Computer Security

A Walk through History

Dimitris Mitropoulos
dimitro@di.uoa.gr

Computer Worms

- November 2, 1988, sometime after 5 pm: the “Morris Worm” is one of the first computer worms distributed via the Internet.
- It worked by exploiting known vulnerabilities in Unix *sendmail*, *finger*, and *rsh/rexec* utilities, as well as weak passwords.
- Two thousand computers were infected within fifteen hours.
- The U.S. Government Accountability Office put the cost of the damage at $100,000 –10,000,000.
- The Morris worm prompted DARPA to fund the establishment of the CERT/CC at Carnegie Mellon University to give experts a central point for coordinating responses to network emergencies

Phishing

- In the 90s: Phishing on AOL (America Online).
- Phishing on AOL was closely associated with the warez community that exchanged unlicensed software and the black hat hacking scene that perpetrated credit card fraud and other online crimes (AOHell).
- AOL enforcement would detect words used in AOL chat rooms to suspend the accounts individuals involved in counterfeiting software and trading stolen accounts.
- '<><' is the single most common tag of HTML that was found in all chat transcripts naturally, and as such could not be detected or filtered by AOL staff.
- Since the symbol looked like a fish, and due to the popularity of phreaking it was adapted as ‘Phishing'.

DDoS

(Distributed Denial of Service)

- February 7, 2000, time 10:30 am: Yahoo.com goes down.
- CNN, Ebay, Buy.com, Etrade, Amazon follow.
- Total loss of revenue for Yahoo alone over $500,000.
- In November 7, 2000, “Mafiaboy” (a Canadian 15 year old) pleads guilty.
- Mafiaboy sentenced to 8 months at a Youth Detention Center (+$160 fine)

XSS

(Cross-Site Scripting)

- October 4, 2005: Sammy Kamkar designed and XSS worm that was propagated across the MySpace social-networking site.
- Within just 20 hours of its release, over one million users had run the payload making it the fastest spreading virus of all time.
- The worm carried a payload that would display the string "but most of all, samy is my hero" on a victim's MySpace profile page as well as send Sammy a friend request.
- When a user viewed that profile page, the payload would then be replicated and planted on their own profile page continuing the distribution of the worm.

Traffic-Analysis Attacks

- 2005: Monitoring the frequency and timing of network packets to reduce the anonymity provided by Tor.

Attacks on TLS

- Heartbleed is a security bug introduced into the OpenSSL cryptography library in 2012 and publicly disclosed in April 2014.
- The vulnerability is classified as a buffer over-read, a situation where more data can be read than should be allowed.
- Although evaluating the total cost of Heartbleed is difficult, eWEEK (www.eweek.com) estimated $500 million as a starting point.

LFI Attacks

(Local File Inclusion)

- 2016: LFI Attacks on the out-of-date Wordpress installation of Mossack Fonseca leads to Panama papers.

January 2018:

Spectre / Meltdown

Βιβλιογραφία

E. H. Spafford. 1989. Crisis and aftermath. *Communications of the ACM*. 32, 6 (June 1989), 678-687.

Yue Zhang, Jason I. Hong, and Lorrie F. Cranor. 2007. Cantina: a content-based approach to detecting phishing web sites. In *Proceedings of the 16th international conference on World Wide Web (WWW '07)*. ACM, New York, NY, USA, 639-648.

Dimitris Mitropoulos, Konstantinos Stroggylos, Diomidis Spinellis, and Angelos D. Keromytis. How to train your browser: Preventing XSS attacks using contextual script fingerprints. *ACM Transactions on Privacy and Security*, 19(1):2:1–2:31, July 2016.

Steven J. Murdoch and George Danezis. 2005. Low-Cost Traffic Analysis of Tor. In *Proceedings of the 2005 IEEE Symposium on Security and Privacy (SP '05)*. IEEE Computer Society, Washington, DC, USA, 183-195.

Zakir Durumeric, James Kasten, David Adrian, J. Alex Halderman, Michael Bailey, Frank Li, Nicolas Weaver, Johanna Amann, Jethro Beekman, Mathias Payer, and Vern Paxson. 2014. The Matter of Heartbleed. In *Proceedings of the 2014 Conference on Internet Measurement Conference (IMC '14)*. ACM, New York, NY, USA, 475-488.