On security aspects of CRISP

Vitaly Kiryukhin

LLC «SFB Lab», JSC «InfoTeCS»

CTCrypt 2023

June 7, 2023

vitaly.kiryukhin@sfblaboratory.ru

CRISP – CRyptographic Industrial Security Protocol

R 1323565.1.029-2019

Information technology – Cryptographic data security

Secure exchange protocol for industrial systems

ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.029—2019

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Протокол защищенного обмена для индустриальных систем

CRISP – CRyptographic Industrial Security Protocol

Security properties

1. confidentiality [optional]
2. integrity
3. replay protection

CRISP – CRyptographic Industrial Security Protocol

Security properties

1. confidentiality [optional]
2. integrity
3. replay protection

Features

- Non-Interactivity – pre-shared keys, NO sessions, NO key exchange

CRISP – CRyptographic Industrial Security Protocol

Security properties

1. confidentiality [optional]
2. integrity
3. replay protection

Features

- Non-Interactivity – pre-shared keys, NO sessions, NO key exchange
- Multicasting – all users can share the same key

CRISP – CRyptographic Industrial Security Protocol

Security properties

1. confidentiality [optional]
2. integrity
3. replay protection

Features

- Non-Interactivity – pre-shared keys, NO sessions, NO key exchange
- Multicasting – all users can share the same key
- Dynamic selection of a cipher suite (CS)

  (for each message, the sender can choose any CS with "confidentiality and integrity" or "only integrity")

1. Description of CRISP

Packet fields

	Name	Length in bits	
1	ExternalKeyIdFlag	1	Header H
2	Version	15	
3	CS	8	
4	KeyId	from 8 to 1024	
5	SeqNum (SN)	48	
6	PayloadData	variable	
7	ICV (tag)	variable	

Max length $\leq$ 2048 bytes

General information

- Each sender has its own unique identifier `SourceIdentifier` (S_{ID}).
- The receiver determines K_{ID} from `ExternalKeyIdFlag`, `KeyId`, and possibly by some external data, $K_{ID} \rightarrow (K, S_{ID})$

General information

- Each sender has its own unique identifier `SourceIdentifier` (S_{ID}).
- The receiver determines K_{ID} from `ExternalKeyIdFlag`, `KeyId`, and possibly by some external data, $K_{ID} \to (K, S_{ID})$
- Before using K, the sender sets the initial value of $SN \in [0, 2^{48} - 1]$
- For each K_{ID} the receiver initializes the window $(\underline{SN}, \overline{SN})$
- The window size is constant $1 \leq Size \leq 256$, $(\overline{SN} - \underline{SN}) \leq Size$

Sender's algorithm

1. master key K, plaintext P, cipher suite CS are selected
2. sequence number SN is increased by 1
3. derived keys K_{MAC} and (possibly) K_{ENC} are computed

$$(K_{ENC}, K_{MAC}) = \text{KDF}(K, prms), \ \ prms \text{ include } CS, S_{ID}, etc$$

4. header H is generated, including K_{ID}, SN and CS
5. If CS provides encryption,
   - then $C = \text{Enc}(K_{ENC}, IV, P)$, $IV = \text{DerIv}(SN)$
   - otherwise, $C = P$
6. tag $T = \text{Mac}(K_{MAC}, H||C)$ is computed
7. message (H, C, T) is sent

Receiver's algorithm

Similar to the sender's algorithm.

The main differences provides protection against replay attacks.

- SN is checked:
  - if $SN < \underline{SN}$, then reject
  - if SN-th bit of W is equal to one, then reject
- If tag is correct, then the window W is updated:
  - if $\overline{SN} < SN$, then $\overline{SN} = SN$ and $\underline{SN} = \min(SN - Size + 1, 0)$
  - the SN-th bit of W is set to one

Cipher suite

CS – tuple of four algorithms

$$\mathrm{CS} = (\mathrm{KDF}, \mathrm{DerIvKDF}, \mathrm{AE}, \mathrm{DerIv})$$

- KDF – key derivation function
- DerIvKDF determines dependence between SN and the input of KDF
- AE:
  - composition of Enc and Mac
  - only one algorithm Mac
  - dedicated authenticated encryption mode
- DerIv determines dependence between SN and a nonce for AE

2. General security analysis

Main idea

The non-interactivity and the declared security properties of CRISP motivate as to consider the protocol as a kind of complex **stateful deterministic authenticated encryption cipher mode** (AEAD).

Provable security

- no idealizations (like assumptions in the Dolev-Yao model) – only **reductions** to the basic problem
- qualitative and **quantitative** estimates

Nonce-based Authenticated Encryption

Definition

The deterministic nonce-based authenticated encryption

is the pair of the algorithms

$$\begin{aligned} \mathrm{AE} :& \boldsymbol{K} \times \boldsymbol{N} \times \boldsymbol{A} \times \boldsymbol{P} && \to \boldsymbol{C} \times \boldsymbol{T}, \\ \mathrm{AE}^{-1} :& \boldsymbol{K} \times \boldsymbol{N} \times \boldsymbol{A} \times \boldsymbol{C} \times \boldsymbol{T} && \to \boldsymbol{P} \cup \{\perp\}, \end{aligned}$$

where $\boldsymbol{K}$, $\boldsymbol{N}$, $\boldsymbol{A}$, $\boldsymbol{P}$, $\boldsymbol{C}$, $\boldsymbol{T}$ are sets of keys, nonces, associated data, plaintexts, ciphertexts, tags, respectively.

If $N \in \boldsymbol{N}$ is uniquely determined by $A \in \boldsymbol{A}$, then the set $\boldsymbol{N}$ is *implicit*.

AE can be defined on some *subset* of $\boldsymbol{A} \times \boldsymbol{P}$, not on the whole $\boldsymbol{A} \times \boldsymbol{P}$.

Security model for Nonce-based AE

Integrity and privacy in one model

Definition

The advantage of $\mathcal{A}$ in the model *NAE* for AE is

$$\mathrm{Adv}_{\mathsf{AE}}^{NAE}(\mathcal{A}) = \Pr\left(K \xleftarrow{\mathrm{R}} \boldsymbol{K} : \mathcal{A}^{\mathsf{AE}_K(\cdot,\cdot,\cdot),\mathsf{AE}_K^{-1}(\cdot,\cdot,\cdot,\cdot)} \Rightarrow 1\right) -$$
$$- \Pr\left(\mathcal{A}^{\$(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot,\cdot)} \Rightarrow 1\right)$$

The oracle \$ returns a random binary string.

The oracle $\perp$ returns error symbol "$\perp$".

The queries to the left oracle (AE or \$) does not contain the same N.

$\mathcal{A}$ does not resend to the right oracle (AE^{-1} or $\perp$) the answers of the left.

$\mathcal{A}$ makes q (resp. v) queries to the left (resp. right) oracle.

CRISP as nonce-based AE

Scenario

Many senders and one receiver have a single pre-shared key

CRISP as nonce-based AE

Scenario

Many senders and one receiver have a single pre-shared key

Sets

- Nonce is (S_{ID}, SN), $\boldsymbol{N}$ is implicit
- $\boldsymbol{K} = V^k$ (all master keys)
- $\boldsymbol{T} = V^{\leq \tau_{\max}}$ (all possible values of `ICV`)
- $\boldsymbol{P} = \boldsymbol{C} = V^{\leq L_P}$ (`PayloadData`)
- $\boldsymbol{A} \subseteq \boldsymbol{A}_{\mathrm{ext}} \times \boldsymbol{H} \times \boldsymbol{P}$, where $\boldsymbol{H} \subset V^{\leq L_H}$ (all possible header values)

CRISP as nonce-based AE

Scenario

Many senders and one receiver have a single pre-shared key

Sets

- Nonce is (S_{ID}, SN), $\boldsymbol{N}$ is implicit
- $\boldsymbol{K} = V^k$ (all master keys)
- $\boldsymbol{T} = V^{\leq \tau_{\max}}$ (all possible values of `ICV`)
- $\boldsymbol{P} = \boldsymbol{C} = V^{\leq L_P}$ (`PayloadData`)
- $\boldsymbol{A} \subseteq \boldsymbol{A}_{\mathrm{ext}} \times \boldsymbol{H} \times \boldsymbol{P}$, where $\boldsymbol{H} \subset V^{\leq L_H}$ (all possible header values)

Notes

"only integrity" – input is $((A_{\mathrm{ext}}, H, P), \emptyset)$

"confidentiality and integrity" – input is $((A_{\mathrm{ext}}, H, \emptyset), P)$

(`KeyId`, `ExternalKeyIdFlag`, A_{ext}) *injectivly* corresponds to (K, S_{ID})

Requirements for CS

- All CS that are used with the same K must use the same KDF
- KDF must be a secure variable-output *PRF (VO-PRF)*
- The input of KDF must include (at least) S_{ID} and CS
- Enc-then-Mac or dedicated AE must be *NAE*-secure
- "only Mac" must be *NAE*-secure

  (*PRF*-security is sufficient, nonce-based schemes are also suitable)
- changing SN must change the input of KDF or/and nonce

Theorem (*NAE*-security of CRISP)

The advantage of the adversary in the *NAE* model attacking the CRISP that uses the cipher suites from the set $\mathsf{CS} = \{\mathsf{CS}_1, \dots, \mathsf{CS}_c\}$,

$$\mathsf{CS}_i = (\mathsf{KDF}, \mathsf{AE}_i, \mathsf{DerIvKDF}, \mathsf{DerIv}_i), \ \ i = 1, \dots, c, \quad \text{is bounded by}$$

$$\mathrm{Adv}^{NAE}_{\mathsf{CRISP}}(t, q, \nu) \leq \mathrm{Adv}^{VO-PRF}_{\mathsf{KDF}}(t', \kappa) + \sum_{j=1}^{\kappa} \mathrm{Adv}^{NAE}_{\mathsf{AE}^{(j)}}(t', q^{(j)}, \nu^{(j)}),$$

$$\text{where } \kappa \leq q + \nu, \quad \sum_{j=1}^{\kappa} q^{(j)} = q, \quad \sum_{j=1}^{\kappa} \nu^{(j)} = \nu, \quad \mathsf{AE}^{(j)} \in \{\mathsf{AE}_1, \dots, \mathsf{AE}_c\}.$$

Provided that:

1) the input of KDF contains S_{ID}, CS, DerIvKDF(SN);

2) for any $SN \neq SN'$: DerIvKDF(SN) $\neq$ DerIvKDF(SN') or/and $\mathsf{DerIv}_i(SN) \neq \mathsf{DerIv}_i(SN')$, $i = 1, \dots, c$.

Security with leakage of keys

VO-PRF-security of KDF

$\Rightarrow$ some security properties are preserved even if

some keys become known to an attacker.

leakage	consequence
one enc. key K_{ENC}	confidentiality of q' messages is violated
one auth. key K_{MAC}	up to q' forgery against each receiver
any number of derived keys	other derived keys and the master key remain secret
master key K	loss of all security

3. Existing cipher suites

Existing cipher suites

CS	Name	Integrity	Confidentiality	Tag (bit)
1	MAGMA-CTR-CMAC	+	+	32
2	MAGMA-NULL-CMAC	+	–	32
3	MAGMA-CTR-CMAC8	+	+	64
4	MAGMA-NULL-CMAC8	+	–	64

- only the block cipher "Magma" [GOST R 34.12-2015]
- the same CMAC-based KDF for all CS
- confidentiality – CTR [GOST R 34.13-2015]
- integrity – CMAC [GOST R 34.13-2015]

Existing cipher suites: KDF

KDF is based on d different calls of CMAC

$$\begin{aligned} \mathrm{KDF}(K, X, d) = &\mathrm{CMAC}(K, 1 \mid\mid X \mid\mid n \cdot d) \mid\mid \\ &\ldots \\ &\mathrm{CMAC}(K, d \mid\mid X \mid\mid n \cdot d) \end{aligned}$$

The derived keys are computed as

$$K_{MAC} || K_{ENC} = \mathrm{KDF}(K, ..., 8) \text{ with } CS \in \{1, 3\}$$
$$K_{MAC} = \mathrm{KDF}(K, ..., 4) \text{ with } CS \in \{2, 4\}$$

The input data X for KDF contains: CS, S_{ID}, $\mathrm{msb}_{35}(SN)$

One derived key (key pair) for $2^{48-35} = 2^{13}$ packets

CTR

Corollary (PRP-PRF Switching Lemma)

The advantage of the adversary in the *IND-CPNA* model attacking the cryptoalgorithm CTR is bounded by

$$\mathrm{Adv}^{\mathit{IND\text{-}CPNA}}_{\mathsf{CTR[E]}}(t, q, l) \leq \mathrm{Adv}^{\mathit{PRP}}_{\mathsf{E}}(t', q \cdot l) + \frac{(q \cdot l)^2}{2^{n+1}}$$

[Rog11] Rogaway P.
Evaluation of Some Blockcipher Modes of Operation – 2011

CMAC

Theorem [CJN22]

The advantage of the adversary in the *PRF* model attacking the cryptoalgorithm CMAC is bounded by

$$\mathrm{Adv}^{PRF}_{\mathsf{CMAC[E]}}(t, q, l) \leq \mathrm{Adv}^{PRP}_{\mathsf{E}}(t', q \cdot l + 1) + \frac{16 \cdot q^2 + q \cdot l^2 + 4 \cdot q \cdot l}{2^n} + \epsilon(q, l),$$

where $t' \approx t$, $q \cdot (l + 1) \leq 2^{n-1}$, $\epsilon(q, l) \approx 0$.

Corollary

$$\mathrm{Adv}^{PRF}_{\mathsf{CMAC[E]}}(t, q, l) \lessapprox \frac{16 \cdot q^2}{2^n}$$

[CJN22] Chattopadhyay S., Jha A., Nandi M.
Towards Tight Security Bounds for OMAC, XCBC and TMAC – 2022

CTR-CMAC

Lemma

The advantage of the adversary in the *NAE* model attacking

$$\text{CTR-CMAC} : \boldsymbol{K} \times \boldsymbol{A} \times \boldsymbol{P} \to \boldsymbol{C} \times \boldsymbol{T},$$

$$\text{CTR-CMAC} : (V^k \times V^k) \times V^{\leq l \cdot n} \times V^{\leq l \cdot n} \to V^{\leq l \cdot n} \times V^{\tau}, \text{ is bounded by}$$

$$\mathrm{Adv}^{NAE}_{\text{CTR-CMAC}}(t, q, \nu) \leq \mathrm{Adv}^{PRF}_{\text{CMAC[E]}}(t', q+\nu, l) + \mathrm{Adv}^{IND-CPNA}_{\text{CTR[E]}}(t', q, l) + \frac{\nu}{2^{\tau}},$$

$t' \approx t$. The query to the left oracle is (A, P) and $A = H$.

NULL-CMAC

Lemma

The advantage of the adversary in the *NAE* model attacking

$$\text{NULL-CMAC} : \boldsymbol{K} \times \boldsymbol{A} \times \boldsymbol{P} \to \boldsymbol{C} \times \boldsymbol{T},$$

$$\text{NULL-CMAC} : V^k \times V^{\leq l \cdot n} \times \emptyset \to \emptyset \times V^\tau, \text{ is bounded by}$$

$$\mathrm{Adv}^{NAE}_{\text{NULL-CMAC}}(t, q, \nu) \leq \mathrm{Adv}^{PRF}_{\text{CMAC[E]}}(t', q + \nu, l) + \frac{\nu}{2^\tau}, \ t' \approx t.$$

The query to the left oracle is $(A, \emptyset)$, $A = H||P$.

KDF-CMAC

Lemma

The advantage of the adversary in the *VO-PRF* model attacking KDF is bounded by

$$\mathrm{Adv}^{\mathit{VO\text{-}PRF}}_{\mathsf{KDF[CMAC[E]]}}(t,\kappa) \leq \mathrm{Adv}^{\mathit{PRF}}_{\mathsf{CMAC[E]}}(t',\kappa \cdot d, l_{KDF} = 7),\ \ t' \approx t,$$

κ is the number of the derived keys (key pairs).

Corollary

$$\mathrm{Adv}^{\mathit{VO\text{-}PRF}}_{\mathsf{KDF[CMAC[E]]}}(t,\kappa) \lessapprox \frac{16 \cdot (\kappa \cdot d)^2}{2^n},\ \ d \in \{4, 8\}.$$

PRP-security of Magma

All the presented reductions use the single basic problem:

the indistinguishability of "Magma" from a random permutation

$$\mathrm{Adv}^{PRP}_{\mathsf{Magma}}(t,q) = \max_{\text{all } \mathcal{A} \text{ with resources}(t,q)} \mathrm{Adv}^{PRP}_{\mathsf{Magma}}(\mathcal{A})$$

"Provable security" can't say anything about the upper bound of $\mathrm{Adv}^{PRP}_{\mathsf{Magma}}$

Here we use a heuristic approach:

$$\mathrm{Adv}^{PRP}_{\mathsf{Magma}}(t,q) \lessapprox \max_{\text{all known } \mathcal{A} \text{ with resources}(t,q)} \mathrm{Adv}^{PRP}_{\mathsf{Magma}}(\mathcal{A})$$

Methods that uses "free precomputations" are excluded from the consideration

PRP-security of Magma

Four methods:

1. key recovery attack: bruteforce
2. key recovery attack: "reflection" [Isobe, 2011]
3. key recovery attack: "fixed point" [Dinur, Dunkelman, Shamir, 2011]
4. distinguishing attack "reflection"+"fixed point" [Kara, Karakoc, 2012]

The general from of the heuristic estimation is $\mathrm{Adv}^{PRP}_{\mathsf{Magma}}(t,q) \lessapprox$

$$\lessapprox \max_{t_1+t_2+t_3=t}\left(\underbrace{\frac{t_1}{2^{256}}}_{(1)}, \underbrace{\min\left(\frac{q}{2^{32}}, \frac{t_2}{2^{224}}\right)}_{(2)}, \underbrace{\min\left(\frac{q}{2^{64}}, \frac{t_3}{2^{192}}\right)}_{(3)},\right) + \underbrace{\min\left(2^{-32}, \frac{q}{2^{64}}\right)}_{(4)}$$

Simplify for $t \ll 2^{192}$ and arbitrary $q < 2^{32}$

$$\mathrm{Adv}^{PRP}_{\mathsf{Magma}}(t,q) \lessapprox \frac{t}{2^{192}} + \frac{q}{2^{64}}$$

Estimates of key capacity

The *NAE* model includes both:

– integrity attacks (forgeries);

– privacy attacks (“reading without key” etc.).

For any used Alg the inequality must hold true

$$\mathrm{Adv}_{\mathsf{Alg}}^{\mathit{NAE}}(t, q, v) < \pi = \min(\pi_{\mathrm{enc}}, \pi_{\mathrm{mac}}).$$

π_{enc} – “the maximum allowable probability of successful application of cryptanalysis”

π_{mac} – “the maximum allowable probability of a single forgery”

Technical Committee 26

R 1323565.1.005–2017 – Acceptable amount of data to be processed without key change for particular block cipher modes of operation GOST R 34.13-2015

Estimates of key capacity

For illustrative purposes, we choose $\pi = \min(\pi_{\text{enc}}, \pi_{\text{mac}}) = 2^{-10}$.

We already have:

$l = 2^8$ – packet length (in n-bit block)

$q' = 2^{13}$ – number of packets per derived key

$n = 64$ – block size (in bits)

We choose:

$\kappa = 2^{21}$ – number of derived keys (key pairs)

$q = \kappa \cdot q' = 2^{34}$ – total number of protected packets

We assume that number of forgery attempts ν (resp. ν')
is much less than q (resp. q').

Estimates of key capacity

$$\mathrm{Adv}_{\mathsf{KDF}}^{\mathit{VO\text{-}PRF}} \lessapprox \frac{16 \cdot (\kappa \cdot d)^2}{2^n} = 2^{-12}$$

$$\mathrm{Adv}_{\mathsf{CTR}}^{\mathit{IND-CPNA}} \lessapprox \frac{(q' \cdot l)^2}{2^{n+1}} = 2^{-23}$$

$$\mathrm{Adv}_{\mathsf{CMAC}}^{\mathit{PRF}} \lessapprox \frac{16 \cdot (q')^2}{2^n} = 2^{-34}$$

$$CS \in \{1,3\} : \mathrm{Adv}_{\mathsf{CTR-CMAC}}^{\mathit{NAE}} \approx \mathrm{Adv}_{\mathsf{CTR}}^{\mathit{IND-CPNA}} + \mathrm{Adv}_{\mathsf{CMAC}}^{\mathit{PRF}} \approx \mathrm{Adv}_{\mathsf{CTR}}^{\mathit{IND-CPNA}}$$

$$CS \in \{2,4\} : \mathrm{Adv}_{\mathsf{NULL-CMAC}}^{\mathit{NAE}} \approx \mathrm{Adv}_{\mathsf{CMAC}}^{\mathit{PRF}}$$

Estimates of key capacity

$$\mathrm{Adv}_{\mathsf{KDF}}^{\mathit{VO\text{-}PRF}} \lessapprox \frac{16 \cdot (\kappa \cdot d)^2}{2^n} = 2^{-12}$$

$$\mathrm{Adv}_{\mathsf{CTR}}^{\mathit{IND-CPNA}} \lessapprox \frac{(q' \cdot l)^2}{2^{n+1}} = 2^{-23}$$

$$\mathrm{Adv}_{\mathsf{CMAC}}^{\mathit{PRF}} \lessapprox \frac{16 \cdot (q')^2}{2^n} = 2^{-34}$$

$$CS \in \{1,3\} : \mathrm{Adv}_{\mathsf{CTR-CMAC}}^{\mathit{NAE}} \approx \mathrm{Adv}_{\mathsf{CTR}}^{\mathit{IND-CPNA}} + \mathrm{Adv}_{\mathsf{CMAC}}^{\mathit{PRF}} \approx \mathrm{Adv}_{\mathsf{CTR}}^{\mathit{IND-CPNA}}$$

$$CS \in \{2,4\} : \mathrm{Adv}_{\mathsf{NULL-CMAC}}^{\mathit{NAE}} \approx \mathrm{Adv}_{\mathsf{CMAC}}^{\mathit{PRF}}$$

For KDF and both CS: $\mathrm{Adv} < \pi$.

If we consider each derived key ***separately*** and $\kappa \le 2^{21}$, $q \le 2^{34}$,

then "the protocol is secure".

Estimates of key capacity

If we consider the ***whole protocol and all the keys***, then

$$\mathrm{Adv}_{\mathsf{CRISP}}^{NAE} \leq \mathrm{Adv}_{\mathsf{KDF}}^{VO-PRF} + \kappa \cdot \mathrm{Adv}_{\mathsf{CS}}^{NAE} < \pi$$

and

$$\text{“confidentiality and integrity”} \; CS \in \{1,3\} : \kappa \leq 2^{12},\; q \leq 2^{25}$$

$$\text{“only integrity”} \; CS \in \{2,4\} : \kappa \leq 2^{21},\; q \leq 2^{34}$$

Some ways to increase key capacity

- CTR-ACPKM
- truncating output to $s < n$ bits in CTR
- double CTR (under the same key with different nonces)
- Kuznyechik – with $n = 128$ we obtain “unreachable” $\kappa \leq 2^{54}$

Conclusion

1. Security proof for the CRISP protocol in the relevant threat model

Conclusion

1. Security proof for the CRISP protocol in the relevant threat model
2. List of sufficient requirements for CS used in CRISP:
    1. KDF must be a secure variable-output PRF
    2. CS used with the same master key must have the same KDF
    3. Encryption and MAC must form a secure deterministic AEAD-scheme

Conclusion

1. Security proof for the CRISP protocol in the relevant threat model
2. List of sufficient requirements for CS used in CRISP:
    1. KDF must be a secure variable-output PRF
    2. CS used with the same master key must have the same KDF
    3. Encryption and MAC must form a secure deterministic AEAD-scheme
3. The existing cipher suites satisfy all the specified requirements

Conclusion

1. Security proof for the CRISP protocol in the relevant threat model
2. List of sufficient requirements for CS used in CRISP:
    1. KDF must be a secure variable-output PRF
    2. CS used with the same master key must have the same KDF
    3. Encryption and MAC must form a secure deterministic AEAD-scheme
3. The existing cipher suites satisfy all the specified requirements
4. Motivated recommendations on the key capacity

Thank you for attention!

Questions?