University of Waterloo Communications Security Lab (ComSec)

About the Lab

The Communications Security Lab (ComSec) is the leading research group for security and privacy technologies in pervasive computing environments. ComSec designs efficient and cost-effective cryptographic algorithms and protocols for protecting all kinds of security applications, corresponding infrastructure and organizational aspects. With its extensive experience in communication system security, the mission of ComSec is to provide real-world software and hardware based security solutions for a wide range of wired and wireless communication networks.

Outstanding Research Team

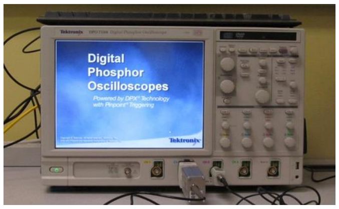
- Led by Prof. Guang Gong
- 3 Collaborating Faculty Members
- 1 Project Manager & Research Associate
- 2 Postdoctoral Fellows
- 5 PhD and 3 Master students

World-Class Research Facilities

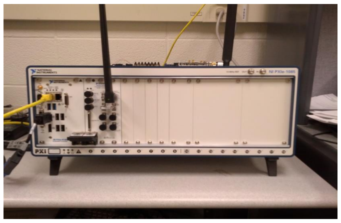
Thanks to generous support from Canadian government and industry partners, ComSec is equipped with world-class research facilities conducting high-quality security and privacy research in a wide range of applications.

SuperServer 5086B-TRF from Supermicro Computer Inc. (80 CPU Cores & 2 GPUs)
Cryptographic analysis tester

Universal Software Radio Peripheral hardware USPR 1 and USRP N210 from Ettus Research
Physical layer security evaluation (MIMA, Relay attack, etc.)



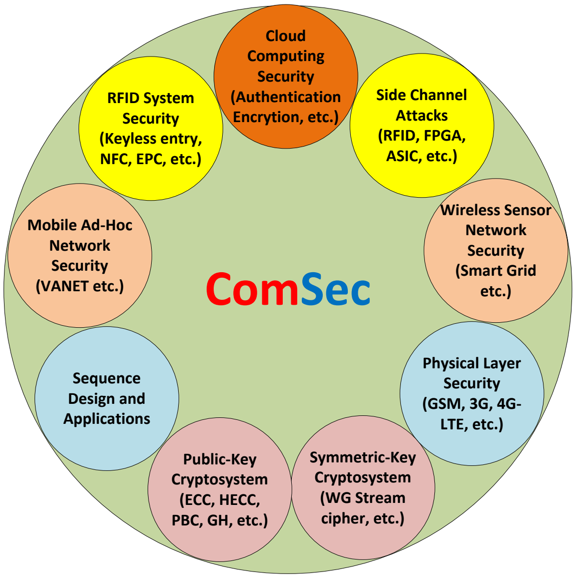
Tektronix DPO 7104 Oscilloscope with passive and differential probes from Tektronix Inc.
Side channel attacks on embedded devices



PXIe-5644R 6GHz RF Vector Signal Transceiver from National Instruments Corp.
Physical layer security evaluation (communication protocol emulations)

Core Research Areas

The researchers in ComSec target the challenging security and privacy issues in different types of communication systems that are widely deployed in industries.



ComSec

Cloud Computing Security (Authentication Encrytion, etc.)

Side Channel Attacks (RFID, FPGA, ASIC, etc.)

Wireless Sensor Network Security (Smart Grid etc.)

Physical Layer Security (GSM, 3G, 4G-LTE, etc.)

Symmetric-Key Cryptosystem (WG Stream cipher, etc.)

Public-Key Cryptosystem (ECC, HECC, PBC, GH, etc.)

Sequence Design and Applications

Mobile Ad-Hoc Network Security (VANET etc.)

RFID System Security (Keyless entry, NFC, EPC, etc.)

Sponsors

We are very grateful to our sponsors, both past and present, for their support, without which ComSec would not have been able to achieve its goals.

NSERC CRSNG

Ontario Research Fund

Pitney Bowes
Engineering the flow of communication™

BlackBerry

OpenText
The Content Experts™

Revere Security

TrustPoint
Innovation Technologies, Ltd.

Collaboration

- Design and analysis of new cryptographic primitives
- Design and analysis of security architectures
- Efficient and secure implementations of software and hardware security solutions
- A wide range of applications: smartphones, RFIDs, smart meters, ZigBee sensors, cloud computing, etc.

Department of Electrical and Computer Engineering
University of Waterloo, 200 University Avenue West
Waterloo, Ontario, Canada, N2L 3G1

http://comsec.uwaterloo.ca/

Contact: Prof. Guang Gong
Phone: +1(519)888-4567 x35650
Email: ggong@uwaterloo.ca