Bootstrapping Trust in Commodity Computers
Bryan Parno, Jonathan McCune, Adrian Perrig
Carnegie Mellon University

A Travel Story
You're on a 30-day trial of Keylogger Express. It has expired. Please enter your registration code or visit our website to purchase a license.

Trust is Critical
Will I regret having done this?

Bootstrapping Trust is Hard!
Challenges:
- Hardware assurance
- Ephemeral software
- User Interaction

Does program P compute F?
Is F what the programmer intended?

Bootstrapping Trust
What F will this machine compute?

Safe?
Yes!

Bootstrapping Trust is Hard!
Challenges:
- Hardware assurance
- Ephemeral software
- User Interaction

Safe?
Yes!

Evil
App
OS
Evil
App
In the paper...

- Bootstrapping foundations
- Transmitting bootstrap data
- Interpretation
- Validation
- Applications
- Human factors
- Limitations
- Future directions
- ... and much more!

1) Establish Trust in Hardware
- Hardware is *durable*

**Open Question:** Can we do better?

2) Establish Trust in Software
- Software is *ephemeral*
- We care about the software *currently* in control
- Many properties matter:

Which property matters most?

... 

What is Code Identity?
- An attempt to capture the behavior of a program
- Current state of the art is the collection of:
  - Program binary
  - Program libraries
  - Program configuration files
  - Initial inputs
- Often condensed into a hash of the above

Code Identity as Trust Foundation
- From code identity, you may be able to infer:
  - Proper control flow
  - Type safety
  - Correct information flow
- Reverse is not true!
What Can Code Identity Do For You?

- Research applications
  - Secure the boot process
  - Thwart insider attacks
  - Count-limit objects
  - Protect passwords
  - Create a Trusted Third Party
- Commercial applications
  - Secure disk encryption (e.g., Bitlocker)
  - Improve network access control
  - Secure boot on mobile phones
  - Validate cloud computing platforms

Establishing Code Identity

\[ f_1 \rightarrow f_2 \rightarrow \ldots \rightarrow f_N \]

Root of Trust

Chain of Trust

Trusted Boot: Recording Code Identity

Attestation: Conveying Records to an External Entity
Interpreting Code Identity

- Traditional
  - Gasser et al. '89, Sailer et al. '04
- Policy Enforcement
  - Marchesini et al. '04, Jaeger et al. '06
- Virtualization
  - England et al. '03, Garfinkel et al. '03
- Late Launch
  - Kauer et al. '07, Grawrock '08
- Targeted Late Launch
  - McCune et al. '07

Load-Time vs. Run-Time Properties

- Code identity provides load-time guarantees
- What about run time?
- Approach #1: Static transformation

Run-Time Policy

- Code
- Attested
- Code'
Load-Time vs Run-Time Properties
• Code identity provides load-time guarantees
• What about run time?

Open Question:
How can we get complete run-time properties?

Roots of Trust
Cheaper

Open Question:
What functionality do we need in hardware?

Human Factors

Open Questions:

Conclusions
• Code identity is critical to bootstrapping trust
• Assorted hardware roots of trust available
• Many open questions remain!

Thank you!
parno@cmu.edu