The New Privacy and Security Threat Model

SCCE: East Coast Regional Compliance & Ethics Conference
Washington DC, May 9, 2014
Chris Cwalina, Holland & Knight and Maggie Mobley, Carrier IQ

Privacy and Security Risks

- FTC
- State AGs
- Other federal regulators
- Congress
- Plaintiffs attorneys
- Consumer groups
- Press
- Customers and Consumers
- Employees
- Bad Actors and "Hacktivists"
- Independent Researchers

The New Threat Model: Independent Researchers

- Independent Researchers:
  - Plaintiffs lawyers pay attention and hire them
  - Regulators hire them
  - Consumer groups use them
  - The press follows them
  - Congress pays attention

- Many of them are highly skilled and experts in their field

- No economic barrier to entry: they tend to leverage social media and blogs and will often publish findings without pay
Example in the News

- Ashkan Soltani – Flash Cookie Re-Spawning and Tracking
  • Research on the re-spawning of flash cookies resulted in numerous plaintiff's class action suits against retailers, tech companies, and others in state and federal courts over the next 3 years in California, New York, Arkansas, and Missouri (e.g. Macy’s, Kohl’s, PetSmart, Nordstrom’s Philips Electronics North America, ETRADE, Skype, Quantcast, ClearSpring, Videoegg, Kissmetrics, Interclick, and Hulu).
  http://gigaom.com/2011/01/05/419-interview-scott-kamber-on-his-spate-of-lawsuits-over-internet-privacy/

Example in the News

- Arvind Naryanan and Vitaly Shmatikov – Data Re-identification
  • Used the Netflix Prize data set—consisting of de-identified end-user information—being re-identified using collateral data sets. Netflix was sued in a class action lawsuit and its subsequent Netflix prize was investigated by the FTC as a result.
  • http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf

Example in the News

- Jonathan Mayer – 3rd Party Cookie Bypass and History Sniffing
  • Discovered and disclosed Google’s end-run around 3rd party cookie blocking on iOS.
  http://techliberation.com/2012/02/19/did-google-defeat-peoples-privacy-preferences/
  The FTC then pursued an enforcement action against Google for the conduct.
  • Outed Epic Marketplace over history sniffing.
    • http://cyberlaw.stanford.edu/node/6695
  • FTC proceeded with enforcement action against Epic Marketplace.
    • http://cyberlaw.stanford.edu/node/6695
Example in the News
—Dan Boneh, Rishita Anubhai, and Vitaly Shmatikov – Faulty SSL Security


• The study found that in many cases, for mobile apps, SSL certificate validation is completely broken

• The results of the study, including its mode of testing, paved the way for the FTC’s 20 Year consent decree against Fandango because Fandango allegedly “Failed to Securely Transmit Sensitive Personal Information”

Internet of Things and Getting “Outed” at DefCon — Vulnerable Baby Monitors

DefCon21 Home Invasion 2.0 Network-Controlled Consumer D...

Internet of Things and Getting “Outed” at Blackhat—Hackable Applications on Smart TVs

Black Hat 2013 - The Outer Limits: Hacking The Samsung Sm...
Other Headlines

- Wall Street Journal (What The Know Series)
- California AG
  suit-against-delta-airlines-for-failure-privacy-policy
- http://www.healthbeat.org/articles/2014/1/31/calif-ag-sues-kaiser-foundation
  health-plan-over-data-breach?view=print (late data breach notification)
- Starbucks
  http://www.hln.com/sites/page/privacy/2014/01/26/starbucks-chose
  convenience-over-security-in-leaving-ios-app-vulnerable/ (mobile app privacy)
- Disney and Sanrio
  http://www.ihealthbeat.org/articles/2014/1/31/calif-ag-sues-kaiser-foundation
  health-plan-over-data-breach?view=print (late data breach notification)
- Starbucks
  http://www.forbes.com/sites/parmyolson/2014/01/16/starbucks
  chose-convenience-over-security-in-leaving-ios-app-vulnerable/ (mobile app privacy)
- Disney and Sanrio
  afoul-childrens-privacy-laws-154577 (COPPA)

More Support for Testing

- HTC (FTC)—Alleged misrepresentations regarding security of mobile devices relative to the Android permissions model and pre-installed mobile apps
- ScanScout/Tremor Video (FTC)—Alleged misrepresentations about flash cookies by 3rd party hosted solution
- PATH (FTC)—Alleged COPPA violations, $800,000 settlement payment
- Datam (New Jersey Attorney General)—State Consumer Fraud Act settlement based on alleged history sniffing end user’s browsers
- W3 Innovations (FTC)—COPPA violations
- Goldenshores (FTC)—More presentations regarding use of unique identifiers and geolocation
- Hulu (Plaintiffs’ Class Action suit)—Alleged violation of the Video Privacy Protection Act based on use of the Facebook Like button

More Information

- See also for more information:
  http://www.hklaw.com/PrivacyBlog/Corporate-Privacy-Compliance-Becomes-More-
  Tech-Focused-11-05-2012/
  http://www.hklaw.com/files/Uploads/Documents/Files/Privacy/Mobile-App_Priva
  cy_The_Hidden_Risks_8-521-6151.pdf
  http://www.computer.org/csdl/mags/ic/2013/03/mic2013030018.html (Trust
  Darknet: Control and Compromise in the Internet’s Certificate Authority Model, IEEE
  Internet Computing, 2013)
Chris Cwalina

- Christopher B. Cwalina is a partner in Sidley & Austin, Washington D.C. He advises clients on emerging technology, intellectual property, data security, and privacy issues. He is a frequent speaker on emerging technology and data security issues and an author of numerous articles on these topics.

- He advises clients on emerging technology issues including data security and privacy, intellectual property, and information technology.

- He writes regularly on emerging technology issues for a variety of law firms and other legal publications.

- He is a frequent speaker on emerging technology and data security issues.

Maggie Mobley

- Maggie Mobley is the Director of Consumer Privacy at Microsoft. She is responsible for leading the company’s privacy efforts across the organization, working with teams across the company to ensure that Microsoft products and services meet the highest standards for privacy and data protection.

- She is a frequent speaker on emerging technology and data security issues.

- She is a frequent speaker on emerging technology and data security issues.

- She is a frequent speaker on emerging technology and data security issues.