A Journalist's Perspective on Security Research

Peter Berghammer
Defcon 15; Riviera, Las Vegas

Friday August 3, 2007
Day 1, Track 4
17:00 – 17:50
(05:00-05:50 pm)

About me

- Peter Berghammer is the owner of a number of companies including:
  - Copernio: an aerospace and defense contractor
  - Future Formats: a CE research and analysis company
  - Tunitas Creek Ventures: a VC firm in the web 2.0 arena
- Additionally he writes (or has written for):
  - Dealerscope: a monthly column covering politics, economics, and corporate ethics
  - MediaLine: a monthly column covering security involving Hollywood studios, retailers and CE manufacturers
  - CreativeCow: a bimonthly column covering developments within the professional film makers community
  - ODS!: occasional contributor regarding topics affecting the optical disc industry
  - One-to-One: occasional contributor on emerging technologies affecting the replication industry

Disclaimer

- The opinions expressed in this talk today are solely those of the author and in no way reflect an endorsement by any of the publications for whom he writes.

- The opinions expressed today are solely those of the author and in no way is meant as public commentary, endorsement or non-endorsement of the products and services of any companies mentioned today.

- The opinions expressed by the author on any legal or ethical matters used by way of example during this talk are in no way meant to be considered or construed as legal or ethical advice.

- Unfortunately in today's world these disclaimers are part of the business.....

Introduction

- Let's start with the ubiquitous terms: "Security" and "Research"
- In most widely read, popular publications and websites security is meant to describe all things related to a consumer's secure use of their hardware and software
- Security research in this context generally describes a company's ***best efforts*** to keep their product safe and secure
- A security researcher therefore becomes something of a lone, mythic scholar protecting us from the harm of viruses, phishing, pfarming trojans and the like
- However, even in this context it is unclear what is meant by keeping a product safe and secure
  - Safe for who? The user, or protecting the company's IP
  - The same goes for research: researching what?, and in who's best interests
  - If you have any questions about this I suggest reading EULAs before you come to any conclusions

Simplest security term

- Security invariably can be broken down into its simplest constituent part:
  - *Identifying, codifying and tracking communications*

- In other words, a device that has no connection to the wider world is of no interest when speaking of security

- In other words, a connected device is mandatory when discussing security

- All issues surrounding security revolve around this

- *The only exception to this rule is when discussing personnel security and access to secured data and systems (but that is another topic completely)*

Security Researchers

- To **security researchers** of all flavors the term security has much more profound implications
- Security is often pursued in the abstract and theoretical (with a view of the day-to-day implications)
  - It very often involves semi-obscure topics such as cryptography and cryptanalysis
  - It almost always involves an intimate familiarity with the intricacies of machine hardware, pattern predictability among a host of other things
- In short the security researcher often works in theory and advanced analysis
  - But they ultimately have to either answer to their own company or to those who retain them
  - The dark hat researcher usually doesn't have this oversight but in a journalist's mind this is not always an advantage

Journalists

- There are a vast number of types of journalists that cover the security area
- The most well known ones are those who cover areas related to firewalls, anti-virus programs and the like
- Others cover security breaches such as the DOD’s loss of laptop computers, identity theft or credit card phishing scams
- Another type covers the “art” of security and sometimes even the ethical implications of covering up security breaches or even in soliciting security breaches in the name of better “open” security
- By and large, most journalists that cover the security beat are well versed, highly competent and minimally compromised by corporate concerns (and most of them are underpaid too)

Publications & Websites

- Typically there is a difference between a printed publication and a website
  - The most notable difference is in timeliness
  - There is near parity nowadays in depth of analysis
- Generally much lower overhead when operating a website
  - This has profound implications when it comes to advertisers and “doble-checking” content

Security research
from a journalist’s perspective:
what it is and why it matters

- Serious journalists typically see the issues surrounding security as matters of law, politics, economics
- Many times issues revolve around personal freedoms, censorship, constitutional law etc.
- At a deeper level however issues revolve around privacy, cryptography and freedom of expression
- At its core a journalists view of security colors the approach and definitions of the above topics

Differences between security bloggers and print journalists

- Security bloggers are the mainstay of serious research
- The timeliness and intensity of near real-time reporting is essential
- Print journalist can bring better analytical and cross-related events to bear
- In some very few cases however print can be “compromised” by the very audience it seeks to reach

Top” security stories of the past year and why they got the coverage

- Veterans Administration losses laptops
- TJMaxx credit card numbers “hacked”
- Sony rootkit fiasco
- HP “spoofing” and corporate spying fiasco

The 5 biggest f***ups: where we screwed up or missed the point completely

- Google, Yahoo, MSN censorship in China
- RIAA methods to obtain data
- Vista phone home issues
- Blu-ray, HD-DVD, HDCP issues surrounding privacy
- Metadata, metamining, metadata repurposing

The best under-reported or not-reported stores of the past 24 months

- Wikileaks
- Apple
- Electronic voting: the case of Accupoll
- Web 2.0 vulnerabilities
- Cyberwar

…and my two personal favorites….

- U.K. judge in e-case asks to have the “internet” explained to him
- U.S. teacher convicted in classroom pop-up porn case convicted

Do security researchers and hackers need to consider what mainstream publications write about them?

- Impact on legitimate software and hardware sales – big bucks at stake
- The credibility factor and how that is relayed to the general public
- Your credibility (even if you are in a grey area legally) and why that is important

How do we select what's relevant or not for publication

- The role editor's play in allowing us to get the story
- The role advertiser's play in allowing us to get the story (or not)
- Who pressures journalists to censor themselves
- Who threatens journalists and how…and why

Government(s) involvement in leaking or suppressing stories

- It really isn’t just the US government that cares.....
- Have you ever tangled with the Russians?.....or the.....or even the.....
- What about SOEs (state owned enterprises)
- Denying visas, denying access

Journalists:
Where we get it right – and wrong

- Funny examples of who is doing a good job...and a bad job

- *Note: due to the sensitivity of the cases cited this portion is oral only*

Developing a “relationship” with your journalist*

- Becoming a trusted source
  - How to contact
  - How to provide data
  - What is relevant
  - Creating/avoiding a paper trail

- Things not to do
  - This is not about you
  - Stay truthful
  - Expose the illegal but stay legal!

Common Misperceptions

- Journalists are lazy
- We're just looking for the sensationalist stories
- We just are earning a buck and don't really care about the area
- Our magazines tell us what to do

What government and industry want to do to you

- Revised DMCA and its implications for researchers
- The link between legislation and industry
- Does the general public even know or care?
- Who really benefits, and who is really hurt by the status quo

What it means to become "famous" by your actions….and the implications thereof

- "So Sue Me" the case of Johansen
- Kiddie scripters and why they get the coverage
- "So sue me…" how to silence a journalist
- The hacker mystique: and why it isn't always so rosy

Just for fun………

Class Exercise

Let's play:

GLOBAL DISINFORMATION

A step by step tutorial on creating a bogus story

Step One:
Pick a topic from current events

- International Space Station loses power during Shuttle mission

- Computers fail

- Possibility of abandoning station

- *It is important to select a topic with a broad range of possibilities such as the international mix of the station, geopolitics between US & Russia, multiple international suppliers, NASA implications*

- *It is important to allude to, but not state, other conspiracy theories such as Area 51, One-Worlders and the Illuminati and so much more!!!!!*

- *Also, don't forget the current year's enemy du jour*

Step Two:
Mix it up with other world events

- For this story possibilities include:
  - Chinese force down US spy plane and hold crew hostage
  - Russian transnational, natural gas pipeline shipments to Europe are imperiled
  - German loan crises to Russia looms
  - Cyberwar between Estonia and Russia
  - China prepares for cyber dominance
  - US Southeast Asian strategy weakens as Iraq war continues
  - As Chinese imports to US and Europe continue to grow, so does Trade Imbalance

Step Three: appeal to people’s fears and make it personal

- Transnational gangs of hackers team up to steal **your** identity
- More jobs being exported abroad…could **your’s** be next?
- Warrantless wiretaps: what is the government trying to secretly learn about **your** life?
- Government Secrecy: what is the government hiding about its plans for **your** future?

Step Four:
Make it up as you go along

- Sample story:
- Dateline: Johnson Space Center
  Houston, Texas
- Headline:
  - **Faulty Cabling Not Sole Source of ISS Computer Failure**
- Tag Line:
  - **Security Researcher Outlines Links Between Sino-Russian Cyberwars and Hacking Intrusions Into Secure NASA Systems**

Step Five: Here is our bogus story

Space Station Woes May Be Just Beginning

“We may never know who is really responsible”

Last month’s computer failures on the International Space Station may not be solely to blame on faulty German cabling according to renowned security expert Mortimer Snerd. The expert contends that the near perfect operation of the cables prior to the deployment of the solar collection units installed by astronauts points to another, perhaps more sinister cause for the station’s repeated computer crashes.

Security Expert Mortimer Snerd:
Photo Courtesy: AmNews File

“Frankly, the near perfect timing of the computer failures almost certainly points toward outside, undetectable hacking intrusions” stated this expert. He continues that “ a well known state of war has been raging in cybersapce under the watchful eyes of Russian intelligence. It is believed that a number of counter measures being employed in this battle are actually lines of code procured by the Chinese from a shot down US spy plane.” Other international experts concur that ……

Kid Drowns While Mom Surfs for Porn

Costa Mesa, CA- A 32 Year old mother is in custody tonight after failing to hear her daughter’s frantic splashes for survival.

Cont. page 29

Moral of the Story

- Be careful what facts you take at face value
- Be Careful who you trust
- Don’t automatically assume interrelated conspiracies
- Always assume an hidden agenda (even for legit stories)

Contact/Tips

pf0t0n [@] hushmail [dot] com

Most current version of this presentation can be obtained by emailing to the above address

Thank you