Beyond BlackHat

Greg Metzler
gregory.metzler@gmail.com

whoami

- Retired US Navy Geek (21+ years)
- 17+ years (and counting)
  - Network Warfare Operations
  - Information security
  - Mission Continuity
  - Application Development
- Perpetual Student

DISCLAIMER

These ramblings are my own…

What I learned on my summer vacation…

- Hardware hacks make for great entertainment
- Rootkits are cool and becoming cooler
- Web 2.0 should be renamed Pwn 2.0
- The Mac Attack has finally arrived
- Virtualization/Cloud Pwning is the new “next big thing”
- It doesn’t have to be new to work
- Security: we are (still) doing it wrong…

Build a better mouse trap - Nature builds a better mouse!

Tracks

Day 1

- Privacy
- Infrastructure
- Legal/Management
- Rootkits
- Testing/exploiting
- Metasploit
- Exploitation
- Panels

Day 2

- Hardware
- Reverse Engineering
- Cloud/Virtualization
- Mobile
- Random
- Panels
- Turbo Talks

Sample Topics

- Veiled: A browser-based darknet
- Sniffing keystrokes with lasers and voltmeters
- Router exploitation
- Beckstrom's Law: Determining network value
- Your mind: legal status, rights and securing yourself
- Economics of the underground economy
- Stoned Bootkit
- Advanced MAC OSX rootkits
- Managed code rootkits
- The insider (Fox in the Henhouse)
- Introducing Ring -3 rootkits (Chipset rootkits)
- Attacking XSS filters
- Post exploitation in hardened PHP environments
- Demystifying fuzzers
- Lock picking (always a favorite)
- Anti-forensics: the rootkit connection
- Breaking the security myths of extended validation SSL certificates (Build your own MD5 collider)
- Taking on Russian organized crime
- Predicting SSNs from public data
- Macsploitation with Metasploit
- Breaking the unbreakable Oracle
- Automatic browser fingerprinting
- MSF & telephony
- Metaphishing
- Practical windows heap exploitation
- Weaponizing the web
- Defeating SSL
- The language of trust (how to violate trust relationships)
- Attacking Intel BIOS
- 16 bit rootkits for 2nd generation Zigbee chips
- Cracking "smart" parking meters
- Reverse engineering
- Exploiting an Apple firmware update
- Cloud computing models and vulnerabilities
- Clobbering the Cloud
- Breaking out of VMWare
- Attacking SMS
- Various phone pwning demos

https://www.blackhat.com/html/bh-usa-09/bh-usa-09-archives.html

Play by play: Keynote (Day 1)

- Douglas C. Merrill (most recently: COO EMI new music- digital business)
  - Security: we are doing it wrong
    - We don't talk to our executives
      - Their priority from an IT challenge perspective: business continuity
      - Ours? Compliance
    - When we do, we get it wrong (e.g., weak ROI arguments)
      - Reputation risk? Correlation?
      - Lost productivity? (efficiency argument)
      - Exposure due to data loss? (pass it on)
    - We have made the user the enemy (or we have become theirs)
      - Building the wall/Digging the moat incentivizes negative innovation
      - Build security around the way your users need to work.
      - Make them your friend
      - Make security their problem
  - Security professionals need to:
    - Change their message (tone and content).
    - Embrace their users and HOW THEY REALLY WORK.

Play by play: Keynote (Day 2)

- Mr Lentz (CSO, DoD)
  - "The web is a global but fragile ecosystem"
  - We are at a cross-over point
    - Content-centric vs. Net-centric
  - Be the starfish in the "Starfish and the Spider"
    - One exception: adopt the spider's web (sensor grid)
    - We must stop playing whack-a-mole (pic included)
    - Shift away from static defenses toward an adaptive, agile "moving target"
  - Mission-based architecture
    - Adversaries will be inside the network. Get used to it.
    - Don't protect based on classification, but rather protect based on what info is required to accomplish the mission (UNCLAS may be critical)
  - We must "drive anonymity out of the web" (imagine how well this went over)
  - Think Globally. Act Locally (cooperative defense). "Cyber Green Movement"
- Opinion: got many things right. Got a few things wrong- way wrong.
  - Drive out anonymity? Do we need yet another Tsar? Is it *really* fragile?
- Common response (from those agreeing with him): How do we get there?

What's old is new again…and again…

- Do you know who Ken Thompson is?
  - Read "Reflections on Trusting Trust"
  - Then check out the talk on Managed Code Rootkits (hacking the JVM, Python, .NET… etc)
- Transverse Directory Attacks: ..\..\..\something bad\reallybad.exe
- Cross site request forgery (CSRF)
- XSS the gift that keeps on giving…

Hardware Hacks

- Are they *really* hardware hacks? No…
- Some were cool:
  - Parking meters: $999.99 on the meter. Lucky day!
  - Keyboard hacks:
    - Laptops using laser microphone bounced of the display
    - PS2 keyboard using *any* ground plug on the same circuit.
  - Hacking high-end digital security locks (even a Swiss safe isn't)
- Others were scary:
  - Chipset rootkits
  - MD5 collisions using GPUs (DIY Certificate Authority duping)
  - Embedded management interface hacks
    - E.g., network attached printers, ip phones, residential routers, etc.
    - Scale of problem

Pwn 2.0

- After 10+ years, we still don't have web services' security right.
- So here's an idea: let's tie them all together!!!!
- Then, let's keep our users connected to us for a "richer experience"
- Result: *Vastly* expanded attack surface
- Sample Hacks:
  - MobileMe: Transverse directory attack (YES, they still work!!!) (pwn'd Wozniak's MobileMe account)
  - Malware distribution using content aggregator sites
  - Twitter's top tweets + CSRF (or other web attack) = Juicy Target
  - Exploiting poor SSL implementations for MITM attacks
  - Social network data mining to aid SSN prediction
  - Tweeting for fun, profit and panic.
    - Information operations target
    - Injecting false stories into citizen journalism sites

Rootkits

- Ring -3 Rootkits: chipset rootkits
  - Intel Q35
- Managed Code Rootkits: “One kit to pwn them all… and in the darkness mine them.”
  - What’s old is new again (Ken Thompson’s Reflections on Trusting Trust: hack the compiler)
  - In this case, hack the JVM or .net framework
  - Even comes with an easy to use tool! (my favorite kind of talk)
- Bootkits: Stoned is back!- injects into master boot record (MBR) and runs in parallel with the OS
- Zigbee chip rootkit: low power wireless chips (metering and monitoring)
- OSX rootkits
  - beyond UNIX-styled attacks against the BSD portion of the OS.
  - exploiting Mach micro-kernal interprocess communication (IPC)
- Anti-forensics and rootkits

Hax1n6 Th3 Cl0ucl

- Cloud hype:
  - "The cloud is secure": no one REALLY knows
  - If you aren't re-writing your software, you don't do cloud computing.
- Legal issues:
  - EULAs promise nothing
  - Give your data to the cloud- you are giving it away.
  - Limited legal controls over civil/criminal requests for information
  - They don't even have to tell you if your data has been taken
- Other issues:
  - Auditing by providers is typically poor (not for your banking infrastructure)
  - Adversary can model your infrastructure (he can play in the same cloud!)
  - Decreased entropy for encryption engines (also a virtualization issue)
  - Version control: regression errors through the stack
  - Definition of "insider threat" changes
- Examples:
  - Amazon Cloud: Take my server… please. Muahaha …promoting malicious servers for others
  - SalesForce.com: free and paid subscriptions on same infrastructure: swimming with sharks
- Bottom line: Cloud today = Web c. 1999

Greg's Favorite Talks

- Cloud Computing Models and Vulnerabilities
  - https://media.blackhat.com/bh-usa-09/video/STAMOS/BHUSA09-Stamos-CloudCompSec-VIDEO.mov
- Economics of Cyber Crime in a Global Recession:
  - http://www.blackhat.com/presentations/bh-usa-09/GUERRA/BHUSA09-Guerra-EconomicsCyberCrime-SLIDES.pdf
- Anti-Forensics: The Rootkit Connection
  - http://www.blackhat.com/presentations/bh-usa-09/BLUNDEN/BHUSA09-Blunden-AntiForensics-SLIDES.pdf
- Managed Code Rootkits
  - http://www.blackhat.com/presentations/bh-usa-09/METULA/BHUSA09-Metula-NETFrameworkRootkits-PAPER.pdf
- Weaponizing the Web: Attacks Against User-generated Content
  - http://www.blackhat.com/presentations/bh-usa-09/HAMIEL/BHUSA09-Hamiel-DynamicCSRF-PAPER.pdf

BlackHat Take-aways

- Aggregation of content is dramatically increasing attack surface
  - If you link to someone else, you are at risk
  - If you are a content aggregator, you are a tasty target
- Virtualization is NOT a security feature: it is a target
- If you are weak, I am Pwn'd
- Hardware is getting tougher to hack. However, nature continues to build better mice.
- Apple is squarely in the gun sights of hackers
- NEVER bring anything electronic into the Con

Now what?

Beyond BlackHat…

Beyond BlackHat

- It's *ALL* about hacking the human
  - Until Sky Net becomes active anyway…
  - Influencing human decision making, stealing from our fellow man, etc.
  - Therefore, human considerations must be central to your security posture
- Don't throw rocks at the moon
  - You can try and stop technology's progress; however you will still be swept up in it
  - Better to recognize the trend and plan early to mitigate its arrival
- Embrace your users
  - Design security for how they need to work, not how you WANT them to work
  - Enable positive innovation, not negative innovation
  - Neighborhood watch
- Learn *and apply* the fundamentals
  - Don't get pwn'd by the things we know! (XSS, CSRF, Transverse directory attacks, buffer overflows, etc.)
  - Don't use the same number (e.g., SSN) for authentication *and* identification

Beyond BlackHat

- We are waging a digital insurgency.
  - "They" are inside the wire. Once you understand that, your approach to security changes.
  - Higher walls and deeper moats won't work
  - Assume your adversary knows (or will learn) your topology, your "white list", your password policy, etc.
  - Embrace your users (see above)
  - Build to mitigate the insider (stolen credentials = insider to a computer)
    - Statistical traffic analysis
    - Yes- encryption isn't THE answer… but you should still be using it to secure your data
  - Understand your environment
    - Do you KNOW how your custom applications REALLY uses the IP stack?
    - What is "normal"?
  - Adopt the tactics of your adversary that actually work!
  - All-source intelligence and information sharing
  - Outbound filtering!!! (cooperative defense)

Beyond BlackHat

- Cooperative Defense:
  - Not necessarily “love thy neighbor”. Rather: don’t kill your neighbor.
    - Market place competitors- cyberspace partners
    - Public-private partnerships: beyond rhetoric
    - International cooperation: work to eliminate jurisdiction shopping
  - Proactive not reactive: “You may not know this, but you’ve been pwn’d.”
  - Outbound filtering: Do It!!!!
    - If the traffic shouldn’t come from you, don’t let it!
    - Implies you know what is normal for your systems
  - Reality check: “Tragedy of the Commons”
    - You probably don’t do enough to protect yourself from others, let alone protect me from you!

You can’t defend yourself unless you are willing to defend others

Beyond BlackHat

- Design Security In
  - Addressing what the Ware Report referred to as “incomplete design”
  - We describe the problems
    - Common Vulnerabilities and Exposures (CVE)
    - Common Weakness Enumeration (CWE)
  - What about solutions- *BEYOND* configuration guidance?
    - I want my CAD!!! (Common Assured Designs)
    - Repository of open, vetted, *ideally* provably secure designs for common tasks (handshakes, shopping carts, password recovery, etc)
    - Use UML-SEC or other recognized methodology for communicating the design in a concise, testable manner.
    - Doesn’t prevent a lousy implementation, but it’s a start
  - The human: make it easier to do it right and people will.

Beyond BlackHat

- Geek Education Reform
  - Your students only know what they have learned
    - Have they read the foundational documents?
    - Have you?
  - Does your curriculum address secure design principles early enough to make a difference in how they think?
  - Do you penalize programmers for using unsafe functions or techniques in their assignments?
  - Is information security part of your general curriculum? NOT just an IT problem. (That includes you, High School teacher)
    - *We teach kids how to balance a checkbook, but not how to protect their identity*
  - Recommendation:
    - Design your curriculum to reinforce best practices EARLY.
    - Impose costs (high costs) for dangerous behavior.
    - Incorporate concepts such as student-led code review
    - Have your students comply with US-CERT's: *Key Practices for Mitigating the Most Egregious Exploitable Software Weaknesses.*

Beyond BlackHat

- Evolve!
  - The web was “built on trust”
    - No. It wasn’t. It was built on idealism.
    - It’s ALL about the human. All that’s good. All that’s bad…
  - Leave behind technologies that no longer suit the environment
    - Sailing ships (now primarily reserved for recreation/sport)
    - Horse and buggy (still around, but not like they used to be… consider THAT infrastructure)
    - Von Neumann (why should I HAVE to use something that cannot distinguish between user input and system commands?)
    - TCP-IP, BGP, ARP (you said it, therefore it must be true!)
    - Why do my critical systems HAVE to rely on untrustworthy technology and protocols?
  - National research agenda for “hard problems”
    - Prioritized
    - Incentivized
  - Get on with it! If we don’t start today, tomorrow never changes!

Final Thoughts

- Contrary to rumor, BlackHat and DEFCON are not dead.
- It's ALL about the human (offense and defense)
  - How we decide; how we work; how we thrive
  - If we want information security to be effective… we must understand this
- Don't fear technology's advance. Shape its arrival.
- Build that mousetrap, but understand the mice are smart (and getting smarter).
- You can't defend yourself unless you are willing to defend others.
- Dollar slots are a rush… but the house ALWAYS wins!


PLAY 3 CREDITS
MAX BET
INSTANT Spin!
WIN PAID
200
$1
CREDIT
224
TOTAL BET
1

Discussion