PURDUE UNIVERSITY

CS526: Information Security
Chris Clifton

December 2, 2004

Trusted Computing Group

Trusted Computing Group (TCG)

- Goal
  Through the collaboration of HW, SW, communications, and technology vendors, drive and implement TCPA specifications for an enhanced HW and OS based trusted computing platform that implements trust into client, server, networking, and communication platforms.
- Implemented through "Trusted Platform Module"
  - Special chip

What Is TCPA?

- Subsystem to support identity/authentication
  - Authenticate platform to software
  - Forbid decryption if platform altered
- Key Concepts
  - Challenger: Entity requesting verification of trust
  - Root of Trust for Measurement: Platform characteristics

Basic Process

- Challenger requests check from Trusted Platform Agent
- TPA gets
  - Measurement from TPM
  - Log of measurement data
  - Validation data for correct platform
- Challenger compares and decides if system is trusted
- Challenger gives keys to TPM
  - Keys tied to integrity metrics
  - Released only if metrics not violated

What are Integrity Metrics?

- *Not Specified*
  - Could be anything
- Most likely software checksums/signatures
  - Can only run software if it is correct
  - Only get decryption key for data if proper software makes the request
- Possibly hardware
  - Verify single-cpu licensing

What about Changes?

- Stores log of changes (sequence)
  - TPM validates log correct
  - Challenger can test if changes acceptable

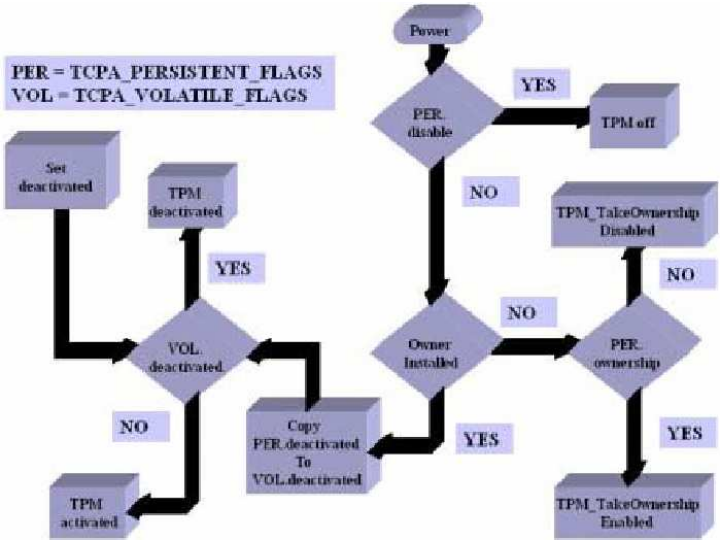
Keys

- Storage Root Key
- Signing keys
  - Private key for signatures
- Storage keys
  - Encrypting data
- Identity keys
- Binding keys
  - Encrypt/decrypt data
- Endorsement key to validate TPM
- Keys can be migratable or non-migratable

Does TCG Help Privacy?

- The system owner has ultimate control and permissions over private information and must “opt-in” to utilize the TCG subsystem.
  - Sounds like “if you want privacy, turn it off”
- In reality, provides capabilities to support key management
  - You can lock your data to your environment
- Will this get used?

Enabling/Disabling TPM



11

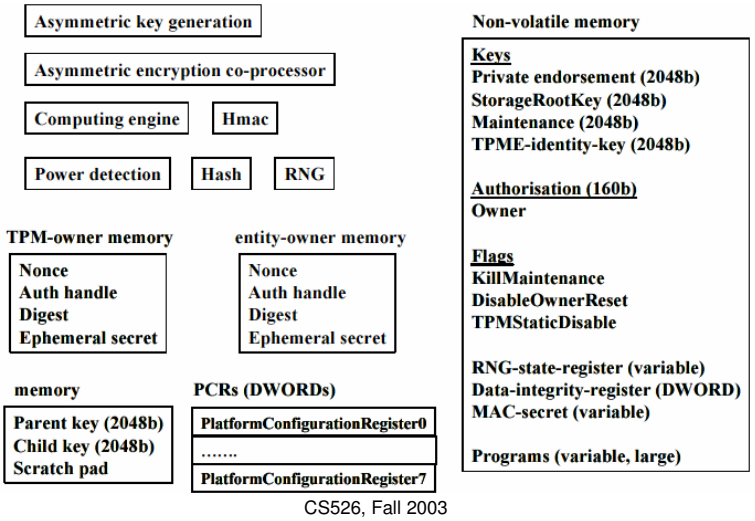
Distributed Use

- TCG spec. also supports remote query
  - Ask remote system if it is in trusted state
  - Same verification done as if local
- If remote system compromised, response won't check out

Trusted Platform Module

- Implements critical features of TCG spec.
  - Stores keys / sensitive data
- (supposedly) tamperproof
  - Evaluated with Common Criteria to Level 3
- Uniquely identified
  - Can optionally add user-specific identification
  - User-specific “aliased IDs” are all that are released

What’s In the TPM?



What is Palladium?
(Next Generation Secure Computing Base)

- Microsoft's answer to TCG
  - Integrated with Windows
  - Windows calls provide application-level support
- Is it TCG?
  - *No* – NGSCB is the software interface
  - TPM v1.1b did not support NGSCB functionality
  - TPM v1.2 does support NGSCB

What are the Added Benefits of NGSCB?

- "Library" supporting
  - Encryption/decryption
  - Key management
  - Digital signatures

  Software could do this
- Tamper resistance
  - Can't spoof the library
- What attacks remain?
  - Modify application to prevent check
  - *Might not be able to decrypt*

What Does it Mean?

- User data can be encrypted
  - Only accessible if platform meets expectations
  - User defines those expectations
- In reality: *Applications* define acceptability
  - Digital Rights Management
    - Check if user alias valid
    - proper viewer software
  - Bets on non-Microsoft .doc viewers?
- Moral: Be careful what you ask for

PURDUE UNIVERSITY

CS526: Information Security
Chris Clifton

Optional Material

Privacy

Privacy and Security Constraints

- Individual Privacy
  - Nobody should know more about any entity after the data mining than they did before
  - Approaches: Data Obfuscation, Value swapping
- Organization Privacy
  - Protect knowledge about a collection of entities
    - Individual entity values may be known to all parties
    - Which entities are at which site may be secret

Individual Privacy: Protect the "record"

- Individual item in database must not be disclosed
- Not necessarily a person
  - Information about a corporation
  - Transaction record
- Disclosure of parts of record may be allowed
  - Individually identifiable information

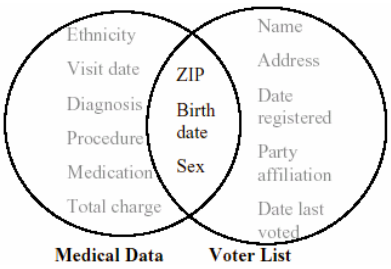
Individually Identifiable Information

- Data that can't be traced to an individual not viewed as private
  - Remove "identifiers"
- But can we ensure it can't be traced?
  - Candidate Key in non-identifier information
  - Unique values for some individuals

Data Mining enables such tracing!

Re-identifying "anonymous" data (Sweeney '01)

- 37 US states mandate collection of information
- She purchased the voter registration list for Cambridge Massachusetts
  - 54,805 people
- 69% unique on postal code and birth date
- 87% US-wide with all three



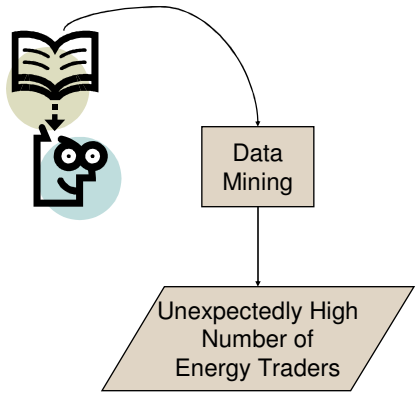
- Solution: *k*-anonymity
  - Any combination of values appears at least *k* times
- Developed systems that guarantee k-anonymity
  - Minimize distortion of results

Collection Privacy

- Disclosure of individual data may be okay
  - Telephone book
  - De-identified records
- Releasing the whole collection may cause problems
  - Trade secrets – corporate plans
  - Rules that reveal knowledge about the holder of data

Collection Privacy Example: Corporate Phone Book

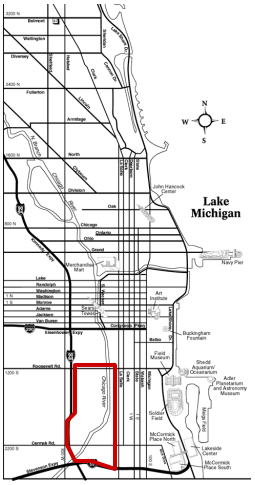
- Telephone Directory discloses how to contact an individual
  - *Intended use*
- Data Mining can find more
  - Relative sizes of departments
  - *Use to predict corporate plans?*
- Possible Solution: Obfuscation
  - Fake entries in phone book
  - *Doesn't prevent intended use*
- Key: Define Intended Use
  - *Not always easy!*



Restrictions on Results

- Use of Call Records for Fraud Detection vs. Marketing
  - FCC § 222(c)(1) restricted use of individually identifiable information
    Until overturned by US Appeals Court
  - 222(d)(2) allows use for fraud detection
- Mortgage Redlining
  - Racial discrimination in home loans prohibited in US
  - Banks drew lines around high risk neighborhoods!!!
  - These were often minority neighborhoods
  - Result: Discrimination (redlining outlawed)

What about data mining that "singles out" minorities?



Sources of Constraints

- Regulatory requirements
- Contractual constraints
  - Posted privacy policy
  - Corporate agreements
- Secrecy concerns
  - Secrets whose release could jeopardize plans
  - Public Relations – "bad press"

Regulatory Constraints: Privacy Rules

- Primarily national laws
  - European Union
  - US HIPAA rules (www.hipaadvisory.com)
  - Many others: (www.privacyexchange.org)
- Often control transborder use of data
- Focus on intent
  - Limited guidance on implementation

European Union Data Protection Directives

- Directive 95/46/EC
  - Passed European Parliament 24 October 1995
  - Goal is to ensure free flow of information
    - *Must preserve privacy needs of member states*
  - Effective October 1998
- Effect
  - Provides guidelines for member state legislation
    - Not directly enforceable
  - Forbids sharing data with states that don't protect privacy
    - Non-member state must provide adequate protection,
    - Sharing must be for "allowed use", or
    - Contracts ensure adequate protection
  - US "Safe Harbor" rules provide means of sharing (July 2000)
    - Adequate protection
    - But voluntary compliance
- Enforcement is happening
  - Microsoft under investigation for Passport (May 2002)
  - Already fined by Spanish Authorities (2001)

EU 95/46/EC: Meeting the Rules

- Personal data is any information that can be traced directly *or indirectly* to a specific person
- Use allowed if:
  - Unambiguous consent given
  - Required to perform contract with subject
  - Legally required
  - Necessary to protect vital interests of subject
  - In the public interest, or
  - Necessary for legitimate interests of processor and doesn't violate privacy

EU 95/46/EC: Meeting the Rules

- Some uses specifically proscribed
  - Can't reveal racial/ethnic origin, political/religious beliefs, trade union membership, health/sex life
- Must make data available to subject
  - Allowed to object to such use
  - Must give advance notice / right to refuse direct marketing use
- Limits use for automated decisions (e.g., creditworthiness)
  - Person can opt-out of automated decision making
  - Onus on processor to show use is legitimate and safeguards in place to protect person's interests
  - Logic involved in decisions must be available to affected person

europa.eu.int/comm/internal_market/privacy/index_en.htm

US Healthcare Information Portability and Accountability Act (HIPAA)

- Governs use of patient information
  - Goal is to protect the patient
  - Basic idea: Disclosure okay if anonymity preserved
- Regulations focus on outcome
  - A covered entity may not use or disclose protected health information, except as permitted or required…
    - To individual
    - For treatment (generally requires consent)
    - To public health / legal authorities
  - Use permitted where "there is no reasonable basis to believe that the information can be used to identify an individual"
- Safe Harbor Rules
  - Data presumed not identifiable if 19 identifiers removed (§ 164.514(b)(2)), e.g.:
    - Name, location smaller than 3 digit postal code, dates finer than year, identifying numbers
  - Shown not to be sufficient (Sweeney)
  - Also not necessary

Moral: Get Involved in the Regulatory Process!

Regulatory Constraints: Use of Results

- Patchwork of Regulations
  - US Telecom (Fraud, not marketing)
    - Federal Communications Commission rules
    - Rooted in antitrust law
  - US Mortgage "redlining"
    - Financial regulations
    - Comes from civil rights legislation
- Evaluate on a per-project basis
  - Domain experts should know the rules
  - You'll need the domain experts anyway – ask the right questions

Contractual Limitations

- Web site privacy policies
  - "Contract" between browser and web site
  - Groups support voluntary enforcement
    - TrustE – requires that web site DISCLOSE policy on collection and use of personal information
    - BBBonline
      - posting of an online privacy notice meeting rigorous privacy principles
      - completion of a comprehensive privacy assessment
      - monitoring and review by a trusted organization, and
      - participation in the programs consumer dispute resolution system
    - Unknown legal "teeth"
      - Example of customer information viewed as salable property in court!!!
  - P3P: Supports browser checking of user-specific requirements
    - Internet Explorer 6 – disallow cookies if non-matching privacy policy
    - PrivacyBird – Internet Explorer plug-in from AT&T Research
- Corporate agreements
  - Stronger teeth/enforceability
  - But rarely protect the individual

Secrecy

- Governmental sharing
  - Clear rules on sharing of classified information
  - Often err on the side of caution
    - Touching classified data "taints" everything
    - Prevents sharing that wouldn't disclose classified information
- Corporate secrets
  - Room for cost/benefit tradeoff
  - Authorization often a single office
    - Convince the right person that secrets aren't disclosed and work can proceed
- Bad Press
  - Lotus proposed "household marketplace" CD (1990)
    - Contained information on US households from public records
    - Public outcry forced withdrawal
  - Credit agencies maintain public and private information
    - Make money from using information for marketing purposes
  - Key difference? *Personal information isn't disclosed*
    - Credit agencies do the mining
    - "Purchasers" of information don't see public data