Timothy Trippel

EECS 588 Project Proposal

Jeremy Erickson

Andrew Quinn

* Author order chosen by pseudo-random placement

Nation State Adversary (NSA)

Disclaimer:
All entities appearing in this work are fictitious. Any resemblance to real entities, living or dead, is purely coincidental.

Nearly unlimited computing power

Hire lots of smart people

Both technical and legal authority

May or may not be constrained by what we consider “lawful”.

Let’s have a tinfoil hat party!

Nation State Adversary (NSA)

Disclaimer:
All entities appearing in this work are fictitious. Any resemblance to real entities, living or dead, is purely coincidental.

What are they [allegedly] doing? (we’re pretty sure)

- APT1
- Stuxnet
- Backdooring Crypto
- Tapping Undersea Cables

What else could they be doing that we don’t know about yet?

Let’s think like the NSA!

Thinking like the NSA

Disclaimer:
All entities appearing in this work are fictitious. Any resemblance to real entities, living or dead, is purely coincidental.

What might be a big juicy target?

- Automatically-Working cloud Systems (AWS)

Supports infrastructure for many businesses

Stores lots of data

Centralized

How might the NSA target AWS?

Disclaimer:
All entities appearing in this work are fictitious. Any resemblance to real entities, living or dead, is purely coincidental.

Collusion - “We’ll scratch your back if you scratch ours”

Coercion - National Security Letter, AKA “Gag Order”

Espionage - Just plain ol’ breaking in

For these to work, only a limited number of people can know

- Unprivileged AWS employees or clients must not discover anything
  - Network traffic must be normal
  - VM should be undisturbed

Narrowing It Down

Disclaimer:
All entities appearing in this work are fictitious. Any resemblance to real entities, living or dead, is purely coincidental.

Assume the NSA can control the Hypervisor

Now what might they want to do?

Let’s explore how the NSA could use the Hypervisor to control system entropy

- Entropy -> Random Number Generation
- Random Number Generation -> Secret Numbers
- Secret Numbers -> Confidentiality/Integrity/Authentication (CIA)

If we control system entropy, we don’t need to leak information

Stealthy!

Our Actual Proposal

Disclaimer:
All entities appearing in this work are fictitious. Any resemblance to real entities, living or dead, is purely coincidental.

- Investigate sources of entropy in a virtualized environment
  - What can the hypervisor control?
  - What tampering can the guest OS detect?
- Build a modified hypervisor that controls VM entropy
  - Xen
  - KVM

Future Research (i.e. not biting off more than we can chew)

- Prevention
  - What can the VM OS can do to prevent hypervisor tampering?
- Detection
  - Can we find someone actually doing this?