온라인 디지털 콘텐츠 공동 저작권 보호에 적합한 부인봉쇄 디지털 다중서명 기법

The undeniable digital multisignature scheme suitable for joint copyright protection on digital contents

윤성현, 한군희*
천안대학교 정보통신학부*

Yun Sung-Hyun, Han Kun-Hee*
Div. of Information and Communication Engineering, Cheonan Univ*

요약

부인봉쇄 서명 기법은 서명자의 동의 없이는 서명을 검증할 수 없는 기법이다. 일반 서명기법이 적용될 수 없는 많은 사회적 영역의 컴퓨터화에 사용될 수 있다. 본 연구에서는 여러 서명자를 필요로 하며 지정된 검증자에게만 다중 서명을 검증할 수 있도록 하는 부인봉쇄 다중서명 기법을 제안한다. 제안한 다중서명 기법은 부인봉쇄 성질을 만족하며 서명자에 의한 다중서명 부정 및 변조 공격에 대해서 안전하다. 또한 디지털콘텐츠 공동 저작권 보호를 위한 제안한 기법의 적용 방안에 대해서 살펴본다.

Abstract

In undeniable digital signature scheme, the signature can not be verified without the signer's cooperation. The undeniable signature scheme can be used to computerize many applications which can not be done by a conventional digital signature scheme. In this study, we propose the undeniable digital multi-signature scheme which requires many signers and designated verifier. The multi-signature can be verified only in cooperation with all signers. The proposed scheme satisfies undeniable property and it is secure against active attacks such as modification and denial of the multi-signature by signers. We also discuss practical applications such as joint copyright protection on digital contents.

I. 서 론

D.Chaum에 의해서 처음으로 제안된 부인봉쇄 서명 기법은 서명자의 동의 없이는 서명을 검증할 수 없는 기법으로 많은 응용 분야를 갖는다[3]. 일반 디지털 서명 기법으로 해결할 수 없었던 많은 사회적 영역에 적용될 수 있다. 기업 내의 기밀 전자 문서와 같은 경우에 서명된 문서가 복제에 의해서 경쟁 관계에 있는 기업으로 유출될 경우에 기업의 손익에 큰 영향을 미칠 수 있다. 특히 일반 서명 기법으로 서명된 경우에 그 특성상 모든 사용자가 서명의 타당성을 검증할 수 있으므로, 경쟁 기업에서 쉽게 해당 전자 문서의 서명을 검증할 수 있게 된다. 따라서 서명자의 동의 없이는 해당 문서의 서명을 검증할 수 없도록 하는 방법이 필요하게 되며, 원하는 수신자만 서

명 검증을 할 수 있도록 하는 특성을 갖는 부인봉쇄 서명 기법의 적용이 필수적이다.

본 논문에서는 여러 서명자의 서명이 필요한 다중 서명 기법에서 부인봉쇄 성질을 만족하는 부인봉쇄 다중서명 기법을 제안한다. 제안한 방법은 El-Gamal 서명식[2]을 변형하여 다중서명의 특성을 포함하고 D.Chaum이 제안한 부인봉쇄 성질[3]을 만족한다. 또한, 서명자들에 의한 다중서명 부인 및 다중서명 변조에 대해서 안전하다.

제안한 부인봉쇄 다중서명 기법은 많은 서명자와 지정된 수신자를 필요로 하는 응용에 있어서 적합하다. 온라인으로 판매되는 디지털 콘텐츠를 여러 저작자가 만든 경우에, 해당 콘텐츠에 대한 저작권을 저작자들이 함께 공유할 수 있어야 한다. 또한, 콘텐츠 판매에 있어서 모든 저작자들의 동의 하에서만 결제가 가능하도록 함으로써 해당 콘텐츠에 대한 공동의 권리를 실질적으로 보장할 수 있다. 공동 저작권과 관련된 분쟁이 발생했을 경우에 부인 프로토콜을 수행하여 공동저작권이 변조된 것인지 저작자들이 올바른 저작권에 대해서 부인하는 것인지 식별할 수 있는 특성을 갖는다.

2장에서 기존의 부인봉쇄 서명 기법과 El-Gamal 서명 기법에 대해서 살펴보고 3장에서 제안한 부인봉쇄 다중서명 기법에 대해서 설명한다. 4장에서 공동 저작권 보호를 위한 제안한 기법의 응용에 대해서 고찰하고 5장에서 결론 및 향후 연구 과제를 제시한다.

II. 관련 연구

2.1. El-Gamal 디지털 서명 기법[2]

El-Gamal 서명 기법은 $GF(p)$ 상에서의 이산 대수 문제의 어려움에 기반 한 서명 방식이다. 암호학적으로 안전한 유한체 $GF(p)$ 는 정의 1과 같고 g 는 $GF(p)$ 상에서 정의된 생성자(generator)이다.

[정의 1] 암호학적으로 안전한 유한체 $GF(p)$

p 는 큰 소수로 유한체 $GF(p)$ 상에서 법 p 에 대한 이산 대수를 구하는 것이 계산상 불가능할 때 $GF(p)$ 를 암호학적으로 안전한 유한체라 정의한다.

서명자의 비밀키 x , 공개키 y , 서명 대상 메시지 m 은 다음과 같다.

$x, m \in Z_{p-1},\ y \equiv g^x \pmod{p}$

(1) 서명 생성 프로토콜

단계 1 : 다음 조건을 만족하는 임의의 난수 k 를 선택한다.

$\gcd(k, p-1) = 1,\ k \in Z_{p-1}$

단계 2 : 서명자는 메시지 m 에 대한 서명 (r, s) 를 다음과 같이 계산한다.

$r \equiv g^k \pmod{p},$

$m \equiv x \cdot r + k \cdot s \pmod{p-1}$

단계 4 : 메시지와 서명 (m, r, s) 를 검증자에게 전송한다.

(2) 서명 검증 프로토콜

검증자는 서명 $(r,\ s)$ 를 다음과 같이 검증한다.

$g^m \equiv y^r \cdot r^s \equiv g^{x \cdot r + k \cdot s} \pmod{p}$

2.2. D.Chaum의 부인봉쇄 서명기법[3]

서명자는 정의 1로부터 암호학적으로 안전한 유한체 $GF(p)$ 와 군 G_q 를 선택한다. g 는 군 G_q 의 원소로 위수 q 를 갖는 생성자이다. 서명자의 비밀키 x 와 공개키 y 는 다음과 같다.

$x \in Z_q,,\ y \equiv g^x \pmod{p}$

(1) 서명 생성 프로토콜

단계 1 : 서명자는 메시지 m 에 대한 부인봉쇄 서명 z 을 생성한다.

$z \equiv m^x \pmod p,\ m \in G_q$

단계 2 : 메시지 m 과 서명 z 을 검증자에게 전송한다.

(2) 서명 확인 프로토콜

단계 1 : 검증자는 Z_q 상에서 임의의 두 난수 (a, b) 를 선택하고 다음과 같이 도전(challenge) w 를 생성한다. 검증자는 도전 w 를 서명자에게 전송한다.

$w \equiv z^a \cdot y^b \pmod p,\ (a, b) \in Z_q$

단계 2 : 서명자는 다음과 같이 응답(response) R 을 생성하여 검증자에게 전송한다.

$R \equiv w^{x^{-1}} \pmod p,\ x \cdot x^{-1} \equiv 1 \pmod q$

단계 3 : 검증자는 다음 식을 통해서 서명을 검증한다.

$R \equiv m^a \cdot g^b \pmod p$: z 는 올바른 서명

$R \neq m^a \cdot g^b \pmod p$: 서명 z 이 잘못됐거나, 서명자가 올바른 서명에 대해서 부인을 하는 경우

(3) 부인 프로토콜(disavowal protocol)

임의의 두 난수 (c, d) 를 이용한 두 번째 도전 w' 과 응답 R' 은 다음과 같다.

$w' \equiv z^c \cdot y^d \pmod p,\ R' \equiv w'^{x^{-1}} \pmod p$

검증자는 다음 판단식을 생성해서 서명자의 부정 여부를 검증한다.

· 서명 z 가 잘못됨

$(R \cdot g^{-b})^c \equiv (R' \cdot g^{-d})^a \pmod p$

· 서명자가 올바른 서명에 대해서 부인

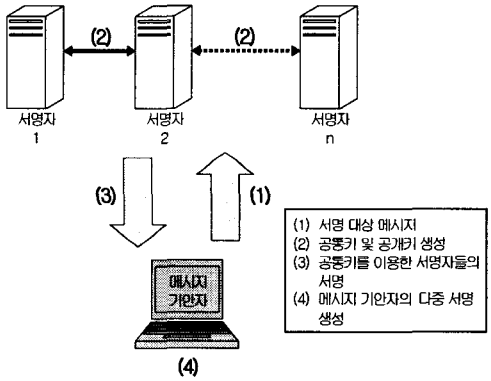
$(R \cdot g^{-b})^c \neq (R' \cdot g^{-d})^a \pmod p$

III. 제안한 부인봉쇄 다중서명 기법

부인봉쇄 다중서명 기법은 서명자들 모두의 동의 없이는 다중서명을 검증할 수 없는 기법이다. 제안한 다중서명 기법은 다중서명 생성, 다중서명 확인, 부인 프로토콜로 구성된다.

3.1. 다중서명 생성 프로토콜

그림 1은 제안한 다중서명 기법에서 다중서명을 생성하는 과정이다. 메시지 기안자는 서명 대상 메시지를 서명자들에게 전송한다. 서명자들은 다중서명에 필요한 공통키를 생성하고 메시지 m 에 대한 부인봉쇄 서명을 만들어 메시지 기안자에게 전송한다. 메시지 기안자는 각 서명자의 부안봉쇄 서명을 조합하여 부인봉쇄 다중서명을 생성한다.



▶▶ 그림 1. 부인봉쇄 다중서명 생성 단계

암호학적으로 안전한 유한체 $GF(p)$ 는 정의 1과 같고 g 는 법 p 에 대한 위수 $p-1$ 을 갖는 생성자이다. 서명자들의 수가 n 명일 때 각 서명자의 비밀키 및 공개키는 다음과 같다.

서명자 i의 비밀키 : $x_i \in Z_{p-1},\ 1 \le i \le n$

서명자 i의 공개키 : $y_i \equiv g^{x_i} \pmod p, 1 \le i \le n$

(1) 첫 번째 서명자의 공통키 생성

단계 1 : 메시지 기안자는 서명 대상 메시지 m 과 해쉬 파라미터 hpr 을 서명자들에게 전송한다. 메시지 m 에 대한 해쉬값 m_h 가 법 p 에 대한 원시근(primitive root)이 되도

록 hpr 을 설정한다.

$m_h = h(m, hpr)$

단계 2 : 첫번째 서명자는 Z_{p-1} 상에서 임의의 난수 k_1 을 선택하고 k_1 에 대한 공개값 r_1 을 생성한다.

$\gcd(k_1, p-1) = 1,\ r_1 \equiv m_h^{k_1} \pmod{p}$

단계 3 : 첫번째 서명자는 서명자들의 대표 공개키 Y 를 생성하기 위해서 Y_1 을 다음과 같이 설정한다.

$Y_1 = y_1$

단계 4 : 첫번째 서명자는 단계 2와 3에서 생성된 (r_1, Y_1) 을 두번째 서명자에게 전송한다.

(2) 서명자 i의 공통키 생성($2 \le i \le n$)

단계 1 : 서명자 i는 서명자 i-1로부터 (r_{i-1}, Y_{i-1}) 을 수신한다.

$r_{i-1} \equiv r_{i-2}^{k_{i-1}} \equiv m_h^{\prod_{j=1}^{i-1} k_j} \pmod{p}$

$Y_{i-1} \equiv Y_{i-2}^{x_{i-1}} \equiv g^{\prod_{j=1}^{i-1} x_j} \pmod{p}$

단계 2 : 서명자 i는 다음과 같이 임의의 난수 k_i 를 선택하고 k_i 에 대한 공개값 r_i 를 생성한다.

$\gcd(k_i, p-1) = 1,\ k_i \in Z_{p-1}$

$r_i \equiv r_{i-1}^{k_i} \equiv m_h^{\prod_{j=1}^{i} k_j} \pmod{p}$

단계 3 : 서명자 i는 자신의 비밀키 x_i 를 이용하여 다음과 같이 Y_i 를 생성한다.

$Y_i \equiv Y_{i-1}^{x_i} \equiv g^{\prod_{j=1}^{i} x_j} \pmod{p}$

단계 4 : 서명자 i는 서명자 i+1에게 (r_i, Y_i) 를 전송한다.

단계 5 : 서명자 i가 마지막 서명자일 때 까지 단계 1부터 단계 4를 반복한다. 마지막 서명자는 다음과 같이 서명자들의 공통키 R 과 대표 공개키 Y 를 구해서 모든 서명자들과 메시지 기안자에게 (R, Y) 를 전송한다.

$R \equiv r_{n-1}^{k_n} \equiv m_h^{\prod_{j=1}^{n} k_j} \pmod{p}$

$Y \equiv Y_{n-1}^{x_n} \equiv g^{\prod_{j=1}^{n} x_j} \pmod{p}$

(3) 다중서명 생성

단계 1 : 각 서명자는 공통키 R 을 이용하여 다음 식을 만족하는 s_i 를 구한다. k_i 와 $p-1$ 은 서로소이므로 s_i 에 대한 유일한 해가 존재한다.

$k_i \cdot s_i \equiv x_i \cdot R - k_i \cdot m_h \pmod{p-1}$

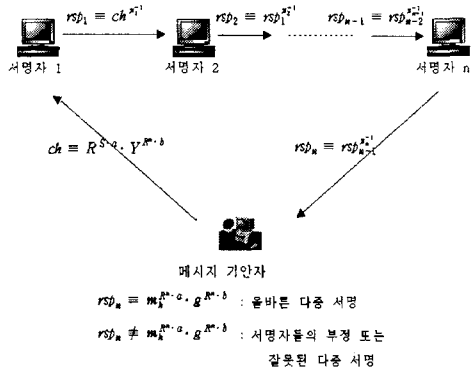
단계 2 : 각 서명자는 부인봉쇄 서명 s_i 를 메시지 기안자에게 전송한다.

단계 3 : 메시지 기안자는 각 서명자로부터 전송받은 s_i 를 조합하여 부인봉쇄 다중서명 S 를 다음과 같이 생성한다.

$S \equiv \prod_{j=1}^{n} (m_h + s_j) \pmod{p}$

3.2. 다중서명 확인 프로토콜

메시지 기안자는 (R, S) 가 메시지 m 에 대한 올바른 다중서명인지 확인하기 위해서 그림 2와 같은 다중서명 확인 프로토콜을 수행한다.



▶▶ **그림 2. 제안한 다중서명 확인 프로토콜**

(1) 메시지 기안자의 도전 생성

단계 1 : 메시지 기안자는 임의의 두 난수 (a, b) 를 선택하고 다음과 같이 도전 ch 를 생성하여 첫번째 서명자에게 ch 를 전송한다.

$$ch \equiv R^{S \cdot a} \cdot Y^{R^n \cdot b} \pmod{p}$$

$$\equiv m_h^{a \cdot R^n \cdot \prod_{j=1}^{n} x_j} \cdot g^{b \cdot R^n \cdot \prod_{j=1}^{n} x_j} \pmod{p}$$

단계 2 : 첫번째 서명자는 다음과 같이 응답 rsp_1 을 생성해서 두번째 서명자에게 전송한다. x_1^{-1} 는 법 $p-1$ 에 대한 x_1 의 모듈라 곱셈의 역이다.

$$rsp_1 \equiv ch^{x_1^{-1}} \pmod{p},$$

(2) 서명자 i의 응답 생성

단계1 : 서명자 i는 서명자 i-1로부터 응답 rsp_{i-1} 을 수신한다.

$$rsp_{i-1} \equiv rsp_{i-2}^{x_{i-1}^{-1}} \equiv ch^{\prod_{j=1}^{i-1} x_j^{-1}} \pmod{p}$$

단계 2 : 서명자 i는 x_i^{-1} 를 이용하여 다음과 같이 응답 rsp_i 를 생성한다.

$$rsp_i \equiv rsp_{i-1}^{x_i^{-1}} \pmod{p}$$

단계 3 : 서명자 i는 서명자 i+1에게 응답 rsp_i 를 전송한다.

단계 4 : 서명자 i가 마지막 서명자일 때 까지 단계 1부터 단계 3을 반복한다. 마지막 서명자는 도전 ch 에 대한 전체 서명자의 응답 rsp_n 을 메시지 기안자에게 전송한다.

(3) 메시지 기안자의 다중서명 검증

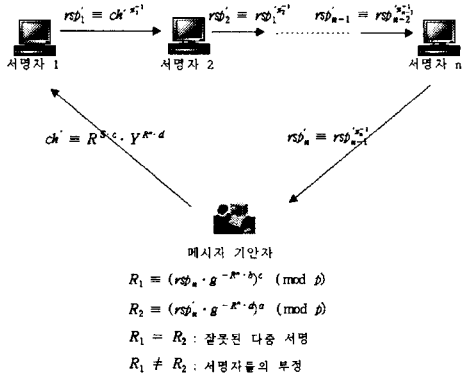
메시지 기안자는 다음과 같이 전체 서명자들의 응답을 검증한다.

$$rsp_n \equiv m_h^{R^n \cdot a} \cdot g^{R^n \cdot b} \pmod{p} \quad (3.1)$$

$$rsp_n \neq m_h^{R^n \cdot a} \cdot g^{R^n \cdot b} \pmod{p} \quad (3.2)$$

식 3.1이 성립하면 메시지 기안자는 (R, S) 가 메시지 m 에 대한 올바른 다중서명임을 확인한다. 식 3.2는 다중서명이 잘못된 경우와 서명자들 중 적어도 한 서명자 이상이 부정을 하는 경우이다. 메시지 기안자는 부인 프로토콜을 이용해서 다중서명이 잘못된 것인지 서명자들이 부정하는 것인지 확인한다.

3.3. 부인 프로토콜



▶▶ **그림 3. 제안한 부인 프로토콜**

메시지 기안자는 3.2 절의 다중서명 확인 프로토콜에서 응답 rsp_n 에 대한 인증에 실패할 경우에 그림

3의 부인 프로토콜을 통해서 서명자들이 부정하는 것인지 다중서명이 잘못된 것인지 확인한다.

메시지 기안자가 임의의 난수 (c, d) 를 선택하여 생성한 두 번째 도전 ch' 과 이에 대한 전체 서명자들의 두 번째 응답 rsp_n'은 다음과 같다.

$$a \cdot d \not\equiv b \cdot c \pmod{p-1}, \quad c, d \in Z_{p-1}$$

$$ch' \equiv R^{S \cdot c} \cdot Y^{R^n \cdot d} \pmod{p}$$

$$rsp_n' \equiv rsp_{n-1}'^{x_n^{-1}} \pmod{p}$$

단계 1 : 메시지 기안자는 다음과 같이 전체 서명자들의 응답을 검증한다.

$$rsp_n' \equiv m_h^{R^n \cdot c} \cdot g^{R^n \cdot d} \pmod{p}$$

$$rsp_n' \neq m_h^{R^n \cdot c} \cdot g^{R^n \cdot d} \pmod{p}$$

단계 2 : 단계 1에서 다중서명 검증에 실패할 경우에 메시지 기안자는 rsp_n 과 rsp_n'을 이용해서 다음 판별식을 만든다.

$$R_1 \equiv (rsp_n \cdot g^{-R^n \cdot b})^c \pmod{p}$$

$$R_2 \equiv (rsp_n' \cdot g^{-R^n \cdot d})^a \pmod{p}$$

단계 3 : R_1 과 R_2 를 비교함으로써 서명자들의 부정인지 다중 서명이 잘못된 것인지 확인한다.

· 다중서명이 잘못됨

$R_1 = R_2$

· 서명자들이 올바른 다중 서명에 대해서 부인

$R_1 \neq R_2$

IV. 부인봉쇄 다중서명 기법을 적용한 공동저작권 보호

디지털 콘텐츠는 많은 저작자들의 창의성과 노력으로 만들어진다. 하지만, 디지털 데이터는 그 특성 상 원본과 복사본의 구분이 불가능하기 때문에 디지털 콘텐츠 파일의 무단 복사 및 도용은 많은 저작자들의 저작 의욕을 저하시킬 뿐만 아니라 디지털 콘텐츠 사업에 심각한 위협을 초래하게 한다. 따라서 디지털 콘텐츠에 대한 불법 복제를 방지하기 위해서 저작권 정보를 생성하고 이를 디지털 콘텐츠 파일에 워터마킹하는 정보보호 기법의 적용은 필수적이다.

디지털 콘텐츠 저작은 개별적으로도 이루어질 수 있지만 대부분 여러 사람의 공동 노력으로 진행된다. 공동 저작물인 경우에 해당 디지털 콘텐츠에 대한 저작권을 저작자들이 함께 공유하여 권리를 똑같이 행사할 수 있도록 해 주는 공동 저작권 생성 및 보호 기법이 필요하다.

제안한 부인봉쇄 다중서명 기법을 적용하여 디지털 콘텐츠에 대한 공동 저작권을 생성하고 보호할 수 있는 방안에 대해서 살펴본다.

공동저작권은 3.1 절의 다중서명 생성 프로토콜을 이용하여 생성된다. 각 저작자는 디지털 콘텐츠에 대한 부인봉쇄 서명을 생성하고 저작권 제작자(copyright maker)에게 이를 전송한다. 저작권 제작자는 각 저작자의 부인봉쇄 서명을 조합하여 부인봉쇄 다중서명을 생성하고 이를 디지털 콘텐츠 파일에 워터마킹한다.

부인봉쇄 다중서명이 삽입된 디지털 콘텐츠를 온라인 상에서 판매할 경우에, 구매자는 3.2 절의 다중서명 확인 프로토콜을 수행하여 디지털 콘텐츠 구매를 시도하게 된다. 부인봉쇄 다중서명의 특성상 모든 저작자의 동의 없이는 해당 디지털 콘텐츠의 저작권 정보를 확인할 수 없고, 저작권 정보가 확인되지 않은 디지털 콘텐츠는 판매할 수 없도록 함으로써, 저작자들의 공동의 권리를 보장한다. 또한, 공동 저작권과 관련된 분쟁이 발생하였을 경우에, 3.3절의 부인 프로토콜을 수행하여 삽입된 저작권 정보가 잘못된 것인지 아니면 저작자 중의 누군가가 올바른 저작권에 대해서 부인하는 것인지 밝혀낼 수 있다. 따라서 저작자들은 올바르게 삽입된 공동 저작권에 대해서 부인할 수 없다.

V. 결 론

본 논문에서는 디지털 콘텐츠 공동 저작권 보호에 사용될 수 있는 부인봉쇄 다중서명 기법을 제안하였다. El-Gamal 서명식을 변형하고 이를 확장하여 D.Chaum이 제안한 부인봉쇄 성질과 다중서명의 특성을 만족한다. 제안한 기법은 일반 다중서명 기법으로는 적용될 수 없는 많은 서명자와 지정된 수신자를 요구하는 응용에 적합하다. 여러 저작자의 공동 노력으로 생성된 디지털 콘텐츠에 대한 공동 저작권 생성 및 보호를 위해서 제안한 다중서명 기법을 적용함으로써, 저작자들이 디지털 콘텐츠에 대한 공동의 권리를 보장받을 수 있다.

▌참고문헌▌

[1] W.Diffie, M.E.Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, Vol. IT-22, No. 6, pp.644-654, 1976.

[2] T.Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, Vol. IT-31, No. 4, pp.469-472, 1985.

[3] D.Chaum, "Undeniable Signatures," Advances in Cryptology, Proceedings of CRYPTO'89, Springer-Verlag, pp.212-216, 1990.

[4] F.Piper, "Digital Signatures," IFIP/SEC'91 Conference, Proceedings of the 7th International Conference and Exhibition on Information Security, pp.62-71, 1991.

[5] S.G.Akl, "Digital Signatures: A Tutorial Survey," IEEE Computer, pp.15-24, 1983.

[6] L.Harn, "(t,n) Threshold Signature and Digital Multisignature," Workshop on Cryptography & Data Security, pp.61-73, 1993.

[7] S.H.Yun, T.Y.Kim. "A Digital Multisignature Scheme Suitable for EDI Message," Proceedings of 11th International Conference on Information Networking, pp.9B3.1-9B3.6., 1997.

[8] S.H.Yun, T.Y.Kim, "Convertible Undeniable Signature Scheme," Proceedings of IEEE High Performance Computing ASIA'97, pp.700-703, 1997.

[9] S.H.Yun, S.J.Lee, "An electronic voting scheme based on undeniable blind signature scheme," Proceedings of IEEE 37th carnahan conference on Security Technology, pp.163-167, 2003.