Mitigating DoS Through Basic TPM Operations

William Enck
enck@cse.psu.edu
August 5, 2005
Protecting Resources

• Client puzzles have been proposed to protect against DoS attacks

• Traditionally, puzzles make clients “pay” for access with CPU resources

• Determining the correct puzzle hardness for a client is difficult
  ‣ Memory-based puzzles (Abadi et. al.)
Using Security Devices

• We have been told the Trusted Computing Group’s (TCG) Trusted Platform Module (TPM) can make our systems more secure

• How can we use the TPM in non-DRM type applications?
TPM-based Client Puzzles

• A novice approach
  ‣ attest remote solution code

• The TPM is slow and we can verify operations, let’s use these facts

• Keep track of TPM accesses
  ‣ The TPM is good at keeping state (PCR values)
High-level Architecture

Client

TPM

Access

Access

Access

{PCR}

Server

Request

Access X times

{PCR}

Puzzle Generator

Puzzle Verifier

Grant Access
Questions?

enck@cse.psu.edu