Autenticazione avanzata nei pagamenti

MASSIMILIANO SALA – UNIVERSITÀ DI TRENTO

ABI CARTE 2013 – APPAGAMENTI PER I CLIENTI

METODOLOGIE E SISTEMI DI SICUREZZA EVOLUTI PER NUOVE SOLUZIONI DI PAGAMENTO

5. 12. 2013

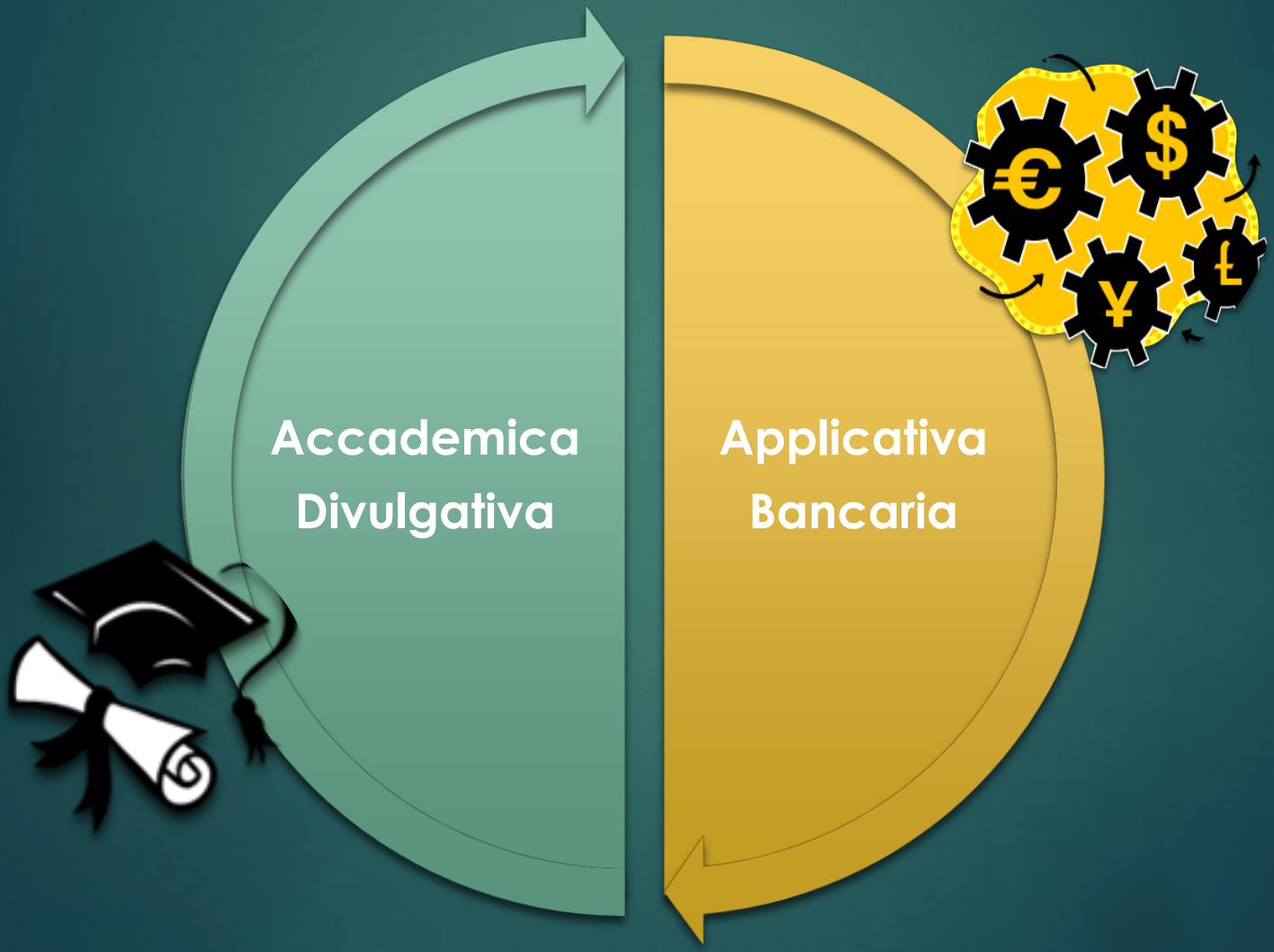
CryptoLabTN

Il Dipartimento di Matematica dell'Università di Trento ha costituito nel 2010 il

Laboratorio di Matematica Industriale e Crittografia

come motore di innovazione alimentato dalle competenze scientifiche del Dipartimento

Attività del **CryptoLabTN**



Attività del **CryptoLabTN**

- **RICERCA** accademica
- Pubblicazioni scientifiche
- Corsi di **LAUREA**
- Corsi per aziende e professionisti
- **KNOWLEDGE TRANSFER**

Knowledge Transfer

Settore Militare e Governativo

Presidenza del Consiglio dei Ministri

Ministero della Difesa

Altri

Settore Bancario

Attività del **CryptoLabTN**

- **VALUTAZIONI** di sicurezza (analisi del rischio e delle minacce)
- Confronto e creazione di **ALGORITMI**
- Sviluppo di **PROTOTIPI**

Valutazioni

Le nostre esperienze

- meccanismi di autenticazione (anche per mobile banking)
- e-payments
- sistemi di pagamento avanzato
- sicurezza transazioni interbancarie
- protezione dei dati sanitari

Algoritmi

Le nostre esperienze

- cifrari per **online banking**
- cifrare per il cloud
- generazione di chiavi forti
- high level security

Sviluppo di prototipi

Ultimi prototipi sviluppati

- autenticazione forte per online banking
- riconoscimento di firme su assegni
- firme biometriche

Security e Authentication

Autenticazione remota

Esempi:

- Internet payments
- home banking
- accesso a dati della pubblica amministrazione (per es. dati sanitari)

BCE: Recommendation for the security of Internet payments (31st Jan 2013)

"The use of two or more of the following elements – categorised as knowledge, ownership and inherence – is required:

- something only the user *knows* (e.g. password, PIN)
- something only the user *possesses* (e.g. token, smartcard mobile phone)
- something the user *is* (e.g. biometric characteristic)

The elements selected must be mutually independent."

BCE: Recommendation for the security of Internet payments (31st Jan 2013)

"The use of two or more of the following elements – categorised as knowledge, ownership and inherence – is required:

- something only the user *knows* (e.g. password, PIN)
- something only the user *possesses* (e.g. token, smartcard mobile phone)
- something the user *is* (e.g. biometric characteristic)

The elements selected must be mutually independent."

"The recommendations should be implemented by PSPs and governance authorities of payment schemes by **1 February 2015**."

Sistemi di autenticazione

Valutazioni fatte dal CryptoLabTN:

- Professionali (settore bancario, pubblica amministrazione)
- Accademiche (progetti a lunga durata)

Sistemi di autenticazione

Valutazioni fatte dal CryptoLabTN:

- Professionali (settore bancario, pubblica amministrazione)
- Accademiche (progetti a lunga durata)

TITAN: progetto con Poste Italiane (15 milioni €)

Sistemi di autenticazione

Metodi consolidati

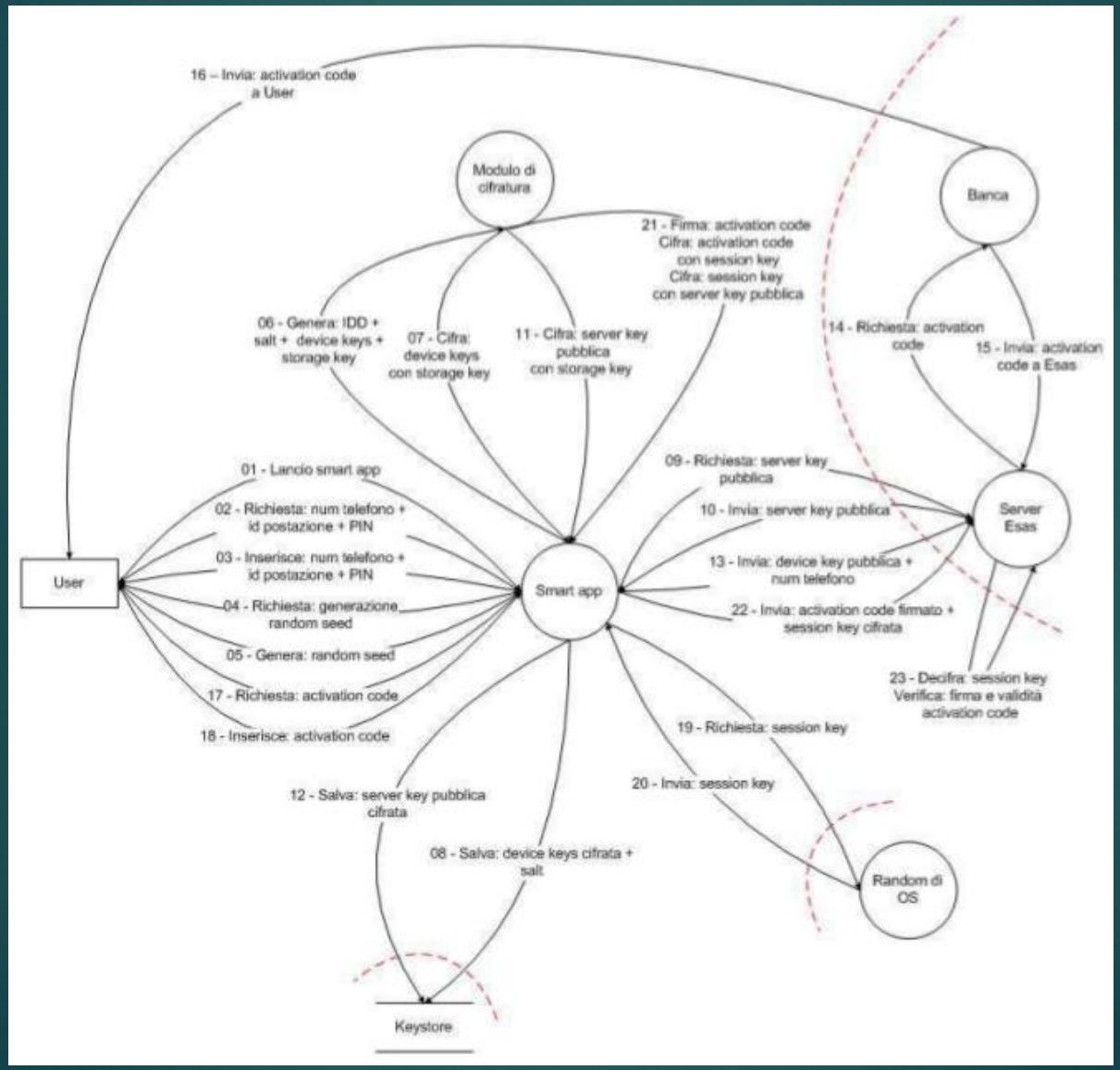
- OTP tramite SMS
- Scheda codici di tipo “battaglia navale”
- Token fisico OTP

Metodi “smart”

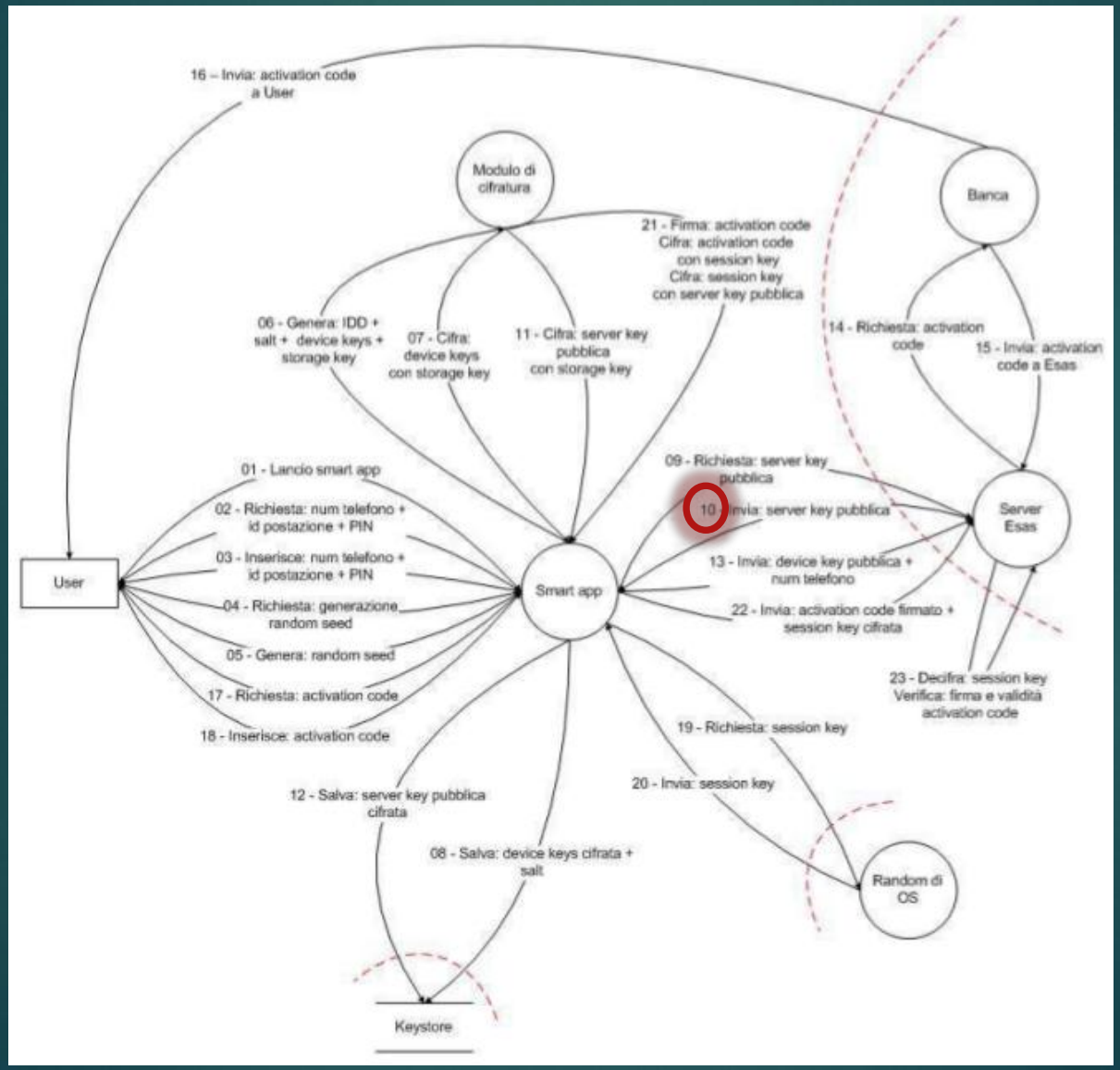
- Soft token
- OTP tramite notifiche push
- OTP con conferma dati transazione

Metodologia: Rischio e Contromisure

STRIDE

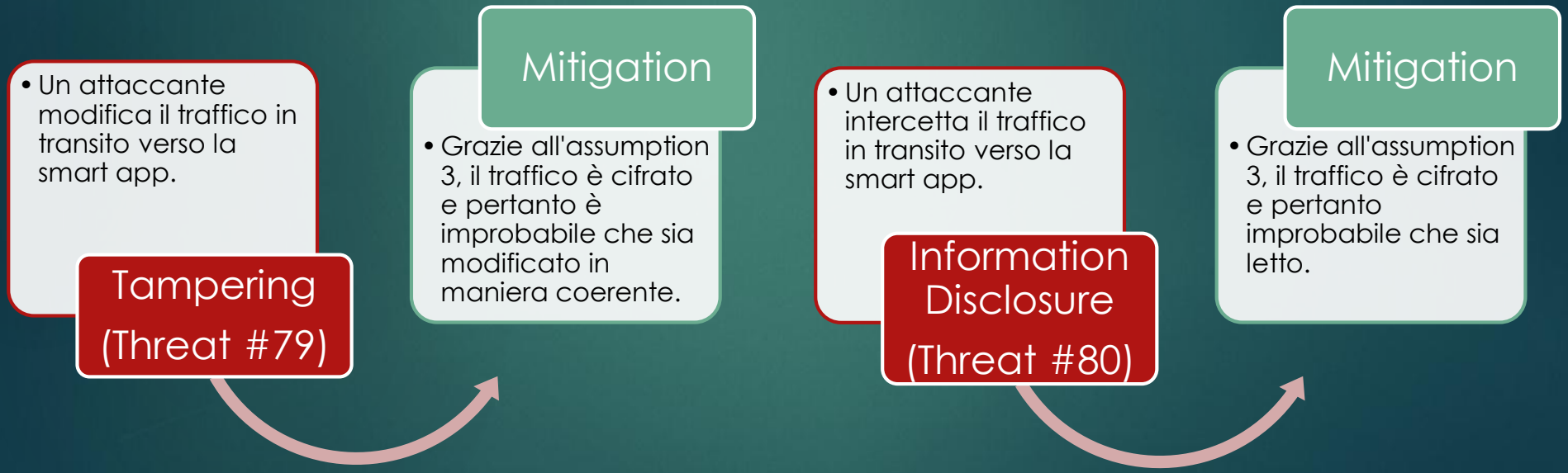

16 – Invia: activation code a User
Modulo di cifratura
Banca
21 - Firma: activation code
Cifra: activation code con session key
Cifra: session key con server key pubblica
06 - Genera: IDD + salt + device keys + storage key
07 - Cifra: device keys con storage key
11 - Cifra: server key pubblica con storage key
14 - Richiesta: activation code
15 - Invia: activation code a Esas
01 - Lancio smart app
02 - Richiesta: num telefono + id postazione + PIN
03 - Inserisce: num telefono + id postazione + PIN
04 - Richiesta: generazione random seed
05 - Genera: random seed
17 - Richiesta: activation code
18 - Inserisce: activation code
User
Smart app
09 - Richiesta: server key pubblica
10 - Invia: server key pubblica
13 - Invia: device key pubblica + num telefono
22 - Invia: activation code firmato + session key cifrata
Server Esas
23 - Decifra: session key
Verifica: firma e validità activation code
19 - Richiesta: session key
20 - Invia: session key
12 - Salva: server key pubblica cifrata
08 - Salva: device keys cifrata + salt
Random di OS
Keystore

STRIDE

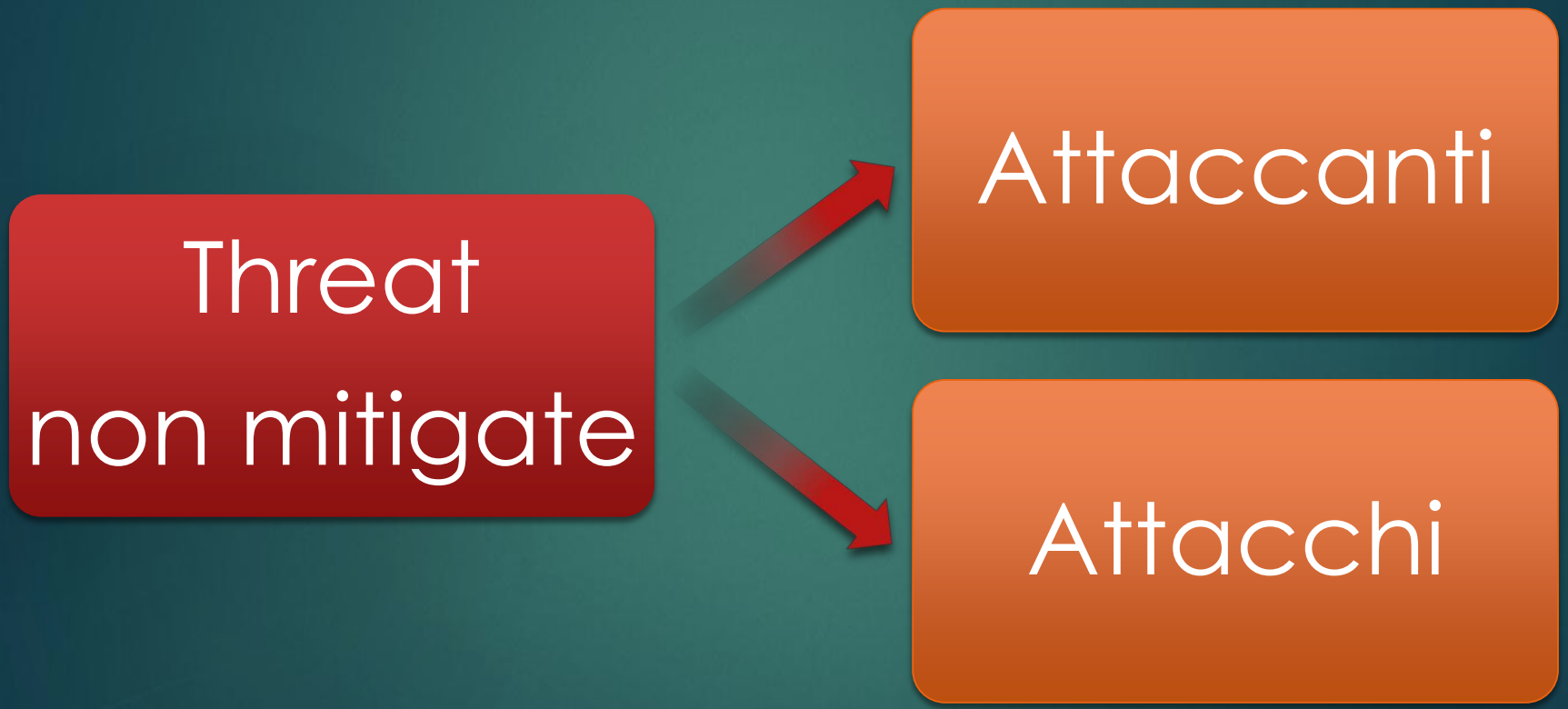

16 – Invia: activation code a User
Modulo di cifratura
Banca
21 - Firma: activation code
Cifra: activation code con session key
Cifra: session key con server key pubblica
06 - Genera: IDD + salt + device keys + storage key
07 - Cifra: device keys con storage key
11 - Cifra: server key pubblica con storage key
14 - Richiesta: activation code
15 - Invia: activation code a Esas
01 - Lancio smart app
09 - Richiesta: server key pubblica
10 - Invia: server key pubblica
Server Esas
02 - Richiesta: num telefono + id postazione + PIN
03 - Inserisce: num telefono + id postazione + PIN
User
Smart app
13 - Invia: device key pubblica + num telefono
04 - Richiesta: generazione random seed
22 - Invia: activation code firmato + session key cifrata
05 - Genera: random seed
23 - Decifra: session key
Verifica: firma e validità activation code
17 - Richiesta: activation code
18 - Inserisce: activation code
19 - Richiesta: session key
20 - Invia: session key
12 - Salva: server key pubblica cifrata
08 - Salva: device keys cifrata + salt
Random di OS
Keystore

STRIDE: Threat/Mitigation

Threats against 10 - Invia: server key pubblica



STRIDE



Punteggio OWASP-like

Impatti tecnici

	VALORI PER COPPIE ATTACCHI/ATTACCANTI					
	don/sniff	don/crack	mal/sniff	mal/crack	fisico/prox	fisico/thief
RISERVATEZZA	5	5	5	5	7	8
RILEVANZA	9	9	9	9	6	6
RESPONSABILITÀ	7	7	9	9	2	5
PUNTEGGIO MEDIO	7.00	7.00	7.67	7.67	5.00	6.33

Appetibilità

	VALORI PER COPPIE ATTACCHI/ATTACCANTI					
	don/sniff	don/crack	mal/sniff	mal/crack	fisico/prox	fisico/thief
ABILITÀ	7	9	7	9	9	1
OPPORTUNITÀ	5	7	5	7	8	4
MOTIVAZIONE	9	9	9	9	8	7
DIMENSIONE	4	1	4	1	5	6
PUNTEGGIO MEDIO	6.25	6.50	6.25	6.50	7.50	4.50

Vulnerabilità

	VALORI PER COPPIE ATTACCHI/ATTACCANTI					
	don/sniff	don/crack	mal/sniff	mal/crack	fisico/prox	fisico/thief
SCOPERTA	7	9	7	9	3	0
CONSAPEVOLEZZA	6	9	6	9	5	1
SFRUTTAMENTO	1	2	1	2	8	1
INTRUSIONI	1	1	5	5	8	4
PUNTEGGIO MEDIO	3.75	5.25	4.75	6.25	6.00	1.50

Sommario

	VALORI PER COPPIE ATTACCHI/ATTACCANTI					
	ATTACCHI MASSIVI				ATTACCHI LOCALI	
	don/sniff	don/crack	mal/sniff	mal/crack	fisico/prox	fisico/thief
APPETIBILITÀ	6.25	6.5	6.25		7.5	4.5
VULNERABILITÀ	3.75	5.25	4.75	6	6	1.5
IMPATTI TECNICI	7	7	7.67	7.67	5	6.33
PUNTEGGIO MEDIO	5.67	6.25	6.22	6.81	6.17	4.11

6.81

6.17

BITCOIN

L'EVOLUZIONE NATURALE DEL DENARO

Attività Bitcoin **CryptoLabTN** 2013

Eventi accademici

- Bolzano 15/5
- Verona 28/5

Knowledge Transfer

- *Bitcoin: the currency of the future*
  Trento 10/6

Eventi mainstream

- *European Electronic Crime Task Force*
  Roma 5/11

European Electronic Crime Task Force

SWOT: Strengths and Weaknesses

Strengths

- Irreversibilità
- Scripting
- Costi di transazione prossimi a zero

Weaknesses

- Lentezza nel confermare le transazioni – fino a dieci minuti
- In caso di furto della chiave privata, le perdite sono totali ed irreversibili

SWOT: Opportunities and Threats

Opportunities

- Numero limitato di bitcoin (“oro digitale”)
- Digitale dalla nascita (intrinsecamente sicuro?)
- Pseudo-anonimità: gli utenti non possono essere facilmente identificati dal loro indirizzo Bitcoin

Threats

- Nessuna autorità centrale
- Pseudo-anonimità: gli utenti non possono essere facilmente identificati dal loro indirizzo Bitcoin

Grazie dell'attenzione!

HTTP://WWW.SCIENCE.UNITN.IT/~SALA/