engineered and to best practices behavior is also crucial.

3. Controlling which devices come and go on your network (BYOD through NAC) is also very important.

4. Most importantly, Host-based Intrusion Prevention is your final resort.

5. The better the HIPS engine in the anti-virus solution, the higher the rating.
So What is Bulletproof IT Security?

• Good Corporate Security Policies
• Frequent Employee Training
• Ongoing Self-Assessment
• Corporate-wide Encryption
• Consistent System Hardening
• Vulnerability Management
• Managing the BYOD Dilemma
• Testing your BCP and DRP Plans
• Leveraging Next Gen Malware Blocking
Was that really so secret?
Before we close, here’s a gift for you...get your free copy...

**Signup Today for FREE E-Subscriptions:**

**FREE MONTHLY NEWSLETTERS**
100+ pages packed with tips, tricks, tools and techniques for better IT Security and Regulatory Compliance

**FREE QUARTERLY MAGAZINE**
Ships in print at RSA Conferences, Covers next generation tools and techniques, Cyber Defense Test Labs (CDTL) INFOSEC product reviews, and much more...

[www.cyberdefensemagazine.com](http://www.cyberdefensemagazine.com)
Thank You!
Bulletproof IT Security: Unclassified Secrets of the NSA

by Gary S. Miliefsky,
Executive Producer,
CyberDefenseMagazine.com

Brought to you by NAISG.org