Render's View

Became interested in the non-academic implications of this; where does the rubber meet the road

I'd seen this effect before

What factors outside of academically perfect conditions affect vulnerability research

Codified some of the extrinsic properties responsible for the honeymoons I had seen

Practical Examples

- Attacker tools not as well documented, surprise!
- Harder to pin down when initially available
- Feature implementation also hard to pin down
- Even on rough time lines, the honeymoon effect can be seen
- Honeymoon effect applies to protocols, not just specific implementations of software

WEP

- Originally Ratified September 1999 – Uses RC4
- Fluhrer, Mantin, Shamir - August 2001 – First Major Cryptanalysis
- August 2001 – Airsnort first released – first “practical?” WEP attack
- 2004-5 Aircrack first released? (Archive.org guess)
- Apple Airport – July 1999 – High Price tag
- Linksys WAP11 ~ Early 2002 Cheap Price tag

WEP

- Once Aircrack released, features added very quickly (ARP-Injection, Chop-Chop, etc)
- 2006 – Aircrack-ng picks up development
- By 2007, fairly idiot proof to break
- Superseded by WPA 2003, deprecated 2004
- PCI standards ban WEP as of March 2009
- TJX Initially penetrated March 2005
- TJX started WPA conversion October 2005

Practical Lessons

- Long honeymoon for practical attacks
- Cost of equipment to research on needed to drop (Airport ~$500 to Linksys ~$100)
- Aircrack framework led to faster development
- 1999 to 2005, WEP is suitable (though weak)
- Post Aircrack, attack vectors multiply and ease of use increases – WEP no longer suitable
- PCI slow to react – In the Divorce period

Other Wireless Fail

- Code Resuse
- WPA TKIP attack utilizes ChopChop attack, originally for WEP
- Deauth attacks still prevalent despite 'new' standards
- Very slow to change a whole protocol
- 802.11n is software reuse – Addendum to the protocol, not a re-write
- Legacy code == regressive vulnerabilities

Other External Factors

- Playstation 3 (2006) – A few minor vulnerabilities found but fairly monolithic for years
- Sony removes 'Install Other OS' option March 2010, pisses off customer base
- December 2010 – Initial weaknesses shown
- January 2010 – Geohot releases master keys
- Lesson: Dont piss off your customer base