

Zero-Day Vulnerabilities: A Primer



Dimitris Gritzalis
June 2017

ΔΙΑΔΙΚΤΥΑΚΗ ΠΥΛΗ ΓΙΑ ΤΗΝ ΠΛΗΡΟΦΟΡΙΑ,
ΤΙΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ, ΤΗΝ ΥΨΗΛΗ ΤΕΧΝΟΛΟΓΙΑ
ΚΑΙ ΤΗΝ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΣΤΗΝ ΕΛΛΑΔΑ
ΚΑΙ ΣΤΟΝ ΚΟΣΜΟ

ICTplus

Zero-Day Vulnerabilities: A Primer

ICTplus

ΔΙΑΔΙΚΤΥΑΚΗ ΠΥΛΗ ΓΙΑ ΤΗΝ ΠΛΗΡΟΦΟΡΙΚΗ,
ΤΙΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ, ΤΗΝ ΥΨΗΛΗ ΤΕΧΝΟΛΟΓΙΑ
ΚΑΙ ΤΗΝ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΣΤΗΝ ΕΛΛΑΔΑ
ΚΑΙ ΣΤΟΝ ΚΟΣΜΟ

3ο ICT Security World Congress
Ιούνιος 2017



ΟΠΑ
AUEB

Καθηγητής Δημήτρης Γκριτζαλης

Διευθυντής Εργαστηρίου Ασφάλειας Πληροφοριών &
Προστασίας Κρίσιμων Υποδομών (INFOSEC Laboratory)
Τμήμα Πληροφορικής | Οικονομικό Πανεπιστήμιο Αθηνών
dgrit@aueb.gr | www.infosec.aueb.gr



InfoSec

Are your systems, indeed, secure?

- ✓ You make use of **state-of-the art security technology**
- ✓ You have implemented a **mature security culture**
- ✓ You have employed **knowledgeable security staff**
- ✓ You are open to **new solutions/ideas/procedures**

Question: **Are your systems** (adequately/really) **secure?**

- ? What about **side-channel attacks?**
- ? What about **zero-day vulnerabilities/exploits?**



What is a zero-day vulnerability?

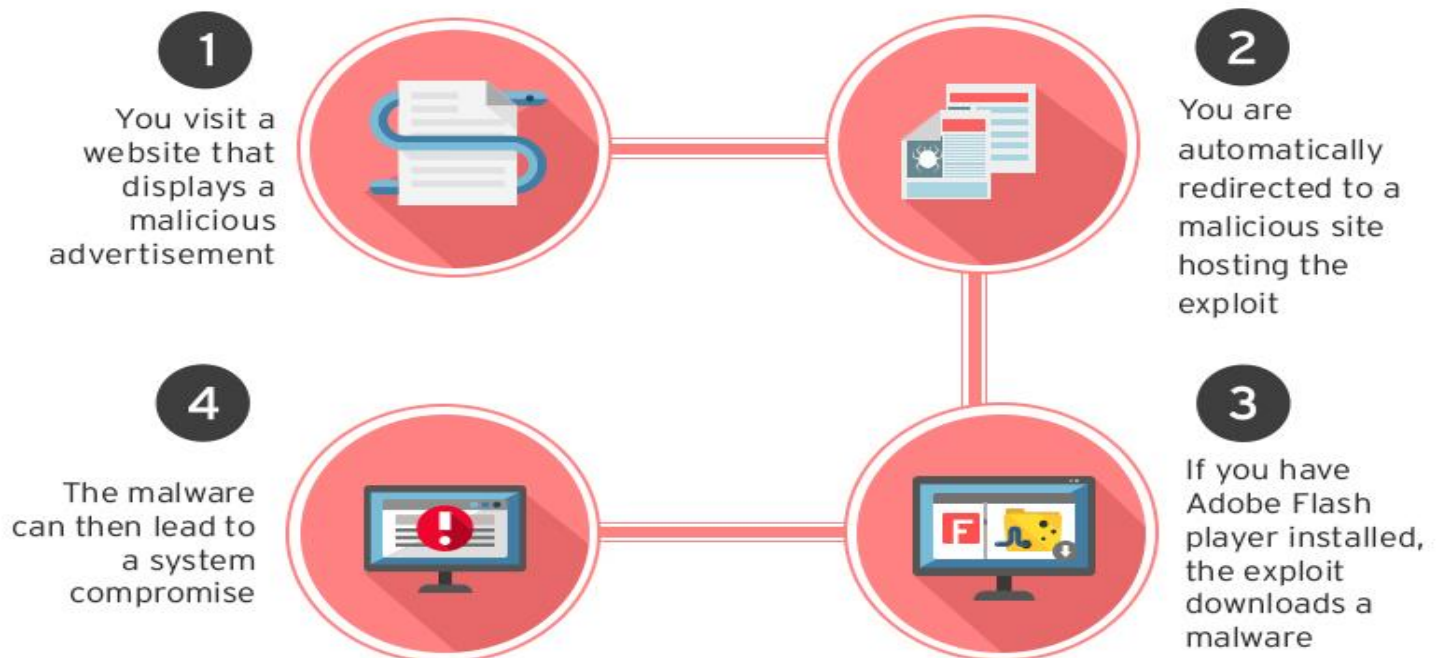
- **Vulnerability.** A type of bug that creates a security weakness in the design, implementation, or operation of a system or application.
- **Zero-day vulnerability.** A software vulnerability for which no patch or fix has been publicly released. The term **zero-day** refers to the number of days a software vendor has known about the vulnerability.
- **Zero-day exploit.** A malicious code that takes advantage of software vulnerabilities to infect, disrupt, or take control of a computer without the user's consent and typically without their knowledge.
 - ✓ Stuxnet worm: Relied on four Microsoft zero-day vulnerabilities to compromise Iran's nuclear program
 - ✓ Heartbleed vulnerability: A vulnerability in OpenSSL (a cryptography library used by millions of websites) that could allow private keys to be leaked.



Example: The Flash zero-day attack

On May 8, 2016, FireEye detected an attack exploiting a previously unknown vulnerability in Adobe Flash Player (CVE-2016-4117)

FLASH ZERO-DAY ATTACK VIA MALVERTISEMENT



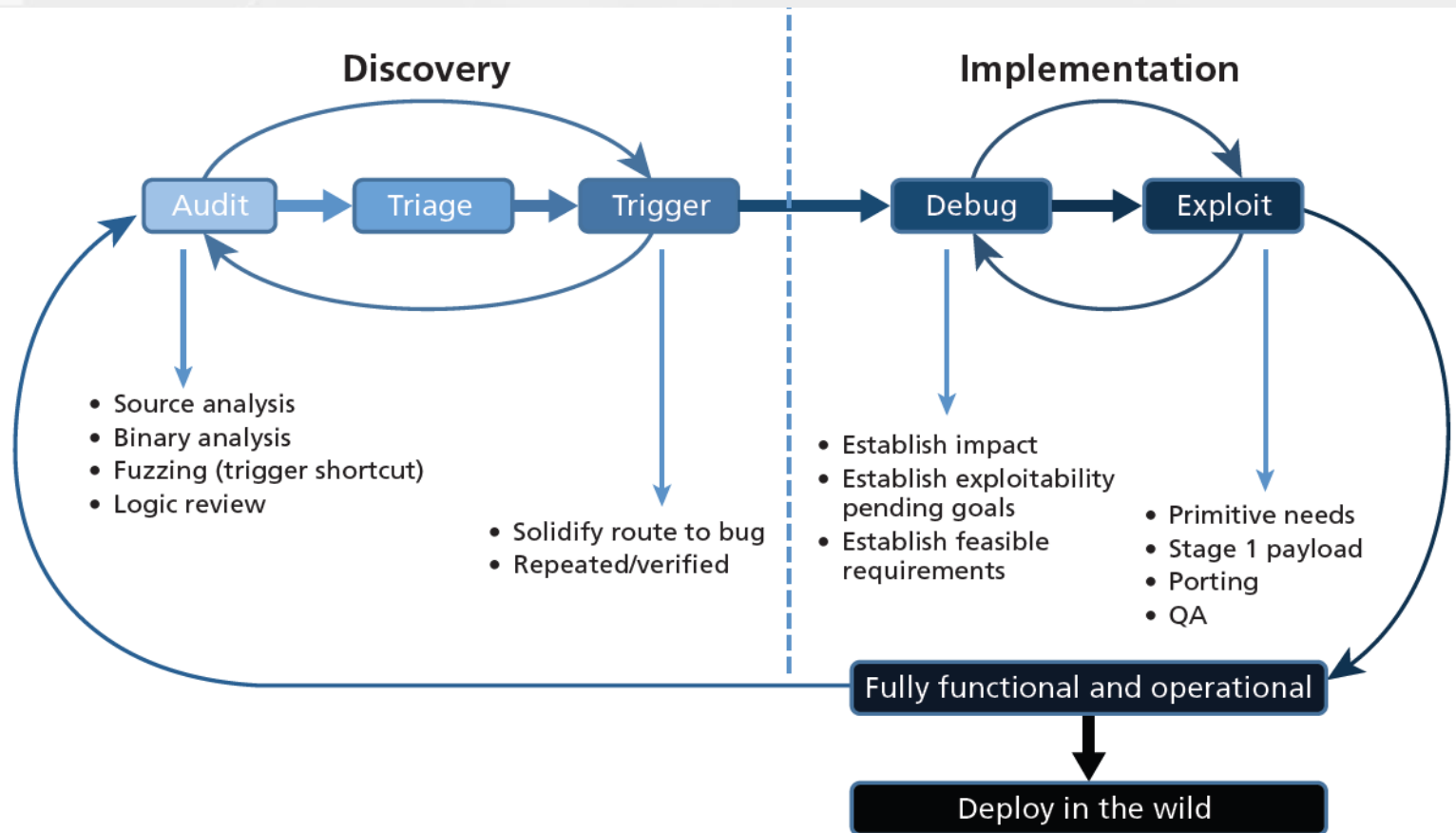
Life status: Is a vulnerability really a zero-day?

- Common practice is to classify a vulnerability simply as:
 - ✓ Alive (publicly unknown) or
 - ✓ Dead (publicly known)
- Vulnerabilities may be alive (publicly unknown) in one codebase but dead (publicly known) in another.
- Example: Code that contained a vulnerability allowing a sandbox escape in a MS product was ported over to a non-MS product:
 - ✓ The vulnerability was discovered and patched in the MS product.
 - ✓ But remains undiscovered (and unpatched) in the non-MS product.



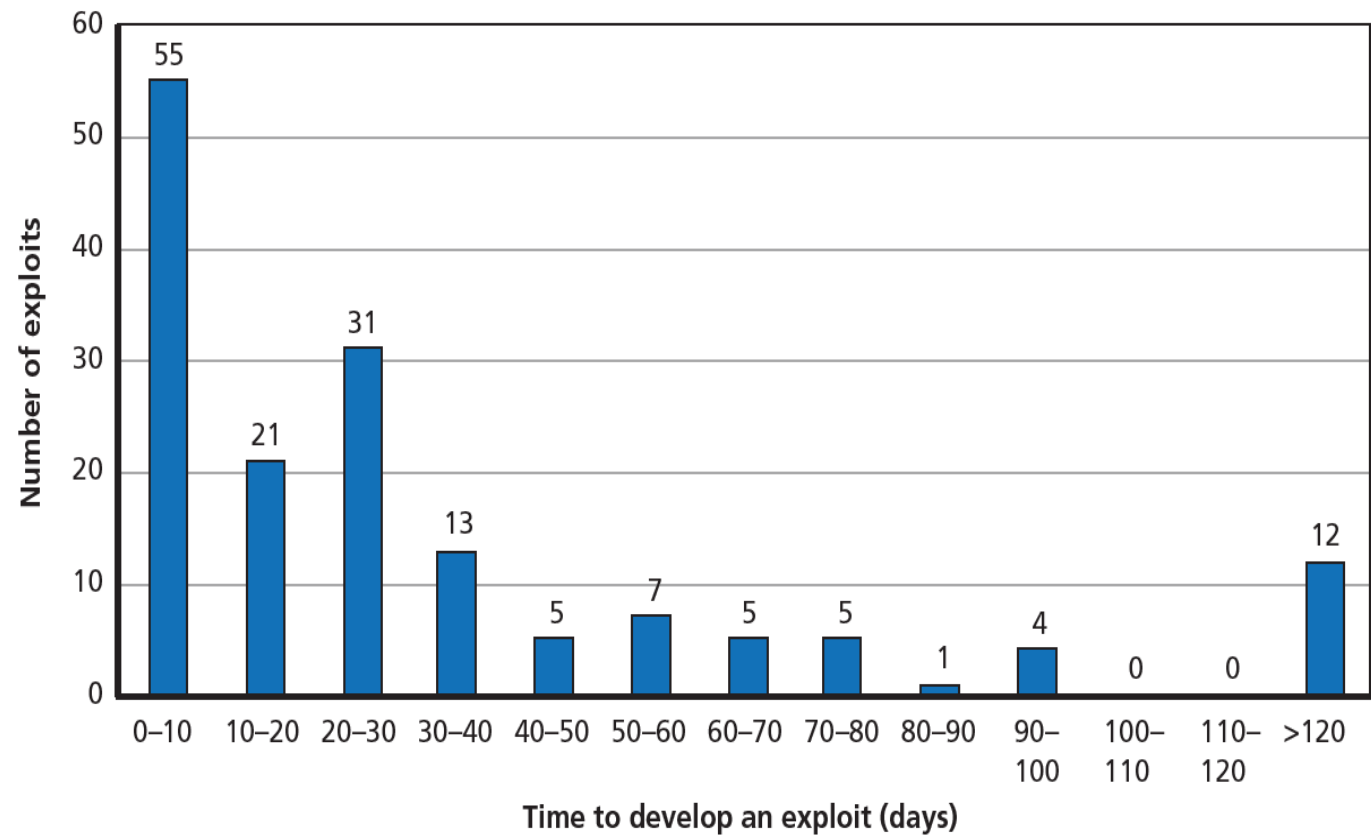
The Exploit Development Life Cycle

The exploit development process consists of many steps, each of which can go through multiple iterations.



Time to develop an Exploit

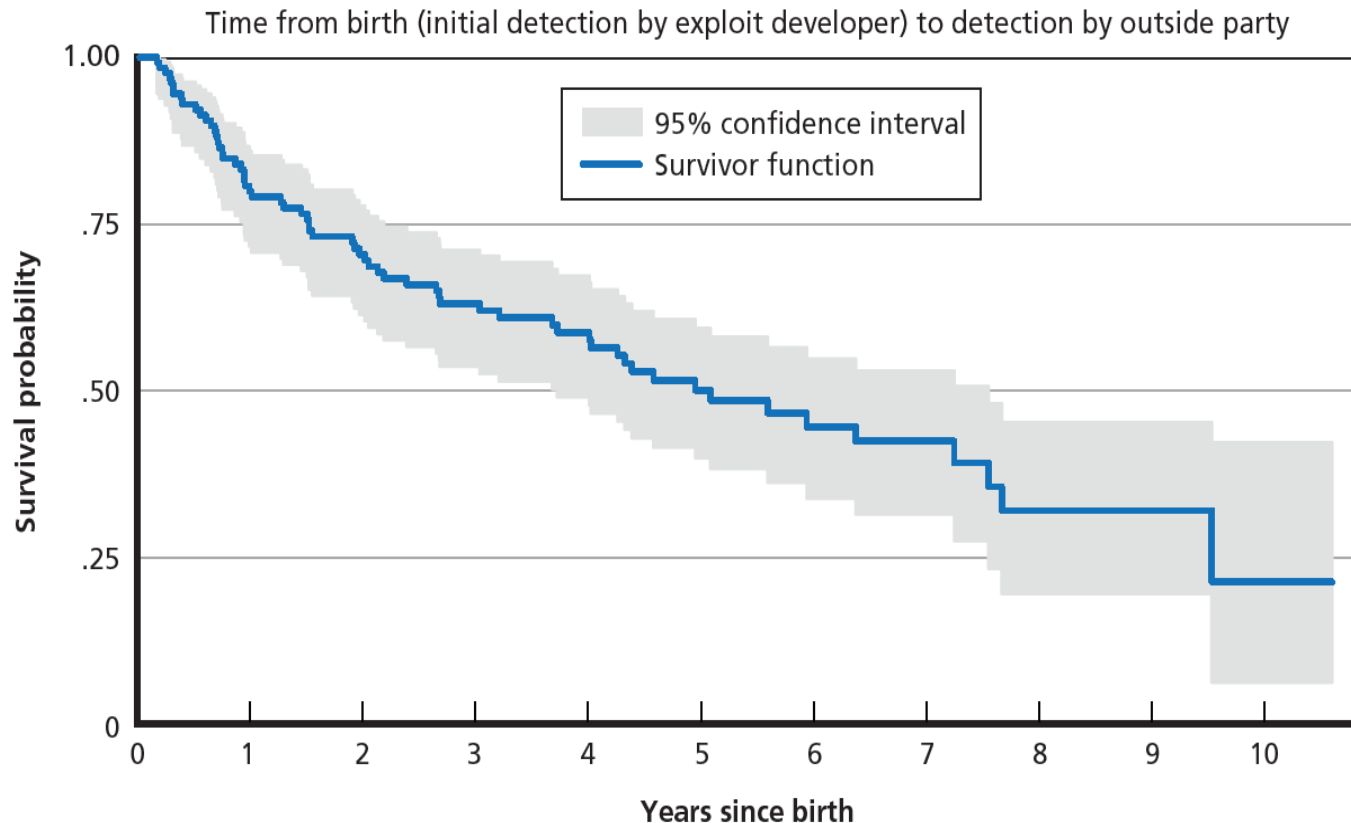
The majority of exploits in an experimental dataset took between 6-37 days to become fully functional with a median of 22 days



Longevity: How long will a vulnerability remain undiscovered/undisclosed to the public?

- Exploits are expected to live 6.9 yrs on average (median survival: 5.07 yrs)
- The Kaplan-Meier plot show the times by which 25% and 75% of died vulnerabilities, as thresholds for long and short lifetimes.

Kaplan-Meier Survival Probability Estimates (n = 127)



Markets for zero-day vulnerabilities

Markets for zero-day vulnerabilities have been growing in recent years and are distinguished by who the *initial buyer* is.

1. *White Market*: Seeks to immediately turn their vulnerabilities over to the affected vendor (often moving them into the public knowledge space) and uses them for defensive purposes.
2. *Gray Market*: (or *Government market*) Vulnerabilities remain private, used for offensive/defensive purposes and may eventually be disclosed to the affected vendor, although they are typically first sold to a government, military, or defense contractor.
3. *Black Market*: Sell zero-day vulnerabilities for criminal use or illicit purposes and aim to keep the vulnerabilities private.



What is the price to sell an exploit for a vulnerability?

- For any market, payment structure comes down to a few factors:
 1. *How easy/hard it is to find the vulnerability*
 2. *How many other vulnerabilities have been found in the product*
 3. *The impact of the vulnerability*
- Most exploits in the Gray/Government Market sell between \$50-100,000. Can go up to \$150-300,000, depending on the exploit.
- The FBI reportedly spent approximately \$1 million for the technique (which many suspect was a zero-day) used to unlock an iPhone. The high demand to unlock the iPhone likely drove up the cost.
- In the Black Market exploits go for less, e.g., a Flash exploit can fetch \$30-50,000.
- Prices for zero-day vulnerabilities on the White Market depend on the individual organization or company.



Conclusions

1. Declaring a vulnerability as *alive* (publicly unknown) or *dead* (publicly known) may be *misleading* or too *simplistic*.
2. *Exploits* and their underlying *vulnerabilities* have a long average life expectancy (6.9 years).
 - ✓ 25% of exploits will not survive >1.5 years
 - ✓ 25% of exploits will survive >9.5 years
3. For a given stockpile of zero-day vulnerabilities, after 1 year approx. 5.7% have been discovered by an outside entity.
4. Once an exploitable vulnerability has been found, the time to develop a fully functioning exploit is *rather fast* (median time: 22 days).
5. The life status of an exploit does not necessarily depend on the life status of the underlying vulnerability.
6. **With so many instances of users *not applying patches for known vulnerabilities*, does it make much sense to focus on the relatively few zero-day vulnerabilities?**



References

1. Ablon, L., Bogart, A., *Zero Days, Thousands of Nights - The Life and Times of Zero-Day Vulnerabilities and Their Exploits*, RAND Corporation, 2017. Available via: http://www.rand.org/pubs/research_reports/RR1751.html
2. Greenberg, A., "Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits," *Forbes.com*, March 23, 2012. Available via: <http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/>
3. Hosenball, M., "FBI Paid Under \$1 Million to Unlock San Bernardino iPhone: Sources," *Reuters*, May 4, 2016. Available via: <http://www.reuters.com/article/us-apple-encryption-idUSKCN0XQ032>
4. Miller, C., *The Legitimate Vulnerability Market: Inside the Secretive World of 0-Day Exploit Sales*, Independent Security Evaluators, May 6, 2007. Available via: <http://weis2007.econinfosec.org/papers/29.pdf>
5. MITRE, *Common Vulnerabilities and Exposures*, undated. January 31, 2017: <https://cve.mitre.org/about/>
6. FireEye, CVE-2016-4117: Flash Zero-Day Exploited in the Wild. Available via: <https://www.fireeye.com/blog/threat-research/2016/05/cve-2016-4117-flash-zero-day.html>
7. ABC-WJLA, *Government matters*. Available via: <https://www.youtube.com/watch?v=DKqP8AErrJ4>
8. Stavrou, V., Kandias, M., Karoulas, G., Gritzalis, D., "Business Process Modeling for Insider threat monitoring and handling", in *Proc. of the 11th International Conference on Trust, Privacy & Security in Digital Business* (TRUSTBUS-2014), Springer, Germany, 2014.
9. Mylonas, A., Meletiadis, V., Tsoumas, B. Mitrou, L., Gritzalis, D., "Dynamic evidence acquisition for smartphone forensics", in *Proc. of the 27th IFIP International Information Security and Privacy Conference*, pp. 245-256, Springer (AICT 267), Greece, 2012.
10. Mylonas, A., Dritsas, S., Tsoumas, V., Gritzalis, D., "Smartphone Security Evaluation - The Malware Attack Case", in *Proc. of the 9th International Conference on Security and Cryptography* (SECRYPT-2011), pp. 25-36, SciTekPress, Spain, 2011.
11. Virvilis, N., Dritsas, S., Gritzalis, D., "Secure Cloud Storage: Available Infrastructure and Architecture Review and Evaluation", in *Proc. of the 8th International Conference on Trust, Privacy & Security in Digital Business*, pp. 74-85, Springer (LNCS 6863), France, 2011.
12. Virvilis, N., Gritzalis, D., "Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?", in *Proc. of 10th IEEE International Conference on Autonomic and Trusted Computing*, IEEE, Italy, 2013.
13. Virvilis, N., Gritzalis, D., "The Big Four - What we did wrong in Advanced Persistent Threat detection?", in *Proc. of the 8th International Conference on Availability, Reliability & Security*, pp. 248-254, IEEE, Germany, 2013.