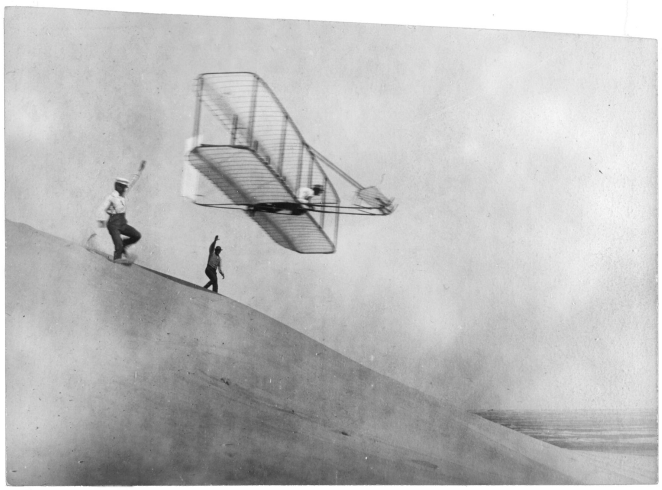
Access Control and Privacy Policies (10)

Email: christian.urban at kcl.ac.uk
Office: S1.27 (1st floor Strand Building)

Slides: KEATS (also homework is there)

Revision

Security Engineering



Wright brothers, 1901

Airbus, 2005

1st Lecture

- chip-and-pin, banks vs. customers

  the one who can improve security should also be liable for the losses

1st Lecture

- chip-and-pin, banks vs. customers

  the one who can improve security should also be liable for the losses

- hashes and salts to guarantee data integrity
- storing passwords (you should know the difference between brute force attacks and dictionary attacks; how do salts help?)

1st Lecture: Cookies

- good uses of cookies?
- bad uses of cookies: snooping, tracking, profiling...the "disadvantage" is that the user is in control, because you can delete them

"Please track me using cookies."

1st Lecture: Cookies

- good uses of cookies?
- bad uses of cookies: snooping, tracking, profiling...the "disadvantage" is that the user is in control, because you can delete them

  "Please track me using cookies."

- fingerprinting beyond browser cookies

  Pixel Perfect: Fingerprinting Canvas in HTML5
  (a research paper from 2012)
  http://cseweb.ucsd.edu/~hovav/papers/ms12.html

1st Lecture: Cookies

- a bit of JavaScript and HTML5 + canvas

Firefox

55b2257ad0f20ecbf927fb66a15c61981f7ed8fc

Safari

17bc79f8111e345f572a4f87d6cd780b445625d3

- no actual drawing needed

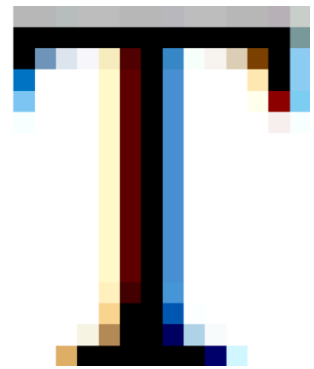
1st Lecture: Cookies

- a bit of JavaScript and HTML5 + canvas

Firefox

55b2257ad0f20ecbf927fb66a15c61981f7ed8fc

Safari



17bc79f8111e345f572a4f87d6cd780b445625d3

- no actual drawing needed
- in May 2014 a crawl of 100,000 popular webpages revealed 5.5% already use canvas fingerprinting

https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf

1st Lecture: Cookies

Remember the small web-app I showed where a cookie protected a counter

- NYT, the cookie looks the "resource" - harm
- imaginary discount unlocked by cookie - no harm

2nd Lecture: E-Voting

Where are paper ballots better than voice voting?

- Integrity
- Ballot Secrecy
- Voter Authentication
- Enfranchisement
- Availability

2nd Lecture: E-Voting

- (two weeks ago) an Australian parliamentary committee found: e-voting is highly vulnerable to hacking and Australia will not use it any time soon

2nd Lecture: E-Voting

- (two weeks ago) an Australian parliamentary committee found: e-voting is highly vulnerable to hacking and Australia will not use it any time soon

- Alex Halderman, Washington D.C. hack

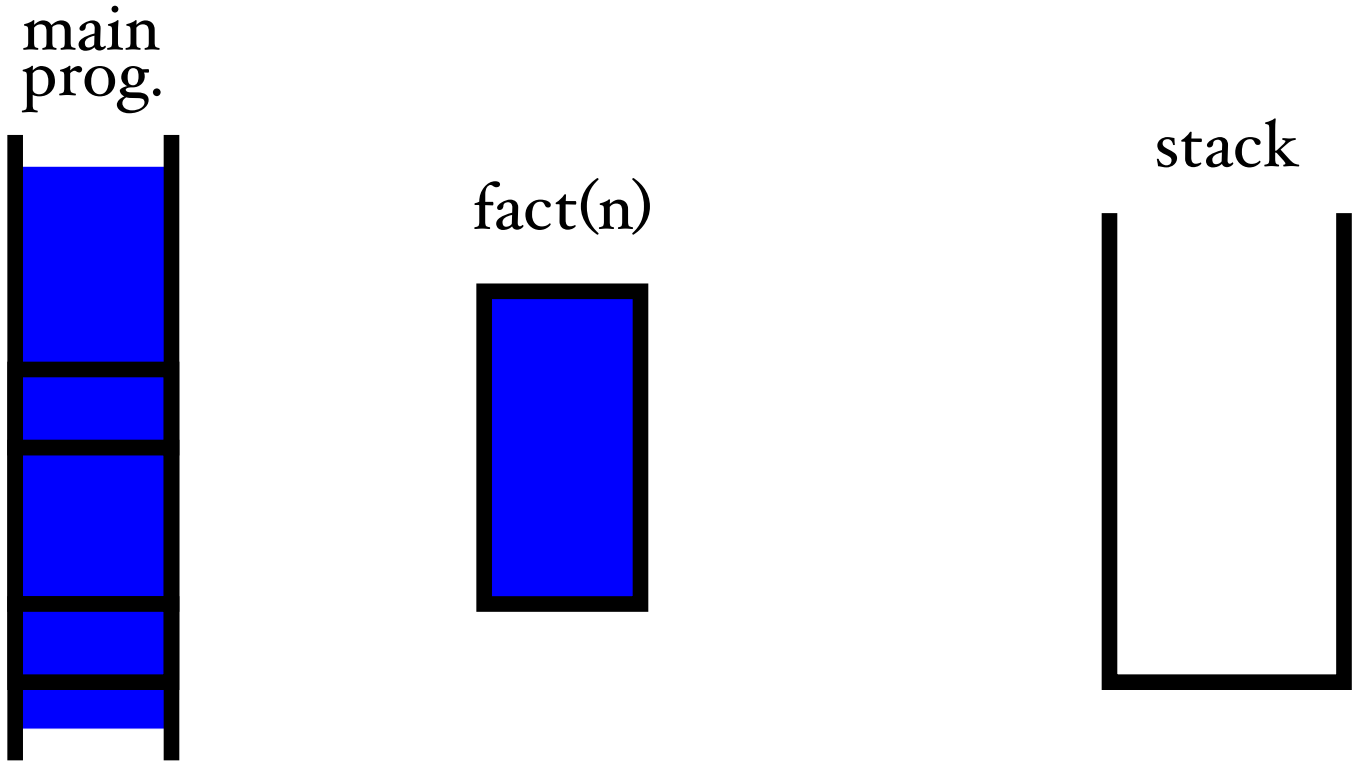
  https://jhalderm.com/pub/papers/dcvoting-fc12.pdf

- PDF-ballot tampering at the wireless router (the modification is nearly undetectable and leaves no traces; MITM attack with firmware updating)

  http://galois.com/wp-content/uploads/2014/11/technical-hack-a-pdf.pdf

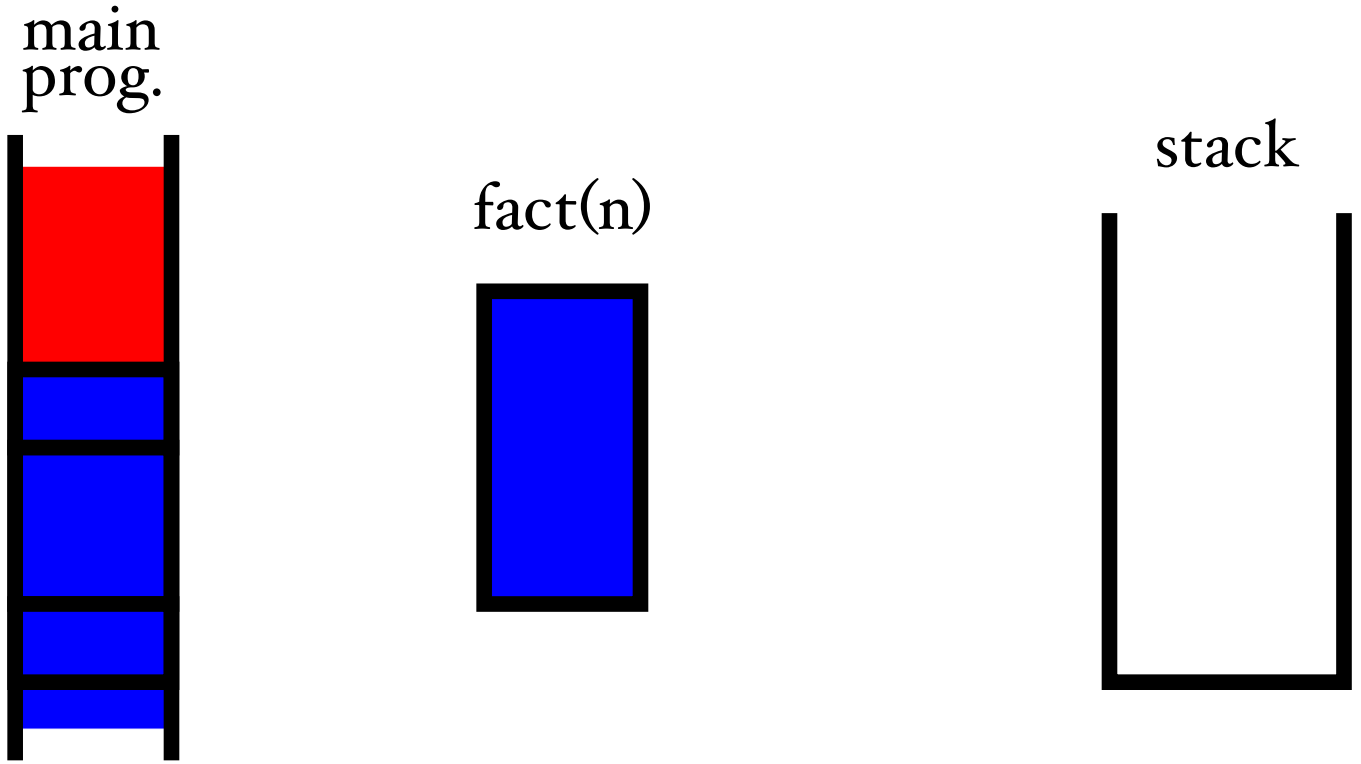
3rd Lecture: Buffer Overflow Attacks

- the problem arises from the way C/C++ organises its function calls



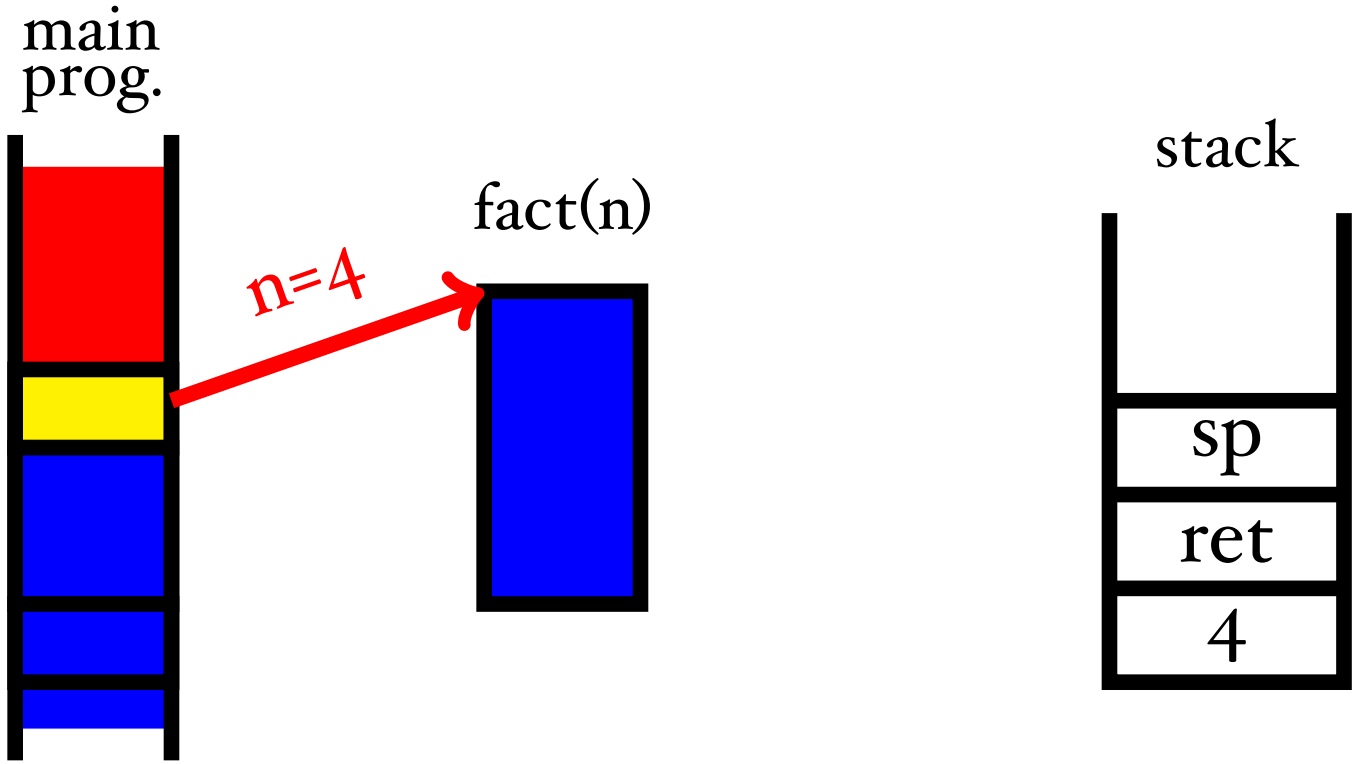
3rd Lecture: Buffer Overflow Attacks

- the problem arises from the way C/C++ organises its function calls



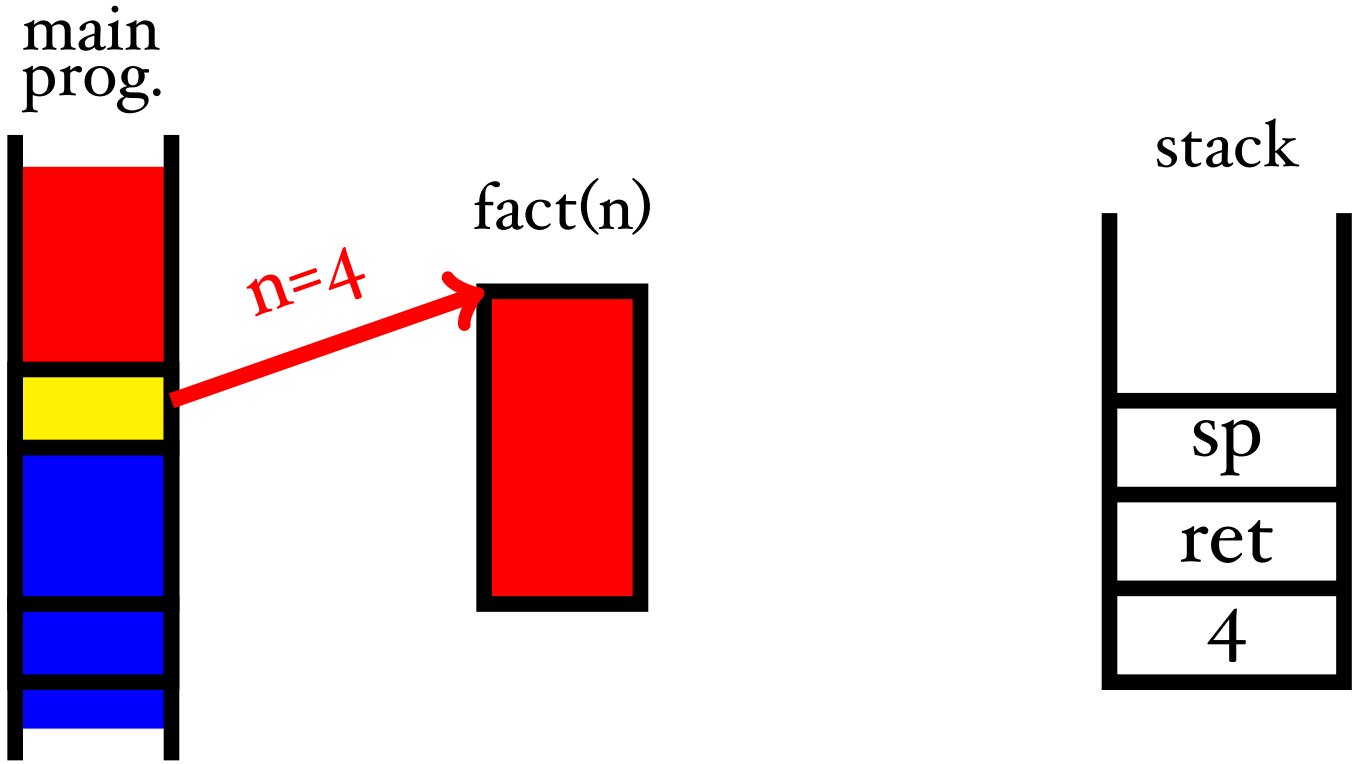
3rd Lecture: Buffer Overflow Attacks

- the problem arises from the way C/C++ organises its function calls



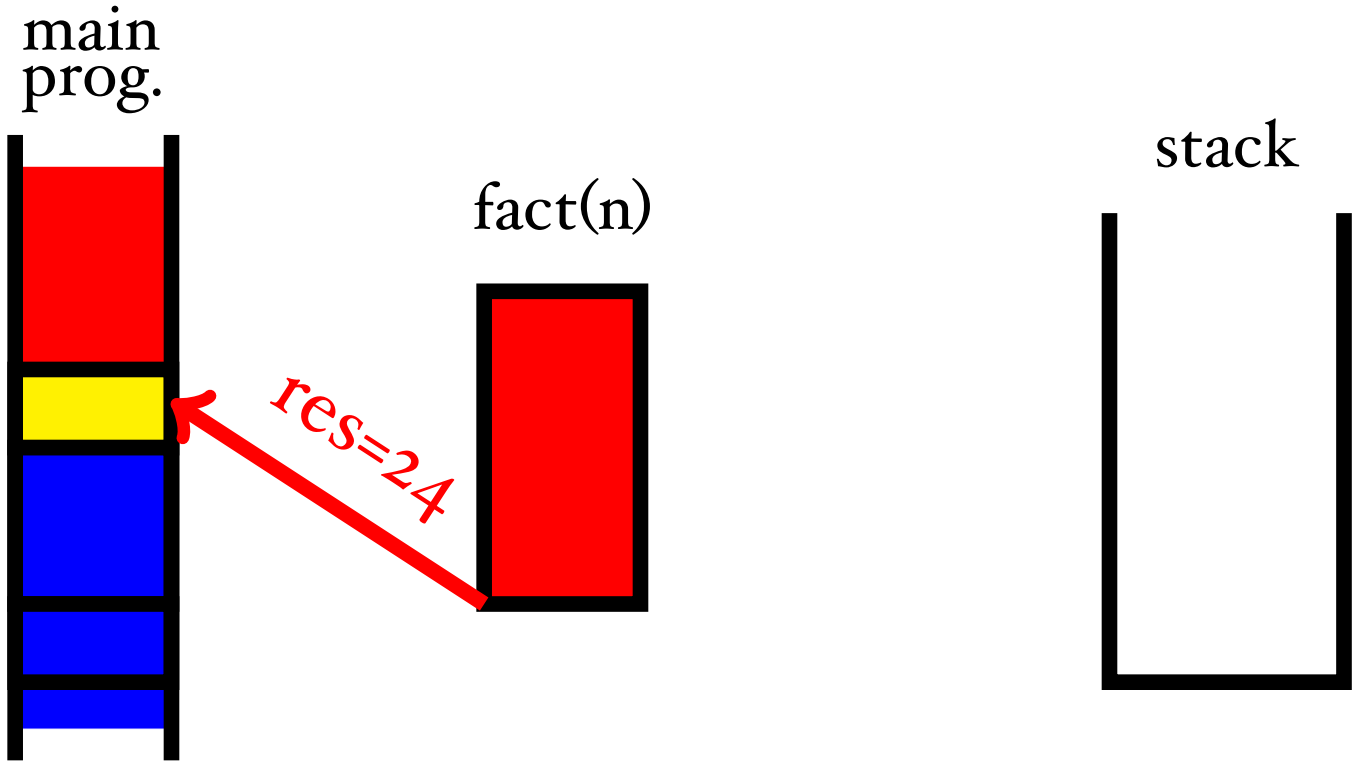
3rd Lecture: Buffer Overflow Attacks

- the problem arises from the way C/C++ organises its function calls



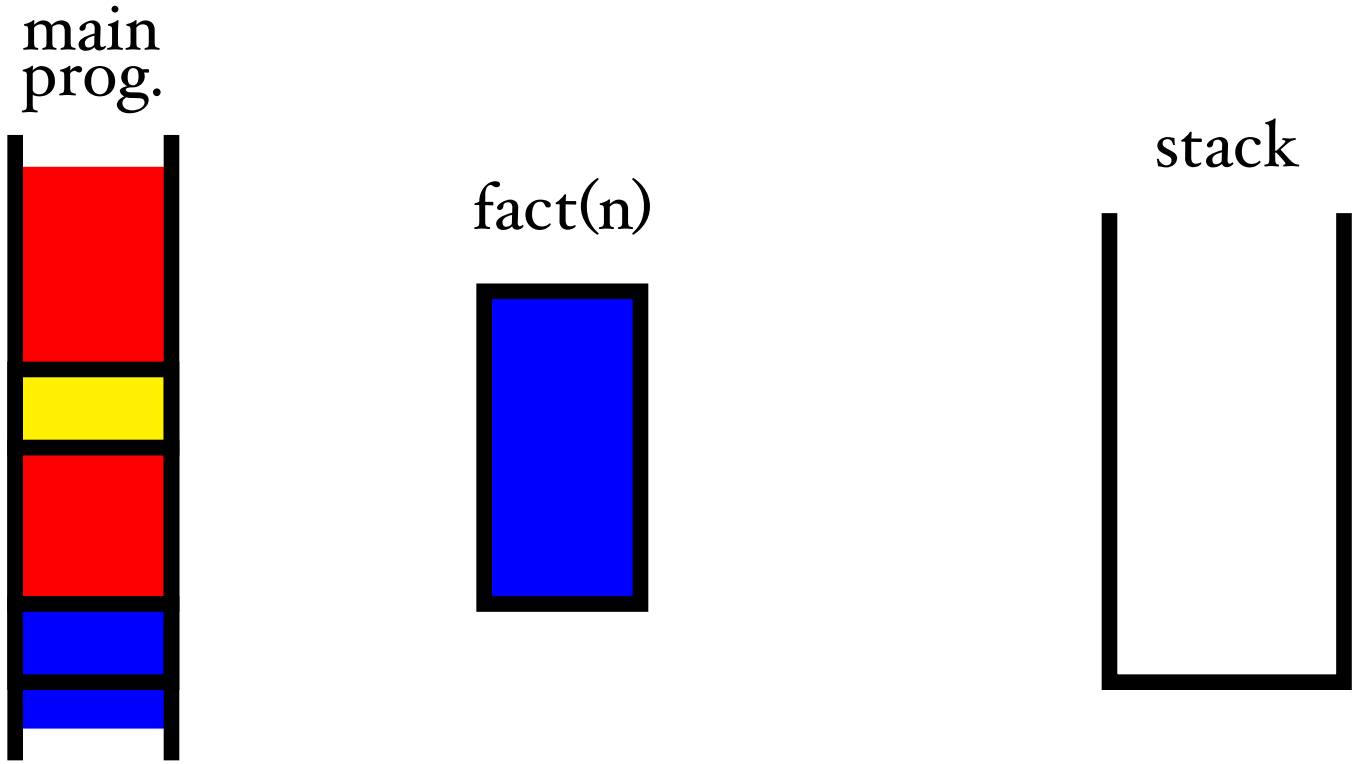
3rd Lecture: Buffer Overflow Attacks

- the problem arises from the way C/C++ organises its function calls



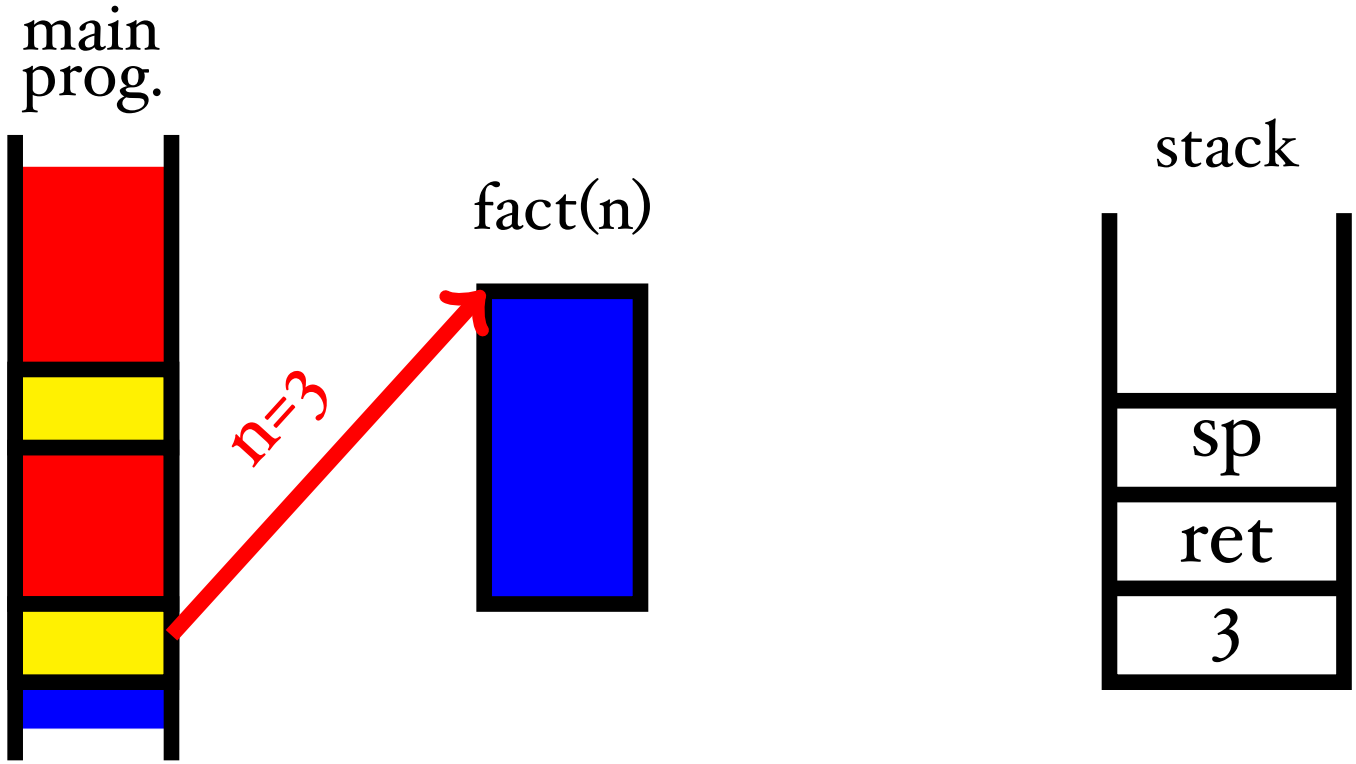
3rd Lecture: Buffer Overflow Attacks

- the problem arises from the way C/C++ organises its function calls



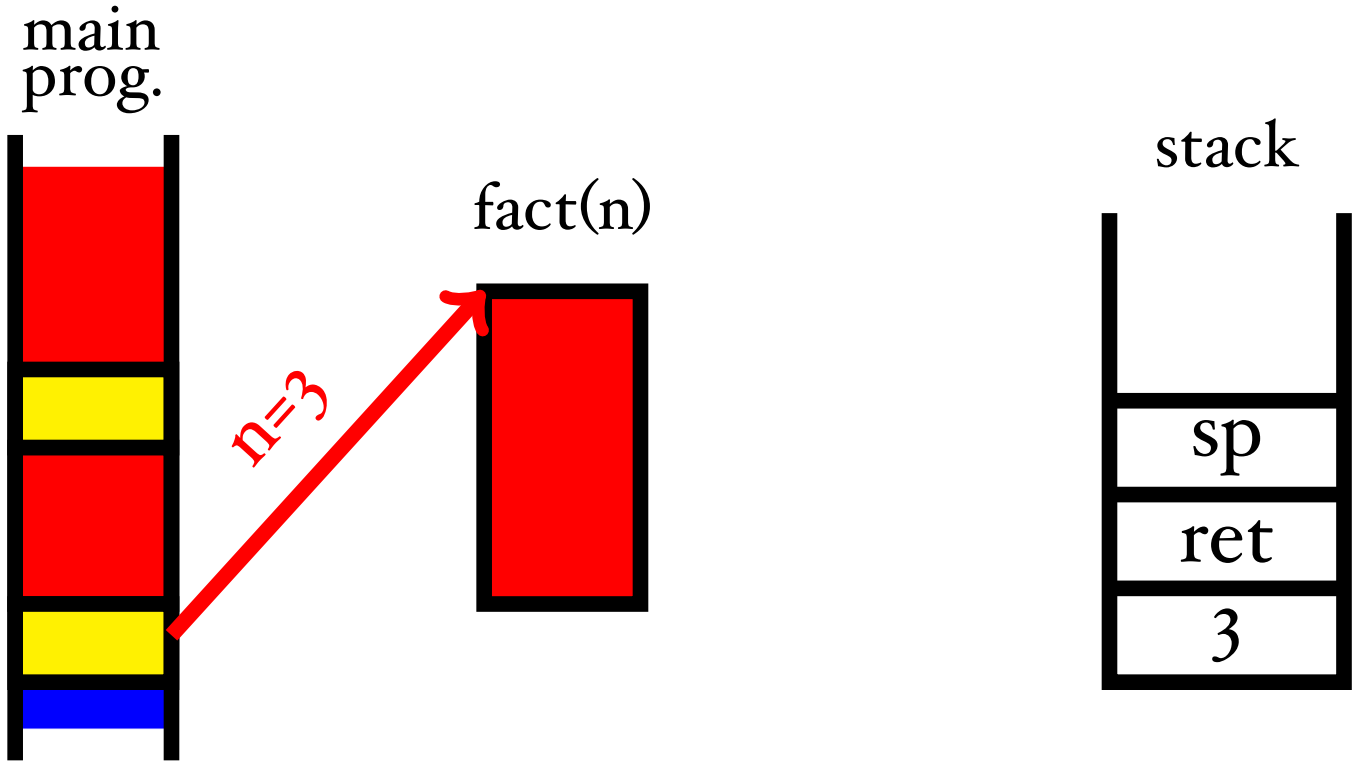
3rd Lecture: Buffer Overflow Attacks

- the problem arises from the way C/C++ organises its function calls



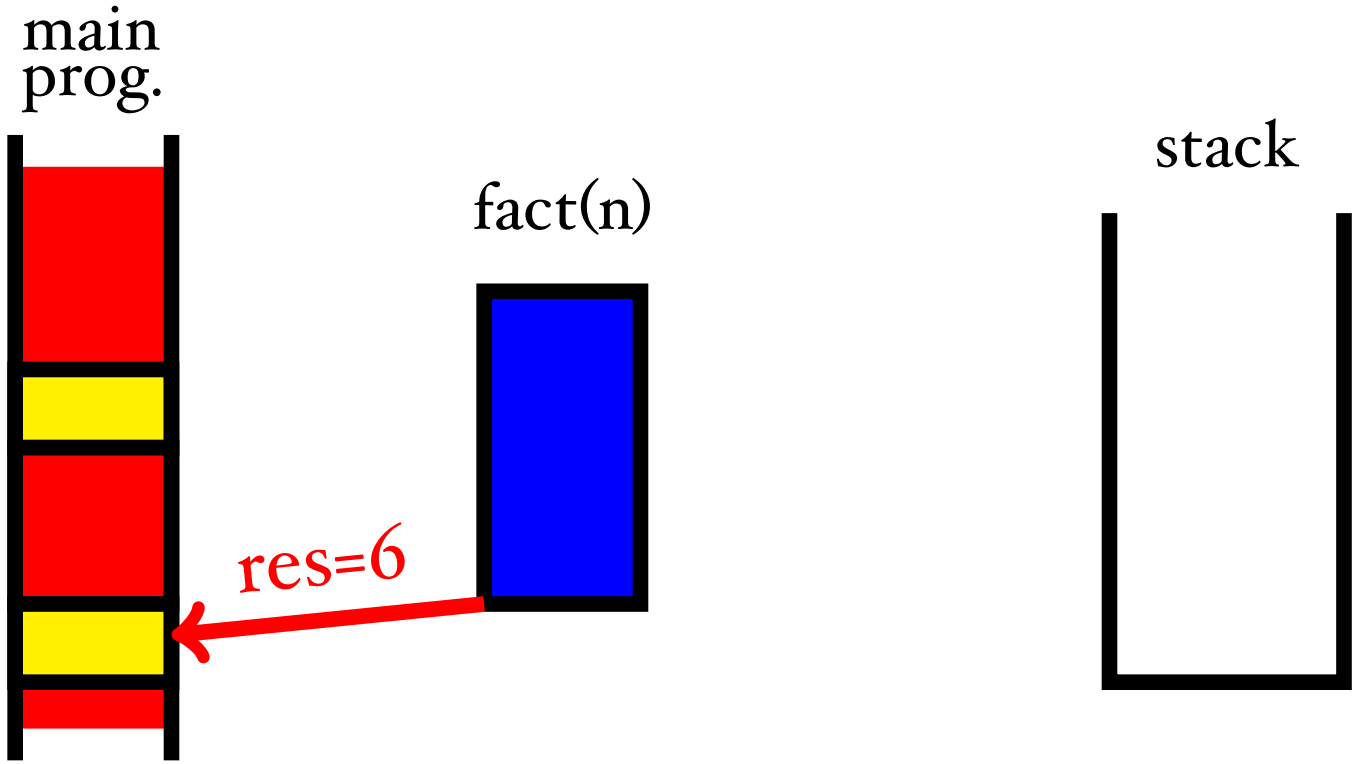
3rd Lecture: Buffer Overflow Attacks

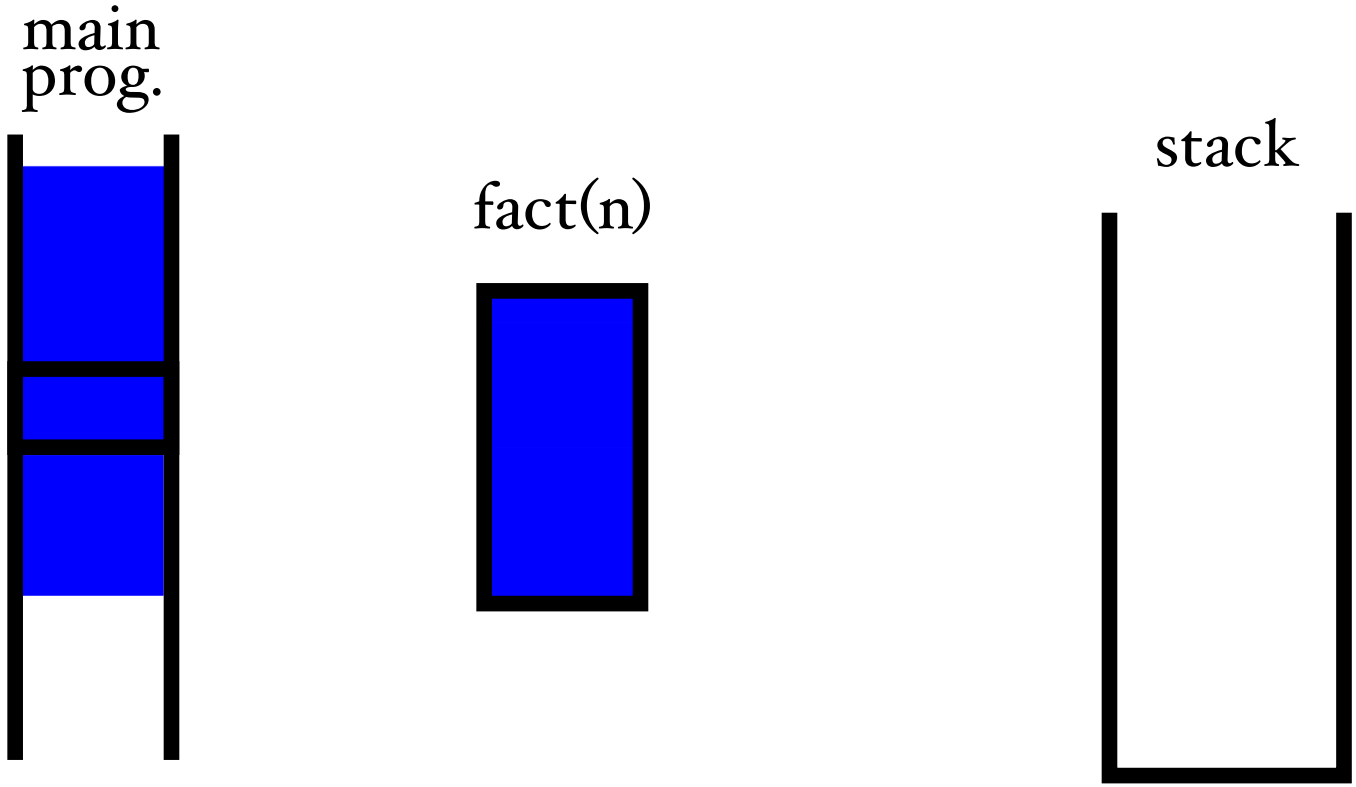
- the problem arises from the way C/C++ organises its function calls

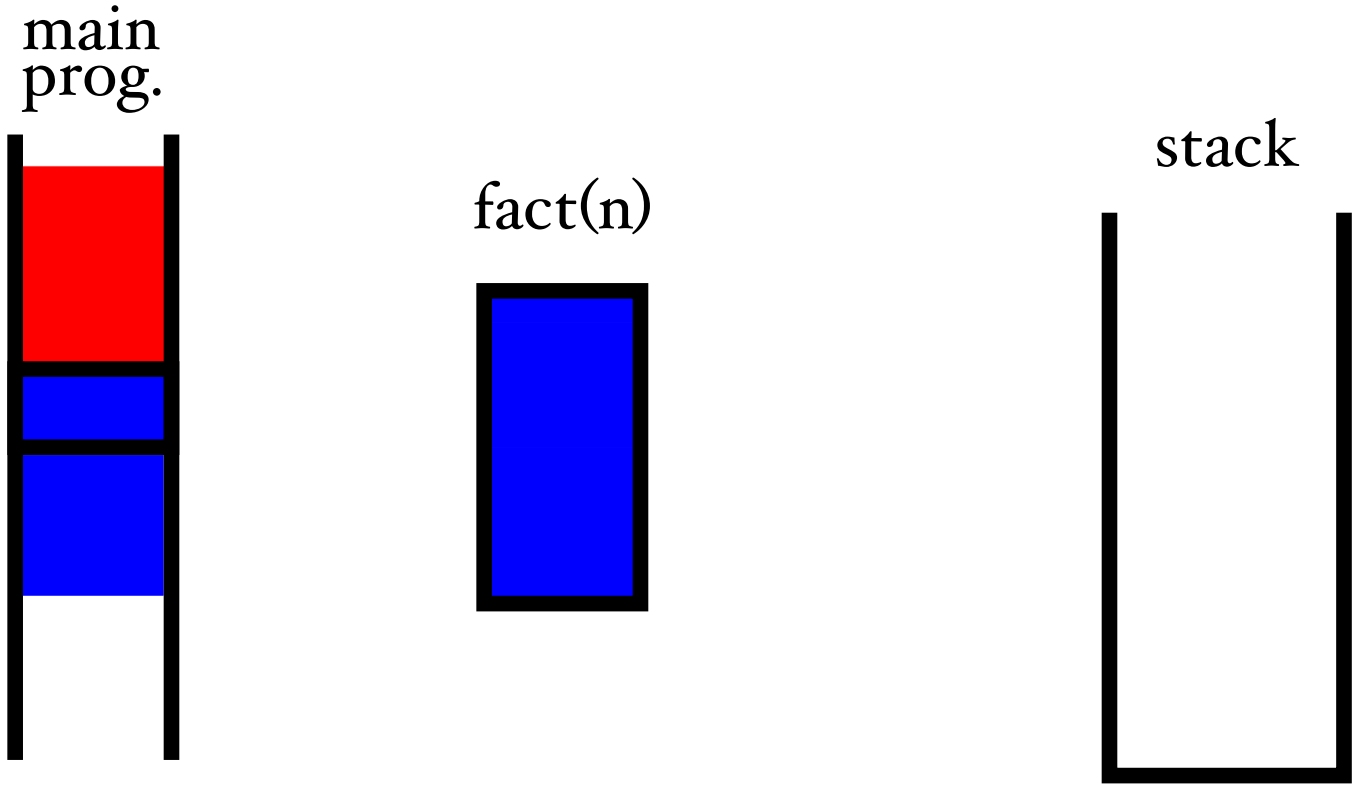


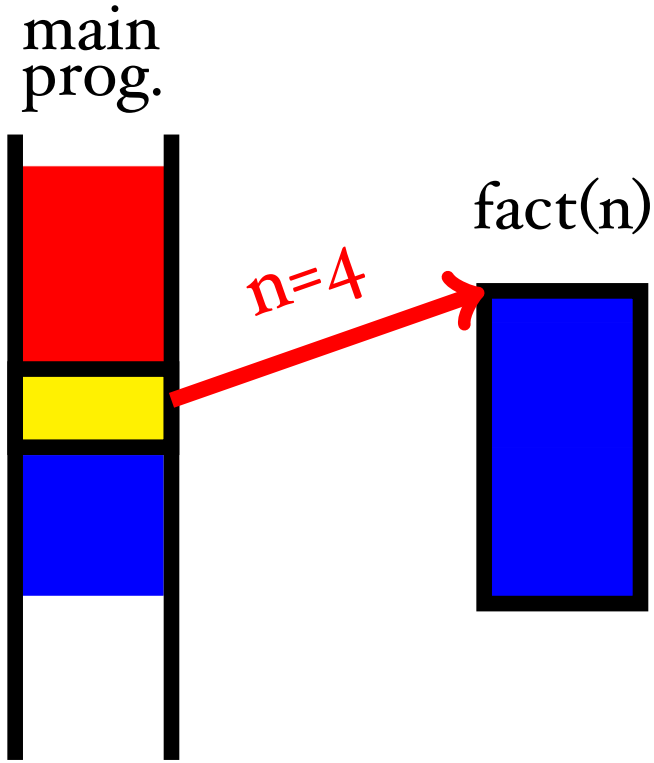
3rd Lecture: Buffer Overflow Attacks

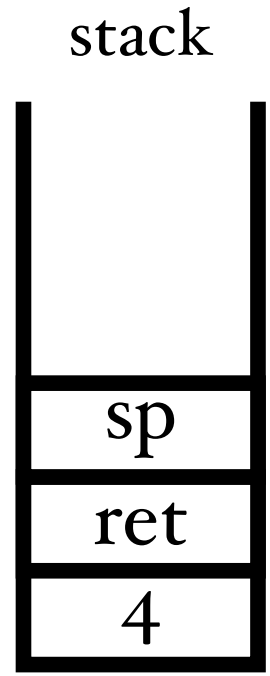
- the problem arises from the way C/C++ organises its function calls

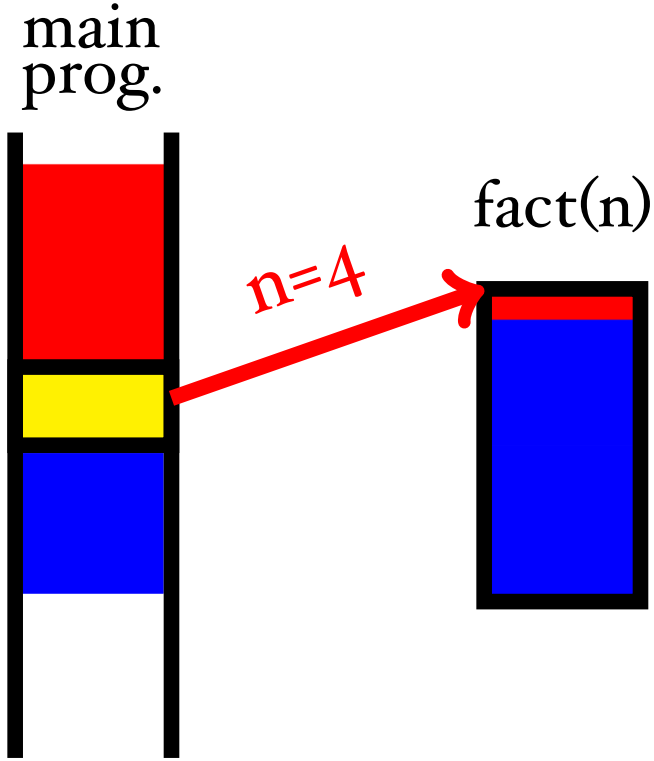


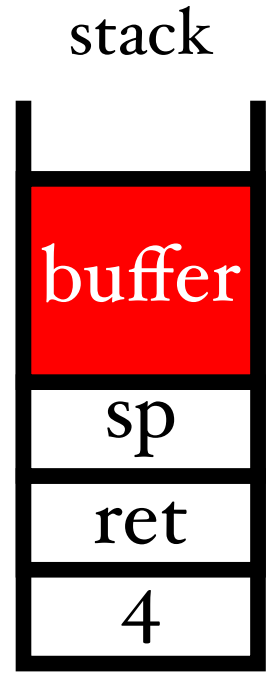

main
prog.
fact(n)
stack

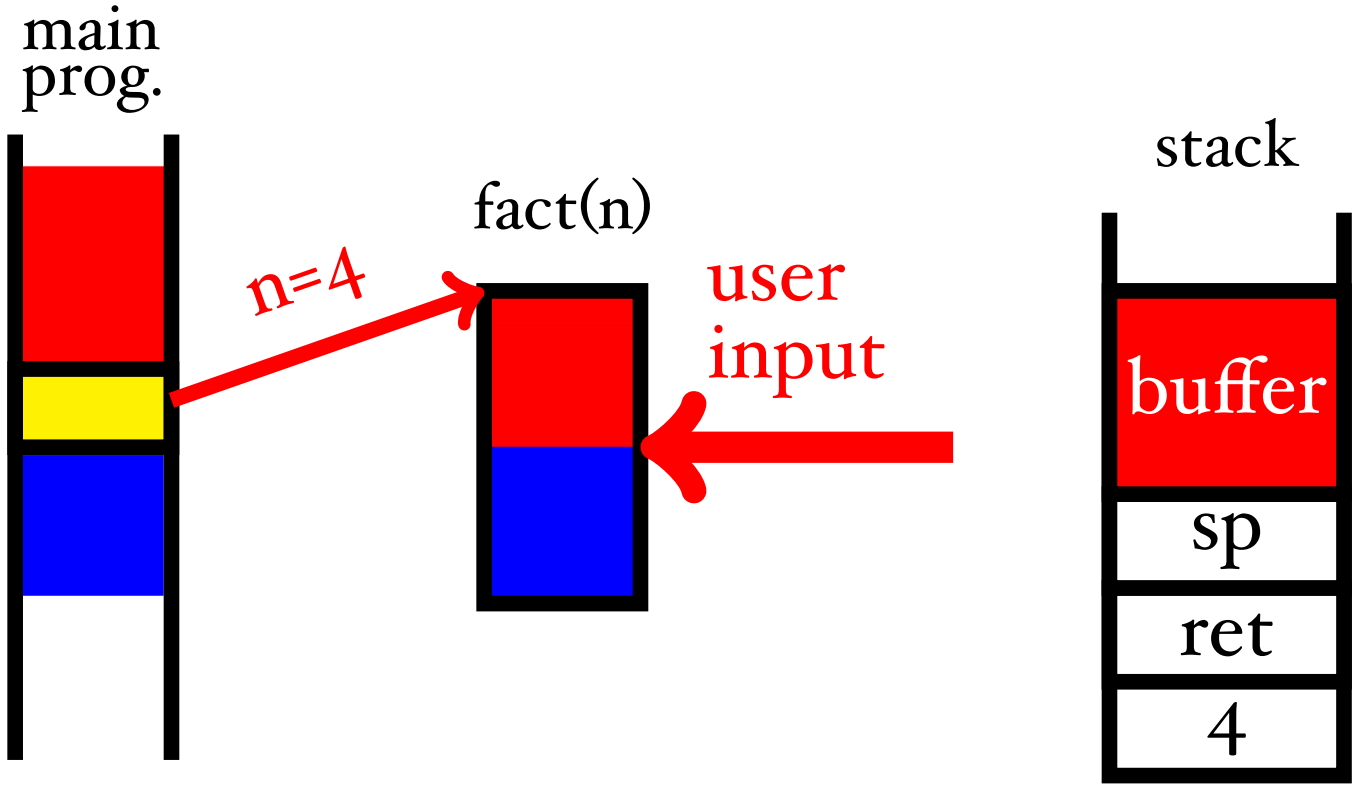

main
prog.
fact(n)
stack

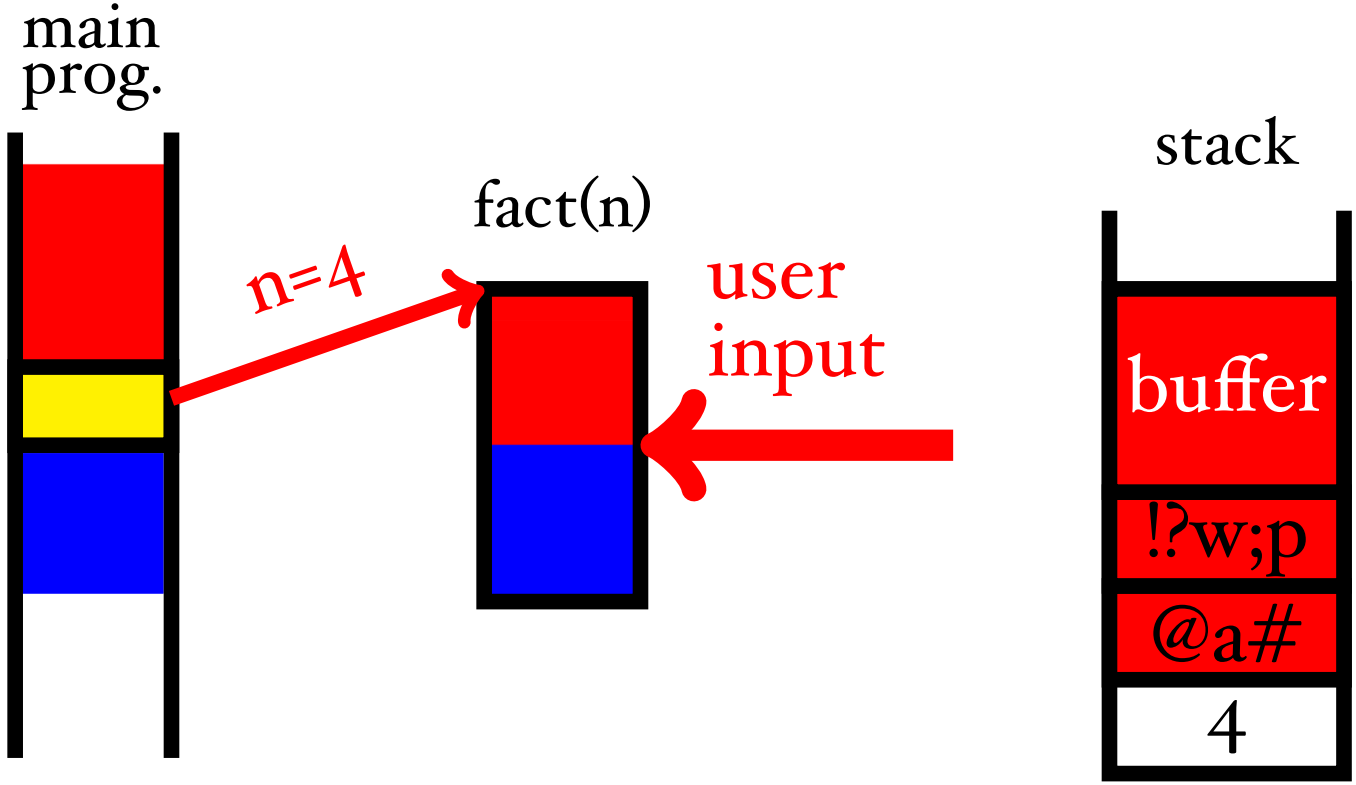

main
prog.
fact(n)
n=4

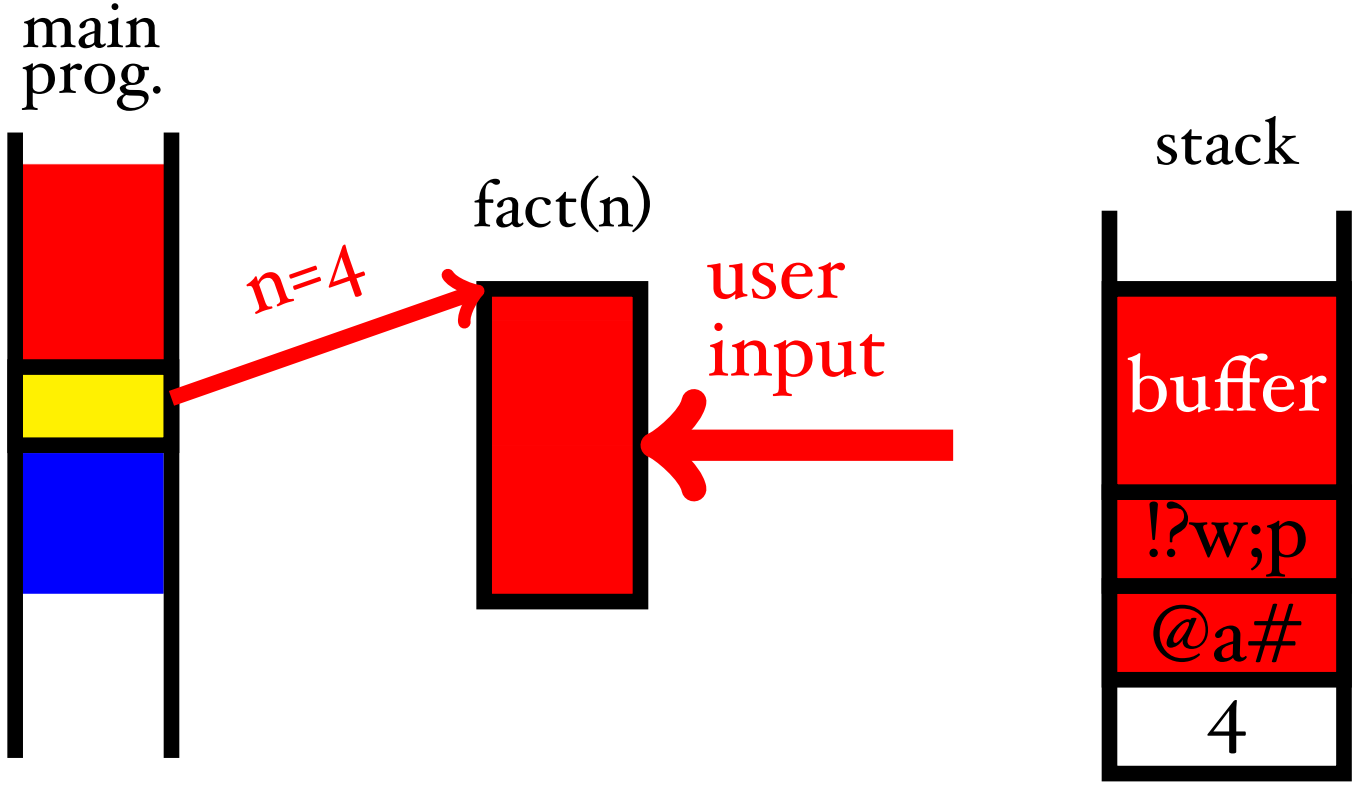

stack
sp
ret
4

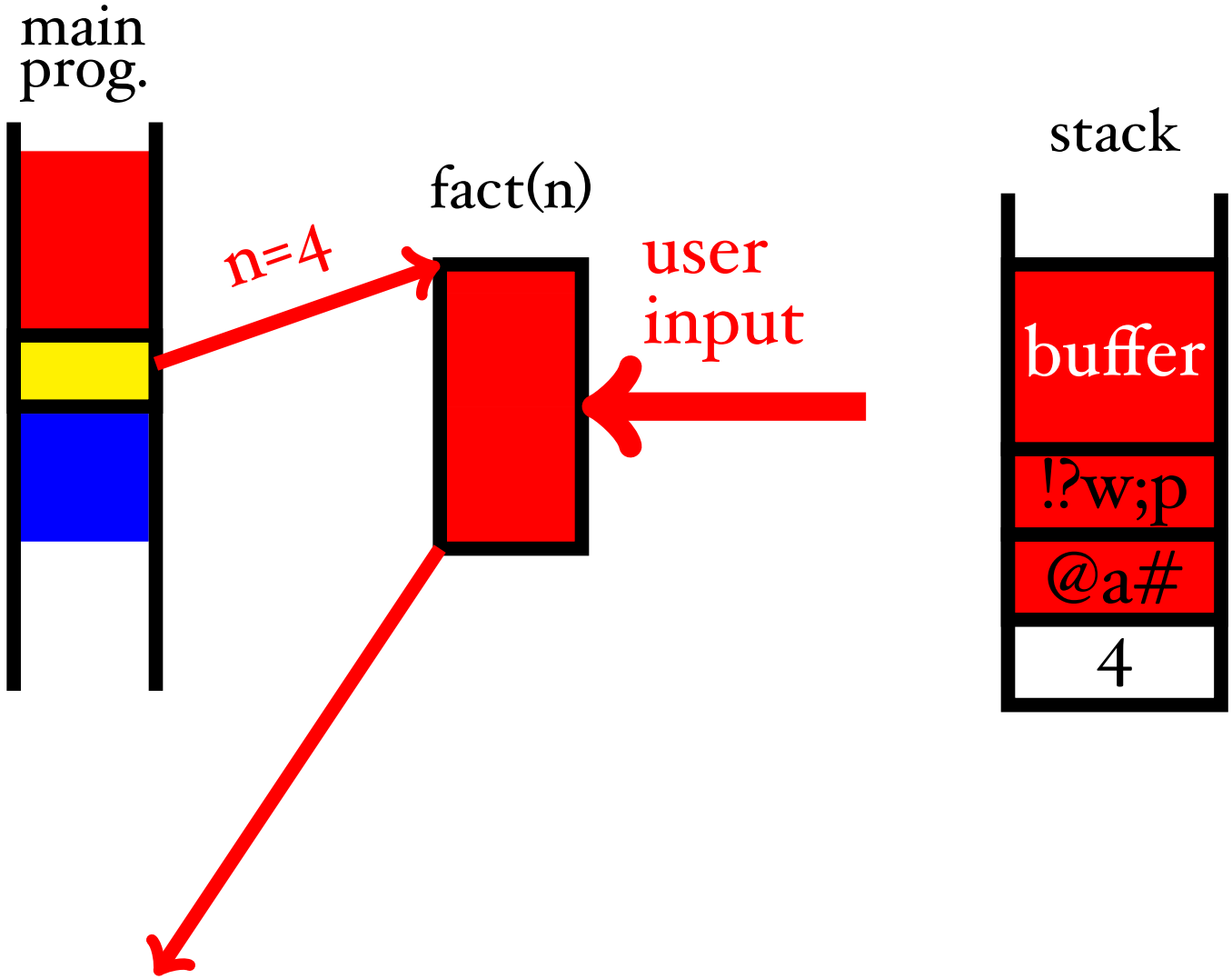

main
prog.
fact(n)
n=4


stack
buffer
sp
ret
4


main
prog.
n=4
fact(n)
user
input
stack
buffer
sp
ret
4

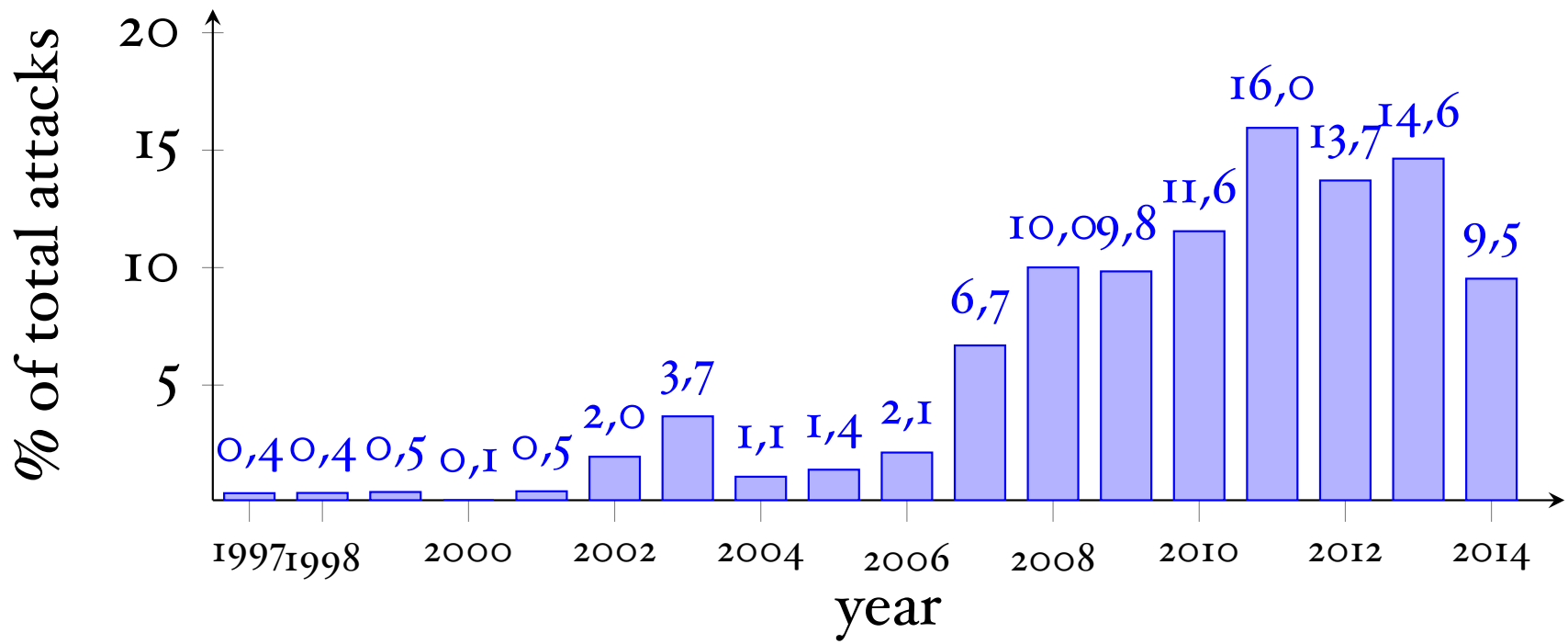

main
prog.
n=4
fact(n)
user
input
stack
buffer
!?w;p
@a#
4


main
prog.
n=4
fact(n)
user
input
stack
buffer
!?w;p
@a#
4


main
prog.
n=4
fact(n)
user
input
stack
buffer
!?w;p
@a#
4

3rd Lecture: Buffer Overflow Attacks

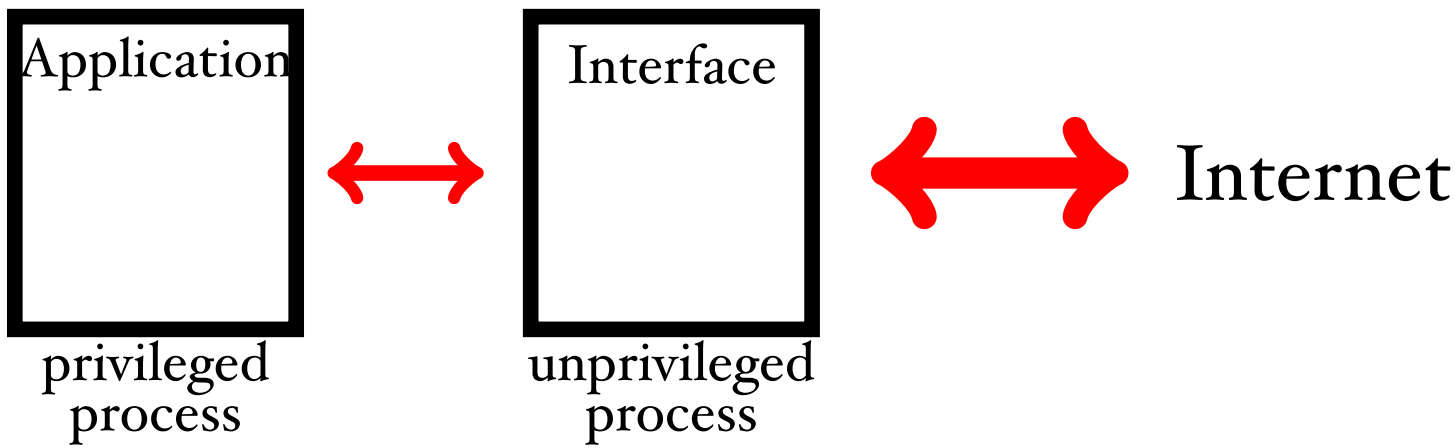
US National Vulnerability Database
(636 out of 6675 in 2014)



http://web.nvd.nist.gov/view/vuln/statistics

4rd Lecture: Unix Access Control

- privileges are specified by file access permissions ("everything is a file")



- the idea is to make the attack surface smaller and mitigate the consequences of an attack

4rd Lecture: Unix Access Control

- when a file with setuid is executed, the resulting process will assume the UID given to the owner of the file

```
$ ls -ld . * */*
drwxr-xr-x 1 ping staff  32768 Apr  2 2010 .
-rw----r-- 1 ping students  31359 Jul 24 2011 manual.txt
-r--rw--w- 1 bob students    4359 Jul 24 2011 report.txt
-rwsr--r-x 1 bob students  141359 Jun  1 2013 microedit
dr--r-xr-x 1 bob staff      32768 Jul 23 2011 src
-rw-r--r-- 1 bob staff      81359 Feb 28 2012 src/code.c
-r--rw---- 1 emma students    959 Jan 23 2012 src/code.h
```

4rd Lecture: Unix Access Control

- Alice wants to have her files readable, except for her office mates.

5rd Lecture: Protocols

Simple Challenge Response
(solving the replay problem):

$$
\begin{array}{lll}
A \rightarrow B: & \text{Hi I am A} & \\
B \rightarrow A: & N & \text{(challenge)} \\
A \rightarrow B: & \{N\}_{K_{AB}} &
\end{array}
$$

5rd Lecture: Protocols

Simple Challenge Response
(solving the replay problem):

$$
\begin{array}{lll}
A \to B: & \text{Hi I am A} & \\
B \to A: & N & \text{(challenge)} \\
A \to B: & \{N\}_{K_{AB}} &
\end{array}
$$

Mutual Challenge Response:

$$
\begin{array}{lll}
A \to B: & N_A & \\
B \to A: & \{N_A, N_B\}_{K_{AB}} & \\
A \to B: & N_B &
\end{array}
$$

5rd Lecture: Protocols

A car-transponder protocol:

1. C generates a random number N
2. C calculates $(F, G) = \{N\}_K$
3. $C \to T$: N, F
4. T calculates $(F', G') = \{N\}_K$
5. T checks that $F = F'$
6. $T \to C$: N, G'
7. C checks that $G = G'$

Authentication: $T \to C$, $C \to T$?

5rd Lecture: Protocols

The interlock protocol ("best bet" against MITM):

1. $A \rightarrow B : K_A^{pub}$
2. $B \rightarrow A : K_B^{pub}$
3. $\{A, m\}_{K_B^{pub}} \mapsto H_1, H_2$
   $\{B, m'\}_{K_A^{pub}} \mapsto M_1, M_2$
4. $A \rightarrow B : H_1$
5. $B \rightarrow A : \{H_1, M_1\}_{K_A^{pub}}$
6. $A \rightarrow B : \{H_2, M_1\}_{K_B^{pub}}$
7. $B \rightarrow A : M_2$

5rd Lecture: Protocols

The interlock protocol ("best bet" against MITM):

1. $A \rightarrow B : K_A^{pub}$
2. $B \rightarrow A : K_B^{pub}$
3. $\{A, m\}_{K_B^{pub}} \mapsto H_1, H_2$
   $\{B, m'\}_{K_A^{pub}} \mapsto M_1, M_2$
4. $A \rightarrow B : H_1$
5. $B \rightarrow A : \{H_1, M_1\}_{K_A^{pub}}$
6. $A \rightarrow B : \{H_2, M_1\}_{K_B^{pub}}$
7. $B \rightarrow A : M_2$

m = How is your grandmother? m' = How is the weather today in London?

Access Control Logic

Ross Anderson about the use of Logic:

> "Formal methods can be an excellent way of finding bugs in security protocol designs as they force the designer to make everything explicit and thus confront difficult design choices that might otherwise be fudged."

Access Control Logic

$$
\begin{array}{rcl}
F & ::= & \mathit{true} \\
 & | & \mathit{false} \\
 & | & a(t_1, \ldots, t_n) \\
 & | & F_1 \wedge F_2 \\
 & | & F_1 \vee F_2 \\
 & | & F_1 \Rightarrow F_2 \\
 & | & P \ \mathit{says}\ F
\end{array}
$$

where $P = \mathit{Alice}, \mathit{Bob}, \mathit{Christian}$

- $\mathit{HoD}\ \mathit{says}\ \mathit{is\_staff}(\mathit{Christian})$

Access Control Logic

...can be used for answering the following questions:

- To what conclusions does this protocol come?
- What assumptions are needed for this protocol?
- Does the protocol uses unnecessary actions, which can be left out?
- Does the protocol encrypt anything which could be sent in plain, without weakening the security?

5th Lecture: Protocols

An article in The Guardian from 2013 reveals how GCHQ and the NSA at a G20 Summit in 2009 sniffed emails from Internet cafes, monitored phone calls from delegates and attempted to listen on phone calls which were made by Russians and which were transmitted via satellite links:

`http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits`

6th Lecture: Zero-Knowledge Proofs

Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer

Roel Verdult[1], Flavio D. Garcia[2], and Barış Ege[1]

[1] Institute for Computing and Information Sciences,
Radboud University Nijmegen, The Netherlands.
(rverdult,b.ege)@cs.ru.nl

[2] School of Computer Science,
University of Birmingham, United Kingdom.
f.garcia@cs.bham.ac.uk

1 Disclaimer

Due to a interim injunction, ordered by the High Court of London on Tuesday 25th June 2013, the authors are restrained from publishing the technical contents of the scientific article *Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer* [1] until further notice.

2 Historical claim

Figure 1 contains the cryptographic hash (SHA-512) of the original final paper which was scheduled to appear in the proceedings of the 22nd USENIX Security Symposium, Washington DC, August 2013.

```
9d05ba88740499eecea3d8609174b444
43683da139f78b783666954ccc605da8
4601888134bf0c23ba46fb4a88c056bf
bbb629e1ddffcf60fa91880b4d5b4aca
```

Figure 1: SHA-512 hash of the final paper

References

1. Roel Verdult, Flavio D. Garcia, and Barış Ege. Dismantling megamos crypto: Wirelessly lockpicking a vehicle immobilizer. In *22nd USENIX Security Symposium (USENIX Security 2013)*. USENIX Association, 2013.

7th Lecture: Privacy

- de-anonymisation attacks
  (Netflix, DNA databases, ...)

7th Lecture: Privacy

- differential privacy for anonymising research data

User	tell me $f(x) \Rightarrow$	Database
	$\Leftarrow f(x) + \text{noise}$	$x_1, \ldots, x_n$

- $f(x)$ can be released, if f is insensitive to individual entries $x_1, \ldots, x_n$
- The intuition: whatever is learned from the dataset would be learned regardless of whether x_i participates

7th Lecture: Privacy

- differential privacy for anonymising research data

User	tell me $f(x) \Rightarrow$	Database
	$\Leftarrow f(x) + \text{noise}$	$x_1, \ldots, x_n$

- $f(x)$ can be released, if f is insensitive to individual entries $x_1, \ldots, x_n$
- The intuition: whatever is learned from the dataset would be learned regardless of whether x_i participates

8th Lecture: Bitcoins

- conclusion: not anonymous, not free from (potential) government interference

- The department has large labs full of computers that are pretty much idle over night. Why is it a bad idea to let them mine for Bitcoins?

8th Lecture: Bitcoins

- conclusion: not anonymous, not free from (potential) government interference

- The department has large labs full of computers that are pretty much idle over night. Why is it a bad idea to let them mine for Bitcoins?

- other cryptocurrencies (Litecoins,...)

  `http://en.wikipedia.org/wiki/Cryptocurrency`

9th Lecture: Static Analysis

- more principled way of writing software
- testing can show the presence of bugs, but not their absence
- "A good attack is one that the engineers never even thought about." —Bruce Schneier

9th Lecture

- model checking
- program logics (Hoare logics, separation logic)
- specifications / correctness proofs

Further Reading

- Risks mailing list

  `http://catless.ncl.ac.uk/Risks`

- Crypto-Gram

  `https://www.schneier.com/crypto-gram.html`

- Light blue touchpaper

  `https://www.lightbluetouchpaper.org`

- you can still send me your hws
- projects