Some Emerging Issues in Security Research

Gene Tsudik
Computer Science Department
University of California, Irvine

Disclaimer

- My opinions are:
  - Mine alone
  - One-sided
  - Myopic
  - Biased
  - Self-serving
- I apologize, in advance, for:
  - Banalities
  - Stereotyping

My research interests

- Applied Cryptography
- Computer/Network Security & Privacy
- Examples:
  - Secure routing, membership in MANETs
  - Privacy + Integrity for outsourced data(bases)
  - Secure data aggregation (e.g., in WSNs)
  - Privacy-preserving security (e.g., authentication, signatures)
  - Secure Group Comm. (e.g., key management)
  - Human-assisted security (e.g., device pairing)

Outline

- The Monoculture Curse
- Privacy Challenges
- Longevity and Integrity
- Usability (sprinkled throughout)
- Conclusions

The Monoculture Curse

Monoculture: one parasite kills all!

- Operating Systems
  - Windows XP
- Communication Protocols
  - TCP/IP, GSM, BGP
- Encryption & Authentication methods
  - MD5, SHA-1, RSA
- Cryptographic Protocols
  - X.509, Kerberos, SSL/TLS
- Formats
  - PKCS, S/MIME, IPSec

Fighting Monoculture?

- Don’t put “all eggs in one basket”
- Heterogeneity
  - Avoid single-track “standards” no matter how many experts claim otherwise
- Hedging
  - Use many mechanisms at once
    - – Expensive
    - + One fails, others stand

Example

- Most (>90%) SSL/TLS server certificates use MD5/RSA or SHA-1/RSA
- Two problems:
  - MD5 – strong collision-resistance property recently shown to be false
  - RSA – relies on *alleged* hardness of factoring large composites, or *alleged* hardness of taking e-ary roots modulo composite (e.g., e=**65537)**
  - What if RSA falls?
  - Recall recent discovery of P-time deterministic primality-testing algorithm

A typical certificate

```
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number: 28 (0x1c)
      Signature Algorithm: md5WithRSAEncryption
      Issuer: C=US, O=Globus, CN=Globus Certification Authority
      Validity
         Not Before: Apr 22 19:21:50 1998 GMT
         Not After : Apr 22 19:21:50 1999 GMT
      Subject: C=US, O=Globus, O=University of Southern California, \
               ou=ISI, CN=bonair.isi.edu
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
         RSA Public Key: (1024 bit)
            Modulus (1024 bit):
               00:bf:4c:9b:ae:51:e5:ad:ac:54:4f:12:52:3a:69:
               <……>
               b4:e1:54:e7:87:57:b7:d0:61
            Exponent: 65537 (0x10000000000000001)
      Signature Algorithm: md5WithRSAEncryption
          59:86:6e:df:dd:94:5d:26:f5:23:c1:89:83:8e:3c:97:fc:d8:
          <……>
```

Example (contd.)

- Pick 2 or 3 hash functions
  - E.g., MD5, SHA, RIPE-MD
- Use a dual-method certificate
  - E.g., RSA/MD5-SHA and DSA/SHA-RIPE-MD
- If one method found to be weak
  - Issue an **ARL**: Algorithm Revocation List, e.g., simultaneously revoke all certificates with MD5 as hash

P.S.

- Hash functions seem to be failing us
- Is it time to reconsider the popular *hash-and-sign* approach?
- For short messages, can we "go back" to the chained (a' la DES-MAC) mode of signing?
  - E.g., for signing public key certificates?
- For long messages, can we use block ciphers to "emulate" a hash function?

Privacy – “the final frontier”

Privacy is a double-edged sword

- Freedom of expression
- Whistle-blowing
- Censorship avoidance
- Freedom of association
- Protection from *Big Brother*, snooping merchants and nosy neighbors

- Libelous accusations
- Anonymous denouncements
- Repugnant, vile speech
- Promoting illegal activities
- Impunity from legal scrutiny

Privacy issues in networking

Not just *contents* of communication

- Who is talking to whom?
  - why is Alice talking to Bob?
- Who is being looked up?
  - a dissident web site?
- Who is “popular”?
  - why is a particular site/host being queried?

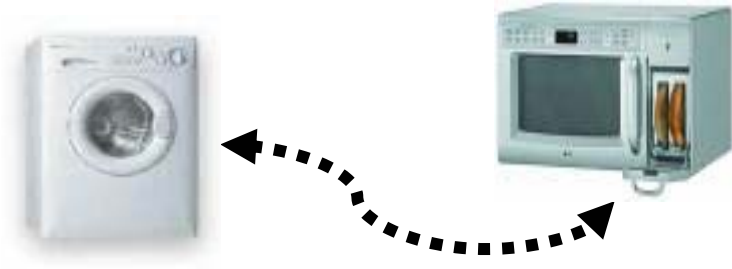
Current privacy techniques

- Anonymous Email (e.g., MIXes)
- Anonymous Web browsing (e.g., anonymizers)
- Anonymous network-layer communication (onion routing + IPSec?)

Privacy issues in everyday networking

- Internet Naming Service: DNS
  - Set of name servers queried about target
- Address Resolution Protocol: ARP
  - All hosts on LAN queried about target
- Certificate Revocation Checking: OCSP, CRLs
  - Server queried about target
- Dynamic Address Assignment: DHCP
  - Host requests IP address from server

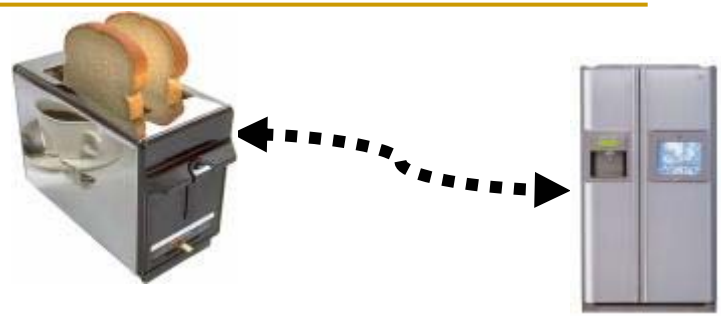
Privacy in the home



- ✓ Home networking is rapidly permeating the developed world
- ✓ Wireless networking predominates
- ✓ How does one control the network *perimeter* ?
- ✓ Firewalls keep things out, but:
  - ✓ Do you know who "comes out" from the inside?
  - ✓ Can you be framed?

  - ✓ What if your firewall/router requests and receives child porn or *subversive* material?

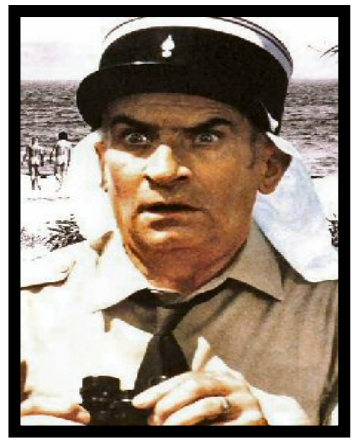
Privacy in the home



What about snooping on, or casing, your residence?

- Are you at home?
- Are your children at home?
- Is your refrigerator talking to your oven?
- Which devices are talking?
- When is a good time to break in?

Privacy in the home



- How to easily and securely introduce, pair, ”train” new networked appliances and devices?
- Measures must be:
  - Human-assisted
  - Meaningful
  - Simple

Privacy in the home: solutions?

- Sensors around the perimeter
  - Monitor incoming wireless signals
  - Directional jamming
  - Reporting/alerting
- Traffic masking – resistance to eavesdropping and traffic analysis
  - Similar to military-type techniques
  - End-points
  - Frequency
  - Amount
- Not only intra-LAN; first external hop too…

Privacy of Web Usage

- Recall recent Google / US Government "conflict"
  - Govt. demanded access to frequent queries
  - Google refused
  - Judge ruled in Govt. favor (sort of)
  - The saga continues…
- Raises justifiable fears about privacy
  - How to do searches while masking true intent?
  - Private Information Retrieval (PIR)
    - Inefficient today → much more research needed!

Privacy in security?

Privacy concerns prompt re-thinking of traditional security services, such as:

- Authentication Protocols
  - Alice and Bob want to authenticate each other
  - Involves exchanging identity information
  - Observable and track-able
  - Encryption does not help much…
- Digital Signatures
  - Alice wants to sign a document (for Bob)
  - Alice tells Bob her name and her public key (certificate)
  - Anyone can link Alice to the signature
  - Anyone can “link” multiple signatures by Alice

Privacy in security?

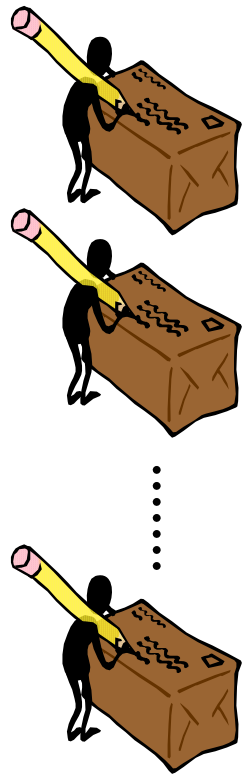
- Anonymous Authentication Protocols ➔ **Secret Handshakes**
- Anonymous Digital Signatures ➔ **Group Signatures**

Secret Handshakes

- Alice and Bob are CIA agents
- CIA agents are not allowed to divulge affiliation except to other secret agents
  - Alice will authenticate to Bob only if he's a CIA agent
  - Bob will authenticate to Alice only if Alice is a CIA agent
  - Others (whether CIA agents or not) should be unable to determine Alice's or Bob's affiliation
- How can Alice and Bob authenticate each other?
- Secret Handshakes = unobservable unlinkable all-or-nothing (privacy-preserving) authentication

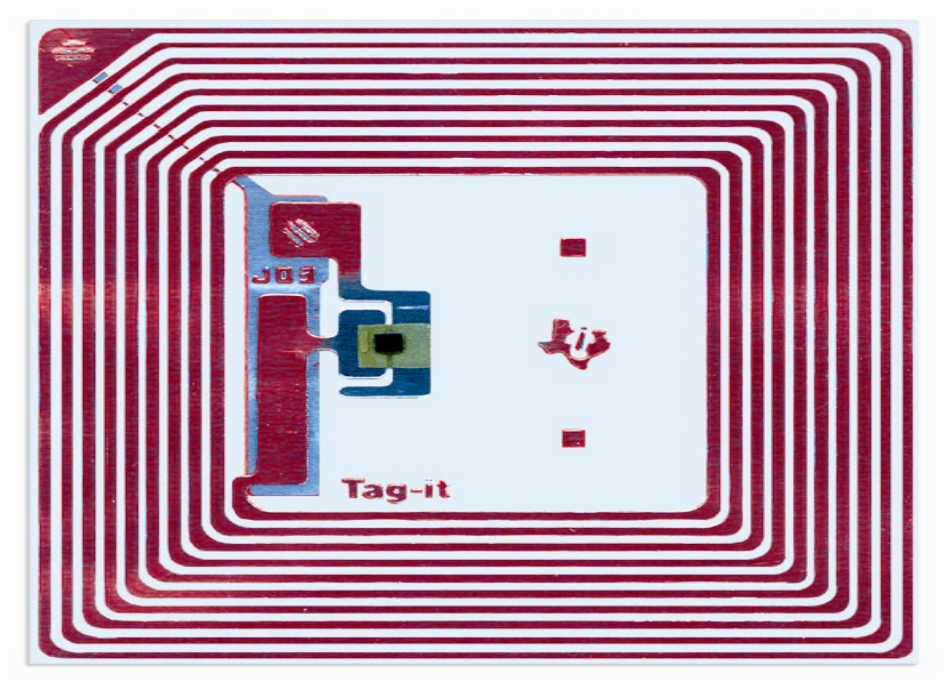
Group Signatures

- Alice needs a prescription drug
- Bob is an authorized doctor who writes (signs) the prescription
- Alice takes the prescription to Eve (pharmacist)
- Eve knows who Bob is…
- It's not enough if Bob adopts a "pseudonym"
- Eve only needs to know that Bob is a *bona fide* doctor



- Similar settings: GSM Roaming, Credit Cards, DHCP
- Group Signatures = Anonymous Unlinkable Signatures (with escrowed anonymity)

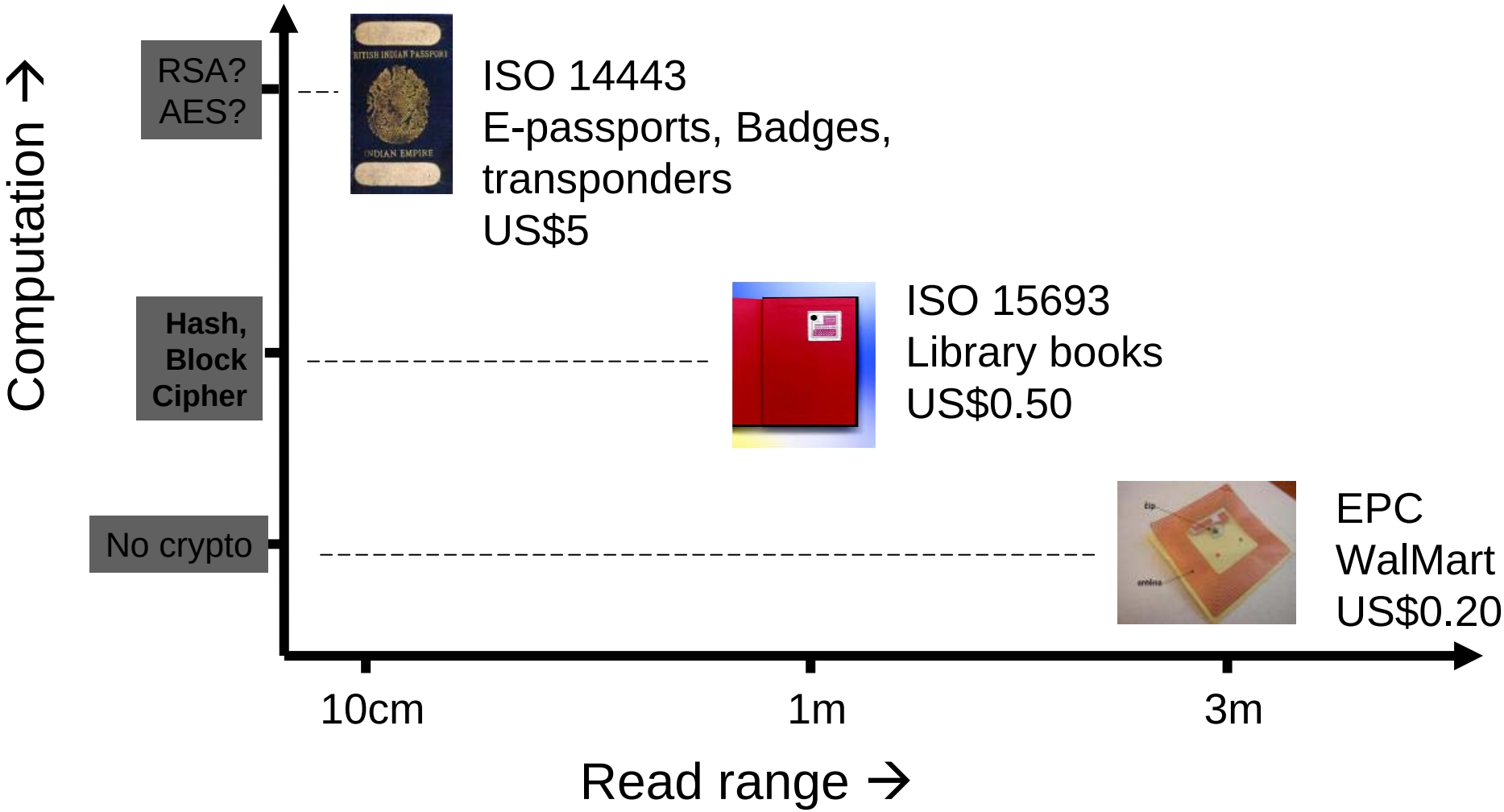
RFID Privacy



RFID System Components

- Tags (*transponders):*
  - affixed to objects, carry identifying data
- Readers *(transceivers)*:
  - read or write tag data and interface with back-end databases
- Back-end databases *(servers):*
  - correlate tag data with objects

Variety of RFID Technologies



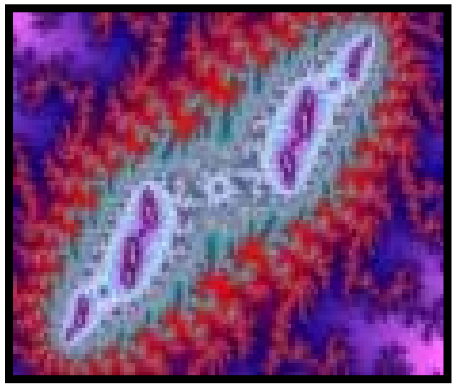
Problems:

- Privacy:
  - Tracking tags by:
    - Eavesdropping on tag←→reader interaction
    - Rogue readers interrogating tags
    - Identifying product-line (merchandise type)
- Security:
  - Tag cloning
- Denial-Of-Service:
  - Killing/incapacitating tags

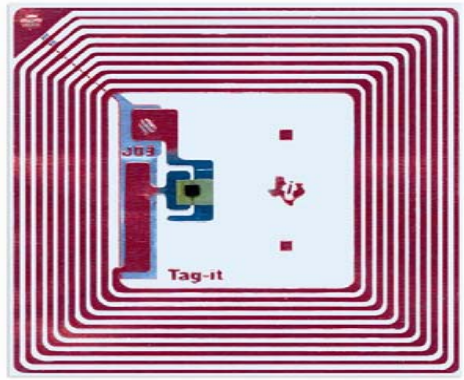
RFID security challenge

How to obtain maximum security & privacy with minimal resources?

An RFID tag is a computational Amoeba



=



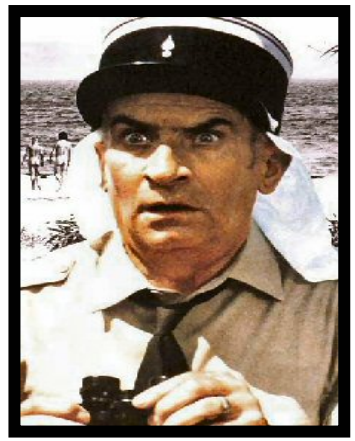
Solutions?

- Encryption (randomized): against eavesdropping (tracking)
- Tag → reader authentication: against cloning / counterfeiting
- Reader → tag authentication: against rogue readers (tracking)
- Tamper-resistance: against tracking and cloning (expensive for very cheap tags…)

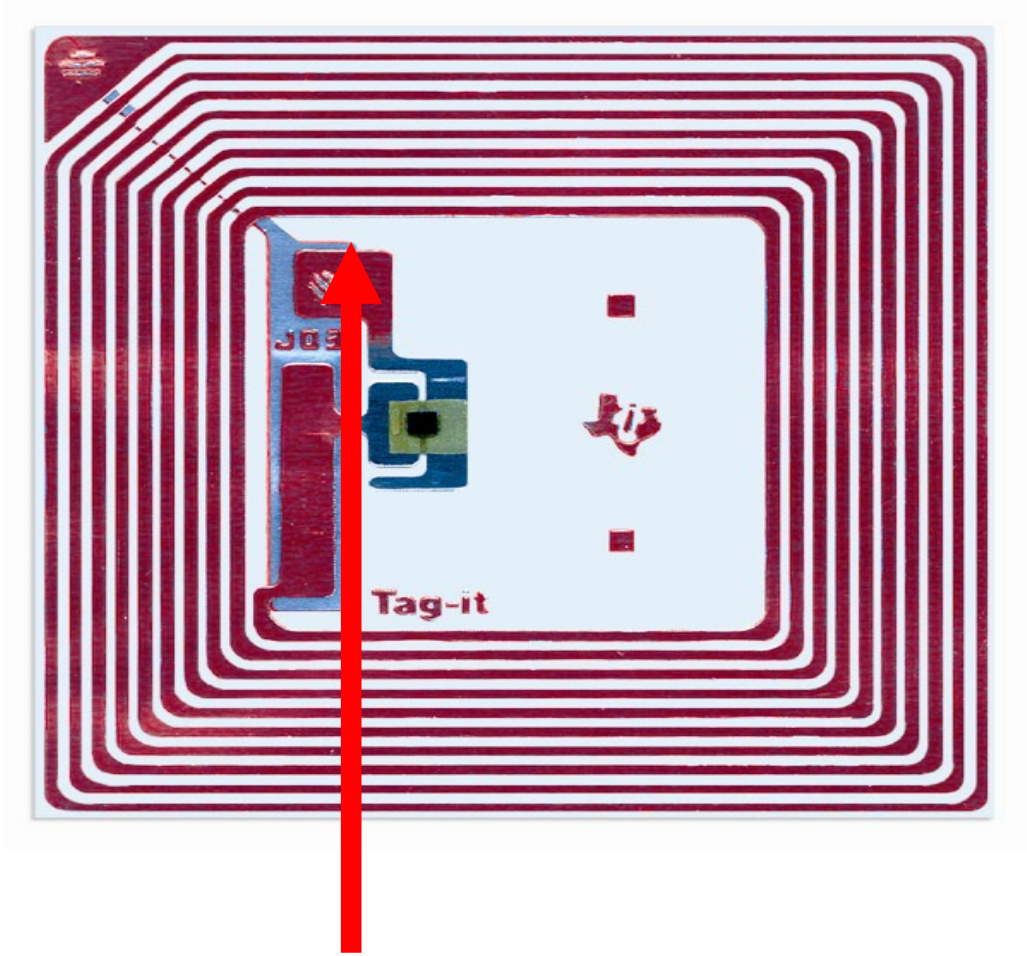
Ideally would use group signatures but cost prohibits it…

RFID acceptance?

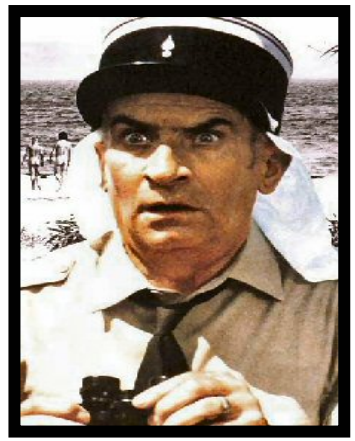
- Ultimately depends on the human user
- How to convince an average user that s/he has control over RFID tags?
- Measures must be:
  - Human-assisted
  - Meaningful (e.g., visual)
  - Simple
  - Inexpensive
  - e.g., “Search and Destroy”



RFID acceptance?



For example, use a toothpick-like piece of plastic to separate chip from antenna



Longevity of security

Of wrinkles, rust and fading

Digital security is relatively new

- How does it withstand the aging process?
- When a new building material is introduced manufacturers know how to simulate aging

- Encryption
- Digital Signatures

Longevity of Secrecy

- Want to keep data secret for a LONG time. How to make sure that encryption does not degrade over the long term?
- Encrypt with a LONG key?
- How long is long enough?

Longevity of Authenticity/Integrity

- Digitally sign a document today
- How to make sure that signature algorithm's strength does not degrade over the long term?
- Sign with a LONG key?
- How long is long enough?
- What if key ever compromised?
- What if signature algorithm becomes weak?

On a related note

- Human (manual) signatures
  - Provide very weak authentication and no integrity
  - Represent value in and of themselves
    - E.g., paintings, manuscripts, sheet music
- Digital signatures
  - Provide strong authentication and integrity
  - Not valued today (yet)
  - What if a digital signature represents value?
  - How does one show a signature without fear of it being copied?

Conclusions

No words of wisdom…but:

- Privacy matters
- Assault on privacy will intensify
  - Home networking
  - Internet in general
  - RFID tags and the like
- Opportunity exists to make Internet more privacy-friendly
  - U.S. NSF Future Internet Design (**FIND**) Program
- Longevity of digital signatures not solved
- Security starts and ends with the (human) user
- No panaceas envisaged against:
  - Phishing Attacks
  - SPAM
  - Denial of Service Attacks

Thank you!

Questions?