

Total Recall: Are Privacy Changes Inevitable?

William C. Cheng
Computer Science Dept. & IMSC, USC

Leana Golubchik
Computer Science Dept. / EE-Systems Dept. / IMSC / ISI, USC

David G. Kay
Donald Bren School of Information and Computer Sciences, UCI

Project URL: <http://bourbon.usc.edu/iml/recall/>
Internet Multimedia Lab, USC

Total Recall Project at USC

- ➔ Continuous recording of personal experiences
 - ⇒ Personal sensors for data acquisition
 - ⇒ Data stored on *Total Recall* servers
 - strong encryption
 - indexing, searching, retrieving, etc.
 - ⇒ Records a *individual perspective* of his/her world
 - whispers and peeks (things that environmental sensors cannot see, hear, or sense)
 - need to address *privacy* issues
 - ⇒ Recall, playback
 - immersive environment, eventually

Total Recall Applications

- ➔ **Not just a memory enhancer**
- ➔ **Health care**
 - ➔ **Recall a patient's food intake and recent environments can help discovery of allergies**
 - ➔ **Monitoring food intake of diabetics can provide warning signals when appropriate**
 - ➔ **Support of elderly and people with disability**
- ➔ **Education**

Transparent Society vs. Big Brother



Transparent Society

- **Total Recall** data can be used in legal proceedings
 - business dealings
 - sexual harassment and rape
- Easy to prove who said what, if data can be **authenticated**
- If everyone is recording, will lead to honesty



Big Brother

- Fear that data collected for one purpose will be used for another purpose
- Privacy, as we know it, will be lost forever



This talk focuses on **privacy** issues



The Role of a Technologist

- ➔ Design and build systems that provide proper *security*, *privacy*, and *integrity mechanisms*
- ➔ Make sure that these mechanisms can enable a wide variety of policies so that legal/social policy development is not hampered by a paucity of technical alternatives
 - ⇒ Without technical flexibility, the inevitable development of technology may result in *poor policy by default*

The Law

- ➔ **Mathematical proof is not required**
 - ▬ Reasonable/plausible explanation is sufficient
- ➔ **Interpretation of a law is a function of many things**
 - ▬ Precedence
 - ▬ Other law
- ➔ **Changing the law is difficult**
 - ▬ Someone (or even many) has to die
 - ▬ Public outcry/outrage
- ➔ **Is this a US issue?**
- ➔ **Future harm vs. profit now?**

Privacy

- ➔ What is the difference between *Total Recall* and human memory?
- ➔ A third party gaining access to *Total Recall* data
 - legal as well as illegal access
 - ➔ Having the system implies that certain records exist
 - ➔ Only way to access human memory is through questions
- ➔ All these give rise to privacy concerns

Are We Allowed to Record Everything?

- ➔ Is it legal under current law?
 - It depends...
 - different states have different laws w.r.t. audio and video recording

- ➔ Fundamental principle
 - People are entitled to privacy where privacy is their *"reasonable expectation"*
 - home vs. walking on a public street
 - tourist can record a street scene for private use
 - legally, little difference between that and *Total Recall*
 - until *Total Recall* becomes widely used -- yet unrecognized legally
 - overlapping web of recorded *memories* -- unknown impact



Consent

- ➔ Obtaining consent can be problematic with pervasive use of *Total Recall*
- ➔ Provide mechanisms for *implied consent*
 - ▬ Recurring beep, flashing lights, etc.
 - ▬ Might degrade the quality of information
- ➔ Implies understanding of data's use
 - ▬ Long standing principle of fair information practices holds that, "*information gathered for one purpose not be used for another without the subject's consent*"

What Can We Do With It?

- ➔ Security measures to protect against unauthorized 3rd party use
- ➔ Legal private use is largely unrestricted
 - Publishing without permission could give rise to liability
- ➔ Use by the judicial system
 - The US Fifth Amendment (protection against self-incrimination) would likely *not* protect *Total Recall* data
 - similar to bank records and e-mail records
 - In civil lawsuits, even an uninvolved 3rd party can be asked to produce *Total Recall* data
 - once asked, destruction or alteration is illegal
 - Threat of ubiquitous use of RFIDs
- ➔ National security concerns

Will We See Legal Support?

- ➔ The law does evolve to accommodate new technology
 - E.g., changes in rules for use of original documents
- ➔ In theory, new rules of evidence could be adopted to exclude or limit use of *Total Recall* data
 - But unlikely due to legitimate use of data
- ➔ Proactive protection is harder to achieve
 - Likelihood of protective legislation in advance is low for potential abuse of an as-yet-undeveloped technology
 - reluctance to inhibit the development of rapidly evolving technologies
 - By the time any technology has even the smallest commercial foothold, its commercial supporters are likely to oppose any restrictions

Will We See Legal Support? (Cont...)

- ➡ Law evolves slower than technology
 - As it should
 - Systems like Total Recall will be developed before comprehensive policy on private of its recordings
 - Changes in nature of privacy are likely inevitable

- ➡ Vital role still exists for technologists
 - Designing highly configurable systems with enough technical "*hooks*" to enable whatever privacy policies are eventually arrived at

Could Technology Help?

- ➔ **Making other users of similar systems invisible**
 - ▬ "Don't record me" preference setting
 - ▬ Comprehensive inauthenticity could diminish utility of such systems

- ➔ **Authenticity-bit**
 - ▬ On if data is original/authentic
 - ▬ Off if data is modified
 - automatic or user directed
 - ▬ One-way transition from authentic to modified

Authenticity-bit



Advantages

- Authentic data can be used against other forms of evidence
- If off by default, one *might* have some protection against non-consensual use of recordings in legal proceedings



But modified data may still be admitted as evidence

- Legal system does not require provable certainty
 - hardly recognizes absolute certainty as a concept
- Legal system provides different levels of required proof
 - beyond a reasonable doubt vs. clear and convincing vs. strength of evidence
- We cannot tell the legal system to ignore information, the legal system will make up its mind, even if the authenticity-bit is off



Authenticity-bit (Cont...)

- ➔ Imagined exchange in the paper
 - [...]
 - Probably the court would rule to admit the evidence under current law

- ➔ Rules of evidence could change
 - *Total Recall* records with authenticity-bit off could be made inadmissible explicitly
 - Need to be skeptical on practical and political grounds
 - Authenticity-bit could provide the hooks on which policymakers could hang a legal protection scheme

A Possible Implementation

- ➔ Using currently available technology
- ➔ Wearable recording device
 - store data on removable memory card
 - user (Alice) can remove card and *edit* data
 - data is eventually uploaded to a server when device is connected to the Internet
 - data can sit on the wearable device for days
 - Alice has plenty of time to modify data
 - need to authenticate data
 - can have the wearable device *digitally sign* every data block it produces
 - but can be problematic -- e.g., Alice drains battery, time-shifts data sequence

— (cont...)

A Possible Implementation (Cont...)



Wearable recording device (cont...)

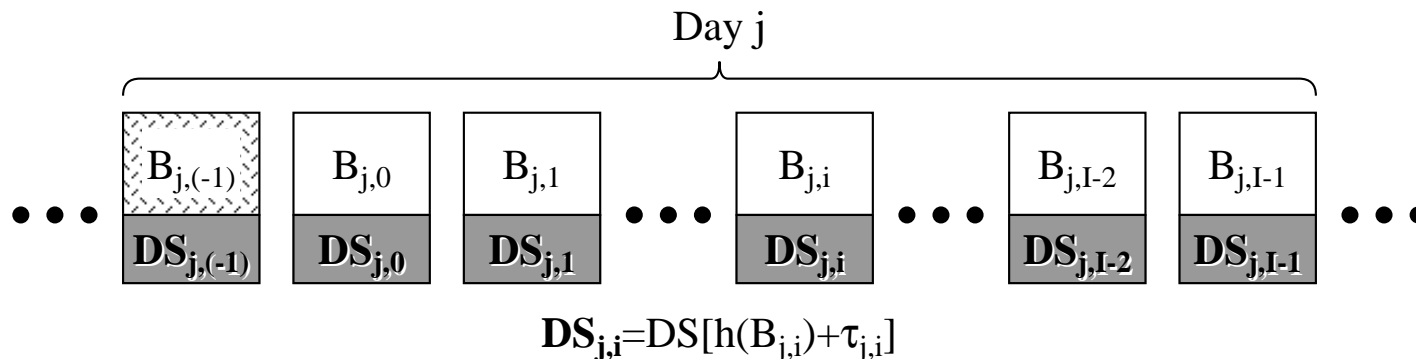
= strong encryption, device equipped with a

cryptographic smartcard

- temper-resistant
- contains a *private-key*
- can perform public-key and secret-key cryptography
- private-key is never exposed
- in order to decrypt something encrypted with the public-key, the corresponding smartcard must be *physically* present (no copy of the private-key)

Third-party Authentication

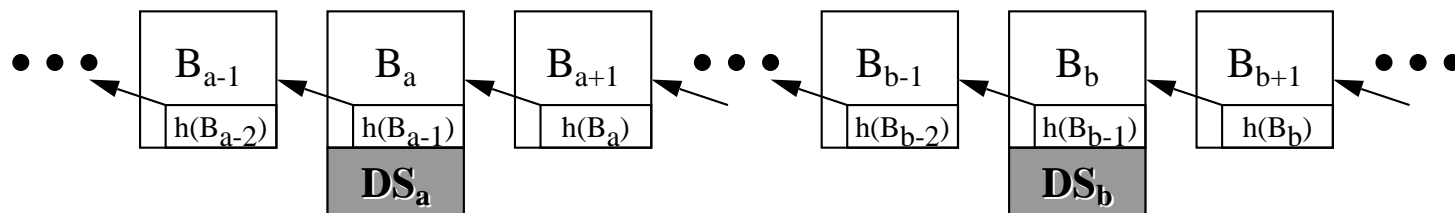
- ➔ Use of a *notary server*
 - Similar to a timestamp server in the *Bistro System*



- ➔ Only way to decrypt the data blocks is with the presence of the smartcard (not possible to transmit the private-key to a server)

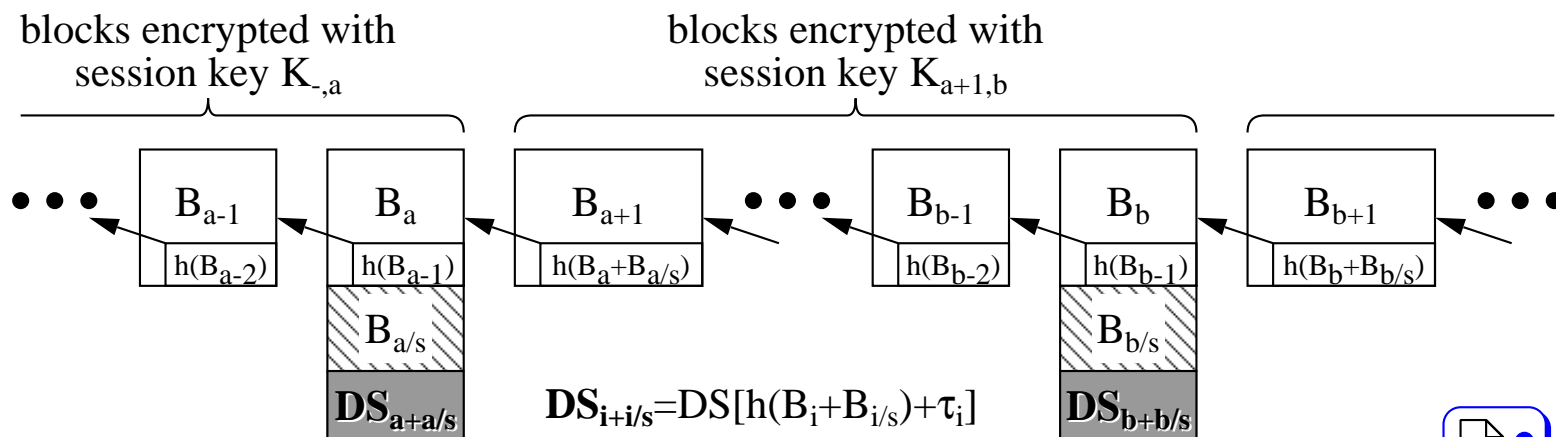
Practical Considerations

- ➔ **Poor/unavailable network connectivity**
 - Alice may trick the device to decrypt the special block to obtain the day key and modify data blocks
 - Although Alice is allowed to modify data, must not let Alice *claim authenticity* if data blocks are modified
- ➔ **Only sign occasionally**
 - Create dependencies between data blocks via *chaining*

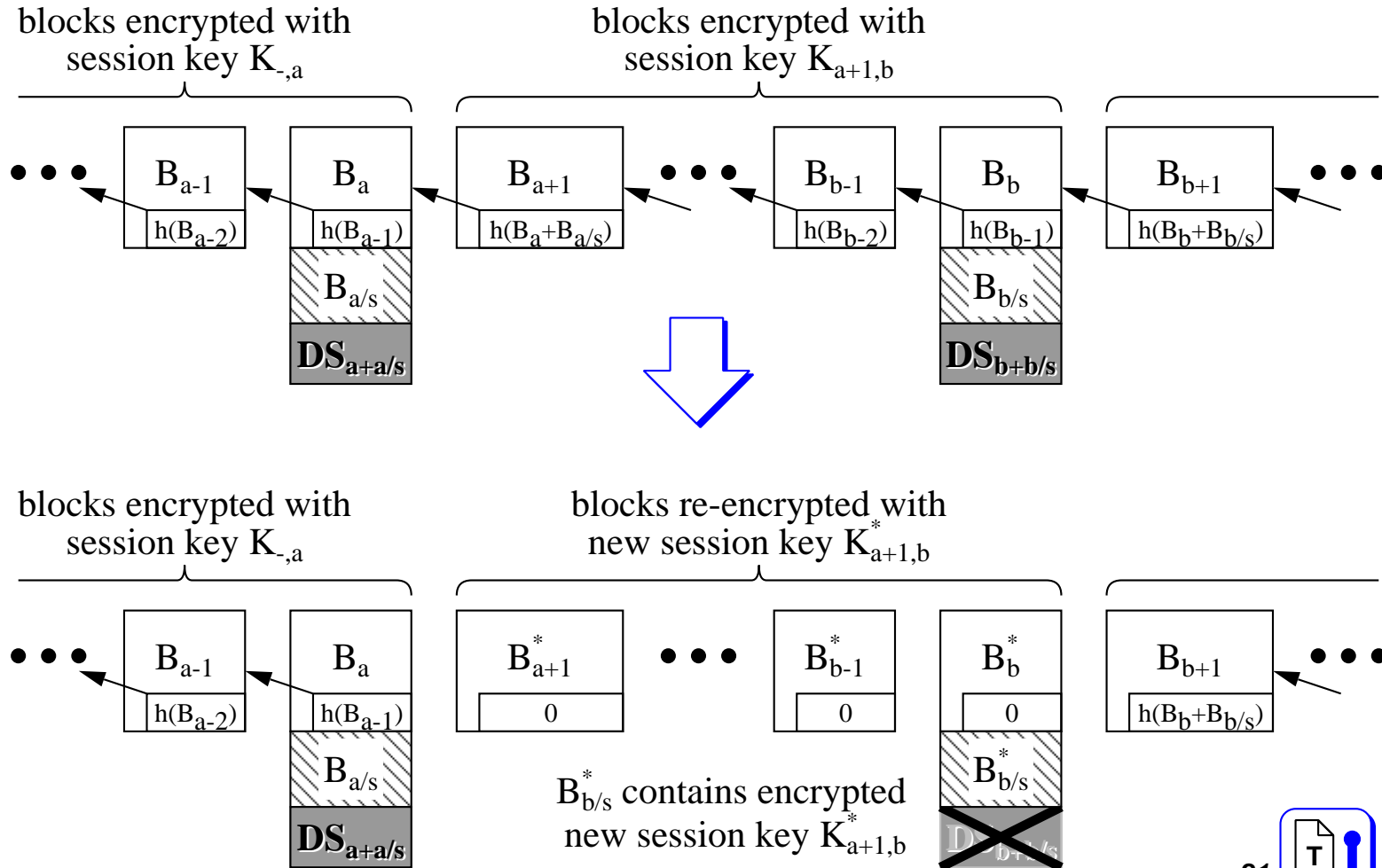


Day Key

- ➔ Day key should only be released when it's no longer used
 - ▢ Also, day key should be released in a notarized block
 - ▢ Otherwise, Alice may modify *some* data
- ➔ May be days before Alice gets network connectivity
 - ▢ Encryption key should not be associated with the calendar -- day key replaced by *session key*



Modifying Data Blocks



Concluding Remarks

- ➔ We have explored privacy concerns in a legal/social setting, offered a potential technical mechanism (authenticity-bit) to address some of the issues
- ➔ There are other broader implications of *Total Recall* deployment
 - ➔ "So, Mr. Jones, you turned your Total Recall off when you met Mr. Smith. What were you trying to hide?"
 - ➔ Will human memorization becomes less important a skill?
- ➔ This is not intended as a definitive solution, but a starting point for future discussions
 - ➔ Much is left to consider, but the potential is great and so worth pursuing

Concluding Remarks (Cont...)

- ➔ We believe that systems like *Total Recall* will get built and will have valuable uses, and will radically change our notions of privacy
 - ➔ Useful technologies are largely inevitable
 - ➔ They often bring social changes with them
 - ➔ And we inevitably both suffer and benefit from their consequences

- ➔ There is not much preventing collection of a lot of data about someone anyway

- ➔ Our job is to provide sufficiently flexible systems