nurit

가볍고 가장 빠른 암호화 알고리즘을 위한

BaroCRYPT 솔루션 소개서

2024. 1.

Content

nurit

Ⅰ. 보안의 필요성

주요 법령

법령명	관련 주요 조항	주요 내용
정보통신망 이용촉진 및 정보보호 등 에 관한 법률	제24조(개인정보의 이용제한)	본래의 개인정보 수집목적과 다르게 이용 금지
	제 28조(개인정보의 보호조치)	① 개인정보를 안전하게 저장 · 전송할 수 있는 암호화 기술 등을 이용한 보안조치
	제28조(개인정보의 누설금지)	②개인정보취급자의 개인정보 훼손 · 침해 또는 누설 금지를 규정
신용정보의 이용 및 보호에 관한 법률	제19조 (신용정보전산시스템의 안전보호)	신용정보업자 등은 신용정보 전산시스템(공동전산망을 포함한다)에 대한 제삼자의 불법접근 또는 입력된 정보의 변경 · 훼손 · 파괴 기타 위험에 대한 기술적 · 물리적 · 관리적 보안대책을 수립하여야 한다
공공기관의 개인정보보호에 관한 법률	제9조 (개인정보의 안전성확보 등)	① 공공기관의 장은 개인정보를 처리함에 있어서 개인 정보가 분실 · 도난 · 누출 · 변조 또는 훼손되지 아니하도록 안전성확보에 필요한 조치를 강구하여야 한다.

정보통신망법의 개인정보보호관련 벌칙규정

법령명	관련 주요 조항	주요 내용	조치사항
정보통신망법의 개인정보보호관련 벌칙규정	행정 형벌 (제71조)	동의받은 목적과 다른 목적으로 개인정보 이용(제24조)	5년 이하 징역 또는 5천만원 이하 벌금
		이용자 동의없는 개인정보 제3자제공(제24조의 2제1항)	
		개인정보 취급자의 개인정보 훼손 · 침해 · 누설(제28조의2)	
		타인정보 훼손, 타인비밀 침해 · 도용 · 누설(제49조)	
	과태료 (제76조)	기술적 · 관리적 조치 미이행(제28조제1항) - 접속기술 위 · 변조 방지조치 - 암호화 기술 등을 이용한 보안 조치	3천만원 이하 과태료
	과징금의 부과 제64조의3	기술적 · 관리적 조치 미이행(제28조제1항2~5) - 개인정보에 대한 불법적 접근차단을 위한 접근 통제장치 설치 · 운영 - 개인정보를 안전하게 저장 · 전송할 수 있는 암호화 기술 등을 이용한 보안조치	매출액의 백분의 1이하 금액 과징금

II. 개인정보 암호화 대상 항목

개인정보를 보호하기 위한 필수 암호화 대상이 되는 항목은 다음과 같습니다.

항목		실명가공	암호화	설명
주민등록번호		O	O	주민, 법인번호
사업자등록번호		O	X	사업자등록번호
성명		O	O	고객명, 법인명 등 이름
전화번호		O	O	전화번호, 핸드폰번호
이메일		O	X	이메일
주소	주소	O	X	-암호화는 주소와 상세주소가 가) 분리되어 있으면 상세 주소만 대상임. 나) 분리되어 있지 않으면 전체 주소가 대상임. -실명 가공은 전체 주소가 대상임.
	상세주소		O	
여권번호		O	O	여권번호
비밀번호		X	O	비밀번호

Ⅲ. 주요 손해 배상 사례

국내 개인정보 관련 주요 손해 배상 사례

▶ **[GS 칼텍스]** (내부자유출) 자회사직원이고객정보DB 외부유출(08. 7)-1,100만명
⇒ 소송건수23건, 4만985명참가-소송가액: 4백억8천만원

▶ **[Auction]** 온라인쇼핑몰 해킹피해로 1,081만명 개인정보유출('08년3월]
⇒ 소송건수24건, 총14만455명참가-소송가액: 1천570억원, 서울지방법원소송제기(08.10월)

▶ **[국민은행]:** 고객 3천여명의 개인정보 유출사건
⇒ 손해배상 소송 제기한 1,024명-> 배상금지급판결(07년), 이름/이메일/주민번호: 20만원

▶ **[SK텔레콤]** 블로그 서비스 토씨(tossi) 이용자 중 이름, 휴대전화번호, 블로그 주소등 2500명의 개인정보 유출('07. 9월) ⇒ 피해자에게 7만원의 상품권 지급 : 총 1억7천5백만원 소모

▶ **[LG전자]** 입사 지원자 정보 유출('06) ⇒ 1인당 70만원 배상 판결

• **기업에서의 개인정보보호란 유·무형의 기업 자산 보호와 직결**

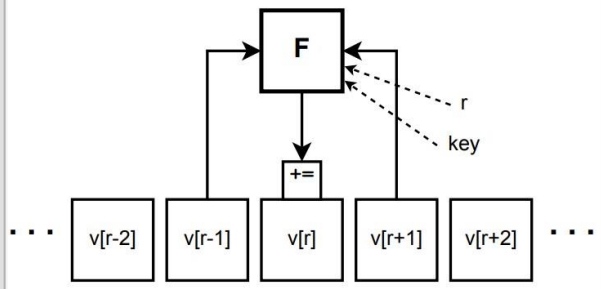
• **실제로 개인정보는 마케팅을 위한 기업의 소중한 자산이며, 제대로 관리되지 못한 경우 고객의 신뢰성 저하로 인한 기업의 이미지가 크게 훼손**

• **최근 기업의 개인정보 유출 사건에 대해 유출 피해자들의 대규모 소송이 제기되고 실제로 대부분의 소송들이 피해배상 판결이 나고 있으므로 개인정보보호는 기업의 경영 수익과도 직결**

Ⅳ. 솔루션 개요

BaroCRYPT 솔루션은 Feistel 암호를 사용하여 크기가 작고 구현이 쉬운 블록 암호화 알고리즘인 XXTEA (Extended Extended Tiny Encryption Algorithm)를 기반으로 하는 가볍고 가장 빠른 암호화 알고리즘입니다.

General



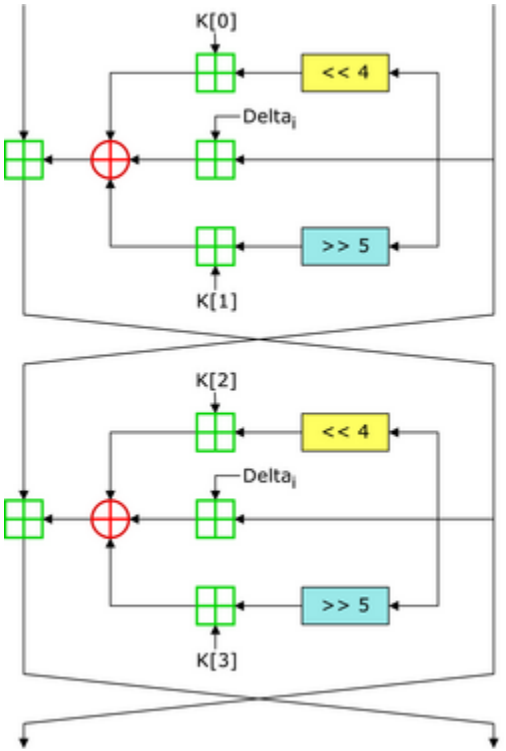
- ✓ Designers – Roger Needham
  David Wheeler .
- ✓ First published – 1994
- ✓ Successors – XXTEA
- ✓ Key sizes – 128 bits
- ✓ Block sizes – 64 bits
- ✓ Structure – Feistel network
- ✓ Rounds – variable; recommended
  64 Feistel rounds
  (32 cycles)

Best public cryptanalysis

```
void xxtea_full_cycle(uint32_t *v, int n, uint32_t *key, int cycle)
{
    uint32_t sum, z, y, e;
    int r;
    sum = cycle*0x9e3779b9;
    e = sum>>2;
    for(r=0; r<n; r++)
    {
        z = v[(r+n-1)%n]; // the left neighboring word
        y = v[(r+1)%n];   // the right neighboring word
        v[r] += ((z>>5^y<<2)+(y>>3^z<<4))^((sum^y)+(key[(r^e)%4]^z));
    }
}
void xxtea(uint32_t *v, unsigned int n, uint32_t *k)
{
    int i, cycles = 6+52/n;
    for(i=1; i<=cycles; i++)
        xxtea_full_cycle(v, n, k, i);
}
```

- ✓ TEA는 동등한 키 (Kelsey et al., 1996)를 겨고 223 개의 선택된 평문과 232의 시간 복잡성을 요구하는 관련 키 공격을 사용하여 손상 될 수 있음.
- ✓ 표준 단일 비밀 키 설정에서 TEA의 최상의 구조적 암호 해독은 전체 Code book 보다 적은 2121.5 시간에 21 라운드를 돌파하는 무결성 암호 해독임.

Two Feistel rounds(one cycle) of TEA



nurit

Ⅴ. 솔루션 특/장점

BaroCRYPT 솔루션은 XXTEA(일명 Corrected Block TEA) 암호화 알고리즘을 기반으로 사용 가능한 RAM의 양이 최소인 레거시 하드웨어 시스템(임베디드)과 같이 극한의 제약이 있는 상황에서도 빠르게 데이터 암복호화를 실행 가능한 최적의 솔루션입니다.

- 작고 구현이 쉬운 블록 암호화 알고리즘으로 페이스텔 암호를 기반으로 하여 크기가 작고 빠르면서 구현이 쉬움
- 64 bit(8byte)를 암호화하는 블록 암호화 알고리즘으로 128 bit(16byte) 키를 사용
- 페이스텔 암호를 기반으로 한 작은 크기의 알고리즘으로 그 크기에 비해서 암호화 강도가 높음
- Corrected Block TEA(XXTEA)는 원래 Block TEA의 약점을 수정하기 위해 고안된 블록 암호화 알고리즘
- 알고리즘의 크기는 작지만 현존하는 가장 빠르고 안전한 알고리즘
- Corrected Block TEA(XXTEA)는 원래 Block TEA의 약점을 수정하기 위해 고안된 블록 암호화 알고리즘
- 다른 블록 암호화 알고리즘에 비해 구현이 용이하고 하드웨어 사양 제약 조건이 큰 환경에 적용이 용이하며 자유롭게 사용
- SQL 문장에서 쉽게 사용할 수 있도록 TO_ENCRYPT(암호화), TO_DECRYPT(복호화) 함수 제공

※ Feistel 암호란?

동일한 대치와 치환을 반복하면서 암호문이 평문으로 부터 암호화되는 반복 블록 암호.
데이터 암호화 표준(DES)과 유사한 암호로서, 평문을 반씩 2개 블록으로 나누어 한쪽은 서브 키를 사용한 기능 F로 치환하고 그 결과를 다른 반쪽에서 배타적 논리합(XOR)한 다음 서로 교환한다. 이러한 과정을 각 치환마다 동일한 패턴으로 하되 마지막 치환에서는 서로 교환하지 않는다. 암호화 시 사용된 서브키는 복호화 시 역으로 사용된다.

1. BaroSolution 제품군

구 분	설 명	비고
BaroPAM	정보자산의 다양한 운영체제 및 애플리케이션에서 2차 인증으로 일회용 인증키를 접목시켜 중앙 집중적 인증 메커니즘을 지원하는 단순하면서도 강력한 정보자산의 접근제어 인증 솔루션.	
BaroCARD	생체정보인 지문정보를 적용한 최적의 본인인증 솔루션으로 생체정보인 지문정보를 플라스틱 카드에 등록한 후 등록된 지문정보를 인식하면 일회용 인증키를 생성하는 카드(지문인식 기능과 인증카드를 내장한 신개념 카드) 로 지문인식 인증카드 솔루션.	
BaroCRYPT	Feistel 암호를 사용하여 크기가 작고 구현이 쉬운 블록 암호화 알고리즘인 XXTEA (Extended Extended Tiny Encryption Algorithm)를 기반으로 하는 가볍고 가장 빠른 암호화 알고리즘을 적용한 솔루션.	
BaroCollector	다양한 Source에서 발생된 많은 양의 로그 데이터(Big Data)를 중앙의 데이터 저장소로 효율적으로 수집해 주는 분산처리, 신뢰성, 가용성을 갖춘 실시간 로그 수집기.	
BaroFDS	이상금융거래탐지 및 대응업무에 대한 모 금융기관의 2년간의 Know-how을 바탕으로 개발된 금융권 유일의 검증된 FDS 솔루션으로서 복잡한 금융권 환경에서 쉽고 빠르게 적용하여, 구축 즉시 효과를 발휘할 수 있음.	
BaroIDS	정보자산(서버, 네트워크장비, 보안장비, 저장장치, 데이터베이스, 애플리케이션, 기타)의 이상접속 탐지 및 차단에 대한 현장의 Know-how을 바탕으로 FDS(Fraud Detection System)를 적용하여 개발된 솔루션.	

감사합니다!

www.nurit.co.kr

서울시 강서구 마곡중앙2로 15, 913호(마곡동, 마곡테크노타워2)
주식회사 누리아이티 대표전화 : 010-2771-4076