CSCI 1800 Cybersecurity and International Relations

Future Directions
John E. Savage
Brown University
Overview

- Code randomization
- Instruction set randomization
- Secure cloud computing
- Norms for nations and technologists
- Undersea cable system
- Global positioning system
- Forecasting
Code Randomization
Code Randomization

• Several authors have proposed modifying compilers to generate different binaries, e.g. Franz at UC Irvine

• Compilers use many optimizations.

• **B**inaries are differentiated by choosing to activate subsets of optimizations.
Compiler-Assisted Code Randomization and Hardening*

• New compiler techniques allows code to be transformed at load time, i.e. often.
• Compiler metadata supplied to code re-writer.
• Re-writer invoked at load time.
• Transformations include permutation/shuffling of functions and basic-blocks and insertion and deletion of control-flow integrity checks.
• Can be used with Shuffler to make it run faster.

* See readings for Module 10. Brown CS faculty member, Kemerlis is co-author.
Instruction Set Randomization
Instruction-Set Randomization

• Code is compiled to hypothetical instruction set
  – If attacker doesn’t know instructions, can’t inject
• At run time, JIT compiler translates code to chip instruction set
  – Note: JIT compilers used to implement Java
• A variant compiles to encrypted binary that is decrypted on the fly
Norms and Ethics
Ethical Use of Robots

• Autonomous vehicles
  – Reduced highway deaths are predicted
  – Who is responsible for accidents?

• **Lethal autonomous weapons** (LAWs) coming!
  – Can robots apply humanitarian principles of necessity
    and proportionality when selecting targets?

• What legal & ethical issues do LAWs introduce?
  – UN created a GGE on LAWs, first meeting 4/9 to 4/13/18
  – This is an issue to watch
Social Control Using Machine Learning

- Will facial recognition be used to track citizens?
  - UK has very large closed-circuit TV system
- Will China deploy its social scoring system?
  - How effective is it likely to be
Governance Issues

• Norms have been proposed by UN GGEs
  – What be done to help nations abide by them?
• What new governance issues will emerge?
  – Will international use of blockchains require norms?
Secure Cloud Computing
Techniques to Secure the Cloud

• Private Information Retrieval
  – Queries of public database hide data that is being sought

• Verifiable Computation
  – Did the cloud run my computation correctly?

• Secure Multi-Party Computation
  – Can several parties compute on secret information without revealing the secrets?

• Secure Database Search
  – Database search when data and queries are encrypted

• Homomorphic Encryption
  – Can all computations be done on secret data?
Verifiable Computation*

- Program P is processed once by client who generates private and public info on P.
- Client processes input, generating public and private information on it.
- Client sends server public information on F and its input to server for computation.
- Server sends output to client who uses private information to verify correct computation.

Secure Multi-Party Computation

• Yao’s example: Millionaire’s Problem
  – Two people each believe they are wealthier
  – They securely share their wealth
  – Do a computation
  – Determine who is wealthier without revealing their wealth

• Yao’s approach:
  – Represent decision function by circuit
  – Garble the circuit so that each party can learn the output of the circuit and nothing else
Fully Homomorphic Encryption

• Goal encrypt input data at home
• Send computation to untrusted server that computes on encrypted input to produce encrypted output
• Decrypt output at home
Homomorphisms

- Let $\otimes$ be an operation that combines two inputs $a$ and $b$ to produce $y = a \otimes b$.
- Let $E(x)$ denote the “encryption” of $x$.
- A homomorphism of $\otimes$ is an operation $\odot$ with the property that if $z = E(a) \odot E(b)$ then $z = E(y)$.
- Thus, a client encrypts $a$ and $b$ and sends $E(a)$, $E(b)$, and $\odot$ to a server, the server computes $z$.
- The client receives $z$ and decrypts it to get $y$. 
Fully Homomorphic Encryption

• Every function $f$ on binary inputs can be computed with AND and XOR

• Every function $f$ can be computed securely if an encryption scheme can be found for which homomorphisms of both AND and XOR exist

• Lattice-based encryption is one encryption scheme for which this is possible.

• FHE implementations for the AES cipher ran in 4 hours – 7 seconds when amortized over many runs!
Applications of FHE

• Verifiable Computation
• Private Information Retrieval
• Multi-party computation
• Secure database search
Undersea Cable System
The Undersea Cable System

- First transatlantic telegraph cable finished 1858
- 99% of international data runs on undersea cables
  - Cables in shallow water have diameter of soda can
  - Deep sea cables have diameter of Magic Marker
- Cost > $100 M to lay a cable across ocean
- Cables vulnerable to boat anchors, earthquakes
- > $10 trillion worth of financial transactions/day
Undersea Cable System

• Spies love underwater cables
  – US submarine tapped Soviet cable during Cold War
  – Secret given to USSR by NSA analyst, Ronald Pelton
• Brazil laying cable to Europe to avoid US
• Submarine communication much faster and cheaper than satellites
• To cripple Internet, cut undersea cables
Global Positioning System
GPS

• Developed and launched by US in 1980s, operational in 1993
• Today consists of 31 satellites, each with atomic clock synced to US Naval Observatory
  – Orbit at 12,000 miles, use solar panels for power
• Provides highly accurate timing information
• Time is important
  – Betting parlor where reports from track are delayed
Dependence on GPS

• Global financial system vulnerable to GPS attack
  – GPS used to route phone calls
  – ATMs and cash registers use it
  – Electrical grid uses it to synchronize generators
  – Stock exchanges use it to regulate trades

• Airlines use it for navigation

• Military uses: get ships to shore, find troops in the field
Risks Associated with GPS

• Major solar flare could severely damage them
• GPS signals can be spoofed
  – Simple receiver/transmitter can amplify GPS signal
  – Cause a station to sync with device
  – Change in timing of GPS signal will mislead station
• GPS spoofing used on ships in Black Sea in 10/17
• DHS reports drug cartels using it to divert drones
• Might be able to create a “flash crash”
Protecting Against Loss of GPS

• Return to terrestrial radio navigation?
  – Earth-based eLORAN (long-range navigation) being considered by many nations
• We also need better solar weather forecasting
Forecasting
Are You Good at Forecasting?

• Neils Bohr: “Making predictions is difficult, especially of the future!”
• Philip Tetlock, Psych prof at Penn, and Dan Gardner book “Superforecasting”.
• Best forecasters have different style of thinking
  – Reject idea any single force determines outcomes
  – Used multiple info sources and analytical tools
  – Combined competing explanations
  – Allergic to certainty
IARPA’s Good Judgment Project

• Designed to identify super-forecasters
• Most successful geopolitical predictions by concentrated group of super-forecasters
• Best forecasters outdid intelligence services
• Some are good in all domains
What Does it take to Forecast Well?

• Nick Hare, head of futures and analytical methods at UK Ministry of Defence
  – A good forecaster is successful not because of knowledge but the “capacity for ‘active, open-minded thinking’: applying the scientific method to look rigorously at data, rather than seeking to impose a given narrative on a situation.”
  – E.g. on forecasting possibility of NK nuclear test, Hare relied on statistics rather than geopolitics
The Fox and the Hedgehog

- Hedgehogs are narrowly invested in one topic
- Foxes have wider, shallower, range of experience
Review

- Code randomization
- Instruction set randomization
- Secure cloud computing
- Norms for nations and technologists
- Undersea cable system
- Global positioning system
- Forecasting