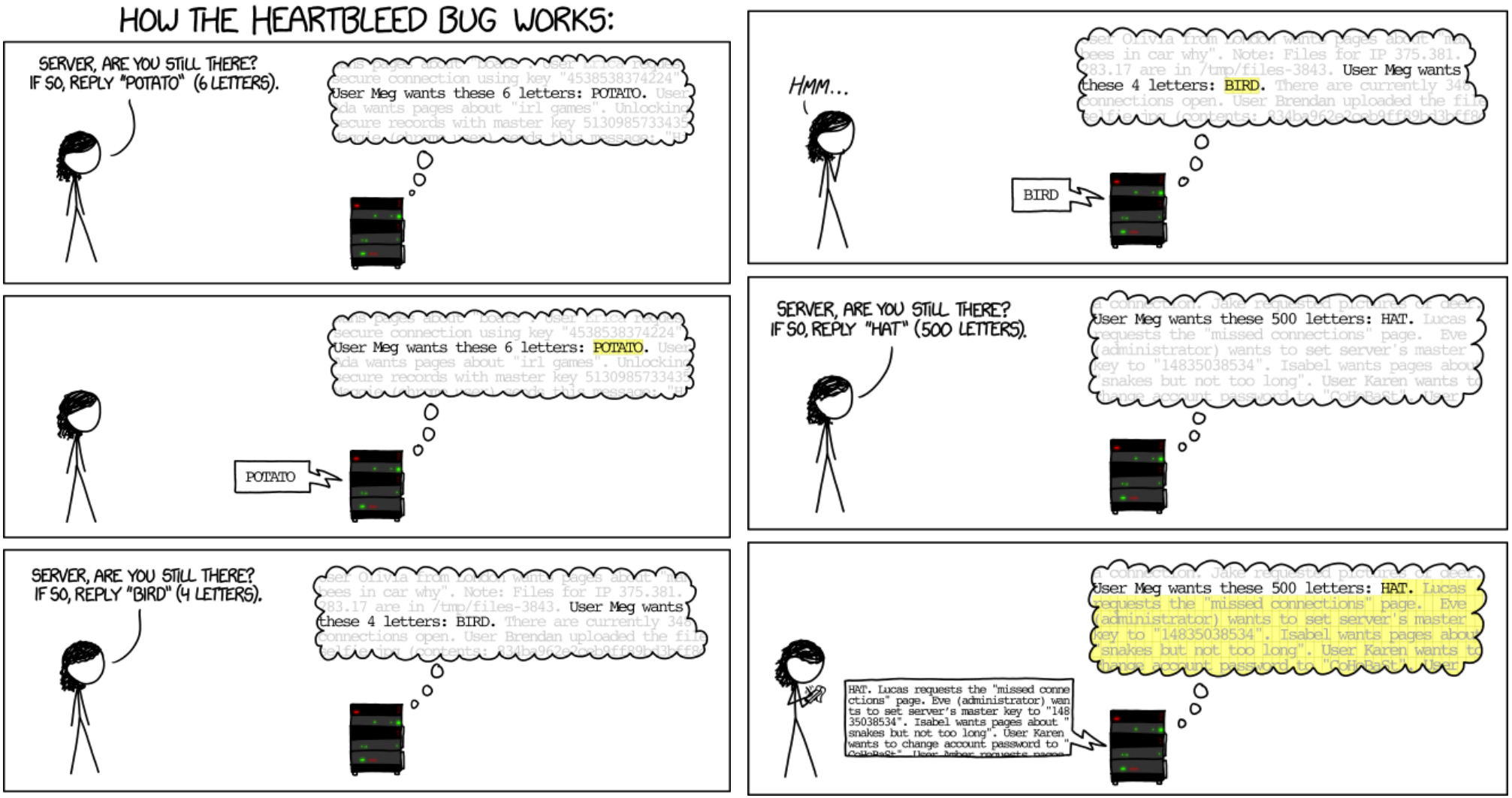
Software Security

Domenico Cotroneo
Roberto Natella

Challenge: Fuzzing OpenSSL

- OpenSSL è una libreria che implementa i protocolli TLS (Transport Layer Security) ed SSL (Secure Socket Layer)
- Nel 2014, è stata riscontrata una vulnerabilità buffer over-read (CVE-2014-0160) nel componente Heartbeat Extension
- È possibile identificarla usando ASAN ed AFL
- La versione vulnerabile della libreria è:
  - https://ftp.openssl.org/source/old/1.0.1/openssl-1.0.1f.tar.gz
- Per suggerimenti e soluzioni:
  - https://github.com/mykter/afl-training/tree/master/challenges/heartbleed

Challenge: Fuzzing OpenSSL



Challenge: Fuzzing OpenSSL

- Compilare OpenSSL abilitando ASAN

```
$ AFL_USE_ASAN=1 CC=afl-clang-fast CXX=afl-clang-fast++ ./config -d –g
$ make
```

- Compilare il test harness abilitando ASAN

```
$ AFL_USE_ASAN=1 afl-clang-fast target.c -o target openssl/libssl.a openssl/libcrypto.a -I openssl/include -ldl
```

Challenge: Fuzzing OpenSSL

- Creare un certificato fittizio

```
$ openssl req -x509 -newkey rsa:512 -keyout
server.key -out server.pem -days 365 -nodes -subj
/CN=a/
```

- Avviare il test harness con AFL

```
$ afl-fuzz -i in -o out -m none -t 5000 ./target
```