INFS 767 Secure Electronic Commerce Fall 2001

Lecture 6 Unlinkable Serial Transactions

Prof. Ravi Sandhu

CASE STUDY OF AN ELECTRONIC COMMERCE PROTOCOL

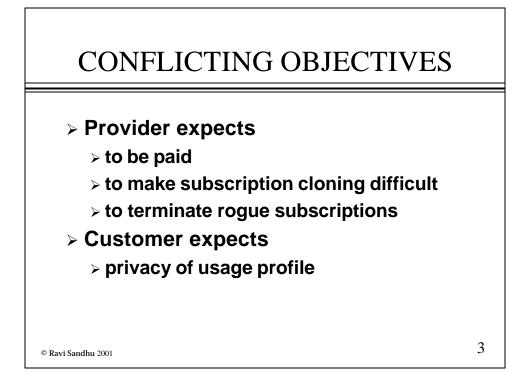
 Unlinkable Serial Transactions: Protocols and Application

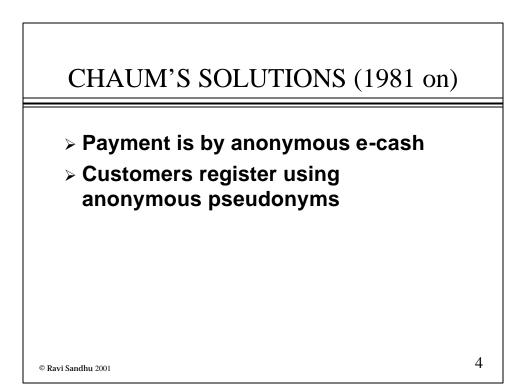
by

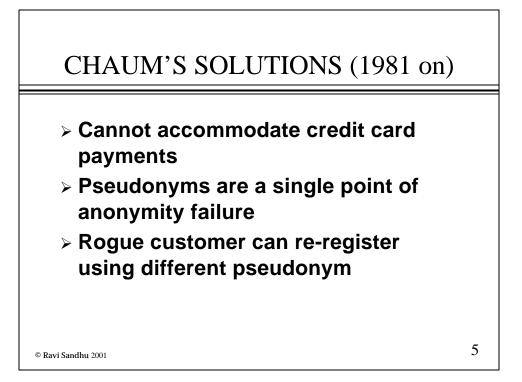
Stubblebine, Syverson and Goldschlag

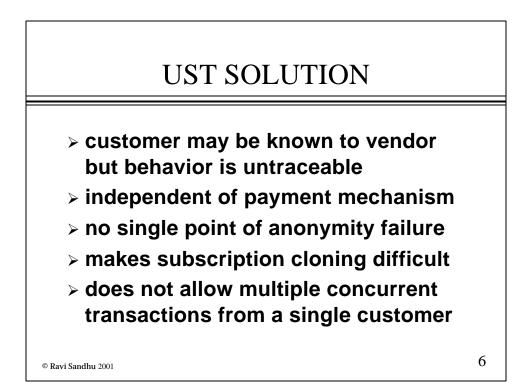
 Paper in November 1999 issue of ACM Transactions on Information and System Security (TISSEC)

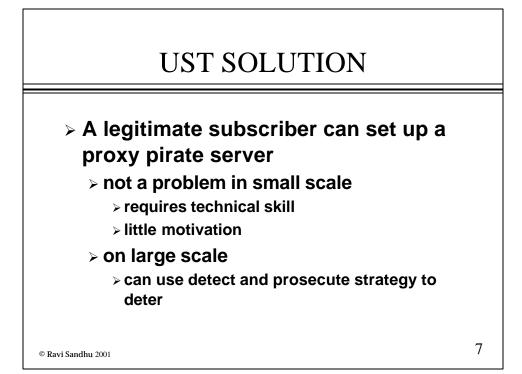
2

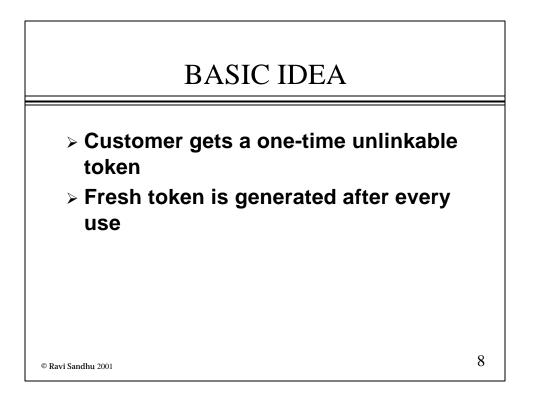


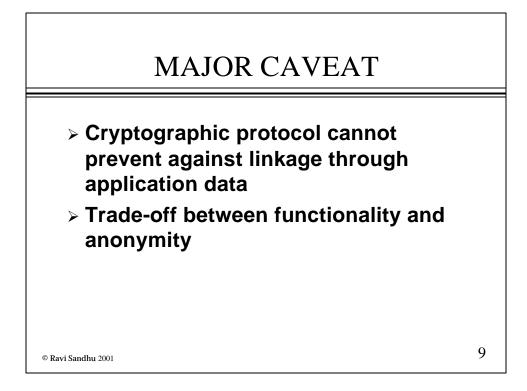


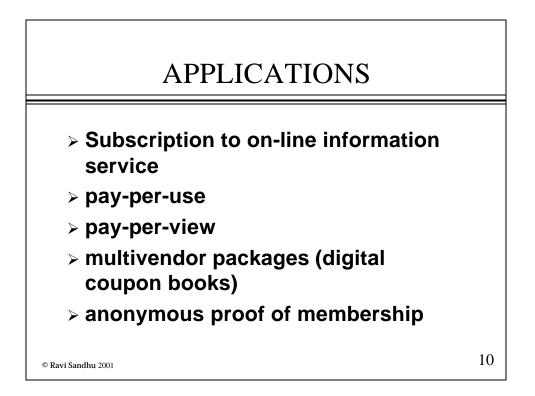












OPERATING ENVIRONMENT ASSUMPTIONS

- A1. Anonymity protected network communications are unlinkable to prior communications provided application content does not enable linkage.
- A2. Entities may collude. However, we assume that collusion among customers is insignificant in the sense that there will always be a sufficient number of non-colluding customers and associated transactions to mask legitimate customer activity.

© Ravi Sandhu 2001

OPERATING ENVIRONMENT ASSUMPTIONS

- A3. We assume that cryptographic keys, nonces, blinding factors, etc. are adequately randomly chosen from an adequately large space to prevent random collisions or revealing of secrets by cryptanalytic attacks.
- A4. We assume that keyed cryptographic operations prevent any undetectable modification of fields to which those operations are applied. Furthermore, we assume the inability of an entity to forge signatures without knowledge of the key.

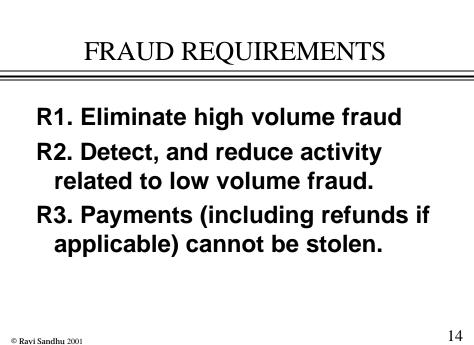
© Ravi Sandhu 2001

OPERATING ENVIRONMENT ASSUMPTIONS

A5. We assume that every message is received as sent after a finite number of attempts to send it.

A6. The vendor will provide services for which he accepts payment.

```
13
```



CUSTOMER PRIVACY REQUIREMENTS

R4. Protect the identity of the customer in a transaction from vendors, other customers, and outsiders.

R5. Prevent the building of customer profiles (including pseudonymous profiles) by vendors, other customers, and outsiders.

15

SERVICE GUARANTEE REQUIREMENTS

R6. Customers cannot be denied service for which they contracted.

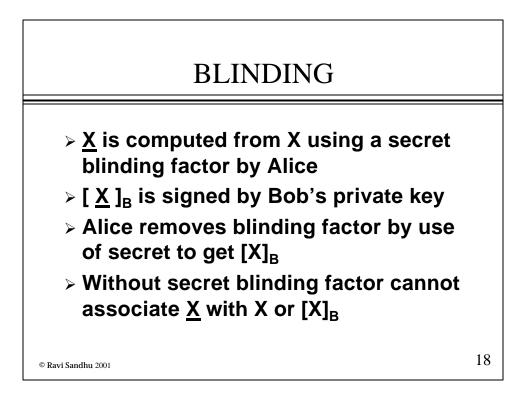
© Ravi Sandhu 2001

© Ravi Sandhu 2001

NOTATION

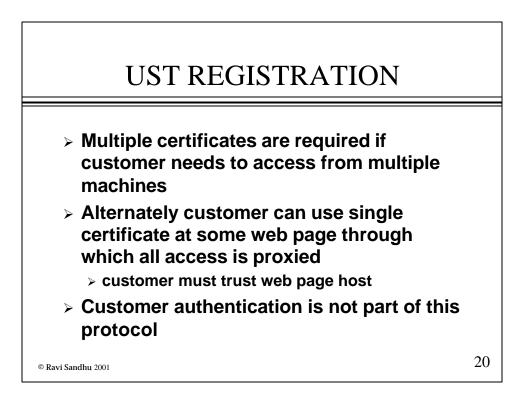
[X]_K: Message integrity of X using K
 {X}_K: Message integrity and confidentiality of X using K
 X: Blinding of X
 h(X): Hash of X

© Ravi Sandhu 2001



UST REGISTRATION

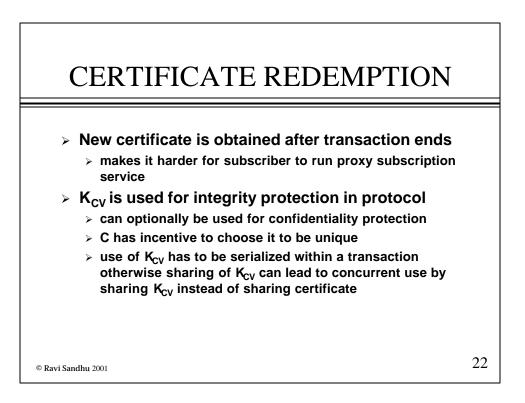
M1. C -> V: {Payment, K_{CV} }_V, [Request for certificate of type S, C, h(N1)]K_{CV} M2. V -> C: [<u>h(N1)</u>]_s M3. C -> V: [Ack] K_{CV} 19



CERTIFICATE REDEMPTION

M1. C -> V: { $[h(Ni)]_S$, Ni, K_{CV} }_V, [Request for transaction of type S, h(Ni+1)] K_{CV} M2. V -> C: [Approved OR Not Approved] K_{CV} M3. C <-> V: [Transaction] K_{CV} M4. V -> C: [h(Ni+1)]_S M5. C -> V: [Ack] K_{CV}

21

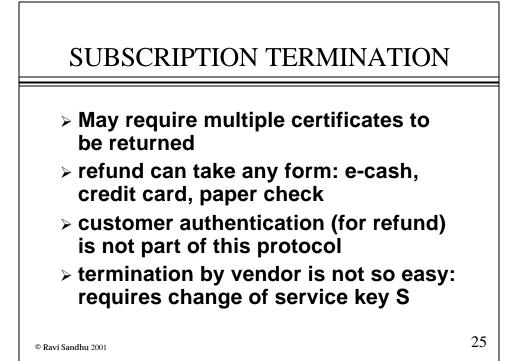


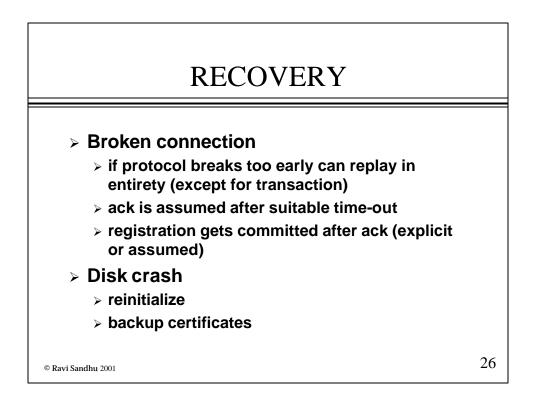


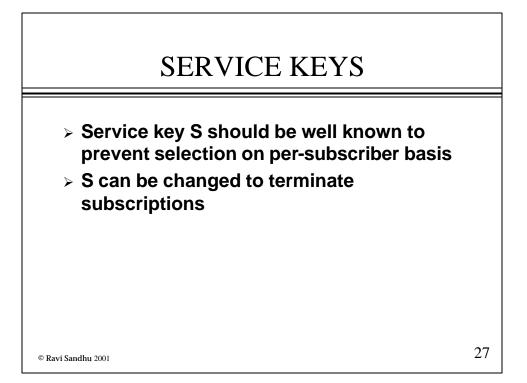
- [Not Approved]K_{CV} is sent only if nonce does not match signed certificate
- > other Not Approved errors sent without K_{CV}
- > makes protocol fail-stop

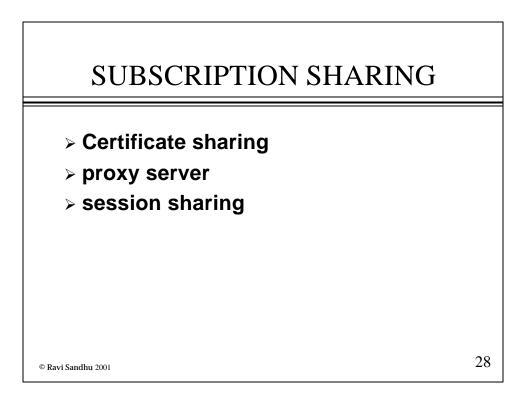
© Ravi Sandhu 2001

SUBSCRIPTION TERMINATION M1. C -> V: { [h(Ni)]_S , Ni, K_{CV}}_V, [Request for transaction of type S terminate, C]K_{CV} M2. V -> C: {Refund}K_{CV} OR [Not approved]K_{CV} M3. C -> V: [Ack]K_{CV}





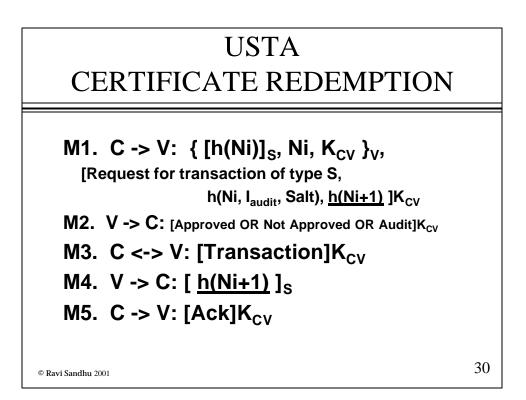




UST WITH AUDIT (USTA) REGISTRATION

M1. C -> V: {Payment, I_{audit}, K_{CV}}_V, [Request for certificate of type S, C, <u>h(N1)</u>]K_{CV}
M2. V -> C: [<u>h(N1)</u>]_S
M3. C -> V: [Ack] K_{CV}

29



AUDIT PROTOCOL

M1. C -> V: { $[h(Ni)]_S$, Ni, K_{CV} }_V, [Request for transaction of type S, $h(Ni, I_{audit}, Salt), \underline{h(Ni+1)}]K_{CV}$ M2. V -> C: $[Audit]K_{CV}$ M3. C -> V: {C, Ni, I_{audit} , Salt} K_{CV} M4. V -> C: [$\underline{h(Ni+1)}$]_S OR [Not approved] K_{CV} M5. C -> V: [Ack] K_{CV}

31

