Our research

Solving security problems
• programming securely with cryptography
• solving
• checking

Devising formal methods
• checking
• syntax checking
• checking

Developing practical tools and systems
• QuickCheck
• QuickCheck
• QuickCheck

Tools and Systems
• F*, miTLS, HACL*, ProVerif, CryptoVerif, ProScript, CryptoCat, QuickChick, ...
Finding attacks in TLS

SMACK: State Machine AttaCKs
Implementations of the Transport Layer handle a variety of protocol versions, modes and key exchange methods, prescribe a different message sequence for each server. We address the problem of implementing a machine that can understand the different messages used by each server.

The Logjam Attack

Tracking the FREAK Attack

The BEAST Wins Again: Why TLS Keeps Failing to Protect HTTP

“FREAK” flaw in Android cripples HTTPS crypto

FREAK Attack Threatens SSL Clients

For the nth time in the last couple of years, security experts are warning about a new Internet-scale vulnerability, this time in some popular SSL clients. The flaw allows an attacker to force clients to downgrade to weakened ciphers and break their supposedly encrypted communications through a man-in-the-middle attack. Researchers recently discovered that some SSL clients, including OpenSSL, will
Researchers

Karthik Bhargavan

Graham Steel

Gilles Gérardin

Cătălin Hrițcu

Christine Rizkallah

Cryptosense
Current team

Researchers (6)                PhD Students (4)                PostDocs (2)

\[ y o \quad o n o \text{ock} \quad o o \quad \text{ck} \quad o n o \]

G G r s o \quad \text{ck} \quad \text{ck} Q o

c cno G \text{ck} \quad o m \quad Y o a o

Interns (4)

\[ \text{ck} \quad \text{ck} \quad \text{ck} \quad \text{ck} \quad \text{ck} \quad \text{ck} o \quad n n \quad n n \quad n n \quad n y \quad n n \quad n \]

Visitors (3)

\[ y n Q \text{ck} o \quad o y o o y o \quad n n \quad n n \quad n y \quad o \]

11 nationalities

Diverse and international

Collaborators

\[ \text{ck} \quad \text{ck} \quad oo \quad o \quad n o \quad Q \quad s n \]

Our working language is English
Use formal methods to achieve security of critical software

- HTTPS stack
- Modern cryptographic library
- Secure messaging app
- Web browser core
- Compilers & monitors
- TCP/IP network stack...
Tools for analyzing abstract models of crypto protocols

• **ProVerif**
  - check check n n y
  - m check check o s check s check check check
  - o check s s y o s s

• **CryptoVerif**
  - check s o n n
  - check o check check s
  - check check check o o o check s check check

• **Recent case studies**
  - Q Q o n
  - s check o Q check o o o s y check o

PROSECCO
From verifying protocol models to actual implementations

• Protocol models
  – 
  – 
  –
  –

• Protocol implementations
  –
  –
  –
  –
• Verified reference implementation of TLS 1.2 & 1.3
• Microsoft Research and Inria
• Built on top of our HACL* crypto library
  – y o o s o Q n Q k s o Q
• Towards a verified HTTPS stack ck y
HTTPS ecosystem critical, complex
HTTPS ecosystem critical, complex and broken

• 20 years of attacks & fixes

• Mainstream implementations

OpenSSL, SChannel, NSS, … Still patched every month!

HTTPS ecosystem critical, complex and broken

The Washington Post
‘FREAK’ flaw undermines security for Apple and Google users, researchers discover
Project Everest Goals

Strong verified security
Widespread deployment

- efficiency
- interoperability
- drop-in replacement for OpenSSL
Everest stack verified with

• Functional programming language
  – n n G m
  – c k n c h n
  – c h c k s n c k o c k

• Semi-automated verification using SMT
  – n o

• Interactive verification using dependent types
  – n o
Is verified code secure in practice?

Unsafe languages
- Web browser/server
  - 2.000.000+ LOC

Insecure interoperability

Ooops

Web browser/server

Compiler F*
- C/C++
- ASM
Secure compilation

- **Secure interoperability with lower-level code**
  - check security of operations at compile-time

- **Dynamic enforcement, but at what cost?**
  - in software, 10x? 100x? 1000x?

- **Micro-policies**
  - new tagged hardware architecture
  - checks large metadata tag to each word
  - software defined, very flexible, fine-grained
  - ... average 10% runtime overhead
Use formal methods to achieve security of critical software

- HTTPS stack
- Modern cryptographic library
- Secure messaging app
- Web browser/server core
- Compilers & monitors
- TCP/IP network stack...