A Secure and Reliable Bootstrap Architecture

"Trust, but Verify"
Old Russian Saying

William A. Arbaugh
Angelos D. Keromytis
Jonathan M. Smith
David J. Farber
University of Pennsylvania
http://www.cis.upenn.edu/~waa

The Problem

- Every Computer System is Currently Invoked by an Untrusted Process- Even "Secure Systems".

- This Leads to a False Sense of Security for the Users of those Systems.

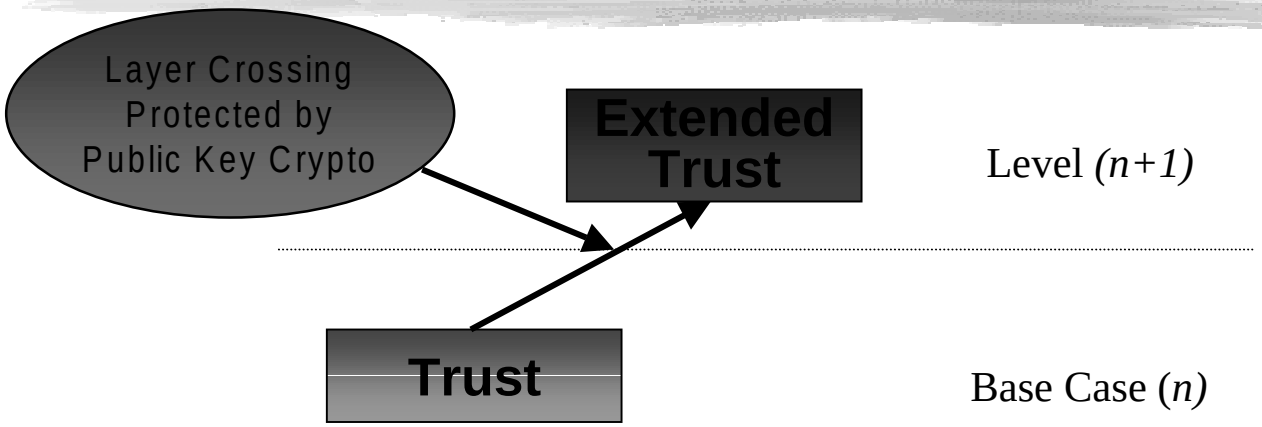
Motivation: Security

- Detect changes to Bootstrap Components
  - Malicious Changes
  - Inadvertent Changes
  - Failures
- Mitigate Some Denial of Service Attacks

Motivation: Administration

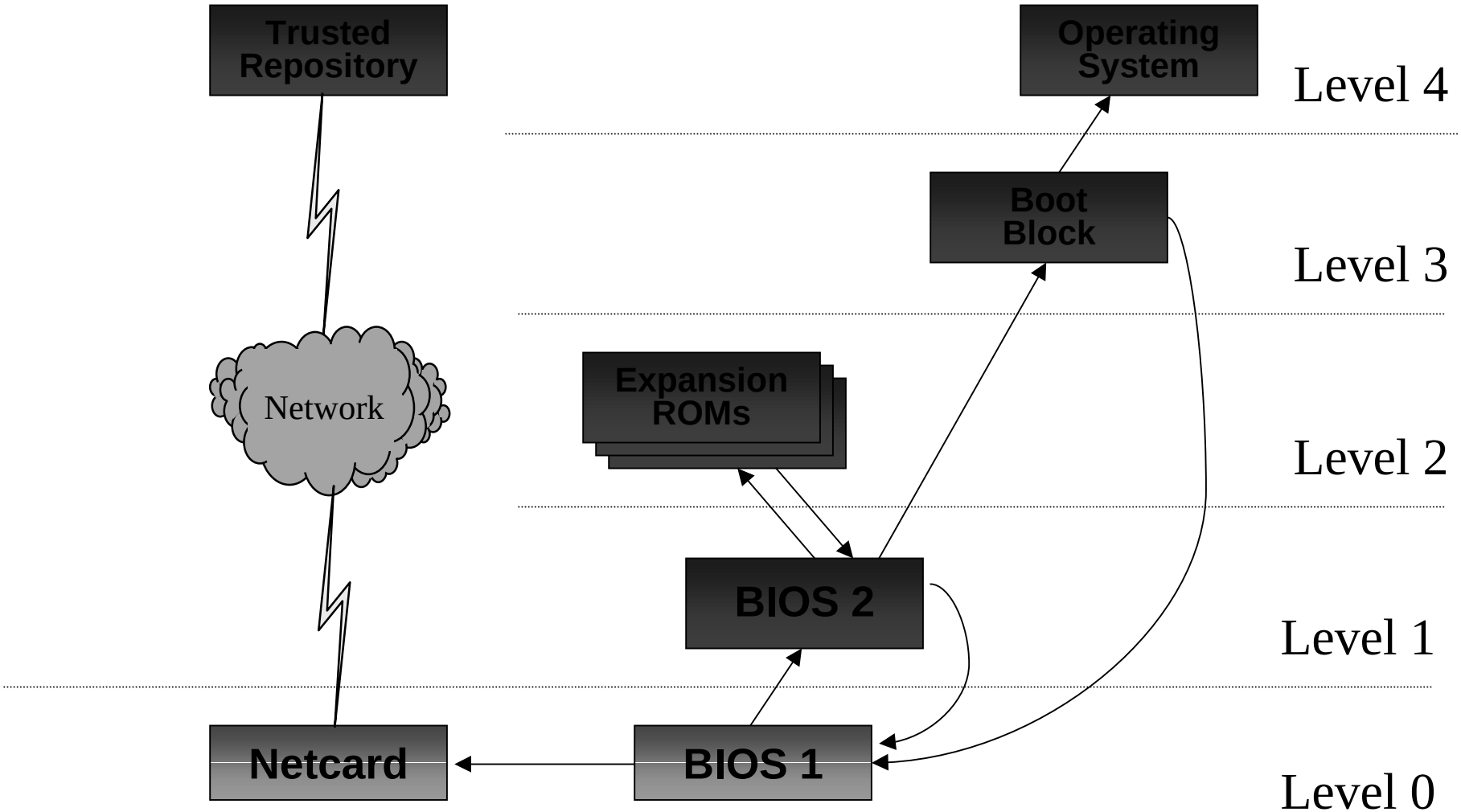
- Security Motivation Plus
  - Reduce Bootstrap Failures
  - Detect Configuration Changes
  - Provide Capability for Remote Management of Bootstrap Process

Approach



- Integrity and Trust Must be "*Grounded*" at the Lowest Possible Point.
- Protect Transitions
- Recover whenever possible.

AEGIS Architecture



Formal Proof

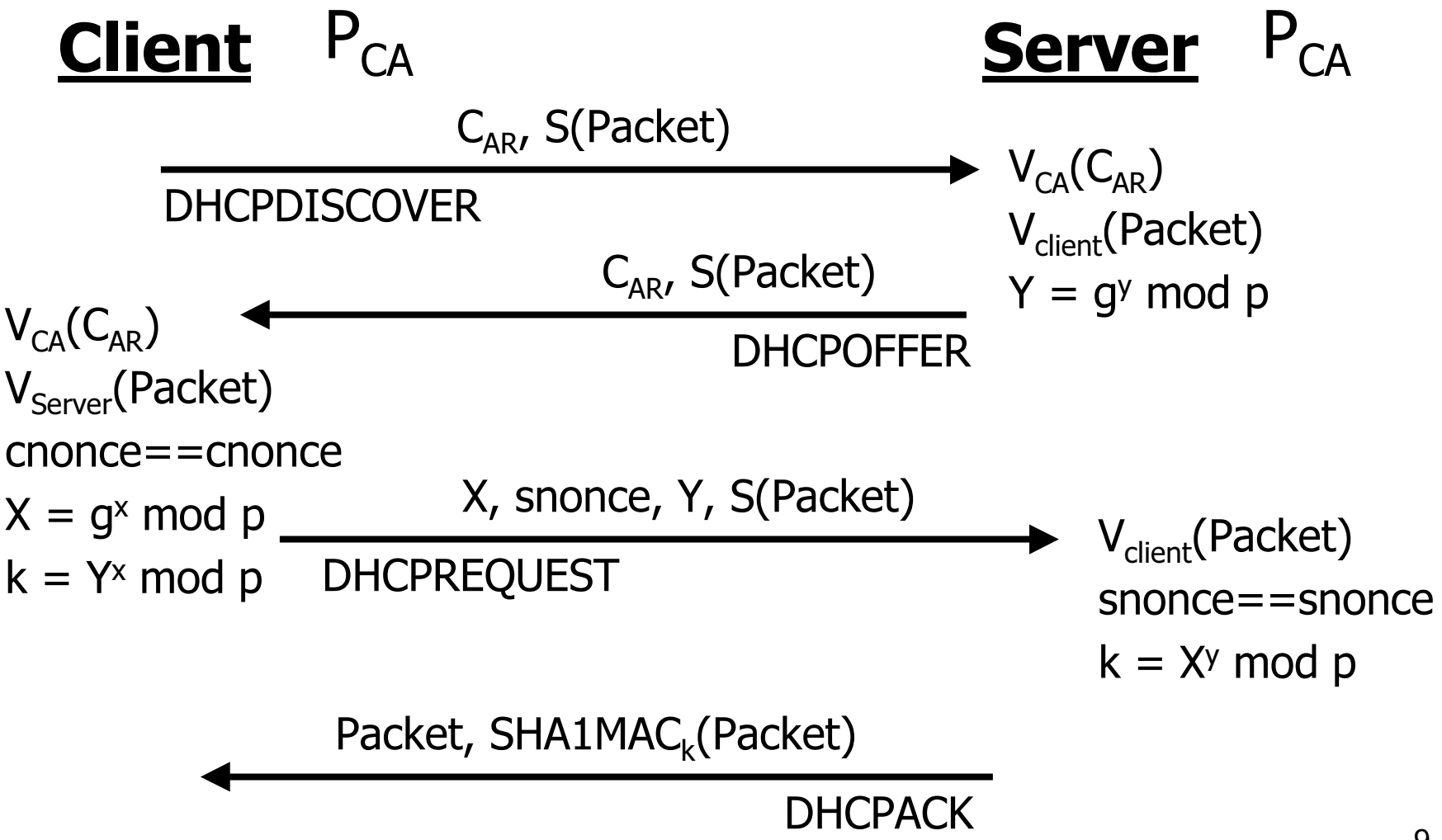
- AEGIS Bootstrap Architecture has been Formally Proven Correct using PVS.
  - Darryl Dieckman and Perry Alexander, University of Cincinnati.

http://www.ececs.uc.edu/~ddieckman

Recovery Protocol

- Uses Well Known Cryptographic Algorithms and Protocols (DSS, Diffie-Hellman).
- Use Well Known RPL Network Protocols (DHCP, TFTP).
- Protocol is FAIL SAFE

Recovery Protocol



What Can We Recover?

Component	Action
BIOS1	Halt
Recovery ROM	Halt
BIOS2	Repair
Expansion Flash	Repair
Expansion EEPROM	Shadow
Boot Block	Repair
OS Kernel	Repair
CMOS	Mitigate
Real Time Clock	Mitigate

Recovery Implementation

- SSLeay 0.8.1 - Eric Young
- Etherboot 4.0Beta4 - Ken Yap et. Al.
- ISC DHCP Server 2.0Beta1- Ted Lemon
- IPSEC - Angelos Keromytis
- Intel EtherExpress Pro 100

ROM and Packet Sizes

- Current ROM image is 85Kb <u>un-compressed</u>
  - 30Kb is for X.509v3 support
  - 35Kb is for cryptographic support

- Approximate Packet Sizes
  - DISCOVER: 901 Bytes
  - OFFER: 1081 Bytes
  - REQUEST: 626 Bytes
  - ACK: 626 Bytes

Client Performance

- Sign Packet: 34ms
- Init and Generation of Random Number Stream: 0.1499 seconds
- DISCOVER: 0.1533 seconds
- REQUEST: 40 ms

266 Mhz Pentium with AEGIS ROM

Server Performance

- Verify Certificate Chain: 76ms
- Verify Packet Signature: 36ms
- Generate DH Public: 93ms
- Sign Packet: 16ms
- Total Generate OFFER: 221ms
- Generate ACK: 126ms
  - Includes generating shared secret

Dual 300 Mhz PentiumII running RedHat Linux 5.0

Optimizations

- Modified StS need only be done once.
  - Client and Server cache exchanged secret for future use.
- Perform some Server Calculations after Sending Response.
- Improve Client Random Initialization.

Conclusions and Future

- Examining the Potential Uses of a Secure Bootstrap:
  - Basis for Active Network Security
  - Secure Periods Processing
  - IP Protection
- Beyond Bootstrap:
  - Secure DHCP
  - Secure NetPC

Questions?