Paper review 1

- Privacy is a Process, not a PET – A Theory for Effective Privacy Practice
- Accepted at New Security Paradigms Workshop 2012
Paper review 2

- Accepted at 2012 ACM annual conference on Human Factors in Computing Systems
Paper review 3

• ’My privacy when adopting a technology – I know what’s important to me’ – An Exploratory Focus Group Study”
• Rejected from Workshop on Privacy in the Electronic Society 2012
Paper review 4

• Would You Sell Your Mother’s Data? Personal Data Disclosure in a Simulated Credit Card Application
• Average rejection but accepted to Workshop on Economics in Information Security (WEIS) 2012
Vulnerability disclosure

• Don’t forget overall goal: improve software safety
• Consider incentives for researchers, software vendors, customers
• Supply chain can be complex
  • Software component developers
  • Open source
  • Resellers
  • White-label software
Initial attempts were chaotic

- Researchers would sometimes tell vendors of vulnerabilities
- Vendors would sometimes threaten researchers
- Bugs would sometimes get fixed
Full Disclosure Policy (RFPolicy)

• “This policy states the 'guidelines' that an individual intends to follow. You basically have 5 days (read below for the definitions and semantics of what is considered a 'day') to return contact to the individual, and must keep in contact with them at least every 5 days. Failure to do so will discourage them from working with you and encourage them to publicly disclose the security problem.”
Full Disclosure Policy (RFPolicy)

• “First and foremost, a wake-up call to the software maintainer: the researcher has chosen to NOT immediately disclose the problem, but rather make an effort to work with you. This is a choice they did not have to make, and a choice that hopefully you will respect and accept accordingly.”
Full Disclosure Policy (RFPolicy)

• “Compensation is meant to include credit for discovery of the ISSUE, and perhaps in some cases, encouragement from the vendor to continue research, which might include product updates, premier technical subscriptions, etc. Monetary compensation, or any situation that could be misconstrued as extortion, is highly discouraged.”
“Vulnerabilities reported to the CERT/CC will be disclosed to the public 45 days after the initial report, regardless of the existence or availability of patches or workarounds from affected vendors. Extenuating circumstances, such as active exploitation, threats of an especially serious (or trivial) nature, or situations that require changes to an established standard may result in earlier or later disclosure. Disclosures made by the CERT/CC will include credit to the reporter unless otherwise requested by the reporter. We will apprise any affected vendors of our publication plans and negotiate alternate publication schedules with the affected vendors when required.”
Responsible Vulnerability Disclosure Process (rejected RFC)

• “The Reporter SHOULD grant time extensions to the Vendor if the Vendor is acting in good faith to resolve the vulnerability.”
Microsoft Coordinated Vulnerability Disclosure

• “We ask the security research community to give us an opportunity to correct a vulnerability before publicly disclosing it, as we ourselves do when we discover vulnerabilities in other vendors' products. This serves everyone's best interests by ensuring that customers receive comprehensive, high-quality updates for security vulnerabilities but are not exposed to malicious attacks while the update is being developed. After customers are protected, public discussion of the vulnerability helps the industry at large improve its products.”
Facebook Whitehat

- If you comply with the policies below when reporting a security issue to Facebook, we will not initiate a lawsuit or law enforcement investigation against you in response to your report. We ask that:
  - You give us reasonable time to investigate and mitigate an issue you report before making public any information about the report or sharing such information with others.
  - You do not interact with an individual account (which includes modifying or accessing data from the account) if the account owner has not consented to such actions.
Facebook Whitehall

• You make a good faith effort to avoid privacy violations and disruptions to others, including (but not limited to) destruction of data and interruption or degradation of our services.

• You do not exploit a security issue you discover for any reason. (This includes demonstrating additional risk, such as attempted compromise of sensitive company data or probing for additional issues.)

• You do not violate any other applicable laws or regulations.
Facebook refusal

• “Recently, a researcher tried to tell us about a bug that would allow users to post on the timeline of another user who was not their friend. He made headlines when he got frustrated with us and used that vulnerability to post on the wall of a real user.”

• “He tried to report the bug responsibly, and we failed in our communication with him. We get hundreds of submissions a day, and only a tiny percent of those turn out to be legitimate bugs.”

• “We will not change our practice of refusing to pay rewards to researchers who have tested vulnerabilities against real users. It is never acceptable to compromise the security or privacy of other people”
Vulnerability markets

• TippingPoint/ZDI
  • Funded through intrusion detection systems
  • Support disclosure to vendors
• No-rules markets
  • Probably used to develop malware
The Likelihood of Vulnerability Rediscovery and the Social Utility of Vulnerability Hunting

• “It is thus possible that vulnerability hunting can result in a more secure product and can provide a social benefit. Patch announcements and vulnerability reports are also used to quantitatively (albeit roughly) demonstrate that vulnerabilities are often independently rediscovered within a relatively short time span.”
Black market

- Unregulated and dubious legality
- Proposals to regulate through munitions control
- Several vendors involved
- Buyers often governments