Low Cost Trustworthy Computing

Mahalingam Ramkumar
Assistant Professor
Department of Computer Science and Engineering
Mississippi State University

MSU October 15 2008 Mahalingam Ramkumar
Overview

- Why?
  - The third wave in computing

- How?
  - Lowering complexity
    - DOWN policy
    - Low complexity key distribution schemes

- What?
  - Can we do with low cost trustworthy computers
The Third Wave

- First wave
  - Networks centered around thousands of mainframe computers

- Second wave
  - Billions of personal computers (desktop, laptop and hand-helds) interconnected by the Internet

- Third wave
  - Trillions of computers
  - Low cost, modest capabilities
  - Special purpose ubiquitous computers
Third Wave Computing

- Ubiquitous computers
- Each UC entrusted with a specific task
  - Temperature / pressure sensor, location sensor, time, traffic sensors, industrial sensors
- Coming together to realize complex networks, performing complex tasks
  - Reduce the need for human intervention in mundane tasks
Implicit Trust

- At the core of emerging networks is the synergy resulting from mutual cooperation.
- Every UC implicitly trusts other UCs to perform their tasks.
- When B receives a message from A, B assumes the following:
  - The message did come from A.
  - The message has not been modified en route.
  - B can rely on the contents of the message.
Cryptographic Authentication

- A UC B receives the following message from UC B “A, 50, 0xffffsddefssseeeee”
  - I'm A
  - 50 is the data
  - 0xffffsddefssseeeee is the *cryptographic authentication*
- B can deduce that
  - The message originated from some one who has access to secrets of A
  - The message has not been modified en route
  - Can B rely on the contents of the message?
Second Wave vs Third Wave

- Second wave personal computers
  - Under the control of a person
  - The owner is responsible for protecting secrets assigned to the computer
- Third wave computers
  - No explicit owner
  - Serving the public in general
  - Many deployed in an unattended manner
  - The computers have to protect their own secrets.
Trustworthy Computing

- Two assurances are required
  - Secrets assigned to A cannot be exposed by anyone apart from A
  - A will be provided secrets only after verifying that the behavior of A cannot be modified by unauthorized parties
  - Read-proofing secrets assigned to computer A
  - Write-proofing software executed by computer A
Salient Properties of UCs

- Emerging applications are based on the premise that UCs will be inexpensive
- UCs should not be power hungry (many will be battery operated)
- UCs need to be trustworthy
  - Read-proof and write-proof
Read-proofing and Write-proofing

Read-proofing

- Secrets assigned to the computer cannot be exposed
  - Secrets are used for authentication
  - Also a stepping stone for write-proofing
    - Software can be authenticated using the secrets protected (to prevent modification)
    - But what about the software that verifies the integrity of the software?
Write-proofing

- Providing an assurance that the code executed by the computer cannot be modified
  - Well understood that this can be achieved with two basic assurances
    - Read-proofing
    - Write-protected counter
Trustworthy Computer Architecture

- A master secret that is protected
- A BIOS that is write protected
- BIOS loads software to be executed
  - Integrity of software verified using the secret
  - And then executed
- Trustworthy computers should be tamper-responsive
- Any attempt to read secret / modify BIOS or modify contents of protected RAM should lead to zeroisation
  - Master secret is erased
Shielding

- Active and passive shields
- Active shields detect intrusions and erase master secret
- Usually a fine wire-mesh
- Cutting the mesh will cut off circuitry that powers the BBRAM with master secret
- Passive shields block intrusions, block radiations emanating from the computer
  Which can be used to figure out what is going on inside the computer
Verification

- Integrity need to be verified before a trustworthy computer is provided secrets
- Issues
  - Who verifies?
  - Will they gain access to secrets?
  - Destructive testing?
  - Can verification be foolproof?
  - How expensive?
Reducing cost

- Low complexity
  - Reduce cost for verification
- Low power consumption
  - Low heat dissipation
  - Shielding will not interfere with heat dissipation
  - Unconstrained shielding
- Complexity of circuitry for tamper-responsiveness
- What we need - low-power, low-complexity computers, with minimal circuitry for tamper-responsiveness.
Cryptographic Security Associations

Will low-power low-complexity computers have the ability to handle cryptographic computations?

- Operations with secrets have to be performed inside the trustworthy computer

Two main types

- One-to-one – for example a shared secret between A and B
- One-to-many – authentication appended by A can be verified by any-one - digital signature
Key Distribution

- Key distribution center
- Nodes with unique identities
- KDC provides secrets to nodes
- Nodes can use secrets to compute / verify cryptographic tokens
Network Scale

- Number of nodes that are assigned secrets
- Solutions for small networks are not very difficult
- We need scalable schemes
  - Large network size (trillions)
  - Seamlessly add new nodes into the network
- Need schemes for one-to-one and one-to-many SAs
Solutions for Large Networks

- Two predominant approaches
  - Certificates based schemes
  - ID Based schemes
  - Some use only symmetric cryptography
  - Some use asymmetric cryptography
    - Public key and private key
    - Operations performed using public key can be inverted using the private key
    - And vice-versa
    - Private key cannot be computed from the public key
    - Schemes rely on trap-door one-way functions
Certificates Based Schemes

- Private keys chosen by nodes
  - Public keys are computed by the nodes
  - Public keys are seemingly random
    - Provide no information about the entity
    - Have to be certified by a certificate authority
- PKI for very large scale networks
  - Hierarchical certificate authorities
  - Need to exchange chains of certificates
ID based Schemes

- Meaningful public values are assigned to nodes – ID itself is the public value
- Public value (ID) is assigned first
- Secrets corresponding to the ID is computed by a KDC and provided to the node.
- Certificates are not needed
- ID based schemes
  - Key predistribution schemes
  - IBE / IBS (asymmetric crypto based)
Key Pre-distribution

- Unlimited network size
- But security limited by the number of colluding nodes
- Storage requirement
  - proportional to the number of colluding nodes that can be tolerated
- We require unrestricted network size
  - Is it reasonable to expect that not more than a finite number of nodes can pool together secrets?
  - Perhaps – for trustworthy UCs
Key Pre-distribution

- Resistance to collusions of one million nodes?
  - Attacker has to expose all secrets from one million nodes to make any kind of dent in security
- Storage proportional to one million keys
  - in practice a few tens of millions – a few hundred MBs
  - How about computational complexity?
  - For most schemes complexity (storage and computations) increase linearly with collusion resistance
Probabilistic Key Predistribution

- Very low computational complexity
- Security limited only by storage
- Implications
  - Obviates the problem of collusion resistance in two ways
    - Low cost of storage implies large collusion resistance
    - Low computational overhead implies better ability to protect secrets
Towards Low Cost Trustworthy Computing

- **Step one**
  - Very low complexity key distribution schemes
  - Low complexity implies
    - Lower verification cost
  - Low power
    - Inexpensive and effective shielding

- **Step two**
  - Eliminating / simplifying tamper-responsive circuitry

- **Step three**
  - How do we productively use modest trustworthy computers?
Decrypt only when necessary
- Relies on the ability to operate with **fractional** parts of secrets
- Applicable to all conventional public key schemes
  - eliminating the need for multi-step countermeasures for safe zeroisation
    - reduces complexity of tamper-proofing mechanisms
Compositing Emerging Networks

- The emerging Internet will include
  - Modest, inexpensive, trustworthy third wave computers
  - Resource rich second wave computers (untrustworthy)
- Can they take advantage of each other?
  - Can modest third wave computers take advantage of untrusted storage / computational resources
  - Can untrusted second wave computers take advantage of trustworthy third wave computers?
Example applications

- Mobile ad hoc networks (MANET)
  - Securing MANET routing protocols
  - Dual-agent approach
- “Shoring up” the Internet for the third wave
  - Low complexity alternatives to existing Internet security protocols like DNSSEC, IPSec and SSL/TLS
Dual Agent Protocols

- MANET nodes have to adhere to the routing protocol
- Each node is seen as consisting of a user agent and a trustworthy network agent
- Network agent has to ensure that the user agent adheres to the protocol
- Network agent should do very little – take advantage of the resources of the user agent to keep tabs on the user agent.
Internet Security Protocols

- DNSSEC for securing domain name system
- IPSec for network layer
- Very low adoption rates
  - Partly due to overheads
  - Partly due to poor design (in my opinion)
The Approach

- The Internet consists of billions of untrusted computers.
- Can adding (say millions) of trustworthy resource limited computers help?
- Yes
  - It can reduce overheads, and
  - Can improve the scope of assurances