Session 04

Exploiting. Part 2: Web & OS & Hardware

Security of Information Systems (SIS)

Computer Science and Engineering Department

October 25, 2023

Notes

Papers

- Linux Kernel Vulnerabilities: State-of-the-Art Defenses and Open Problems (APSys'11)
- Securing Web Applications from Injection and Logic Vulnerabilities: Approaches and Challenges (Information & Software Technology, Volume 74, 2016)

Notes

Web App architecture

- front end
- back end
- database

Notes

Common Targets

- hosting web server
- other web servers
- privileged users
- other users

Notes

Attack Vectors

- HTTP protocol
- URL
  - GET
  - POST
- file upload
- other users

Notes

Common Web Vulnerabilities 2017

- OWASP 2017 TOP 10
- Injection
- Broken Authentication and Session Management
- Sensitive Data Exposure
- XML External Entity XXE
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting XSS
- Insecure Deserialization
- Components with known vulnerabilities

Notes

Injection

- SQL
- OS
- LDAP

Notes

Broken Authentication Vulnerabilities

- compromise / steal
  - passwords
  - keys
  - session Tokens
- assume other users identities

Notes

Sensitive Data Exposure

- data in transit
- data at rest

Notes

XML External Entities (XXE)

- Extensible Markup Language (XML)
- Document Type Definition (DTD)
- billion laughs attack

Notes

Broken Access Control

- bypass access control checks
- metadata manipulation
- browsing to authenticated pages as unauthenticated user

Notes

Security Misconfiguration

- unnecessary features
- debug mode
- obsolete backward compatibility

Notes

Cross-Site Scripting (XSS)

- reflected XSS
- stored XSS
- DOM XSS

Notes

Insecure Deserialization

- Java object serialization
- JSON
- COAP

Notes

Components with Known Vulnerabilities

- direct components
- nested dependencies
- 3rd party software

Notes

Bonus: CSRF & SSRF

- same-origin policy
- Cross Site Request Forgery
- Server Side Request Forgery

Notes

Common tools

- Dirb
- Burp
- Acunetix
- BeEF
- sqlmap
- Metasploit

Notes

OS Exploiting

- information leak
- local privilege escalation
- remote command execution
- resource exhaustion

Notes

Linux Kernel CVEs So far

- `https://www.cvedetails.com/vulnerability-list/vendor_id-33/product_id-47/cvssscoremin-7/cvssscoremax-7.99/Linux-Linux-Kernel.html`

Notes

Common tools

- exploitdb: `https://github.com/offensive-security/exploitdb`
- LES (Linux Exploit Suggester): `https://github.com/mzet-/linux-exploit-suggester`
- Metasploit: `https://www.metasploit.com/`

Notes

Hardware Flaws

- side channel + microarchitectural attacks
- undocumented instructions
- hardware synchronization issues (due to speed / performance updates)

Notes

Side Channel Attacks

- cache attacks
- microarchitectural attacks

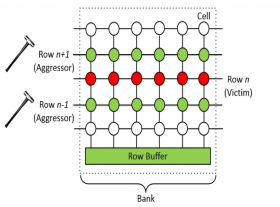
Notes

Rowhammer

- `http://users.ece.cmu.edu/~yoonguk/papers/kim-isca14.pdf`

Notes

Rowhammer



`https://medium.com/baiduxlab/pc-security-facing-another-heavy-hammer-baidu-security-discovers-a-new-rowhammer-attack-be3dce8d1e92`

Notes

Meltdown & Spectre

- https://meltdownattack.com/
- Meltdown: https://www.cve.org/CVERecord?id=CVE-2017-5754
- bypass checks, cache side-channel attack
- Spectre: https://www.cve.org/CVERecord?id=CVE-2017-5753, https://www.cve.org/CVERecord?id=CVE-2017-5715
- speculative execution
- arbitrary memory access

Notes

Sandsifter

- https://github.com/xoreaxeaxeax/sandsifter
- fuzzing of CPU instructions

Notes

Summary

- TODO
- TODO
- TODO

Notes

Keywords

- web application
- injection
- broken access control
- XEE
- XSS
- CSRF
- exploitdb
- Metasploit
- rowhammer
- Meltdown
- Spectre
- Sandsifter

Notes

Resources

- TODO
- TODO
- TODO

Notes

Notes

Notes

Notes