Who Am I?

- senior lecturer at UNSW@ADFA
- professional interests include:
  - cryptography, communications and computer systems security, and safe mobile code execution
- teaches courses in:
  - computer security, cryptography, data communications and java programming
- co-authored text on Computer Security

UNSW@ADFA

- campus of UNSW (mostly in Sydney)
- UNSW@ADFA located in Canberra
- undergraduate (bachelor) students are all defence force officer cadets
- postgraduate (masters/PhD) students any

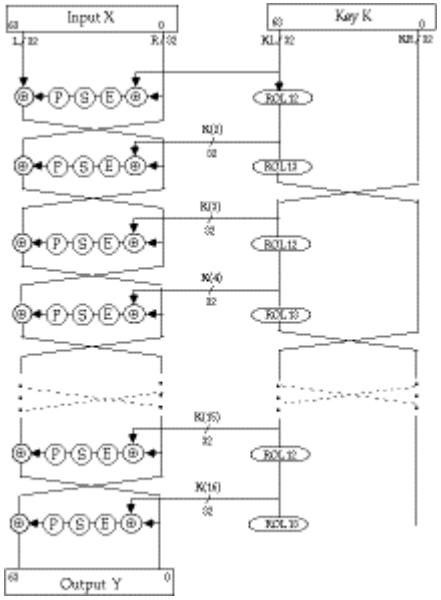
Teaching at UNSW@ADFA

- Cryptography (bachelor & masters) '93+
- Computer Security (masters) '01+
- Data Structures & Representation (bachelor) '07+

- previously: Computing Technology, Data Communications, Intro Java Programming

Research - LOKI89/91

- PhD on analysis of DES & design of LOKI
- new 64-bit block cipher (designed '87-'91)
  - Exp, 12->8 bit Subs, 32bit P
- redesinged key schedule in '91
- weaknesses published
  - Lars Knudsen – key, DC
  - Biham & Shamir - key



Research - LOKI97

- AES candidate 128-bit block cipher
  - only southern hemisphere submission
  - work done during SSP97 to NTNU & UOW
- evolution of LOKI91
  - f has 2 S-P layers
- broken (DC) by
  - Rijmen & Knudsen
  - 1st publicised so 1st broken
- is target of analysis

Research – Safe Erlang

- moved attention to mobile code security
  - in SSP97 at RMIT & NTNU; SSP92 RMIT
- rather than focus on procedural languages
- consider inherently safer functional lg
  - chose Erlang from Ericsson CSL (RMIT link)
- identified needed safety extensions
  - PID capabilities, custom node, remote context
- then examined use of safety policies
- trial implementation in RMIT EC compiler

Research – eCommerce Trust

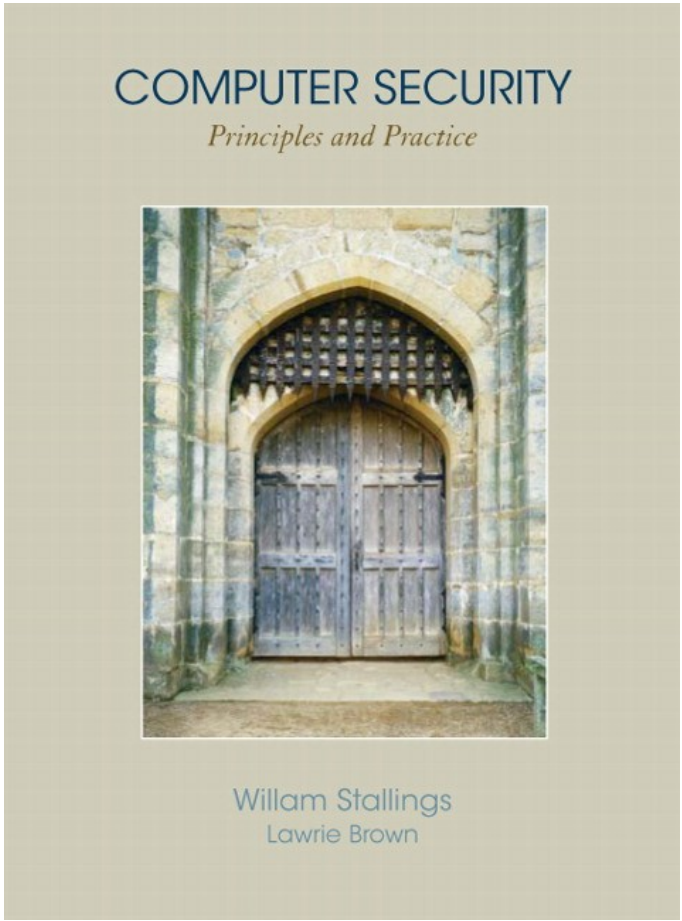
- research by Yinan Yang
  - PhD '97-'04, subsequent research papers
- looking at computing trust level based on various environment indicators
  - modelled on physical world interaction
  - ISP, DNS host, links from other known sites

Research – Periodical Payment

- work by Grigori Goldman
  - PhD '05-'09
- issue is lack of specificity in contract between customer & merchant
- explore means to specify exact payment policy in X.509 restricted proxy certificate
- then presented by merchant to payment gateway to validate right to request funds

Textbook – Computer Security

- co-author with William Stallings
- Computer Security: Principles & Practice
- Pearson 2008
- wrote 5 chapters
- sample slides
- edited remainder



SSP10

- currently visiting NTNU on sabbatical
- as NordSecMob scholar
  - teaching in InfoSec
  - research in mobile security
  - also brief visit to DTU
- exploring possible collaborations

Research – Proxy Certs for Mobile Authentication

- on use of (restricted) proxy certificates in various mobile authentication scenarios
- as better alternative to short-lived certs
  - Sharma et al 2009 (NordSecMob Masters): Short-Lived Certs as Mobile Authentication
  - Nyre, Jaatun et al (OASIS project) Secure MANET Routing for First Responders
- as general means of delegating right of temporary access to some service

Further Information

- http://www.unsw.adfa.edu.au/~lpb/
- Lawrie.Brown@adfa.edu.au

- Any Questions ????