CSCI 1800 Cybersecurity and International Relations

Future Directions

John E. Savage

Brown University

Overview

- Active Defense
- Moving targets defense against code reuse
- Norms for nations and technologists
- Secure cloud computing
- Undersea cable system
- Global positioning system
- Forecasting

Active Defense

What is Active Defense?

- DoD Definition
  - Limited use of offensive action and counterattacks to deny a contested area or position to the enemy
- Deception is useful but not active defense
- Nor is incident response & threat intelligence
- Moving targets, i.e. maneuverability, is active!
  - Frustrate attacker by changing the environment
  - Reduce defender effort, increase attacker work

Moving Targets Defense

Moving Target Defense

- What is the Problem?
  - Monocultures – same code on many platforms
  - Find a vulnerability, apply it everywhere
- Goal: Diversify*– Make attacker work harder, e.g.
  - Statically relocate binaries, e.g. ASLR - next slide
  - Dynamically apply ASLR – code shuffling

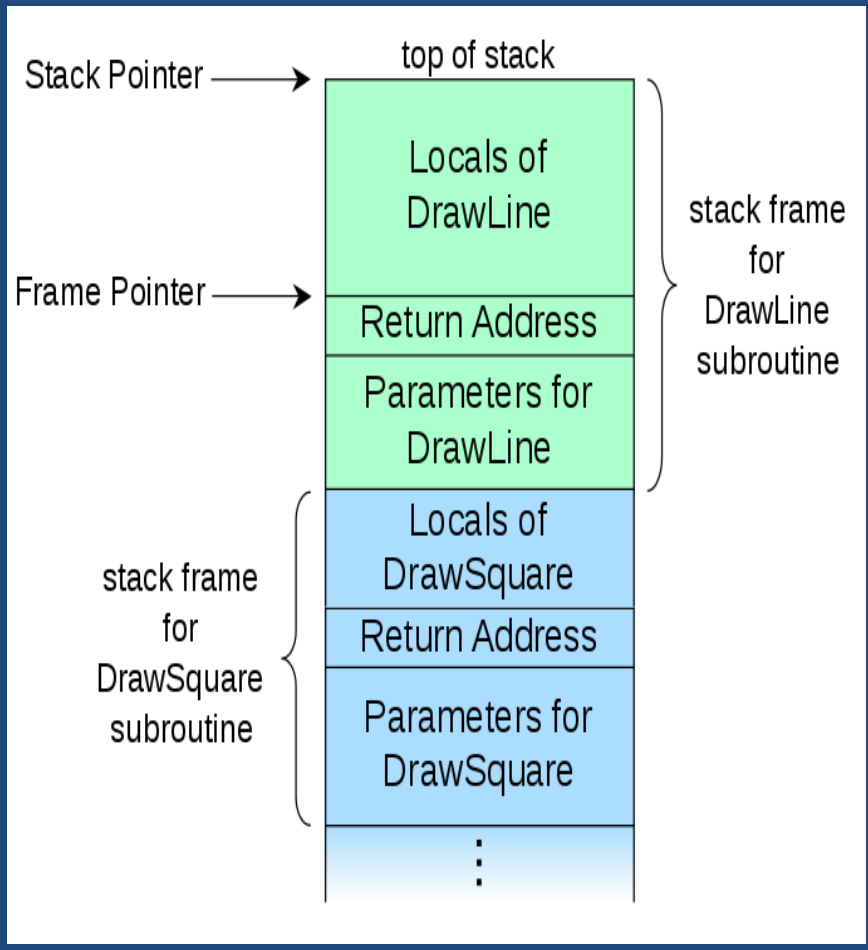
* Diversity in Cybersecurity, Computer, April 2016 – See readings

Address Space Layout Randomization (ASLR)

- ASLR is staticlLocation randomization
- When booting, offset regions in virtual memory, e.g. stack, heap, libraries and executable areas
- Protects somewhat against advanced attacks
- Attacker must first discover the offsets.
- On 32-bit chips, 16 bits of randomness available
  - Brute force can reveal offsets in minutes!
- More difficult on 64-bit chips, 40 random bits

Buffer Overflow Attack

- Overwrite stack
  - Code author failed to do bounds checking
- Stack frame overwritten
  - Code is injected
- Return address altered
- Also called stack smashing



Buffer Overflow Attacks on Stacks

- Result of buffer overflow attack:
  - Malware put on stack & return address points to it
  - Malware executed from stack
  - Data Execution Protection (DEP) bit prevents code execute from stack – eliminates some code injections
- Basic protections against buffer overflow:
  - Canaries – fixed strings, placed at head of stack. Will be modified during overflow and detected!
  - ASLR and DEP – strong protection against many attackers

Advanced Buffer Overflow Attacks

- Buffer overflow now used for code reuse attack
  - Called return-oriented programming* (ROP)
- Attacker injects pointers onto the stack. Each one points to the tail end of a library function, which ends in a RETURN (RET) instruction.
- Tails form "gadgets" that act like an instruction
- ROP uses gadgets to place a program on stack

* https://en.wikipedia.org/wiki/Return-oriented_programming

Dynamic Code Relocation

Shuffler* – Dynamic Code Relocation

- Rearranges memory faster (milliseconds) than attacker can use discover offset information!
- Code is put into shuffleable form so that code segments can be moved around quickly.
- Function boundaries within code are found
  - Periodically the following steps are taken:
    - Functions are randomly arranged in memory
    - Links between functions are updated

* See readings

Shuffler

- While one copy of a shuffled binary is run, the Shuffler processes a second copy of the code
  - After milliseconds a relocated copy is ready
- Thus, Shuffler shuffles itself, its libraries and the code to be shuffled
- The increase in computation time and storage space to implement Shuffler are modest.

Norms and Ethics

Ethical Use of Robots

- Autonomous vehicles
  - Reduced highway deaths are predicted
  - Who is responsible for accidents?
- Lethal autonomous weapons (LAWs) are 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 - 4/13/18
  - This is an issue to watch

* GGE = Government Group of Experts, a UN committee

Social Control Using Machine Learning

- Will facial recognition be used to track citizens?
  - UK estimated to have 14 CCTV cameras/person
- China is deploying its social scoring system
  - It is being used in Xinjiang province
  - How effective is it?
  - What impact might it have if deployed nationally?

Governance Issues

- Norms have been proposed by UN GGEs
  - What can 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
  - Hide data being sought when database is compute-limited
- Verifiable Computation
  - Did the cloud run my computation correctly?
- Secure Multi-Party Computation
  - Can several parties compute on shared secret information without revealing the secrets?
- Secure Database Search
  - Database search when data and queries are encrypted
- Homomorphic Encryption
  - Can computation be done on secret data without leaks?

Verifiable Computation*

- Program P is processed once by client who generates private and public info on P.
- Client sends public information on P to server along with the input to P.
- Server sends output and a “certificate” to the client who uses private information to verify the computation with much less effort than it would take to do the computation itself.

* Walfish, Michael; Blumberg, Andrew J. (2015-01-01). "Verifying Computations Without Reexecuting Them". *Commun. ACM*. **58** (2): 74–84.

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

- See next slide on homomorphisms
- 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 $\odot$ be an operation that combines two inputs a and b to produce y = a $\odot$ b.
- Let E(x) denote the "encryption" of x.
- A homomorphism of $\odot$ is an operation $\bigcirc$ with the property that if z = E(a) $\bigcirc$ E(b) then z = E(y)
- Thus, a client encrypts a and b and sends E(a), E(b), and $\bigcirc$ to a server, the server computes z
- Client receives z = E(y) and decrypts it to get y!

Fully Homomorphic Encryption (FHE)

- 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 hour, 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
- >97% of international data travels 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
  - Russia has deep manned subs, US uses robots
- Brazil laid 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
  - They orbit at 12,00 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 attack
  - ATMs and cash registers use it
  - Stock exchanges use it to regulate trades
- Electrical grid uses it to synchronize generators
- GPS used to route phone calls
- Airlines use it for navigation
- Military: get ships to shore, find troops in field

Risks Associated with GPS

- Major solar flare could severely damage them
- GPS signals can be spoofed
  - Simple receiver/transmitter can amplify GPS signal
  - Can cause a station to sync with GPS spoofing device
  - Change in timing of GPS signal can mislead station
- GPS spoofing used on ships in Black Sea in 10/17
- DHS – drug cartels use spoofing to divert drones
- Might be able to create a “flash crash”

How to Protect Against Loss of GPS

- Return to terrestrial radio navigation?
  - Earth-based eLORAN (long-range navigation) being considered by many nations
  - Sailors use coastal radio stations to triangulate

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 wrote book “Superforecasting”.
- Best forecasters have different style of thinking
  - Reject idea that any single force determines outcomes
  - They use multiple info sources and analytical tools
  - They combine competing explanations
  - Are allergic to certainty

IARPA's Good Judgment Project

- Designed to identify super-forecasters
- Most successful geopolitical predictions done by concentrated group of super-forecasters
- Best forecasters
  - Outdid intelligence services
  - Were not experts in the area of forecast
  - They were good at forecasting 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 butt 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

- Which type is better at forecasting?

Review

- Active Defense
- Moving targets defense against code reuse
- Dynamic code relocation
- Norms for nations and technologists
- Secure cloud computing
- Undersea cable system
- Global positioning system
- Forecasting