Software Security and Exploitation
CSCI 1650

Software Security and Exploitation
CSCI 1650

Focus: memory safety

Software Security and Exploitation
CSCI 1650

Focus: memory safety

Exploitation (offense)

Security (defense)

Software Security and Exploitation
CSCI 1650

---

focus: memory safety

Exploitation (offense)

Security (defense)

- code injection
  - NOP sled
  - jmp %esp
  - register spring
  - ...
  - NULL-free shellcode
  - alnum -11-
  - ...
  - polymorphic -11-
  - egghunter -11-
  - multi-stage -11-
  - ...


Exploitation (offense)
Security (defense)
code reuse
ret2libc
ROP
JIT-ROP
...
%esp lifting
chaining
JOP
COP
BROP
CROP
COOP
...
PIROP
Speculative CR
...

Software Security and Exploitation
CSCI 1650

---

focus: memory safety

Exploitation (offense)

- code injection
  - NOP sled
  - jmp %esp
  - register spring
  - ...
  - NULL-free shellcode
  - alnum -11-
  - ...
  - polymorphic -11-
  - egghunter -11-
  - multi-stage -11-
  - ...

Security (defense)

- Non-executable memory
  - W^X
- ASLR
  - partial
  - full


Exploitation (offense)
Security (defense)
code reuse
ret2libc
ROP
JIT-ROP
...
%esp lifting
chaining
JOP
COP
BROP
CROP
COOP
...
PIROP
Speculative CR
...
Stack canaries
SSP
RELRO
BINDNOW
FORTIFY_SOURCE
=1
=2
CFI
PAC
diversification
+
XOM
...
micro. architectural hardening.

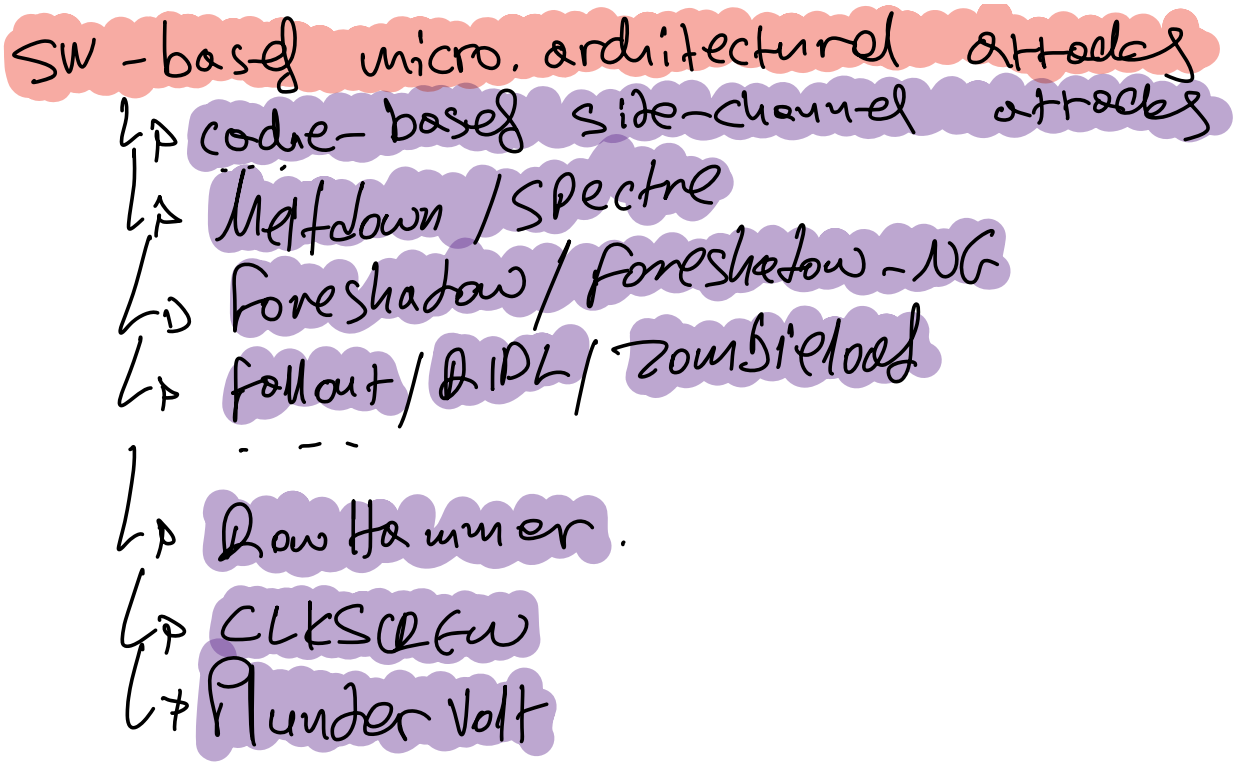
Theme: Control-flow Hijacking.

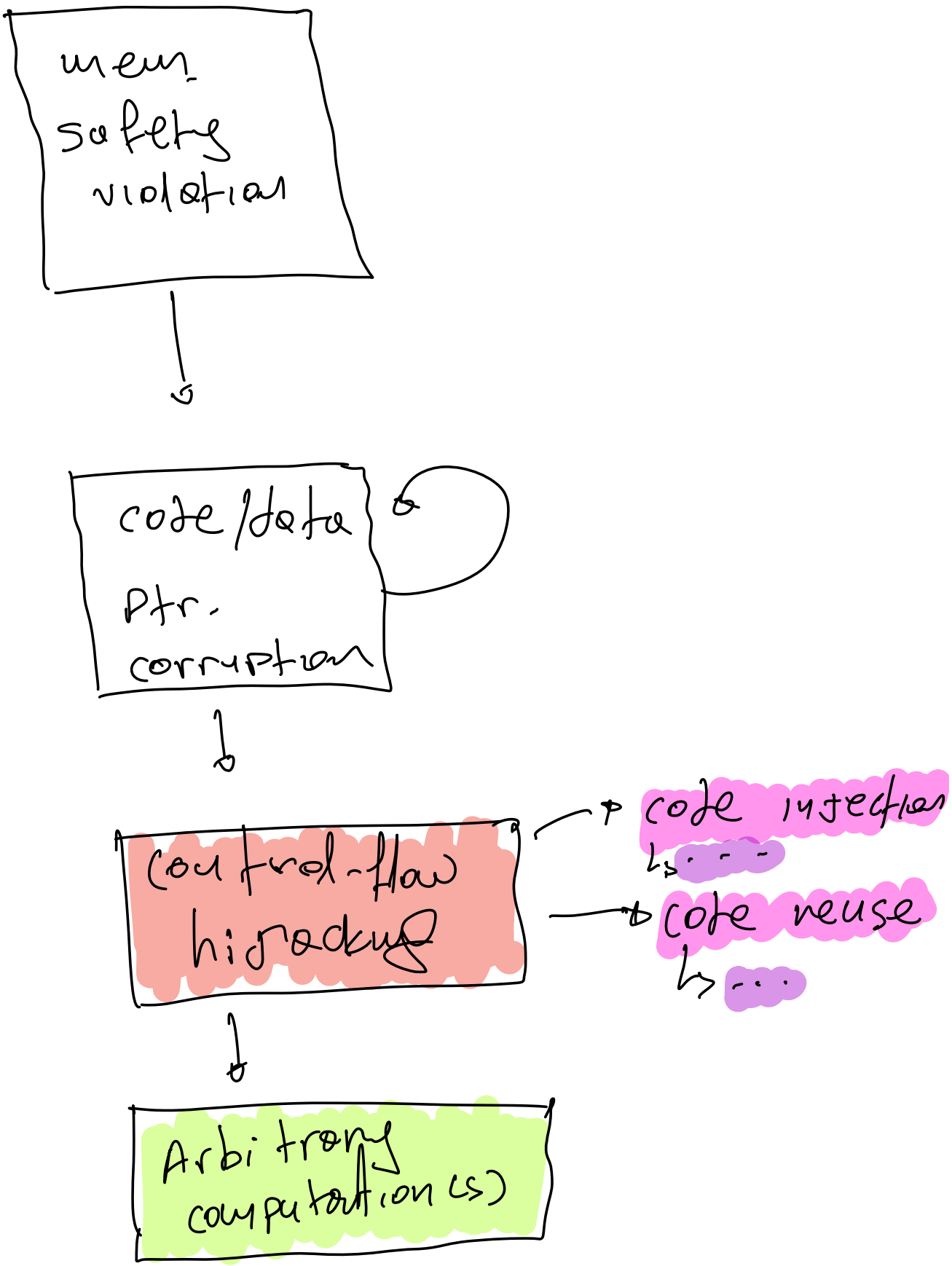
Theme: Control-flow Hijacking.

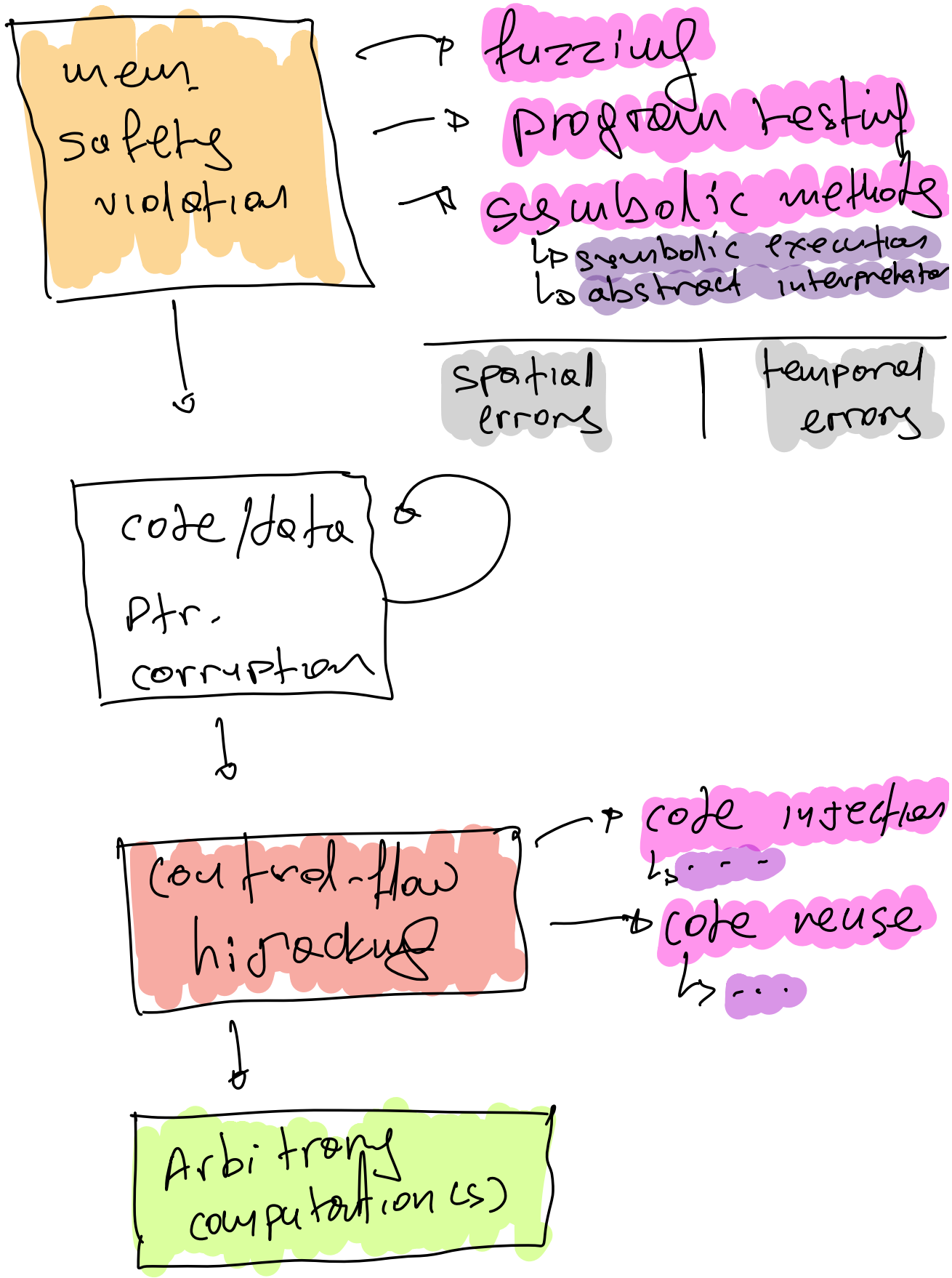
- Other topics
  - DOP
  - BOP
  - ...
  - CFI-resistant CR.
  - ...

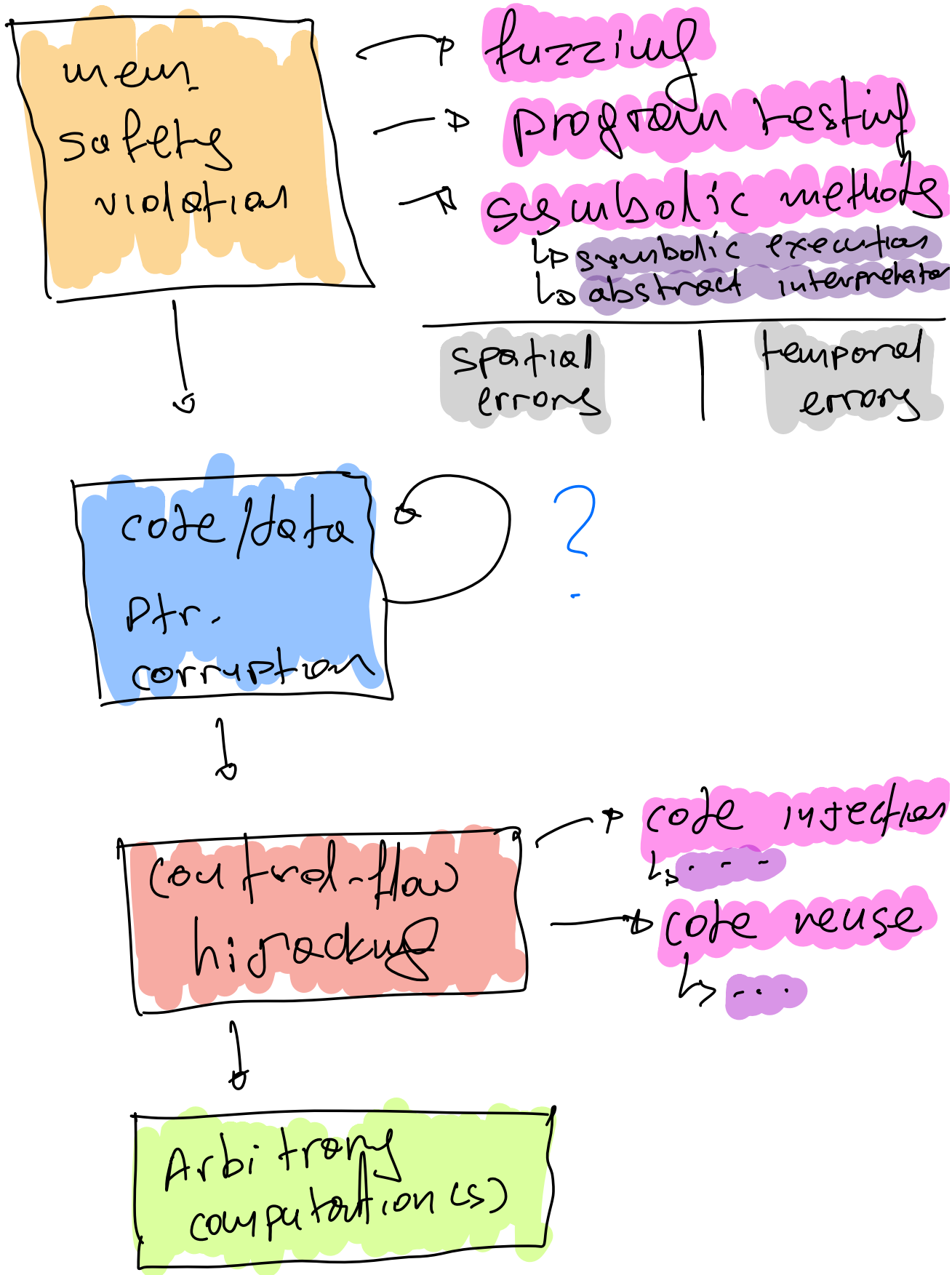
- Heap exploitation
- C++ exploitation
- Kernel exploitation
  - Jailbreaking.

- Data-only attacks
- ...


SW-based micro. architectural attacks
code-based side-channel attacks
Meltdown / Spectre
Foreshadow / Foreshadow-NG
Fallout / RIDL / ZombieLoad
RowHammer.
CLKSCREW
Plundervolt


mem.
safety
violation
code/data
ptr.
corruption
control-flow
hijacking
code injection
code reuse
Arbitrary
computation(s)

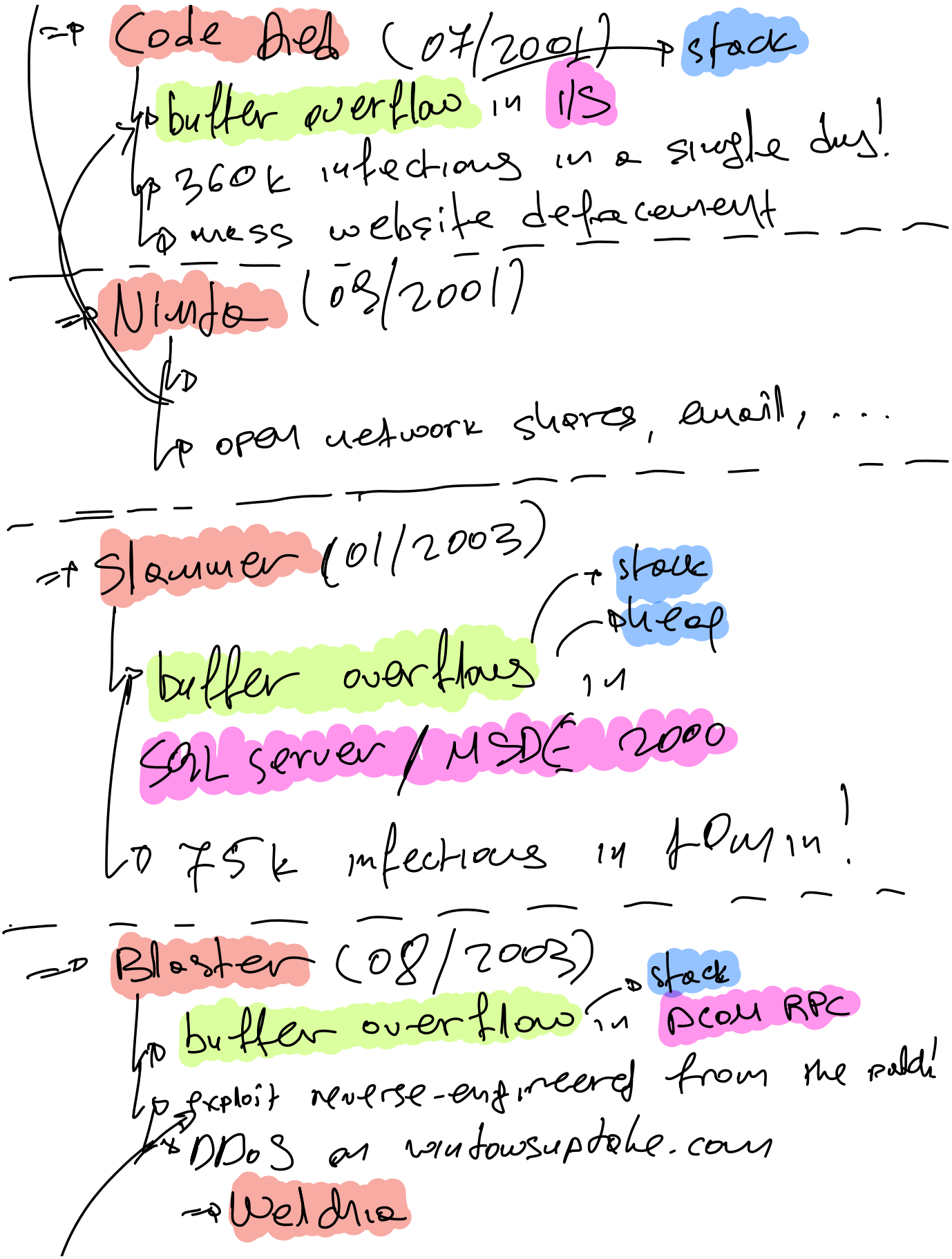

mem. safety violation
fuzzing
program testing
symbolic methods
symbolic execution
abstract interpretation
spatial errors
temporal errors
code/data ptr. corruption
control-flow hijacking
code injection
code reuse
Arbitrary computation(s)


mem. safety violation
fuzzing
program testing
symbolic methods
symbolic execution
abstract interpretation
spatial errors
temporal errors
code/data ptr. corruption
?
control-flow hijacking
code injection
...
code reuse
...
Arbitrary computation(s)

Why Software Security and Exploitation Matters.

⇒ Morris Worm (11/1988) → stack.
- ↳ buffer overflow in fingerd } + password guessing
- ↳ sendmail trapdoor (DEBUG)
- ↳ DEC VAX (4BSD), Sun-3 (SunOS)
- ↳ 200 - 10M (OS GAO)
- ↳ ~6k USENIX machines got infected.
  - ↳ ~10% of the total "Internet"
- ↳ 1st felony convictions under the Computer Fraud and Abuse Act.
- ↳ DARPA ⇒ CERT/CC

⇒ Sadmind (05/2001) → stack (brute force)
- ↳ buffer overflow in sdtuning
  - ↳ Solaris/SunOS
- ↳ access control bypass in IIS
- ↳ mass website defacement
  - ↳ anti-US messages


Code Red (07/2001)
stack
buffer overflow in IIS
360k infections in a single day!
mass website defacement
Nimda (09/2001)
open network shares, email, ...
Slammer (01/2003)
stack
heap
buffer overflows in
SQL server / MSDE 2000
75k infections in 10min!
Blaster (08/2003)
stack
buffer overflow in DCOM RPC
exploit reverse-engineered from the patch!
DDoS on windowsupdate.com
Welchia

- Sasser (04/2003)
  - buffer overflow in LSASS → stack.
  - AFP, Delta Air Lines, Sampo Bank, British Coastguard, Goldman Sachs, Deutsche Post, European Commission, Lund University Hospital (X-rays), University of Missouri, ...

- Conficker (11/2008)
  - buffer overflow in NetBIOS → stack
  - BM - ISM infections
  - Botnet! (+ self-defense)
  - French Navy, UK Ministry of Defense, Sheffield Hospital, German Bundestag, Norwegian Police, ...

=> Stuxnet (06/2010)

- cyberweapon (~2006) -> Israel(?)
  - SCADA/PLC
- function-pointer overwrite in kernel in Windows
- access control bypass in Print Spooler
- unauthorized direct code execution in windows Shell
- ~200k/1k PLCs hosts
  - ~58% in Iran
- kernel-mode rootkit
  - signed driver.
    - 2x compromised certificates
- man-in-the-middle -> Step 7

⇒ Dooqu (09/2011)
- memory corruption
  - kernel
  - heap
- code "similar" to Stuxnet
- intelligence gathering

⇒ Flame (05/2012)
- cyber espionage
- (most sophisticated piece of malware at the time.
  - targets Middle Eastern Countries)

- access control bypass in Print Spooler
- unauthorized direct code execution in windows Shell

⇒ Compromises Microsoft Certificate
- sign a fake audio driver rootkit

- Mirai (08/2016)
  - authentication bypass
    - IoT devices
    - 600k infections
    - 1 Tbit/s DDoS attack!

- WannaCry (05/2017)
  - integer overflow
    - kernel
    - memory OOB
    - } NSA's exploit
  - heap spraying + massage
    - code-reuse + code injection
  - ransomware
    - ~200k infections
      - UK's NHS
      - Nissan
      - Renault
      - Telefonica
      - FedEx
      - ...

Thank you :)